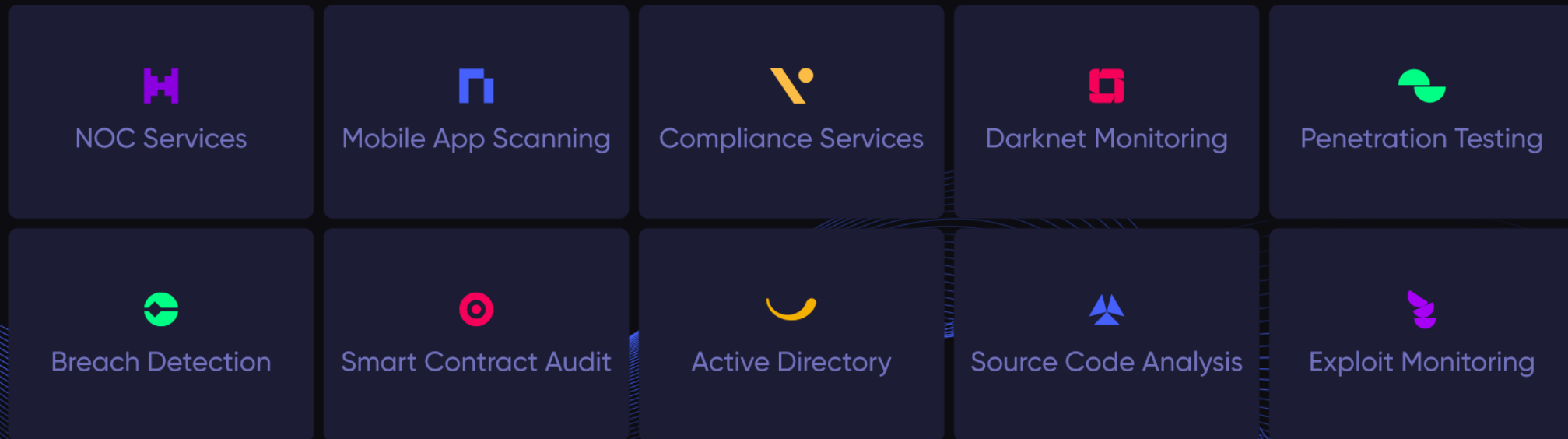


CRYEYE



CRYEYE - Fortifying Your Digital Horizon

CRYEYE is a trailblazing cloud-based solution that redefines cybersecurity through continuous deep audits and robust security monitoring. This all-in-one SaaS cybersecurity platform seamlessly integrates an array of tools, offering an encompassing suite of services. Embrace automated vulnerability detection spanning servers, websites, mobile applications, source code, and cloud solutions. The platform's automated security auditing boasts a diverse range of integrations, encompassing both commercial and open-source tools for thorough scans of internal and external assets.



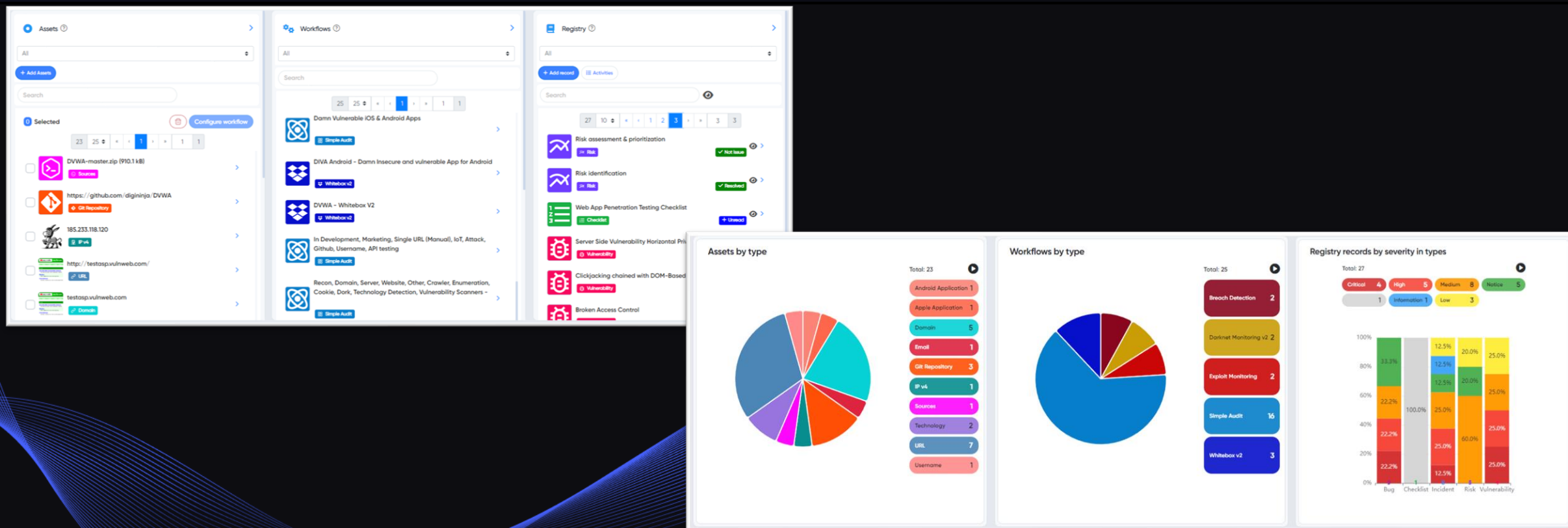
WORKSPACES - Your Agile Hub for Success!

Dive into our Cloud Platform, enabling users to effectively manage individual projects with customizable goals, conduct thorough security audits, capture valuable insights with notes, and create comprehensive checklists for streamlined productivity and growth.

The screenshot displays the Cryeye Workspaces interface. On the left is a dark sidebar with the Cryeye logo and navigation options: 'Workspaces System', 'Realm', 'Pinned', 'Assets', 'Vulnerable Project', 'Digital Defence', 'Support', 'Docs', 'Sign Out', and 'Demo'. The main content area is titled 'Workspaces' and includes a search bar, a '+ Create workspace' button, and 'Activities' and 'Notifications' tabs. A grid of workspace cards is shown, each with a title, icon, and asset tags. The cards include: 'Vulnerable Project' (a year ago, Default, Pinned), 'Assets' (6 months ago, Pinned, Owner), 'Digital Defence' (a day ago), 'Security team' (5 months ago, Owner), 'Exploit monitoring' (a year ago, Owner), 'SOC service' (a year ago, Owner), 'Whitebox' (a year ago, Owner), 'Demonstration' (a year ago), and 'Demo' (2 years ago, Owner). Each card lists associated assets such as 'Technology', 'IP v4', 'Keyword', 'URL', 'Android Application', 'Apple Application', 'Email', 'Git Repository', 'Source', and 'URL'.

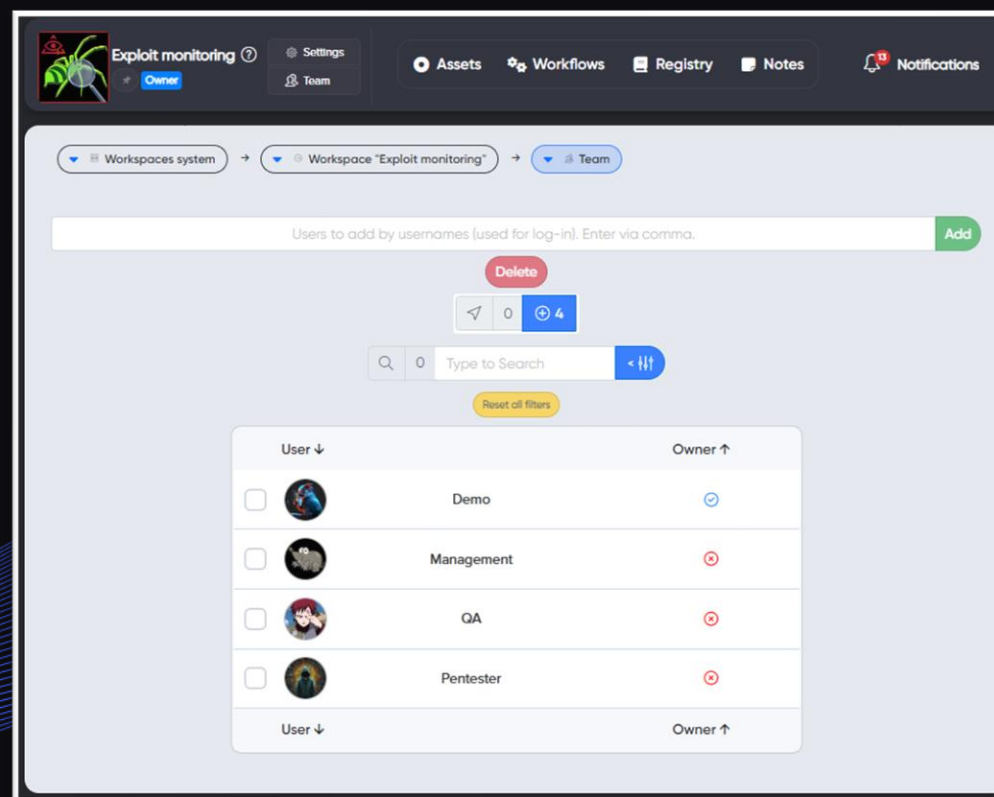
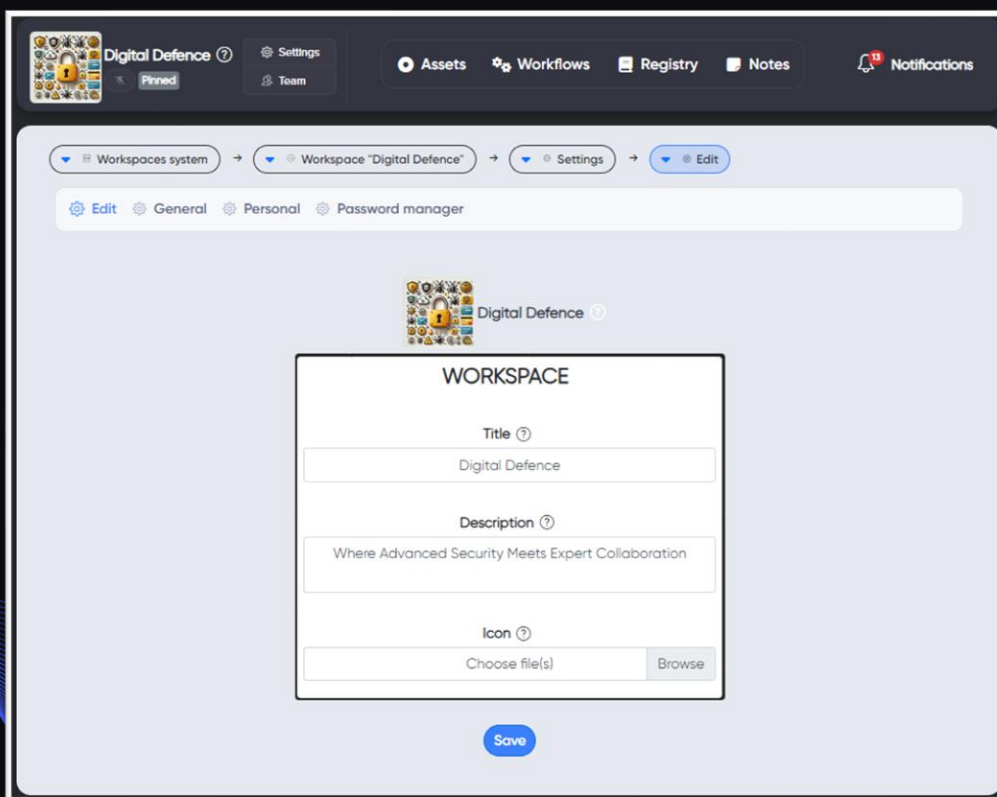
WORKSPACES

Immerse yourself in a world of possibilities! Our Cloud Platform introduces an array of asset types within every Workspace. Explore URLs, IPs, Android and Apple Applications, Git Repositories, Dockerfiles, Docker Images, AWS CloudFormation, Azure Resource Manager, Emails, Phone Numbers, Keywords, Kubernetes, Terraform, Technology, and more – all at your disposal for comprehensive project management and innovation.



WORKSPACES

Each Workspace is a canvas waiting for your touch – personalize it with a name, description, and image that resonate with your project's essence. Moreover, our Workspace system thrives on collaboration, uniting developers, security specialists, QA experts, management, and more. Seamlessly integrate users, team members, clients, and customers, fostering a shared environment that fuels innovation and success.

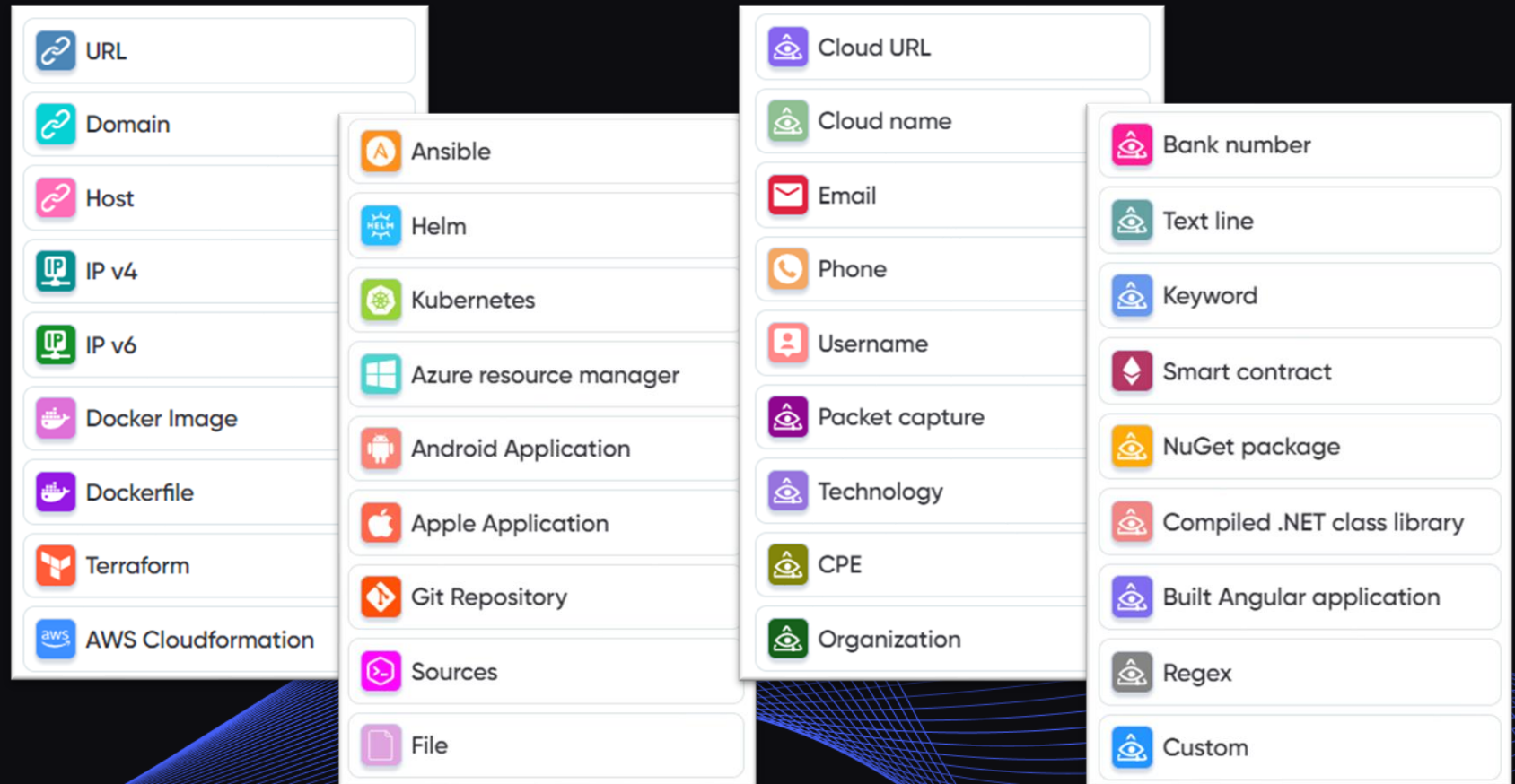


Assets Management

You can add a many different asset types to your Workspace for scanning by the audit system to find vulnerabilities, misconfigurations, information leaks, etc.

Assets categories

Web, Infrastructure, Mobile, Source Code Analysis, Binary Analysis, Recon, Network Forensics, Names, Titles or Identifications and other.



WORKSPACES

Configure workflow x

Configure workflow for selected assets.
With creating related project, if needed.

Select Service Type

- Uptime monitoring
- Singular target audit project
- Simple audit
Only make audits. With results, facts, solutions.
- Breach detection
Detect breaches.
- Darknet monitoring
Monitor feeds from forums, blogs, etc.

☰ Continue

Navigate to the “Assets” Tab. Here, you have the power to add your objectives effortlessly. For instance, by selecting the 'URL' objective type, you can input individual objectives, a list of multiple assets, or even upload a file with items.

Select asset type

Search

- URL
- Domain
- Host
- IP v4
- IP v6
- Docke Image

Create URL asset(-s) ?

Please, separate several items by Coma

https://example.com Add

Drag and drop files to here to upload.
or

+ Select file

This stage offers a dual purpose – you can either seamlessly add objectives that will appear in the “Assets” tab, ready for further actions, or take it a step further by directly creating projects. Send objectives for Breach Detection, Darknet Monitoring, Whitebox Analysis, Uptime Monitoring, and beyond – all within your grasp.

NOC - Uptime Monitoring

NOC is a tool designed to empower you with real-time insights into your asset availability. This powerful feature allows you to effortlessly track the uptime of your assets. By adding supported assets to your Workspace and connecting them to Uptime Monitoring, you gain a comprehensive view of their accessibility status.

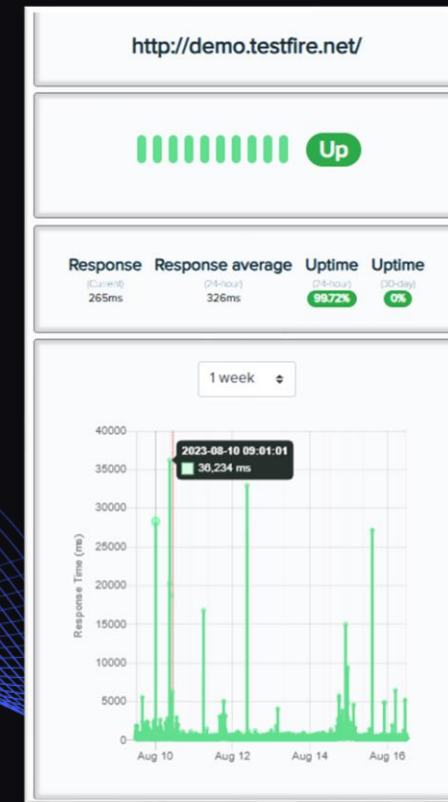
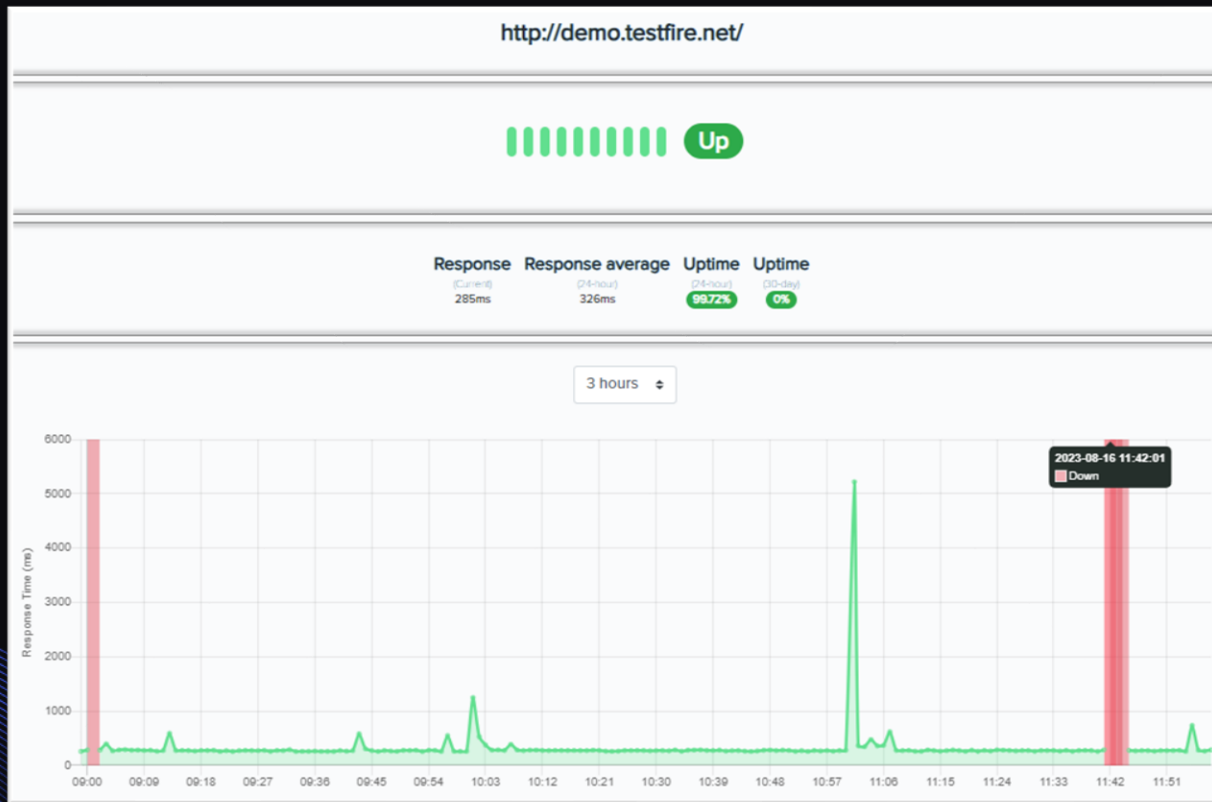
Current Status ↓	Asset ↓	Monitor Type ↓	Heartbeats	Response ↓	24Hr Average Response ↓	24Hr Availability ↓	Time Since Last Check ↓
Down	zero.webappsecurity.com	Ping (ICMP)		N/A	N/A	0%	3 minutes ago
Down	http://testaspnet.vulnweb.com/	HTTP(s)		377ms	695ms	0%	a minute ago
Up	185.233.118.120	Ping (ICMP)		33ms	32ms	99.31%	2 minutes ago
Up	testphp.vulnweb.com	Ping (ICMP)		155ms	155ms	99.31%	2 minutes ago
Up	demo.testfire.net	Ping (ICMP)		124ms	124ms	99.17%	2 minutes ago
Up	8.8.8.8	Ping (ICMP)		1ms	1ms	99.31%	2 minutes ago
Up	testaspnet.vulnweb.com	Ping (ICMP)		148ms	148ms	99.31%	a minute ago
Up	testasp.vulnweb.com	Ping (ICMP)		148ms	148ms	99.31%	a minute ago
Up	google.com	Ping (ICMP)		1ms	1ms	98.47%	a few seconds ago
Up	http://demo.testfire.net/	HTTP(s)		315ms	690ms	99.79%	a minute ago
Up	http://testasp.vulnweb.com/	HTTP(s)		383ms	699ms	99.93%	a minute ago
Disabled	http://zero.webappsecurity.com/	HTTP(s)		N/A	N/A	0%	-
Disabled	http://testphp.vulnweb.com/	HTTP(s)		N/A	N/A	0%	-

The image shows a configuration interface for an uptime monitor. It is divided into two main sections: 'GENERAL CONFIG' and 'SPECIFIC CONFIG'.
In the 'GENERAL CONFIG' section:
- 'Type' is set to 'HTTP(s)'.
- 'Is enabled' is checked with a blue checkbox.
- 'Heartbeat interval' is set to 60 seconds.
- 'Retries amount' is set to 0.
- 'Is upside down' is unchecked.
In the 'SPECIFIC CONFIG' section:
- 'Accepted status codes' is set to 'required'.
- 'Method' is set to 'GET'.
- 'Body' and 'Headers' fields are empty.

We regularly assess the condition of your assets, akin to checking their 'heartbeat.' The 'pulse' varies depending on the selected monitor type. Whether it's HTTP(s), Ping (ICMP), Socket, or Push monitors, you have the flexibility to tailor your monitoring strategy. With shared and individual settings, including customizable status codes for HTTP(s) monitors, you can fine-tune each asset monitor. Control request methods, intervals, request bodies, and more.

NOC - Uptime Monitoring

Delve into the world of statistics powered by 'heartbeat checks,' granting you the ability to monitor asset availability trends. Discover key insights, such as the average availability of a resource over 24 hours or 30 days, along with the average response time if applicable. Visualize your asset's availability statistics through intuitive diagrams. Access diagrams covering periods like the last hour, 3 hours, 24 hours, and 1 week.



NOC - Uptime Monitoring

When assets experience downtime or restoration, we capture these moments as pivotal 'Border Events.' This ensures that you are never in the dark about asset status changes while you're immersed in other tasks. Through 'NOC: UPTIME MONITORING,' you gain the ability to observe your assets in real-time. With default sorting in the table, assets encountering downtime are automatically prioritized, moving to the top of the list. Conversely, when asset monitoring is disabled, it is listed at the bottom. Additionally, you can monitor key monitor metrics. Embrace ultimate control with the capability to enable/disable monitors, manage associations, and even clear the history of pulse checks and border events for specific assets.

Icon	Title	Availability	DateTime	Message
	http://demo.testfire.net/	Up	13 minutes ago	200 - OK
	http://demo.testfire.net/	Down	16 minutes ago	ClientConnectorError: Cannot connect to host demo.testfire.net:80 ssl:False [Connect call failed ('65.61.137.117', 80)]
	http://testphp.vulnweb.com/	Up	an hour ago	200 - OK
	http://testhtml5.vulnweb.com/	Up	an hour ago	200 - OK
	http://testhtml5.vulnweb.com/	Down	an hour ago	TimeoutError:
	http://testphp.vulnweb.com/	Down	an hour ago	TimeoutError:
	http://testphp.vulnweb.com/	Up	2 hours ago	200 - OK
	http://testphp.vulnweb.com/	Up	2 hours ago	200 - OK
	http://testhtml5.vulnweb.com/	Up	2 hours ago	200 - OK
	http://testhtml5.vulnweb.com/	Up	2 hours ago	200 - OK

The control panel features a summary bar at the top with 'Up 10' and 'Down 4' indicators. Below this is a 'Monitors' section with a horizontal bar containing a green '+' button, a blue play button, a red pause button, and a red trash button. Underneath are two buttons: a grey one with a location pin icon and '0', and a blue one with a plus icon and '14'. At the bottom is a search bar with a magnifying glass icon, '0' results, the text 'Type to Search', and a blue button with a left arrow and a vertical double-headed arrow icon.

NOC - Uptime Monitoring

Introducing a seamless reporting feature where users can effortlessly export customized reports for any chosen asset from the list. Reports are generated in CSV format, ensuring compatibility and ease of use. With the export configuration window, tailor your report by selecting the fields that matter most to you. A simple click on the 'Export' button below initiates the process.

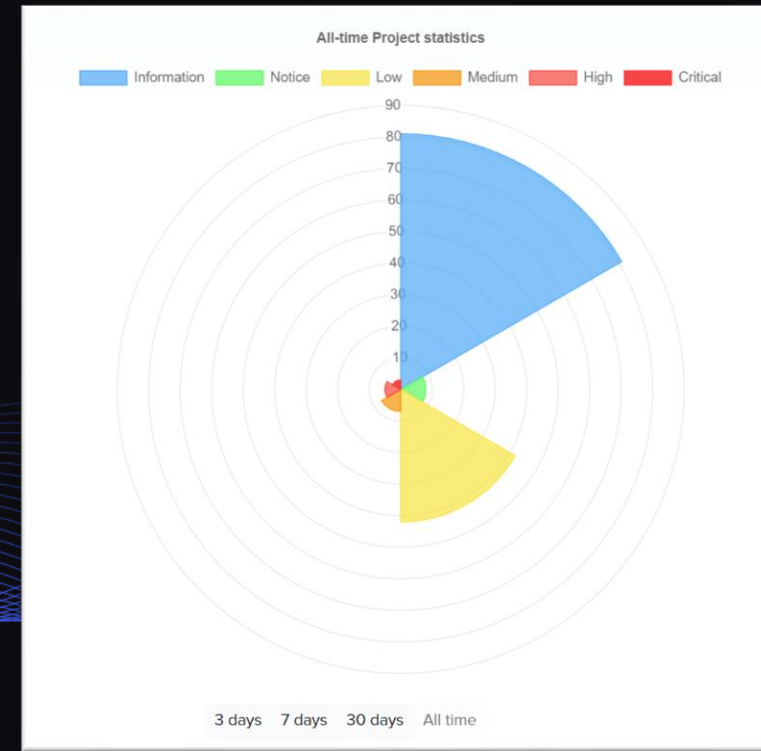
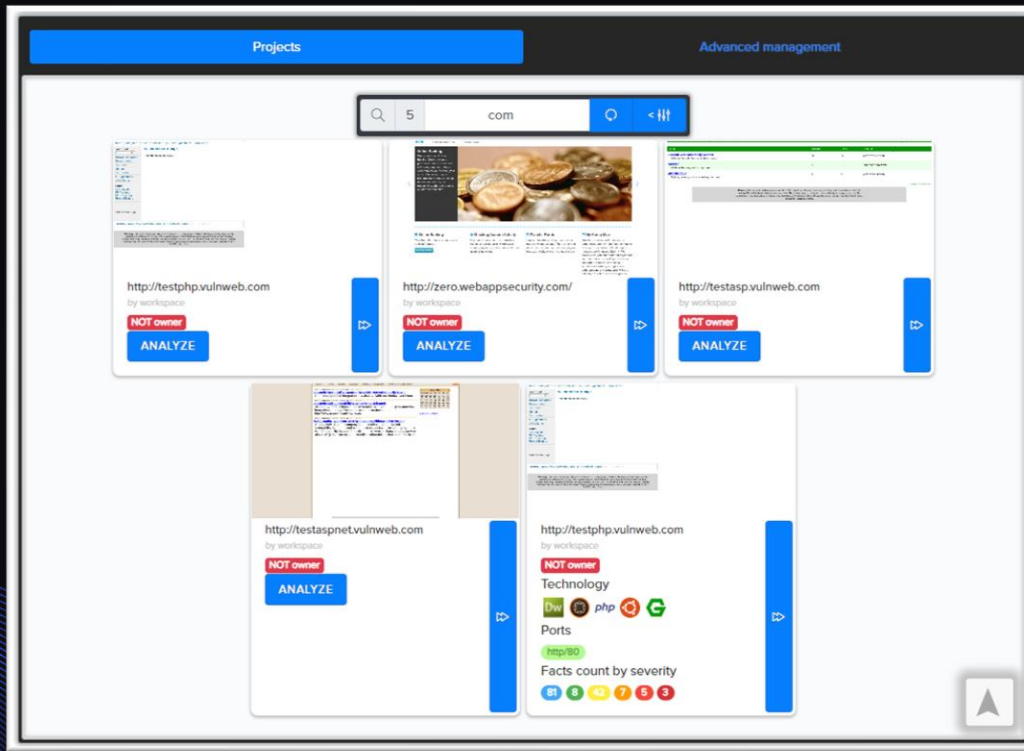
Icon	Title ↓	Availability ↓	DateTime ↑	Message ↓	Add to registry	Details
	http://185.233.118.120:666/	Down	5 days ago	ServerDisconnectedError: Server disconnected	Create Incident	
	185.233.118.120	Down	5 days ago	TimeoutError:	Create Incident	
	testaspnet.vulnweb.com	Down	5 days ago	TimeoutError:	Create Incident	
	demo.testfire.net	Up	5 days ago	Ok	Create Incident	
	demo.testfire.net	Up	6 days ago	Ok	Create Incident	
	http://185.233.118.120:8080/	Down	6 days ago	ServerDisconnectedError: Server disconnected	Create Incident	
	http://185.233.118.120:666/	Down	7 days ago	ServerDisconnectedError: Server disconnected	Create Incident	
	http://185.233.118.120:666/	Down	7 days ago	ServerDisconnectedError: Server disconnected	Create Incident	
	http://185.233.118.120:666/	Down	7 days ago	ServerDisconnectedError: Server disconnected	Create Incident	
	http://185.233.118.120:666/	Down	7 days ago	ServerDisconnectedError: Server disconnected	Create Incident	

	A	B	C	D	E	
1	UID	Config UID	Title	Availability	DateTime	Message
2	0189d9c9-2197-b17e-7503-e337dcec2df3	01887c62-c4bc-8ceb-2542-2fe8a7a53cd6	http://demo.testfire.net/	0 Down	2023-08-09T10:13:01.274965Z	ClientConnectorError: Cannot connect to host
3	0189d9ca-1641-a0f9-dd05-fece73d31e8c	01887c62-c4bc-8ceb-2542-2fe8a7a53cd6	http://demo.testfire.net/	2 Up	2023-08-09T10:14:01.275775Z	200 - OK
4	0189db4a-b4ed-1bc2-8a85-b92b5e3d855e	01887c62-c4bc-8ceb-2542-2fe8a7a53cd6	http://zero.webappsecurity.com/	0 Down	2023-08-09T17:14:01.385632Z	ClientConnectorError: Cannot connect to host
5	0189db4b-962d-2394-8009-52fd50d6a4d2	01887c62-c4bc-8ceb-2542-2fe8a7a53cd6	http://zero.webappsecurity.com/	2 Up	2023-08-09T17:15:01.395860Z	200 - OK
6	0189dd47-9e51-a461-c913-9b2509802c3d	01887c62-c4bc-8ceb-2542-2fe8a7a53cd6	http://demo.testfire.net/	0 Down	2023-08-10T02:30:01.500324Z	ClientConnectorError: Cannot connect to host
7	0189dd48-9c66-c0e3-bb92-9dbf527de444	01887c62-c4bc-8ceb-2542-2fe8a7a53cd6	http://demo.testfire.net/	2 Up	2023-08-10T02:31:01.466722Z	200 - OK
8	0189dd49-77c2-7aea-03d7-21a4271835e3	01887c62-c4bc-8ceb-2542-2fe8a7a53cd6	http://demo.testfire.net/	0 Down	2023-08-10T02:32:01.462514Z	ClientConnectorError: Cannot connect to host
9	0189dd4a-6c00-217c-5b42-5ae53ef4d057	01887c62-c4bc-8ceb-2542-2fe8a7a53cd6	http://demo.testfire.net/	2 Up	2023-08-10T02:33:01.493492Z	200 - OK
10	0189ddb5-97e5-0248-c0e7-b76ec288b4b1	01887c62-c4bc-8ceb-2542-2fe8a7a53cd6	http://zero.webappsecurity.com/	0 Down	2023-08-10T04:30:01.532725Z	ClientConnectorError: Cannot connect to host
11	0189ddb6-8096-f10c-9706-0486bab98b29	01887c62-c4bc-8ceb-2542-2fe8a7a53cd6	http://zero.webappsecurity.com/	2 Up	2023-08-10T04:31:01.541614Z	200 - OK
12	0189ddb8-c3ce-7f15-36be-4d07ae4754ec	01887c62-c4bc-8ceb-2542-2fe8a7a53cd6	http://zero.webappsecurity.com/	0 Down	2023-08-10T04:38:01.456905Z	ClientConnectorError: Cannot connect to host
13	0189ddb9-4b0f-727f-0117-66e2959723bd	01887c62-c4bc-8ceb-2542-2fe8a7a53cd6	http://zero.webappsecurity.com/	2 Up	2023-08-10T04:39:01.335780Z	200 - OK
14	0189ddb1-2404-3696-7d1b-92788afa5fab	01887c62-c4bc-8ceb-2542-2fe8a7a53cd6	http://demo.testfire.net/	0 Down	2023-08-10T05:46:01.577641Z	ClientConnectorError: Cannot connect to host
15	0189dd1c-14b9-8ef8-5153-18e298ee81dd	01887c62-c4bc-8ceb-2542-2fe8a7a53cd6	http://demo.testfire.net/	2 Up	2023-08-10T05:47:01.642277Z	200 - OK
16	0189de02-63cf-1ed7-f434-01441d2d8ed7	01887c62-c4bc-8ceb-2542-2fe8a7a53cd6	http://demo.testfire.net/	0 Down	2023-08-10T05:54:01.635787Z	ClientConnectorError: Cannot connect to host
17	0189de03-634f-3786-eb91-10a29afaa9cc	01887c62-c4bc-8ceb-2542-2fe8a7a53cd6	http://demo.testfire.net/	2 Up	2023-08-10T05:55:01.434185Z	200 - OK
18	0189de08-0443-770e-8b8d-0c7fe14232e1	01887c62-c4bc-8ceb-2542-2fe8a7a53cd6	http://demo.testfire.net/	0 Down	2023-08-10T06:00:01.569975Z	ClientConnectorError: [Errno 104] Connection reset b
19	0189de09-4bf0-727f-0117-66e2959723bd	01887c62-c4bc-8ceb-2542-2fe8a7a53cd6	http://demo.testfire.net/	2 Up	2023-08-10T06:01:01.715203Z	200 - OK
20	0189de16-6411-cb22-4908-bb758918f60a	01887c62-c4bc-8ceb-2542-2fe8a7a53cd6	http://zero.webappsecurity.com/	0 Down	2023-08-10T06:15:01.498751Z	TimeoutError:
21	0189de1f-1dba-92a8-e8f1-86ace16da05c	01887c62-c4bc-8ceb-2542-2fe8a7a53cd6	http://zero.webappsecurity.com/	2 Up	2023-08-10T06:25:01.468616Z	200 - OK
22	0189de3d-ed3b-348b-9144-609374f97a71	01887c62-c4bc-8ceb-2542-2fe8a7a53cd6	http://demo.testfire.net/	0 Down	2023-08-10T06:59:01.487581Z	ClientConnectorError: Cannot connect to host
23	0189de3f-0962-56ca-b37e-fbe76cbf13b	01887c62-c4bc-8ceb-2542-2fe8a7a53cd6	http://demo.testfire.net/	2 Up	2023-08-10T07:00:01.030413Z	200 - OK
24	0189de3f-bb96-b7a3-9b0b-28c438f778c4	01887c62-c4bc-8ceb-2542-2fe8a7a53cd6	http://demo.testfire.net/	0 Down	2023-08-10T07:01:01.428449Z	ClientConnectorError: Cannot connect to host
25	0189de41-9f3f-32d6-6a9d-70e528d9d069	01887c62-c4bc-8ceb-2542-2fe8a7a53cd6	http://demo.testfire.net/	2 Up	2023-08-10T07:03:01.451367Z	200 - OK
26	0189de62-85fc-05e6-0f99-e1ae5a83868c	01887c62-c4bc-8ceb-2542-2fe8a7a53cd6	http://demo.testfire.net/	0 Down	2023-08-10T07:39:01.514285Z	ClientConnectorError: Cannot connect to host
27	0189de7d-45d3-47b7-4183-544abb118149	01888c11-495a-55b9-62d2-b9bb14f320b9	http://testhtml5.vulnweb.com/	0 Down	2023-08-10T08:08:01.590405Z	Status 500 is not allowed
28	0189de7e-2e18-369d-72a4-f8ecad0b439	01887c62-c4ad-6a30-c355-1ee329575d9a	http://testphp.vulnweb.com/	0 Down	2023-08-10T08:09:00.840614Z	Status 500 is not allowed

Singular Audits

Singular Audits introduce a dedicated domain within which each target undergoes analysis within its individual project space.

Here, every project boasts its own set of customizable Settings, an intuitive Notes system, a comprehensive Reporting infrastructure, and statistics. The power of singular focus, backed by robust features, takes your analysis experience to a new level.



Singular Audits

Options

Cookies

Extra

Extra settings

Extra settings. As other headers and blocked paths

SAVE

Use Request Manager

Allow to inject cookies, headers and exclude paths from scans

User Agent

Basic Auth

ADD EXTRA HEADERS

ADD EXCLUDED PATH

Singular Audits bring you the power to personalize headers and conduct scans with authentication, effortlessly transferring cookies or Auth tokens.

Moreover, Cryeye scans offer an adaptable audit scheduling mechanism, ensuring audits are launched according to your preferences.

Set scheduler

Trigger type

Repeatable Advanced

TRIGGER CONFIG

Run multiple times. Advanced customization. Can use cron-like syntax: "", "*/", "*/", "2-12/13"

Start End

in 48 years

2071-09-03 05:15

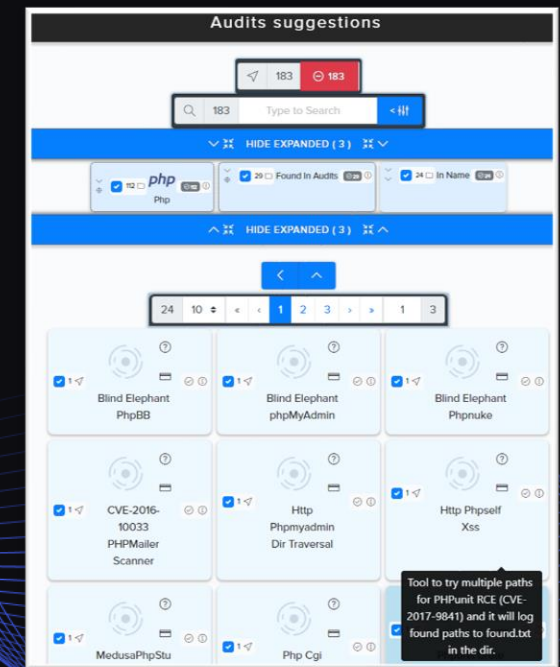
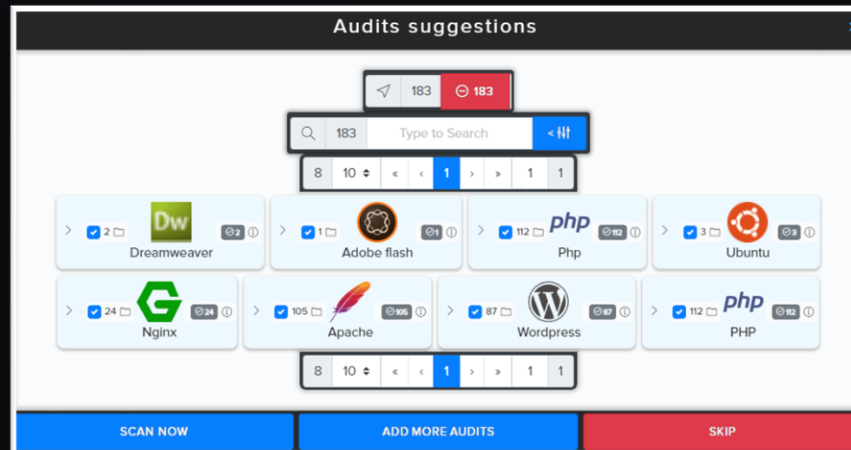
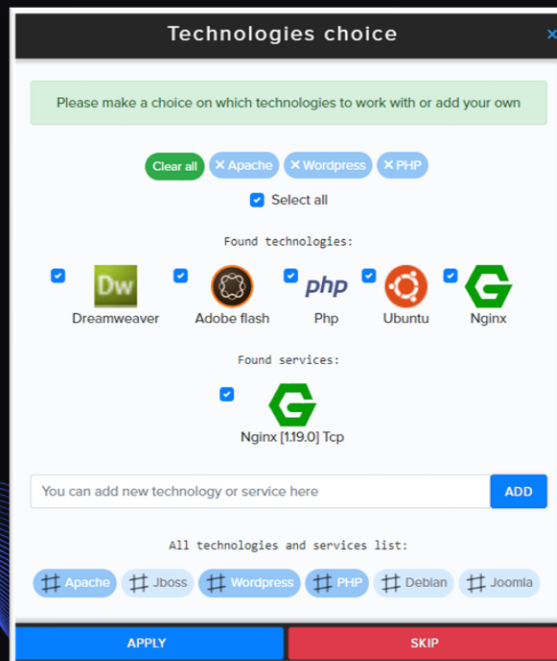
Year Month Day Week Day of week Hour Minute

25 8-35 mon-fri 9-16

Singular Audits - Wizard

Refining Security Audits with CryAI Wizard

A paramount task in every security assessments is the accurate identification of utilized technologies to run relevant audits. The CryAI Wizard system evaluates website technologies and services, cross-referencing them with its database. It then proposes audits that align with the identified criteria and technologies. Beyond the automated detections, you can manually add technologies. This empowers you to launch a comprehensive array of suggested audits categorized by technology or select specific ones.



Singular Audits - Streamlined Audit Management

Within the Singular Audits system, you'll find a user-friendly audit management panel that goes beyond tracking the progress and performance metrics of each audit. It equips you with the ability to pause, resume, or halt scans, as well as initiate new scans. Furthermore, it facilitates the creation of reports and enables the upload of reports from external scanners.

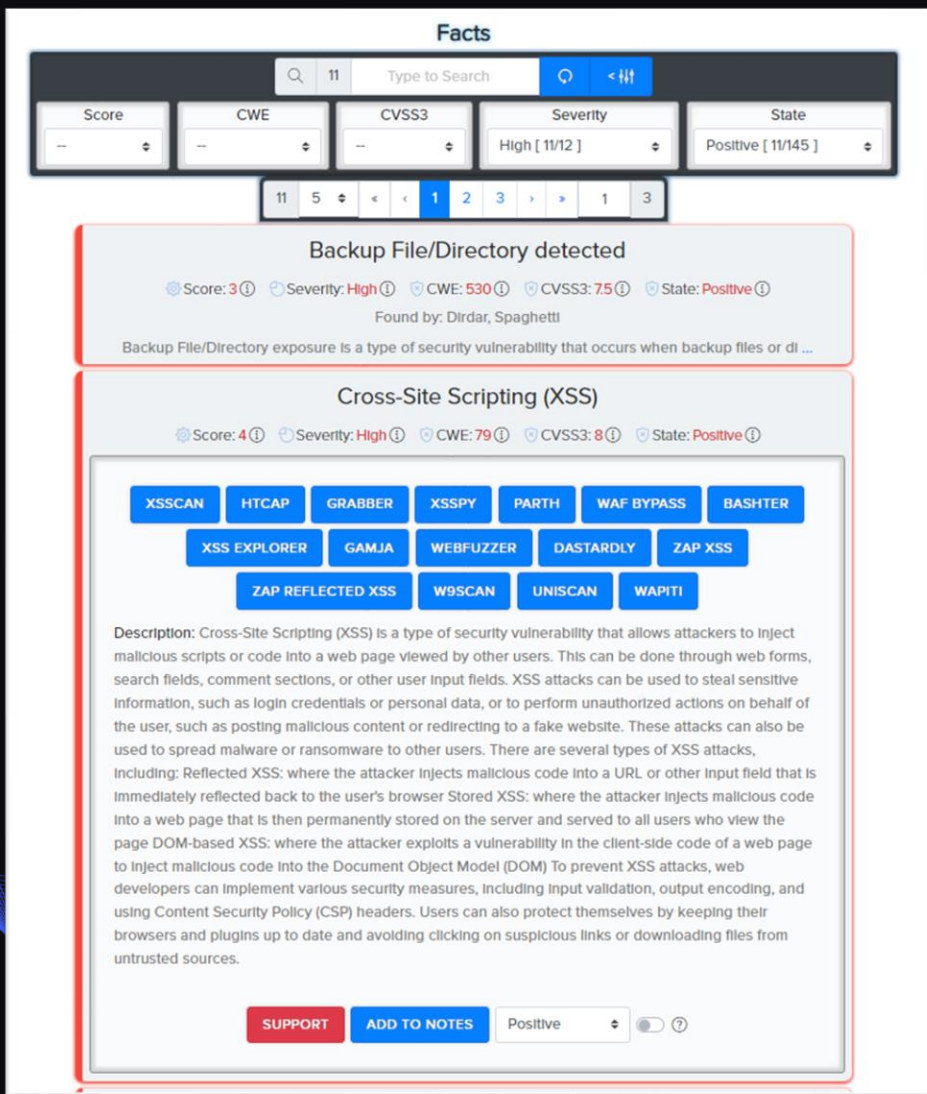
The screenshot shows the Singular Audits management interface. At the top, there's a progress bar with 23 items in red and 303 in green. Below it, a navigation bar includes 'Info', 'Control FINISHED', 'Facts 147', 'Solutions 65', 'Results 303', 'Resources 1471', and 'Interesting 34'. A central control panel features buttons for 'RERUN AS NEW AUDIT', 'CREATE NEW', 'FULL STOP', 'RE-RUN UNCOMPLETED', 'PAUSE', 'RESUME', 'CREATE REPORT', and 'UPLOAD'. A progress indicator shows 'FINISHED' and 'Progress 99%'. Below this is the 'Audits states' section with a search bar and an 'EXPORT' button. The main part of the interface is a table with the following data:

Title	Datetime	State	Last Message	Depends On	Required For	Weight
ZAP SQL	-	COMPLETED		0	0	2
ZAP All	-	COMPLETED		0	0	3
XSS Recon Crawl	-	COMPLETED		0	0	1
Web cache vulnerability scanner	-	COMPLETED		0	0	0
Sitadel	-	COMPLETED		0	0	2

The screenshot shows the 'Upload scan report' dialog box. It prompts the user to 'Select your scan report file to upload'. A dropdown menu is open, displaying a list of supported scanner formats:

- OpenVAS CSV
- HackerOne Cases
- Hadolint Dockerfile check
- Harbor Vulnerability Scan
- HuskyCI Report
- IBM AppScan DAST
- Immuniweb Scan
- JFrog Xray Scan
- Kiuwan Scan
- Microfocus Webinspect Scan
- MobSF Scan
- Mozilla Observatory Scan
- NPM Audit Scan
- Nessus Scan
- Netsparker Scan
- Nexpose Scan
- Nikto Scan
- Nmap Scan
- Node Security Platform Scan
- ORT evaluated model Importer
- OpenVAS CSV

Singular Audits - Facts & Solutions



Facts

Score: -- | CWE: -- | CVSS3: -- | Severity: High [11/12] | State: Positive [11/145]

11 5 < 1 2 3 > 1 3

Backup File/Directory detected

Score: 3 | Severity: High | CWE: 530 | CVSS3: 7.5 | State: Positive

Found by: Dirdar, Spaghetti

Backup File/Directory exposure is a type of security vulnerability that occurs when backup files or di ...

Cross-Site Scripting (XSS)

Score: 4 | Severity: High | CWE: 79 | CVSS3: 8 | State: Positive

XSSCAN | HTCAP | GRABBER | XSSPY | PARTH | WAF BYPASS | BASHTER

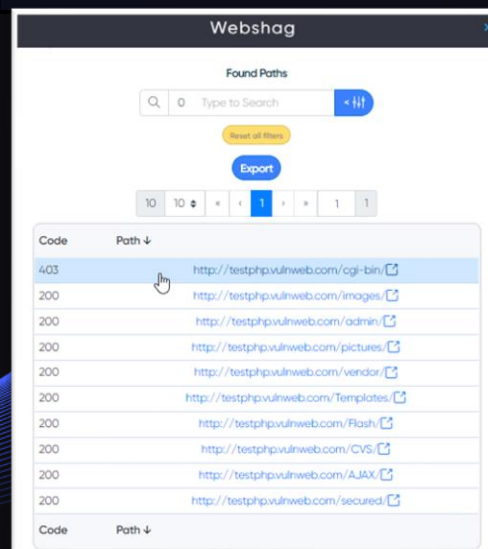
XSS EXPLORER | GAMJA | WEBFUZZER | DASTARDLY | ZAP XSS

ZAP REFLECTED XSS | W9SCAN | UNISCAN | WAPITI

Description: Cross-Site Scripting (XSS) is a type of security vulnerability that allows attackers to inject malicious scripts or code into a web page viewed by other users. This can be done through web forms, search fields, comment sections, or other user input fields. XSS attacks can be used to steal sensitive information, such as login credentials or personal data, or to perform unauthorized actions on behalf of the user, such as posting malicious content or redirecting to a fake website. These attacks can also be used to spread malware or ransomware to other users. There are several types of XSS attacks, including: Reflected XSS: where the attacker injects malicious code into a URL or other input field that is immediately reflected back to the user's browser. Stored XSS: where the attacker injects malicious code into a web page that is then permanently stored on the server and served to all users who view the page. DOM-based XSS: where the attacker exploits a vulnerability in the client-side code of a web page to inject malicious code into the Document Object Model (DOM). To prevent XSS attacks, web developers can implement various security measures, including input validation, output encoding, and using Content Security Policy (CSP) headers. Users can also protect themselves by keeping their browsers and plugins up to date and avoiding clicking on suspicious links or downloading files from untrusted sources.

SUPPORT | ADD TO NOTES | Positive

Facts, derived from scan findings, exhibit varying attributes such as severity, CVSS3 score, and CWE number. Within the Singular Audits system, these facts are accompanied by comprehensive descriptions and remediation solutions. Audit results can be directly accessed, and users can assign statuses like Positive / False Positive / Accept Risk / Retest / Fixed. Moreover, the system enables users to integrate Notes, mark items as 'Interesting,' or create Support tickets. With an array of intuitive filters and search functionalities, it offers a complete analytical toolkit.



Webshag

Found Paths

0 Type to Search

Reset all filters

Export

10 10 < 1 > 1 1

Code	Path
403	http://testphp.vulnweb.com/cgi-bin/
200	http://testphp.vulnweb.com/images/
200	http://testphp.vulnweb.com/admin/
200	http://testphp.vulnweb.com/pictures/
200	http://testphp.vulnweb.com/vendor/
200	http://testphp.vulnweb.com/Themes/
200	http://testphp.vulnweb.com/Flash/
200	http://testphp.vulnweb.com/CVS/
200	http://testphp.vulnweb.com/AJAX/
200	http://testphp.vulnweb.com/secured/



Ffuf Default

Fuzz	Position	Status	Length	Words	Lines	Url
admin/	699	200	262	66	8	http://testphp.vulnweb.com/admin/
admin	5520	200	262	66	8	http://testphp.vulnweb.com/admin
images/?pattern=/etc/*&sort=name	2275	200	377	128	9	http://testphp.vulnweb.com/images/?pattern=/etc/*&sort=name
images/	2274	200	377	128	9	http://testphp.vulnweb.com/images/
images	4140	200	377	128	9	http://testphp.vulnweb.com/images
images	5266	200	377	128	9	http://testphp.vulnweb.com/images
images	5561	200	377	128	9	http://testphp.vulnweb.com/images

Singular Audits - Effortless Access to Audit Findings

The Singular Audits system goes a step further by providing a unified display of outcomes across all conducted audits. Audits are thoughtfully categorized for seamless navigation.

By simply toggling a button, you can swiftly mark any result of interest as 'Interesting,' functioning much like bookmarks.

The screenshot displays the 'Results by Categories' section of the Singular Audits interface. It features a search bar with 34 results and a 'Type to Search' field. Below the search bar, there are two 'HIDE EXPANDED (1)' buttons. A 'Security' filter is visible. A list of categories is shown, including 'Cookie audit', 'Dork', 'Technology detection', 'Combined checks', 'Enumeration', 'Exploit check', 'Other', 'Crawler', 'Vulnerability Scanners', and 'Info leak'. Each category has a corresponding icon and a count. At the bottom, there is a pagination control showing '10' items per page and a page number '1'.

The screenshot displays the 'Found 31 urls' section of the Singular Audits interface. It shows a list of URLs with their corresponding Method, Status code, and Content length. The list is as follows:

URL	Method	Status code	Content length
http://testphp.vulnweb.com/?:	GET	200	4958
http://testphp.vulnweb.com/admin/?login	GET	200	262
http://testphp.vulnweb.com/crossdomain.xml	GET	200	224
http://testphp.vulnweb.com/CVS/Root	GET	200	1
http://testphp.vulnweb.com/favicon.ico	GET	200	894
http://testphp.vulnweb.com/idea/encodings.xml	GET	200	171
http://testphp.vulnweb.com/idea/misc.xml	GET	200	266
http://testphp.vulnweb.com/idea/modules.xml	GET	200	275
http://testphp.vulnweb.com/idea/name	GET	200	6
http://testphp.vulnweb.com/idea/scopes/scope_settings.xml	GET	200	143

The interface also includes a 'Show 10' dropdown, a search bar, and a pagination control at the bottom showing '1' of 4 pages.

The screenshot displays the 'Severity information' and 'Metrix' sections of the Singular Audits interface. The 'Severity information' section features a pie chart showing the distribution of vulnerabilities by severity level:

- Information: 28
- High: 14
- Medium: 17
- Low: 2
- Critical: 2

The 'Metrix' section includes a search bar with 0 results and an 'EXPORT' button. Below the Metrix section, there is a table with the following data:

Target	Total Requests	Total vulnerabilities
testphp.vulnweb.com	147058	63

Multi Target Audits - Empower Your Scans, Multiply Your Efficiency

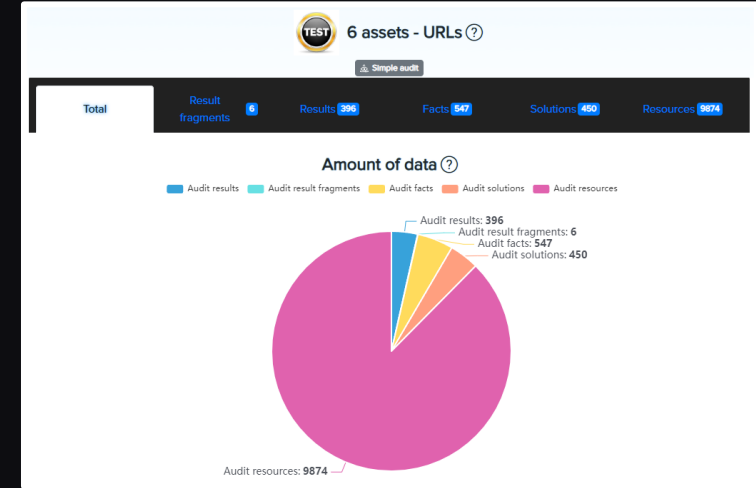
Introducing our cutting-edge Multi-Target Audits system, where efficiency meets versatility. With this innovative feature, users gain the power to manage multiple projects simultaneously, each capable of scanning a diverse range of targets. Whether it's URLs, IPs, mobile application files, source code links, or other available targets, our platform allows seamless integration. Tailor your audits for different targets effortlessly, as our system intelligently selects the most suitable audits based on your chosen purpose.

The screenshot displays the CryEye workflow management interface. On the left, a list of workflows is shown, including 'Combo Check', 'ComboScanExtra V1 - 9/9/2024', and 'ComboScan V1 - 9/6/2024'. A dropdown menu is open, listing various audit types: 'All', 'Simple Audit', 'Whitebox v2', 'Exploit Monitoring', 'Breach Detection', 'Darknet Monitoring v2', and 'Vault'. The main panel shows a detailed view of a 'Simple Audit' workflow. It includes a 'Delete' button, a 'Create and Run New Workflow' button, and a 'Delete workflow(s)' button. Below these are workflow statistics: 0 workflows, 17475 items, 431 warnings, 318 errors, and 145 successes. The workflow is titled 'Aquamarine Steven 21' and is in a 'STARTED' state.

Title ↓	Workflow Type ↓	Progress State ↓	Storage	Created ↑	Details
Aquamarine Steven 21	Simple audit	1 7 5 2 STARTED	17475 +17475 431 318 145 20564 +20564	4 days ago	

Multi Target Audits – Streamlined Workflow Management

Explore the intuitive Workflow management within Multi-Target Audits, where the orchestration of multiple stages becomes effortless. In its simplest form, Workflow encompasses initiation, scanning stages for individual targets, data preservation, and more. It culminates in completion, including notifications if needed. In a more advanced configuration, the Workflow evolves to feature dynamic components like agent-based single-target scans, extraction of potential new targets, scans on previously identified targets, and conditional initiation of additional stages.



Workflow configs

Project Title: 43

Project Type: Workflow Type: State:

10 assets - 2023-06-02 13:59:20.944305 [10]
10 assets - 2023-06-02 14:00:55.625184 [1]
185.185.185-2023-06-14 12:28:02.308353 [1]
2 assets - Vulnerable-Code-Snippets [1]
3 assets - 2023-06-05 13:28:37.383251 [1]
3 assets - 2023-06-12 08:33:41.378120 [1]
4 assets - 04-09 [1]
4 assets - Recon & Vuln scan [1]
4 test emails [4]
6 assets - URLs [2]
apache 2.4 [1]
apache 2.4 [1]
apache httpd 2.4.37 [1]
cryeye 2023-08-08 13:07 [1]
cve 2023-08-04 11:34 [1]
Dockerfile [5-9-45] 2023-06-05 - redowned [1]
donkyparty 2023-08-07 09:52 [1]
donkyparty 2023-08-07 10:03 [1]

6/12/2023, 11:33:41 AM

Some tests

6/12/2023, 9:39:09 AM (Apache 2.4)

Emails 6/12/2023, 9:36:37 AM (username@gmail.com)

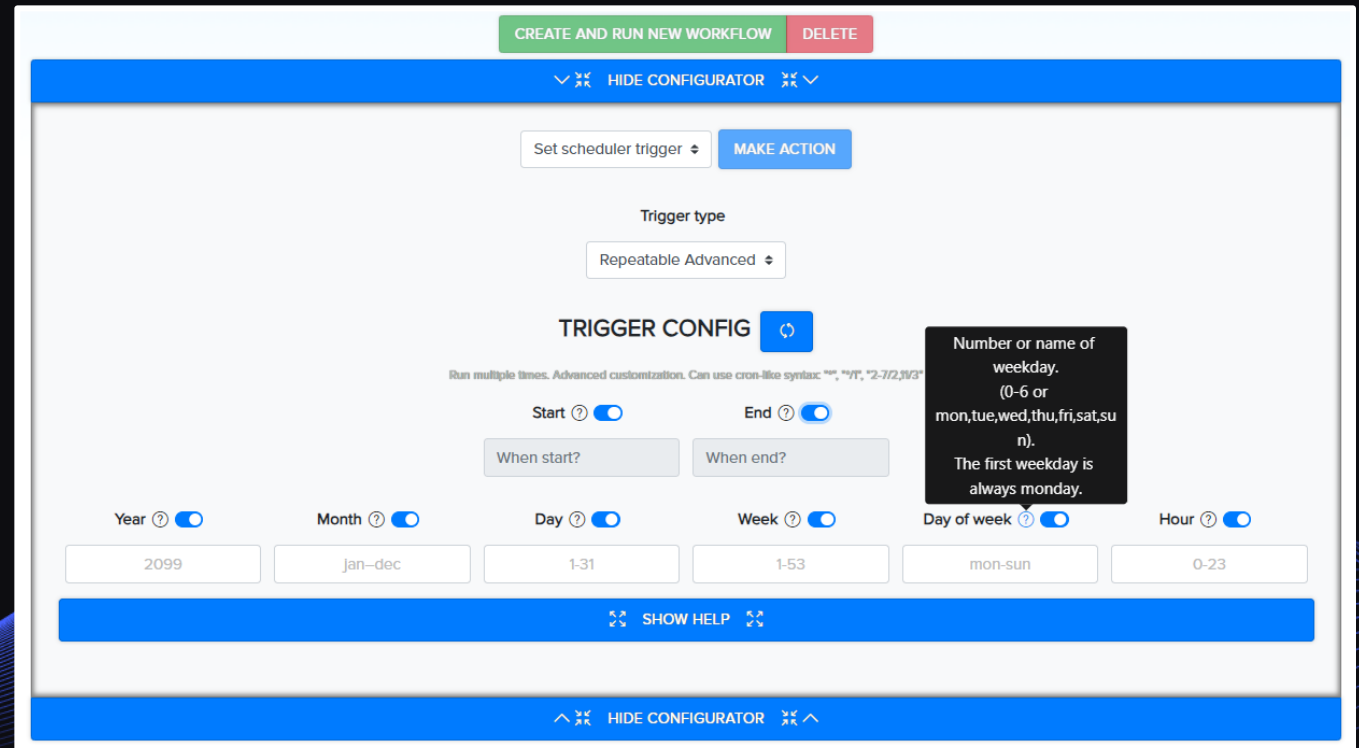
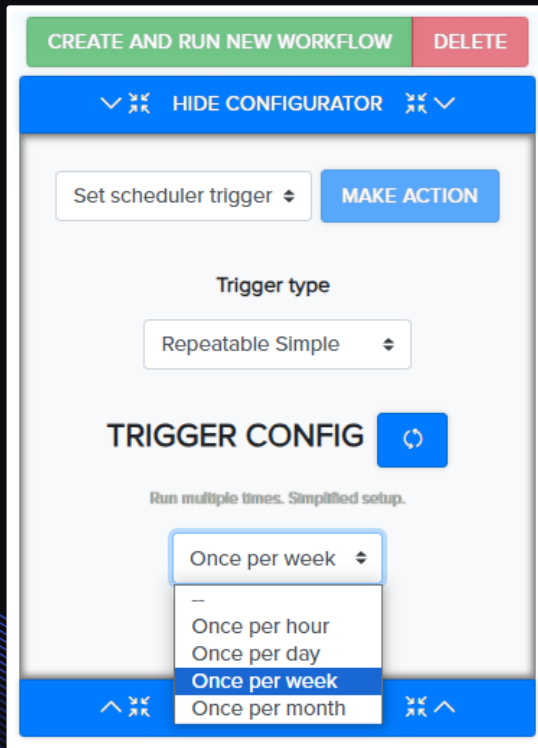
Emails 6/12/2023, 9:36:37 AM (john@gmail.com)

Emails 6/12/2023, 9:36:37 AM (qwerfingmail.com)

Project Title	Title	Config Modified	Workflows amount	Next	Latest	Progress	State	Workflow Modified	Storage	Details
6 assets - URLs	6/29/2023 Vulnerability scanners, Crawler, Enumeration	2 months ago	2	-	18 hours ago	1 6 1	STARTED	18 hours ago	RFS + N 994 RFS + N 492 + U 9992	
https://donkyparty/xwwa 2023-08-14 13:21	8/14/2023, 4:21:23 PM	20 hours ago	1	-	20 hours ago	1 1 1	STARTED	20 hours ago	RFS + N 258 RFS + N 620	
test@gmail.com	8/9/2023, 11:45:03 AM (test@gmail.com)	6 days ago	1	-	6 days ago	1 3	COMPLETED	6 days ago	RFS + N 1	
cryeye 2023-08-08 13:07	8/8/2023, 4:07:17 PM	7 days ago	1	-	7 days ago	3	COMPLETED	7 days ago	RFS + N 8 RFS + N 9	
Nginx NJS v0.75	8/8/2023, 11:49:08 AM (Nginx NJS v0.75)	7 days ago	1	-	7 days ago	4	COMPLETED	7 days ago	RFS + N 93	

Multi Target Audits – Seamless Scheduling Mastery

Embark on the Multi Target Audits journey, where the comprehensive management system boasts easily customizable schedulers. Experience the 'Repeatable Simple' mode, enabling automated task execution at your preferred intervals – be it hourly, daily, weekly, or monthly. Dive into the 'Repeatable Advanced' mode, where you can craft flexible scanning configurations using diverse Trigger Configs. The user-friendly interface, complete with intuitive tooltips, empowers you to navigate with confidence.



Multi Target Audits – Facts – Unified Insights for Diverse Targets

Explore the 'Facts' section within our Multi-Target Audits system, where the power of scanning various targets converges seamlessly. This unified space allows you to sort presented results by severity, creation date, CWE, and audit name. With a wealth of highly customizable filters at your disposal, you can effortlessly navigate through extensive data. Simply click the 'Show Modal' button to delve directly into the audit results. And that's not all – with just one click, you can quickly transfer the audit results to our Notes system.

The screenshot displays the 'Findings' section of a security tool. At the top, there are navigation tabs for 'Total', 'Result Fragments', 'Results', 'Facts', 'Solutions', and 'Resources'. Below this is a search bar and a 'Reset all filters' button. A row of filter buttons includes 'Asset I', 'Asset Type I', 'Target I', 'Audit Title I', 'Fact title I', 'Severity I', 'Score I', 'CWE I', and 'CVSS3 I'. A dropdown menu for 'Asset Type I' is open, showing options for 'Domain [345]', 'IP v4 [8]', and 'URL [228]'. Below the filters is a table with columns: Target, Audit Title, Fact title, Severity, Score, CWE, CVSS3, Created, Show modal with result, and Create registry. The table contains five rows of data, each representing a different audit finding.

Target	Audit Title	Fact title	Severity	Score	CWE	CVSS3	Created	Show modal with result	Create registry	
testphp.vulnweb.com	Domain	Htcap	Cross-Site Scripting (XSS)	HIGH	4	79	8	9 days ago	Show modal	Add Note Add record
testasp.vulnweb.com	Domain	Xss explorer	Cross-Site Scripting (XSS)	HIGH	4	79	8	9 days ago	Show modal	Add Note Add record
testaspnet.vulnweb.com	Domain	ZAP XSS	Cross-Site Scripting Reflected	MEDIUM	4	79	6.5	9 days ago	Show modal	Add Note Add record
testasp.vulnweb.com	Domain	ZAP XSS	Cross-Site Scripting Reflected	MEDIUM	4	79	6.5	9 days ago	Show modal	Add Note Add record
testasp.vulnweb.com	Domain	ZAP All	Detected information disclosure vulnerability	HIGH	4	0	0	9 days ago	Show modal	Add Note Add record

Multi Target Audits – Navigate, Evaluate, Empower

Uncover the capabilities of the Multi Target Audits system, designed to effortlessly manage and review generated results. This includes outcomes from continuous monitoring, allowing you to allocate various statuses to individual facts, all elegantly displayed within the 'State' category. From 'New' and 'Unread' to 'Issue,' 'Not Issue,' 'Resolved,' 'Ignored,' and 'False Positive,' our platform equips you with a spectrum of choices. With a single click, easily transition to the precise target result, facilitating prompt verification and assessment. Experience the realm of streamlined result control and actionable decision-making.

The screenshot displays the Multi Target Audits interface. At the top, there are filters for Asset, Asset Type, Target, and State, along with an Export button and a pagination control showing page 1 of 2. Below this is a table with columns for Target, Attack, Confidence, Param, Method, and Url. The table contains five rows of audit results, all with a Medium confidence level and a javascript:alert(1) attack. The second row is highlighted in blue. To the right, a browser window shows a notification from Acunetix Web Vulnerability Scanner Beta Released! with an OK button. A green dashed arrow points from the notification to the second row in the table.

Target ↓	Attack ↓	Confidence ↓	Param ↓	Method ↓	Url ↓
<input type="checkbox"/> testaspnet.vulnw eb.com Domain	javascript:alert(1);	Medium	NewsAd	POST	http://testaspnet.vulweb.com/ReadNews.aspx?NewsAd=javascript%3Aalert%281%29%3B&id=3
<input checked="" type="checkbox"/> testaspnet.vulnw eb.com Domain	javascript:alert(1);	Medium	NewsAd	GET	http://testaspnet.vulweb.com/ReadNews.aspx?NewsAd=javascript%3Aalert%281%29%3B&id=3
<input type="checkbox"/> testaspnet.vulnw eb.com Domain	</div><script>alert(1);</script></div>	Medium	tbComment	POST	http://testaspnet.vulweb.com/Comments.aspx?id=3
<input type="checkbox"/> testaspnet.vulnw eb.com Domain	javascript:alert(1);	Medium	NewsAd	POST	http://testaspnet.vulweb.com/ReadNews.aspx?NewsAd=javascript%3Aalert%281%29%3B&id=2
<input type="checkbox"/> testaspnet.vulnw eb.com Domain	javascript:alert(1);	Medium	NewsAd	GET	http://testaspnet.vulweb.com/ReadNews.aspx?NewsAd=javascript%3Aalert%281%29%3B&id=2

Target ↓	Attack ↓	Confidence ↓	Param ↓	Method ↓	Evidence ↓
					javascript:alert(1);

Multi Target Audits – Audit Variety, Unified Control

The screenshot displays a dashboard with a table of audits at the top. Below the table is a 'Workflows configs' section with buttons for 'CREATE AND RUN NEW WORKFLOW', 'DELETE', and 'SHOW CONFIGURATOR'. A search bar and a 'Workflow Type' dropdown are also visible. At the bottom, there is a detailed table of workflow configurations.

Title	Extra	Configs amount	Modified at	Details
4 assets 06-09	Simple audit	1	4 days ago	
6 assets - URLs	Simple audit	2	4 days ago	

Title	Config Modified	Workflows amount	Next	Latest	Progress	Workflow Modified	Storage	Details
6/29/2023 Vulnerability scanners, Crawler, Enumeration	2 months ago	2	-	21 hours ago	6 / 2	8 hours ago	[Icons]	
6/15/2023, 1:33:06 PM	2 months ago	1	-	2 months ago	6 / 2	2 months ago	[Icons]	

Explore an additional advantage of the Multi Target Audits system – the ability to launch various audit types on groups of selected targets within a single unified space. Moreover, with just a single click, users can effortlessly restart the same set of audits. You can then delve into scan histories, identify changes, and evaluate developments.

For instance, Workflows history allows you to check for the emergence of new vulnerabilities and assess whether previous issues have been successfully addressed.

The screenshot shows the 'Workflows history (2)' section with buttons for 'CREATE AND RUN NEW WORKFLOW' and 'DELETE WORKFLOW(S)'. It includes a search bar and a 'State' dropdown. Below is a table listing workflow runs with their titles, types, progress, storage, and creation dates.

Title	Workflow Type	Progress	Storage	Created	Details
Yellow William 43	Simple audit	6 / 2	[Icons]	21 hours ago	
AliceBlue Michael 29	Simple audit	8	[Icons]	2 months ago	

Vulnerability management CRM - Checklists

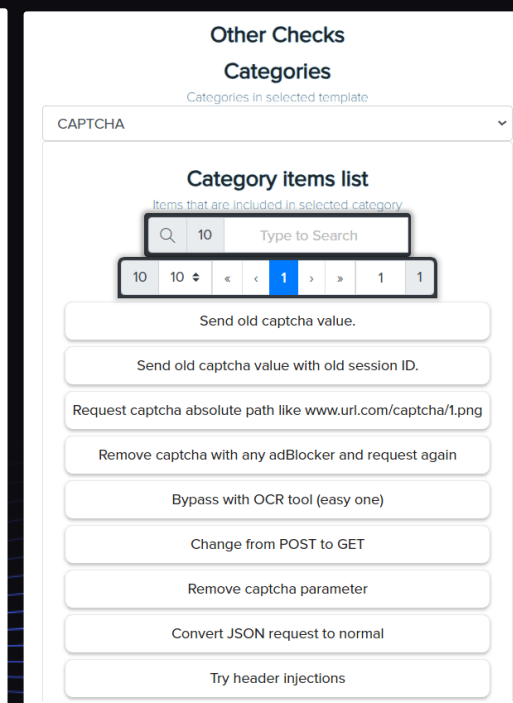
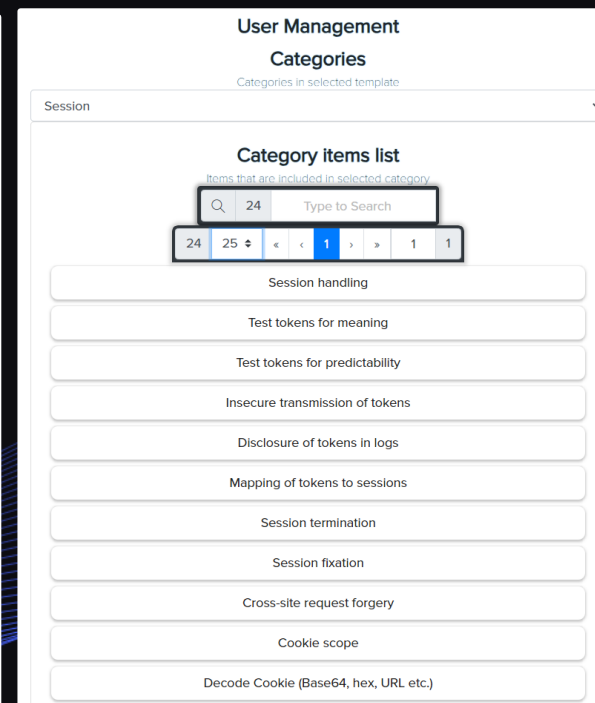
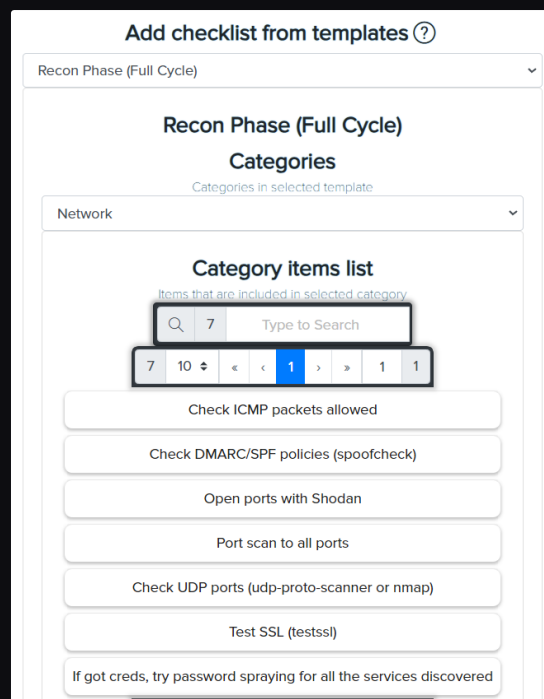
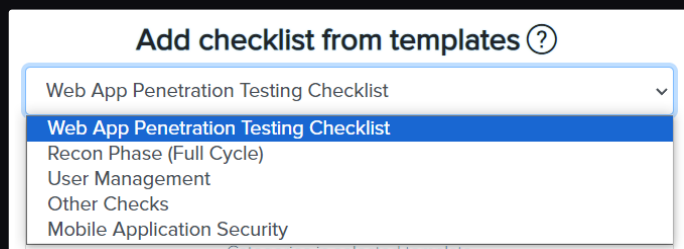
To ensure nothing of significance goes unnoticed, adhering to a pentest plan is crucial. That's why we've integrated Checklists functionality into our CRM system. This feature offers an array of pre-set checklist templates and the flexibility to create custom templates. Each step can be conveniently marked off, accompanied by any relevant information as evidence, enabling thorough test coverage.

The screenshot shows the CRM interface with a top navigation bar containing 'Workspace Notes', 'New Note', 'Workspace Checklists', and 'New Checklist'. Below the navigation, there are two checklist cards: 'Mobile Application Security' (created 14 days ago, 8 categories in progress) and 'Web App Penetration Testing Checklist' (created 2 months ago, 12 categories in progress). An 'Advanced filter' overlay is active, showing a search bar and a list of filter criteria: 'Created [Text]', 'Name [Text]', 'Finished [Text]', 'Categories [Text]', 'Project [Text]', and 'Project multi [Text]'. A 'CREATE ONE' button is visible at the bottom right of the interface.

The screenshot displays the 'Web App Penetration Testing Checklist' interface. The top bar includes 'EDIT CHECKLIST INFO' and 'DELETE CHECKLIST' buttons. The checklist is organized into sections: 'Information Gathering' (7 elements, 'IN PROGRESS'), 'Configuration Management' (8 elements, 'IN PROGRESS'), 'Secure Transmission' (6 elements, 'IN PROGRESS'), 'Authentication' (12 elements, 'IN PROGRESS'), 'Session Management' (12 elements, 'IN PROGRESS'), 'Authorization' (5 elements, 'IN PROGRESS'), and 'Cryptography' (3 elements, 'IN PROGRESS'). A detailed view of the 'Information Gathering' task is shown, listing items like 'Spider/crawl X Comments: 0', 'Check to metafiles X Comments: 0', 'Review webpage-comments X Comments: 0', 'Identify web application framework and technologies used X Comments: 0', 'Fingerprint web server X Comments: 0', 'Identify application entry points X Comments: 0', and 'Identify Web services X Comments: 0'. Below the list, there is a 'New Item' input field and a 'New comment' section with a rich text editor and a file upload area.

Vulnerability management CRM - Checklists

For your convenience, we've integrated a selection of predefined checklist templates, including Web Application Penetration Testing, Recon Phase, User Management, Other Checks, and Mobile Application Security. These templates are also fully editable to align with your business requirements. Screenshots showcase sample subcategories within the checklists, ensuring you have the flexibility to tailor assessments as needed.



Enhanced Cybersecurity Management with Cryeye's Registry

In our unwavering commitment to innovation, Cryeye is excited to introduce 'Registry Records' – a sophisticated CRM system designed with precision to elevate your cybersecurity journey. Registry Records brings dedicated categories like 'Vulnerabilities,' 'Risks,' 'Incidents,' and 'Checklists' right to your fingertips. This rich feature set seamlessly integrates across our all-inclusive platform, making your cybersecurity management effortless and efficient.



Enhanced Cybersecurity Management with Cryeye's Registry

Elevate your workflow with the flexibility to add Registry Records both manually and effortlessly, in just a single click from the outcomes of your audits. Enjoy user-friendly categorization, dynamic status updates, and the power of collaborative teamwork. Keep a vigilant eye on all changes made by team members, complete with comment capabilities. Welcome to a new era of streamlined, efficient cybersecurity management with Cryeye's Registry Records.



Server Side Vulnerability Horizontal Privilege Escalation
Vulnerability ▲ Issue

Clickjacking chained with DOM-Based XSS
Vulnerability ✓ Resolved

Broken Access Control
Vulnerability ▲ Issue

Memory corruption vulnerabilities
Vulnerability — Ignored

Custom notes

Amstahago (vs)

Access granted
Explains broken access control

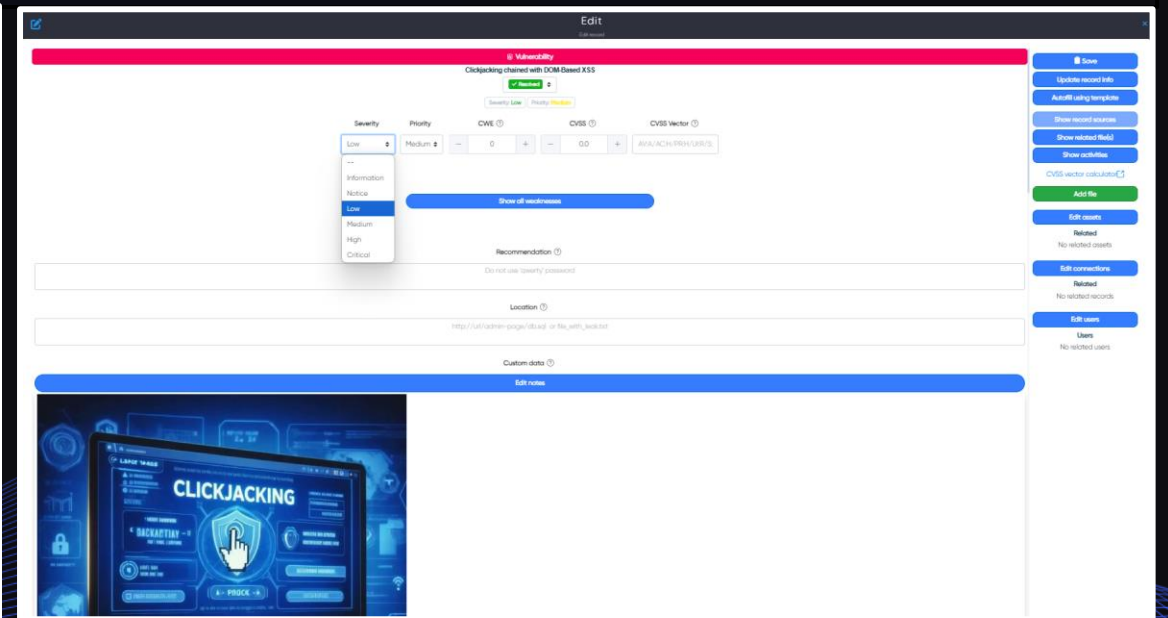
Related
No related assets

Related
No related records

Related
Users
No related users

Show record sources
Show related file(s)
Show activities
Edit assets
Edit connections
Edit users

A web application uses access control, also known as authorization, to allow some users to access certain content and functionalities while preventing others from doing so. Following authentication, these checks control the actions that "authorized" users are permitted to take. Although access control seems like a straightforward issue, proper implementation is quite challenging. The content and features that a website offers are strongly related to the access control model of that application. Furthermore, users can belong to many roles or groups, each with unique privileges and capabilities.



Edit

Vulnerability
Clickjacking chained with DOM Based XSS
Priority: 2

Severity: Low
Priority: Medium
CWE: 0
CVSS: 0.0
CVSS Vector: AV:A/ACH/PR/S/RS

Recommendation
Do not use "admin" password

Location
http://url(address-google/ibid) or file_path/ibid

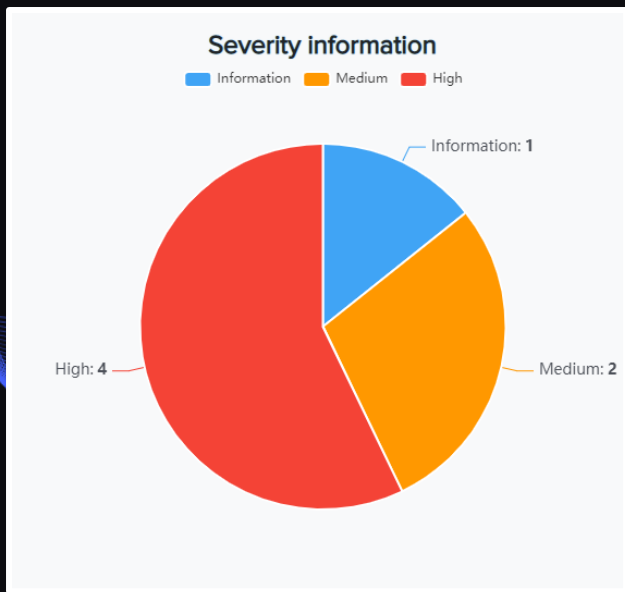
Custom data
Edit notes

Show
Update record info
Autofill using template
Show record source
Show related fields
Show activities
CVSS vector calculator
Add file
Edit assets
No related assets
Edit connections
No related records
Edit users
Users
No related users

Exploit Monitoring

Exploits Search is uncovering vulnerabilities and exploits across a diverse range of services and technologies. It forms the foundation for specialized algorithms that carefully analyze exploit headers. It also discovers exploits with undefined version ranges, as well as those falling outside the technology or service version range. The results are presented through straightforward histograms that display exploit counts for exact versions, variations beyond the software version, and even instances without version details, along with Nmap scripts and Metasploit modules.

The histograms and charts provide an easy-to-grasp visual representation, categorizing exploits by CVSS score or risk level.



Icon	Title	CVSS score	Published	Is Have exploit code	Is Have references	
	Apache HTTP Server 2.4.50 - Remote Code Execution (RCE) (3)	75	2 years ago [?]	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	Apache HTTP Server 2.4.50 - Remote Code Execution (RCE) (2)	75	2 years ago [?]	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	Apache HTTP Server 2.4.50 - Path Traversal & Remote Code Execution (RCE)	75	2 years ago [?]	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	Apache HTTP Server 2.4.49 - Path Traversal & Remote Code Execution (RCE)	43	2 years ago [?]	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	Apache 2.4.17 < 2.4.38 - 'apache2ctl graceful' 'logrotate' Local Privilege Escalation	72	4 years ago [?]	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

Exploit Monitoring

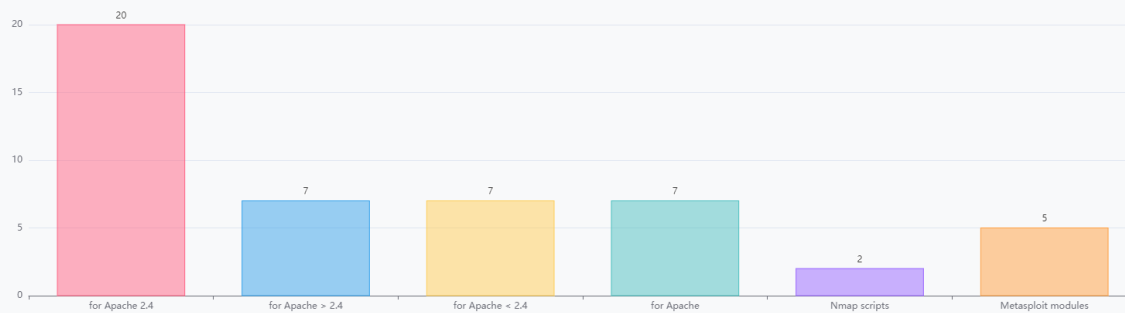
SHOW EXPLOITS

SHOW CVES

SHOW NEWS

CVE dashboard

Number of exploits



SHOW EXPLOITS FOR APACHE 2.4 (20)

SHOW EXPLOITS FOR APACHE > 2.4 (7)

SHOW EXPLOITS FOR APACHE < 2.4 (7)

SHOW EXPLOITS FOR APACHE (7)

SHOW NMAP SCRIPTS FOR APACHE (2)

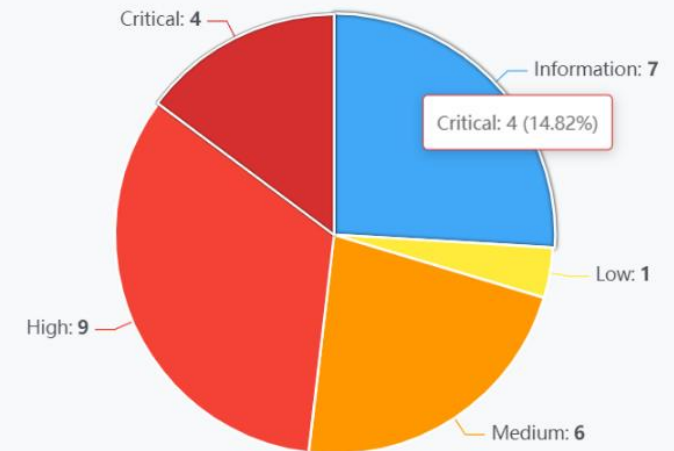
SHOW METASPLOIT MODULES FOR APACHE (5)

Exploits statistics by version

[Link to Documentation](#)

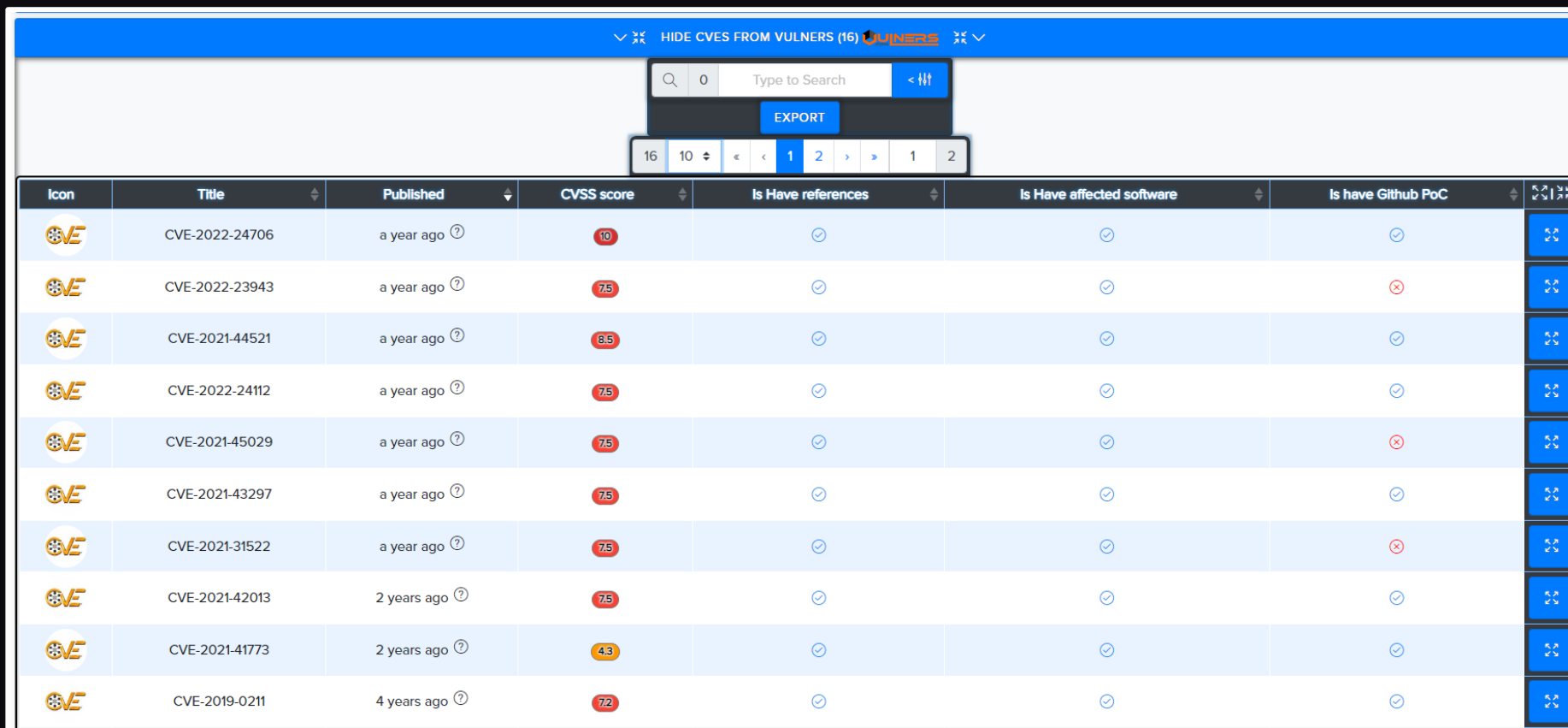
Severity information

Information Low Medium High Critical












CVE statistics by severity

Exploit Monitoring

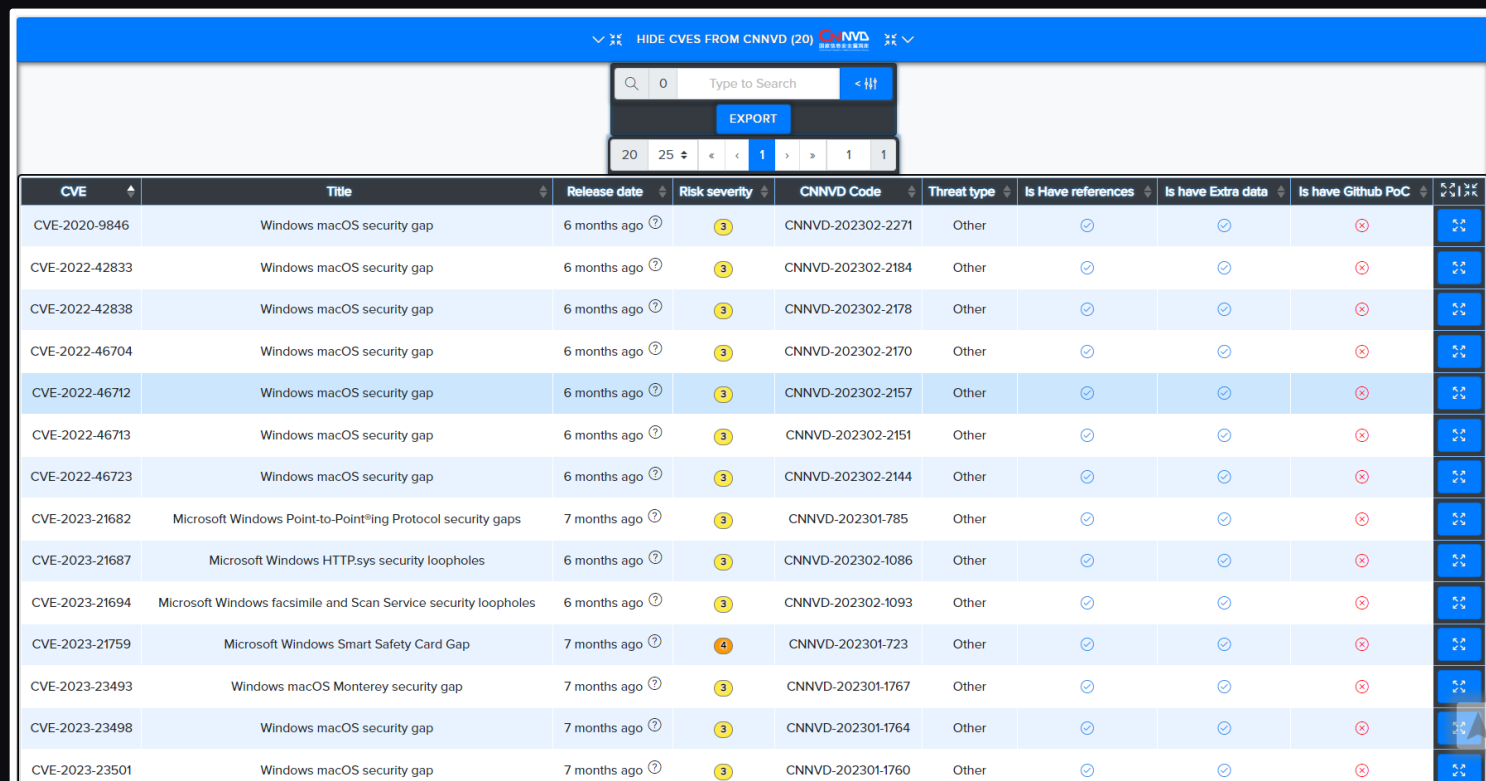


The screenshot displays the Vulners website interface. At the top, there is a search bar with the text "Type to Search" and a search icon. Below the search bar is an "EXPORT" button. A pagination bar shows "16" items, "10" items per page, and page numbers "1" and "2". The main content is a table with the following columns: Icon, Title, Published, CVSS score, Is Have references, Is Have affected software, and Is have Github PoC. The table contains 10 rows of CVE data.

Icon	Title	Published	CVSS score	Is Have references	Is Have affected software	Is have Github PoC
	CVE-2022-24706	a year ago	10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	CVE-2022-23943	a year ago	7.5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	CVE-2021-44521	a year ago	8.5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	CVE-2022-24112	a year ago	7.5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	CVE-2021-45029	a year ago	7.5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	CVE-2021-43297	a year ago	7.5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	CVE-2021-31522	a year ago	7.5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	CVE-2021-42013	2 years ago	7.5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	CVE-2021-41773	2 years ago	4.3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	CVE-2019-0211	4 years ago	7.2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Vulners is a comprehensive vulnerability database and search engine that aggregates information from various sources to provide security professionals, researchers, and organizations with easy access to information about security vulnerabilities, patches, and exploits.

Exploit Monitoring



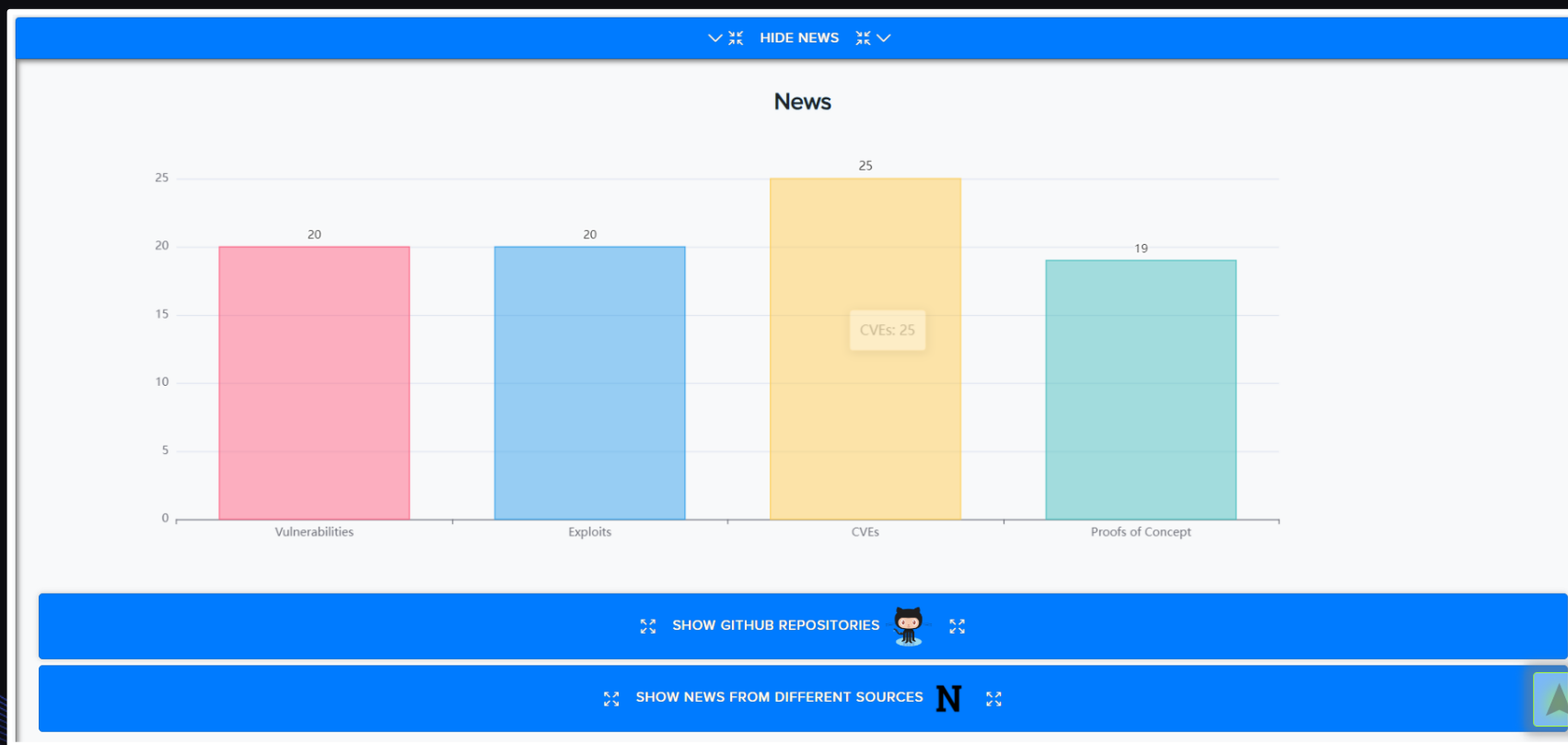
The screenshot displays the CNNVD interface with a search bar and a table of vulnerabilities. The table columns include CVE ID, Title, Release date, Risk severity, CNNVD Code, Threat type, and checkboxes for 'Is Have references', 'Is have Extra data', and 'Is have Github PoC'. The table lists 15 vulnerabilities, primarily related to Windows macOS security gaps and Microsoft Windows protocols.

CVE	Title	Release date	Risk severity	CNNVD Code	Threat type	Is Have references	Is have Extra data	Is have Github PoC
CVE-2020-9846	Windows macOS security gap	6 months ago	3	CNNVD-202302-2271	Other	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
CVE-2022-42833	Windows macOS security gap	6 months ago	3	CNNVD-202302-2184	Other	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
CVE-2022-42838	Windows macOS security gap	6 months ago	3	CNNVD-202302-2178	Other	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
CVE-2022-46704	Windows macOS security gap	6 months ago	3	CNNVD-202302-2170	Other	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
CVE-2022-46712	Windows macOS security gap	6 months ago	3	CNNVD-202302-2157	Other	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
CVE-2022-46713	Windows macOS security gap	6 months ago	3	CNNVD-202302-2151	Other	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
CVE-2022-46723	Windows macOS security gap	6 months ago	3	CNNVD-202302-2144	Other	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
CVE-2023-21682	Microsoft Windows Point-to-Pointing Protocol security gaps	7 months ago	3	CNNVD-202301-785	Other	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
CVE-2023-21687	Microsoft Windows HTTP.sys security loopholes	6 months ago	3	CNNVD-202302-1086	Other	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
CVE-2023-21694	Microsoft Windows facsimile and Scan Service security loopholes	6 months ago	3	CNNVD-202302-1093	Other	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
CVE-2023-21759	Microsoft Windows Smart Safety Card Gap	7 months ago	4	CNNVD-202301-723	Other	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
CVE-2023-23493	Windows macOS Monterey security gap	7 months ago	3	CNNVD-202301-1767	Other	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
CVE-2023-23498	Windows macOS security gap	7 months ago	3	CNNVD-202301-1764	Other	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
CVE-2023-23501	Windows macOS security gap	7 months ago	3	CNNVD-202301-1760	Other	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Chinese National Vulnerability Database (CNNVD) Similar to other vulnerability databases like the Common Vulnerabilities and Exposures (CVE) system, CNNVD collects, tracks, and provides information about known vulnerabilities in software, hardware, and other information technology products. It's primarily focused on vulnerabilities that have an impact on Chinese systems and networks.

Exploit Monitoring

Empower your defenses with Exploit Monitoring. By tracking technology vulnerabilities in real-time, our platform keeps you steps ahead of potential exploits. Through NewsAPI service integration and GitHub repository searches, users gain insights into vulnerabilities, CVEs, exploits, and POCs, enabling proactive security measures.



Exploit Monitoring

By monitoring CVE-related activity on GitHub, our platform empowers proactive identification of vulnerabilities, patches, and discussions. This essential tool ensures that users are well-prepared to address emerging security challenges with informed decisions.



The screenshot displays a web interface for monitoring CVEs. At the top, there is a blue header with a toggle for 'HIDE GITHUB REPOSITORIES' and a GitHub logo. Below the header, the title 'CVEs' is centered. A search bar with the placeholder 'Type to Search' and a magnifying glass icon is present, along with an 'EXPORT' button. A pagination control shows '20' items per page and page numbers '1', '2', '3', '4'. The main content is a table with the following columns: 'Icon', 'Repository name', 'Created', and 'Last updated'. Each row includes a small profile icon, the repository name, the creation time, and the last update time, with a blue button containing a double arrow icon on the right side of each row.

Icon	Repository name	Created	Last updated
	CVE-2014-6271	a month ago	a day ago
	Apache-Dubbo-CVE-2023-23638-exp	3 months ago	3 days ago
	CVE-2023-37582_EXPLOIT	24 days ago	5 days ago
	CVSS-Analysis	13 days ago	12 days ago
	CVE-2021-41773-EXPLOIT	3 months ago	13 days ago

Darknet Monitoring

The Darknet Monitoring tool helps collect and respond to data from various news text feeds.

If your data is seen on the Darknet, you will be the first to know about it. It helps you to predict future leaks or used technology vulnerabilities and protect your organisation in advance.

E	Exploits watch. SecurityFocus	https://www.securityfocus.com/rss/vulnerabilities.xml	✖	-
F	Freedomf0x	https://rsshub.app/telegram/channel/Freedomf0x	✔	12 days ago
L	leaks_db telegram	https://rsshub.app/telegram/channel/leaks_db	✖	-

Feed monitoring

Allows you to view the feed with posts from subscribed channels. And then go to the remote post via the link.

Darknet feeds monitoring refers to the practice of monitoring and analysing information, discussions, and activities that take place on the darknet, which is a part of the internet that is intentionally hidden and not indexed by traditional search engines. The darknet includes many anonymizing platforms that allow users to access websites and services while maintaining a higher level of privacy and anonymity.

The screenshot displays a feed of security-related news items. Each item includes a category letter (Security, I, I, R), a title, a brief description, a source, and a timestamp. A blue button with a share icon is visible on the right of each item.

- Security**: NoName Hackers Use RansomHub in Recent Cyber Campaigns. Despite active attacks by gangs such as the NoName ransomware group, which has targeted small and me... 2 days ago. Source: CySecurity News - Latest Information Security and Hacking Incidents.
- I**: Ivanti Cloud Service Appliance flaw is being actively exploited in the wild. Ivanti warned that recently patched flaw CVE-2024-8190 in Cloud Service Appliance (CSA) is being act... 2 days ago. Source: Security Affairs.
- I**: Ivanti Cloud Service Appliance flaw is being actively exploited in the wild. Ivanti warned that recently patched flaw CVE-2024-8190 in Cloud Service Appliance (CSA) is being act... 2 days ago. Source: Security Affairs.
- R**: Raisecom Gateway Command Injection (CVE-2024-7120). What is the Attack?FortiGuard Labs observes attack attempts targeting certain models of Raisecom Gat... 2 days ago. Source: FortiGuard Labs | FortiGuard Center - Threat Signal Report.

Darknet Monitoring

Subscriptions

Subscribe to notifications about blogs, sites and marketplaces on the Darknet that interest you.

Darknet feeds sources are platforms, websites, forums, marketplaces, and other online spaces within the darknet where information, discussions, and activities take place. These sources serve as channels through which users on the darknet communicate, share information, trade goods, and engage in various activities. Darknet feeds sources can include both legitimate and illicit content, making them important areas of interest for cybersecurity professionals, law enforcement, threat intelligence analysts, and researchers.

Icon	Title	Url	State	Fetches at	Created at
	Combo List	https://combo-list.com/feed/		12 minutes ago	3 hours ago
	Dark Reading	https://www.darkreading.com/rss_simple.asp		27 minutes ago	3 hours ago
	CISA Cybersecurity Advisories	https://www.us-cert.gov/ncas/alerts.xml		27 minutes ago	3 hours ago
	Darknet – Hacking Tools, Hacker News & Cyber Security	https://www.darknet.org.uk/feed/		12 minutes ago	3 hours ago
	Other leaks Latest Topics	https://www.crackingpro.com/index.php?forum/124-other-leaks.xml/		28 minutes ago	3 hours ago
	Vulnerabilities – Threatpost	https://threatpost.com/category/vulnerabilities/feed/		12 minutes ago	3 hours ago
	The Daily Swig Cybersecurity news and views	https://portswigger.net/daily-swig/rss		12 minutes ago	3 hours ago
	Dataleaks Утечки баз данных - Telegram Channel	https://rsshub.app/telegram/channel/dataleaks		28 minutes ago	3 hours ago
	Sinful Site - Combolists	https://sinfulsite.com/syndication.php?fid=59		28 minutes ago	3 hours ago
	Hacks – Threatpost	https://threatpost.com/category/hacks/feed/		12 minutes ago	3 hours ago

Darknet Monitoring

Triggers

If you want to track the appearance of some special publications. You can create triggers. It can be a simple keyword like name of Organisation or a complex regular expression.

Monitoring organization feeds is a proactive approach that helps organizations and security professionals understand the activities and intentions of specific threat actors or groups. This information is crucial for making informed decisions, preparing defences, and responding effectively to potential threats.

Title	Value	Created at
Apache	apache	3 months ago ?
CVE	cve	3 months ago ?
CVE-2021-43306	cve-2021-43306	a few seconds ago ?
jQuery	jquery	17 minutes ago ?
jQuery 3.2.1	jquery 3.2.1	16 minutes ago ?
jQuery Migrate 3.0.0	jquery migrate 3.0.0	14 minutes ago ?
jQuery UI 1.13.0	jquery ui 1.13.0	16 minutes ago ?
Telegram	telegram	3 months ago ?
Twitter	twitter	3 months ago ?
XSS	xss	17 minutes ago ?

Darknet Monitoring

Reactions

Reactions are feed posts that match a trigger.

Reactions sources play a significant role in threat intelligence and cybersecurity. Security professionals and analysts monitor these sources to:

Learn about emerging threats, attack techniques, and vulnerabilities exploited by cybercriminals.

Understand the activities and intentions of threat actor groups and cybercriminal organizations.

Stay updated on trends in cybercrime, hacking, and illicit activities.

Identify instances where sensitive data, credentials, or other information is being traded or sold.

Develop strategies and countermeasures to defend against evolving threats.

Trigger	Publications amount
Twitter	776
CVE	7924
Apache	224
Telegram	112
XSS	944
jQuery	15

The screenshot shows a news feed with four items. Each item includes a small image, a title, a snippet, a timestamp, and a source logo. A blue button with a share icon is on the right of each item.

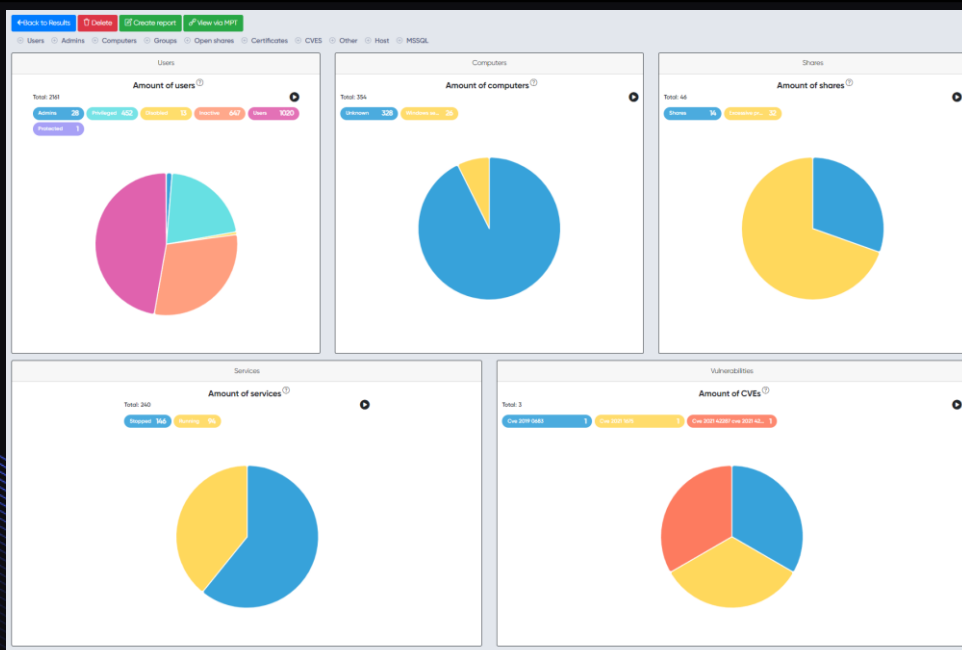
- Item 1:** Title: "MI5 confirms it was monitoring 16-year-old girl as Britain's youngest terror suspect before she took her own life having been sexually exploited by far right extremists, inquest hears". Snippet: "A statement from the security service was read to the pre-inquest review hearing into Rihanari's death...". Source: "Articles | Mail Online".
- Item 2:** Title: "How to Protect Your Accounts from 2FA Vulnerabilities: Avoid Common Security Pitfalls". Snippet: "Securing an account with only a username and password is insufficient because these can be easily s...". Source: "CySecurity News - Latest Information Security and Hacking Incidents".
- Item 3:** Title: "Metasploit Weekly Wrap-Up 09/13/2024". Snippet: "SPIP Modules This week brings more modules targeting the SPIP publishing platform. SPIP has gained s...". Source: "Rapid7 Blog".
- Item 4:** Title: "Metasploit Weekly Wrap-Up 09/13/2024". Snippet: "SPIP Modules This week brings more modules targeting the SPIP publishing platform. SPIP has gained s...". Source: "Rapid7 Cybersecurity Blog".

Active Directory Services

Automatic Active Directory security audits and Attack monitoring will help you to verify the security of environment and identify potential vulnerabilities in your infrastructure.

We created this tool for easy analysing Microsoft's directory services for operating systems of the Windows Server family.

General information of the project shown on the General information chart



Integrated tools to the AD audits system:

- ACLight
- ADHuntTool
- ADReaper
- ADRecon
- Certify
- FindUncommonShares
- GetDomainController
- Get-RBCD-Threaded
- noPac
- PingCastle
- PowerUpSQL
- PowerView
- PrintNightmareScanner
- SharpSpray
- Snaffler
- SpoolerScanner

Active Directory Services

Enumeration of the password setting policy within the AD

Password policy

Search: 10

Ip	Info	Domain	Password information
10.3.1.2	POLENUM	DC.example.local	Minimum password length: 4
10.3.1.2	POLENUM	DC.example.local	Password history length: 24
10.3.1.2	POLENUM	DC.example.local	Maximum password age: 41 days 23 hours 53 minutes
10.3.1.2	POLENUM	DC.example.local	Password Complexity Flags: 000000
10.3.1.2	POLENUM	DC.example.local	Domain Refuse Password Change: 0
10.3.1.2	POLENUM	DC.example.local	Domain Password Store Cleartext: 0
10.3.1.2	POLENUM	DC.example.local	Domain Password Lockout Admins: 0
10.3.1.2	POLENUM	DC.example.local	Domain Password No Clear Change: 0
10.3.1.2	POLENUM	DC.example.local	Domain Password No Anon Change: 0
10.3.1.2	POLENUM	DC.example.local	Domain Password Complex: 0

Page navigation: 1 2

Users privileges

Search: 10

Domain	Ip	Info	User	Privileges	Description
DC.example.local	10.3.1.2	SHAREFINDER	\\DC.example.local\ADMIN\$	READ WRITE	Remote Admin
DC.example.local	10.3.1.2	SHAREFINDER	\\DC.example.local\C\$	READ WRITE	Default share
DC.example.local	10.3.1.2	SHAREFINDER	\\DC.example.local\CertEnroll	READ WRITE	Active Directory Certificate Services share
DC.example.local	10.3.1.2	SHAREFINDER	\\DC.example.local\Corporate Files	READ WRITE	Corporate Files data for 2020
DC.example.local	10.3.1.2	SHAREFINDER	\\DC.example.local\CSV-Files	READ	
DC.example.local	10.3.1.2	SHAREFINDER	\\DC.example.local\DBA Backup	READ WRITE	Romania DB Backup
DC.example.local	10.3.1.2	SHAREFINDER	\\DC.example.local\IPC\$	READ	Remote IPC
DC.example.local	10.3.1.2	SHAREFINDER	\\DC.example.local\IT Tools	READ WRITE	IT Team Important Tools
DC.example.local	10.3.1.2	SHAREFINDER	\\DC.example.local\NETLOGON	READ WRITE	Logon server share
DC.example.local	10.3.1.2	SHAREFINDER	\\DC.example.local\Old Backup	READ WRITE	All Backup

Page navigation: 1 2

Enumeration of users with privileges and admins

Active Directory Services

Accounts with password don't expire

Search 10

Username	Full Name
vagrant	vagrant
adadmin	AdAdmin DDDD

< < 1 > >

List of users whose password will never expire (when creating a user in AD you should set the password expiry date, this screen shows that there are users whose password will never expire, which indicates that the user was created incorrectly, not for security reasons).

Enumeration of domain SPNs.

N/A	dc.example.local	DC\$	Dfsr-12F9A27C-BF97-4787-9364-D31B6C55EB04/dc.example.local
N/A	dc.example.local	DC\$	ldap/dc.example.local/ForestDnsZones.example.local
N/A	dc.example.local	DC\$	ldap/dc.example.local/DomainDnsZones.example.local
N/A	dc.example.local	DC\$	TERMSRV/DC
N/A	dc.example.local	DC\$	TERMSRV/dc.example.local
N/A	dc.example.local	DC\$	DNS/dc.example.local
N/A	dc.example.local	DC\$	GC/dc.example.local/example.local
N/A	dc.example.local	DC\$	RestrictedKrbHost/dc.example.local
N/A	dc.example.local	DC\$	RestrictedKrbHost/DC
N/A	dc.example.local	DC\$	RPC/ab560d87-6eaa-443e-9ac4-1e350f822cf4._msdcs.example.local

Active Directory Services

Enumeration of users with the same password

These accounts have no password set [Show Details](#)

Passwords of these accounts have been found in the dictionary [Show Details](#)

These groups of accounts have the same passwords [Hide Details](#)

Username

Search 10

EXAMPLE\ia.glasbey
EXAMPLE\ia.hejine
EXAMPLE\ia.hulance
EXAMPLE\ia.kneeland
EXAMPLE\ia.krahl
EXAMPLE\ia.famie
EXAMPLE\ia.legrand
EXAMPLE\ia.lempel
EXAMPLE\ia.mathou
EXAMPLE\ia.mcgahey

1 2 3 4

Domain Controller policies

Domain controller policy

Search 10

Login Status	Role Details
SeInteractiveLogonRight	BUILTIN\Print Operators
SeInteractiveLogonRight	BUILTIN\Server Operators
SeInteractiveLogonRight	BUILTIN\Account Operators
SeInteractiveLogonRight	BUILTIN\Backup Operators
SeInteractiveLogonRight	BUILTIN\Administrators
SeBatchLogonRight	BUILTIN\Performance Log Users
SeBatchLogonRight	BUILTIN\Backup Operators
SeBatchLogonRight	BUILTIN\Administrators
SeBatchLogonRight	BUILTIN\IIS_IUSRS
SeInteractiveLogonRight	BUILTIN\Print Operators

1 2 3

Active Directory Services

Enumeration of accounts with MSSQL Service SPN

Accounts with MSSQL Service SPNs

Search 10

Accounts Information Details

CN=MSSQL_SVC,CN=MANAGED SERVICE ACCOUNTS,DC=EXAMPLE,DC=LOCAL [Hide Details](#)

Details

Search 10

Service Principal Name SAM Account Name

mssql_svc/mssqlserver.example.local	mssql_svc\$
-------------------------------------	-------------

CN=VAGRANT,CN=USERS,DC=EXAMPLE,DC=LOCAL [Show Details](#)

Received admin password with configured LAPs

LAPS Passwords

Search 10

Computer Name	Distinguished Name	Password	Expire Time	Operation System
KINGSLANDING	CN=KINGSLANDING.OU=Domain Controllers,DC=sevenkingdoms,DC=local	"L%KCWv#3mlvV+1"	"2023-02-19 07:07:27"	Windows Server 2019 Datacenter Evaluation

[1](#)

OSINT when using gMSA policy

gMSA Information

0 Type to Search [EXPORT](#)

S AMAccount Name	Object Sid	Root Key Guid	Msd-Managed Password ID
gmsaMskSQL1\$	S-1-5-21-2095822386-2508765295-3408761845-1422	911694f4-87e2-73ce-e961-6d9f84050ada	AQAAAAIEU0sCAAAAQEAQAkAAAAATAAAAJQWkeKHznPpYW2ftAUK2gAAAAoAAAAKAAAAHMAZQB2AGUAbgBrAGkAbgBnAGQAbWBL... show more

Active Directory Services

Example of simply PDF report. The report provides a streamlined overview of the Active Directory configuration, user accounts, group memberships, and potential security vulnerabilities.

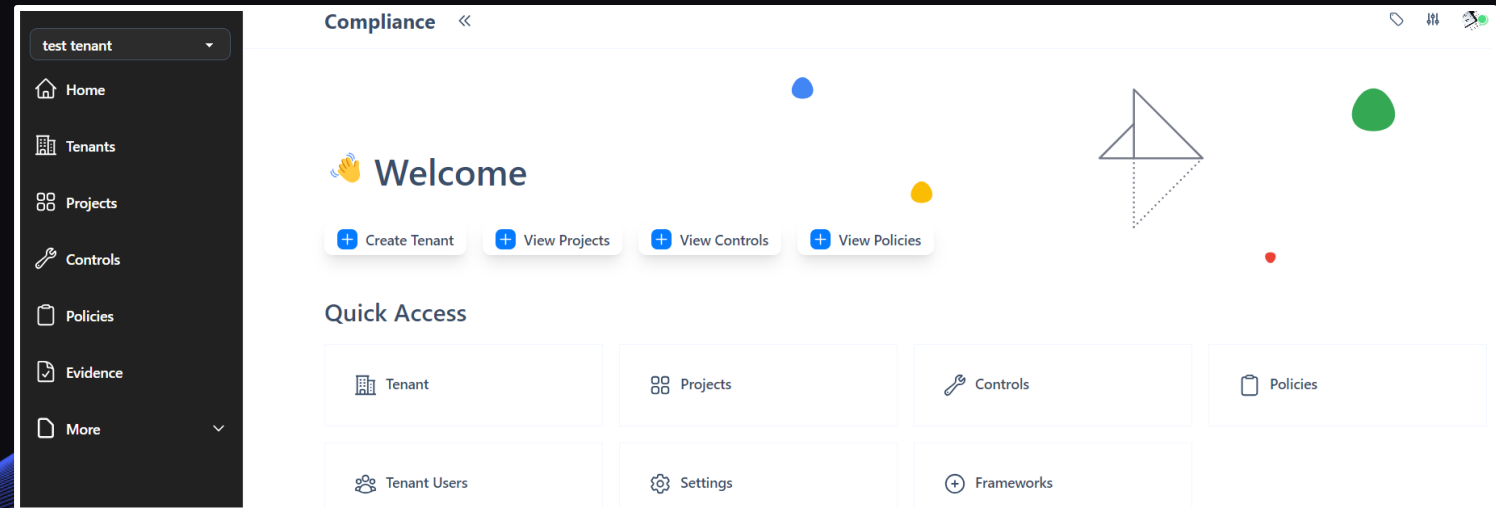
Shares

Share	Computer	Is Everyone Allowed	Is Current User Allowed
ADMIN\$	dc.example.local	True	True
C\$	dc.example.local	True	True
CertEnroll	dc.example.local	True	True
Corporate Files	dc.example.local	True	True
CSV-Files	dc.example.local	False	True
DBA Backup	dc.example.local	True	True
IT Tools	dc.example.local	True	True
NETLOGON	dc.example.local	True	True
Old Backup	dc.example.local	True	True
Operations Team	dc.example.local	True	True
Salary Details	dc.example.local	True	True
Sales Data	dc.example.local	True	True
SYSVOL	dc.example.local	True	True

Share Name	Computer	UNC Path	Comment	Stype Flags
CertEnroll	dc.example.local	\\10.3.1.2\CertEnroll\	Active Directory Certificate Services share	STYPE_DISKTREE, STYPE_SPECIAL, STYPE_TEMPORARY
Corporate Files	dc.example.local	\\10.3.1.2\Corporate Files\	Corporate Files data for 2020	STYPE_DISKTREE, STYPE_SPECIAL, STYPE_TEMPORARY
CSV-Files	dc.example.local	\\10.3.1.2\CSV-Files\		STYPE_DISKTREE, STYPE_SPECIAL, STYPE_TEMPORARY
DBA Backup	dc.example.local	\\10.3.1.2\DBA Backup\	Romania DB Backup	STYPE_DISKTREE, STYPE_SPECIAL, STYPE_TEMPORARY
IT Tools	dc.example.local	\\10.3.1.2\IT Tools\	IT Team Important Tools	STYPE_DISKTREE, STYPE_SPECIAL, STYPE_TEMPORARY
Old Backup	dc.example.local	\\10.3.1.2\Old Backup\	All Backup	STYPE_DISKTREE, STYPE_SPECIAL, STYPE_TEMPORARY
Operations Team	dc.example.local	\\10.3.1.2\Operations Team\	Engineering Operations daily data	STYPE_DISKTREE, STYPE_SPECIAL, STYPE_TEMPORARY
Salary Details	dc.example.local	\\10.3.1.2\Salary Details\	Finance Team 2020	STYPE_DISKTREE, STYPE_SPECIAL, STYPE_TEMPORARY
Sales Data	dc.example.local	\\10.3.1.2\Sales Data\	Latest Sales Team Shared folder	STYPE_DISKTREE, STYPE_SPECIAL, STYPE_TEMPORARY

Compliance

Compliance and Governance Technology stands as your organization's internal control and risk management system, ensuring alignment with legal, ethical, and corporate standards. Our integrated Compliance solution within Cryeye enables you to track progress towards meeting the criteria necessary for various compliance requirements. Once achieved, you can invite external auditors to evaluate your adherence based on provided evidence, safeguarding against financial penalties and reputational setbacks.



Compliance

Choose the certification framework that suits your needs. Our platform offers a range of pre-installed frameworks encompassing diverse standards like ISO 27001, HIPAA, SOC2, and more. Furthermore, should your requirements demand, our dedicated development team can seamlessly integrate other frameworks to ensure a tailored compliance solution.

New Project

Project Name
Give your project a name

Description
Short description of the project

Select Framework (you can always add additional controls later)

Empty

- Select framework
- SOC2
- CMMC
- ISO27001
- HIPAA
- NIST_800_53_V4
- NIST_CSF_V1.1**
- ASVS_V4.0.1
- SSF
- CISV8
- PCI_3.1
- CMMC_V2
- Empty

Tenant
Your Tenant Name

SAVE

Compliance

Control Dashboard

Allows you to conveniently track, control and edit your assets

Home > Projects > Test > Controls

GENERATE REPORT REFRESH DATA

SOC2 0.0% 6/7/2023 Summary Controls Policies Evidence Matrix Scratchpad Comments Report Settings

Quick Filters CONTROL'S I OWN CONTROL'S I OPERATE INFOSEC: NOT STARTED INFOSEC: IN PROGRESS INFOSEC: ACTION AUDITOR: READY FOR AUDITOR COMPLETE

Project Controls (36) Grouping: Controls All

Show 25 entries Search:

ID	REF CODE	NAME	STATUS	REVIEW	TODO	IMPLEMENTED	VIEW
1	CC1.1	COSO Principle 1: The Entity Demonstrates A Commitment To Integrity And Ethical Values.	Not Started	0/5	0/0	0	
2	CC1.2	COSO Principle 2: The Board Of Directors Demonstrates Independence From Management And Exercises Oversight Of The Development And Performance Of Internal Control.	Not Started	0/4	0/0	0	
3	CC1.3	COSO Principle 3: Management Establishes, With Board Oversight, Structures, Reporting Lines, And Appropriate Authorities And Responsibilities In The Pursuit Of Objectives.	Not Started	0/5	0/0	0	
4	CC1.4	COSO Principle 4: The Entity Demonstrates A Commitment To Attract, Develop, And Retain Competent Individuals In Alignment With Objectives.	Not Started	0/7	0/0	0	
5	CC1.5	COSO Principle 5: The Entity Holds Individuals Accountable For Their Internal Control Responsibilities In The Pursuit Of Objectives.	Not Started	0/5	0/0	0	
6	CC2.1	COSO Principle 13: The Entity Obtains Or Generates And Uses Relevant, Quality Information To Support The Functioning Of Internal Control.	Not Started	0/4	0/0	0	
7	CC2.2	COSO Principle 14: The Entity Internally Communicates Information, Including Objectives And Responsibilities For Internal Control. Necessary To	Not Started	0/11	0/0	0	

Compliance

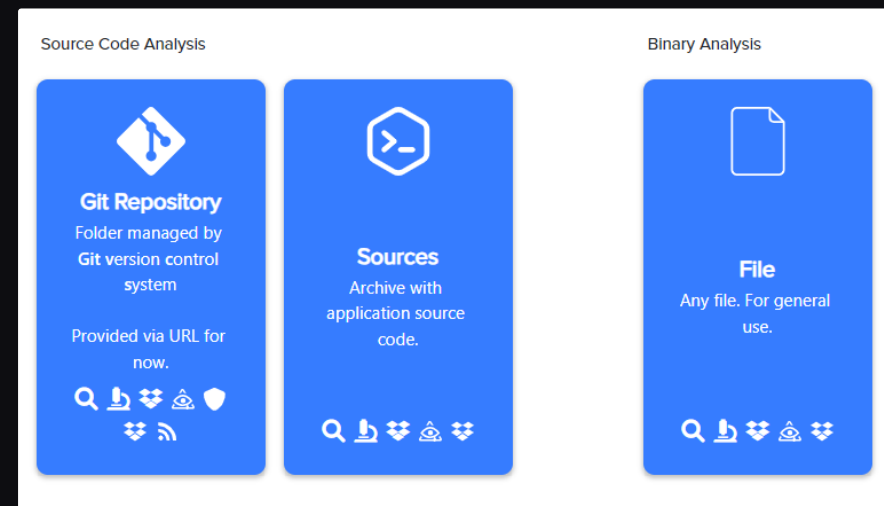
Track Progress of Controls

Efficiently monitor and manage the implementation and effectiveness of controls with our Compliance service.

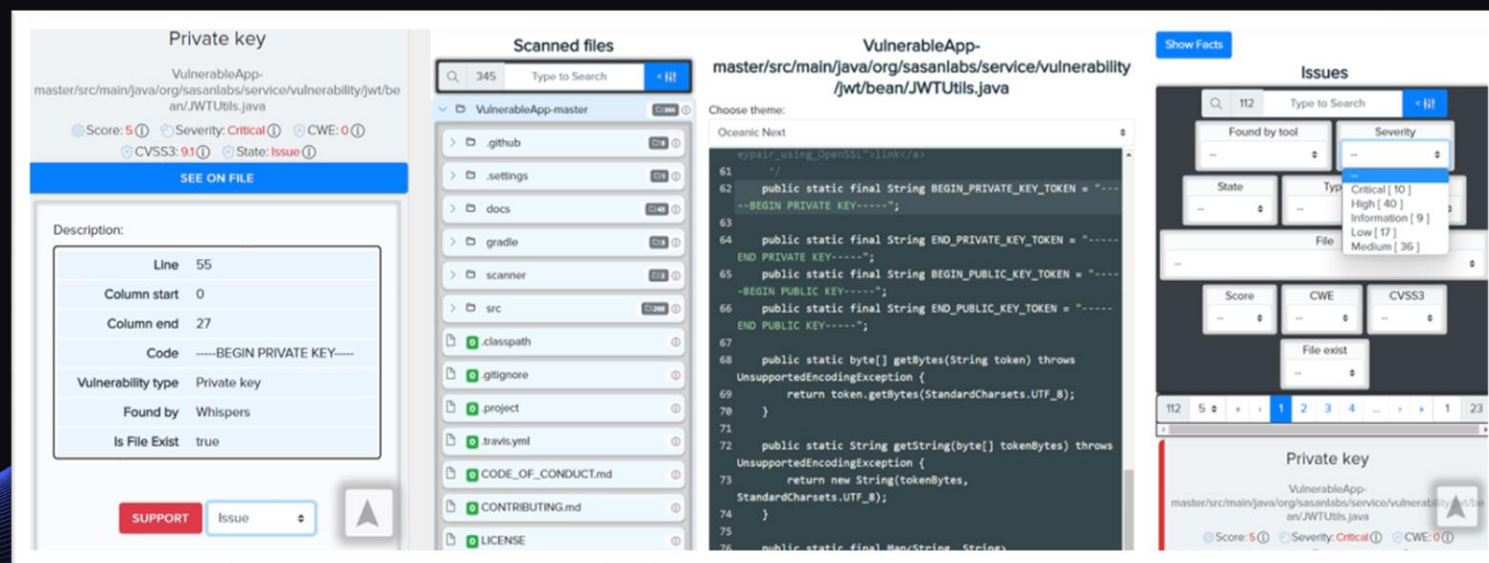
The screenshot displays the 'Projects > Test > Controls > CC1.1' page. At the top right, there is a 'SET AS: NOT APPLICABLE' button and a 'RELOAD' button. Below the breadcrumb, there are tabs for 'Overview', 'Subcontrols', 'Comments (0)', and 'Notes'. The 'Overview' tab is active, showing '1 - Control Details' with a 'VIEW GUIDANCE' button. The control details include: Status (In Progress), Reference Code (CC1.1), Complete (False), Name (COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.), Description (COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.), Guidance (null), Category (Security), Subcategory (Control Environment), and Creation (Wed, 07 Jun 2023 19:52:53 GMT). On the right side, there are two donut charts: 'Controls Implemented' at 45% and 'Evidence Collection' at 60%. A vertical sidebar on the left contains navigation icons, and a blue chat bubble icon is at the bottom right.

Whitebox / Source code review

You can easily upload a zip archive of your source code or GitHub repository to Cryeye's platform. Once uploaded, Cryeye conducts a comprehensive scan of the codebase for potential vulnerabilities and security issues. The scan results are presented in a user-friendly interface, allowing you to sort the findings by severity, score, CWE (Common Weakness Enumeration), and apply various filtering options to streamline the analysis process.



Integrated commercial Whitebox tools



Whitebox / Source code review

Whitebox enables thorough code analysis, aiding security audits, performance optimization, and vulnerability identification in the whitebox service environment.

Repository	Preset	Status	Total Scans	Issues	Not Issues	Resolved
Damn-Vulnerable-Source-Code-master.zip	All in one	finished	1	18	0	0
https://github.com/h4x0r101/Damn-Vulnerable-Source-Code	All in one	finished	1	18	0	0
https://github.com/digininja/DVWA	All in one	finished	1	2224	0	0
xvwa-master.zip	All in one	finished	1	1077	0	0
dypwa-master.zip	All in one	finished	1	438	0	0

Whispers

Source Manage Facts 2 Solutions 4

Vulnerabilities

0 Type to Search

Reset all filters

Type I File I Severity I

Export

Type key	Type ↓	File ↓	Line ↓	Code ↓	Severity ↓
db_password	Password	config/config.inc.php.dist	21	pa:ssw0rd	CRITICAL
MYSQL_ROOT_PASSWORD	Password	compose.yml	28	dvwa	CRITICAL
MYSQL_PASSWORD	Password	compose.yml	31	pa:ssw0rd	CRITICAL

- Awap [14]
- Bandit [2]
- BughoundPhp [15]
- Drek [516]
- DumpsterDiver [1]
- EsLint [21]
- Graudit [85]**
- Hawkeye [31]
- Horusec [12]
- Insiderlos [13]
- KicsSources [7]
- PhpCs [108]
- PhpShellFinder [84]
- ProgPilot [45]
- RepoScrapper [16]
- SnykSources [69]
- Whispers [3]

Audits example

Python, GO, PHP sources

Whitebox / Source code review

Vulnerability analysis provides comprehensive details, including vulnerability description, its precise location, and the specific line of vulnerable code. This level of transparency enables thorough understanding and effective mitigation of vulnerabilities within the system.

The screenshot displays a security tool interface with three main sections:

- File Explorer (Left):** A sidebar showing a directory tree with folders like 'ajax', 'classes', 'configuration', 'documentation', 'images', 'includes', 'javascript', 'labs', 'passwords', 'styles', and 'webservices'. Each folder has a count and an information icon.
- Source Code (Middle):** A code editor showing PHP code. The highlighted line is: `require_once (__SITE_ROOT__ . '/classes/CustomErrorHandler.php');` at line 10. Other lines include session initialization and error handling logic.
- Vulnerability Details (Right):** A panel showing the following information:
 - State:** --
 - Type of Vulnerability:** File Inclusion/Download [4]
 - File:** --
 - Score:** --
 - CWE:** --
 - CVSS3:** --
 - File exist:** --

Below the details panel, a red bar highlights the vulnerability description: **File Inclusion/Download**. The details include the file path `mutillidae-master/ajax/jwt.php`, a score of 5, severity of Critical, CWE 0, CVSS3 9.1, and state of Issue. It is attributed to 'BughoundPhp' and has a 'SEE ON FILE' button.

Whitebox / Source code review

Detailed whitebox reports, now effortlessly exportable to PDF format. This functionality allows for thorough documentation of findings, making analysis and sharing of whitebox assessment results efficient and accessible.

This endpoint handler performs a file system operation and does not use a rate-limiting mechanism. It may enable the attackers to perform Denial-of-service attacks. Consider using a rate-limiting middleware such as express-limit.

Type: javascript/NoRateLimitingForExpensiveWebOperation

Found by: SnykSources

CVSS3: 4.1 Score: 3 CWE: 0 Severity: medium

Location: target/routes/products.js

Line of code: 62 Start column: 62 End column: 55

File content:File does not exist

Description: This endpoint handler performs a file system operation and does not use a rate-limiting mechanism. It may enable the attackers to perform Denial-of-service attacks. Consider using a rate-limiting middleware such as express-limit.

General Information

Severity Information



Information: 0

Notice: 0

Low: 72

Medium: 0

High: 5

Critical: 0

Total Issues: 77

Signature of StrNCat

Type: Regular Expression

Found by: Drek

CVSS3: 2.1 Score: 2 CWE: 0 Severity: low

Location: seeve-master/seeve-master/CWE-193/src/test1.c

Line of code: 2 Start column: 1 End column: 8

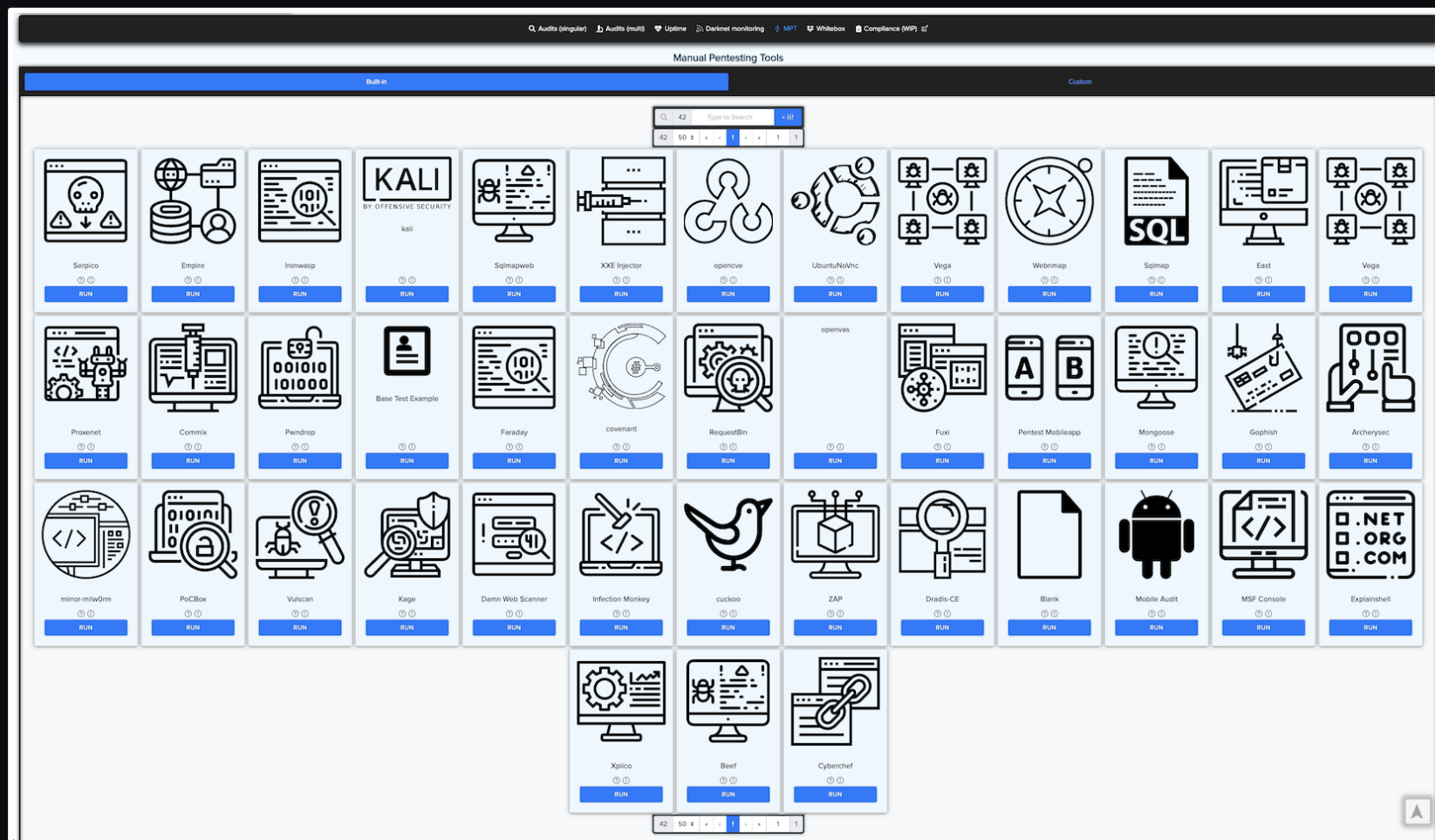
File content:/*In this example,the code does not account for the terminating null character, and it writes one byte beyond the end of the buffer.The first call to strncpy() appends up to 20 characters plus a terminating null character to fullname[]. There is plenty of allocated space for this, and there is no weakness associated with this first call. However, the second call to strncpy() potentially appends another 20 characters. The code does not account for the terminating null character that is automatically added by strncpy().

This terminating null character would be written one byte beyond the end of the fullname[] buffer. Therefore an off-by-one error exists with the second strncpy() call, as the third argument should be 19.*/

Description: A vulnerability signature is a representation (e.g., a regular expression) of the vulnerability language. Unlike exploit-based signatures whose error rate can only be empirically measured for known test cases, the quality of a vulnerability signature can be formally quantified for all possible inputs.

Manual Penetration testing Tools

A full cloud solution for manual checks on vulnerabilities. It allows users to use a full cycle of a vulnerability assessment or penetration testing.



List of the MPT tools

Manual Penetration testing Tools

The screenshot displays the WE3MAP web interface. At the top left is the logo 'WE3MAP'. Below it is a vertical sidebar with icons for home, network, add, more, social, refresh, star, and share. The main content area features four colored boxes representing statistics: 'XML Files' (0), 'Open ports' (0), 'Closed ports' (0), and 'Filtered ports' (0). Below these is a table with the following headers: 'Filename', 'Timestamp', 'Host Count', and 'Stats'. At the bottom of the interface, there is a disclaimer: 'WebMap master. This project is currently a beta, please DO NOT expose WebMap to internet. This version is NOT production ready.'

Nmap, a widely used network scanning tool, is accessible through a web-based interface within CryEye Cloud

Manual Penetration testing Tools

IronWASP Start-up Settings

Interception Proxy Settings:

IronWASP needs to start a local HTTP proxy server to enable browser traffic analysis.

Port number on which this proxy server must listen:

Should this proxy server accept connections from remote hosts? Yes No

Activate Traffic Interception:

Do you want to start capturing traffic from your Internet Explorer, Google Chrome and Safari? Yes No
(you can configure this later by selecting 'Set as System Proxy' option in the Proxy tab)

For better HTTPS traffic interception you can import IronWASP as a trusted CA on your machine. To find out how [click here](#).

Upstream Proxy Settings:

Sometimes your company/network provider requires you to use their proxy server for web browsing

Should IronWASP use the same proxy settings as your Internet Explorer or Google Chrome?

Yes (recommended. If the upstream proxy requires NTLM or other auth then this setting handles it automatically.)

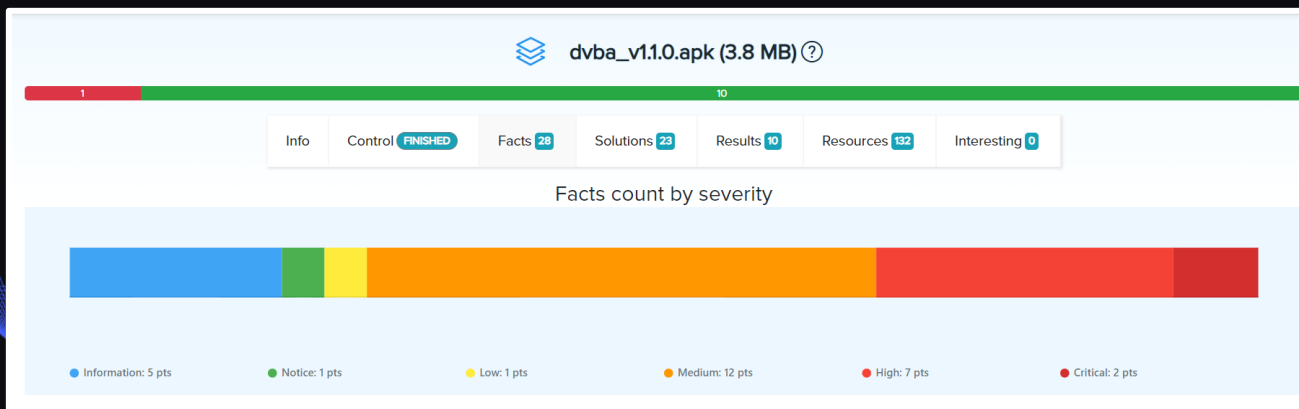
No

Use this custom upstream proxy setting instead: IP/Hostname: Port:

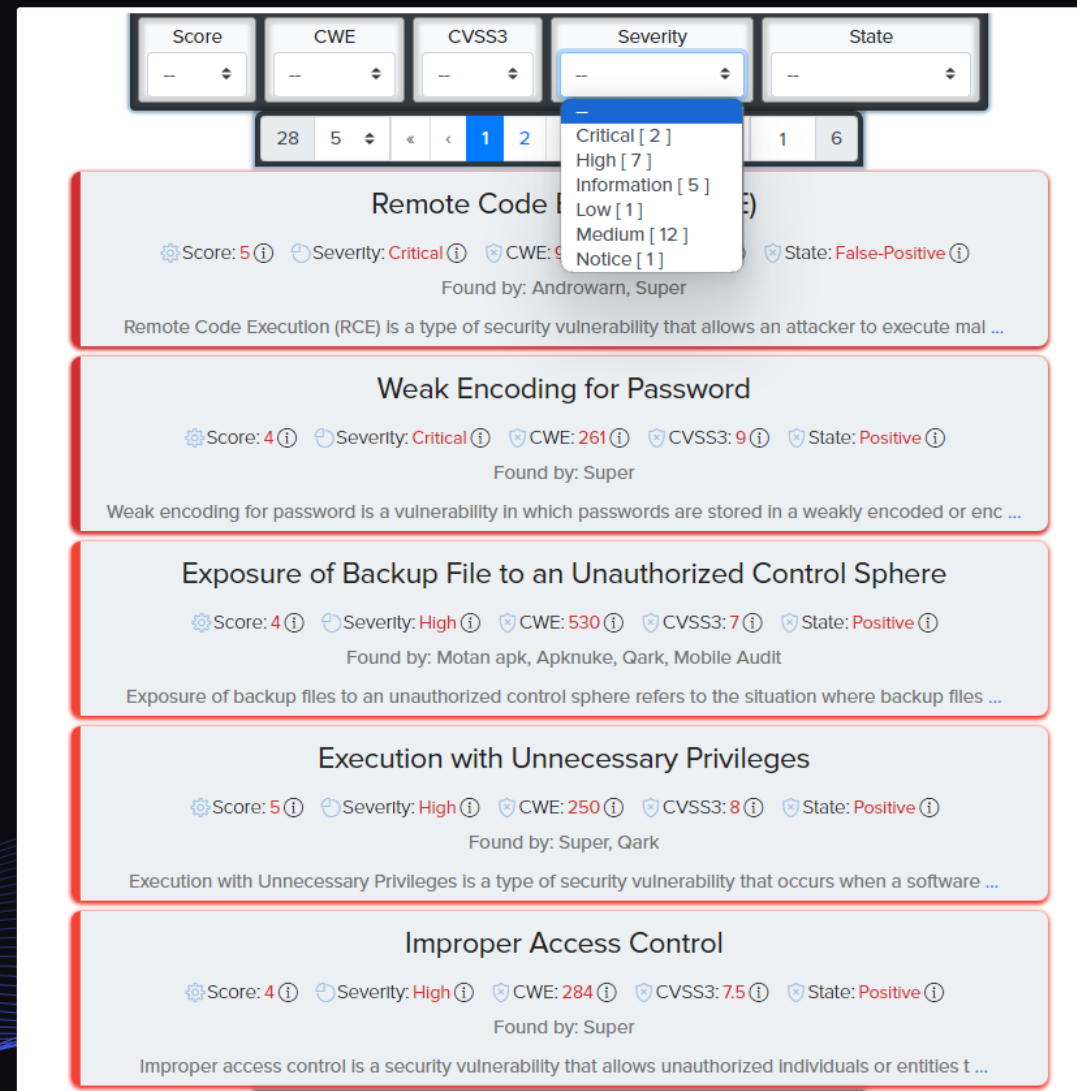
IronWASP, a web security testing tool, is seamlessly accessible via a web-based interface within CryEye Cloud

Mobile App Security Scanning

Mobile App Security Scan is a robust and reliable solution designed to safeguard Android and iOS apps from potential threats. It conducts a thorough analysis of the app's underlying code structure, meticulously identifying and addressing potential security vulnerabilities before they can be exploited, thus preventing potential harm and data breaches. The service uses a combination of commercial and open-source tools to achieve the best result and detect the greatest number of potential vulnerabilities.



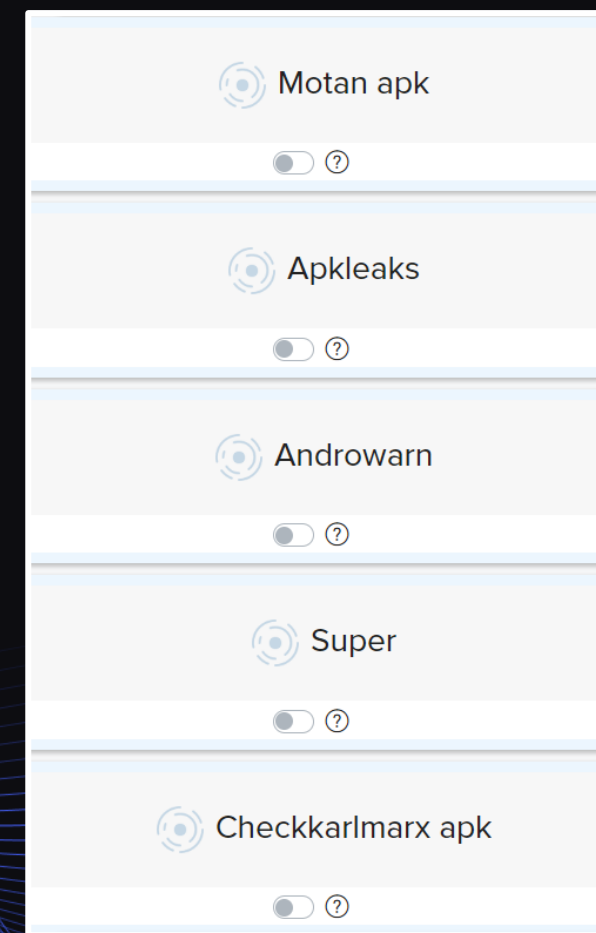
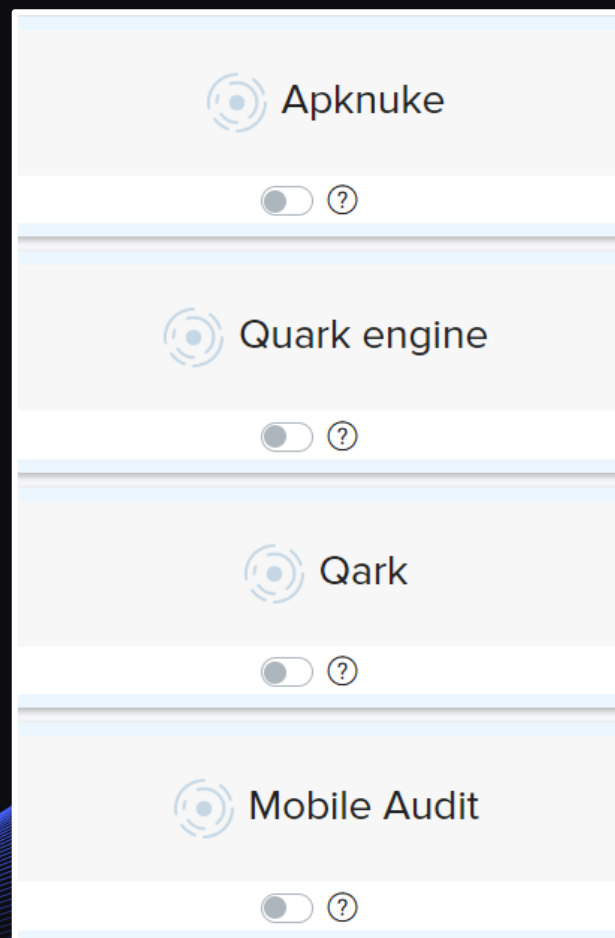
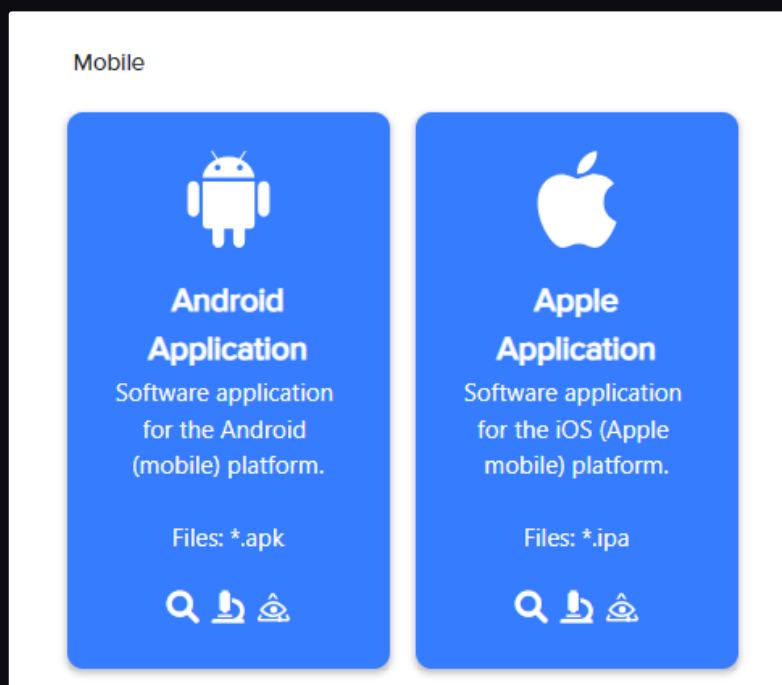
Convenient panel with results statistics



Potential vulnerabilities found by mobile scan

Mobile App Security Scanning

To get started, just select an asset IPA/APK file and run automatic scanning. Cryeye will automatically select a list of necessary tools for testing your application



Android App Security Scanning

Vulnerability identification in Android applications helps developers ensure a resilient app environment, protect user data, and position themselves for long-term success in the app landscape. The service allows you to find not only potential vulnerabilities, but also leaks of keys and other user data.

▼

Motan apk

Name	Description
AndroidManifest Adb Backup Checking	Show Details
AndroidManifest Exported Components Checking	Show Details
External Storage Accessing	Show Details
WebView Local File Access Attacks Checking	Show Details
WebView Intercept request	Show Details
WebView Potential XSS Attacks Checking	Show Details
WebView override url	Show Details

▼

Apkleaks

Package: com.app.damnvulnerablebank

Name	Matches
Firebase	Show Details
Google_API_Key	Hide Details
AlzaSyBbOHG6DDa6DOcRGeg57mw9nXYXcw6la3c	
Google_Cloud_Platform_OAuth	Hide Details
932398433474-59j4a17sqbfr9mf2eqqlreo6a5qsmt.apps.googleusercontent.com	
IP_Address	Show Details
JSON_Web_Token	Show Details
LinkFinder	Show Details

iPhone App Security Scanning

By investing in the identification of vulnerabilities in iOS applications, developers establish a secure app environment, safeguard user information, and position themselves for sustained success in the iOS app ecosystem. Secure applications instill confidence in users, leading to higher adoption rates and positive reviews, contributing to the app's success. Motan IPA and Checkmarks are among the many tools integrated into Cryeye for identifying potential vulnerabilities in your IOS application.

Name	Description
Binary not encrypted	Show Details
Insecure API(s) usage	Show Details
NSAllowsArbitraryLoads	Show Details
Insecure Random API(s)	Show Details
Logging function(s) usage	Show Details
Malloc function usage	Show Details
Runpath Search Path	Show Details
Restricted Segment	Show Details
Weak Hashing APIs	Show Details

Name	Info	Os	Tag	Severity	Locations
NS Allows Arbitrary Loads	Disable ATS restrictions globally excepts for individual domains specified under NSExceptionDomains	ios	network	Normal	Show Details
Http Insecure URLs	Http URLs starts with http	all	urls	Minor	Show Details
Http Insecure URLs	Http URLs starts with http	all	urls	Minor	Show Details
Http Insecure URLs	Http URLs starts with http	all	urls	Minor	Show Details
Http Insecure URLs	Http URLs starts with http	all	urls	Minor	Show Details

Breach Detection

Breach Detection is a powerful tool designed to keep your digital information safe. This service is built to track potential data leaks of emails, domains, cloud storage, URLs, company names, etc. Breach service not only prevents data breaches but also helps you comply with privacy regulations and manage your reputation.

The dashboard features a 'Projects' section with a 'Create project' button. Below it are buttons for 'Select all', 'Deselect all', and 'Delete selected'. A pagination control shows '1' of 1 items. A 'Demo Breach' card includes a settings gear, 'Assets: 7', and buttons for 'Explore', 'Delete', and 'Never monitor'.

The 'Add asset' form includes an 'Asset type' dropdown menu with 'Domain' selected. A text input field for 'Domain' is present with a 'This field is required' error message and an '+ Add' button. Below is a 'file with assets' section with a 'Browse' button and a note: '.csv or .txt file expected with size < 5 MB. (txt format: each asset on a new line)'. The 'Monitoring frequency' dropdown is set to 'never monitor' with another 'This field is required' error message. 'Save' and 'Clear' buttons are at the bottom.

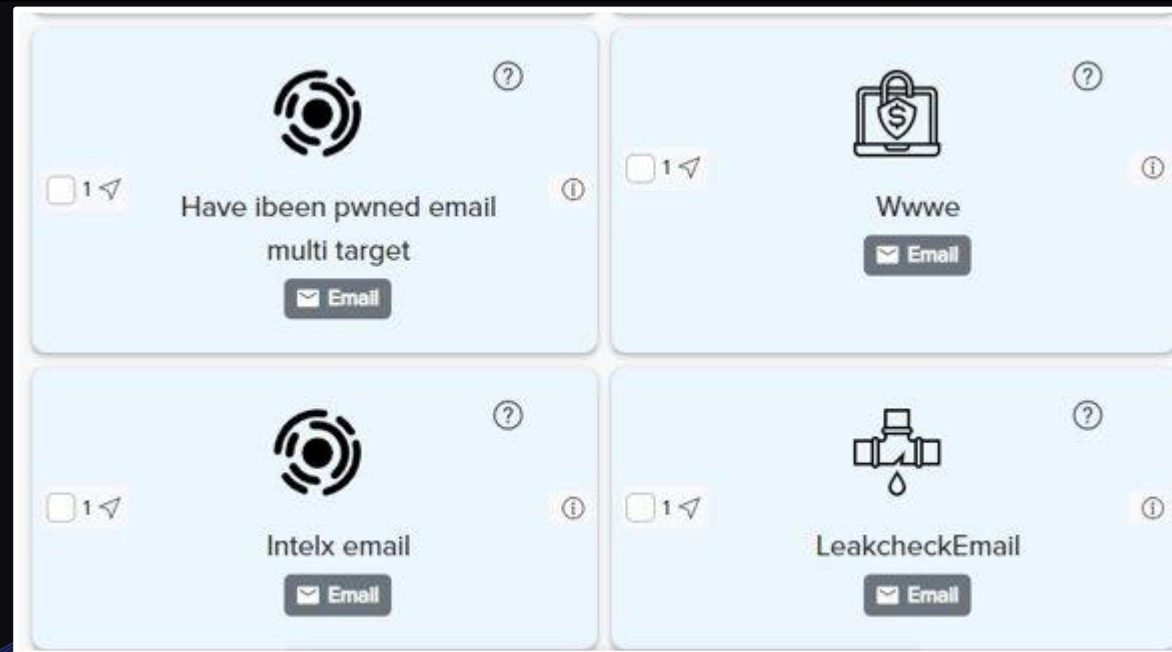
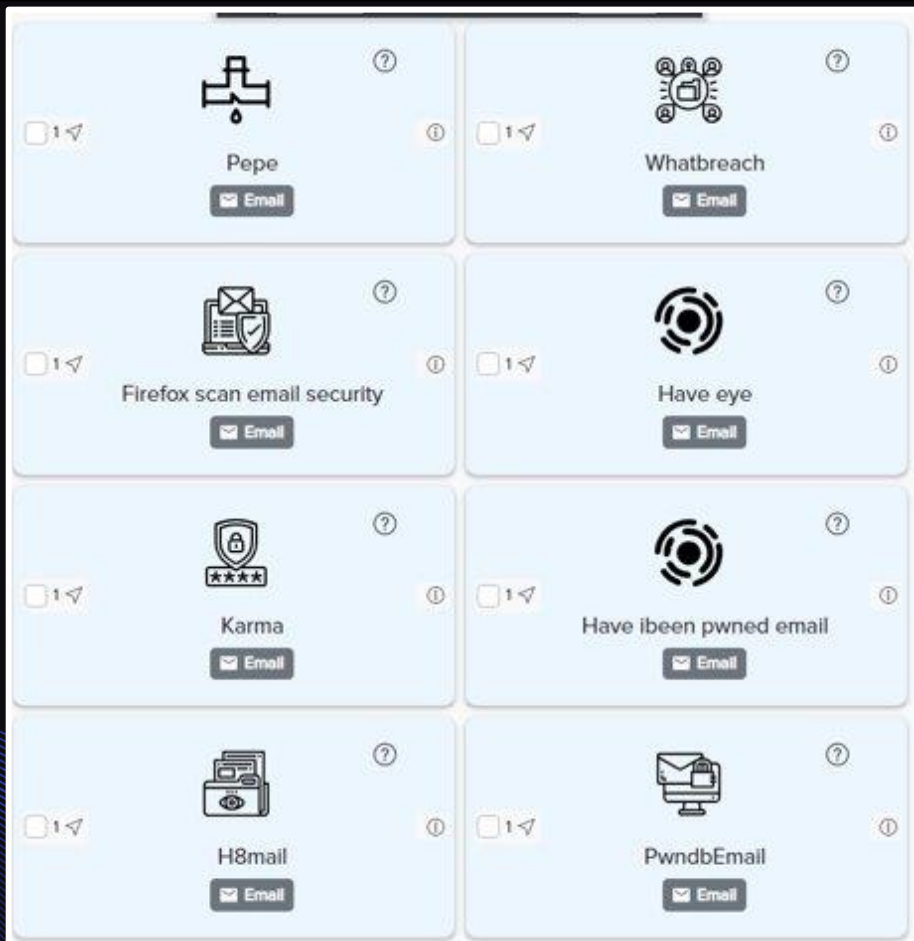
The dropdown menu for 'Asset type' shows 'Select asset type' and a 'This field is required' error message. 'Save' and 'Clear' buttons are visible below the menu.

The asset type selection list includes: 'Select asset type' (checked), 'Domain', 'IP address', 'URL', 'Company', 'Git', 'Email', 'Cloud', 'Cloud name', 'Bank Identification Number', and 'Keyword'.

The monitoring frequency options are: 'once a day', 'once a week', 'once a month', and 'never monitor' (checked).












Breach Detection

The Breach Detection system encompasses a rich array of integrated open-source and commercial tools, working in tandem to provide an exhaustive monitoring mechanism for detecting potential leaks across your assets.










Breach Detection

Wide range of tools that help keep URLs, domains, and subdomains secure. With these tools, you can better protect your online assets from potential threats and risks.

-  Nuclei DNS Scan
-  Nmap Vulners Aggressive
-  The Harvester Subdomain
-  Dns twist
-  Dnsmorph
-  Grayhatwarfare shorteners
-  Frog auth
-  Have I been pwned Domain
-  Isithacked domain
-  Grayhatwarfare Buckets
-  Intelx domain

Title	Amount
Found buckets from Intelx API for Domain	1






Target	HTTP Banner	DNS Records
 donky.party <small>donky.party</small>  Domain	openresty	 3.64.163.50
 donky.party <small>donky.party</small>  Domain	cloudflare	 104.21.53.77  172.67.210.100

Title
Nmap Vulners Aggressive Ports Info
Nmap Vulners Aggressive Scan IP and Host Discovery

Breach Detection

The Breach Detection service also includes the identification of password leaks, using various audits including Have I Been Pwned and Leakcheck, allowing not only see passwords and emails, but also the date of the leak and its source

Line	Email only	Last breach
john@gmail.com:123qwe	0	
john@gmail.com:123456789	0	2020-01
john@gmail.com:dakota06	0	
john@gmail.com:19kitahanon48	0	
JOHN@GMAIL.COM:50328694	0	2019-01
JOHN@GMAIL.COM:JOHNCENA	0	2019-01
JOHN@GMAIL.COM:hanco	0	2019-01
JOHN@gmail.com:198027	0	2019-01
JOHN@gmail.com:503286940	0	
JOHN@gmail.com:503286941	0	

Audit Title
 Have eye
 H8mail
 Have I been pwned Email
 Leakcheck
 EmailRep

Breach Detection

You can track leaks at specific intervals that you establish using the scheduler. Additionally, you'll receive email notifications whenever a leak or hack is detected.

The screenshot shows the 'Assets' management interface. At the top, there is a 'Delete' button and an 'Add asset' button. Below that is a search bar and a dropdown menu for 'types'. The main area is a table listing assets with columns for 'Created', 'Search', '10', and 'types'. Each row represents an asset with its name, analyzing status, date, and issue counts (Issues, not issues, resolved). A 'view' button is present for each asset.

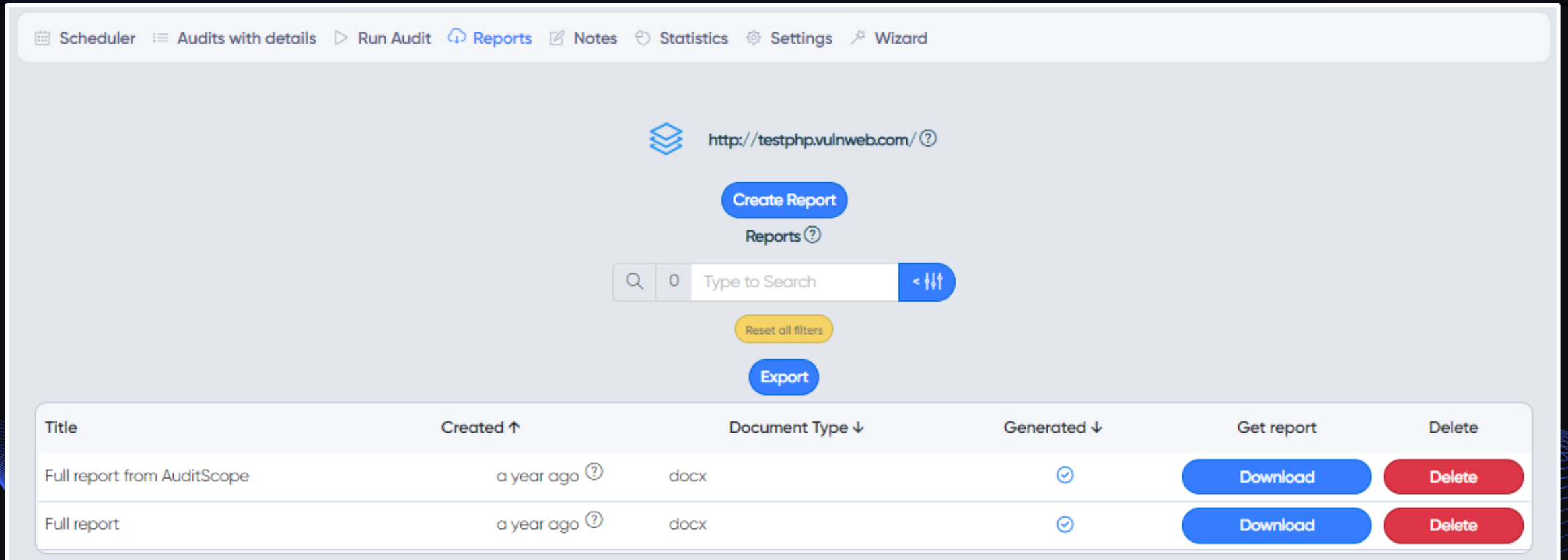
Asset	Analyzing status	Date	Issues	not issues	resolved	Actions
rayfon@list.ru	done	2023-06-27 at 09:53	5	0	0	view
donky.party	done	2023-06-27 at 09:52	15	0	0	view
apple.com	done	2023-02-08 at 09:55	5000	0	0	view
https://mail.ru/	done	2023-02-08 at 07:35	5001	0	0	view
https://twitter.com/	done	2023-02-08 at 07:35	5002	0	0	view
john@gmail.com	done	2023-02-08 at 07:32	307	0	0	view
admin@gmail.com	done	2023-02-08 at 07:31	196	0	0	view

The screenshot shows the detailed view of an asset scan for 'https://twitter.com/'. At the top, there is a 'hide' button and a 'select scan' dropdown. Below that is a search bar and a dropdown menu for 'Show 10'. The main area is a table listing issues with columns for 'Select', 'Audit', 'Issue type', and 'data'. Each row represents an issue with its type and a 'View data' button.

Select	Audit	Issue type	data
<input type="checkbox"/>	GrayhatwarfareShorteners	ISSUE	View data
<input type="checkbox"/>	GrayhatwarfareShorteners	ISSUE	View data
<input type="checkbox"/>	GrayhatwarfareShorteners	ISSUE	View data
<input type="checkbox"/>	GrayhatwarfareShorteners	ISSUE	View data
<input type="checkbox"/>	GrayhatwarfareShorteners	ISSUE	View data
<input type="checkbox"/>	GrayhatwarfareShorteners	ISSUE	View data
<input type="checkbox"/>	GrayhatwarfareShorteners	ISSUE	View data
<input type="checkbox"/>	GrayhatwarfareShorteners	ISSUE	View data
<input type="checkbox"/>	GrayhatwarfareShorteners	ISSUE	View data
<input type="checkbox"/>	GrayhatwarfareShorteners	ISSUE	View data

Report System

Convenient report generator generates customizable reports from the facts, results, and resources extracted during a vulnerability assessment. It includes a QR code, allowing you to easily access the HTML-based results right in your browser - ensuring that you don't miss anything in your report. Generate your custom report, and you are good to go.



The screenshot displays the 'Reports' section of a web application. At the top, a navigation bar includes 'Scheduler', 'Audits with details', 'Run Audit', 'Reports', 'Notes', 'Statistics', 'Settings', and 'Wizard'. The main content area shows the target URL 'http://testphp.vulnweb.com/' with a 'Create Report' button and a 'Reports' link. Below this is a search bar with '0' results and a 'Type to Search' input, accompanied by a 'Reset all filters' button and an 'Export' button. A table lists the generated reports:

Title	Created ↑	Document Type ↓	Generated ↓	Get report	Delete
Full report from AuditScope	a year ago ?	docx	✓	Download	Delete
Full report	a year ago ?	docx	✓	Download	Delete

Report generating

The report generator empowers you to craft comprehensive reports by seamlessly incorporating all vulnerability information or selectively opting for specific elements. For instance, you can focus solely on critical findings of high severity. This flexibility ensures that your final report is both tailored and visually appealing.

The screenshot displays the report generator's configuration interface. It features two sections for selecting content to include in the report. The first section, 'What notes include?', has a checked 'Add Notes' option and a table with two entries: 'DOM-based Cross-Site Scripting (XSS)' with a 'HIGH' severity and 'Open port(s) identified' with a 'NOTICE' severity. The second section, 'What data to include in the report?', has 'Select all' checked, along with 'Files', 'Status', 'CWE', and 'Checklists'. The third section, 'What checklists include?', has a table with one entry: 'Web App Penetration Testing Checklist'.

Name	Severity	Created
DOM-based Cross-Site Scripting (XSS)	HIGH	4 months ago
Open port(s) identified	NOTICE	4 months ago

Name	Created
Web App Penetration Testing Checklist	4 months ago

Report Generator

Make your own report of audit

- Add Audit Scope
 - Add Notes
 - Checklists
 - Custom Logo
- Custom document header
 - Indicate author
- Add custom content
- Add report summary

What document type to generate?

MS Office edition

Title

Full report

Report generating

The reports encompass a wealth of detailed vulnerability insights, encompassing their exact location, comprehensive descriptions, and effective remediation methods. Moreover, the reports feature a recon section that outlines the technologies employed, ports utilized, and the target's IP address. This meticulous combination ensures that the reports offer a holistic view, empowering you with actionable intelligence to enhance security measures.

Facts about vulnerabilities

Title	CWE	CVSS3	Score	Severity
Description				
Extra data [Optional]				
SQL-injection	89	10.0	5	critical

SQL injection (SQLi) is a type of security vulnerability that allows an attacker to manipulate SQL queries to access or modify data stored in a database. SQL is a programming language used to manage and manipulate relational databases, and it is commonly used by web applications to store and retrieve data.


SQL injection attacks occur when an attacker is able to insert malicious SQL statements into an application's input fields, such as search or login forms. This can trick the application into executing unintended SQL commands, which can allow the attacker to view or modify sensitive data, or even take control of the entire database.


There are several types of SQL injection attacks, including:

- Union-based SQLi: where the attacker adds an SQL query to extract data from another table
- Error-based SQLi: where the attacker uses SQL queries that generate errors to extract information from the database
- Blind SQLi: where the attacker sends queries that do not return any results, but can be used to infer information about the database

To prevent SQL injection attacks, web developers should implement secure coding practices, such as input validation and parameterized queries, which can help prevent attackers from injecting malicious SQL statements. Additionally, organizations should regularly monitor their databases for unusual activity and conduct regular security audits to identify and mitigate any vulnerabilities that may exist.

In the event of a suspected SQL injection attack, organizations should take immediate steps to mitigate the attack, such as disabling the affected application or implementing security patches to prevent further exploitation. Additionally, affected databases should be examined for signs of compromise and any compromised data should be restored from backups, if possible.


[WafBypass](#)


[Xsscr4py](#)

Technology

Value
ThinkPHP 5.0
NT 10.0
Wapiti 3.0.0

Sub-domain

Value
www.donky.party

IP v6

Value
2606:4700:3032::6815:354d
2606:4700:3035::ac43:d264
::ffff:216.58.214.20

IP v4

Value
127.0.0.1
172.67.210.100
104.21.48.0

Support system

The support system enables you to swiftly access assistance from our developers by creating a request through our support service. You can generate a request related to any feature of Cryeye and receive prompt support across all functionalities. Within the ticket page, you can view existing tickets, open them to track their status, or even modify the tickets to suit your needs.

Workspaces system Breach detection Active Directory **Support**

Tickets New Statistics

[Audits need clarification]: [Parth, WafBypass, Xsscrapy, Sqlmap, Uniscan]
[SQL-injection]
SQL injection (SQLi) is a type of security vulnerability that allows an attac...
12 days ago
Resolved Audit Facts 3. Normal

[Audits need clarification]: [HostHeaderAttackTest]
[Host header injection attack]
The host header specifies which website or web application sho...
12 days ago
Resolved Audit Facts 3. Normal

Search: 2 Type to Search
Status: -- Resolved [2]
Priority: --

HIDE RESPOND TO TICKET

Actions required: 1

RESPOND TO THIS TICKET

Comment/Resolution required

Ok. Thank you! :)

New status ?

Attach File (optional) ?

Choose file(s) Browse

CREATE

Support system

The screenshot shows a ticket detail page for a ticket titled "[Audits help to fix]: [Lance]". The top navigation bar includes "Tickets", "New", "Ticket", and "Statistics". On the left, there is a sidebar with a "HIDE TICKET SUMMARY" button, a table of ticket details, another "HIDE TICKET SUMMARY" button, and a "SHOW RESPOND TO TICKET" button. The table contains the following information:

Status	Open
Queue	Audit Facts
Priority	3. Normal
Submitted at	a month ago ?
Assigned to	Unassigned

The main content area shows a search bar with "1" results and a "Type to Search" input. Below the search bar, a "Ticket Opened" notification from "Gleb" is shown, dated "a month ago". The ticket description is: "[Remote Code Execution (RCE)] Remote code execution is the ability an attacker has to access someone else's computing device and make changes, no matter where the device is geographically located. Vulnerabilities can provide an attacker with the ability to execute malicious code and take complete control of an affected system with the privileges of the user running the application. After gaining access to the system, attackers will often attempt to elevate their privileges."



















The screenshot shows a "SUBMIT A TICKET" form. At the top, it indicates "Actions required: 3". The form includes a "Queue" dropdown menu (required), a "Summary of the problem" text area (required) containing "I can't make this action", a "Description of your issues" text area (required) containing "When I do first, I receive second. But I expect a third." and "Also, there are extra details...", a "Priority" dropdown menu (required) set to "3. Normal", and an "Attach File (optional)" section with a "Browse" button. A green "CREATE" button is at the bottom.

An example of a ticket creation panel with the ability to sort by the importance of the request

This close-up shows the "Priority" dropdown menu. The menu is open, displaying a list of priority levels: "3. Normal" (selected), "1. Critical", "2. High", "4. Low", and "5. Very Low". The "CREATE" button is visible at the bottom of the form.

Social media mentions

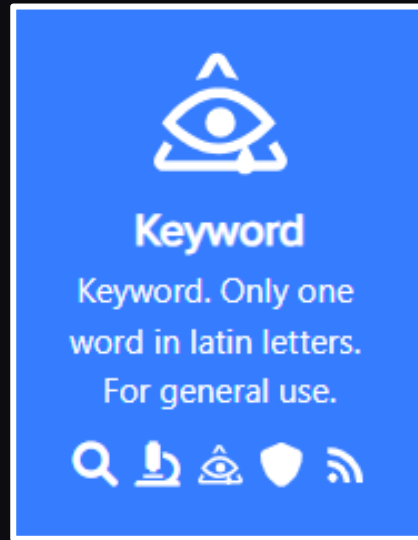
With SocialMediaMentionsFounder and Brand Parser, you gain the power to instantly track real-time mentions across major social media platforms, including Facebook, Instagram, and Twitter, where millions of users engage daily. Furthermore, you'll have the ability to access the latest updates from news websites, track discussions on Reddit, and even explore multimedia content on platforms like Dailymotion and Vimeo.

Target	Source	Posted date	Content	Sentiment	URL	State	Modified at
 cr y e y e cry eye	 Keyword web	21 hours ago 	The Cryeye Project, Worlds largest automated security aggregator with over 1500+ auditing scripts th... show more	neutral	https://cryeye.net/ 	 New	12 hours ago 
 cr y e y e cry eye	 Keyword facebook	21 hours ago 	May 24, 2021 — Why choose #Cryeye Project? Most of the tools on the market do not allow you to do cu... show more	neutral	https://www.facebook.com/Cryeye.CQR/photos/a.1743791565882834/2819500491645264/?type=3 	 New	12 hours ago 
 cr y e y e cry eye	 Keyword web	21 hours ago 	Jul 15, 2022 — The Cryeye project, Worlds largest automated security aggregator with over 1,500+ aud... show more	neutral	https://www.linkedin.com/company/cryeye-cqr 	 New	12 hours ago 

Social media mentions

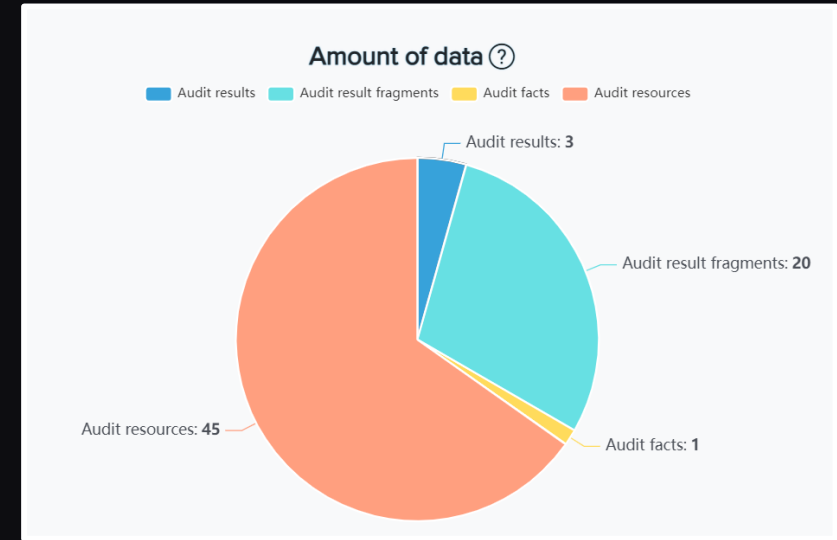
To start you just need to select the "Keyword" asset and run the audit SocialMediaMentionsFounder and Brand Parser. Convenient filters are available, content can be divided into:

- Resource where mention was found
- Post release date
- Post content
- Sentiment score (positive, negative, neutral)
- Link to post




Keyword
Keyword. Only one word in latin letters.
For general use.

Icons: Search, Document, Eye, Shield, RSS



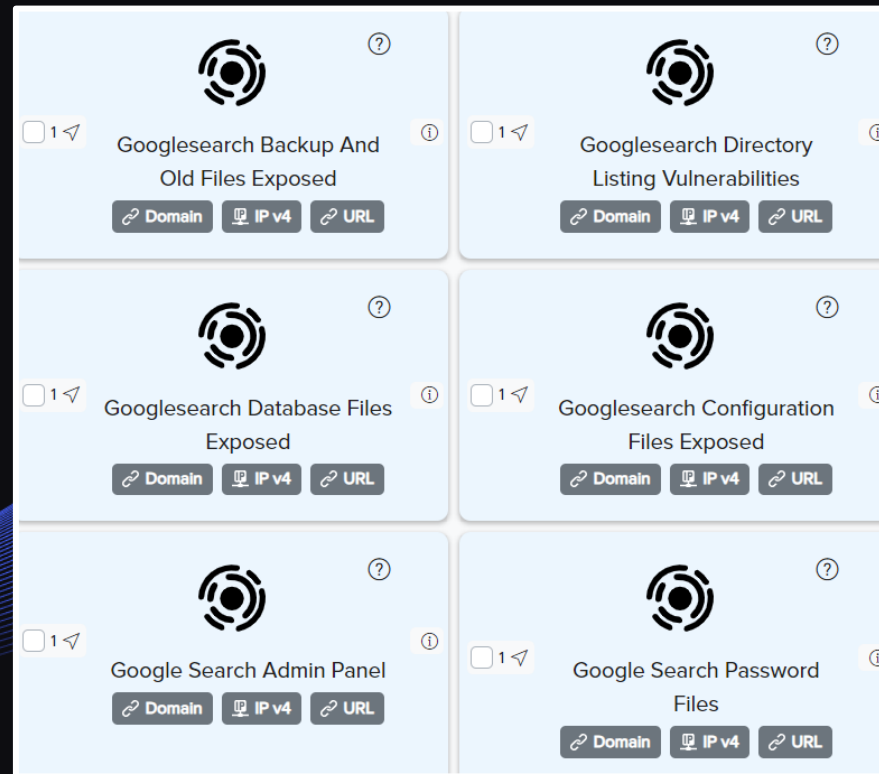
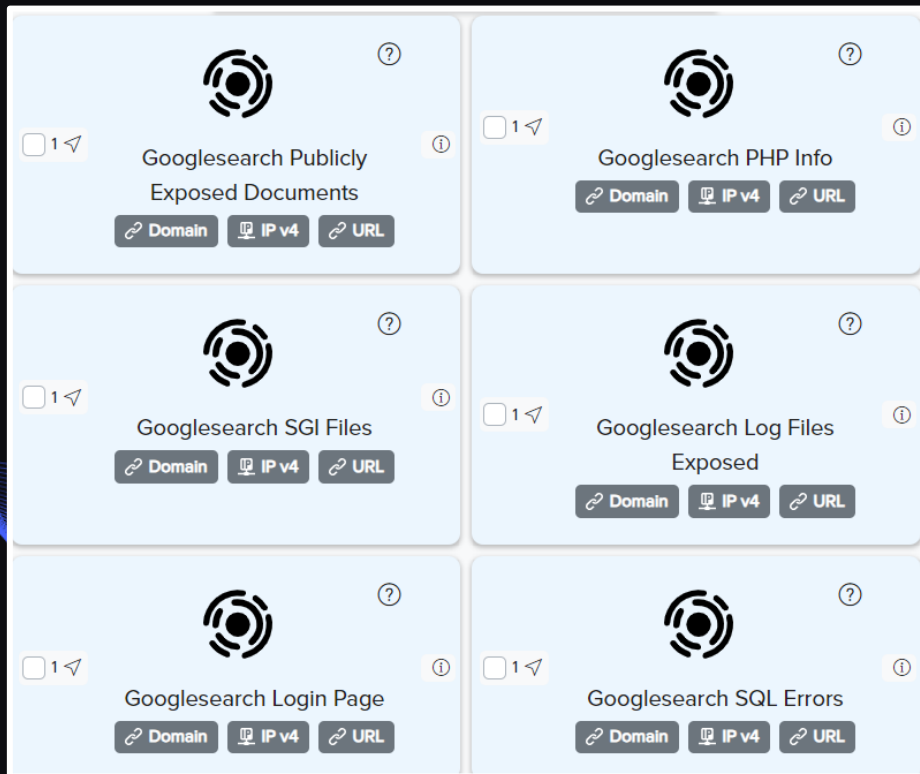
Target	Audit Title
 cryeye Keyword	 Brand parser
 cryeye Keyword	 Social media mentions founder

Target	Source	Posted date	Content	Sentiment	URL	State	Modified at
 cryeye	facebook	21 hours ago	CryEye detects intrusions when they occur using real-time visibility of network traffic through an i... show more	neutral	https://m.facebook.com/Cryeye.CQR/photos/3092330741028903/?locale=ms_MY	+ New	12 hours ago

Mentions with Google Dorks

Google Searcher - audit for search mentions by keywords using the functionality of Google Dorks with convenient filters and ability to split into:

- Title (title of the article or found resource)
- Link to source
- Snippet - a short preview of the content



Network Scanning Solutions

NetworkScan

Afrog netscan

Db Scanner

Ero SMB

Frog Auth NetworkScanner

Ladon go recon

Silver Scan

Nuclei netscan

Login Hunter NetworkScan

Nmap portscan netscan

Nmap Vulners NetworkScan

Ladon go vulnerability

HostGetter

NmapBannersAndTitleGetter

OsDetection

Pocsplloit Netscan

SmbOsDetection

Router Sploit NetworkScanner

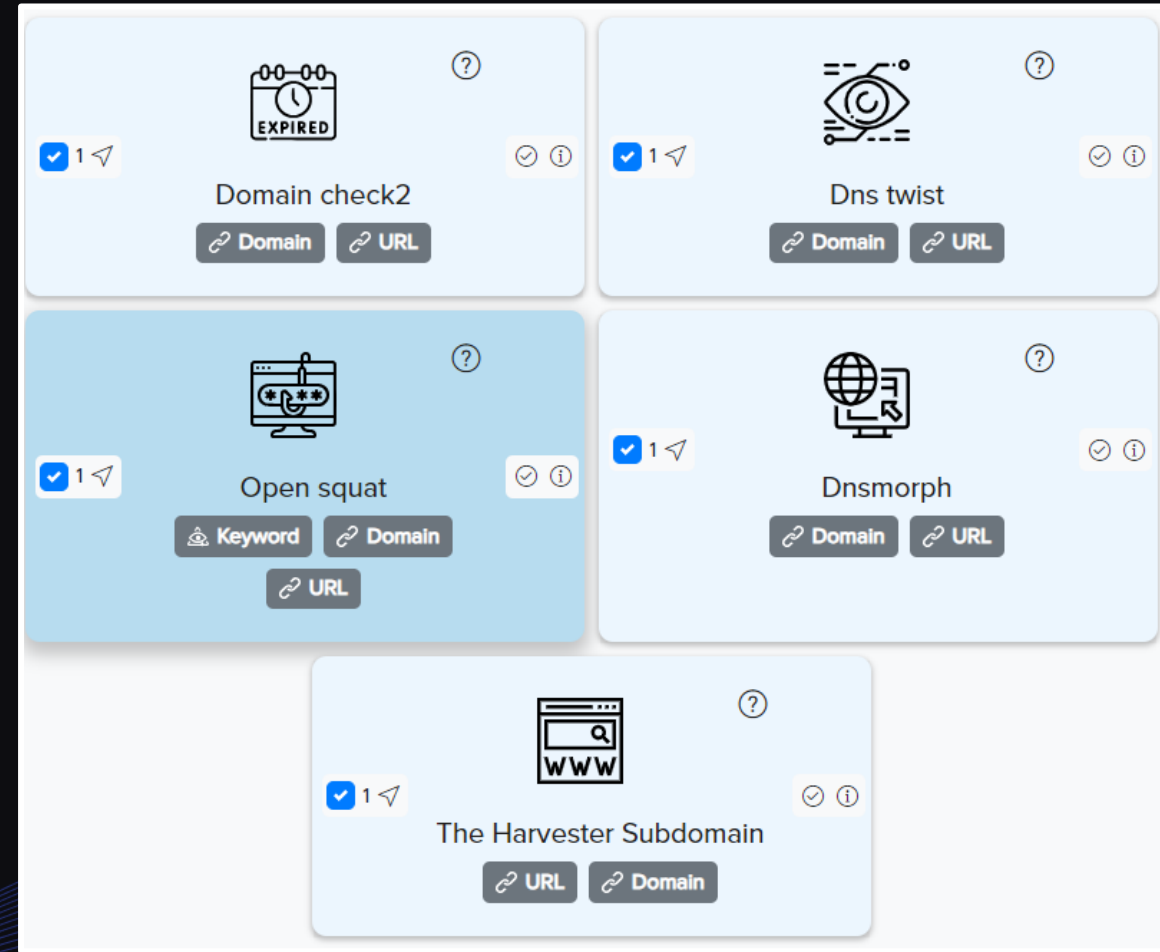
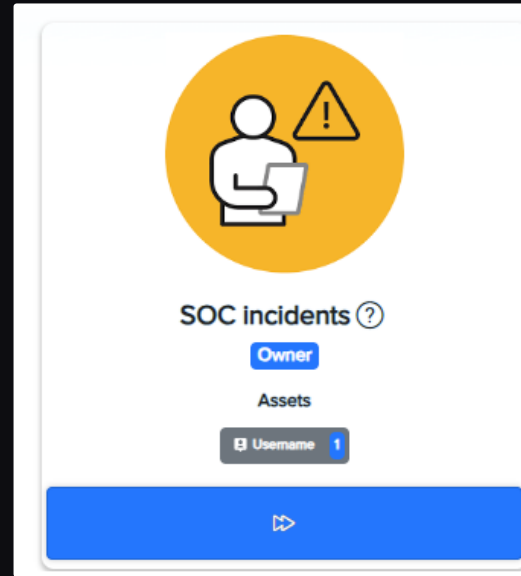
Our Cryeye Cybersecurity platform includes a flexible Network Scanner that lets you run all audits concurrently or perform selected checks.

Our tools cover all you need to identify vulnerabilities, detect illegal access, or evaluate security systems.

Combining Nmap portscan, Smb Detection, Ladon Go Recon, and more offers a robust network security solution. Make sure your infrastructure is safe using all-in-one or precisely targeted scans.

SOC service/Phishing

Using the CryEye functionality, you can actively track phishing incidents in real-time based on keywords, domains, and URLs. This will greatly simplify and enhance the effectiveness of your SOC team, allowing you to quickly detect suspicious activities.



Forensic agent

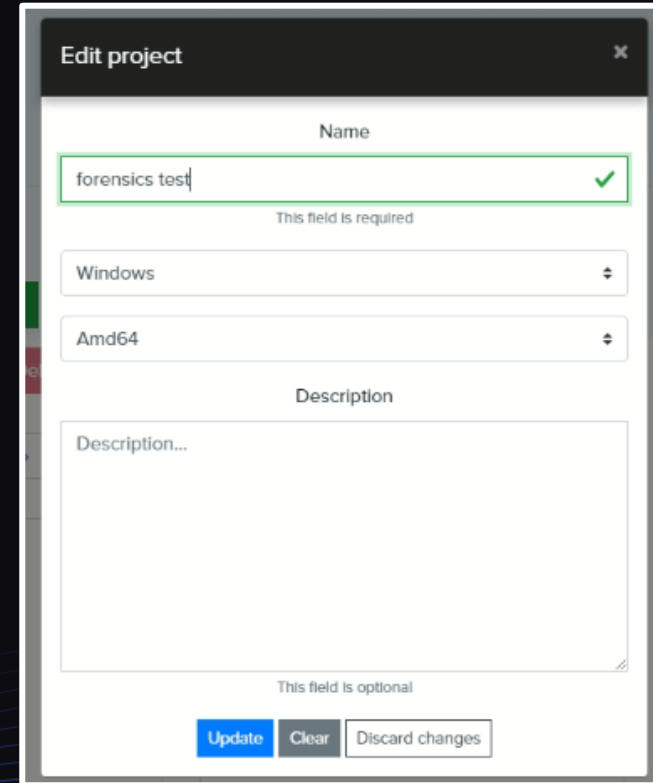
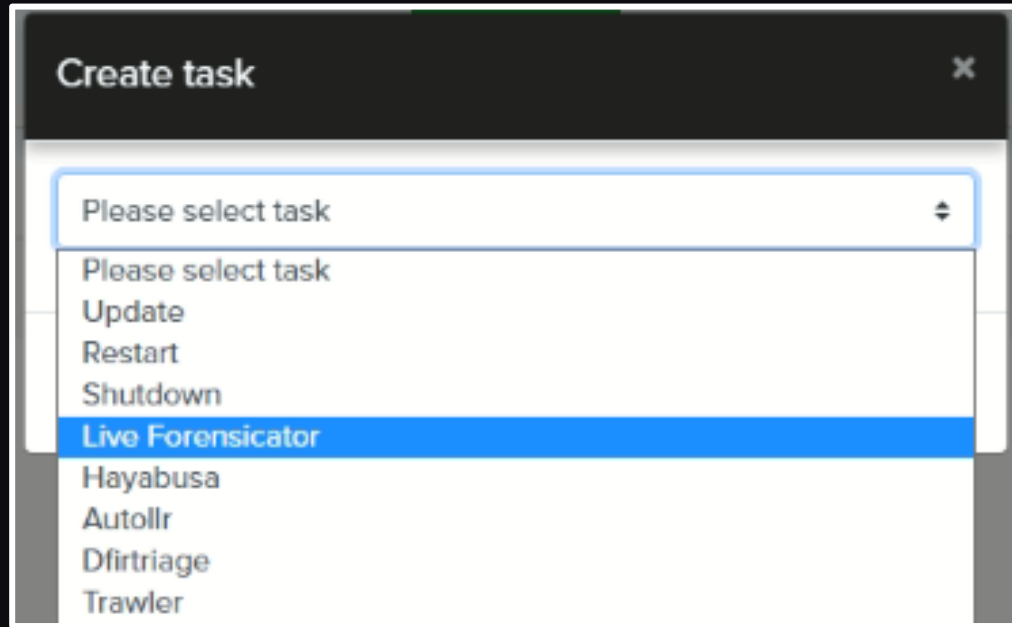
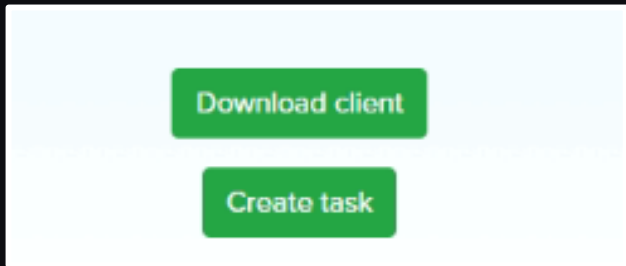
Forensic agent is part of CryEye tools, its aim is to assist Forensic Investigators and Incidence responders in carrying out a quick live forensic investigation. It achieves this by gathering different system information for further review for anomalous behaviour or unexpected data entry, it also looks out for unusual files or activities and points it out to the investigator.

```
[*] Gathering Network & Network Settings
[!] Network Information Gathering Completed
[*] Gathering User & Account Information
[!] User & Account Information Gathering Completed
[*] Gathering Installed Programs
[!] Installed Programs Gathering Completed
[*] Gathering System Information
[!] System Information Gathering Completed
[*] Gathering Processes and Tasks
[!] Gathering of Processes and Tasks Completed
[*] Checking Registry for persistence
[!] Registry Check Completed
[*] Running Other Final Checks
[*] Lets Get hold of some webloggs
[!] NOTE: This can take a while if you have large Apache/IIS Log Files
[!] Cannot find Tomcat software keys in registry
[!] Cannot find Tomcat install path in registry
[*] Creating and Formatting our Index file
[*] Collecting GPO Results
```

The screenshot displays the CryEye forensic agent interface. On the left is a vertical menu with the following items: Home, Users & Accounts, System Information, Network Information, System Processes, Other Information, Event Log Analysis (highlighted in red), User Actions, Logon Events, Object Access, Process Execution, and Suspicious Activities. On the right, the 'System Information' section is expanded, showing a list of items: Installed Programs, Installed Programs - From Registry, Environment Variables, System Information, Operating System Information, Hotfixes, and Windows Defender Status.

Forensic agent

To get started, you simply need to download the agent onto your device and run it to collect information about the machine.



Key Location: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\prbrush.exe, Entry Name: (default), Entry Value: C:\Windows\System32\mspaint.exe	Medium	Registry	T1546: Event Triggered Execution	Potential App Path Hijacking - Executable Name does not match Registry Key
Key Location: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\WRITE.EXE, Entry Name: (default), Entry Value: *C:\Program Files\Windows NT\Accessories\WORDPAD.EXE*	Medium	Registry	T1546: Event Triggered Execution	Potential App Path Hijacking - Executable Name does not match Registry Key
FileType: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\msstyles\file\shell\open\command, Current Association: C:\Windows\system32\rundll32.exe C:\Windows\system32\shell32.dll,Control_RunDLL C:\Windows\system32\desk.cpl desk,@Appearance /Action:OpenMSTheme /file:%1*	High	Registry	T1546.001: Event Triggered Execution: Change Default File Association	Possible File Association Hijack - Suspicious Keywords

Forensic agent

Automatic audit of incidents, collection of logs, actions and information about target machine.

Offline

Download client

Create task

1

<input type="checkbox"/>	Delete				
<input type="checkbox"/>		2023-10-08 at 05:20	Hayabusa	Queued	Details
<input type="checkbox"/>		2023-10-06 at 14:13	Shutdown	Done	Details
<input type="checkbox"/>		2023-10-06 at 14:12	Trawler	Done	Details

Key Location: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\WRITE.EXE, Entry Name: (default), Entry Value: "C:\Program Files\Windows NT\Accessories\WORDPAD.EXE"

Medium

Registry

T1546: Event Triggered Execution

Potential App Path Hijacking - Executable Name does not match Registry Key

FileType: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\msstylesfile\shell\open\command, Current Association: C:\Windows\system32\rundll32.exe C:\Windows\system32\shell32.dll,Control_RunDLL C:\Windows\system32\desk.cpl desk,@Appearance /Action:OpenMSTheme /file:"%1"

High

Registry

T1546.001: Event Triggered Execution: Change Default File Association

Possible File Association Hijack - Suspicious Keywords

Registry Path: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{08EB4FA6-6FFD-11D1-B0E0-00C04FD8DCA6}\InprocServer32, DLL Path: C:\Windows\system32\dsadmin.dll

Medium

Registry

T1546.015: Event Triggered Execution: Component Object Model Hijacking

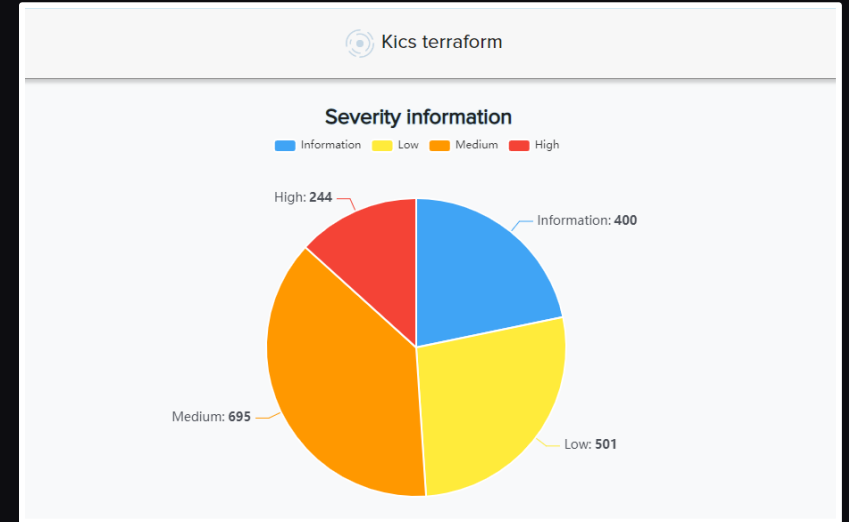
Potential COM Hijack

Infrastructure security scanning

Infrastructure code security scanning, is the process of evaluating the security of the code used to define and configure an organization's infrastructure.

Infrastructure code security scanning helps organizations identify and address security vulnerabilities and misconfigurations early in the development and deployment process. By ensuring the security of infrastructure code, organizations can reduce the risk of security breaches, ensure compliance, and improve the overall security posture of their infrastructure.

Example of Infrastructure scanning result:



Example of Infrastructure scanning result:

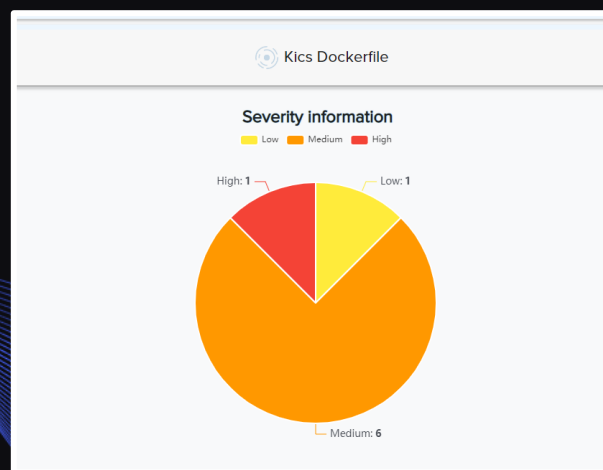
Name	Description	Platform	Category	Severity	
CMK Rotation Disabled	Customer Master Keys (CMK) must have rotation enabled, which means the attribute 'enable_key_rotation' must be set to 'true' when the key is enabled.	Terraform	Observability	HIGH	
CloudFront Without Minimum Protocol TLS 1.2	CloudFront Minimum Protocol version should be at least TLS 1.2	Terraform	Insecure Configurations	HIGH	
Cloudfront Viewer Protocol Policy Allows HTTP	Checks if the connection between CloudFront and the viewer is encrypted	Terraform	Encryption	HIGH	
DB Instance Publicly Accessible	RDS must not be defined with public interface, which means the field 'publicly_accessible' should not be set to 'true' (default is 'false').	Terraform	Insecure Configurations	HIGH	
DB Instance Storage Not Encrypted	AWS DB Instance should have its storage encrypted by setting the parameter to 'true'. The storage_encrypted default value is 'false'.	Terraform	Encryption	HIGH	

Infrastructure security scanning for Docker files and images

Infrastructure code security scanning of Docker files refers to the process of evaluating the security of Dockerfiles, which are used to build Docker images.

By conducting infrastructure code security scanning of Docker files, organizations can identify potential security risks and vulnerabilities in the containerization process. This allows them to address these issues early on, ensuring that Docker images are built securely and minimizing the risk of container-based attacks or compromises.

Example of Docker files Infrastructure scan result:



A table titled 'Vulnerabilities' showing the results of a scan. The table has columns for Name, Description, Platform, Category, and Severity. It lists four vulnerabilities with their respective descriptions and severity levels.

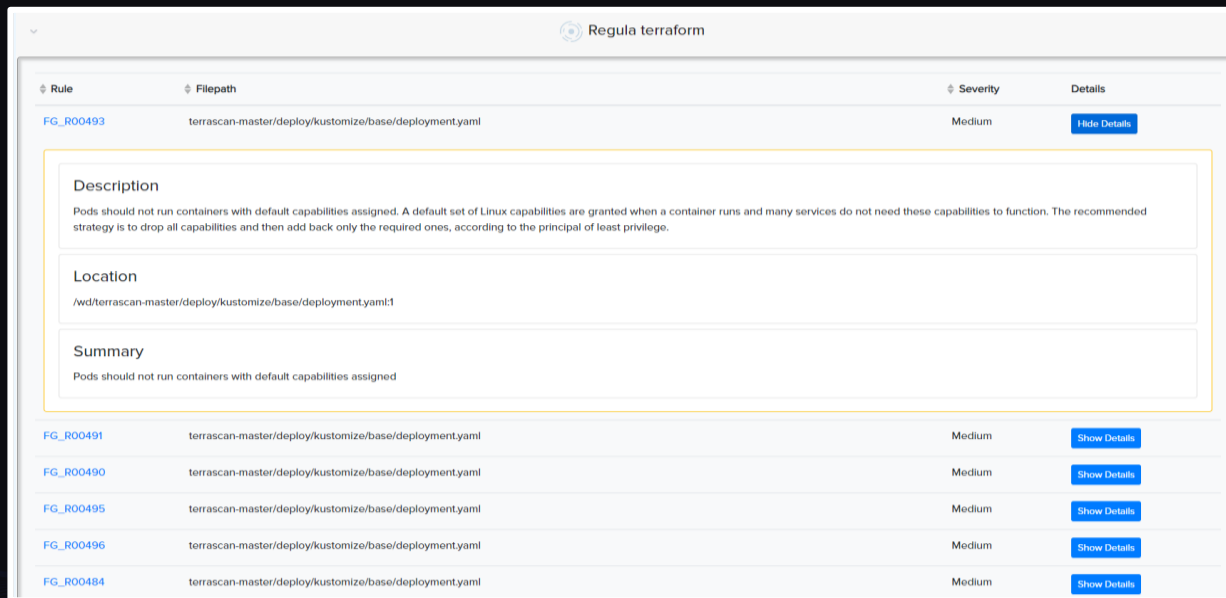
Name	Description	Platform	Category	Severity
Missing User Instruction	A user should be specified in the dockerfile, otherwise the image will run as root	Dockerfile	Build Process	HIGH
Apt Get Install Pin Version Not Defined	When installing a package, its pin version should be defined	Dockerfile	Supply-Chain	MEDIUM
RUN Instruction Using 'cd' Instead of WORKDIR	When using RUN command 'cd' should only be used for full path. For relative path make use of WORKDIR command instead.	Dockerfile	Build Process	MEDIUM
Healthcheck Instruction Missing	Ensure that HEALTHCHECK is being used. The HEALTHCHECK instruction tells Docker how to test a container to check that it is still working	Dockerfile	Insecure Configurations	LOW

Terraform Infrastructure security

Infrastructure code security scanning of Terraform code refers to the process of evaluating the security of Terraform configuration files.

Infrastructure code security scanning of Terraform code helps organizations identify and address security issues in their infrastructure deployments. By conducting these scans, organizations can reduce the risk of misconfigurations, vulnerabilities, or non-compliance, ultimately strengthening the security of their infrastructure provisioned with Terraform.

Example of Terraform Infrastructure scan result:



The screenshot shows the Regula terraform interface. At the top, it says "Regula terraform". Below that is a table with columns: Rule, Filepath, Severity, and Details. The first row is highlighted with a yellow border and contains the following information:

Rule	Filepath	Severity	Details
FG_R00493	terrascan-master/deploy/kustomize/base/deployment.yaml	Medium	Hide Details

The details for rule FG_R00493 are shown in a yellow-bordered box:

- Description:** Pods should not run containers with default capabilities assigned. A default set of Linux capabilities are granted when a container runs and many services do not need these capabilities to function. The recommended strategy is to drop all capabilities and then add back only the required ones, according to the principal of least privilege.
- Location:** /wd/terrascan-master/deploy/kustomize/base/deployment.yaml:1
- Summary:** Pods should not run containers with default capabilities assigned

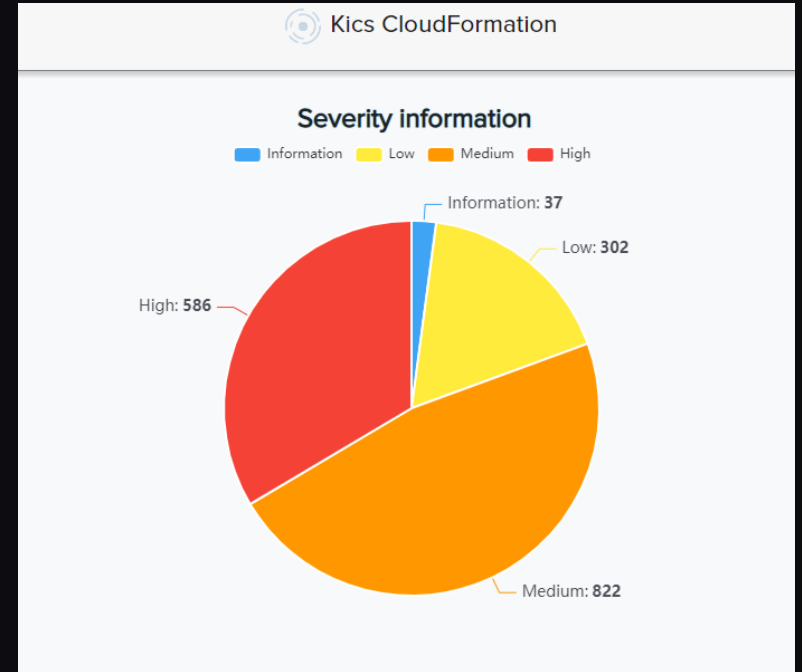
Below the details box, there is a list of other findings:

FG_R00491	terrascan-master/deploy/kustomize/base/deployment.yaml	Medium	Show Details
FG_R00490	terrascan-master/deploy/kustomize/base/deployment.yaml	Medium	Show Details
FG_R00495	terrascan-master/deploy/kustomize/base/deployment.yaml	Medium	Show Details
FG_R00496	terrascan-master/deploy/kustomize/base/deployment.yaml	Medium	Show Details
FG_R00484	terrascan-master/deploy/kustomize/base/deployment.yaml	Medium	Show Details

AWS CloudFormation Infrastructure security

Infrastructure code security scanning of AWS CloudFormation code refers to the process of evaluating the security of AWS CloudFormation templates.

Infrastructure code security scanning of AWS CloudFormation code helps organizations identify and address security issues in their AWS infrastructure deployments. By conducting these scans, organizations can ensure that their CloudFormation templates are configured securely, reduce the risk of misconfigurations or vulnerabilities, and align with best security practices.



Example of AWS Cloud Formation Infrastructure scan result:

Name	Description	Platform	Category	Severity	
ALB Listening on HTTP	AWS Application Load Balancer (alb) should not listen on HTTP	CloudFormation	Networking and Firewall	HIGH	🔍
CMK Unencrypted Storage	Ensure that storage is encrypted.	CloudFormation	Encryption	HIGH	🔍
CloudFront Without Minimum Protocol TLS 1.2	CloudFront Minimum Protocol version should be at least TLS 1.2	CloudFormation	Insecure Configurations	HIGH	🔍
Cloudfront Viewer Protocol Policy Allows HTTP	Checks if the connection between CloudFront and the viewer is encrypted	CloudFormation	Encryption	HIGH	🔍
Connection Between CloudFront Origin Not Encrypted	Checks if the connection between the CloudFront and the origin server is encrypted	CloudFormation	Encryption	HIGH	🔍

Ansible Infrastructure security

Infrastructure code security scanning of Ansible code refers to the process of evaluating the security of Ansible playbooks and configuration files.

By conducting infrastructure code security scanning of Ansible code, organizations can identify and address security issues in their infrastructure automation processes. This helps ensure that Ansible playbooks and configuration files are built securely, minimizing the risk of misconfigurations, vulnerabilities, or non-compliance.

Example of Ansible Infrastructure scan result:

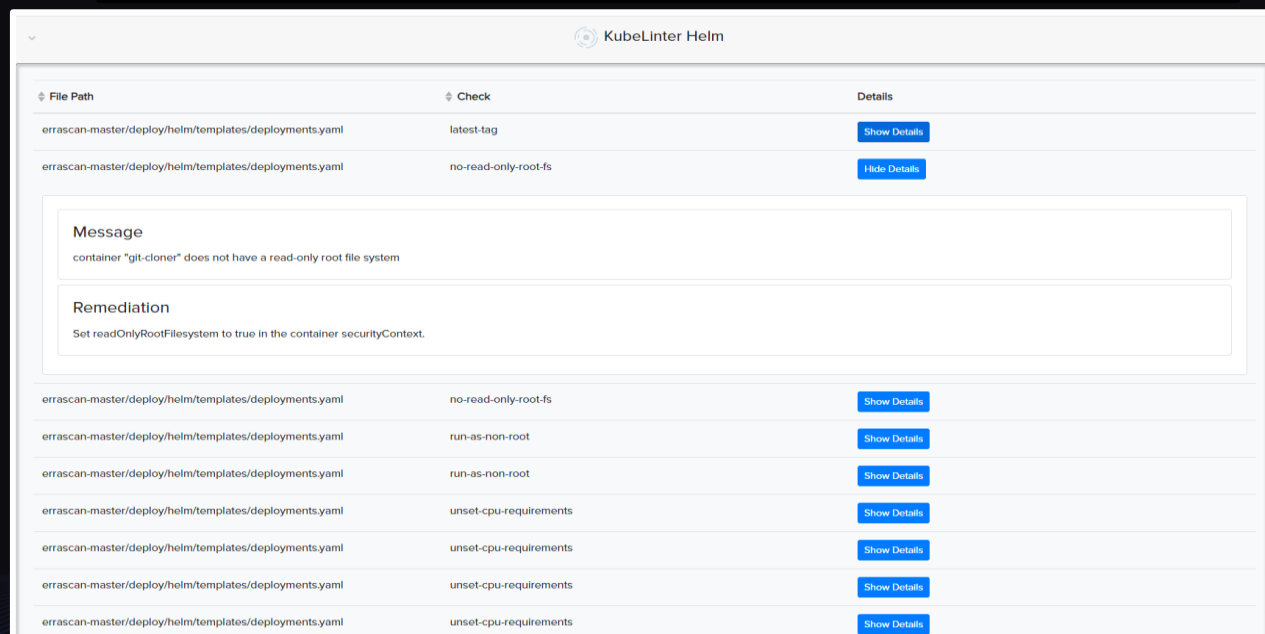
Name	Description	Platform	Category	Severity	
IAM Policies With Full Privileges	IAM policies shouldn't allow full administrative privileges (for all resources)	CloudFormation	Access Control	HIGH	
IAM Policy Grants Full Permissions	IAM policy should not grant full permissions to resources from the get-go, instead of granting permissions gradually as necessary.	CloudFormation	Access Control	HIGH	
Passwords And Secrets - Generic Password	Query to find passwords and secrets in infrastructure code.	Common	Secret Management	HIGH	
Unknown Port Exposed To Internet	AWS Security Group should not have an unknown port exposed to the entire Internet	CloudFormation	Networking and Firewall	HIGH	
Unrestricted Security Group Ingress	AWS Security Group Ingress CIDR should not be open to the world	CloudFormation	Networking and Firewall	HIGH	
Auto Scaling Group With No Associated ELB	AWS Auto Scaling Groups must have associated ELBs to ensure high availability and improve application performance. This means the attribute 'LoadBalancerNames' must be defined and not empty.	CloudFormation	Availability	MEDIUM	
IAM Policies Attached To User	IAM policies should be attached only to groups or roles	CloudFormation	Access Control	MEDIUM	
IAM User Without Password Reset	IAM User Login Profile should exist and have PasswordResetRequired property set to true	CloudFormation	Best Practices	MEDIUM	
Instance With No VPC	EC2 Instances should be configured under a VPC network. AWS VPCs provide the controls to facilitate a formal process for approving and testing all network connections and changes to the firewall and router configurations.	Ansible	Insecure Configurations	MEDIUM	
Security Group Ingress With Port Range	AWS Security Group Ingress should have a single port	CloudFormation	Networking and Firewall	MEDIUM	

Helm Infrastructure security

Infrastructure code security scanning of Helm code refers to the process of evaluating the security of Helm charts. Helm charts are packages that contain the necessary files and configurations to deploy and configure applications on Kubernetes.

Infrastructure code security scanning of Helm code helps organizations identify and address security issues in their Kubernetes deployments. By conducting these scans, organizations can ensure that their Helm charts are configured securely, reduce the risk of misconfigurations or vulnerabilities, and align with best security practices.

Example of Helm Infrastructure scan result:



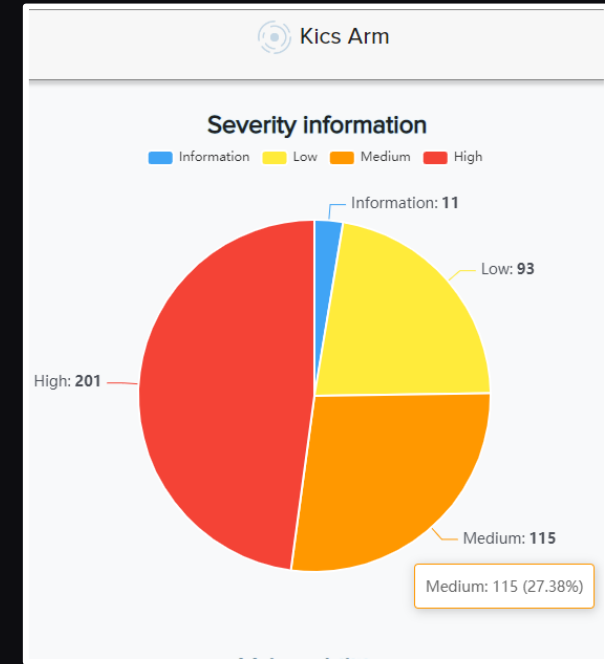
The screenshot displays the KubeLinter Helm interface. At the top, it shows the title 'KubeLinter Helm'. Below this is a table with three columns: 'File Path', 'Check', and 'Details'. The table lists several findings, including 'latest-tag', 'no-read-only-root-fs', 'run-as-non-root', and 'unset-cpu-requirements'. A detailed message is shown for the 'no-read-only-root-fs' check, stating: 'container "git-cloner" does not have a read-only root file system'. Below the message is a 'Remediation' section with the instruction: 'Set readOnlyRootFilesystem to true in the container securityContext.'.

File Path	Check	Details
errascan-master/deploy/helm/templates/deployments.yaml	latest-tag	Show Details
errascan-master/deploy/helm/templates/deployments.yaml	no-read-only-root-fs	Hide Details
Message container "git-cloner" does not have a read-only root file system		
Remediation Set readOnlyRootFilesystem to true in the container securityContext.		
errascan-master/deploy/helm/templates/deployments.yaml	no-read-only-root-fs	Show Details
errascan-master/deploy/helm/templates/deployments.yaml	run-as-non-root	Show Details
errascan-master/deploy/helm/templates/deployments.yaml	run-as-non-root	Show Details
errascan-master/deploy/helm/templates/deployments.yaml	unset-cpu-requirements	Show Details
errascan-master/deploy/helm/templates/deployments.yaml	unset-cpu-requirements	Show Details
errascan-master/deploy/helm/templates/deployments.yaml	unset-cpu-requirements	Show Details
errascan-master/deploy/helm/templates/deployments.yaml	unset-cpu-requirements	Show Details

Azure Resource Manager Infrastructure security

Azure Resource Manager is the deployment and management service for Azure. It provides a management layer that enables you to create, update, and delete resources in your Azure account.

Infrastructure code security scanning of Azure Resource Manager code helps organizations identify and address security issues in their Azure deployments. By conducting these scans, organizations can ensure that their ARM templates are configured securely, reduce the risk of misconfigurations or vulnerabilities, and align with best security practices.



Example of ARM Infrastructure scan result:

Name	Description	Platform	Category	Severity
Azure Instance Using Basic Authentication	Azure Instances should use SSH Key instead of basic authentication	AzureResourceManager	Best Practices	HIGH
Azure Managed Disk Without Encryption	Azure Disk Encryption should be enabled	AzureResourceManager	Encryption	HIGH
Key Vault Not Recoverable	Key Vault should have 'enableSoftDelete' and 'enablePurgeProtection' set to true	AzureResourceManager	Backup	HIGH
MySQL Server SSL Enforcement Disabled	'Microsoft.DBforMySQL/servers' should enforce SSL	AzureResourceManager	Networking and Firewall	HIGH
Network Security Group With Unrestricted Access To RDP	Port 3389 (Remote Desktop) is exposed to the Internet	AzureResourceManager	Networking and Firewall	HIGH
Network Security Group With Unrestricted Access To SSH	Port 22 (SSH) is exposed to the Internet	AzureResourceManager	Networking and Firewall	HIGH
Passwords And Secrets - Generic Password	Query to find passwords and secrets in infrastructure code.	Common	Secret Management	HIGH
PostgreSQL Database Server SSL Disabled	Microsoft.DBforPostgreSQL/servers sslEnforcement property should be set to 'Enabled'	AzureResourceManager	Networking and Firewall	HIGH
SQL Database Server Firewall Allows All IPS	SQL Database Server Firewall endIpAddress should not be '255.255.255.255' when startIpAddress is '0.0.0.0' since this allows all IPS	AzureResourceManager	Networking and Firewall	HIGH
Secret Without Expiration Date	All Secrets must have an expiration date defined	AzureResourceManager	Best Practices	HIGH

Password Manager

A password manager is a tool designed to securely store and manage your sensitive data, such as passwords, API keys, and certificates on a platform. The main idea is to offer a safe way to keep all your important information in one place, so you can easily access it whenever you need. Additionally, a password manager allows you to share secrets, like passwords or secure notes, with other users directly through the platform.

