

Intruder Attack Scan Report

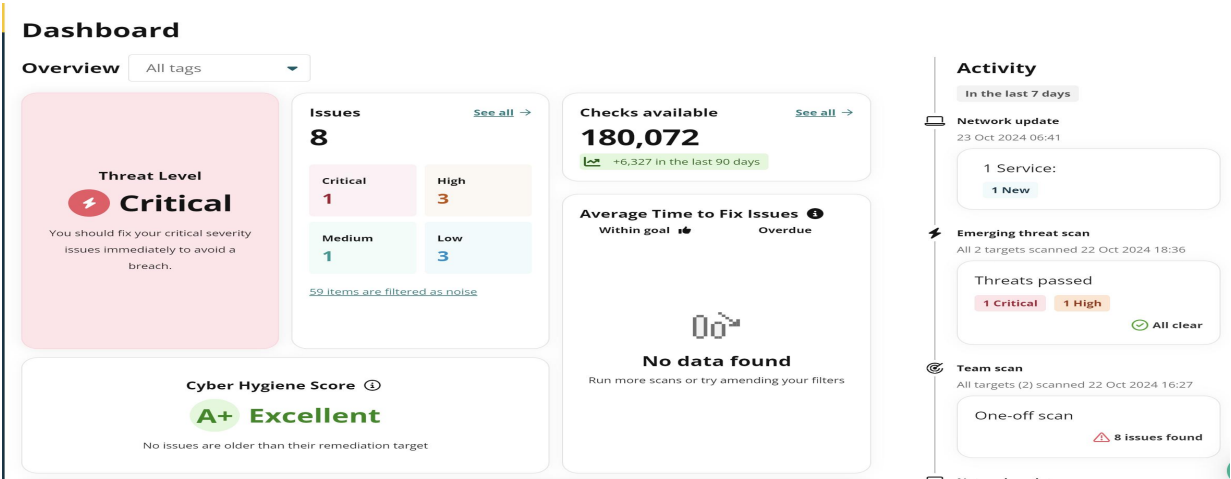
Overview

Intruder is a powerful vulnerability management tool designed to help organizations identify and mitigate security risks across their digital assets. It features a comprehensive dashboard that provides insights into various security aspects, including targets, scans, issues, reports, and attack surfaces.

Key Features

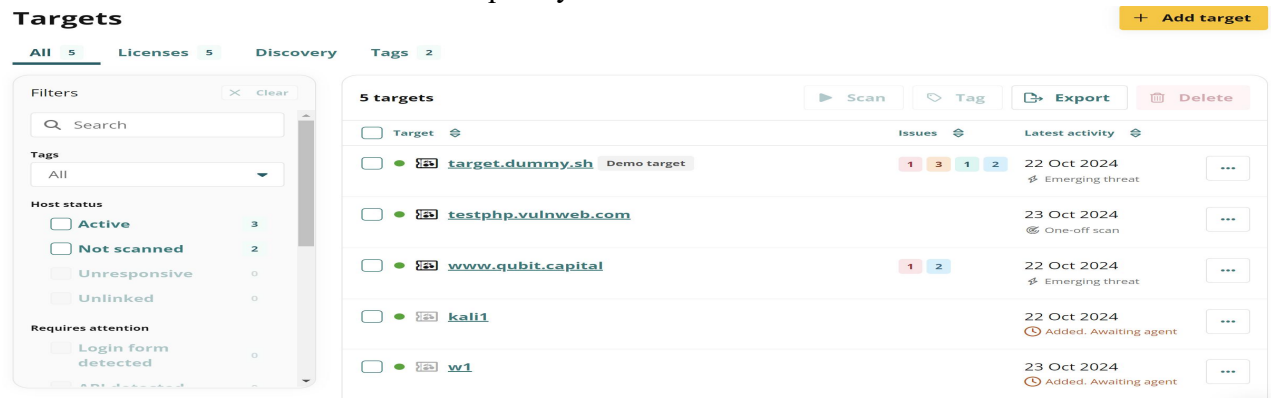
1. Dashboard

- Centralized Monitoring: Provides an overview of all scanned assets and their security status.
- Visual Insights: Displays key metrics, such as the number of vulnerabilities detected, scan results, and overall security health.
- User-Friendly Interface: Intuitive layout for easy navigation, allowing users to quickly assess their security posture.



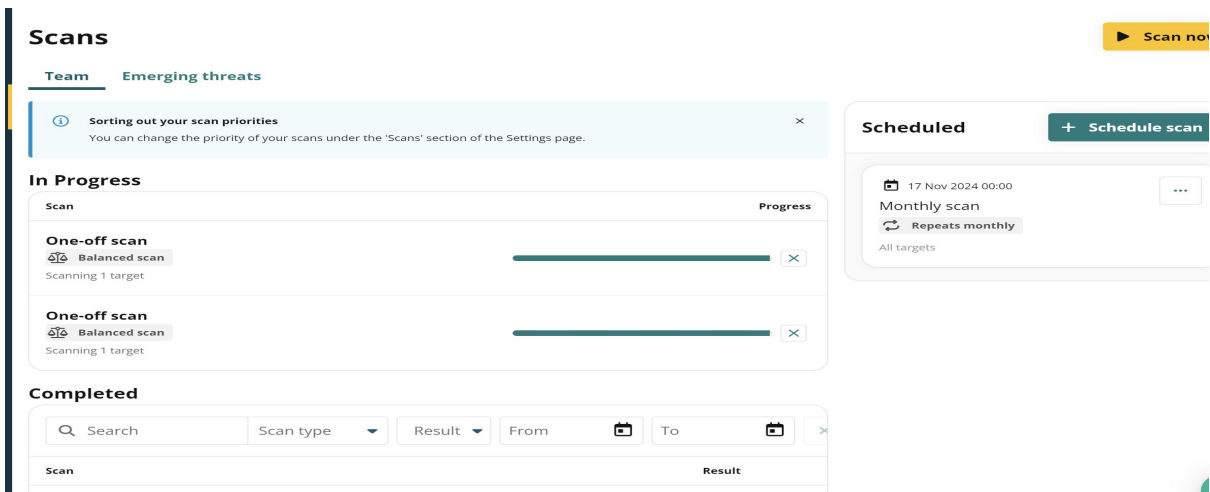
2. Targets

- Asset Management: Users can easily add, manage, and categorize their targets, whether they are external websites, internal servers, or cloud services.
- Target Configuration: Set specific parameters for scans, including the types of vulnerabilities to focus on and the frequency of scans.



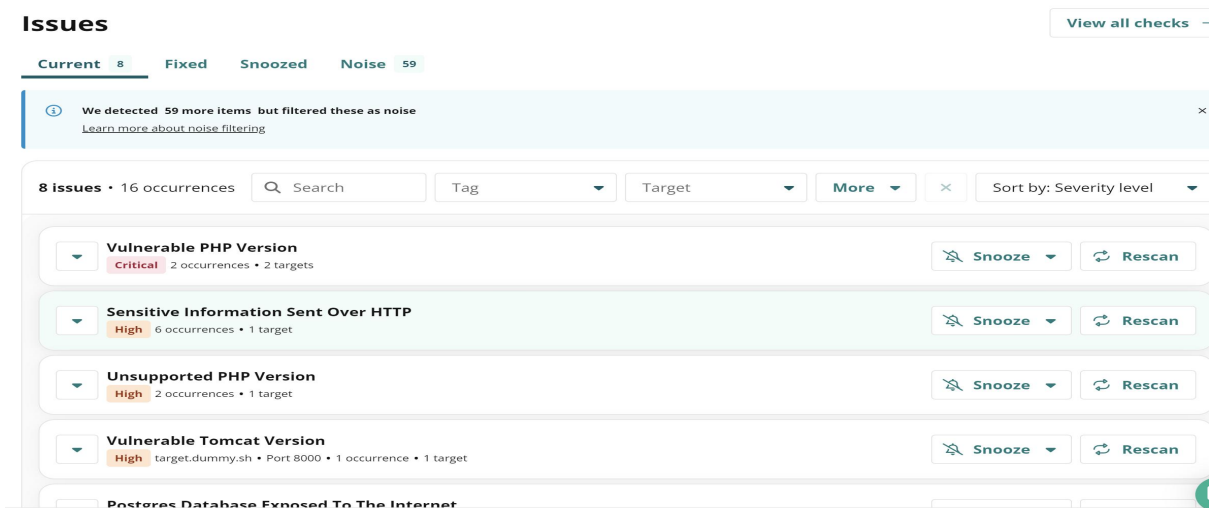
3. Scans

- Flexible Scan Types: Choose from various scan types, including external scans, internal scans, and scheduled scans.
- Advanced Scanning Engines: Utilize industry-leading engines to detect vulnerabilities such as misconfigurations, missing patches, and common application flaws.
- Customization Options: Tailor scans to focus on particular vulnerabilities or areas of concern.



4. Issues

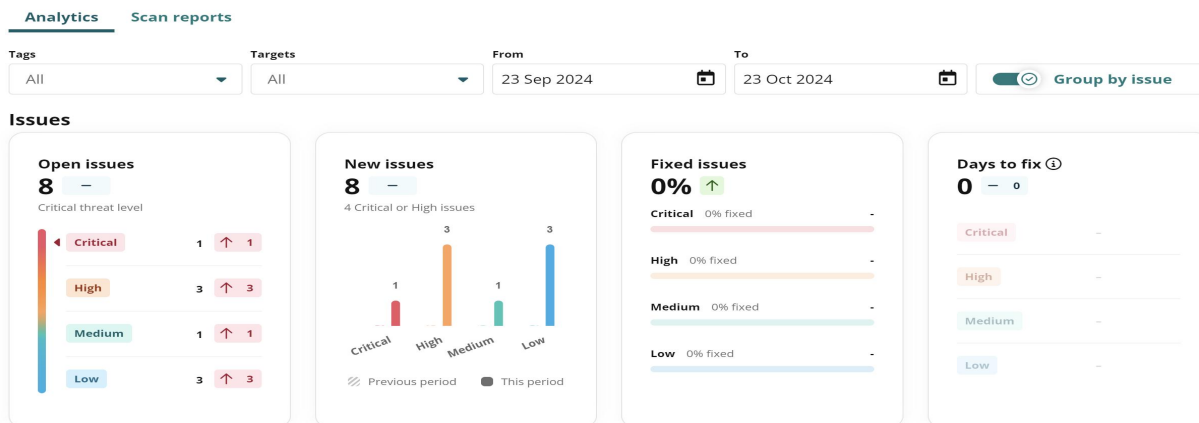
- Vulnerability Management: Automatically aggregates and categorizes detected vulnerabilities for easy review.
- Severity Ratings: Each issue is assigned a severity level (e.g., low, medium, high), helping prioritize remediation efforts.
- Detailed Insights: Provides information on the nature of each vulnerability, affected components, and recommended remediation steps.



5. Reports

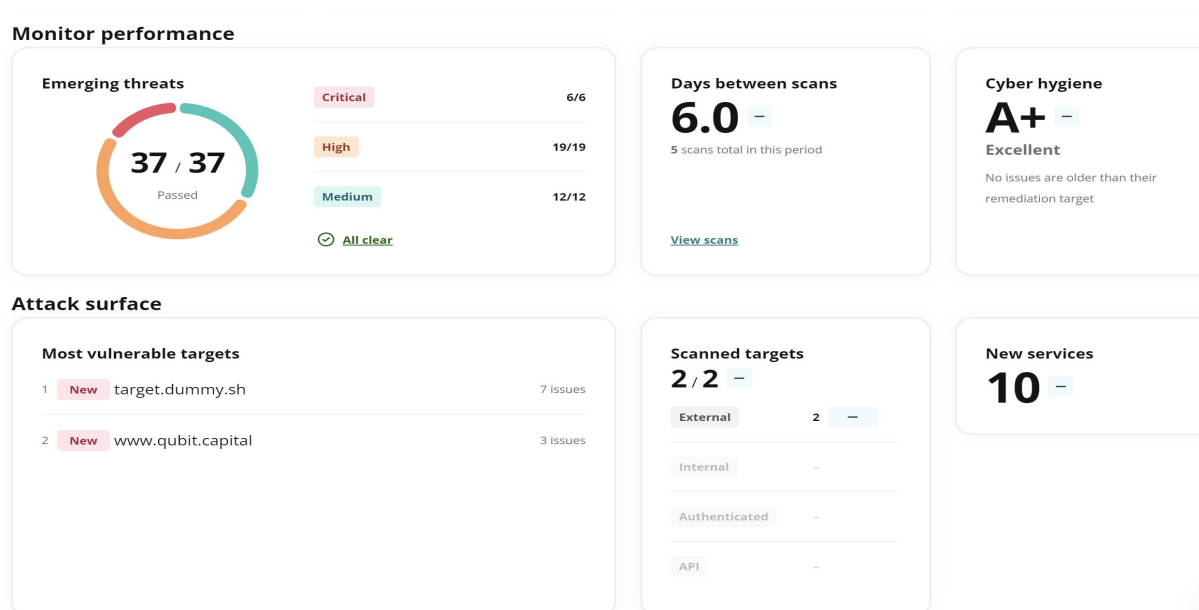
- Comprehensive Reporting: Generate detailed reports that summarize scan results, vulnerabilities found, and remediation recommendations.
- Export Options: Reports can be exported in various formats (e.g., PDF, CSV) for sharing with stakeholders.
- Historical Data: Access previous scan results for trend analysis and compliance purposes.

Reports



6. Attack Surface

- Mapping Exposure: Visualize the attack surface by identifying all publicly accessible assets and their vulnerabilities.
- Risk Assessment: Assess potential risks associated with each asset, helping prioritize security efforts.
- Continuous Monitoring: Regularly updates the attack surface as new assets are added or existing assets change.



Target Domains Scanned

Target Domains Scanned

1. qubit.capital

Scan Type: External Website Scan

Vulnerabilities Found:

Vulnerable PHP Version: The installed version contains known vulnerabilities that could compromise the system. For details, refer to CVE Details for PHP.

Debug Script Information Disclosure: A publicly accessible page using phpinfo() discloses sensitive system information.

Strict Transport Security HTTP Header Not Set: The server lacks an HSTS header, increasing vulnerability to Man-in-the-Middle (MitM) attacks.

Recommendations

Update PHP Version: Upgrade to a secure version.

Remove Access to phpinfo(): Restrict or disable access to sensitive pages.

Implement HSTS: Add the HTTP Strict Transport Security header.

www.qubit.capital

Active

+ Add tag

Add note

Location

Pune, Maharashtra, IN

License

Infrastructure license

Released on 21 Nov 2024

Latest activity

22 Oct 2024

Emerging threat

Last network scan

22 Oct 2024 12:57

Next scan 29 Oct 2024

Issues3

Authentications

APIs

Services3

Activity

Vulnerable PHP Version

Critical

www.qubit.capital • Port 443 • 1 occurrence • 1 target

Debug Script Information Disclosure (phpinfo)

Low

www.qubit.capital • Port 443 • 1 occurrence • 1 target

Strict Transport Security HTTP Header Not Set

Low

www.qubit.capital • Port 443 • 1 occurrence • 1 target

2. target.dummy.sh

Scan Type: External Website Scan

Issues Identified: 7

Vulnerabilities Found :

Vulnerable PHP Version

Severity: Critical


Details: Contains known vulnerabilities.

Sensitive Information Sent Over HTTP

target.dummy.sh

[▶ Scan now](#)

● Active Demo target X + Add tag

[Add note](#)**Location**
London, England, GB**License**
 Infrastructure license
Released on 21 Nov 2024**Latest activity**
22 Oct 2024
 Emerging threat**Last network scan**
17 Oct 2024 08:33
Next scan 24 Oct 2024**Issues** 7 **Authentications** **APIs** **Services** 5 **Activity****Vulnerable PHP Version**
Critical target.dummy.sh • Port 80 • 1 occurrence • 1 target**Sensitive Information Sent Over HTTP**
High 6 occurrences • 1 target**Unsupported PHP Version**
High 2 occurrences • 1 target**Vulnerable Tomcat Version**
High target.dummy.sh • Port 8000 • 1 occurrence • 1 target

1. Severity: High
Occurrences: 6 instances.
Details: Sensitive data transmitted over unsecured connections.
Unsupported PHP Version
2. Severity: High
Occurrences: 2 instances.
Details: Increases risk of vulnerabilities.
Vulnerable Tomcat Version
3. Severity: High
Details: Known vulnerabilities present.
Postgres Database Exposed to the Internet
4. Severity: Medium
Details: Accessible over the internet.
Debug Script Information Disclosure (phpinfo)
5. Severity: Low
Details: Sensitive information exposed.
WordPress User Enumeration
6. Severity: Low
Details: Susceptible to user enumeration attacks.
Ports and Services
Port 80: Vulnerable PHP version detected.
Port 5432: Postgres database exposed.
Port 8080: Debug script information disclosure found.
Port 8000: Vulnerable Tomcat version detected.
Port 801: WordPress user enumeration possible.

Recommendations

Update PHP and Tomcat Versions: Upgrade to the latest supported versions.

Implement HTTPS: Configure the server to use HTTPS.

Restrict Database Access: Limit access to trusted IPs.

Remove Access to Debug Scripts: Disable public access to sensitive scripts.

Mitigate User Enumeration Risks: Implement protections against user enumeration.

Internal System Agent Installation and Scan

Installation

- System: Kali Linux VM

- Agent Installation Steps:

1. Download the agent package from the Intruder website.

2. Open terminal

In the terminal, change to the directory you downloaded the installer.

3. Install & configure agent

Run the following command:

```
sudo dpkg -i NessusAgent-10.7.3-debian10_amd64.deb
```

```
sudo /opt/nessus_agent/sbin/nessuscli agent link --name=065a8617-4d85-46cb-a93a-677827b775e7_kali1 --
```

```
key=819652a91d674e8d5be08e21299f1a3c69bd9806c72e24bc05df6b32b8db7fe1 --cloud
```

4. Reboot

Note that the location of nessuscli might vary depending on your version of Linux.

Internal Scan Results

- Scan Type: Internal Network Scan

kali1▶ Scan now

● Not scanned yet

+ Add tag

Add note

License
 No license assigned

Latest activity
22 Oct 2024
 Added. Awaiting agent

Issues

Activity

No issues found
You currently don't have any issues for this target
[Target's detail page](#)

Conclusion

Intruder's comprehensive suite of features—ranging from a robust dashboard to detailed reporting—empowers organizations to effectively manage their security posture. The results from the scans highlight critical vulnerabilities that need attention. By implementing the recommended remediation strategies, organizations can significantly reduce their exposure to potential threats. Continuous monitoring and regular updates will ensure ongoing security resilience.