VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

REPORT ON THE PROJECT OF INFORMATION SECURITY AND AUDIT LAB

TEAM MEMBERS

- **SIMRAN PRASAD -21BCB0014**
- **HARDIK SINGH – 21BCE3124**

AIM:-

TO CHECK THE VULNERBILITIES INSIDE THE RAILWAYS TICKETING SYSTEM USING WEB SECURITY

APPLICATIONS USED

- NESSUS
- SELENIUM WEBDRIVER
- BUGZILLA

DOMAIN INTRODUCTION

Network security is most important to computer users, organizations and in the military. Security is essential for networks and applications. Existence of communication gap between developers of networks and the developers of security technology has to be considered in part of network security. Network security is a concern about computers at each end of the communication chain. There is a possibility that the communication channel is vulnerable to attack when transmitting data. Hackers could intend the communication channel, acquire the data, decrypt, and re-insert a false data.

After running a scan, Nessus client itself will list each vulnerability found, reporting its level of severity and suggesting how this problem could be fixed. Nessus categorises the vulnerabilities of risk as Low, Medium, High and Critical as in by generating report.

ABSTRACT:

Nessus reports all categories of vulnerabilities by scanning a network. Our tool refines only the major vulnerabilities using Selenium Web Driver. Bugzilla on the other hand, reports the bug and performs ticketing by manually assigning bug.

ARCGITECTURE:

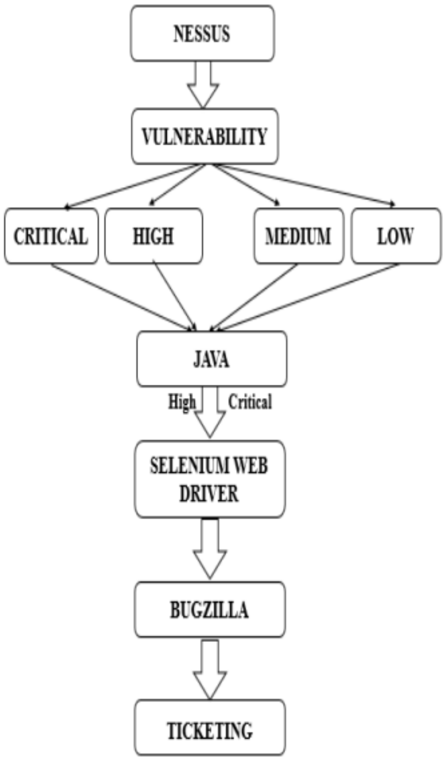


Fig 1. Block Diagram of the Automation tool

RELATED WORKS:

GENERATION OF VULNERABILITY REPORT USING NESSUS

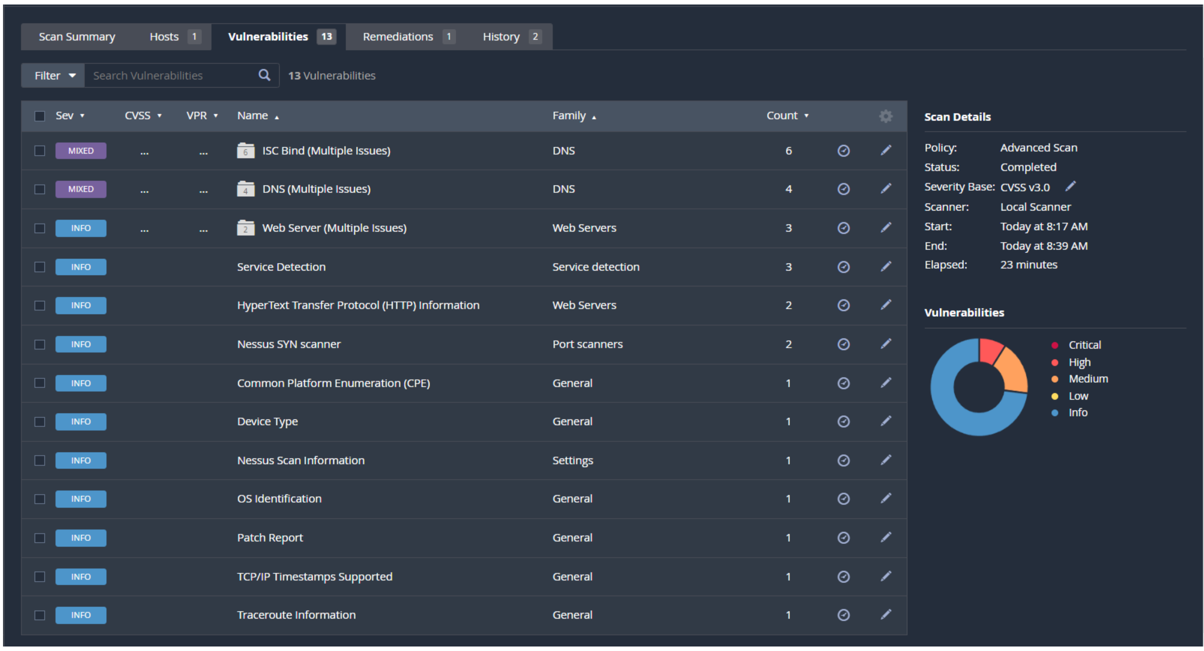
Nessus is vulnerability scanner developed by Tenable Network Security. Nessus is a powerful tool to help keep the domains free of vulnerabilities that viruses and hackers commonly target to exploit in any computer (or group of computers) connected to the internet. . Nessus is a tool which does not actively prevent attacks but scans the computer network for any vulnerability that hackers try to exploit.

After running a scan, Nessus client itself will list each vulnerability found, reporting its level of severity and suggesting how this problem could be fixed. Nessus categorises the vulnerabilities of risk as Low, Medium, High and Critical as in by generating report.

Nessus does not make assumptions about the server configuration unlike other scanners which leads the scanners to miss real vulnerabilities. Nessus clients generate more elaborative and graphical reports in a variety of different formats about the vulnerabilities. The formats in which the report can be exported are, .nessus –

This format uses an expanded set of XML tags to make extracting and parsing information. This report does not allow chapter selection HTML - A report generated using standard HTML that allows chapter selection and opens in a new tab in your browser. PDF - A report generated in PDF format that allows chapter selection.

Nessus DB - A proprietary encrypted database format that contains all the information from a scan, including the results and audit trials. CSV- A comma-separated values (CSV) report that can be used to be imported into many external programs like spreadsheets, databases and more. This report does not allow chapter selection.



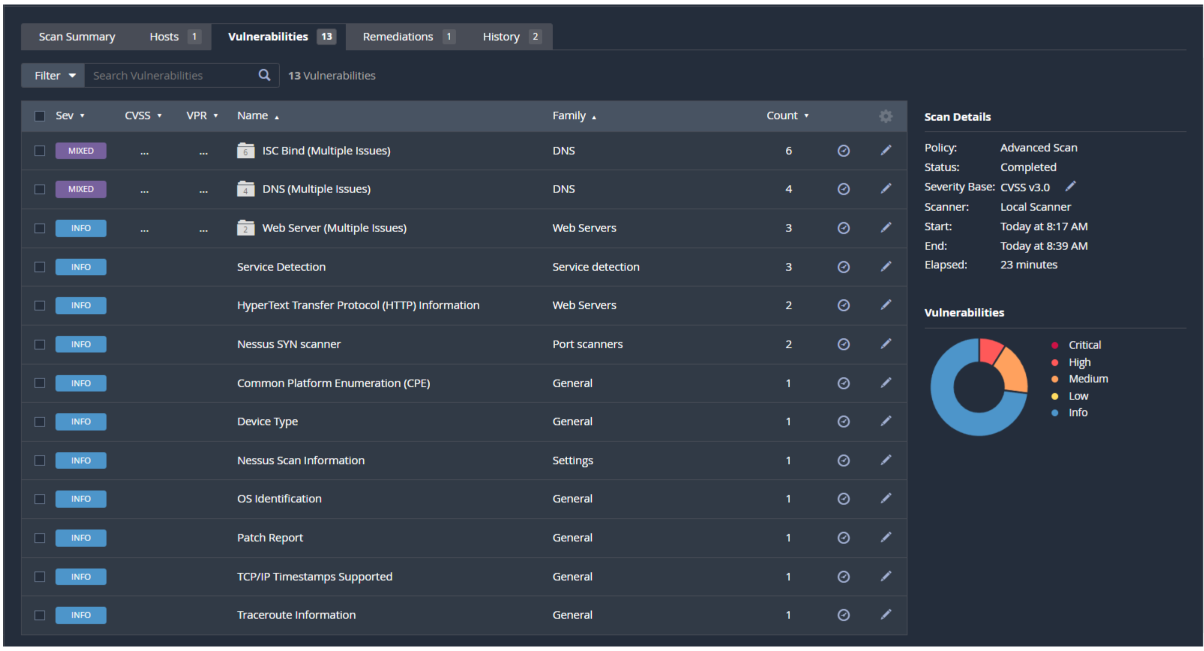
13 Vulnerabilities

☐	Sev	CVSS	VPR	Name	Family	Count
☐	MIXED	...	...	ISC Bind (Multiple Issues)	DNS	6
☐	MIXED	...	...	DNS (Multiple Issues)	DNS	4
☐	INFO	...	...	Web Server (Multiple Issues)	Web Servers	3
☐	INFO			Service Detection	Service detection	3
☐	INFO			HyperText Transfer Protocol (HTTP) Information	Web Servers	2
☐	INFO			Nessus SYN scanner	Port scanners	2
☐	INFO			Common Platform Enumeration (CPE)	General	1
☐	INFO			Device Type	General	1
☐	INFO			Nessus Scan Information	Settings	1
☐	INFO			OS Identification	General	1
☐	INFO			Patch Report	General	1
☐	INFO			TCP/IP Timestamps Supported	General	1
☐	INFO			Traceroute Information	General	1

Scan Details

Policy: Advanced Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 8:17 AM
End: Today at 8:39 AM
Elapsed: 23 minutes

Vulnerabilities



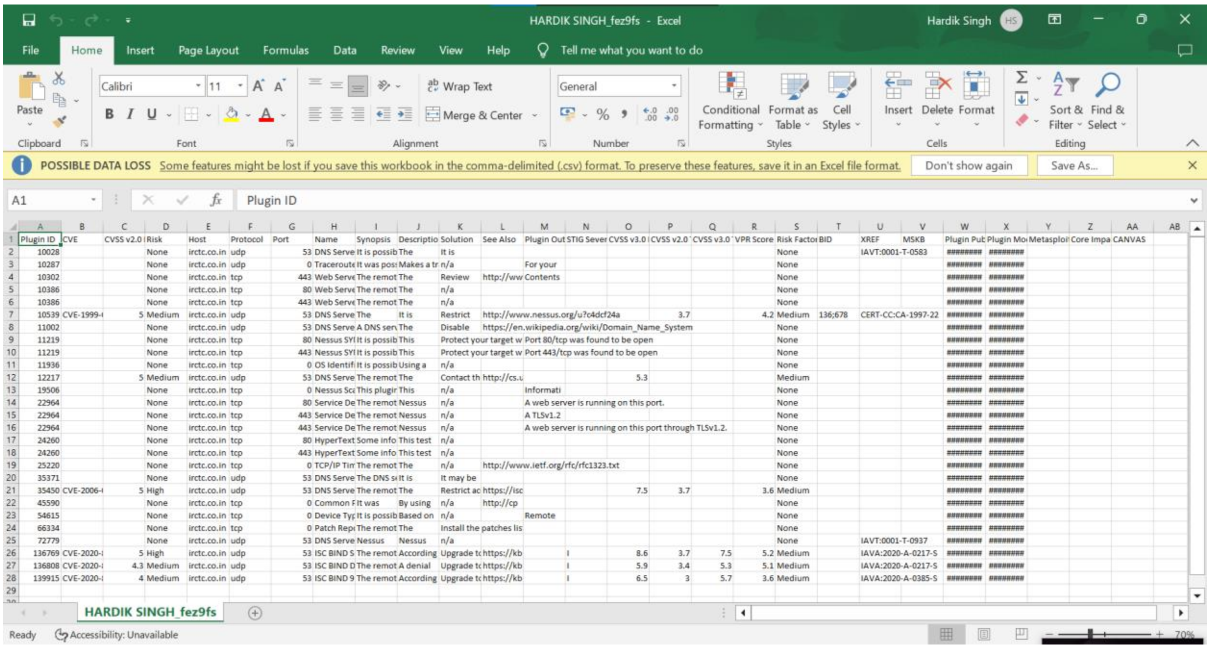
13 Vulnerabilities

☐	Sev	CVSS	VPR	Name	Family	Count
☐	MIXED	...	...	ISC Bind (Multiple Issues)	DNS	6
☐	MIXED	...	...	DNS (Multiple Issues)	DNS	4
☐	INFO	...	...	Web Server (Multiple Issues)	Web Servers	3
☐	INFO			Service Detection	Service detection	3
☐	INFO			HyperText Transfer Protocol (HTTP) Information	Web Servers	2
☐	INFO			Nessus SYN scanner	Port scanners	2
☐	INFO			Common Platform Enumeration (CPE)	General	1
☐	INFO			Device Type	General	1
☐	INFO			Nessus Scan Information	Settings	1
☐	INFO			OS Identification	General	1
☐	INFO			Patch Report	General	1
☐	INFO			TCP/IP Timestamps Supported	General	1
☐	INFO			Traceroute Information	General	1

Scan Details

Policy: Advanced Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 8:17 AM
End: Today at 8:39 AM
Elapsed: 23 minutes

Vulnerabilities



POSSIBLE DATA LOSS Some features might be lost if you save this workbook in the comma-delimited (.csv) format. To preserve these features, save it in an Excel file format.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB
1	Plugin ID	CVE	CVSS v2.0	Risk	Host	Protocol	Port	Name	Synopsis	Descriptio	Solution	See Also	Plugin Out	STIG Sever	CVSS v3.0	CVSS v2.0	CVSS v3.0	VPR Score	Risk Factor	BID	XREF	MSKB	Plugin Pub	Plugin Mo	Metasploi	Core Impa	CANVAS	
2	10028			None	irctc.co.in	udp	53	DNS Serve	It is possib	The	It is								None		IAVT:0001-T-0583		########	########				
3	10287			None	irctc.co.in	udp	0	Traceroute	It was pos	Makes a tr	n/a		For your						None				########	########				
4	10302			None	irctc.co.in	tcp	443	Web Serve	The remot	The	Review	http://ww	Contents						None				########	########				
5	10386			None	irctc.co.in	tcp	80	Web Serve	The remot	The	n/a								None				########	########				
6	10386			None	irctc.co.in	tcp	443	Web Serve	The remot	The	n/a								None				########	########				
7	10539	CVE-1999-	5	Medium	irctc.co.in	udp	53	DNS Serve	The	It is	Restrict	http://www.nessus.org/u?c4dcf24a				3.7		4.2	Medium	136;678	CERT-CC:CA-1997-22		########	########				
8	11002			None	irctc.co.in	udp	53	DNS Serve	A DNS serv	The	Disable	https://en.wikipedia.org/wiki/Domain_Name_System							None				########	########				
9	11219			None	irctc.co.in	tcp	80	Nessus SYN	It is possib	This	Protect your target w		Port 80/tcp was found to be open						None				########	########				
10	11219			None	irctc.co.in	tcp	443	Nessus SYN	It is possib	This	Protect your target w		Port 443/tcp was found to be open						None				########	########				
11	11936			None	irctc.co.in	tcp	0	OS Identifi	It is possib	Using a	n/a								None				########	########				
12	12217		5	Medium	irctc.co.in	udp	53	DNS Serve	The remot	The	Contact th	http://cs.u			5.3				Medium				########	########				
13	19506			None	irctc.co.in	tcp	0	Nessus Sca	This plugin	This	n/a		Informati						None				########	########				
14	22964			None	irctc.co.in	tcp	80	Service De	The remot	Nessus	n/a		A web server is running on this port.						None				########	########				
15	22964			None	irctc.co.in	tcp	443	Service De	The remot	Nessus	n/a		A TLSv1.2						None				########	########				
16	22964			None	irctc.co.in	tcp	443	Service De	The remot	Nessus	n/a		A web server is running on this port through TLSv1.2.						None				########	########				
17	24260			None	irctc.co.in	tcp	80	HyperText	Some info	This test	n/a								None				########	########				
18	24260			None	irctc.co.in	tcp	443	HyperText	Some info	This test	n/a								None				########	########				
19	25220			None	irctc.co.in	tcp	0	TCP/IP Tim	The remot	The	n/a	http://www.ietf.org/rfc/rfc1323.txt							None				########	########				
20	35371			None	irctc.co.in	udp	53	DNS Serve	The DNS s	It is	It may be								None				########	########				
21	35450	CVE-2006-	5	High	irctc.co.in	udp	53	DNS Serve	The remot	The	Restrict ac	https://isc			7.5	3.7		3.6	Medium				########	########				
22	45590			None	irctc.co.in	tcp	0	Common F	It was	By using	n/a	http://cp							None				########	########				
23	54615			None	irctc.co.in	tcp	0	Device Typ	It is possib	Based on	n/a		Remote						None				########	########				
24	66334			None	irctc.co.in	tcp	0	Patch Rep	The remot	The	Install the patches lis								None				########	########				
25	72779			None	irctc.co.in	udp	53	DNS Serve	Nessus	Nessus	n/a								None		IAVT:0001-T-0937		########	########				
26	136769	CVE-2020-	5	High	irctc.co.in	udp	53	ISC BIND S	The remot	According	Upgrade t	https://kb		I	8.6	3.7	7.5	5.2	Medium		IAVA:2020-A-0217-S		########	########				
27	136808	CVE-2020-	4.3	Medium	irctc.co.in	udp	53	ISC BIND D	The remot	A denial	Upgrade t	https://kb		I	5.9	3.4	5.3	5.1	Medium		IAVA:2020-A-0217-S		########	########				
28	139915	CVE-2020-	4	Medium	irctc.co.in	udp	53	ISC BIND 9	The remot	According	Upgrade t	https://kb		I	6.5	3	5.7	3.6	Medium		IAVA:2020-A-0385-S		########	########				
29																												

VULNERABILITIES REFINEMENT USING SELENIUM WEBDRIVER

Selenium WebDriver accepts commands and pass them to the browser. The CSV report format from the Nessus is passed as an input to the Selenium WebDriver using Java. This format is taken as it contains vast information about the vulnerabilities compared to other formats. Then the elements from the report are refined for further processing using Bugzilla. The significant elements to be extracted from the report comprises of Common Vulnerabilities and Exposures (CVE), Common Vulnerability Scoring System (CVSS), name and description from the high risk vulnerability. CVE system is maintained by MITRE Corporation that defines CVE identifiers as common, unique identifiers for publicly known information-security vulnerabilities [5]. CVSS is free and industry standard for estimating the severity of computer system security vulnerabilities [6]. This attempts to assign scores ranging from 0-10 for the severity of vulnerabilities which is calculated by formula depending on metrics that approximates the impact and ease of exploit. We are taking the vulnerability scores above 7, which represents high and critical in the severity scale. Name and description gives the name and description of the vulnerability.

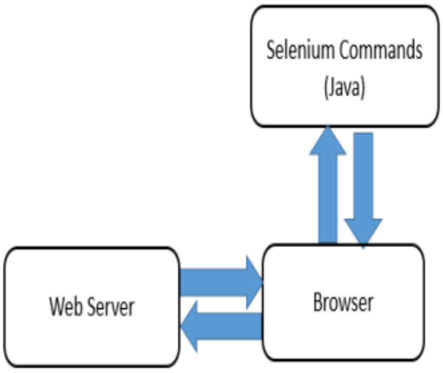


Fig 2. Architecture of Selenium Web driver

TICKET CREATION USING BUGZILLA AND AUTOMATION

Bugzilla version 4 is an open source product, used as a bug-tracking/defect-tracking system which allows an individual or groups of developers to have track on critical bugs effectively in their product [4]. Our automation tool utilizes Bugzilla in order to perform ticketing, as Bugzilla does ticketing by requiring a person to assign bug manually. It is initiated by connecting through localhost and feeding the input from the previous stage which extracted CVE, CVSS, name and description from Nessus. Our tool manages to send a report about the bug one by one through e-mail to the group of people concerned in networking department without the need of a person to assign tickets manually

CONCLUSION

Nessus reports all categories of vulnerabilities by scanning a network. Our tool refines only the major vulnerabilities using Selenium Web Driver. Bugzilla on the other hand, reports the bug and performs ticketing by manually assigning bug. This tool overcomes that by an automation process by which it takes only the critical vulnerabilities significant elements produced from Nessus and using Bugzilla to create tickets and produce bug report to the employees. This tool has been developed for the vulnerability issue tracking using Bugzilla. This will help to improve Strong link between review and bugs and commit queue integration and Comments are emailed out automatically. Tracking bugs improves communication, ensures accountability and increases security. The employees can review the report in a formatted way which would help minimizing the time to solve the bug. We can check the employees work accordingly

- We have scan the vunerability the of irctc.io.in by nessus application then we made a report from by nessus application
- After making that report we will use the selinuim webdriver then we filter out all the vulnerability by using java code and that app
- After that we will take that file use it for buzilla software the we will remove all the bugs from that site

<u>REFERENCES:</u>

Research papers.