

Phase 3

Identify Vulnerabilities

Phase 3. Identify Vulnerabilities

Tool/Resources 1: Nessus

Description: Nessus is an enterprise network vulnerability scanner that identifies technical vulnerabilities on the device. Vulnerabilities that an attacker could exploit. Nessus can use for host discovery on internal networks, scan internal network hosts for vulnerabilities and use to scan VPS cloud servers for vulnerabilities.

Ways to use Nessus to discover vulnerabilities:

- Host Discovery Scan: configurable for host enumeration and OS/Service detection
- Basic Network Scan: A quick vulnerability scan service
- Advanced Scan: Configure a full vulnerability scan service
- Advanced Dynamic Scan: This scan can filter scan options such as CVE with severity score, CWE (common weakness enumeration) classes, and more.
- Malware Scan: Scan for malware internally on Windows and Unix systems.
- Active Directory Scan: Scan for any misconfiguration in the Active Directory.
- CISA Alerts Scan: Scan and detect any vulnerabilities from recent CISA alerts.
- Ransomware Scan: scan and detect any vulnerabilities used by ransomware.
- TerraScan: A static code analyzer for infrastructure used in automated pipelines to identify policy violations before insecure infrastructure is provisioned.

Reason to use Nessus:

- Very easy to scan for vulnerabilities, and the UI is user-friendly.
- Results from the network enumeration and port scanning are very good.
- Compatible with various operating systems such as Kali Linux, Fedora, FreeBSD, macOS, Red Hat/CentOS/Oracle, Ubuntu, and Windows.
- Very customizable to organizations' preferences for the result's severity.
- It provides encryption for the scan data to have more protection.
- Cover around 50,000 CVEs (Common Vulnerabilities and Exposure)
- Very good customer support.

Potential drawbacks or limitations of Nessus:

- Networks can overload sometimes.
- Appears hostile when used to scan.
- It is not free, which might not be viable for smaller companies.
- Nessus doesn't provide as many advanced options and flexibility as Nmap when it runs port scanning.
 - Nmap can use the Kali Linux command line for:
 - Nmap -sS (IP): TCP syn scan, nmap -sT (IP): TCP connects scan, nmap -sU (IP): scan for UDP, etc.

- Nessus can only run scan types such as Host enumeration, OS identification, Port Scan(common ports), Port scan(all ports), and custom for your port range.
- Once the encryption password for data at rest is lost, there is no way of recovering it.

Nessus basic vulnerability Scan Screenshot:

The screenshot displays the Nessus Essentials web interface in a Mozilla Firefox browser. The main content area shows the results of a scan titled 'My Basic Network Scan'. A table lists various vulnerabilities found, categorized by severity (e.g., MIXED, INFO) and family (e.g., HTTP, TLS, SSH, Netstat). To the right of the table, a 'Scan Details' section provides metadata such as the policy used, scanner type, and completion time. Below this, a 'Vulnerabilities' donut chart visualizes the distribution of findings by severity level: Critical, High, Medium, Low, and Info.

Sev	Name	Family	Count
MIXED	SSL (Multiple Issu...	HTTP (Multiple Issues)	10
MIXED	HTTP (Multiple Is...	Web Servers	8
MIXED	TLS (Multiple Issu...	Service detection	4
MIXED	SSH (Multiple Iss...	Misc.	3
INFO	Netstat Portscanner (S...	Port scanners	15
INFO	Remote listeners enum...	Service detection	12
INFO	SSH (Multiple Iss...	General	6
INFO	Service Detection	Service detection	6
INFO	DMI (Multiple Issu...	General	3
INFO	RPC (Multiple Iss...	RPC	2
INFO	RPC Services Enumer...	Service detection	2
INFO	SSL / TLS Versions Su...	General	2
INFO	Additional DNS Hostna...	General	1

Source: (Jon Good) <<https://www.youtube.com/watch?v=x87gbgQD4eg&t=569s>>

Nessus Port Scan options Screenshot:

This screenshot shows the 'New Scan / Host Discovery' configuration page in Nessus. The 'Settings' tab is active, and a dropdown menu for 'Scan Type' is open. The menu lists several options: Host enumeration, OS identification, Port scan (common ports), Port scan (all ports), and Custom. The 'Port scan (all ports)' option is currently selected. Below the menu, there are fields for 'TCP', 'ARP', and 'ICMP (2 retries)'. At the bottom of the configuration area, there are 'Save' and 'Cancel' buttons.

Source:(Tenable Product Education), <<https://www.youtube.com/watch?v=ntJbLPhX58s>>

Tool/Resources 2: OpenVAS

Description: OpenVAS, or Open Vulnerability Assessment System, is a free software that provides vulnerability assessment services. It is a tool that scans the target system's software version, configuration, and settings to see if there are any vulnerabilities.

Ways to use OpenVAS to discover vulnerabilities:

- Scan for vulnerabilities with multiple options.
 - Full Scan: Full vulnerability scan for network, server, and web applications.
 - Web Server Scan: A vulnerability scan focusing more on web servers and applications (ports 80 and 443).
 - WordPress Scan: A scan that tests for known WordPress vulnerabilities and web server issues.
 - Joomla Scan: A scan that tests for known Joomla vulnerabilities and web server issues.
- OpenVAS can also scan for host discovery and system discovery.

Reason to use OpenVAS:

- It is derived from Nessus before version 3. The vulnerability database continued to expand and update free of use.
- Free, since it is open-source, there are a lot of experts online that can help navigate through problems.
- It can provide a report listing all the vulnerabilities and sorting them by severity after scanning. Also shows the QoD (quality of Detection): shows a percentage of the detected vulnerabilities' reliability.
- The result summary from the report is very detailed and even shows the solution to that specific vulnerability.
- Super easy to export and import the report from/to OpenVAS with HTML, PDF, and CSV.

Potential drawbacks or limitations of OpenVAS:

- It covers fewer vulnerabilities compared to Nessus. Might miss some flaws that Nessus would have detected. Only supports around 26,000 CVEs.
- Limitation on OS support only runs on Unix and Linux systems. Doesn't support Windows or macOS users.

Screenshot of OpenVAS scanned results:

Report: Results 1 - 100 of 102 (total: 233) PDF 78%

Filter: sort-reverse=severity result_hosts_only=1 min_cvss_base= min_qo

Vulnerability	Severity	QoD	Host	Location	Actions
X Server	10.0 (High)	80%	192.168.56.101	6000/tcp	
PostgreSQL weak password	9.0 (High)	99%	192.168.56.101	5432/tcp	
PostgreSQL Multiple Security Vulnerabilities	8.5 (High)	80%	192.168.56.101	5432/tcp	
TikiWiki Versions Prior to 4.2 Multiple Unspecified Vulnerabilities	7.5 (High)	80%	192.168.56.101	80/tcp	
phpinfo() output accessible	7.5 (High)	80%	192.168.56.101	80/tcp	
ProFTPD Long Command Handling Security Vulnerability	6.8 (Medium)	80%	192.168.56.101	2121/tcp	
PostgreSQL Multiple Security Vulnerabilities	6.8 (Medium)	80%	192.168.56.101	5432/tcp	
phpMyAdmin Bookmark Security Bypass Vulnerability	6.5 (Medium)	80%	192.168.56.101	80/tcp	
PostgreSQL 'bitsubstr' Buffer Overflow Vulnerability	6.5 (Medium)	80%	192.168.56.101	5432/tcp	
PostgreSQL 'intarray' Module 'gettoken()' Buffer Overflow Vulnerability	6.5 (Medium)	80%	192.168.56.101	5432/tcp	
PostgreSQL PL/Perl and PL/Tcl Local Privilege Escalation Vulnerability	6.0 (Medium)	80%	192.168.56.101	5432/tcp	
http TRACE XSS attack	5.8 (Medium)	99%	192.168.56.101	80/tcp	
PostgreSQL 'RESET ALL' Unauthorized Access Vulnerability	5.5 (Medium)	80%	192.168.56.101	5432/tcp	
Check if Mailserver answer to VRFY and EXPN requests	5.0 (Medium)	99%	192.168.56.101	25/tcp	
/doc directory browsable ?	5.0 (Medium)	80%	192.168.56.101	80/tcp	
TikiWiki CMS/Groupware Input Sanitation Weakness Vulnerability	5.0 (Medium)	80%	192.168.56.101	80/tcp	
SSH Weak Encryption Algorithms Supported	4.3 (Medium)	95%	192.168.56.101	22/tcp	

Source: rapid7

<<https://www.rapid7.com/blog/post/2016/11/22/how-to-use-openvas-to-audit-the-security-of-your-network-22/>>

Screenshot of OpenVAS scanned downloaded report PDF:

report-2a463ef1-80df-4fb4-90e8-07d9fad820b8-4.pdf - Mozilla Firefox

file:///tmp/mozilla_kali0/report-2a463ef1-80df-4fb4-90e8-07d9fad820b8-4.pdf

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Africa/Harare", which is abbreviated "CAT". The task was "Metasploitable". The scan started at Mon Aug 2 19:07:31 2021 CAT and ended at Mon Aug 2 19:59:55 2021 CAT. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

- 1 Result Overview 2
 - 1.1 Host Authentications 2
- 2 Results per Host 2
 - 2.1 192.168.43.43 2
 - 2.1.1 High 2121/tcp 3
 - 2.1.2 High 21/tcp 3
 - 2.1.3 High 3306/tcp 4
 - 2.1.4 High 5432/tcp 5
 - 2.1.5 High 8180/tcp 5
 - 2.1.6 High 22/tcp 6
 - 2.1.7 Medium 2121/tcp 7
 - 2.1.8 Medium 21/tcp 7
 - 2.1.9 Medium 80/tcp 8
 - 2.1.10 Low 5900/tcp 9

Source: OPENVAS <<https://www.youtube.com/watch?v=G9MXIId9Vt8>>

Tool/Resources 3: Acunetix

Description: Acunetix is a scalable, quick, and powerful vulnerability scanner with a high level of automation. The scanner audits the web application by checking vulnerabilities such as SQL injection, XSS, weak passwords, and other exploitable vulnerabilities.

Ways to use Acunetix to discover vulnerabilities:

- Scan a website using Acunetix.
 - Go to the applications' targets tab and click on add target.
 - Type in the website that the user wants to target.
 - Click on Scan and select the scan type: Full scan, high-risk vulnerabilities, Cross-site scripting vulnerabilities, SQL injection vulnerabilities, or weak password scan.
 - Click scan.

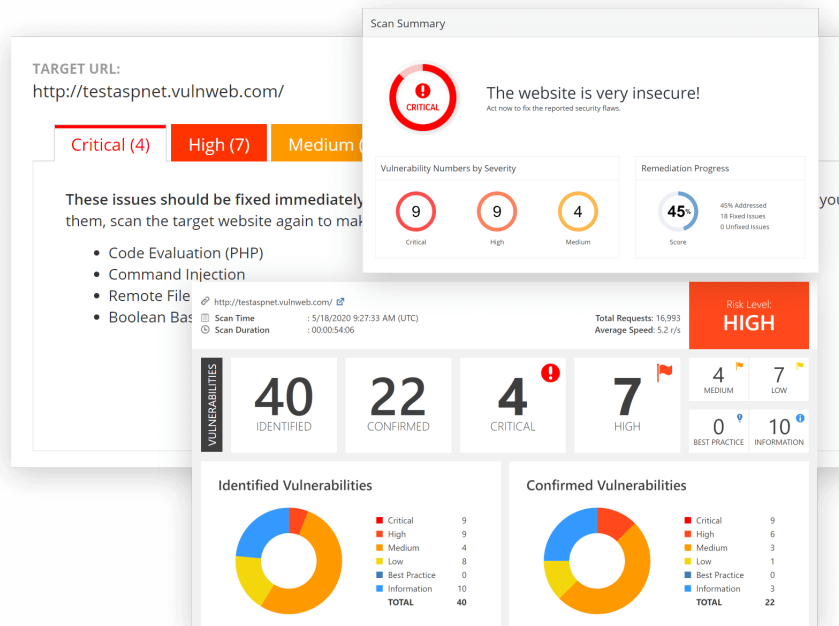
Reason to use Acunetix:

- Very user-friendly GUI and is available for Windows, Linux, and macOS.
- Ability to detect SQL injection vulnerabilities.
- Has very good report options. Users can locate and fix the vulnerability very quickly. It is because Acunetix provides details about the vulnerability, such as source-code line number, stack trace, and affected query.
- Low rate of getting a false positive when scanning a website because the tool understands the web application's behavior.

Potential drawbacks or limitations of Acunetix:

- Once configured the website, the user can not edit it. So the user has to be very careful when configuring the options. And when dealing with customer service, it can be a very slow response time.
- It only has a trial period of 14 days. The scanner is not available in the free version.
- The price of the tool can be expensive for smaller companies. The price can be from \$4500 to \$26600.

Screenshot of Acunetix report of the impact:



Source: acunetix <<https://www.acunetix.com/product/acunetix360/>>

Tool/Resources 4: Wireshark

Description: Wireshark is a free and open-source powerful packet-capturing tool that can deep dive into a user's network to analyze the traffic and discover the problem. It is a tool that lets the user put the network traffic under a microscope and examine it to find the root cause of the problem.

Ways to use Wireshark to discover vulnerabilities:

- Scan for network vulnerabilities
 - Capture the traffic packets for a few minutes, then stop the capturing.
 - Check if all the traffic belongs there.
 - If a protocol looks suspicious, you click on it and see whether it is an attack or an error.
 - Can also go to the statistics tab and look at the protocol hierarchy.
 - If a protocol has the word "data" under it, that means Wireshark doesn't recognize the application, and the user can filter to that specific protocol.

Reason to use Wireshark:

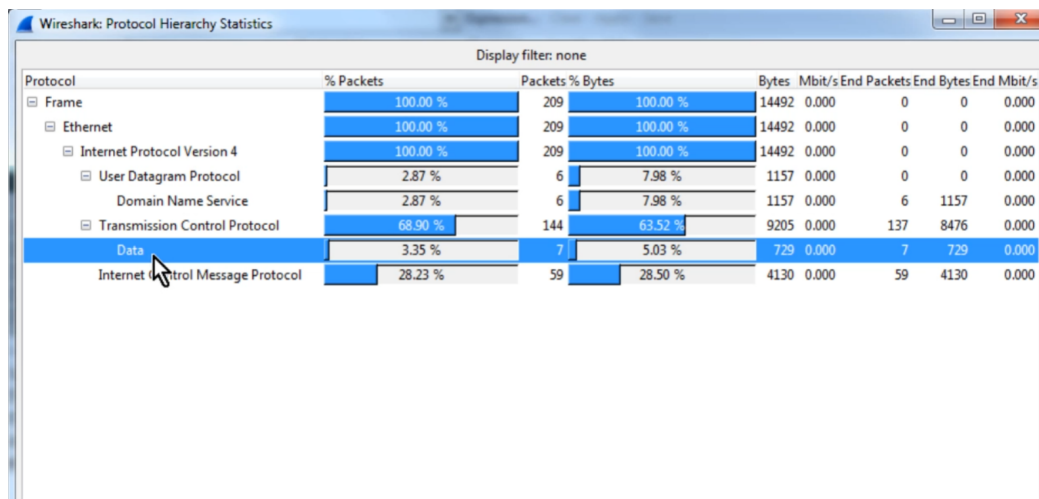
- Free software and open-source.
- Available in various operating systems, Windows and UNIX.

- Easy to use, one click can see the details of the packet traffic.

Potential drawbacks or limitations of Wireshark:

- Since it's free, it is a very easy tool for hackers to sniff out network traffic for an attack if the hacker gets into the Wi-Fi.
- The protocols are very confusing for beginners to understand. Therefore, it's not user-friendly.
- It can be a very long and tedious wait to capture and analyze all the packages.

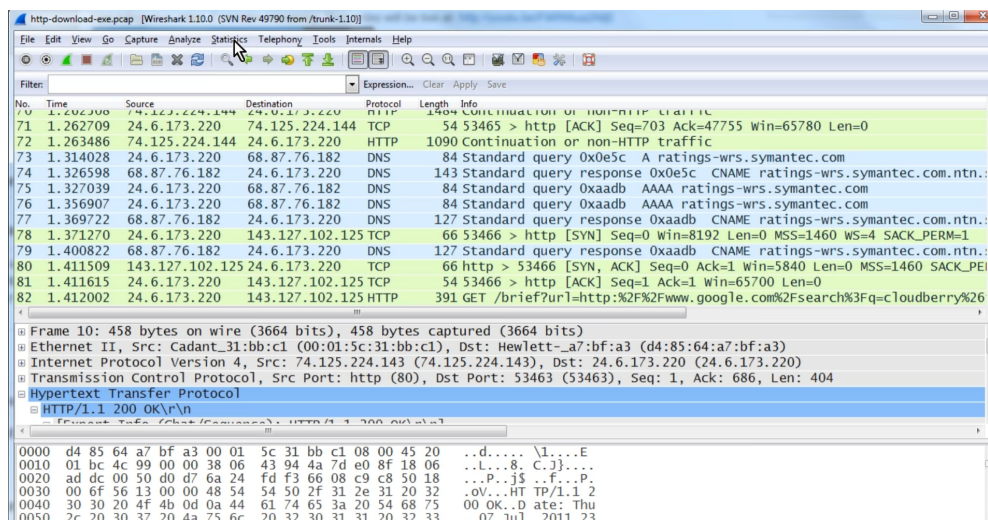
Screenshot of Wireshark Protocol Hierarchy Statistics Has Data:



Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End	Packets	End	Bytes	End	Mbit/s
Frame	100.00 %	209	100.00 %	14492	0.000		0		0		0.000
Ethernet	100.00 %	209	100.00 %	14492	0.000		0		0		0.000
Internet Protocol Version 4	100.00 %	209	100.00 %	14492	0.000		0		0		0.000
User Datagram Protocol	2.87 %	6	7.98 %	1157	0.000		0		0		0.000
Domain Name Service	2.87 %	6	7.98 %	1157	0.000		6		1157		0.000
Transmission Control Protocol	68.90 %	144	63.52 %	9205	0.000		137		8476		0.000
Data	3.35 %	7	5.03 %	729	0.000		7		729		0.000
Internet Message Protocol	28.23 %	59	28.50 %	4130	0.000		59		4130		0.000

Source: Laura Chappell <<https://www.youtube.com/watch?v=OwQmwbD1uls&t=217s>>

Screenshot of Wireshark Capturing packets:



No.	Time	Source	Destination	Protocol	Length	Info
70	1.262709	24.6.173.220	74.125.224.144	TCP	54	53465 > http [ACK] Seq=703 Ack=47755 Win=65780 Len=0
71	1.263486	74.125.224.144	24.6.173.220	HTTP	1090	Continuation or non-HTTP traffic
72	1.314028	24.6.173.220	68.87.76.182	DNS	84	Standard query 0x0e5c A ratings-wrs.symantec.com
73	1.326598	68.87.76.182	24.6.173.220	DNS	143	Standard query response 0x0e5c CNAME ratings-wrs.symantec.com.ntn.
74	1.327039	24.6.173.220	68.87.76.182	DNS	84	Standard query 0xaadb AAAA ratings-wrs.symantec.com
75	1.356907	24.6.173.220	68.87.76.182	DNS	84	Standard query 0xaadb AAAA ratings-wrs.symantec.com
76	1.369722	68.87.76.182	24.6.173.220	DNS	127	Standard query response 0xaadb CNAME ratings-wrs.symantec.com.ntn.
77	1.371270	24.6.173.220	143.127.102.125	TCP	66	53466 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
78	1.400822	68.87.76.182	24.6.173.220	DNS	127	Standard query response 0xaadb CNAME ratings-wrs.symantec.com.ntn.
79	1.411509	143.127.102.125	24.6.173.220	TCP	66	http > 53466 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
80	1.411615	24.6.173.220	143.127.102.125	TCP	54	53466 > http [ACK] Seq=1 Ack=1 Win=65700 Len=0
81	1.412002	24.6.173.220	143.127.102.125	HTTP	391	GET /brief?url=http%3F%2Fwww.google.com%2Fsearch%3Fq=c%2Fcloudberry%26

Frame 10: 458 bytes on wire (3664 bits), 458 bytes captured (3664 bits)											
Ethernet II, Src: Cadant_31:bb:c1 (00:01:5c:31:bb:c1), Dst: Hewlett-a7:bf:a3 (d4:85:64:a7:bf:a3)											
Internet Protocol Version 4, Src: 74.125.224.143 (74.125.224.143), Dst: 24.6.173.220 (24.6.173.220)											
Transmission Control Protocol, Src Port: http (80), Dst Port: 53463 (53463), Seq: 1, Ack: 686, Len: 404											
Hypertext Transfer Protocol											
HTTP/1.1 200 OK											

Offset	Dissection	Raw Data
0000	d4 85 64 a7 bf a3 00 01 5c 31 bb c1 08 00 45 20	..d....\1....E
0010	01 bc 4c 99 00 00 38 06 43 94 a7 d0 e0 8f 18 06	..l...8. C.}....
0020	ad dc 00 50 d0 d7 6a 24 fd f3 66 08 c9 c8 50 18	...P...j\$. .f...P.
0030	00 6f 56 13 00 00 48 54 54 50 2f 31 2e 31 20 32	..ov...HT TP/1.1 2
0040	30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 54 68 75	00 OK..D ate: Thu
0050	2c 20 30 37 20 4a 75 6c 20 32 30 31 31 20 32 33	, 07 Jul 2011 23

Source: Laura Chappell <<https://www.youtube.com/watch?v=OwQmwbD1uls&t=217s>>

Tool/Resources 5: Burp Suite

Description: Burp Suite is a Web penetration testing framework based on Java. It helps users identify the vulnerabilities and attack vectors that affect web-based applications. Burp Suite has three versions: free, professional, and enterprise-licensed editions. Burp Suite configures the browser to divert traffic with the help of the proxy. The proxy will act as a man-in-middle to capture and analyze every response from the web application.

Ways to use Burp Suite to discover vulnerabilities:

- Proxy tool: intercepts proxies that let users see and modify the contents of requests and responses during their transmission.
- Spider tool: used to map the target web application to observe its functionality and discover potential vulnerabilities.
- Scanner tool: used to scan the website application automatically for common vulnerabilities.
- Intruder tool: A fuzzer that runs a set of values through an input point. Used for Brute-force, dictionary attack, and testing the attacking rate limit on the web application.
- Repeater tool: let the user send requests repeatedly with modifications of their liking.
- Sequencer tool: An entropy checker that checks for the randomness of token generation by the webserver.
- Decoder tool: Used for decoding URLs, HTML, Base64, Hex, and more. It is also used for construction payload for vulnerability.

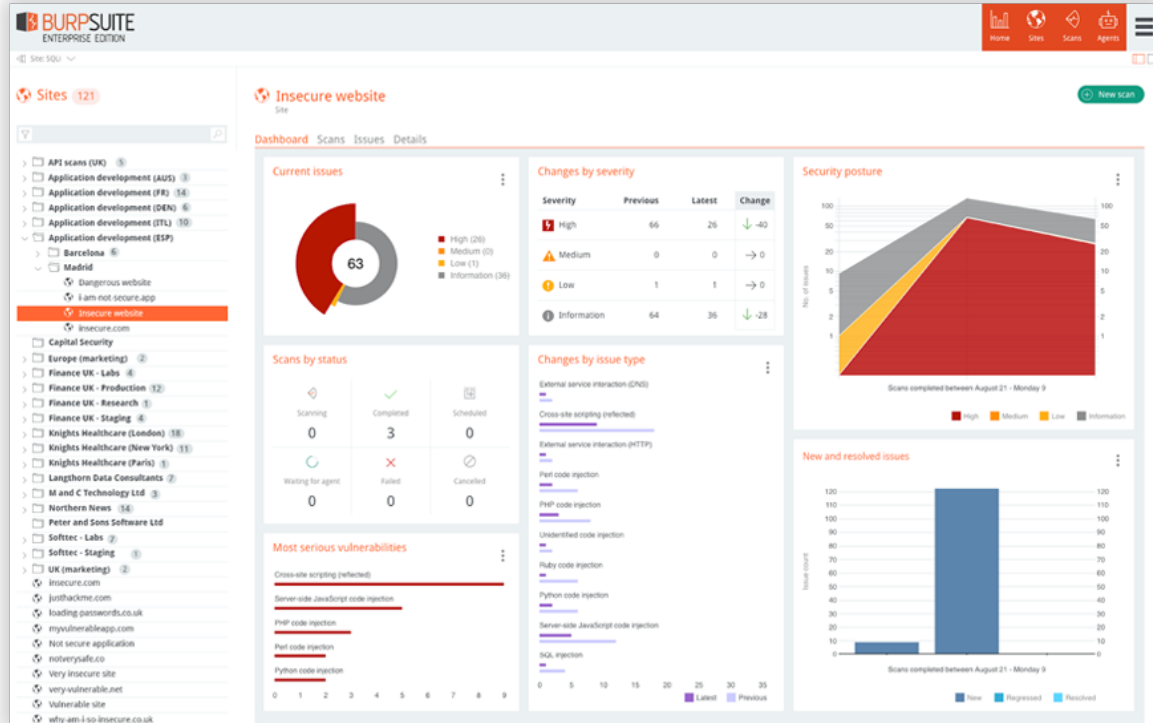
Reason to use Burp Suite:

- Burp Suite is available on the most popular operating systems: Windows, Linux, and Mac OS X.
- Burp Suite is also available on Android mobile.
- Burp Suite has various tools to use and find right on the GUI, and the community version is free.
- It is very easy to install and set up. And the report is very GUI is very user-friendly.
- Using Burp Suite, users can find vulnerabilities such as injection, broken authentication, XSS, CSRF, insurance direct object references, security misconfiguration, and sensitive data exposure.

Potential drawbacks or limitations of Burp Suite:

- False positive results can be high but can mark as false positives for future reports.
- It can crash when the user uses a high number of threads.
- The function (scanner tool) is not available in the free version.
- Price: The Enterprise edition can be expensive, 6000 per year. And the professional is 450 for one user per year.

Screenshot of Burp Suite scanned results:



Source: portswigger <<https://portswigger.net/organizations/security-reporting>>