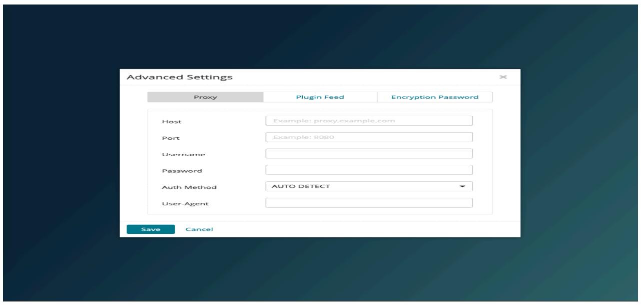
Vulnerability Scanning

It is an essential part of the pen-testing process. It allows the tester to see security holes in the system’s target that auditors can use to compromise. The following five applications are commonly used for this purpose.

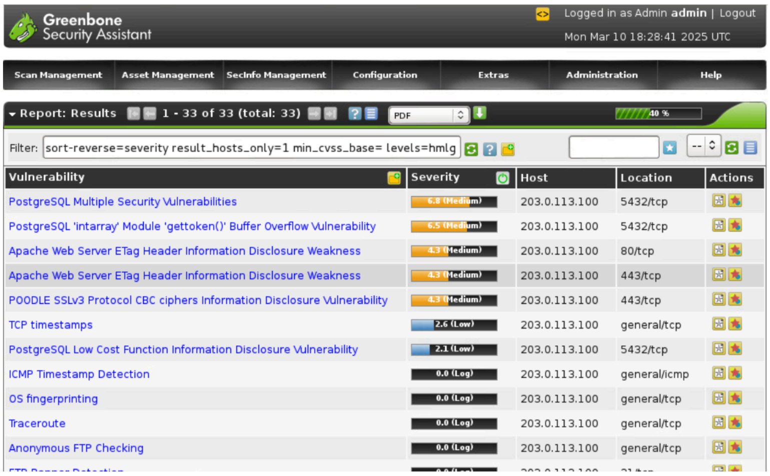
Nessus is a widespread vulnerability scanner that can scan local and remote systems. It utilizes a database of discovered vulnerabilities to detect them. Also, it allows users to configure the scan and customize reports with its user-friendly interface. (*Advanced Vulnerability Assessment with Nessus Professional*, n.d.) However, this tool has disadvantages, such as Network Address Translation(NAT), IPS, firewalls, load balancers, or proxies affecting the scan result and possibly missing vulnerabilities; the scan is slow when the network is extensive (*Benefits and Limitations (Tenable Nessus Agent 10.7)*, n.d.).



Advanced Settings

Host: Example: proxy.example.com
Port: Example: 8080
Username:
Password:
Auth Method: AUTO DETECT
User-Agent:

OpenVAS is another well-known application that is similar to Tenable Nessus. Still, this one is an open-source and free web-based application. Some of its features include unauthenticated and authenticated testing, several high—and low-level internet and industrial protocols, and performance tuning for large-scale scans. (*OpenVAS - Open Vulnerability Assessment Scanner*, n.d.) However, this tool has limitations, such as fewer CVEs, a slower scan, and less detailed reports than Nessus. Also, the installation process requires some technical knowledge, the support for operating systems is limited, and it doesn't offer policy management. (Lugsden, 2024; *OpenVAS vs. Nessus*, n.d.)



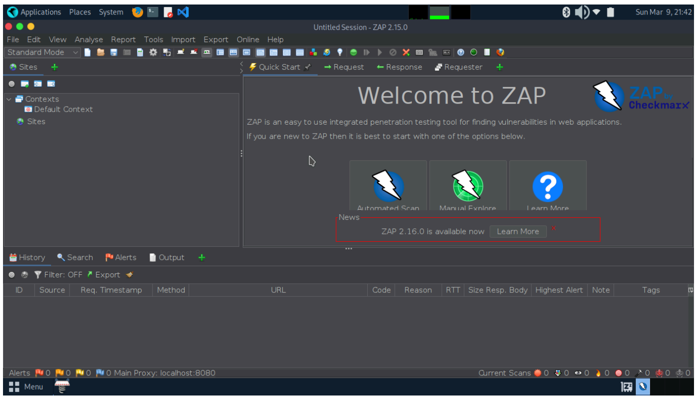
Logged in as Admin admin | Logout
Mon Mar 10 18:28:41 2025 UTC

Report: Results 1 - 33 of 33 (total: 33)

Filter: sort-reverse=severity result_hosts_only=1 min_cvss_base= levels=hmlg

Vulnerability	Severity	Host	Location	Actions
PostgreSQL Multiple Security Vulnerabilities	6.8 (Medium)	203.0.113.100	5432/tcp	
PostgreSQL 'intarray' Module 'gettoken()' Buffer Overflow Vulnerability	6.5 (Medium)	203.0.113.100	5432/tcp	
Apache Web Server ETag Header Information Disclosure Weakness	4.3 (Medium)	203.0.113.100	80/tcp	
Apache Web Server ETag Header Information Disclosure Weakness	4.3 (Medium)	203.0.113.100	443/tcp	
POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability	4.3 (Medium)	203.0.113.100	443/tcp	
TCP timestamps	2.6 (Low)	203.0.113.100	general/tcp	
PostgreSQL Low Cost Function Information Disclosure Vulnerability	2.1 (Low)	203.0.113.100	5432/tcp	
ICMP Timestamp Detection	0.0 (Log)	203.0.113.100	general/icmp	
OS fingerprinting	0.0 (Log)	203.0.113.100	general/tcp	
Traceroute	0.0 (Log)	203.0.113.100	general/tcp	
Anonymous FTP Checking	0.0 (Log)	203.0.113.100	general/tcp	

OWASP is a testing tool that can expose security holes in web applications, such as SQL injection, cross-site scripting (XSS), sensitive data exposure, and insecure deserialization vulnerabilities. Its user-friendly interface allows users to configure the scan, intercept proxies, fuzzer, and view the results. It can also integrate with other tools, such as Metasploit, but it can request many system resources during scans. (*The ZAP Homepage*, n.d.) However, it has several limitations, such as consuming many resources, not having an intuitive interface, struggling with false positives, and lacking online documentation. Also, the capacity to customize reports based on user requirements is limited, impacting usability. (*OWASP Zap: Pros and Cons 2025*, n.d.; *Software Secured | Burp vs. Zap in the World of Vulnerability Scanning | USA*, n.d.)



Welcome to ZAP

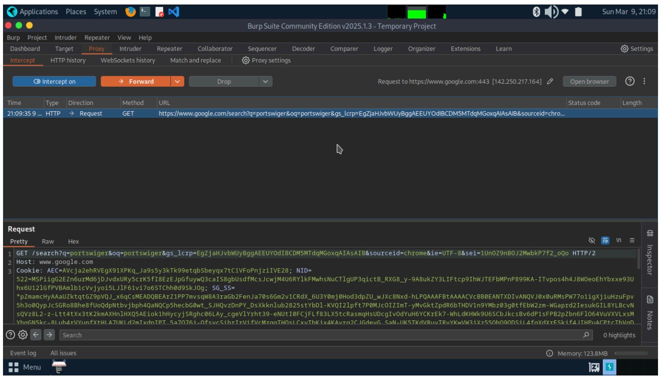
ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

If you are new to ZAP then it is best to start with one of the options below.

ZAP 2.16.0 is available now

Burp Suite is an integrated platform for conducting security testing of web applications. Its diverse tools work seamlessly together to help the entire testing procedure, from initial mapping and examination of an application's attack surface to encountering and exploiting security vulnerabilities.

It gives the user complete control, combining cutting-edge manual approaches with automation to make your work faster and more effective. (*Features - Burp Suite Enterprise Edition*, n.d.) However, this tool has some limitations, such as low performance, especially when set to the highest level of thoroughness. It doesn't support the DevOps process and can produce false positives. (*Burp Suite vs. ZAP*, n.d.)

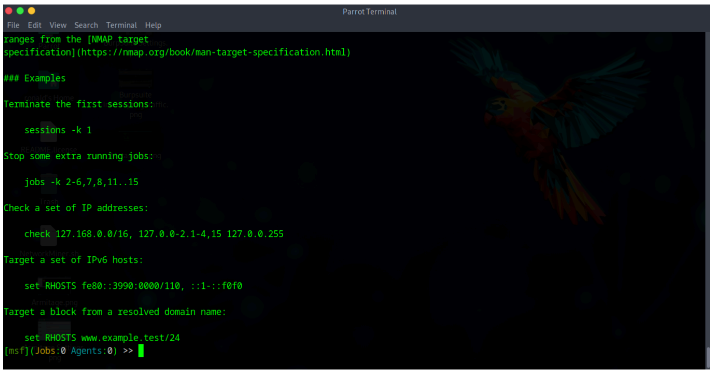


Request to https://www.google.com:443 [142.250.217.164]

Time	Type	Direction	Method	URL	Status code	Length
21:09:35 9 ...	HTTP	→ Request	GET	https://www.google.com/search?q=portswiger&oq=portswiger&gs_lcrp=EgZjaHJvbWUyBggAEEUYOdIBCDM5MTdqMGoxqAIAsAIB&sourceid=chro...		

```
GET /search?q=portswiger&oq=portswiger&gs_lcrp=EgZjaHJvbWUyBggAEEUYOdIBCDM5MTdqMGoxqAIAsAIB&sourceid=chrome&ie=UTF-8&sei=1UnOZ9nBOJ2MwbkP7f2_oQo HTTP/2
Host: www.google.com
Cookie: AEC=AVcja2ehRVEgX91XPKq_Ja9s5y3kTk99etqbSbeyqx7tC1VFoPnjziIVE28; NID=
522=MSPiigG2EZn6urMd6jDJvdxURy5crK5fI8EzEJpGfuywQ3caIS8gbUsdfMcsJcwjM4U6RYlkFMwhsNuCTlgUP3qictB_RXG8_y-9A8ukZY3LIFtcp9IhWJTEFbMPnP899KA-ITvpos4h4J8WOeoEhYbxxe93U
hx6U12lGfPVBAmlb1cVvjyoi5LJlF61vi7o6STChh0d9SkJOg; SG_SS=
*pZmamcHyAAaUZktqtGZ9pVQJ_x6qCsMEADQBEArZ1PP7mvsqW8A3raGb2FenJa70s6Gm2v1CRdX_6U3Y0mj0Hod3dpZU_wJXc8Nxd-hLPQAAAFBtAAAACVcBB0EANTXDIvANQVJ0x0uRMsPW77o1igXjiuHzuFpv
5h3o0QypJcSGRo8Bhe8fUoQdpNtbvjbph4QaNQCp5hecbG0wt_SJHQvzDnPY_DsXkknlub2825stYbDl-KVQI2lpft7P0MJcOIZImT-yMvGktZpdR6bTHDV1n9YMbz03g0tfEbW2zm-WGaprd2IesukGIL8YLBcvN
sQVz8L2-z-Ltt4tXx3tK2kmAXHnlHXQ5AEiok1hHycyjSRghc06LAy_cgeVlYrht39-eNUtI0FCjFLf83LX5tcRasmqHsUDcgIvOdYuH6YCKrEk7-WhLdKHWk9U6SCbJkcsBv6dP1sFPB2pZbn6Fl064VuVXVLxsM
```

Metasploit is an open-source pen-testing tool for identifying vulnerabilities in systems and exploiting them to gain access. It has a database of known vulnerabilities and exploits used to test weaknesses. It can also create post-exploitation modules to aid with privilege escalation, lateral movement, or inner enumeration. However, it has several limitations, such as being unable to conduct stealthy operations, limited reporting capabilities, dependence on a public exploit, and limited shell access. (Team, 2023)



```
ranges from the [NMAP target
specification](https://nmap.org/book/man-target-specification.html)

### Examples

Terminate the first sessions:

    sessions -k 1

Stop some extra running jobs:

    jobs -k 2-6,7,8,11..15

Check a set of IP addresses:

    check 127.168.0.0/16, 127.0.0-2.1-4,15 127.0.0.255

Target a set of IPv6 hosts:

    set RHOSTS fe80::3990:0000/110, ::1-::f0f0

Target a block from a resolved domain name:

    set RHOSTS www.example.test/24
[msf](Jobs:0 Agents:0) >>
```

References

Advanced Vulnerability Assessment with Nessus Professional. (n.d.). Tenable®. Retrieved March 9, 2025, from https://www.tenable.com/products/nessus/nessus-professional

Benefits and Limitations (Tenable Nessus Agent 10.7). (n.d.). Retrieved March 9, 2025, from https://docs.tenable.com/nessus-agent/10_7/Content/benefits-and-limitations.htm

Burp Suite vs. ZAP: Features, Key Differences & Limitations. (n.d.). Retrieved March 10, 2025, from https://www.pynt.io/learning-hub/burp-suite-guides/burp-suite-vs-zap-features-key-differences-limitations

Features—Burp Suite Enterprise Edition. (n.d.). Retrieved March 9, 2025, from https://portswigger.net/burp/enterprise/features

Lugsden, A. (2024, July 18). *OpenVAS vs Nessus: Which Scanner Is For You?* Forge Secure. https://forgesecure.com/openvas-vs-nessus/

OpenVAS - Open Vulnerability Assessment Scanner. (n.d.). Retrieved March 9, 2025, from https://openvas.org/

OpenVAS vs. Nessus: How Different are the Two? (n.d.). Wisdomplexus. Retrieved March 10, 2025, from https://wisdomplexus.com/blogs/openvas-vs-nessus/

OWASP Zap: Pros and Cons 2025. (n.d.). Retrieved March 9, 2025, from https://www.peerspot.com/products/owasp-zap-pros-and-cons

Software Secured | *Burp vs. Zap in the World of Vulnerability Scanning* | *USA*. (n.d.). Retrieved March 9, 2025, from https://www.softwaresecured.com/post/burp-versus-zap

Team, C. W. (2023, June 22). *What is Metasploit: Tools, Uses, History, Benefits, and Limitations*. Cyber Security News. https://cybersecuritynews.com/what-is-metasploit/

The ZAP Homepage. (n.d.). ZAP. Retrieved March 9, 2025, from https://www.zaproxy.org/