

Helium: Automate Vulnerability Assessment with powerful cloud-based tools



Organization Pain Point



The tools are separately and stand-alone

You must sit all day in front of your computer to run the tools.



Configure the tools take time

Tools are from multiple sources. You must configure it correctly.



Each tool shows a different user interface and results

For new testers, you will not be familiar with several different user interfaces and results.



Lack of OS and Infrastructure

Not all tools can be stable in one infrastructure and operating system. You need more.



Costly with no support

Installing, configuring, and learning the tools by yourself with no support while you've paid high.

User (Pentester) Pain Point



It is difficult to manage and update

You must organize by your self while you use multiple tools from various sources.



Your machine won't stay up along the time

You can't leave them running overnight since your machine are limited.



No scans scheduling

You must do it now, can't be scheduled, while you sleep.



Scan results are stored separately and sometimes lost

You must manage the results carefully.



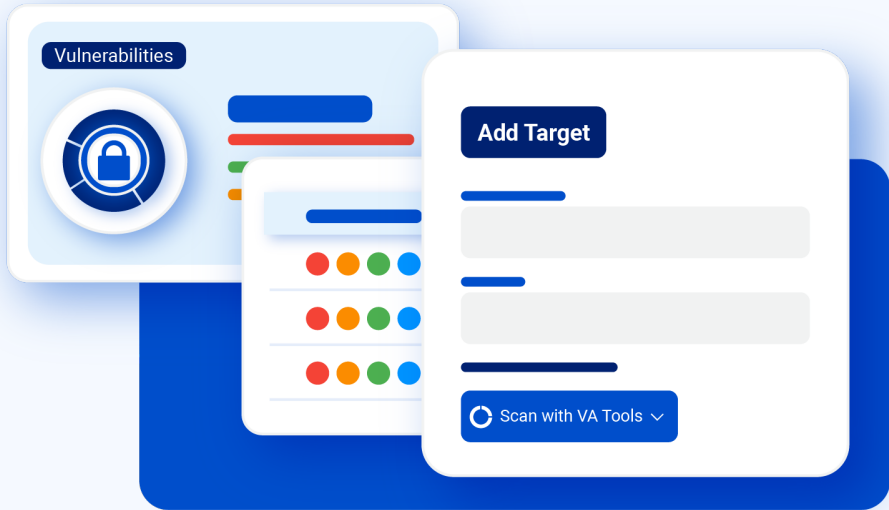
Each tool shows a different user interface and results

For new testers, you will not be familiar with several different user interfaces and results.

Powerful Cloud-based

Vulnerability Assessment Platform

Vulnerability Assessment is the process of identifying risks and vulnerabilities in systems, computer networks, applications, or other parts of the IT ecosystem.



www.helium.sh

Benefits



Automate Continuous Security Assessment

Schedule your scans and periodically evaluate your systems for the vulnerabilities.



Easy to use

No need to install a bunch of tools on your machine. You only need login and run the assessment, no hassle anymore. Helium also provide API Access.



Team Collaboration

Working with the team to collaborate and deliver better security assessment.



Save Time

Don't worry about configuration and maintenance. All you need here and always up to date, including the latest tools.



Speed up your scans

Helium running while you have logout. You can scan and go to sleep. We'll do for the rest.



Cost Efficient for All

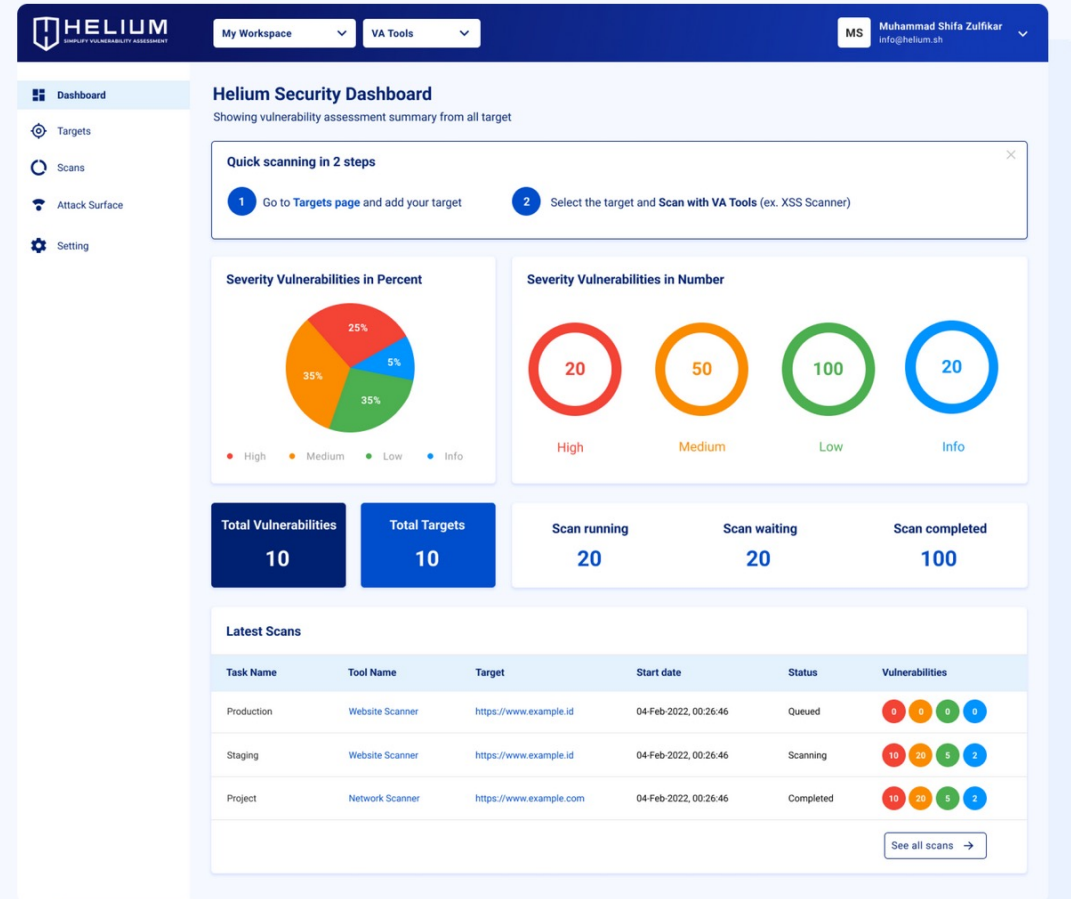
Cost efficient for personal or companies of all size. Helium provides vulnerability scanning with unlimited assessments for affordable price.

Automate Vulnerability Assessment with powerful cloud-based tools

Try to scan your website

I am authorized to scan this target and I agree to the [Terms of Service](#)





HELIUM My Workspace VA Tools MS Muhammad Shifa Zulfikar info@helium.sh

Helium Security Dashboard
Showing vulnerability assessment summary from all target

Quick scanning in 2 steps

- Go to **Targets** page and add your target
- Select the target and **Scan with VA Tools** (ex. XSS Scanner)

Severity Vulnerabilities in Percent

Severity	Percentage
High	25%
Medium	35%
Low	35%
Info	5%

Severity Vulnerabilities in Number

Severity	Count
High	20
Medium	50
Low	100
Info	20

Total Vulnerabilities: 10 **Total Targets: 10**

Scan running: 20 **Scan waiting: 20** **Scan completed: 100**

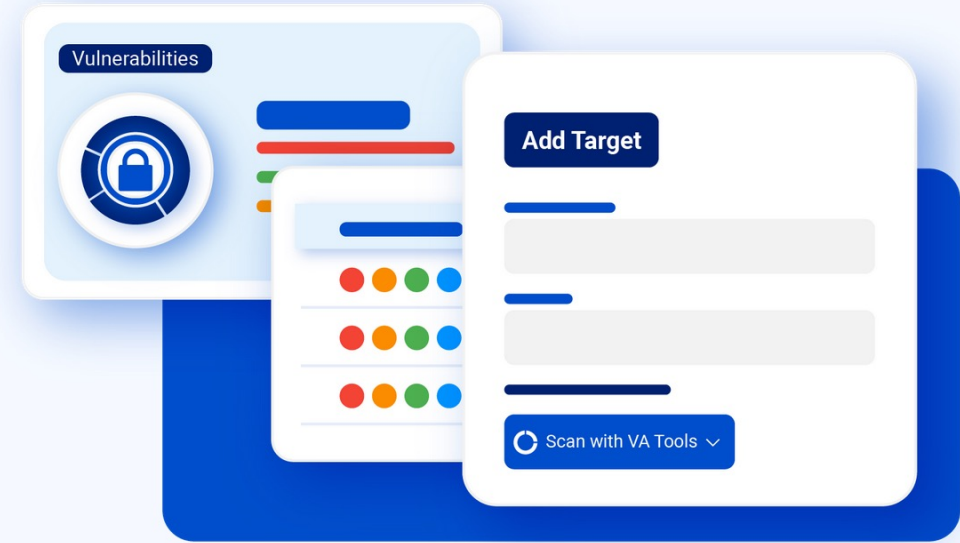
Latest Scans

Task Name	Tool Name	Target	Start date	Status	Vulnerabilities
Production	Website Scanner	https://www.example.id	04-Feb-2022, 00:26:46	Queued	0 High, 0 Medium, 0 Low, 0 Info
Staging	Website Scanner	https://www.example.id	04-Feb-2022, 00:26:46	Scanning	10 High, 20 Medium, 5 Low, 2 Info
Project	Network Scanner	https://www.example.com	04-Feb-2022, 00:26:46	Completed	10 High, 20 Medium, 5 Low, 2 Info

[See all scans →](#)

Explore our full suite of vulnerability assessment tools

Helium Security runs a comprehensive set of vulnerability scans to cover Web Apps, Mobile Apps, Infrastructure and Encryption.



Vulnerability Assessment Scanner

Automatically find vulnerabilities in a few minutes

Website Scanner

Uncover known vulnerabilities that impact web applications: Log4j, SQL Injection, XSS and more thousand vulnerabilities.

Network Scanner

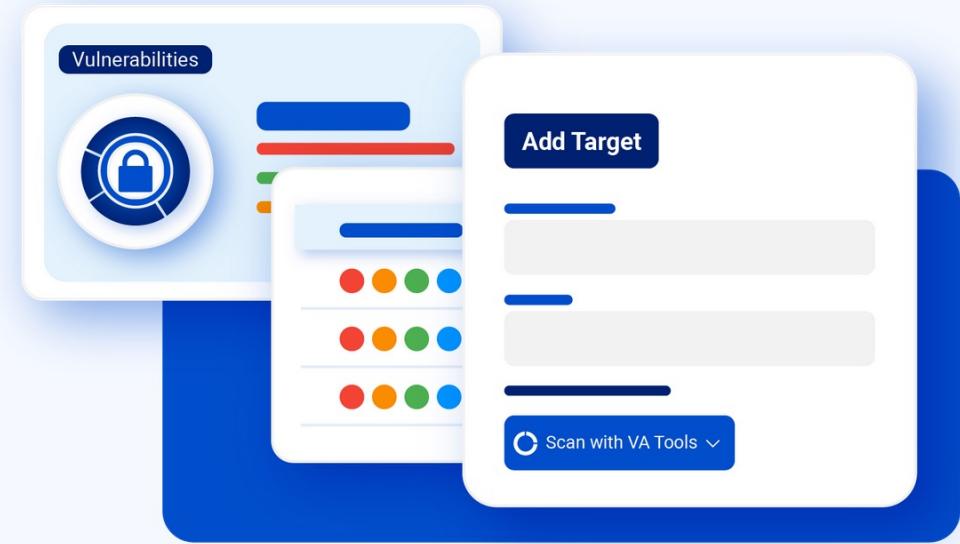
Discover outdated network services, insecure software configuration, missing security patches and more vulnerabilities.

Mobile Apps Scanner

Uncover known vulnerabilities that impact mobile applications (Android and IOS): Insecure Data Storage, Client Code Quality, and more.

Explore our full suite of vulnerability assessment tools

Helium Security runs a comprehensive set of vulnerability scans to cover Web Apps, Mobile Apps, Infrastructure and Encryption.



Pentest Tools

Find vulnerabilities with pentest tools from Reconnaissance to Exploitation

Bruteforce

Find service credentials on Web Apps, SSH, FTP, MySQL, Telnet and more.

Find DNS

Find name servers of a target domain vulnerable to DNS Zone.

Find Git Exposure

Discover source code via exposed .git folder.

Find Open Ports and Services

Discover network services, operating systems, misconfigurations, and more.

Find Security Headers

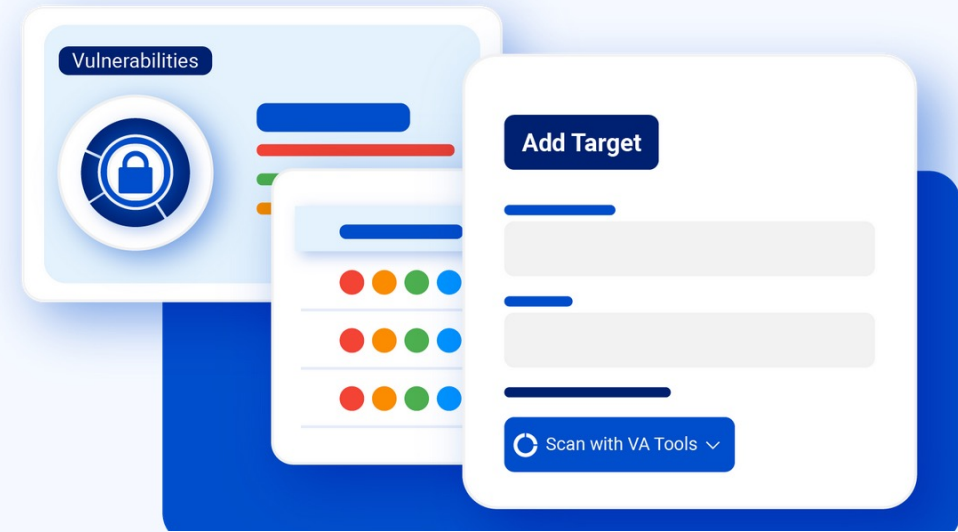
Discover the Security Header policies in place adds another level of protection that can stop common attacks such as code injection, XSS attacks and clickjacking.

Find Subdomain

Discover subdomains and enumerate the vulnerabilities.

Explore our full suite of vulnerability assessment tools

Helium Security runs a comprehensive set of vulnerability scans to cover Web Apps, Mobile Apps, Infrastructure and Encryption.



Find Website Directory

Discover hidden directories and files in website, make it easier for you for information gathering.

Find Website Tech

Find useful information about the technologies used by a target web application - server-side and client-side.

SSL/TLS Scanner

Discover the SSL/TLS configuration of your targets, and detects bad certificates, weak ciphers, Heartbleed, ROBOT, TLS version support, etc.

SQLi Exploitation

Discover SQL Injection vulnerabilities in web applications.

Spring4Shell

Detect and mitigate new zero-day vulnerabilities in the Java Spring Framework.

Website Recon

Find useful information about Misconfiguration and sensitive folder/file used by a target web application - server-side and client-side.

Whois Lookup

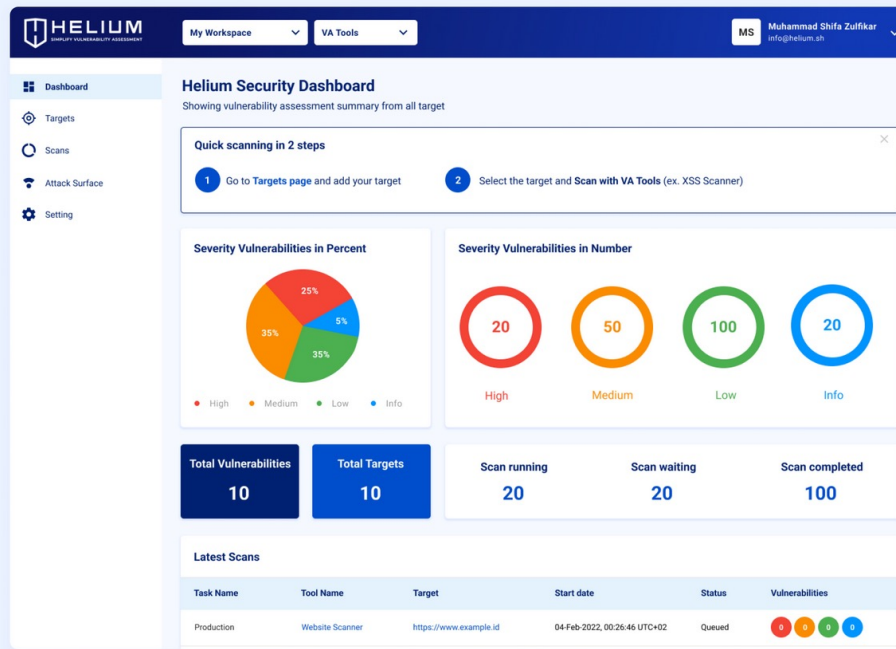
Discover data about an Internet resource such as domain name or IP address.

Wordpress Scanner

Discover security issues and vulnerabilities in the target WordPress website.

XSS Scanner

Discover Cross Site Scripting (XSS) vulnerabilities in web applications.



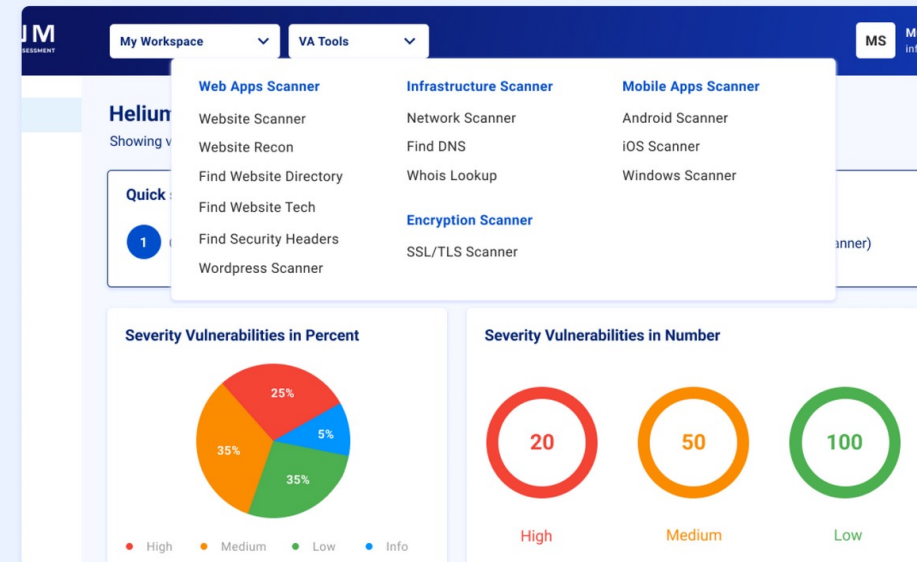
Continuous Monitoring

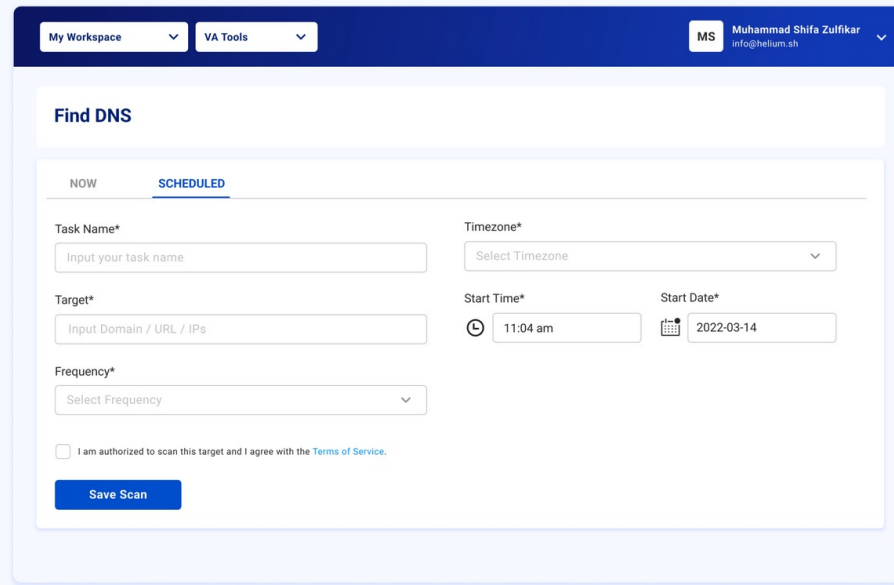
You can monitor through the Dashboard that gives you a visual of all vulnerabilities levels obtained from the scan.

Features

Scan with VA Tools

All the tools are available for you to scan the Web Apps, Mobile Apps, Infrastructure and Encryption. The tools can perform **Scan in background**, so you can sleep well.





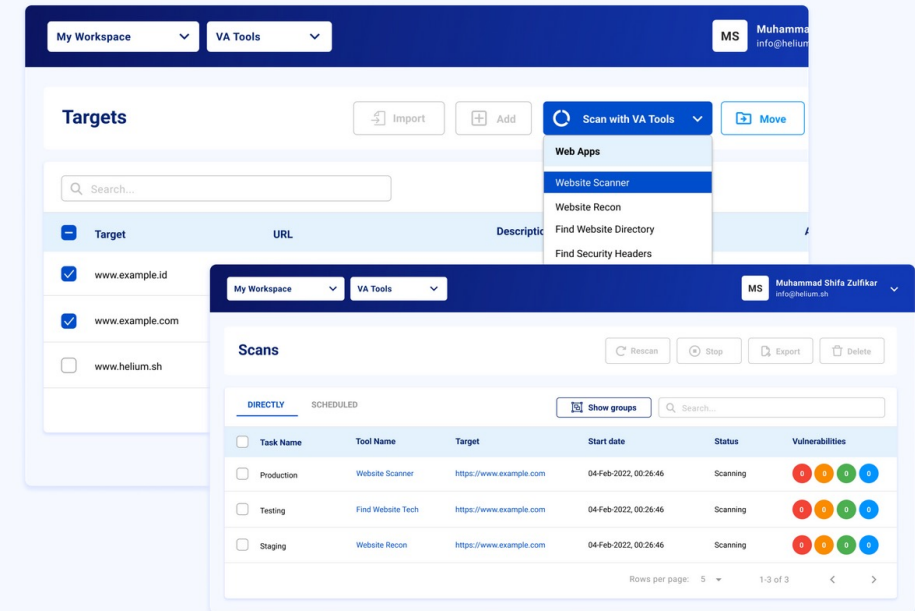
Schedule your scans

Schedule your scans and periodically evaluate your systems for the vulnerabilities. You can set them up to run once, daily, weekly, or monthly at a specific date and time.

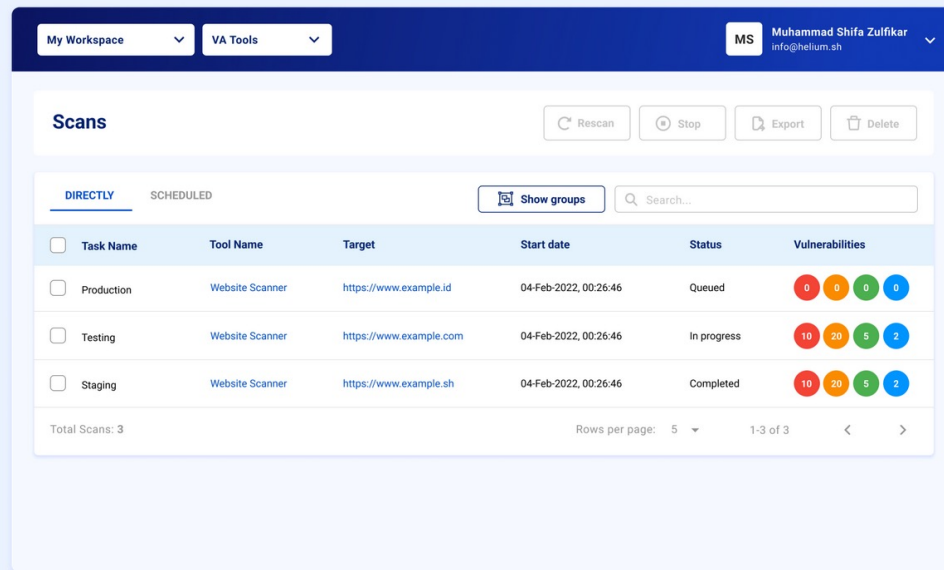
Features

Parallel & Bulk Scanning

We provided you a parallel scan. You can scan a lot of targets at one time. You can also select multiple targets that you want to scan and run a scanner against them.



Task Name	Tool Name	Target	Start date	Status	Vulnerabilities
Production	Website Scanner	https://www.example.com	04-Feb-2022, 00:26:46	Scanning	8 1 0 0 0
Testing	Find Website Tech	https://www.example.com	04-Feb-2022, 00:26:46	Scanning	0 0 0 0 0
Staging	Website Recon	https://www.example.com	04-Feb-2022, 00:26:46	Scanning	0 0 0 0 0



Scans

My Workspace | VA Tools | MS | Muhammad Shifa Zulfikar | info@helium.sh

Rescan | Stop | Export | Delete

DIRECTLY | SCHEDULED | Show groups | Search...

<input type="checkbox"/>	Task Name	Tool Name	Target	Start date	Status	Vulnerabilities
<input type="checkbox"/>	Production	Website Scanner	https://www.example.id	04-Feb-2022, 00:26:46	Queued	0 0 0 0
<input type="checkbox"/>	Testing	Website Scanner	https://www.example.com	04-Feb-2022, 00:26:46	In progress	10 20 5 2
<input type="checkbox"/>	Staging	Website Scanner	https://www.example.sh	04-Feb-2022, 00:26:46	Completed	10 20 5 2

Total Scans: 3 | Rows per page: 5 | 1-3 of 3

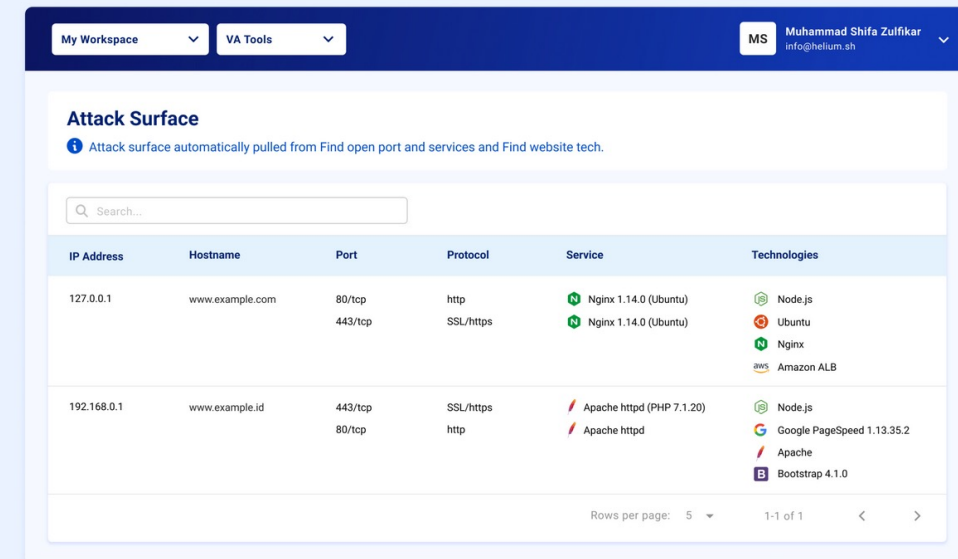
Keep history of your scans

Having a history of your scans allows you to see how the security of your targets has evolved. You can compare old results with new ones and see what has changed. You also can choose to export the scans history.

Features

Discover your attack surface

Automatically detect open ports, services, and running software from all of your targets. The Attack Surface pulls results from scanners to give you an overview of your targets.



Attack Surface

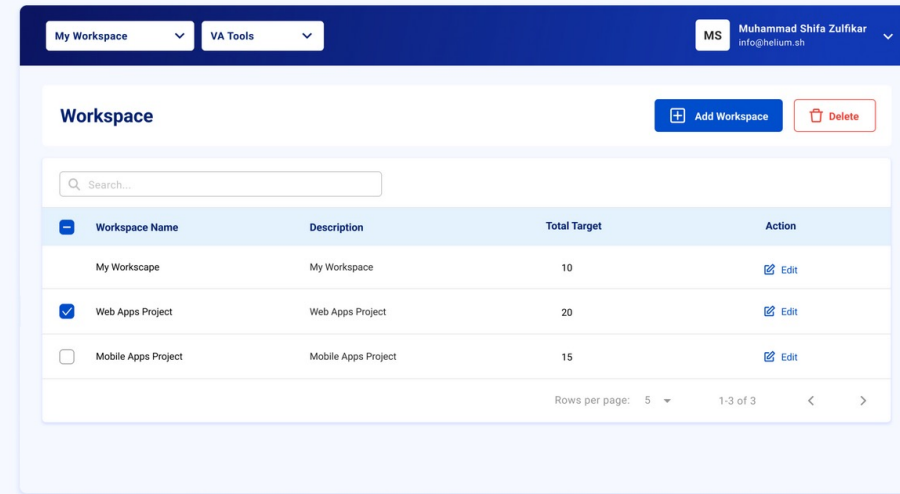
Attack surface automatically pulled from Find open port and services and Find website tech.

Search...

IP Address	Hostname	Port	Protocol	Service	Technologies
127.0.0.1	www.example.com	80/tcp	http	Nginx 1.14.0 (Ubuntu)	Node.js
		443/tcp	SSL/https	Nginx 1.14.0 (Ubuntu)	Ubuntu Nginx Amazon ALB
192.168.0.1	www.example.id	443/tcp	SSL/https	Apache httpd (PHP 7.1.20)	Node.js
		80/tcp	http	Apache httpd	Google PageSpeed 1.13.35.2 Apache Bootstrap 4.1.0

Rows per page: 5 | 1-1 of 1

Features



The screenshot shows the 'Workspace' management page. At the top, there are dropdown menus for 'My Workspace' and 'VA Tools', and a user profile for 'Muhammad Shifa Zulfikar'. Below the header, there are buttons for 'Add Workspace' and 'Delete'. A search bar is present above a table with the following data:

Workspace Name	Description	Total Target	Action
My Workscape	My Workscape	10	Edit
<input checked="" type="checkbox"/> Web Apps Project	Web Apps Project	20	Edit
<input type="checkbox"/> Mobile Apps Project	Mobile Apps Project	15	Edit

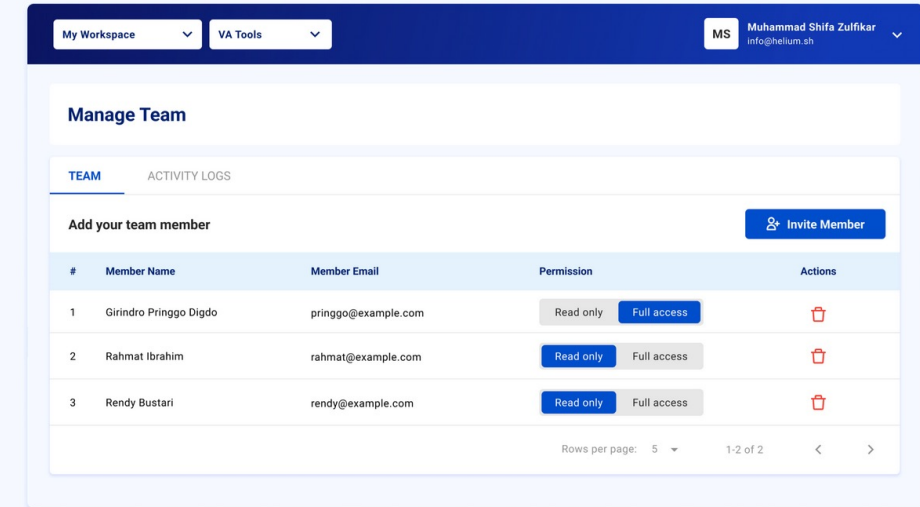
At the bottom of the table, there is a pagination control showing 'Rows per page: 5' and '1-3 of 3'.

Workspaces

Workspace allows you to organize your targets based on the project that you're working at, the client name, etc. All the works that you are doing goes into the current workspace. You also can move targets between workspaces and delete them if they are no longer necessary.

Manage Team

Working with the team to collaborate and deliver better security assessment. You can also see the team activity log.

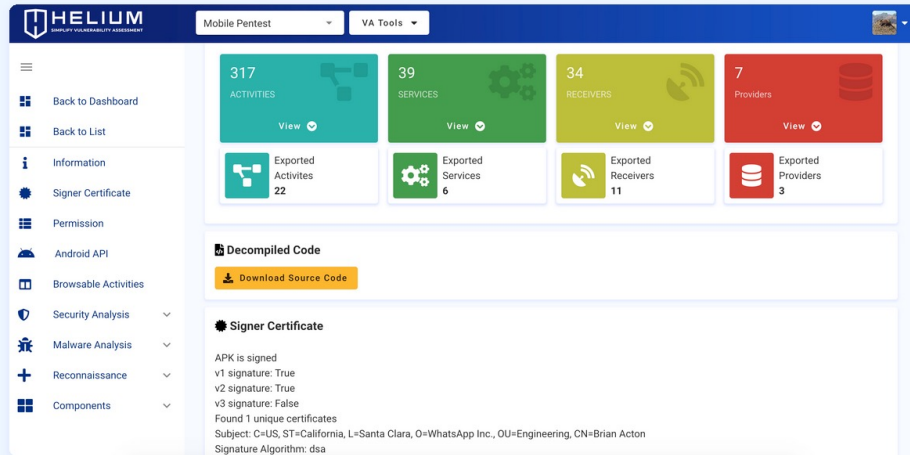


The screenshot shows the 'Manage Team' page. At the top, there are dropdown menus for 'My Workspace' and 'VA Tools', and a user profile for 'Muhammad Shifa Zulfikar'. Below the header, there are tabs for 'TEAM' and 'ACTIVITY LOGS'. A button 'Add your team member' and 'Invite Member' are visible. Below this is a table with the following data:

#	Member Name	Member Email	Permission	Actions
1	Girindro Pringgo Digdo	pringgo@example.com	Read only Full access	Delete
2	Rahmat Ibrahim	rahmat@example.com	Read only Full access	Delete
3	Rendy Bustari	rendy@example.com	Read only Full access	Delete

At the bottom of the table, there is a pagination control showing 'Rows per page: 5' and '1-2 of 2'.

Features

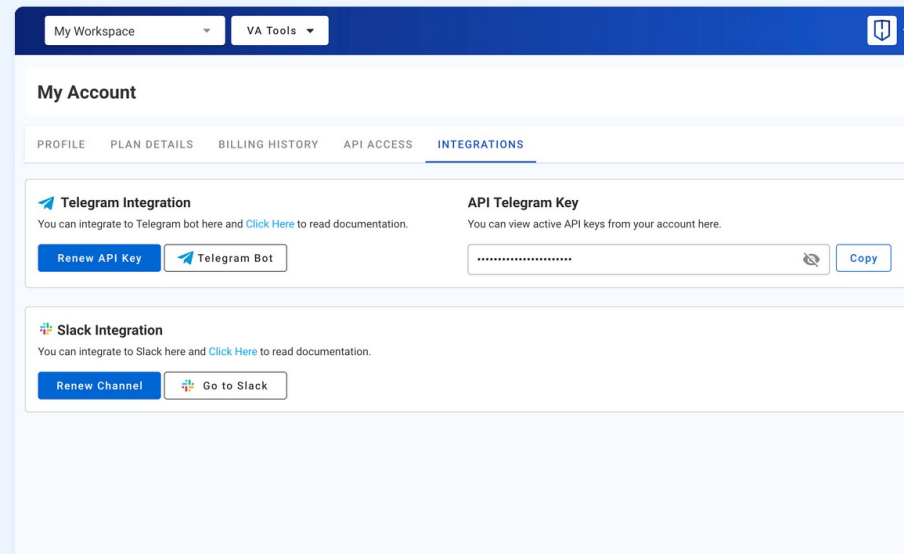


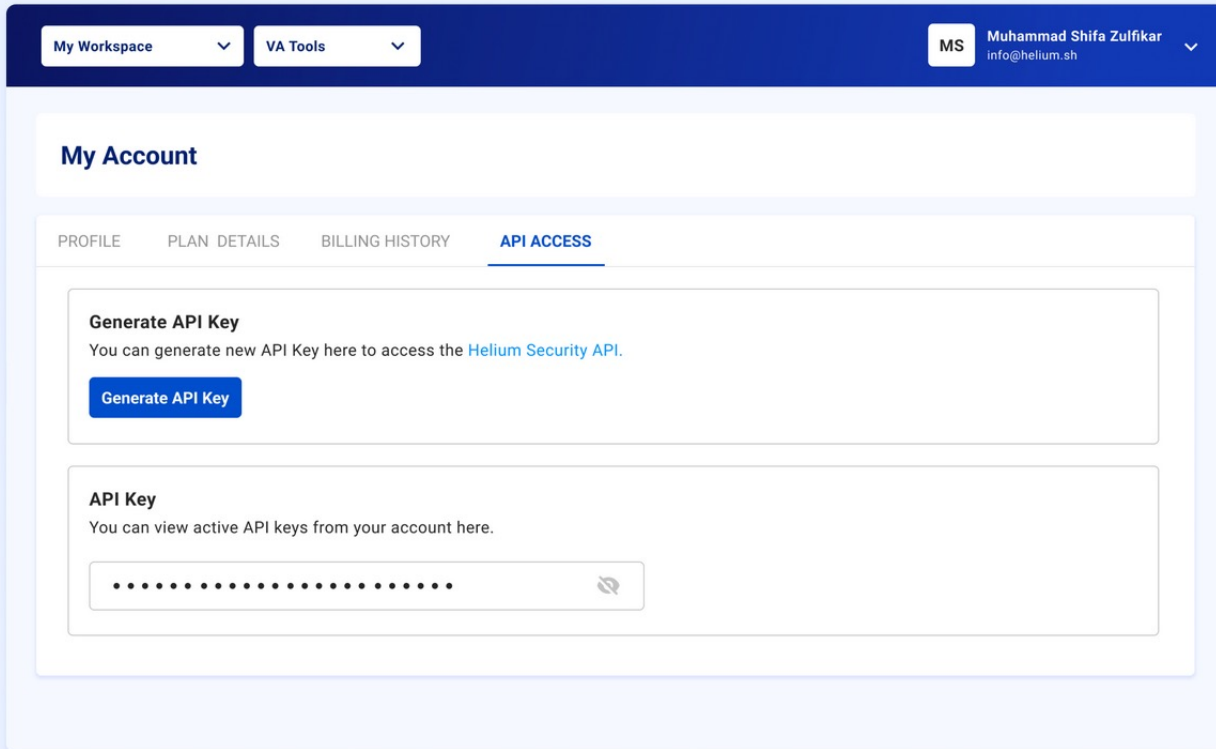
Mobile Apps Scanner

Mobile Static Application Security Testing allows you to do a static analysis in mobile apps. It covers iOS and Android apps. So, you don't have to install a lot of mobile pentest tools. This will save your time from installation and configuration.

Slack and Telegram Integrations

You can do a Scan via Telegram/Slack until you get a notification of the scan results, you can do it anywhere without bringing a computer.





API Access

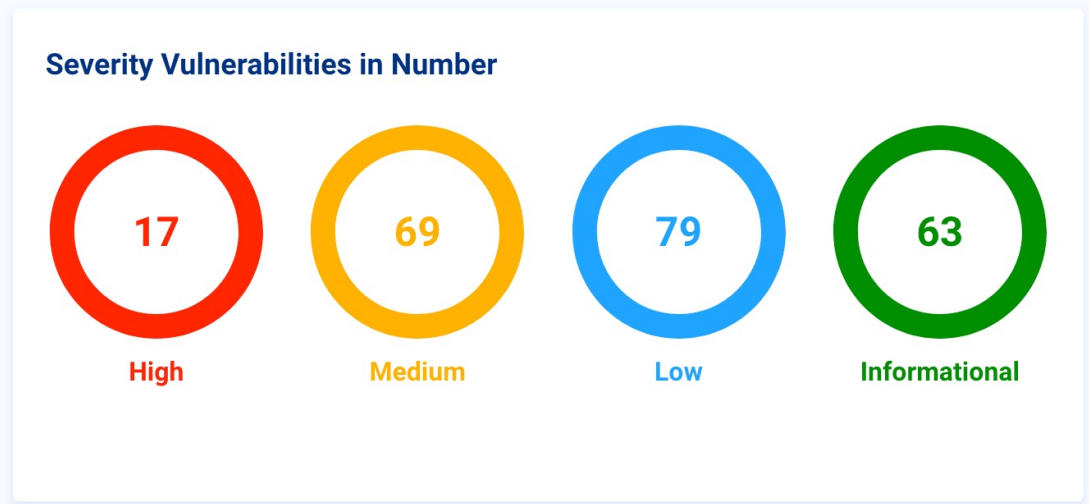
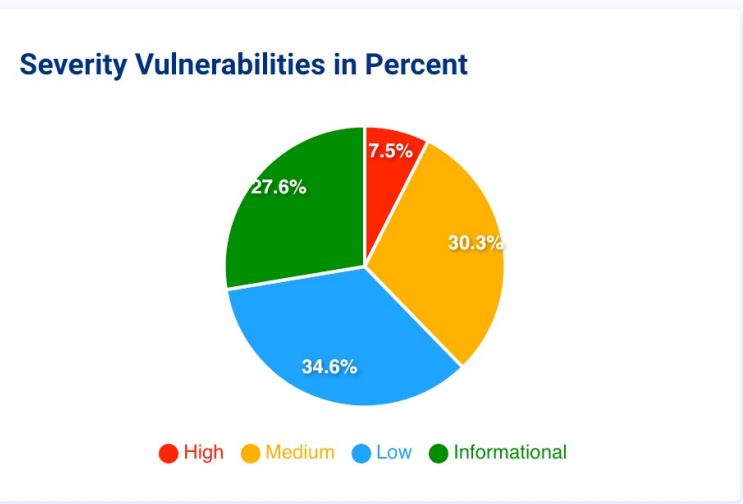
The API allows you to integrate our platform with your tools and internal workflows. For instance, you can trigger automatic scans whenever you deploy a new website, or you make a change in your application. Furthermore, you can develop your own tools based on our scanning engines.

[API Documentation](#) →

- Dashboard
- Targets
- Scans
- Attack Surface
- Reports
- Settings

Helium Security Dashboard

Showing vulnerability assessment summary from all target



Total Vulnerabilities
228

Total Targets
39

Scan running	Scan waiting	Scan completed
0	0	298

Latest Scan

Task Name	Target	Workspace	Start Date	Status	Vulnerabilities
		My Workspace	06-09-2022, 17:13	Completed	
		My Workspace	06-09-2022, 17:12	Completed	

LIVE DEMO  **HELIUM**
SIMPLIFY SECURITY TESTING

Go to <https://www.helium.sh/>



Contact

pringgo@cyberarmy.id

  +62852-6787-6548



PT Global Inovasi Siber Indonesia

Address: Jl. Naripan No.53, Kb. Pisang, Sumur Bandung

Kota Bandung, Jawa Barat, Indonesia

Phone Number : +62812 9393 1337

Email : info@helium.sh

Website : www.helium.sh

