Vulnerability Assessment & Penetration Testing

Project report submitted in partial fulfilment of the requirement for the degree of

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE ENGINEERING

By

Devesh Nijhawan (191279)

Under the supervision of

Dr. Pankaj Dhiman

Department of Computer Science & Engineering

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY,
WAKNAGHAT May 2023

Certificate

I hereby declare that the work reported in the **B.Tech** Project Report entitled "**Vulnerability Assessment & Penetration Testing**" submitted at the **Jaypee University of Information Technology, Waknaghat,** India is an authentic record of our work carried out under the supervision of **Dr. Pankaj Dhiman** and **Mr. Ankit Khare**. I have not submitted this work elsewhere for any other degree or diploma.

Devesh Nijhawan
191279

This is to certify that the above statement made by the candidates is correct to the best of my knowledge.

Dr. Pankaj Dhiman
Date:

Mr. Ankit Khare
CTO, Shivalik Small Finance Bank
Date: 12/05/2023
Head of the Department/Project Coordinator

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

PLAGIARISM VERIFICATION REPORT

Date: ………………………….

Type of Document (Tick): □ **PhD Thesis** □ **M.Tech Dissertation/ Report** □ **B.Tech Project Report** □ **Paper**

Name:______________________________**Department:**__________________**Enrolment No**

____ **Contact**

No._____________________________________**E-**

mail.____ **Name of the**

Supervisor:

____

____________________________________ **Title of the Thesis/Dissertation/Project Report/Paper (In Capital letters):** _______________________________________

____

____

UNDERTAKING

I undertake that I am aware of the plagiarism related norms/ regulations, if I found guilty of any plagiarism and copyright violations in the above thesis/report even after award of degree, the University reserves the rights to withdraw/revoke my degree/report. Kindly allow me to avail Plagiarism verification report for the document mentioned above.

Complete Thesis/Report Pages Detail:

- Total No. of Pages =
- Total No. of Preliminary pages =
- Total No. of pages accommodate bibliography/references =

(Signature of Student)

FOR DEPARTMENT USE

We have checked the thesis/report as per norms and found **Similarity Index** at..................(%). Therefore, we
are forwarding the complete thesis/report for final plagiarism check. The plagiarism verification report may behanded over to the candidate.

(Signature of Guide/Supervisor) **Signature of HOD**

FOR LRC USE

The above document was scanned for plagiarism check. The outcome of the same is reported below:

Copy Received on	**Excluded**	**Similarity Index (%)**	**Generated Plagiarism Report Details** (Title, Abstract & Chapters)	
	• All Preliminary Pages • Bibliography/Images/Quotes		Word Counts	
Report Generated on			Character Counts	
		Submission ID	Total Pages Scanned	

	• 14 Words String		File Size	

Checked by
Name & Signature **Librarian**

....

Please send your complete thesis/report in (PDF) with Title Page, Abstract and Chapters in (Word File)through the supervisor at plagcheck.juit@gmail.com

LIST OF FIGURES

ACKNOWLEDGEMENT

Firstly, I express my heartiest thanks and gratefulness to Almighty God for his divine blessing in making it possible to complete the project work successfully.

I am grateful and wish my profound indebtedness to Supervisor **Dr. Pankaj Dhiman, Assistant Professor (SG)** Department of CSE **Jaypee University of Information Technology, Waknaghat** and **Mr. Ankit Khare, CTO**, **Shivalik Small Finance Bank,** Deep Knowledge & keen interest of my supervisor in the field of **Machine Learning** to carry out this project. His endless patience, scholarly guidance, continual encouragement, constant and energetic supervision, constructive criticism, valuable advice, and reading many inferior drafts and correcting them at all stages have made it possible to complete this project.

I would like to express my heartiest gratitude to **Dr. Pankaj Dhiman, Department** of CSE and **Mr. Ankit Khare**, Shivalik Small Finance Bank, for his kind help in finishing my project.

I would also generously welcome each of those individuals who have helped me straightforwardly or in a roundabout way to make this project a win. In this unique situation, I might want to thank the various staff individuals, both educating and non-instructing, which have developed their convenient help and facilitated my undertaking

Finally, I must acknowledge with due respect the constant support and patients of my parents.

Devesh Nijhawan(191279)

TABLE OF CONTENT

LIST OF ABBREVIATIONS

LSTM – long short-term memory

GA- genetic algorithm

SVM- support vector machine

HMM- hidden Markov model

ML-Machine learning

Tech. - techniques

SMP-stock market prediction

ANN- artificial neural network

CNN- Convolutional Neural Network

RNN- Recurrent Neural Network

PCA – Principal Component analysis

LDA – Linear Discriminant Analysis

ABSTRACT

Shivalik changed its name from Urban Cooperative Bank to become India's first Small Finance Bank. In providing retail banking products and services, we have more than 24 years of banking experience. Shivalik has always placed a strong emphasis on technology, with customer centricity as a fundamental tenet. The Infosys Finacle Core Banking and Digital Banking Suite, which includes online and mobile banking, power the Bank. The Bank has unequalled agility thanks to the cloud-based architecture, which enables cost-effective scale management and growth. Shivalik is a direct member of the National Financial Switch and is accessible on all retail payment platforms.

While a penetration test (Pen Test) seeks to exploit the vulnerabilities to see if unauthorized access or other harmful behaviour is possible, a vulnerability assessment only finds and reports reported issues. Penetration testing should take place from both inside the network and from the outside (external testing), and it often comprises network penetration testing, application security testing, policies and processes around the networks and applications.

At the request of [CLIENT NAME], [Red Team] carried out a Red Team engagement to assess the entire scope of a plausible danger. The [Red Team] team discovered several exploitable flaws that might be used to gain access, increase privileges, cover more ground, and remove confidential data from the network. Based on the path shown during the assessment, [Red Team] determines that an external threat can successfully compromise [CLIENT NAME] systems. None of the actions detailed in this report required the use of any highly specialized tools or exploits.

CHAPTER 1 – INTRODUCTION

1.1. INTRODUCTION

Shivalik small finance Bank is a flourishing Indian based financial institution that provides an extensive range of banking Solution or individuals and businesses alike. By offering inclusive financial solutions that are suited to their requirements, the bank's primary goal is to empower those who have been left out of standard banking procedures. Shivalik Small Finance Bank, a small finance bank registered with the RBI, focuses on providing services to the underbanked or unbanked communities in rural and semi-urban areas. Farmers and low-income people make up their main client base demography, which is primarily made up of MSMEs.

Shivalik Small Finance Bank is an Indian financial institution that operates as a small finance bank in accordance with the regulations set by the Reserve Bank of India (RBI). Established in 2017, Shivalik Small Finance Bank aims to provide accessible and inclusive banking services to individuals, micro and small enterprises, and the unbanked and underbanked sections of society.

As a small finance bank, Shivalik focuses on offering a range of financial products and services tailored to meet the specific needs of its target customer segments. Savings accounts, current accounts, fixed deposits, recurring deposits, and small business loans are among the services that are generally provided.

loans, microfinance, and remittance services.

Shivalik Small Finance Bank prioritises financial inclusion and works to close the gap between the underserved community and standard banking services. The bank seeks to improve the usability, affordability, and accessibility of financial services for its clients by utilising cutting-edge methods and technology.

In line with its commitment to promoting financial literacy and empowerment, Shivalik Small Finance Bank engages in various community development activities and initiatives. These efforts include conducting financial literacy programs, skill development training, and providing support to local entrepreneurs and self-help groups.

The bank operates through a network of branches, customer service centres, and digital channels to cater to the diverse banking needs of its customers. Shivalik is driven by a customer-centric approach and aims to provide personalized services while maintaining high standards of transparency, integrity, and ethical business practices.

As a small finance bank, Shivalik is regulated by the RBI and adheres to the guidelines and regulations set by the central bank to ensure the safety and security of its customers' funds.

Overall, Shivalik Small Finance Bank plays a crucial role in fostering financial inclusion by providing accessible banking services and promoting economic growth in the communities it serves.

1.2. Shivalik Bank

The ideals of the organization are incorporated with diverse elements of nature in the Shivalik Bank logo. The small green mountain/triangle and the blue on top of the image icon in the photo stand for the earth and the sky, respectively. It also suggests reaching upward because there is an arrow pointing up. These characteristics are essential to the company's value since Shivalik Bank strives to stand securely on the ground while reaching for the stars.

Mountains are symbolic of stability, strength, and growth when seen abstractly. The image's mountain range, which is hidden by other mountains, symbolizes the brand's forward-thinking nature. For all of our services, we are interconnected, and the team's collective effort is as powerful as a mountain range. This shows how effectively we service both our internal and external clients. The blue portion of the sky represents the universe, which also represents our potential customers. This reveals a lot about our potential and goals.

The icon's rounded blue edge illustrates our clients' humble, polite, friendly, and professional communication skills.

The earthy tones used by Shivalik Bank to represent a grounded attitude are the inspiration for the colour green. Despite having a clear goal of continuing to develop, we never placed our customers before anything. Our practical approach is what gives Shivalik Bank its "client first" mentality.

With purposeful omission, the negative space demonstrates how Shivalik Bank supports growth.

SHIVALIK
Shivalik Small Finance Bank

1.1 Shivalik Small Finance Bank Logo

1.3. Products & Services at Shivalik

Shivalik Small Finance Bank offers a range of products and services designed to cater to the diverse banking needs of its customers. Here are some of the key offerings provided by Shivalik:

→ Accounts

1. Savings Accounts: Shivalik offers regular savings accounts, which are designed for individuals to deposit and save their money while earning interest on their balances. These accounts typically provide features such as ATM/debit cards, online banking, and mobile banking.

2. Current Accounts: Current accounts are typically used by corporations, independent contractors, and non-profit organisations. Shivalik offers current accounts with features including chequebooks, overdraft capabilities, and electronic fund transfers that enable frequent transactions such as deposits, withdrawals, and payments.

3. Basic Savings Accounts: Shivalik offers simple savings accounts for customers who might not have easy access to formal banking services in an effort to promote financial inclusion. These accounts feature minimal minimum balance requirements and fewer complicated criteria.

4. Fixed Deposit Accounts: Shivalik provides fixed deposit accounts that let consumers deposit a large quantity of money for a set amount of time at a set interest rate. These accounts offer many tenure options and give higher interest rates than savings accounts.

5. Recurring Deposit Accounts: By making a fixed contribution every month for a specified period of time, recurring deposit accounts let people save money on a regular basis. Shivalik provides flexible tenure options and excellent interest rates for recurring deposit accounts.

6. NRI Accounts: Shivalik provides Non-Resident Indian (NRI) accounts for Indian citizens residing abroad. These accounts cater to the unique banking requirements of NRIs, allowing them to manage their finances and make transactions in India.

7. Pension Accounts: Shivalik offers pension accounts for individuals who receive a pension, such as retired employees. These accounts provide convenient access to pension funds and may offer additional benefits and services specifically tailored for pensioners.

→ Deposits

- Savings Deposits: Savings deposits are accounts where individuals can deposit and save their money while earning interest on their balances. Shivalik offers savings deposit accounts with features such as ATM/debit cards, online banking, and mobile banking.

- Current Deposits: Current deposits are primarily designed for businesses, self-employed individuals, and organizations. Shivalik offers current deposit accounts that allow frequent transactions, including deposits, withdrawals, and payments, with features like check books, overdraft facilities, and electronic fund transfers.

- Fixed Deposits: Fixed deposits (also known as term deposits) are accounts where customers can deposit a lump sum amount for a specific period at a fixed interest rate. Shivalik offers fixed deposit accounts with competitive interest rates and flexible tenure options. The interest rates and tenures may vary based on the specific deposit scheme.

- Recurring Deposits: Recurring deposits enable individuals to save regularly by depositing a fixed amount every month for a predefined duration. Shivalik offers recurring deposit accounts with competitive interest rates and flexible tenure options. These accounts are suitable for customers who want to save overtime systematically.

- Tax-Saver Deposits: Shivalik may offer tax-saver deposit schemes where customers can invest a specified amount for a fixed period and avail of tax benefits under the applicable tax laws of India. These deposits often come with a lock-in period and offer tax deductions on the invested amount.

→ Loans

- Personal Loans: Shivalik offers personal loans that can be used for various personal expenses such as medical emergencies, education, home renovation, travel, or any other legitimate personal need. These loans are typically unsecured and based on the borrower's creditworthiness and repayment capacity.

- Business Loans: Shivalik provides business loans to micro and small enterprises (MSEs) to support their working capital requirements, expansion plans, purchase of equipment or machinery, and other business-related needs. These loans can help MSEs grow and manage their businesses effectively.

- Microfinance Loans: Shivalik specializes in microfinance and offers small-ticket loans to individuals from low-income segments and micro-entrepreneurs. These loans are designed to promote financial inclusion and support income-generating activities such as small businesses, agriculture, and livestock rearing.

- Agriculture Loans: Shivalik offers agriculture loans to farmers and agriculturists for various agricultural activities such as crop cultivation, purchase of seeds and fertilizers, irrigation, farm equipment, and other agricultural needs. These loans aim to support the growth and development of the agricultural sector.

- Home Loans: Individuals and families can obtain house loans from Shivalik to buy or build residential homes. These loans enable borrowers to realise their dream of house ownership and offer flexible repayment options and low interest rates.

- Vehicle Loans: Shivalik offers vehicle loans to individuals for purchasing various types of vehicles, including cars, two-wheelers, and commercial vehicles. These loans provide financing options to customers who wish to own a vehicle or expand their transportation business.

- Gold Loans: Shivalik provides gold loans where customers can pledge their gold ornaments or assets as collateral and receive funds against it. Gold loans are an effective way to meet short-term financial needs quickly by leveraging the value of gold.

- Education Loans: Shivalik offers education loans to support students in pursuing higher education in India or abroad. These loans cover tuition fees, books, accommodation, and other related expenses, enabling students to fulfil their educational aspirations.

→ Debit card

- Classic Debit Card: Shivalik's Classic Debit Card is a standard card that allows customers to make purchases and withdraw cash from ATMs. It offers basic features and functionalities for day-to-day banking needs.

- Platinum Debit Card: Shivalik may offer a Platinum Debit Card that provides enhanced benefits and privileges compared to a classic card. It may include features such as higher daily transaction limits, special discounts, rewards programs, and additional security features.

- Business Debit Card: Shivalik provides Business Debit Cards specifically designed for business account holders. These cards offer features tailored to meet the banking and payment needs of businesses, including higher transaction limits, expense management tools, and detailed reporting.

- Contactless Debit Card: Shivalik may offer contactless debit cards that allow customers to make quick and secure payments by simply tapping the card on a contactless-enabled payment terminal. These cards use near-field communication (NFC) technology and provide a convenient and fast payment experience.

- Rupay Debit Card: Shivalik may issue Rupay Debit Cards, which are part of the domestic card payment network in India. Rupay cards are accepted at most ATMs and merchant establishments in the country and offer benefits and rewards specific to the Rupay network.

→ Digital Banking

- Internet Banking: Shivalik offers internet banking services, allowing customers to access and manage their accounts online through a secure web portal. Internet banking enables customers to perform various banking activities such as checking account balances, viewing transaction history, transferring funds between accounts, paying bills, and applying for additional services.

- Mobile Banking: Shivalik provides mobile banking services through dedicated mobile applications for smartphones and tablets. Mobile banking allows customers to perform banking transactions on the go, including checking account balances, transferring funds, making payments, and accessing various banking services through their mobile devices.

- Mobile Wallet: Shivalik may offer a mobile wallet service that enables customers to store funds digitally and make payments using their smartphones. Mobile wallets provide a convenient and secure way to make purchases, pay bills, and transfer money to other individuals or merchants.

- SMS Banking: Shivalik may provide SMS banking services, allowing customers to receive

- account-related information, transaction alerts, and notifications through text messages. This service enables customers to stay updated on their account activities and balances without the need for internet access.

- UPI (Unified Payments Interface): Shivalik may facilitate UPI-based payment services, allowing customers to make instant and secure payments using their smartphones. UPI enables customers to link their bank accounts and perform transactions through a single mobile application, making it convenient to send and receive money in real-time.

- Online Bill Payment: Shivalik's digital banking services may include online bill payment facilities. Customers can conveniently pay their utility bills, credit card bills, insurance premiums, and other bills directly through the bank's digital channels, saving time and effort.

- E-Statements: Shivalik may provide electronic statements (e-statements) to customers, replacing traditional paper statements. E-statements can be accessed securely through internet banking or mobile banking, allowing customers to view and download their account statements anytime.

1.4 Products & Services at Shivalik

The banking industry is a crucial sector within the broader financial services industry. It plays a vital role in facilitating economic activities by providing various financial products and services to individuals, businesses, and governments. The banking industry serves as a bridge between those who have surplus funds (depositors) and those who need funds (borrowers).

- Core Functions: Banks perform essential functions such as accepting deposits, granting loans, facilitating payments, and providing a safe place for customers to store their money. These functions are central to industry and contribute to the overall stability and functioning of the economy.

- Financial Intermediation: Banks act as financial intermediaries by collecting deposits from individuals and institutions and channeling these funds towards productive activities through loans and investments. This process of financial intermediation helps mobilize savings and allocate capital efficiently in the economy.

- Types of Banks: The banking industry consists of various types of banks, including commercial banks, investment banks, retail banks, central banks, and specialized banks (such as small finance banks and development banks). Each type of bank has specific roles, functions, and regulatory frameworks.

- Regulatory Framework: The banking industry operates under strict regulations and supervision by regulatory authorities. In most countries, central banks or financial regulatory bodies oversee banks to ensure their safety, stability, and compliance with regulatory standards. Regulatory frameworks aim to protect depositors, maintain financial stability, and promote fair and transparent banking practices.

- Technology and Digital Transformation: Banks are embracing technological advancements and digital transformation to enhance their services and improve customer experiences. Online banking, mobile banking, digital payments, and other digital innovations have become integral parts of the banking industry, providing customers with convenient and efficient banking options.

- Risk Management: Banks face various risks, including credit risk, market risk, liquidity risk, operational risk, and regulatory compliance risk. Risk management is a critical aspect of banking operations, involving robust frameworks and processes to identify, measure, monitor, and mitigate risks.

- International Banking: Banks engage in cross-border activities and international banking services, including foreign exchange transactions, trade finance, correspondent banking, and international fund transfers. International banking facilitates global trade, investment, and financial integration.

- Financial Inclusion: The banking industry plays a significant role in promoting financial inclusion by extending banking services to underserved and unbanked populations. Initiatives such as branch expansion, mobile banking, and microfinance aim to provide access to financial services and improve financial literacy.

1.5 About Regulating Body – RBI

The Reserve Bank of India (RBI) is the central bank of India and is responsible for the formulation and implementation of monetary policy in the country. Established on April 1, 1935, under the Reserve Bank of India Act, the RBI serves as the regulator and supervisor of the Indian banking system and the overall financial system. The RBI formulates and implements monetary policy with the objective of maintaining price stability while supporting economic growth. It determines the key policy rates, such as the repo rate and the reverse repo rate, which influence borrowing costs and liquidity conditions in the economy. The RBI is the only entity with the power to create and administer the Indian rupee. It administers currency reserves, makes ensuring there is an adequate quantity of coins and notes in circulation, and tries to keep the currency's security and integrity intact. In India, the RBI oversees and regulates banks and other financial organizations. Sets guidelines The RBI tracks and evaluates threats to the financial system's stability. By undertaking stress tests, establishing capital adequacy rules for banks, and developing frameworks for the resolution and recovery of stressed financial organizations, it tackles systemic concerns. To promote stability, transparency, and the protection of depositor interests, the FDIC issues guidelines and regulations for banks, carries out audits and inspections, and supervises their activities.

1.6 About NPCI

In India, the retail payment and settlement systems are run under the auspices of the National Payments Corporation of India (NPCI). In accordance with the terms of the Payment and Settlement Systems Act, 2007, it was founded in 2008 as a not-for-profit organisation. In order to advance digital transactions and financial inclusion in the nation, NPCI seeks to develop effective, secure, and easily accessible payment systems. Promoting Financial Inclusion: NPCI plays a vital role in promoting financial inclusion by providing accessible and cheap payment options to all areas of society. The organisation focuses on creating systems and products that fulfil underserved and unbanked people' needs. Interoperability and Standardization: The NPCI promotes standardisation and ensures interoperability between various payment systems to enable easy and secure transactions between several banks and payment service providers. This enables clients to transact effortlessly and efficiently across numerous platforms. Security and risk management are top priorities for NPCI when it comes to payment systems. To safeguard the integrity and confidentiality of transactions and customer data, it utilises strong security measures, fraud detection systems, and risk management frameworks. Research and Innovation: The NPCI encourages research and innovation in the payment sector. It fosters the development of new payment products, technologies, and business models through partnership with banks, fintech businesses, and other stakeholders. In order to comprehend changing payment trends and client preferences, NPCI also undertakes research and analysis. International Collaboration: To exchange knowledge, best practices, and technological solutions, NPCI works with international payment organizations and takes part in international forums. It works to improve cross-border payment systems and looks into chances for global expansion.

CHAPTER 2
VAPT/VA & RED TEAMING

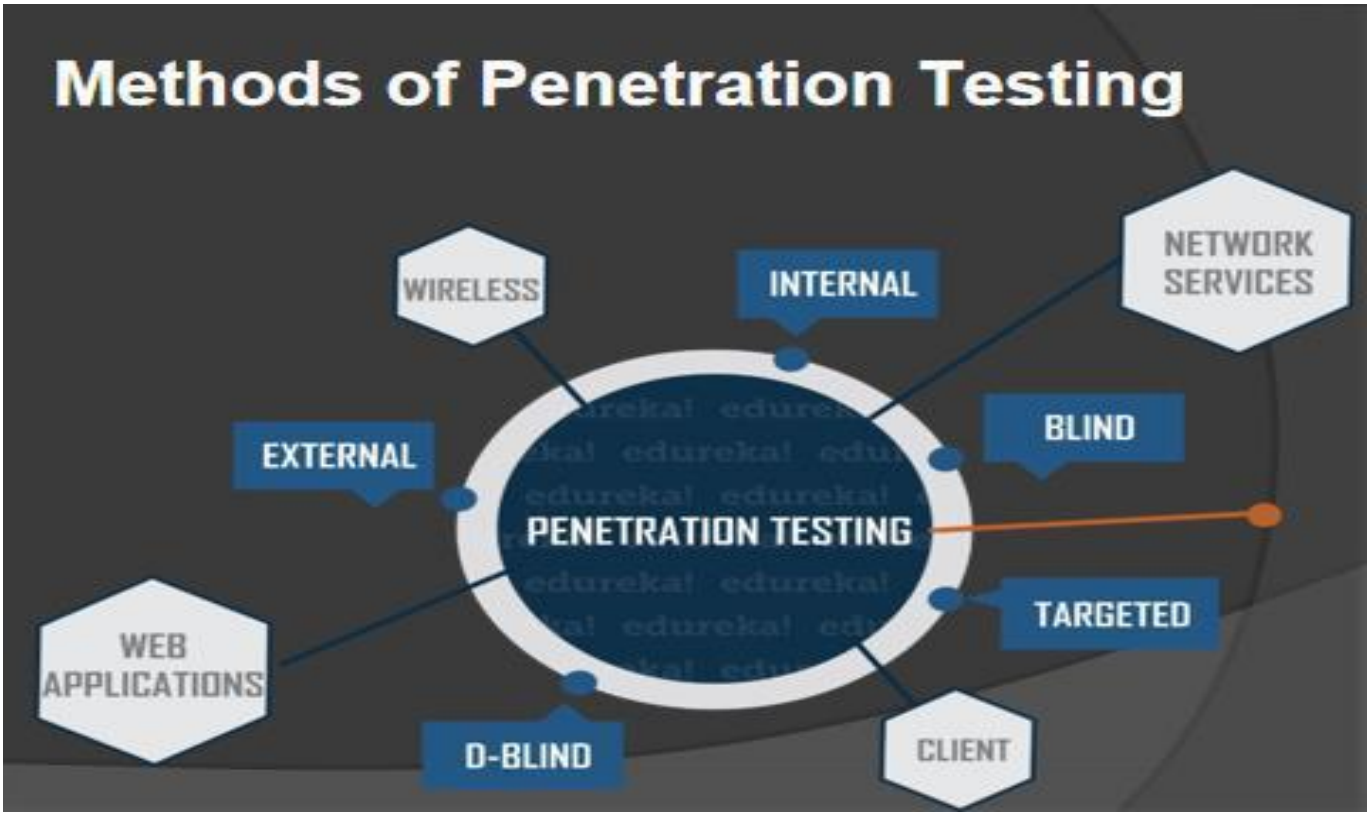
2.1 VAPT/VA

While VA stands for Vulnerability Assessment, VAPT stands for Vulnerability Assessment and Penetration Testing. Both VAPT and VA are security testing methods that are used to find holes and weak points in computer programmers, networks, and systems. They are frequently carried out in tandem to offer a thorough security assessment.

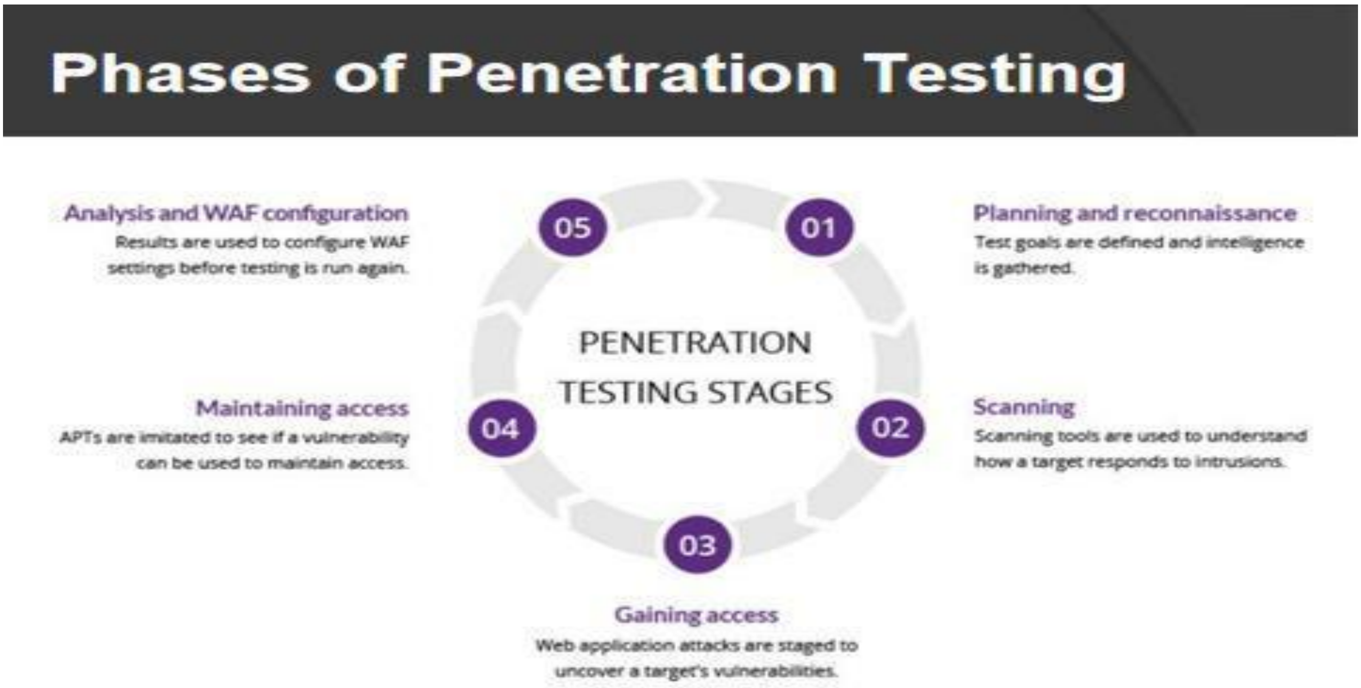
- Vulnerability Assessment (VA): The process of detecting and evaluating vulnerabilities in a system or network is known as vulnerability assessment (VA). It entails scanning the targeted system, network, or application to find security flaws, configuration errors, weak passwords, and other known vulnerabilities. The goal of VA is to give organizations a prioritized list of vulnerabilities and their possible effects so they may take the appropriate corrective measures.
- Penetration Testing (PT): Penetration testing (PT), also referred to as ethical hacking, replicates actual attacks to gauge how secure a system or network is. It entails actively exploiting flaws and making attempts to obtain unauthorized access to sensitive information or systems. The effectiveness of current security mechanisms is tested during penetration testing, which goes beyond vulnerability assessment by locating potential attack paths.

VAPT is a complete method that includes penetration testing and vulnerability assessment. The process begins with a vulnerability assessment to pinpoint areas of weakness, then it moves on to penetration testing to actively exploit flaws and gauge the consequences of successful attacks. VAPT helps prioritize remedial activities by giving a more thorough picture of an organization's security posture.

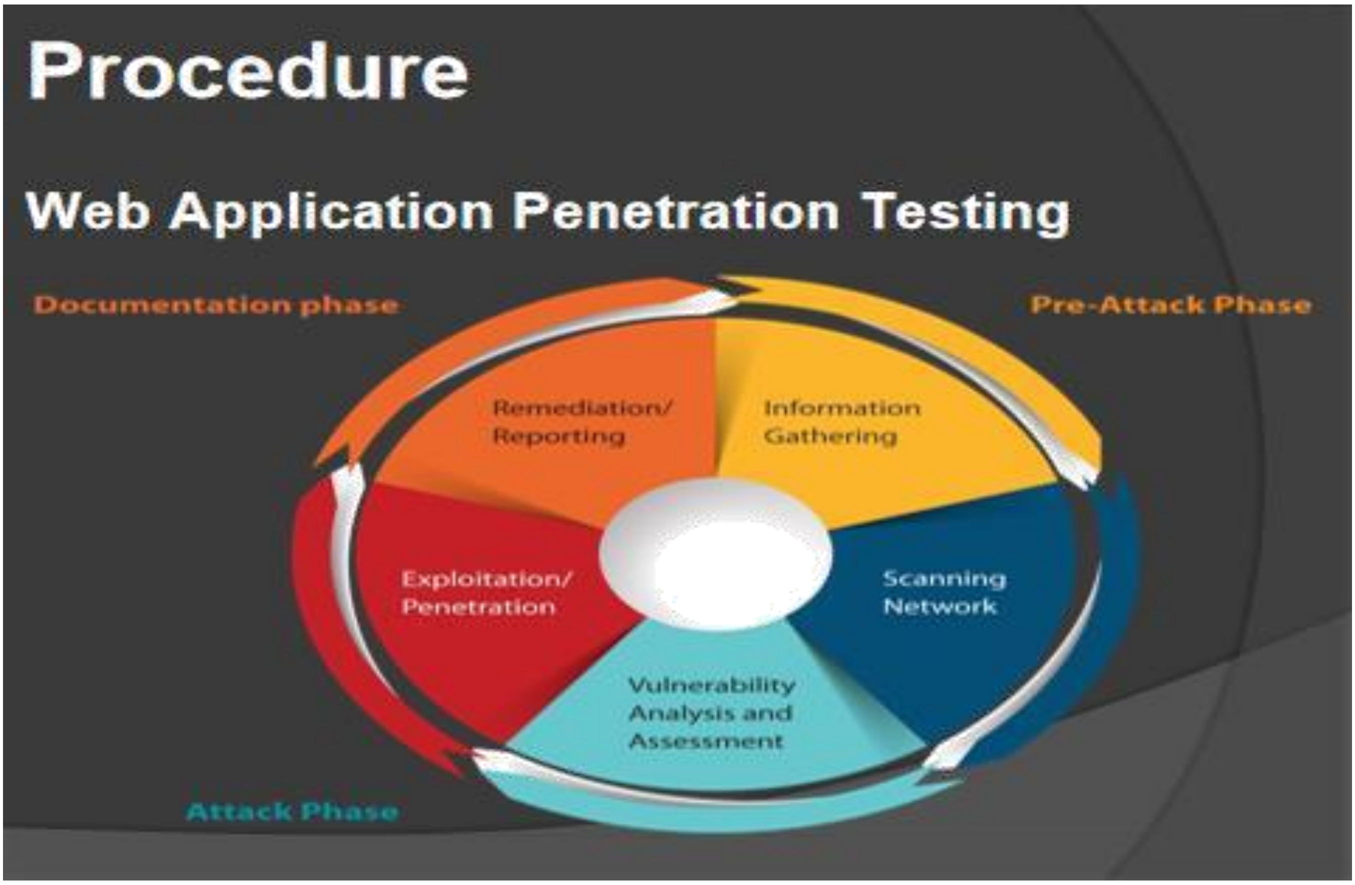
2.1.1 Penetration Testing



2.1.1 Methods of Penetration Testing


Phases of Penetration Testing
PENETRATION TESTING STAGES
01
Planning and reconnaissance
Test goals are defined and intelligence is gathered.
02
Scanning
Scanning tools are used to understand how a target responds to intrusions.
03
Gaining access
Web application attacks are staged to uncover a target's vulnerabilities.
04
Maintaining access
APTs are imitated to see if a vulnerability can be used to maintain access.
05
Analysis and WAF configuration
Results are used to configure WAF settings before testing is run again.

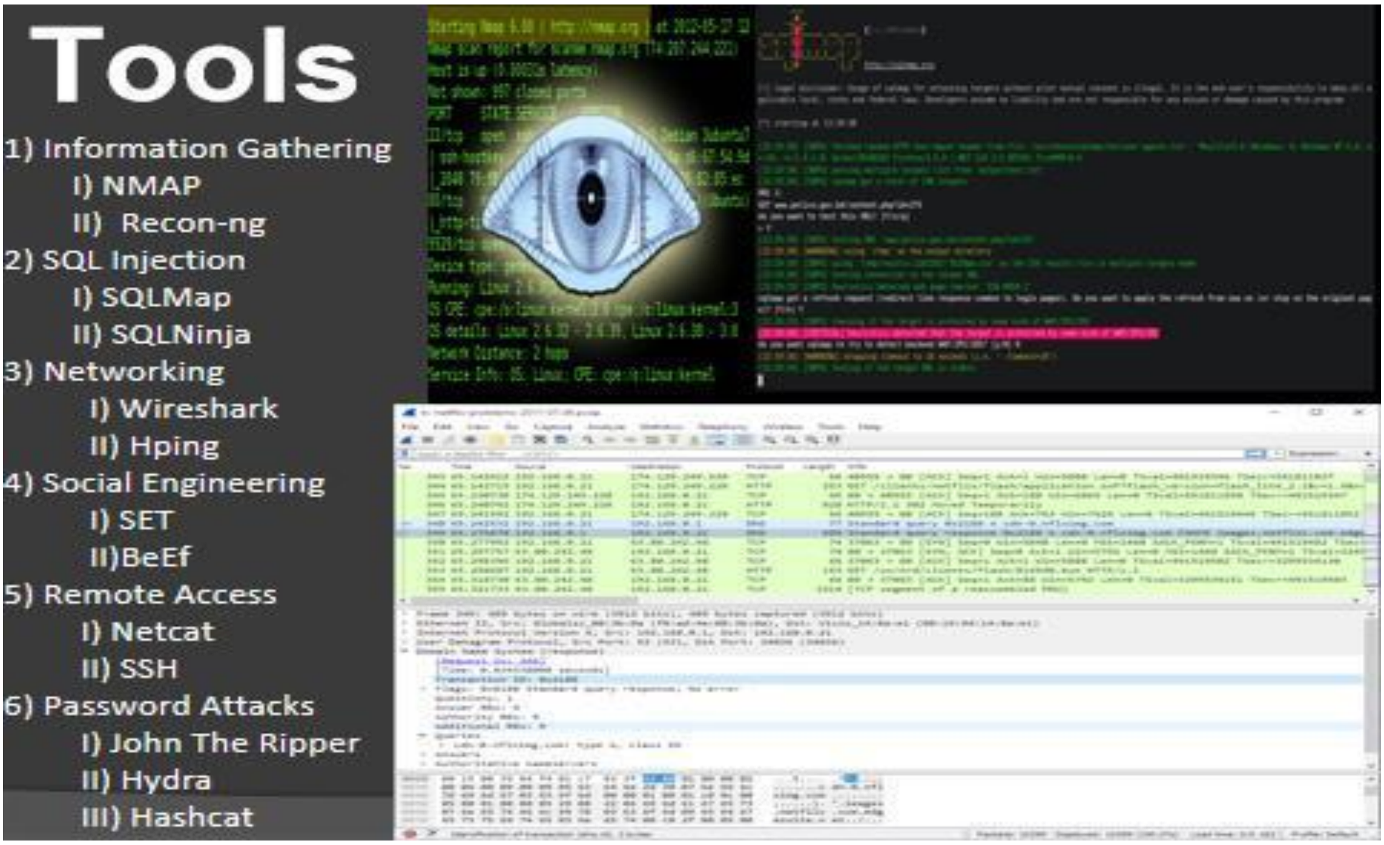
2.1.2 Phases of Penetration Testing.



Procedure

Web Application Penetration Testing

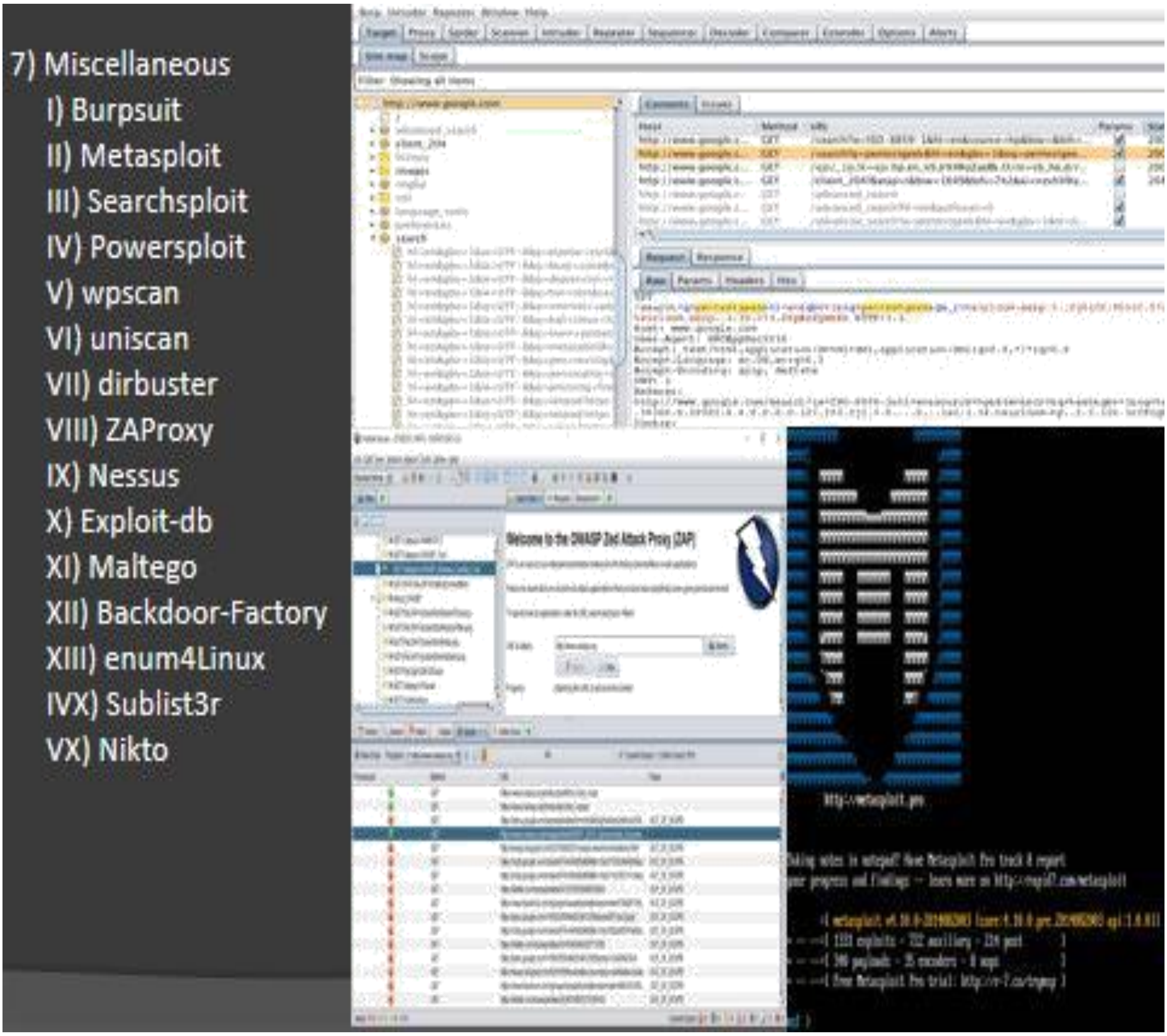
2.1.3 Procedure of Penetration Testing



Tools

1) Information Gathering
   I) NMAP
   II) Recon-ng
2) SQL Injection
   I) SQLMap
   II) SQLNinja
3) Networking
   I) Wireshark
   II) Hping
4) Social Engineering
   I) SET
   II)BeEf
5) Remote Access
   I) Netcat
   II) SSH
6) Password Attacks
   I) John The Ripper
   II) Hydra
   III) Hashcat

2.1.4 List of Tools



7) Miscellaneous

I) Burpsuit

II) Metasploit

III) Searchsploit

IV) Powersploit

V) wpscan

VI) uniscan

VII) dirbuster

VIII) ZAProxy

IX) Nessus

X) Exploit-db

XI) Maltego

XII) Backdoor-Factory

XIII) enum4Linux

IVX) Sublist3r

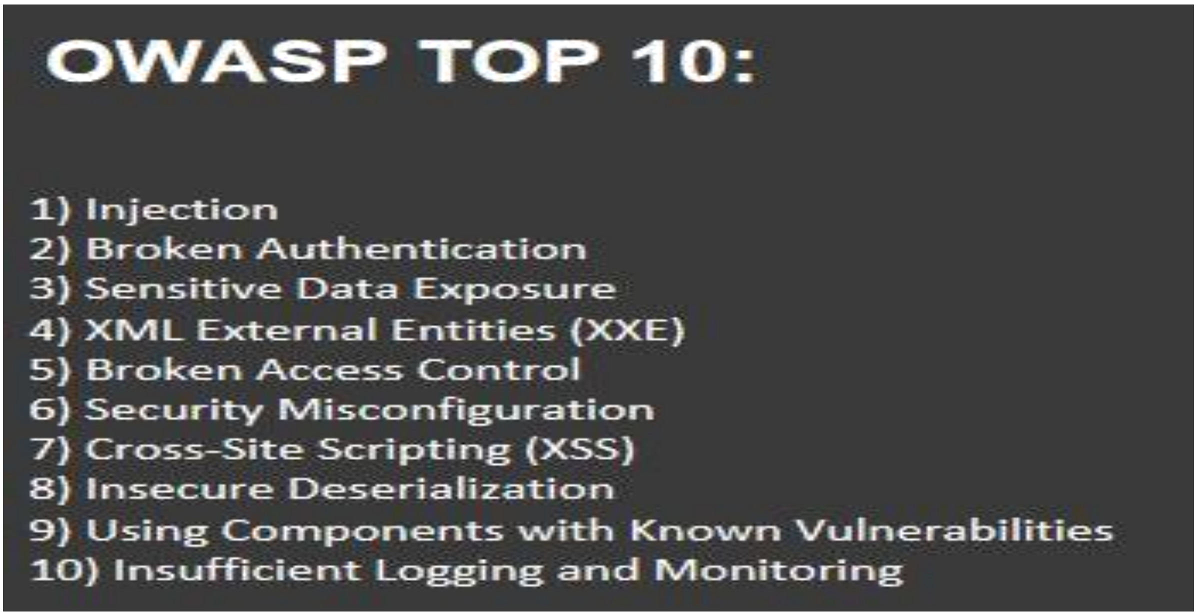
VX) Nikto

```
http://metasploit.pro

Taking notes in notepad? Have Metasploit Pro track & report
your progress and findings -- learn more on http://rapid7.com/metasploit

       =[ metasploit v4.10.0-[illegible] [core:4.10.0.pre.[illegible] api:1.0.0]]
+ -- --=[ [illegible] exploits - [illegible] auxiliary - [illegible] post        ]
+ -- --=[ [illegible] payloads - [illegible] encoders - [illegible] nops        ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
```

2.1.5 List of Tools



OWASP TOP 10:

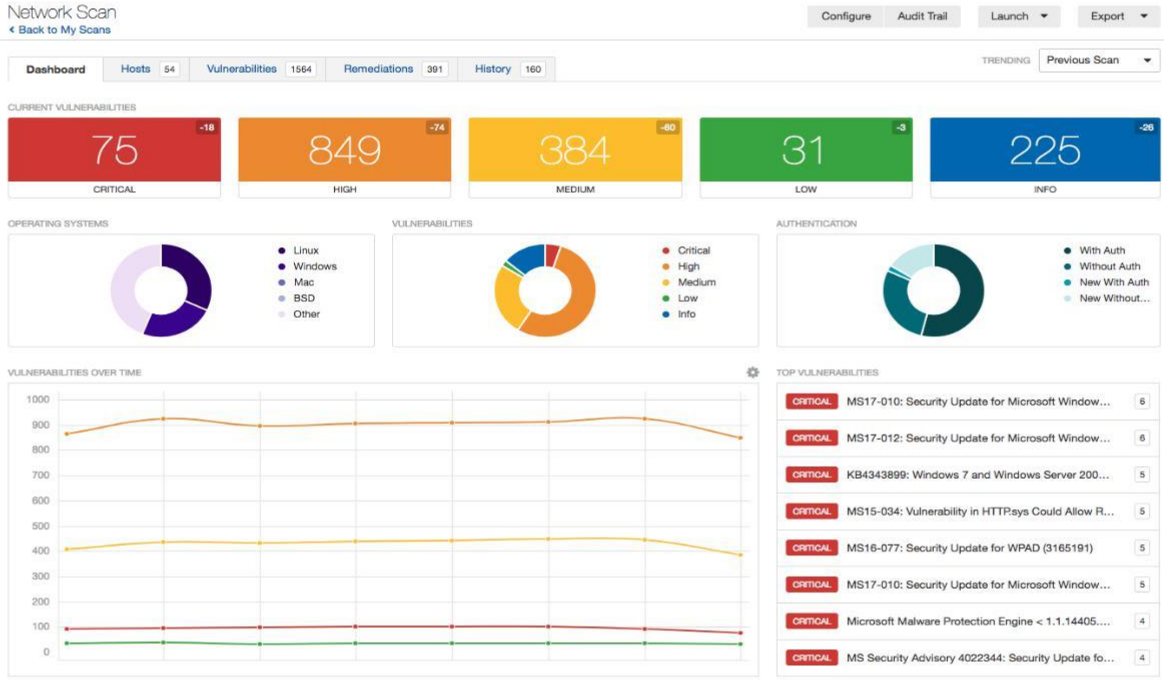
1) Injection
2) Broken Authentication
3) Sensitive Data Exposure
4) XML External Entities (XXE)
5) Broken Access Control
6) Security Misconfiguration
7) Cross-Site Scripting (XSS)
8) Insecure Deserialization
9) Using Components with Known Vulnerabilities
10) Insufficient Logging and Monitoring

2.1.6 OWASP TOP 10

2.1.2 VA Tools

VAPT (Vulnerability Assessment and Penetration Testing) is A vital procedure for locating and correcting security flaws in a system or network. There are numerous technologies available to support VAPT activities.

- Nessus: Nessus is a well-known vulnerability scanning tool that finds weaknesses in applications, systems, and networks. It delivers a variety of security tests and configuration audits, has extensive scanning capabilities.

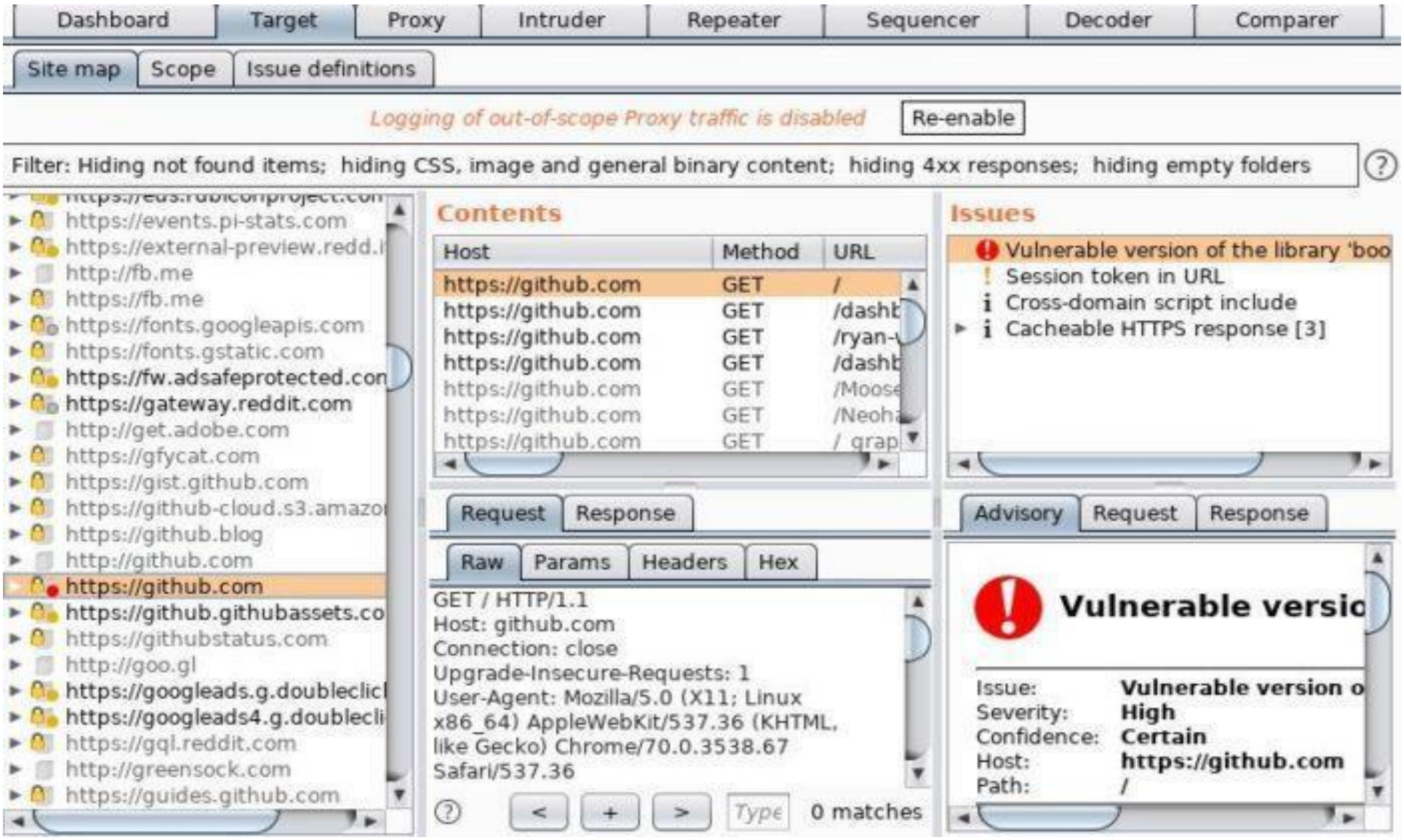


CRITICAL	MS17-010: Security Update for Microsoft Window...	6
CRITICAL	MS17-012: Security Update for Microsoft Window...	6
CRITICAL	KB4343899: Windows 7 and Windows Server 200...	5
CRITICAL	MS15-034: Vulnerability in HTTP.sys Could Allow R...	5
CRITICAL	MS16-077: Security Update for WPAD (3165191)	5
CRITICAL	MS17-010: Security Update for Microsoft Window...	5
CRITICAL	Microsoft Malware Protection Engine < 1.1.14405....	4
CRITICAL	MS Security Advisory 4022344: Security Update fo...	4

2.1.7 Network Scan.

- OpenVAS: OpenVAS (Open Vulnerability Assessment System) is an open-source vulnerability scanning tool that helps in identifying security issues in networks and applications. It offers a wide range of vulnerability tests and provides detailed reports.

- Burp Suite: Burp Suite is a powerful web application security testing tool used for both vulnerability assessment and penetration testing. It helps in identifying vulnerabilities such as SQL injection, cross-site scripting (XSS), and more. Burp Suite includes various modules for different security testing tasks.



Logging of out-of-scope Proxy traffic is disabled

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

https://eus.rubiconproject.com
https://events.pi-stats.com
https://external-preview.redd.i
http://fb.me
https://fb.me
https://fonts.googleapis.com
https://fonts.gstatic.com
https://fw.adsafeprotected.con
https://gateway.reddit.com
http://get.adobe.com
https://gfycat.com
https://gist.github.com
https://github-cloud.s3.amazo
https://github.blog
http://github.com
https://github.com
https://github.githubassets.co
https://githubstatus.com
http://goo.gl
https://googleads.g.doubleclic
https://googleads4.g.doublecli
https://gql.reddit.com
http://greensock.com
https://guides.github.com

Host	Method	URL
https://github.com	GET	/
https://github.com	GET	/dashb
https://github.com	GET	/ryan-\
https://github.com	GET	/dashb
https://github.com	GET	/Moose
https://github.com	GET	/Neoh
https://github.com	GET	/_grap

Vulnerable version of the library 'boo
Session token in URL
Cross-domain script include
Cacheable HTTPS response [3]

```
GET / HTTP/1.1
Host: github.com
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux
x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/70.0.3538.67
Safari/537.36
```

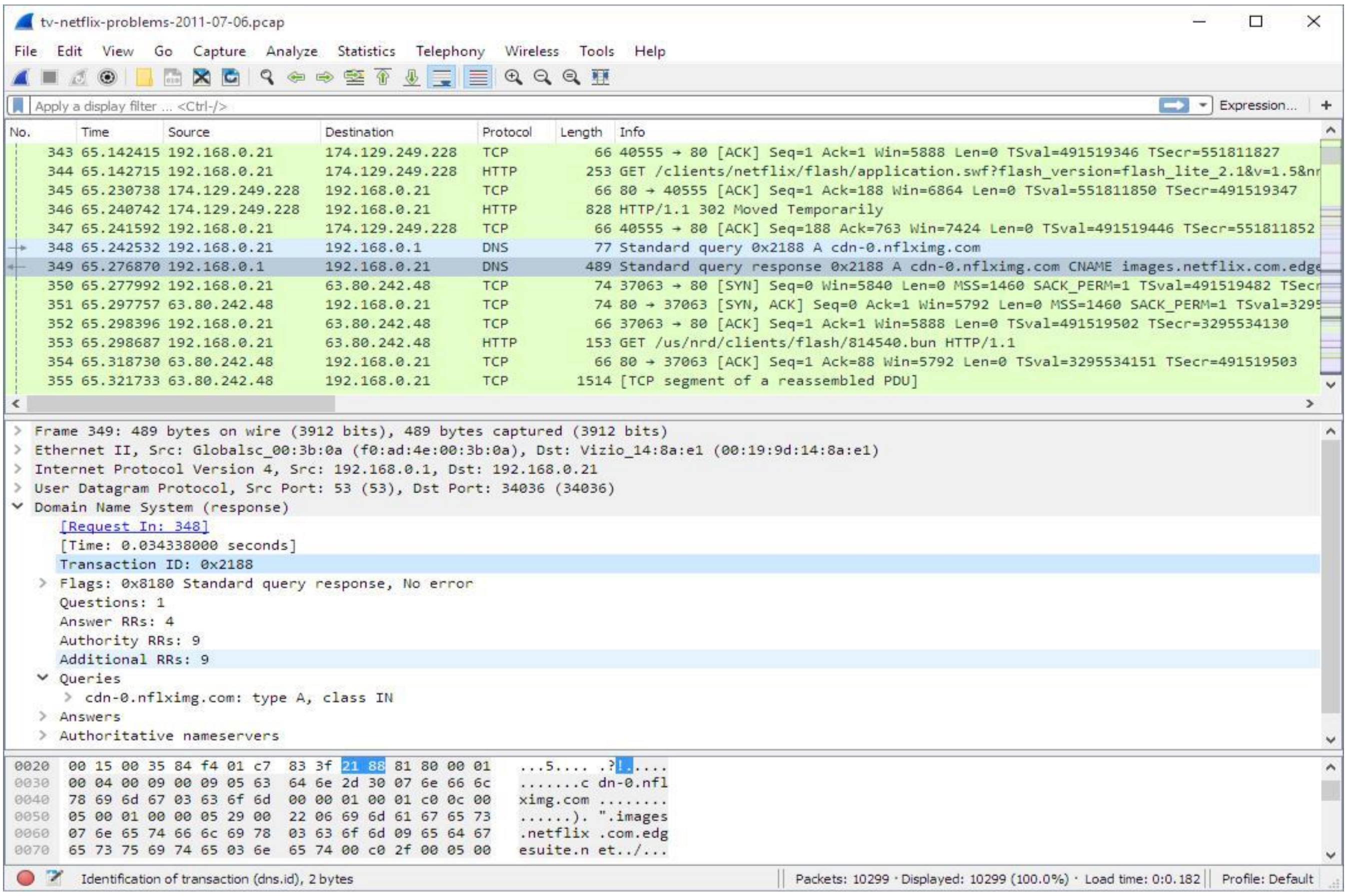
Vulnerable versio

Issue:	Vulnerable version o
Severity:	High
Confidence:	Certain
Host:	https://github.com
Path:	/

2.1.8 Burp Suite.

- Metasploit: A popular framework for penetration testing is Metasploit. It provides a wide range of tools, payloads, and exploits to model attacks and evaluate the security of networks and systems. Metasploit offers alternatives for penetration testing and assists in locating vulnerabilities.

- Wireshark: A network protocol analyser that records and examines network traffic is called Wireshark. It is beneficial for locating security flaws, examining network behaviour, and looking at network problems.



```
No.  Time      Source          Destination     Protocol Length Info
 343 65.142415 192.168.0.21    174.129.249.228 TCP        66 40555 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519346 TSecr=551811827
 344 65.142715 192.168.0.21    174.129.249.228 HTTP      253 GET /clients/netflix/flash/application.swf?flash_version=flash_lite_2.1&v=1.5&nr
 345 65.230738 174.129.249.228 192.168.0.21    TCP        66 80 → 40555 [ACK] Seq=1 Ack=188 Win=6864 Len=0 TSval=551811850 TSecr=491519347
 346 65.240742 174.129.249.228 192.168.0.21    HTTP      828 HTTP/1.1 302 Moved Temporarily
 347 65.241592 192.168.0.21    174.129.249.228 TCP        66 40555 → 80 [ACK] Seq=188 Ack=763 Win=7424 Len=0 TSval=491519446 TSecr=551811852
 348 65.242532 192.168.0.21    192.168.0.1     DNS        77 Standard query 0x2188 A cdn-0.nflximg.com
 349 65.276870 192.168.0.1     192.168.0.21    DNS       489 Standard query response 0x2188 A cdn-0.nflximg.com CNAME images.netflix.com.edge
 350 65.277992 192.168.0.21    63.80.242.48    TCP        74 37063 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=491519482 TSecr
 351 65.297757 63.80.242.48    192.168.0.21    TCP        74 80 → 37063 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=3295
 352 65.298396 192.168.0.21    63.80.242.48    TCP        66 37063 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519502 TSecr=3295534130
 353 65.298687 192.168.0.21    63.80.242.48    HTTP      153 GET /us/nrd/clients/flash/814540.bun HTTP/1.1
 354 65.318730 63.80.242.48    192.168.0.21    TCP        66 80 → 37063 [ACK] Seq=1 Ack=88 Win=5792 Len=0 TSval=3295534151 TSecr=491519503
 355 65.321733 63.80.242.48    192.168.0.21    TCP      1514 [TCP segment of a reassembled PDU]
```

```
> Frame 349: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits)
> Ethernet II, Src: Globalsc_00:3b:0a (f0:ad:4e:00:3b:0a), Dst: Vizio_14:8a:e1 (00:19:9d:14:8a:e1)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.21
> User Datagram Protocol, Src Port: 53 (53), Dst Port: 34036 (34036)
v Domain Name System (response)
    [Request In: 348]
    [Time: 0.034338000 seconds]
    Transaction ID: 0x2188
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 4
    Authority RRs: 9
    Additional RRs: 9
  v Queries
    > cdn-0.nflximg.com: type A, class IN
  > Answers
  > Authoritative nameservers
```

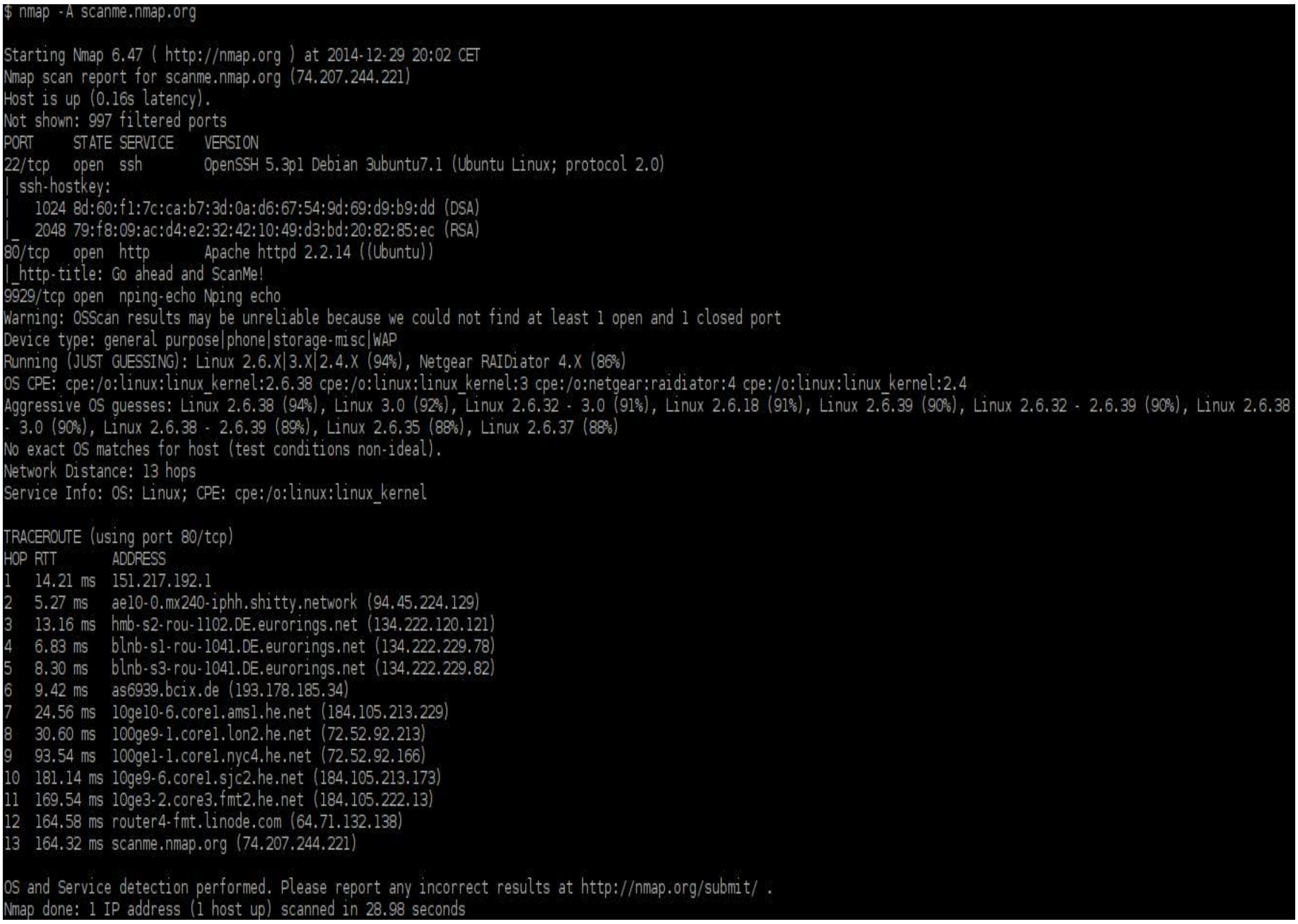
```
0020  00 15 00 35 84 f4 01 c7  83 3f 21 88 81 80 00 01   ...5.... .?!.....
0030  00 04 00 09 00 09 05 63  64 6e 2d 30 07 6e 66 6c   .......c dn-0.nfl
0040  78 69 6d 67 03 63 6f 6d  00 00 01 00 01 c0 0c 00   ximg.com ........
0050  05 00 01 00 00 05 29 00  22 06 69 6d 61 67 65 73   ......). ".images
0060  07 6e 65 74 66 6c 69 78  03 63 6f 6d 09 65 64 67   .netflix .com.edg
0070  65 73 75 69 74 65 03 6e  65 74 00 c0 2f 00 05 00   esuite.n et../...
```

```
Identification of transaction (dns.id), 2 bytes || Packets: 10299 · Displayed: 10299 (100.0%) · Load time: 0:0.182 || Profile: Default
```

2.1.9 Wireshark.

- Nikto: Nikto is an open-source web server scanner that identifies potential vulnerabilities in web servers and web applications. It performs tests for known security issues, misconfigurations, and outdated software versions.

- Nmap: Nmap (Network Mapper) is a versatile network scanning tool used for host discovery, port scanning, and service enumeration. It helps identify open ports, available services, and potential vulnerabilities in networked systems.



```
$ nmap -A scanme.nmap.org

Starting Nmap 6.47 ( http://nmap.org ) at 2014-12-29 20:02 CET
Nmap scan report for scanme.nmap.org (74.207.244.221)
Host is up (0.16s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 5.3p1 Debian 3ubuntu7.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 8d:60:f1:7c:ca:b7:3d:0a:d6:67:54:9d:69:d9:b9:dd (DSA)
|_  2048 79:f8:09:ac:d4:e2:32:42:10:49:d3:bd:20:82:85:ec (RSA)
80/tcp   open  http       Apache httpd 2.2.14 ((Ubuntu))
|_http-title: Go ahead and ScanMe!
9929/tcp open  nping-echo Nping echo
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|phone|storage-misc|WAP
Running (JUST GUESSING): Linux 2.6.X|3.X|2.4.X (94%), Netgear RAIDiator 4.X (86%)
OS CPE: cpe:/o:linux:linux_kernel:2.6.38 cpe:/o:linux:linux_kernel:3 cpe:/o:netgear:raidiator:4 cpe:/o:linux:linux_kernel:2.4
Aggressive OS guesses: Linux 2.6.38 (94%), Linux 3.0 (92%), Linux 2.6.32 - 3.0 (91%), Linux 2.6.18 (91%), Linux 2.6.39 (90%), Linux 2.6.32 - 2.6.39 (90%), Linux 2.6.38
- 3.0 (90%), Linux 2.6.38 - 2.6.39 (89%), Linux 2.6.35 (88%), Linux 2.6.37 (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 13 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   14.21 ms  151.217.192.1
2   5.27 ms   ae10-0.mx240-iphh.shitty.network (94.45.224.129)
3   13.16 ms  hmb-s2-rou-1102.DE.eurorings.net (134.222.120.121)
4   6.83 ms   blnb-s1-rou-1041.DE.eurorings.net (134.222.229.78)
5   8.30 ms   blnb-s3-rou-1041.DE.eurorings.net (134.222.229.82)
6   9.42 ms   as6939.bcix.de (193.178.185.34)
7   24.56 ms  10ge10-6.core1.ams1.he.net (184.105.213.229)
8   30.60 ms  100ge9-1.core1.lon2.he.net (72.52.92.213)
9   93.54 ms  100ge1-1.core1.nyc4.he.net (72.52.92.166)
10  181.14 ms 10ge9-6.core1.sjc2.he.net (184.105.213.173)
11  169.54 ms 10ge3-2.core3.fmt2.he.net (184.105.222.13)
12  164.58 ms router4-fmt.linode.com (64.71.132.138)
13  164.32 ms scanme.nmap.org (74.207.244.221)

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.98 seconds
```

2.1.10 Nmap

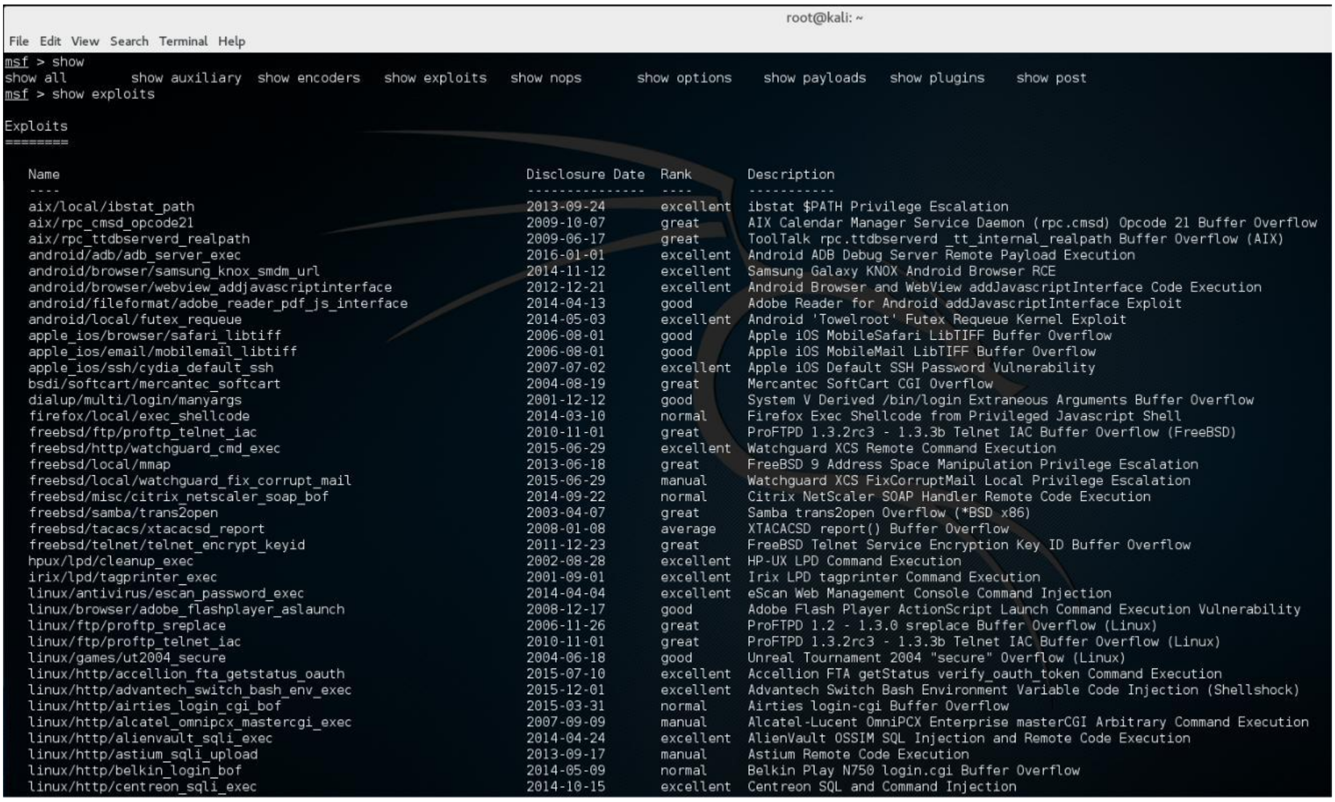
2.2 Red Teaming

Red Teaming, on the other hand, is a more comprehensive idea that extends beyond VAPT. In order to evaluate an organization's total security readiness, it requires modelling real-world attacks and scenarios. In-depth Red Team exercises, which replicate sophisticated adversaries aiming to target an organization's people, processes, and technology, often require a team of skilled professionals. By testing presumptions and identifying blind spots, red teaming seeks to detect vulnerabilities, test defensive capabilities, and enhance overall security effectiveness.

2.2.1 Red Teaming Tools

A rigorous and proactive approach to testing and evaluating the security of organisations, networks, and systems is red teaming. It mimics actual attacks to identify flaws and vulnerabilities. Red teaming activities include more than just using tools, however some tools might be helpful. Cobalt Strike: Cobalt Strike is a popular commercial penetration testing tool used for red teaming. It provides a wide range of capabilities, including spear phishing, social engineering, command and control (C2), and post-exploitation techniques.

- Metasploit: Metasploit, mentioned earlier as a penetration testing tool, is also utilized in red teaming engagements. It offers a vast collection of exploits, payloads, and modules for various stages of an attack.



```
msf > show
show all        show auxiliary  show encoders   show exploits   show nops       show options    show payloads   show plugins    show post
msf > show exploits

Exploits
========

   Name                                                           Disclosure Date  Rank       Description
   ----                                                           ---------------  ----       -----------
   aix/local/ibstat_path                                          2013-09-24       excellent  ibstat $PATH Privilege Escalation
   aix/rpc_cmsd_opcode21                                          2009-10-07       great      AIX Calendar Manager Service Daemon (rpc.cmsd) Opcode 21 Buffer Overflow
   aix/rpc_ttdbserverd_realpath                                   2009-06-17       great      ToolTalk rpc.ttdbserverd _tt_internal_realpath Buffer Overflow (AIX)
   android/adb/adb_server_exec                                    2016-01-01       excellent  Android ADB Debug Server Remote Payload Execution
   android/browser/samsung_knox_smdm_url                          2014-11-12       excellent  Samsung Galaxy KNOX Android Browser RCE
   android/browser/webview_addjavascriptinterface                 2012-12-21       excellent  Android Browser and WebView addJavascriptInterface Code Execution
   android/fileformat/adobe_reader_pdf_js_interface               2014-04-13       good       Adobe Reader for Android addJavascriptInterface Exploit
   android/local/futex_requeue                                    2014-05-03       excellent  Android 'Towelroot' Futex Requeue Kernel Exploit
   apple_ios/browser/safari_libtiff                               2006-08-01       good       Apple iOS MobileSafari LibTIFF Buffer Overflow
   apple_ios/email/mobilemail_libtiff                             2006-08-01       good       Apple iOS MobileMail LibTIFF Buffer Overflow
   apple_ios/ssh/cydia_default_ssh                                2007-07-02       excellent  Apple iOS Default SSH Password Vulnerability
   bsdi/softcart/mercantec_softcart                               2004-08-19       great      Mercantec SoftCart CGI Overflow
   dialup/multi/login/manyargs                                    2001-12-12       good       System V Derived /bin/login Extraneous Arguments Buffer Overflow
   firefox/local/exec_shellcode                                   2014-03-10       normal     Firefox Exec Shellcode from Privileged Javascript Shell
   freebsd/ftp/proftp_telnet_iac                                  2010-11-01       great      ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)
   freebsd/http/watchguard_cmd_exec                               2015-06-29       excellent  Watchguard XCS Remote Command Execution
   freebsd/local/mmap                                             2013-06-18       great      FreeBSD 9 Address Space Manipulation Privilege Escalation
   freebsd/local/watchguard_fix_corrupt_mail                      2015-06-29       manual     Watchguard XCS FixCorruptMail Local Privilege Escalation
   freebsd/misc/citrix_netscaler_soap_bof                         2014-09-22       normal     Citrix NetScaler SOAP Handler Remote Code Execution
   freebsd/samba/trans2open                                       2003-04-07       great      Samba trans2open Overflow (*BSD x86)
   freebsd/tacacs/xtacacsd_report                                 2008-01-08       average    XTACACSD report() Buffer Overflow
   freebsd/telnet/telnet_encrypt_keyid                            2011-12-23       great      FreeBSD Telnet Service Encryption Key ID Buffer Overflow
   hpux/lpd/cleanup_exec                                          2002-08-28       excellent  HP-UX LPD Command Execution
   irix/lpd/tagprinter_exec                                       2001-09-01       excellent  Irix LPD tagprinter Command Execution
   linux/antivirus/escan_password_exec                            2014-04-04       excellent  eScan Web Management Console Command Injection
   linux/browser/adobe_flashplayer_aslaunch                       2008-12-17       good       Adobe Flash Player ActionScript Launch Command Execution Vulnerability
   linux/ftp/proftp_sreplace                                      2006-11-26       great      ProFTPD 1.2 - 1.3.0 sreplace Buffer Overflow (Linux)
   linux/ftp/proftp_telnet_iac                                    2010-11-01       great      ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (Linux)
   linux/games/ut2004_secure                                      2004-06-18       good       Unreal Tournament 2004 "secure" Overflow (Linux)
   linux/http/accellion_fta_getstatus_oauth                       2015-07-10       excellent  Accellion FTA getStatus verify_oauth_token Command Execution
   linux/http/advantech_switch_bash_env_exec                      2015-12-01       excellent  Advantech Switch Bash Environment Variable Code Injection (Shellshock)
   linux/http/airties_login_cgi_bof                               2015-03-31       normal     Airties login-cgi Buffer Overflow
   linux/http/alcatel_omnipcx_mastercgi_exec                      2007-09-09       manual     Alcatel-Lucent OmniPCX Enterprise masterCGI Arbitrary Command Execution
   linux/http/alienvault_sqli_exec                                2014-04-24       excellent  AlienVault OSSIM SQL Injection and Remote Code Execution
   linux/http/astium_sqli_upload                                  2013-09-17       manual     Astium Remote Code Execution
   linux/http/belkin_login_bof                                    2014-05-09       normal     Belkin Play N750 login.cgi Buffer Overflow
   linux/http/centreon_sqli_exec                                  2014-10-15       excellent  Centreon SQL and Command Injection
```

2.2.1 Metasploit

- Empire: Empire is an open-source post-exploitation framework that focuses on offensive PowerShell capabilities. It enables red teamers to execute PowerShell-based attacks and maintain persistence within a compromised system.

- PowerSploit: PowerSploit is a collection of PowerShell scripts designed for offensive purposes. It provides red teamers with a wide range of capabilities, including privilege escalation, credential theft, and lateral movement within a network.

- Mimikatz: Powerful tools like Mimikatz are utilised for post-exploitation tasks, including credential collection and password dumping. Red team members can use it to retrieve passwords, hashes, and other authentication information from infected systems.

- BeEF: A red teaming tool called BeEF (Browser Exploitation Framework) is made exclusively for aiming at web browsers. Red team members can use it to carry out a number of client-side assaults, including as cross-site scripting (XSS), HTML injection, and browser-based phishing.

- BloodHound: An Active Directory (AD) reconnaissance and mapping tool is called BloodHound. It aids red team members in comprehending the network architecture, recognising trust relationships, and figuring out possible attack avenues in an AD system.

2.3 Review of Daily Alerts & Advisory

Reviewing daily alerts and advisories is Maintaining a solid security posture and remaining updated about potential threats and vulnerabilities requires continuous review of alerts and advisories. For the purpose of keeping a pro-active security posture, it is essential to evaluate daily warnings and advisories. It enables businesses to stay up to date on the changing threat landscape, quickly resolve vulnerabilities and install updates, and quickly detect and respond to possible security issues. To enable efficient monitoring and warning response, this task must be assigned to qualified employees or dedicated security teams.

- Daily Alert Review: Security systems, such as intrusion detection systems, firewalls, and antivirus solutions, generate alerts when they detect suspicious activities or potential security incidents. These alerts need to be reviewed daily to identify any actual threats or signs of compromise.

- Triaging and Prioritization: Not all alerts are equal in terms of severity or relevance. The review process involves triaging and prioritizing alerts based on their potential impact, the affected systems or assets, and the likelihood of an actual security incident. This helps focus resources on the most critical issues.

- Incident Response: If an alert indicates a potential security incident, it triggers an incident response process. The appropriate personnel should be notified, and the incident should be investigated and addressed according to established protocols. This may involve isolating affected systems, gathering evidence, and mitigating the impact of the incident.

- Patch and Vulnerability Management: Daily alert review also involves monitoring for security advisories and updates from software vendors, security organizations, and other trusted sources. These advisories may highlight newly discovered vulnerabilities or provide patches and mitigations for known issues. Timely application of patches and proactive vulnerability management helps protect against known vulnerabilities.

- Threat Intelligence: Daily alert review should include monitoring threat intelligence feeds and advisories. These sources provide information about emerging threats, attack trends, and indicators of compromise (IOCs). Staying updated with threat intelligence allows organizations to proactively adapt their security controls and defenses.

2.4 Review of SOPs & Policies

Reviewing Standard Operating Procedures (SOPs) and policies is a crucial procedure for ensuring that an organization's security measures, processes, and standards comply with industry best practices and legal requirements is reviewing its Standard Operating Procedures (SOPs) and policies. To keep an organization's security structure functional and up to date, regular evaluation of SOPs and policies is essential. It assists in ensuring regulatory compliance, reducing risks, and encouraging a security-conscious workplace culture.

- Scope and Coverage: Start by defining the scope of the review, which may include all security-related SOPs and policies or focus on specific areas such as access control, incident response, or data protection. Ensure that the review encompasses all relevant policies and SOPs to provide a comprehensive assessment.

- Compliance and Regulatory Requirements: Evaluate whether the existing policies and SOPs meet the compliance standards and regulatory requirements relevant to the organization's industry. This includes assessing alignment with regulations such as GDPR, HIPAA, PCI DSS, or industry-specific frameworks like NIST, ISO 27001, or CIS Controls.

- Currency and Relevance: Policies and SOPs should be up to date and reflect the current security landscape, technologies, and business practices. Review them for relevance and applicability to the organization's current operations, systems, and processes. Identify any outdated or obsolete policies that need to be revised or removed.

- Consistency and Coherence: Ensure that policies and SOPs are consistent with each other and do not conflict. Look for any gaps or overlaps in coverage, and address inconsistencies to maintain a coherent and effective security framework. This helps prevent confusion among employees and ensures a unified approach to security.

- Clarity and Accessibility: Policies and SOPs should be clearly written, using concise and unambiguous language. Evaluate the readability and understandability of the documents. Additionally, assess their accessibility to employees, ensuring they are readily available and easily accessible through appropriate channels (e.g., intranet, document management systems).

- Employee Awareness and Training: Evaluate whether policies and SOPs are effectively communicated to employees and if there are mechanisms in place to ensure their understanding. Regular training and awareness programs should be conducted to educate employees about the policies and SOPs, emphasizing their importance and providing guidance on compliance.

- Incident Response and Escalation: Review the incident response procedures outlined in the policies and SOPs. Assess their clarity, effectiveness, and alignment with industry incident response best practices. Verify that escalation paths, roles, and responsibilities are clearly defined, ensuring a coordinated and efficient response to security incidents.

- Continuous Improvement: Establish a mechanism for regular review and update of policies and SOPs to accommodate changes in the security landscape, regulatory requirements, and organizational needs. Encourage feedback from relevant stakeholders and consider incorporating industry best practices to enhance security measures.

2.5 Vendor Coordination

Vendor coordination plays a significant role in effectively managing alerts and VAPT (Vulnerability Assessment and Penetration Testing) processes. Effective vendor coordination helps leverage external expertise and resources to enhance your organization's security posture. By establishing clear roles, responsibilities, and communication channels, you can ensure a smooth collaboration and optimize the effectiveness of alert management and VAPT efforts. You can promote effective collaboration and maximize the success of alert management and VAPT activities by clearly defining roles, responsibilities, and communication channels.

- Selecting Reliable Vendors: Choose reputable vendors with expertise in security services, such as managed detection and response, incident response, and VAPT. Consider their track record, industry reputation, and the comprehensiveness of their services.

- Clearly Defined Roles and Responsibilities: Establish clear roles and responsibilities for both your organization and the vendor. Clearly outline the expectations, deliverables, and timelines for alert management and VAPT activities. This ensures a mutual understanding of each party's responsibilities.

- Service Level Agreements (SLAs): Define SLAs with the vendor to establish agreed-upon response times for addressing alerts and conducting VAPT activities. SLAs should include response and resolution timeframes, communication protocols, escalation procedures, and reporting requirements.

- Incident Escalation and Communication: Establish escalation paths and communication channels between your organization and the vendor. Define procedures for escalating critical incidents, security breaches, or urgent vulnerabilities identified during VAPT. This enables prompt communication and collaboration during security incidents.

- Regular Meetings and Reporting: Schedule regular meetings with the vendor to discuss ongoing alert management, VAPT findings, progress, and any necessary actions. Review reports provided by the vendor and seek clarifications or additional information as needed.

- Collaborative Incident Response: In the event of a security incident or breach, work closely with the vendor to coordinate incident response efforts. This may involve joint investigations, information sharing, and collaboration on remediation actions to mitigate the impact and prevent future incidents.

- Continuous Improvement: Encourage a feedback loop with the vendor to ensure continuous improvement of their services. Provide constructive feedback on the quality and timeliness of their response to alerts, the effectiveness of VAPT activities, and suggestions for enhancing collaboration and outcomes.

- Knowledge Transfer and Training: Request knowledge transfer sessions from the vendor to help your internal teams understand and interpret the alerts generated by their systems. Additionally, leverage vendor expertise for training sessions or workshops to enhance your organization's knowledge and capabilities in handling security incidents and VAPT activities.

2.5 OWASP TOP 10

The top 10 web application security vulnerabilities are listed in the OWASP (Open Web Application Security Project) Top 10 by a team of international security professionals. Every few years, the list is updated to reflect changes in the threat environment.

The OWASP Top 10 2021 is:

1. Injection: When untrusted data is provided to an interpreter as part of a command or query, injection flaws, such as SQL, NoSQL, OS, and LDAP injection, take place. The interpreter is tricked into executing unauthorised commands or accessing unauthorised data by the attacker's malicious input.
2. Defective Authentication: When authentication and session management are improperly carried out, attackers can access user accounts or session data and use it to steal confidential information or carry out unauthorised actions.Sensitive Data Exposure: Sensitive Data Exposure occurs when an application does not properly protect sensitive data, such as credit card numbers or personal information. Attackers can exploit this to steal sensitive data.
3. XML External Entities (XXE): When an application parses XML input from untrusted sources, XXE vulnerabilities can occur. These flaws can provide attackers access to sensitive information or even grant them remote code execution or denial-of-service attacks.
4. Broken Access Control: A programme is considered to have violated access control if it allows unauthorised access to resources or functions. Attackers may exploit this to gain access to the accounts of other users, steal data, or commit unlawful acts.
5. Security Misconfiguration: Security When a software is improperly configured to protect against common security risks, misconfiguration occurs. This may involve unneeded services, unsecured files, or insecure default settings.
6. Cross-Site Scripting (XSS): Cross-Site Scripting occurs when an attacker puts malicious code onto a website that is seen by other users. This gives the attacker the ability to steal sensitive data, commit unlawful acts, or compromise the accounts of other users.

7. Insecure Deserialization: Insecure deserialization occurs when an application deserializes untrusted data without sufficient validation. Attackers can use this to execute arbitrary code or launch different kinds of attacks.
8. Applications: Use third-party components that are known to be vulnerable, including libraries or frameworks. If these components have known vulnerabilities, attackers may use them to compromise user data or gain access to the programme.
9. Inadequate logging and monitoring: It is difficult to recognise and respond to security occurrences when recording and monitoring are inadequate. Over time, attackers can use this to maintain control over a compromised machine or steal crucial data.

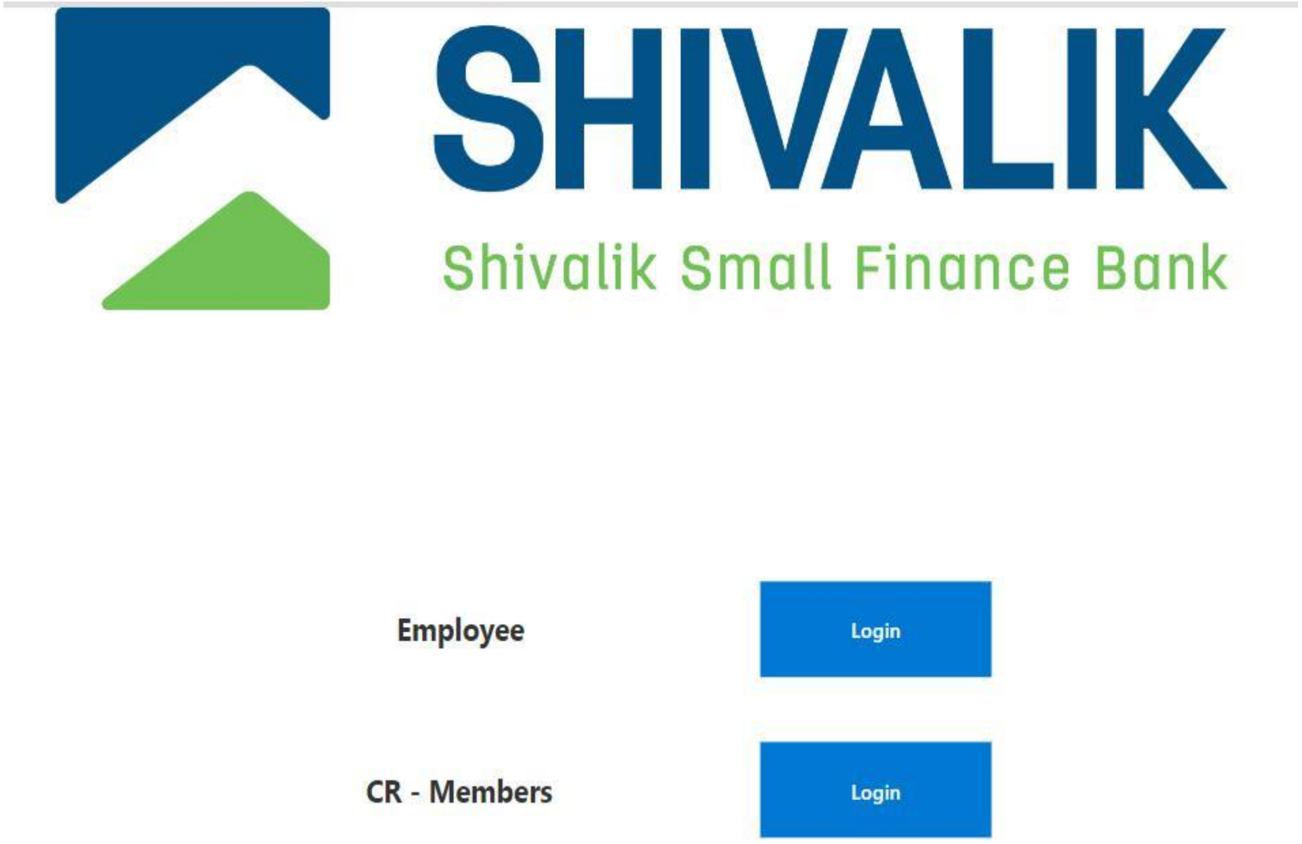
It is crucial to keep in mind that this list is not complete and that there can be other vulnerabilities unique to your application or environment. The OWASP Top 10 is merely a place to start when developing secure online applications; it is not a comprehensive security programme.

CHAPTER 3

Technology Change Request Form Using Power App

3.1 Introduction to Power App

Microsoft's Power Apps low-code development platform enables customers to create unique business applications without having to have a deep understanding of coding. With simple visual tools and pre-made templates, it makes it possible to create mobile and web-based apps. Power Apps is a user-friendly platform for creating unique business apps, allowing businesses to quickly construct solutions catered to their unique needs. Power Apps enables users to create applications that improve productivity, accelerate digital transformation, and optimise business operations thanks to its low-code approach, data integration capability, and wide range of connectivity possibilities. Low-Code Development: Power Apps frees users from the requirement for traditional coding by allowing them to create applications using a visual interface and drag-and-drop components. It offers a variety of pre-built connectors, controls, and functions, opening up app development to a larger audience. Connectivity and Integration: Power Apps readily interface with other Microsoft products including Dynamics 365, SharePoint, and Office 365. Additionally, it provides connections to a number of external systems, databases, and APIs, enabling you to combine data from different sources and build networked applications. Web and Mobile Applications: Power Apps make it possible to build both web-based and mobile applications. Users can access and engage with apps on smartphones, tablets, and computers thanks to responsive design, which ensures that apps function flawlessly across various devices and screen sizes. Power Apps' integration with Microsoft's Common Data Service (CDS) offers a uniform data platform for the storage and management of application data. You can connect to multiple data sources, including as on-premises databases and cloud services, and create apps that interact with and change that data. AI Capabilities: By integrating with Azure AI services, Power Apps provide built-in artificial intelligence (AI) capabilities. This makes it possible for you to add AI features to your applications that will improve their functionality and user interfaces, such as picture recognition, natural language processing, and predictive analytics. Power Apps offers a variety of pre-built templates and sample apps that may be modified to meet unique company requirements. The Power Apps marketplace also provides a large range of pre-built controls, solutions, and components that have been contributed by the Power Apps community. Collaboration and Sharing: Within a company, Power Apps facilitate application sharing and collaboration. You may enable collaboration on app development projects, create rights and responsibilities, and distribute apps with users or groups. Power Apps' integration with Microsoft's security and governance frameworks enables businesses to impose rules for access controls, data protection, and policies. It offers solutions for data encryption, authentication, and adherence to legal requirements.



3.1 Welcome to Shivalik small finance bank.

3.2 Login Page

You can use the methods below to make a login page for administrators and staff members:

- Design the Login Page: Make the login page aesthetically pleasing and user-friendly. Include a "Login" button and input fields for the user name and password. Additionally, you can include company logos or branding components on the website.

- User Authentication: Put in place a user authentication system to check the login information entered by administrators and employees. Several techniques, including username and password authentication, single sign-on (SSO), and interaction with an identity provider like

Active Directory or OAuth, can be used to do this.

- Secure Password Storage: Ensure that passwords are securely stored in your system. Implement password hashing techniques, such as crypt or Argon2, to protect user credentials from unauthorized access.

- Role-Based Access Control: Differentiate between employees and administrators based on their roles. Assign specific permissions and access levels to each role. This ensures that employees have limited access to certain functionalities, while administrators have elevated privileges.

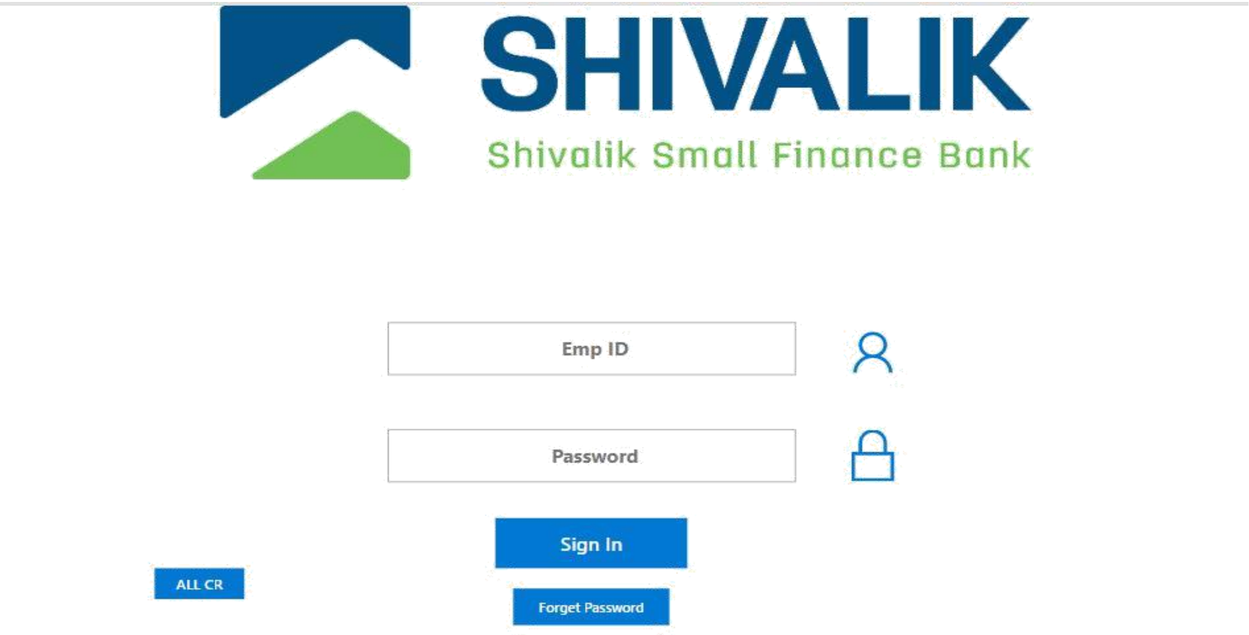
- Authorization and Access Management: Implement an authorization mechanism to control access to different parts of the application. Define the specific pages, features, or data that each role can access. This helps maintain data privacy and security.

- Error Handling and Validation: Implement proper error handling and validation mechanisms on the login page. Display meaningful error messages when incorrect credentials are entered or if there are any other login-related issues. This helps users understand and address any login problems they may encounter.

- Session Management: Implement secure session management to maintain user sessions after successful login. This includes generating session tokens, setting session timeouts, and securely storing session data.

- Password Reset and Account Recovery: Provide mechanisms for employees and administrators to reset their passwords or recover their accounts in case they forget their credentials. This can be done through email verification, security questions, or other appropriate methods.

- Security Measures: Implement additional security measures such as CAPTCHA, account lockout after multiple failed login attempts, and SSL/TLS encryption to enhance the security of the login process.



3.2 Login.

3.3 I/T Equipment Requests App

When testing is done in UAD, workers of a corporation can request modifications in production using the Technology Change Requests App. Before anything is done, requests must be granted by the employee's immediate management and the I/T manager. When a employee want to do some changes in production Then a employee create a new technology change request form & he/she will land on the first page where they have to fill the following fields.

Unique ID: A unique ID, also known as a unique identifier, is a code or number assigned to a specific entity or object to distinguish it from others. The purpose of a unique ID is to ensure that each item or individual can be identified uniquely and accurately.

Date of request: The current date of your request on the date the employee has requested.

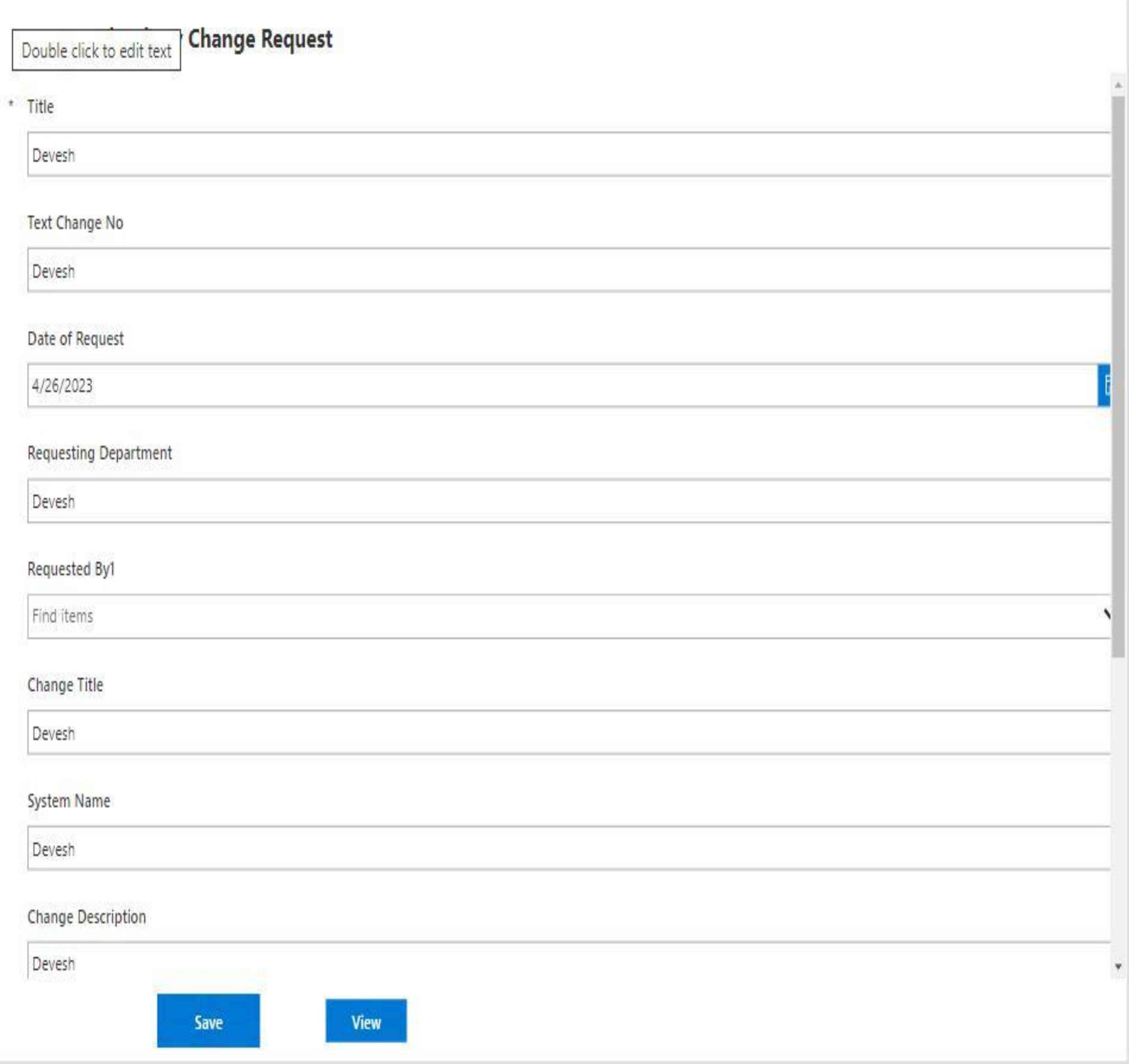
Requesting Department: It refers to the specific department or team that initiates a request or seeks assistance for a particular task, project, or requirement within the organization. The department may vary depending on the nature of the request and the structure of the company.

Request By: The person who is requesting for Technology change request.

Change Type: The type of change the user wants to make. It could be Scheduled, Unscheduled, Emergency.

System type: The type of system in which the changes have to be made.

Change Category: It could be Standard, Minor, Major, Significant.



Double click to edit text
Change Request

* Title
Devesh

Text Change No
Devesh

Date of Request
4/26/2023

Requesting Department
Devesh

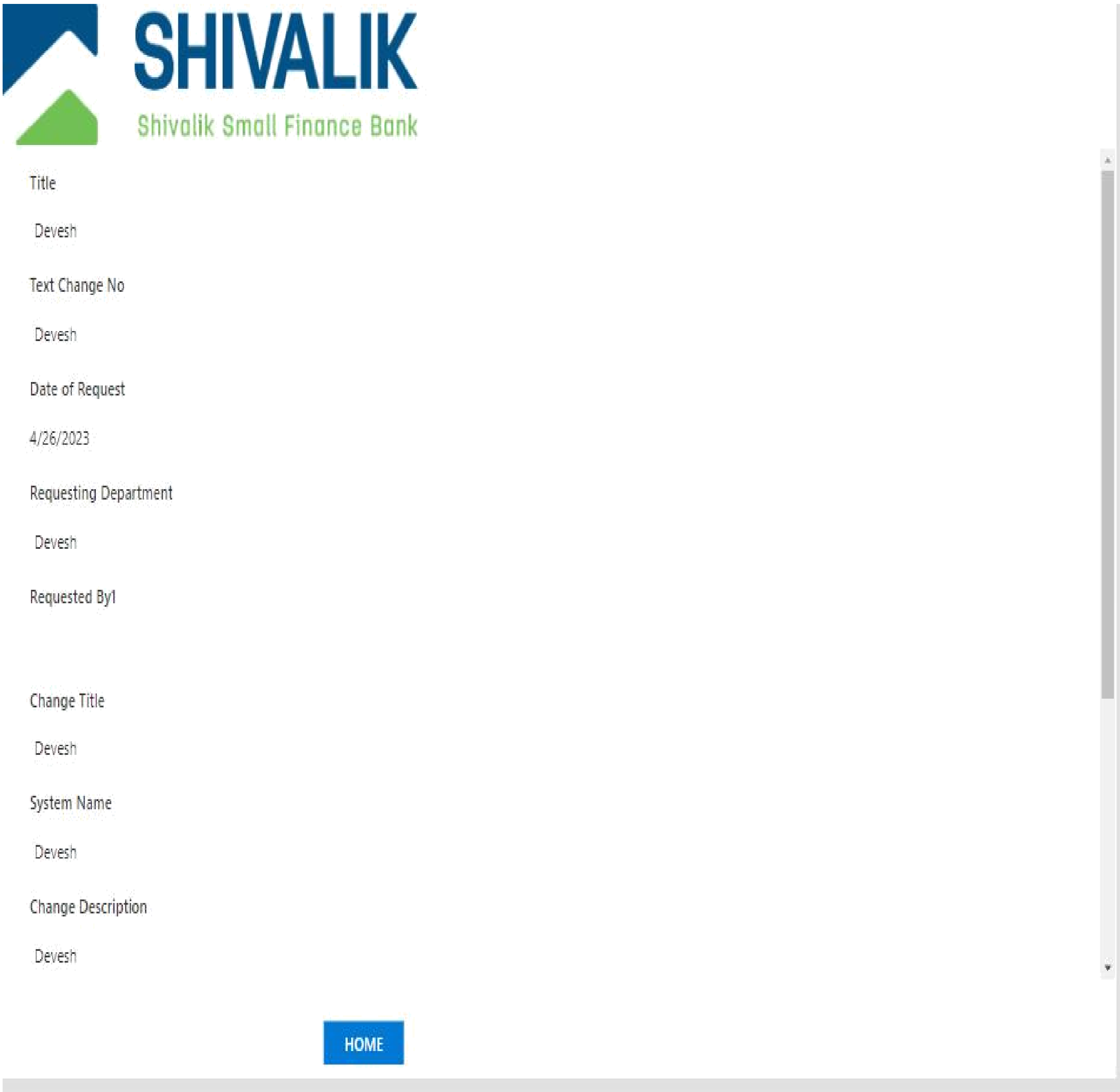
Requested By1
Find items

Change Title
Devesh

System Name
Devesh

Change Description
Devesh

3.3 Technology change request form.



Title

Devesh

Text Change No

Devesh

Date of Request

4/26/2023

Requesting Department

Devesh

Requested By1

Change Title

Devesh

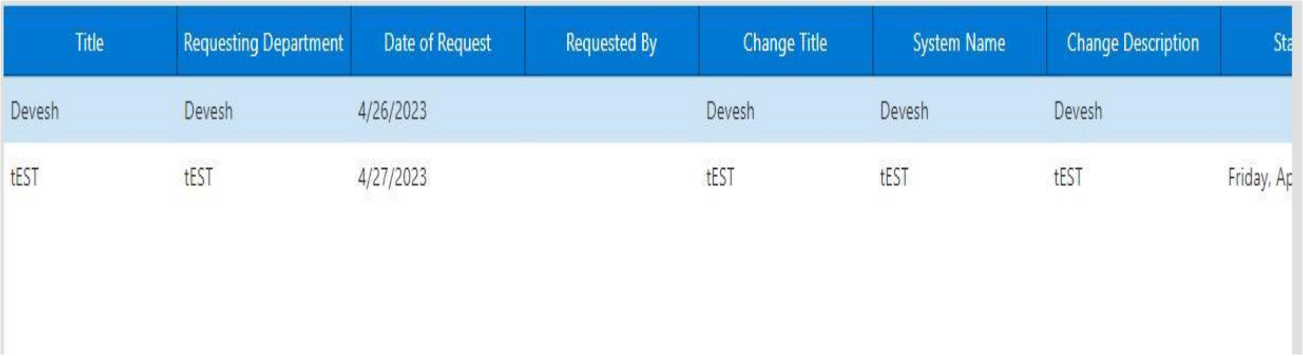
System Name

Devesh

Change Description

Devesh

3.4 View of forms



Title	Requesting Department	Date of Request	Requested By	Change Title	System Name	Change Description	Sta
Devesh	Devesh	4/26/2023		Devesh	Devesh	Devesh	
tEST	tEST	4/27/2023		tEST	tEST	tEST	Friday, Ap

3.5 Data base

CHAPTER 4

Technology Change Request Form Website Using PHP

4.1 Introduction to PHP

PHP (Hypertext Pre-processor) is The server-side programming language PHP (Hypertext Pre-processor), which was initially created for web development, is well-liked and often used. Rasmus Lerdorf developed it in 1994, and since then it has developed into a strong and adaptable language for developing dynamic and interactive web applications. PHP is largely used for server-side scripting in web development. This indicates that the web server executes PHP code to produce dynamic content, which is then transmitted to the client's web browser. PHP is known for being simple and simple to learn, which makes it accessible to beginners. Since its syntax is comparable to that of C and other computer languages, developers with programming experience should have little trouble learning it.

PHP is one of the programming languages used most frequently for web development. Millions of websites are powered by it, and a sizable developer community supports it by offering a wealth of resources, libraries, and frameworks.

PHP is easily integrated into HTML code, enabling developers to combine PHP with HTML to build dynamic web pages. To distinguish PHP code from HTML, it is contained behind special tags (?php and?>).

Integration of databases: PHP includes support for connecting to and interacting with a number of databases, including MySQL, PostgreSQL, Oracle, and others. This makes it simple for PHP application developers to save and retrieve data from databases.

Wide-ranging Built-in Functions and Libraries: PHP has a wide array of built-in functions and libraries, giving developers a wide choice of tools to handle tasks like file manipulation, database operations, form management, and more. A lot of third-party tools and frameworks are also accessible for creating reliable and scalable web applications.

Cross-Platform Compatibility: PHP works with a wide range of web servers and all of the main operating systems, including Windows, Linux, and macOS. This enables PHP applications to be deployed on several platforms without requiring substantial changes.

Scalability: PHP is capable of meeting both high traffic and scalability demands. It may be set up to run in a clustered or load-balanced environment and is frequently used in conjunction with web servers like Apache or Nginx.

With the ability to be used for everything from small personal websites to extensive enterprise systems, PHP is a popular choice for web development. Its sustained success in the web development industry is largely attributed to its broad community support and robust ecosystem of tools and frameworks.

4.2 Login Page

To create a login page for employees and administrators, you can follow these steps:

- Design the Login Page: Create a visually appealing and user-friendly login page. Include input fields for username and password, along with a "Login" button. You can also add branding elements or company logos to the page.

- User Authentication: Implement a user authentication mechanism to verify the credentials entered by employees and administrators. This can be achieved through various methods such as username and password, single sign-on (SSO), or integration with an identity provider like Active Directory or OAuth.

- Secure Password Storage: Ensure that passwords are securely stored in your system. Implement password hashing techniques, such as crypt or Argon2, to protect user credentials from unauthorized access.

- Role-Based Access Control: Differentiate between employees and administrators based on their roles. Assign specific permissions and access levels to each role. This ensures that employees have limited access to certain functionalities, while administrators have elevated privileges.

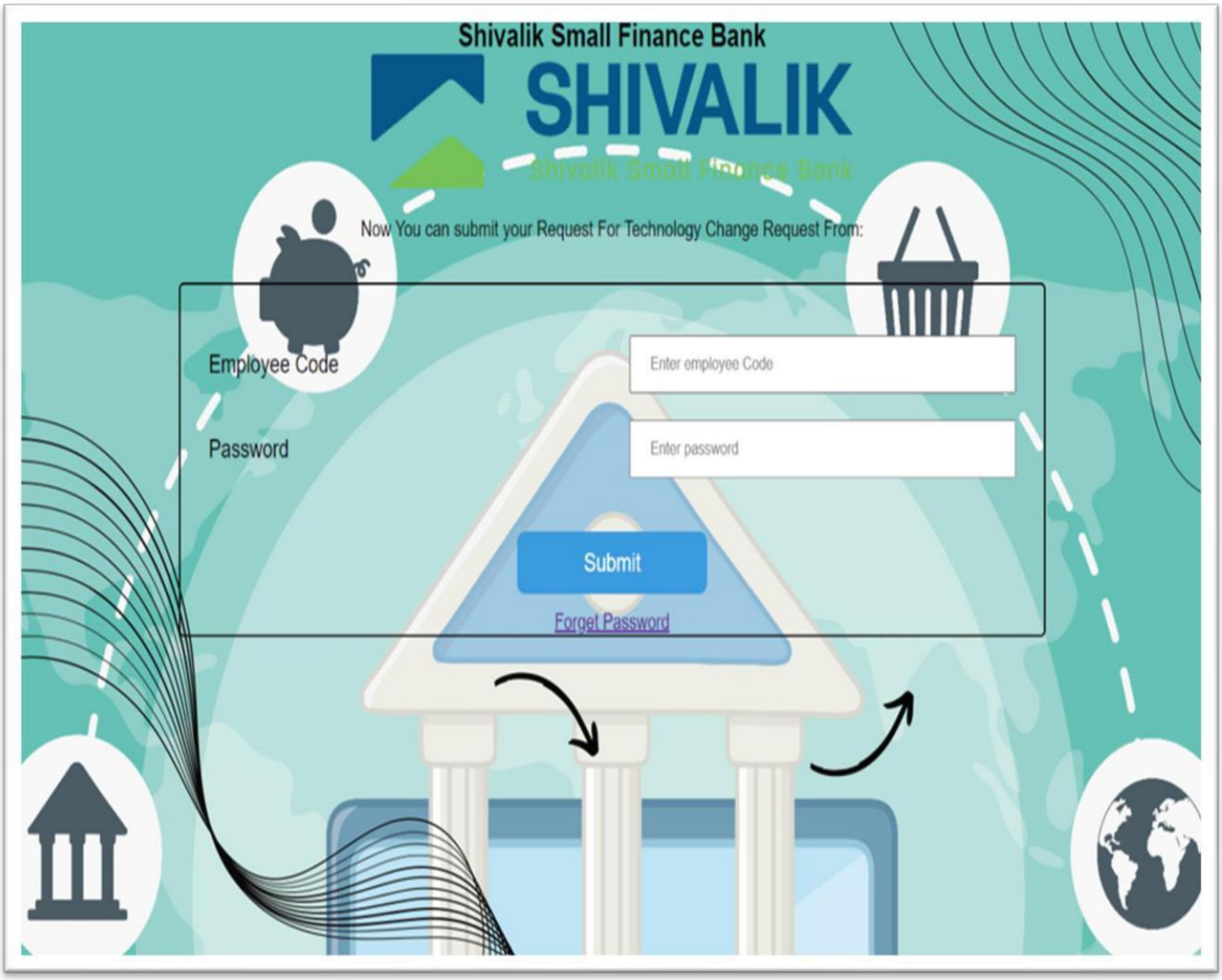
- Authorization and Access Management: Implement an authorization mechanism to control access to different parts of the application. Define the specific pages, features, or data that each role can access. This helps maintain data privacy and security.

- Error Handling and Validation: Implement proper error handling and validation mechanisms on the login page. Display meaningful error messages when incorrect credentials are entered or if there are any other login-related issues. This helps users understand and address any login problems they may encounter.

- Session Management: Implement secure session management to maintain user sessions after successful login. This includes generating session tokens, setting session timeouts, and securely storing session data.

- Password Reset and Account Recovery: Provide mechanisms for employees and administrators to reset their passwords or recover their accounts in case they forget their credentials. This can be done through email verification, security questions, or other appropriate methods.

- Security Measures: Implement additional security measures such as CAPTCHA, account lockout after multiple failed login attempts, and SSL/TLS encryption to enhance the security of the login process.



Shivalik Small Finance Bank

Now You can submit your Request For Technology Change Request From:

4.1 Login Page

4.3 Submit A New Request

An employee chooses the equipment they would like to request, writes a justification in the comments field and clicks submit to send the form to their manager for approval. The other fields of the form should be filled in automatically to prevent data-entry errors.

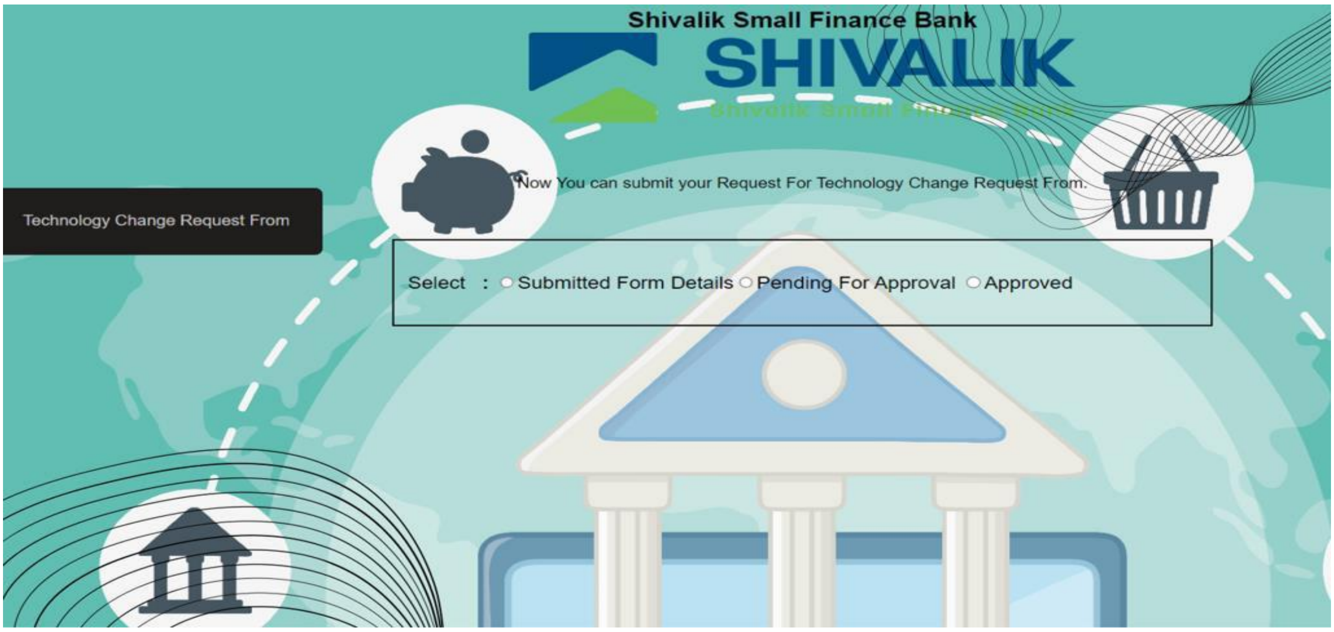
4.4 Status

Submitted form details contain all the CR details including:

- CR Raised
- Pending for Approval
- Approved

Pending for approval - When an employee creates a new request an email is sent to their direct manager asking for an approval. The manager clicks on the link in the email which opens Power Apps to the filled-in request form. Two new buttons appear on the screen: ‘Approve’ and ‘Reject’. Approving the form will send an email to the IT Manager. If they also approve the employee will receive a notification that their request was approved. Or, if either of the managers click Reject then the employee will get an email stating that the request was denied.

Approved- Approval typically means that your form has met the necessary requirements or criteria and it must be live on production.



Shivalik Small Finance Bank

Now You can submit your Request For Technology Change Request From.

Select : ○ Submitted Form Details ○ Pending For Approval ○ Approved

4.2 Inputs of Data base

Unique ID: A unique ID, also known as a unique identifier, is a code or number assigned to a specific entity or object to distinguish it from others. The purpose of a unique ID is to ensure that each item or individual can be identified uniquely and accurately.

Date of request: The current date of your request on the date the employee has requested.

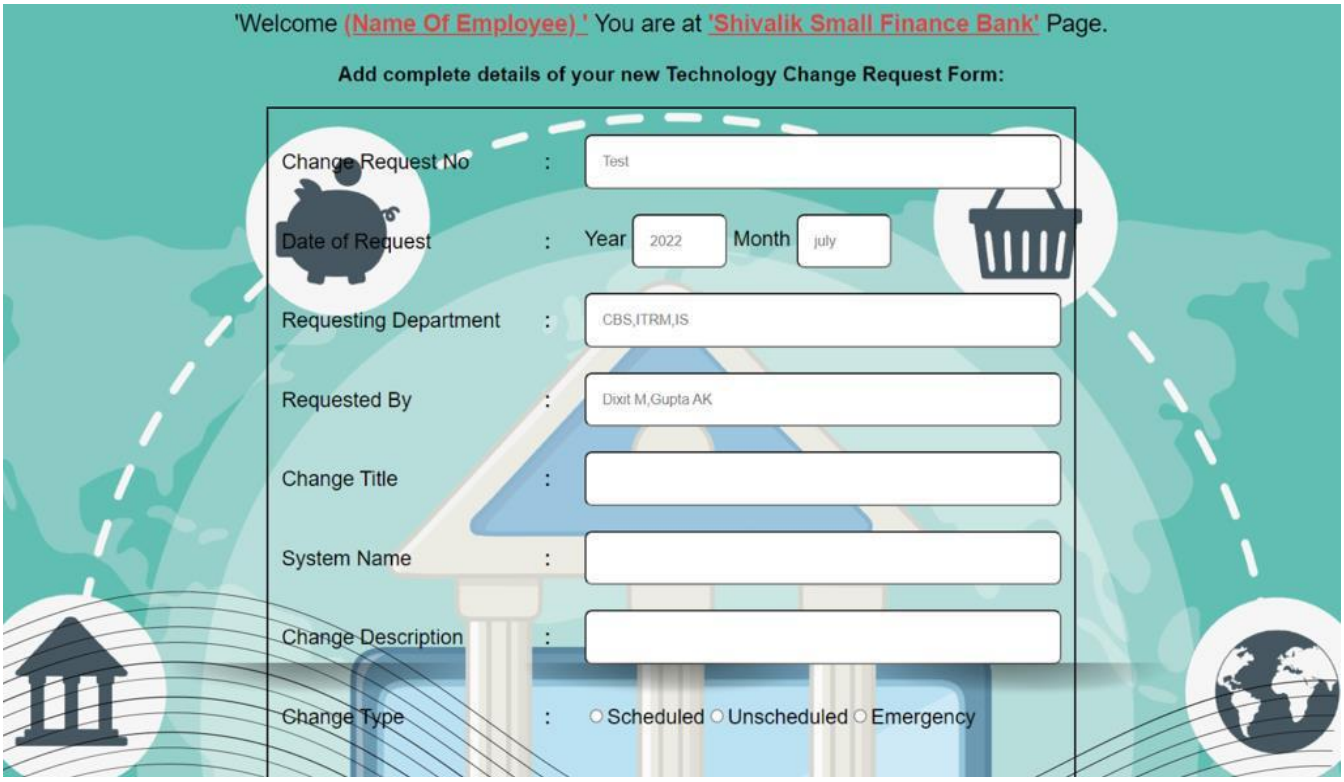
Requesting Department: It refers to the specific department or team that initiates a request or seeks assistance for a particular task, project, or requirement within the organization. The department may vary depending on the nature of the request and the structure of the company.

Request By: The person who is requesting for Technology change request.

Change Type: The type of change the user wants to make. It could be Scheduled, Unscheduled, Emergency.

System type: The type of system in which the changes must be made.

Change Category: It could be Standard, Minor, Major, Significant.



'Welcome (Name Of Employee) ' You are at 'Shivalik Small Finance Bank' Page.

Add complete details of your new Technology Change Request Form:

Change Request No : Test

Date of Request : Year 2022 Month july

Requesting Department : CBS,ITRM,IS

Requested By : Dixit M,Gupta AK

Change Title :

System Name :

Change Description :

Change Type : ○ Scheduled ○ Unscheduled ○ Emergency

4.3 Technology change request form.

CHAPTER 5 – RESULTS & DISCUSSION

Its hard to imagine banking without the convenience of mobile applications. The ability to manage finances anytime anywhere has become essential for modern day consumers. Our report examines the efficacy of a bank's mobile app as well as its Technology change request functions across head office and all branch.

The approvals form will be functional at this point but it could still benefit from some additional styling. I have created a component to visualize the status of an Approval

The results of VAPT and VA testing are typically specific to the systems, networks, or applications being tested and can vary widely based on their configuration and security posture.

5.1 Vulnerability Assessment (VA) Results:

- List of identified vulnerabilities: VA testing involves scanning and assessing systems for known vulnerabilities. The results will provide a comprehensive list of identified vulnerabilities, including their severity levels and descriptions.

- Risk prioritization: The identified vulnerabilities may be categorized based on their potential impact and likelihood of exploitation, helping organizations prioritize their remediation efforts.

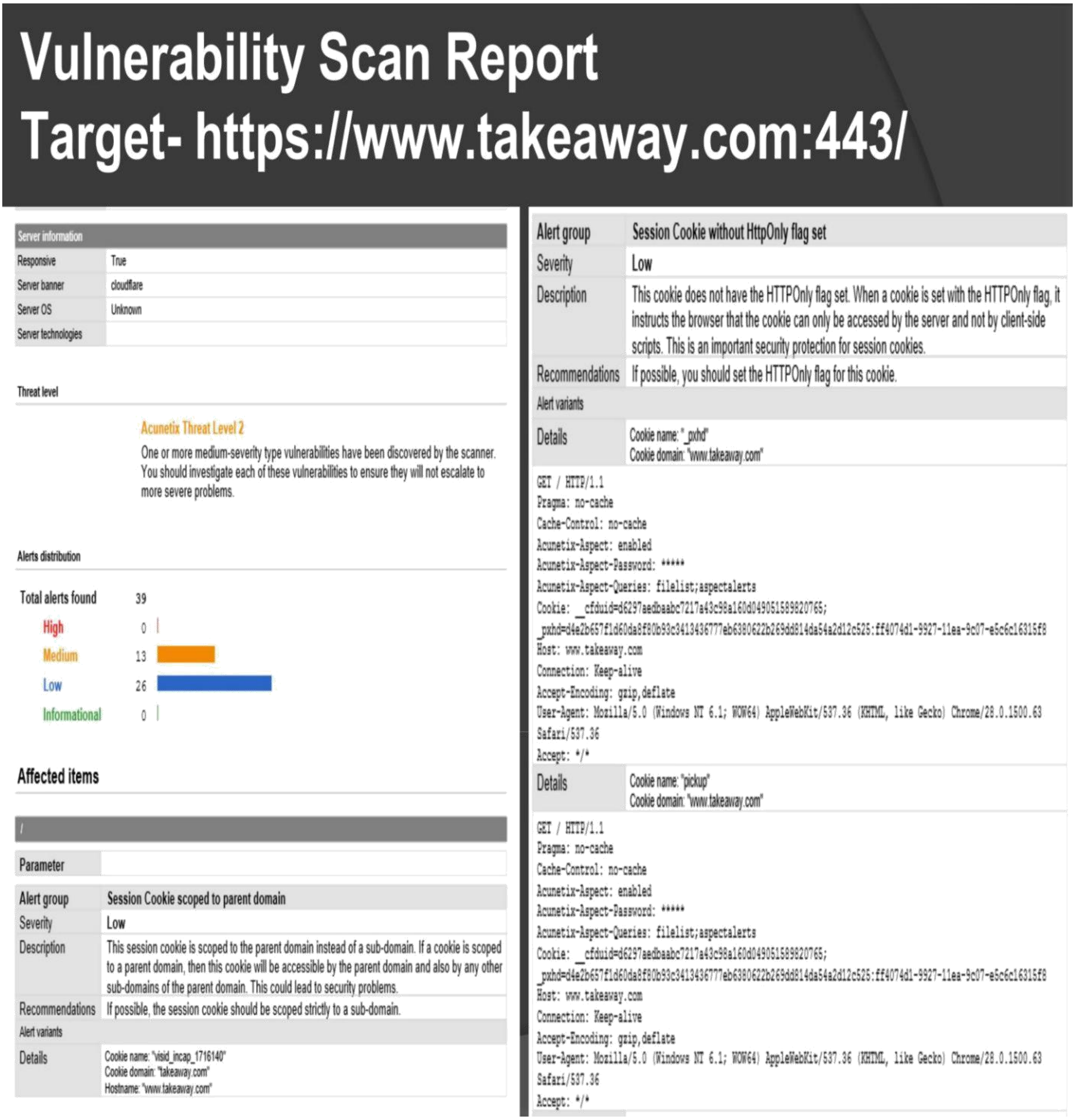
- Recommendations for remediation: VA testing typically includes recommendations and mitigation strategies to address the identified vulnerabilities. These recommendations may include applying patches, updating configurations, or implementing additional security controls.

5.2 Penetration Testing (PT) Results:

- Exploitable vulnerabilities: Penetration testing involves actively attempting to exploit vulnerabilities to gain unauthorized access or demonstrate the potential impact. The results may include a list of successfully exploited vulnerabilities, highlighting the potential risks associated with them.

- Access and compromise details: Penetration testing results may provide detailed information on the methods used to gain unauthorized access, escalate privileges, or compromise systems. This information helps organizations understand the potential attack vectors and their impact.

- Recommendations and remediation steps: Penetration testing results typically include recommendations for addressing the identified vulnerabilities and improving overall security. These recommendations may focus on hardening configurations, strengthening access controls, or enhancing network segmentation.



Vulnerability Scan Report
Target- https://www.takeaway.com:443/

Server information	
Responsive	True
Server banner	cloudflare
Server OS	Unknown
Server technologies	

Threat level

Acunetix Threat Level 2

One or more medium-severity type vulnerabilities have been discovered by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe problems.

Alerts distribution

Total alerts found	39
High	0
Medium	13
Low	26
Informational	0

Affected items

/

Parameter	

Alert group	Session Cookie scoped to parent domain
Severity	Low
Description	This session cookie is scoped to the parent domain instead of a sub-domain. If a cookie is scoped to a parent domain, then this cookie will be accessible by the parent domain and also by any other sub-domains of the parent domain. This could lead to security problems.
Recommendations	If possible, the session cookie should be scoped strictly to a sub-domain.
Alert variants	
Details	Cookie name: "visid_incap_1716140" Cookie domain: "takeaway.com" Hostname: "www.takeaway.com"

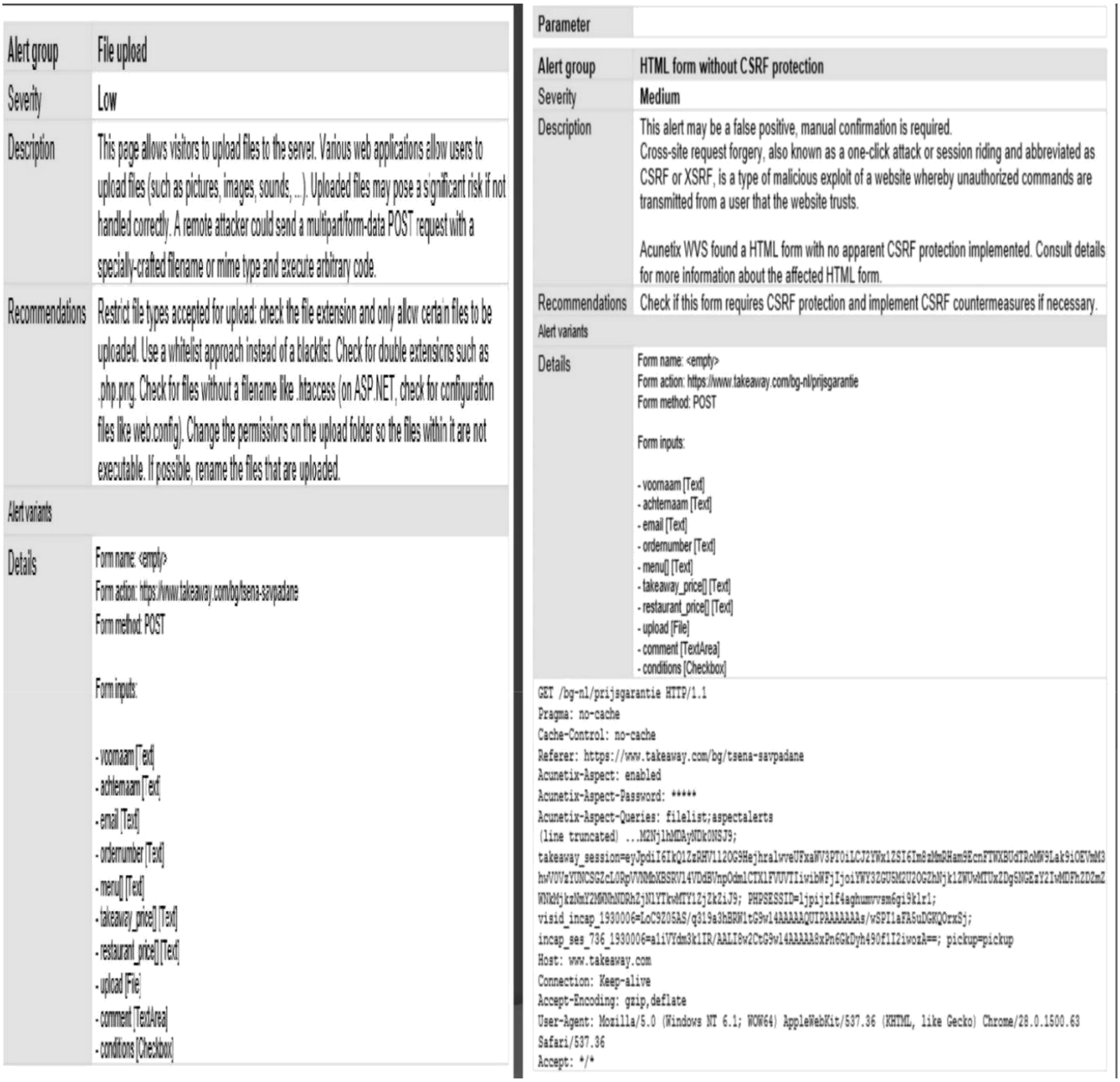
Alert group	Session Cookie without HttpOnly flag set
Severity	Low
Description	This cookie does not have the HTTPOnly flag set. When a cookie is set with the HTTPOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies.
Recommendations	If possible, you should set the HTTPOnly flag for this cookie.
Alert variants	
Details	Cookie name: "_pxhd" Cookie domain: "www.takeaway.com"

```
GET / HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: __cfduid=d6297aedbaabc7217a43c98a160d049051589820765;
_pxhd=d4e2b657f1d60da8f80b93c3413436777eb6380622b269dd814da54a2d12c525:ff4074d1-9927-11ea-9c07-e5c6c16315f8
Host: www.takeaway.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.63
Safari/537.36
Accept: */*
```

Details	Cookie name: "pickup" Cookie domain: "www.takeaway.com"

```
GET / HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: __cfduid=d6297aedbaabc7217a43c98a160d049051589820765;
_pxhd=d4e2b657f1d60da8f80b93c3413436777eb6380622b269dd814da54a2d12c525:ff4074d1-9927-11ea-9c07-e5c6c16315f8
Host: www.takeaway.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.63
Safari/537.36
Accept: */*
```

5.1 Acunetix scan report

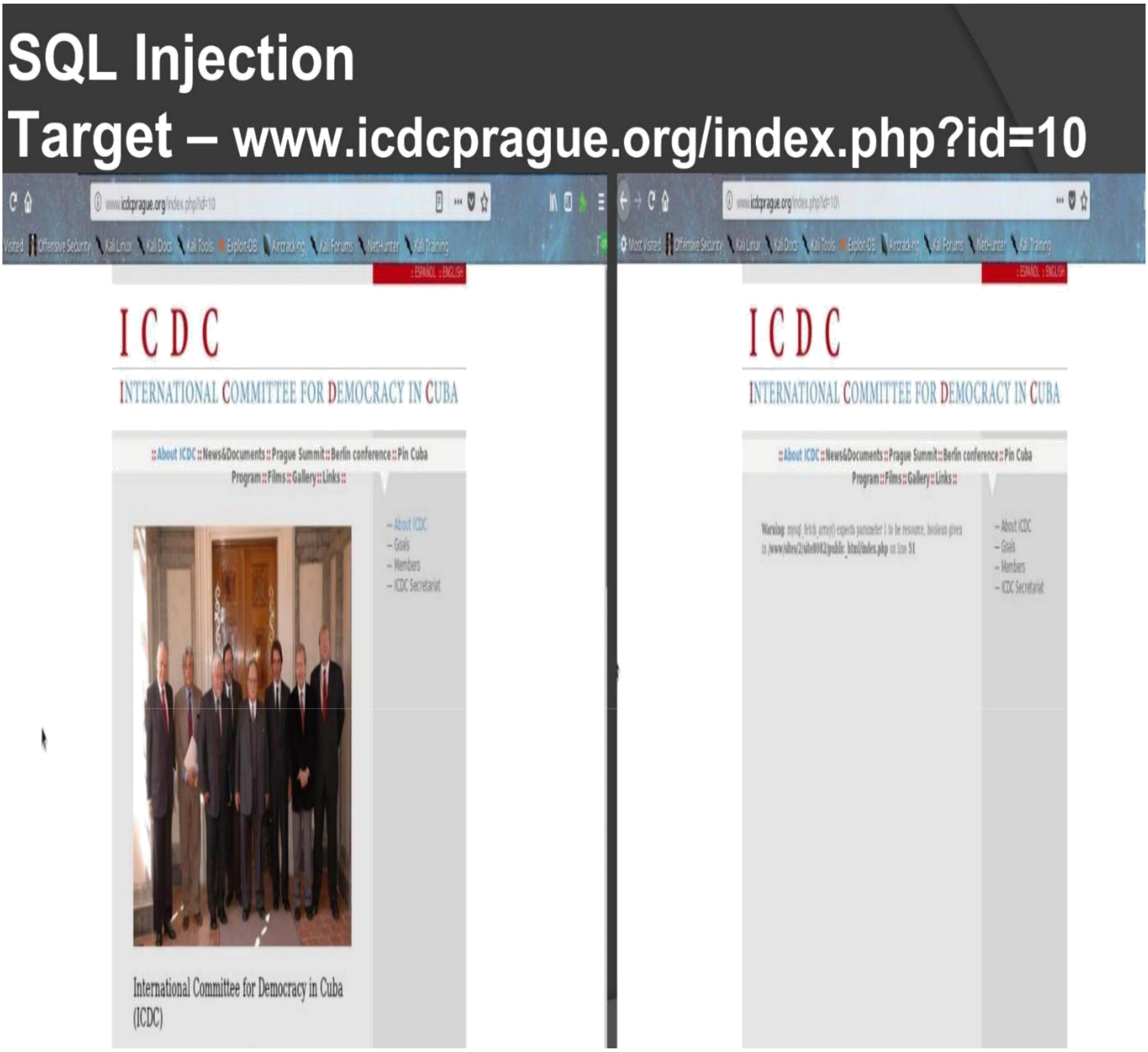


Alert group	File upload
Severity	Low
Description	This page allows visitors to upload files to the server. Various web applications allow users to upload files (such as pictures, images, sounds, ...). Uploaded files may pose a significant risk if not handled correctly. A remote attacker could send a multipart/form-data POST request with a specially-crafted filename or mime type and execute arbitrary code.
Recommendations	Restrict file types accepted for upload: check the file extension and only allow certain files to be uploaded. Use a whitelist approach instead of a blacklist. Check for double extensions such as .php.png. Check for files without a filename like .htaccess (on ASP.NET, check for configuration files like web.config). Change the permissions on the upload folder so the files within it are not executable. If possible, rename the files that are uploaded.
Alert variants	
Details	Form name: <empty> Form action: https://www.takeaway.com/bg/tsena-savpadane Form method: POST Form inputs: - voornaam [Text] - achternaam [Text] - email [Text] - ordernumber [Text] - menu[] [Text] - takeaway_price[] [Text] - restaurant_price[] [Text] - upload [File] - comment [TextArea] - conditions [Checkbox]

Parameter	
Alert group	HTML form without CSRF protection
Severity	Medium
Description	This alert may be a false positive, manual confirmation is required. Cross-site request forgery, also known as a one-click attack or session riding and abbreviated as CSRF or XSRF, is a type of malicious exploit of a website whereby unauthorized commands are transmitted from a user that the website trusts. Acunetix WVS found a HTML form with no apparent CSRF protection implemented. Consult details for more information about the affected HTML form.
Recommendations	Check if this form requires CSRF protection and implement CSRF countermeasures if necessary.
Alert variants	
Details	Form name: <empty> Form action: https://www.takeaway.com/bg-nl/prijsgarantie Form method: POST Form inputs: - voornaam [Text] - achternaam [Text] - email [Text] - ordernumber [Text] - menu[] [Text] - takeaway_price[] [Text] - restaurant_price[] [Text] - upload [File] - comment [TextArea] - conditions [Checkbox]

```
GET /bg-nl/prijsgarantie HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://www.takeaway.com/bg/tsena-savpadane
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
(line truncated) ...M2NjlhMDAyNDk0NSJ9;
takeaway_session=eyJpdiI6IkQ1ZzRHV1l2OG9HejhralvveUFxaWV3PTOiLCJ2YWx1ZSI6Im8zMmRHam9EcnFTWXBUdTRoMW9Lak9iOEVmM3
hwV0VzYUNCSGZcL0RpVVNMbXBSRV14VDdBVnpOdmlCTXlFVUVTIiwibWFjIjoiYWY3ZGU5M2U2OGZhNjk1ZWUwMTUxZDg5NGEzY2IwMDFhZDZmZ
WNkMjkzNmY2MWNhNDRhZjN1YTkwMTY1ZjZkZiJ9; PHPSESSID=1jpijrlf4aghumvvsm6gi9klr1;
visid_incap_1930006=LoC9Z05AS/q319a3hBRW1tG9wl4AAAAAQUIPAAAAAAAs/wSPI1aFA5uDGKQOrxSj;
incap_ses_736_1930006=a1iVYdm3k1IR/AALI8w2CtG9wl4AAAAA8xPn6GkDyh490f1I2iwozA==; pickup=pickup
Host: www.takeaway.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.63
Safari/537.36
Accept: */*
```

5.2 Vulnerability Detail



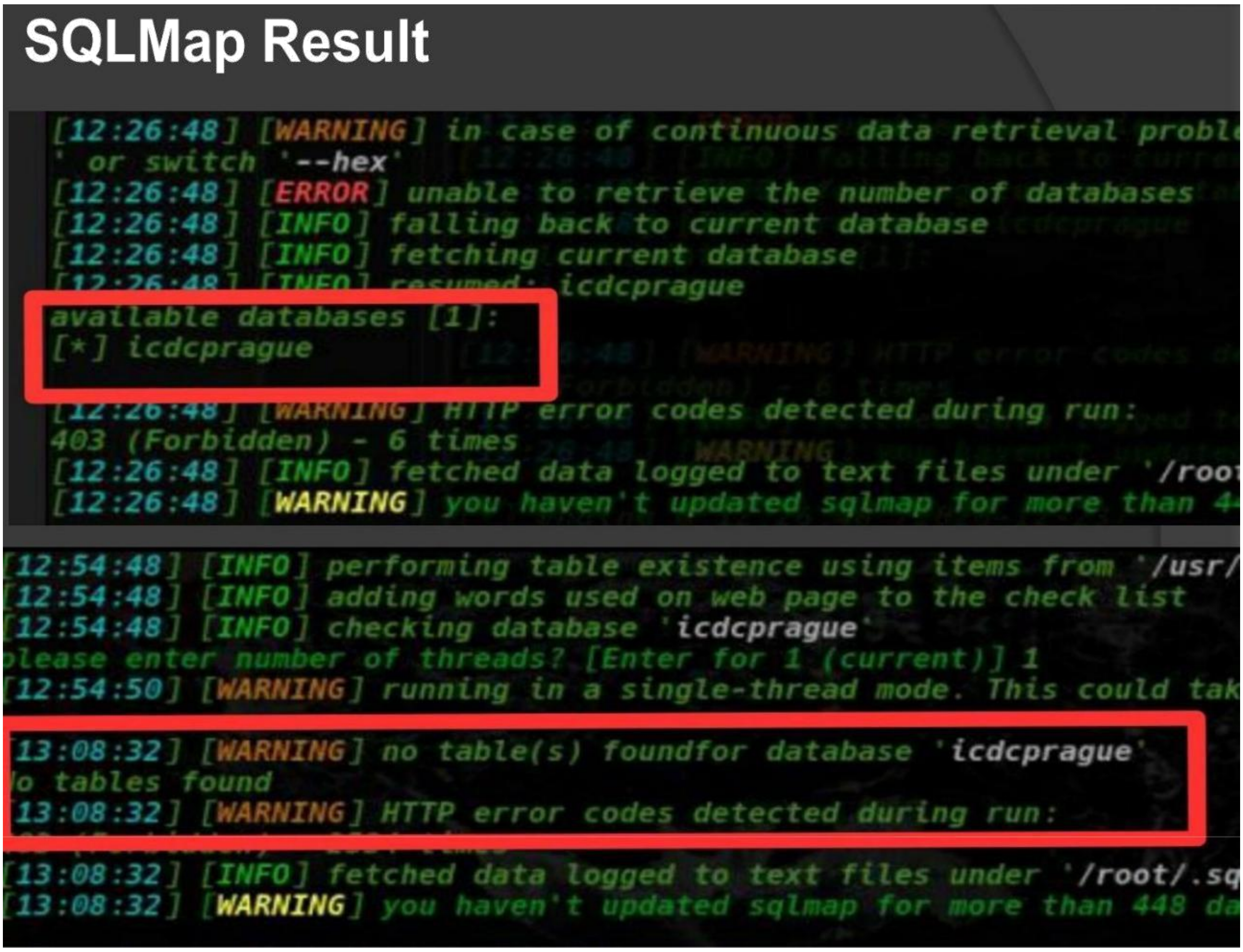
SQL Injection

Target – www.icdcprague.org/index.php?id=10

www.icdcprague.org/index.php?id=10
Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Kali Training
:: ESPAÑOL :: ENGLISH
ICDC
INTERNATIONAL COMMITTEE FOR DEMOCRACY IN CUBA
:: About ICDC :: News&Documents :: Prague Summit :: Berlin conference :: Pin Cuba Program :: Films :: Gallery :: Links ::
– About ICDC
– Goals
– Members
– ICDC Secretariat
International Committee for Democracy in Cuba (ICDC)
www.icdcprague.org/index.php?id=10'
Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Kali Training

```
Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /www/sites/2/site8082/public_html/index.php on line 51
```

5.3 SQL Injection.



SQLMap Result

```
[12:26:48] [WARNING] in case of continuous data retrieval proble
' or switch '--hex'
[12:26:48] [ERROR] unable to retrieve the number of databases
[12:26:48] [INFO] falling back to current database
[12:26:48] [INFO] fetching current database
[12:26:48] [INFO] resumed: icdcprague
available databases [1]:
[*] icdcprague

[12:26:48] [WARNING] HTTP error codes detected during run:
403 (Forbidden) - 6 times
[12:26:48] [INFO] fetched data logged to text files under '/roo
[12:26:48] [WARNING] you haven't updated sqlmap for more than 4
```

```
[12:54:48] [INFO] performing table existence using items from '/usr/
[12:54:48] [INFO] adding words used on web page to the check list
[12:54:48] [INFO] checking database 'icdcprague'
please enter number of threads? [Enter for 1 (current)] 1
[12:54:50] [WARNING] running in a single-thread mode. This could tak

[13:08:32] [WARNING] no table(s) foundfor database 'icdcprague'
No tables found
[13:08:32] [WARNING] HTTP error codes detected during run:
[13:08:32] [INFO] fetched data logged to text files under '/root/.sq
[13:08:32] [WARNING] you haven't updated sqlmap for more than 448 da
```

5.4 SQLMAP report.

CHAPTER 6– CONCLUSION

The conclusion of a VAPT (Vulnerability Assessment and Penetration Testing) and Red Teaming exercise typically involves summarizing the key findings, assessing the overall security posture, and providing recommendations for improving the organization's security defences. Summary of Findings Give a brief summary of the flaws, weaknesses, and potential points of compromise found throughout the testing. This could involve both procedural problems and technical flaws. Risk assessment: Consider the potential impact and likelihood of exploitation of the vulnerabilities and flaws that have been found. According to the level of danger they bring to the organization's assets and activities, this helps prioritize the mitigation actions. Impact Analysis: Examine the possible repercussions of successful system breach or successful exploitation of discovered vulnerabilities. This may include effects on the organization's finances, operations, reputation, and legal standing.

Recommendations: Make concrete suggestions for resolving the shortcomings and vulnerabilities found. These suggestions ought to be useful and ranked according to their importance and the resources and competencies of the organization. They could involve adding more security measures, increasing access restrictions, patching systems, updating configurations, and security awareness training.

Strategies for Mitigation: Offer detailed plans for reducing the threats that have been found and boosting the organization's security defences. To address the weaknesses and boost the overall security posture, this may entail a combination of technical measures, process improvements, and personnel training.

Lessons Learned: Outline any lessons discovered throughout the VAPT and Red Teaming exercise, such as gaps in incident response protocols, weak points in current security controls, or places where staff awareness and training might be strengthened. Ongoing Inspection and Upkeep: To guarantee that the organization's security procedures are effective over time, emphasise the necessity of continual monitoring, maintenance, and periodic reassessment. This involves routine patch management, vulnerability scanning, and employee security awareness training.

A Technology Change Request Approval Form's conclusion provides a summary of the choice made and the result of the request. The following components can be included to a technology change request approval form's conclusion:

1. Approval Decision: Indicate whether the proposal for a technology change has been accepted, refused, or postponed for additional review. Explain the decision's justification, taking into account elements including viability, influence on current systems, required resources, and alignment with organizational goals. Key Stakeholders: Acknowledge the individuals or departments involved in the decision-making process, including the approver(s) and any other relevant parties.

2. Approved Changes: If the request has been approved, clearly outline the details of the approved changes. This may include a description of the proposed technology change, expected benefits, timeline for implementation, and any conditions or dependencies.

3. Explain why the request was rejected, if applicable. If the request was denied, give a succinct justification. This could serve as direction for subsequent requests and assist the requester in understanding the thinking behind the decision.

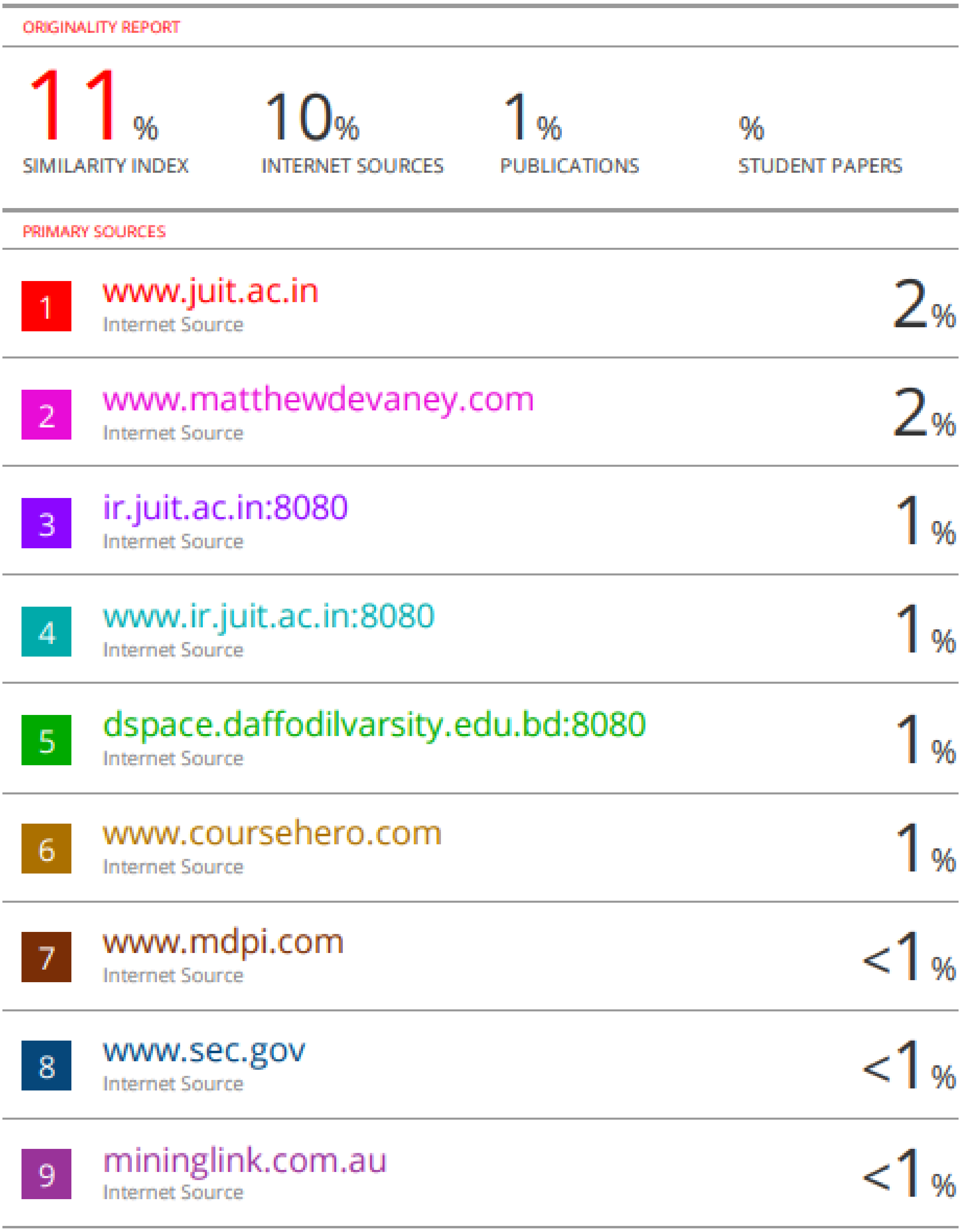
4. Next Steps: Describe the actions or steps that must be taken in light of the decision. This may entail informing the requester, informing the appropriate teams of the decision, starting the implementation process, or, if more time is needed, setting up more discussions or evaluations.

5. The requester, the project team, and any other impacted parties should be informed of the decision and its outcome in a clear and concise manner. Making sure everyone is informed of the decision and has time to make plans is made easier with clear and prompt communication.

REFERENCES

1. https://owasp.org/
2. https://portswigger.net/
3. https://www.hackthebox.com/
4. https://www.kali.org/
5. https://www.tenable.com/products/nessus
6. https://www.qualys.com
7. https://www.youtube.com/
8. https://www.nist.gov/
9. https://attack.mitre.org/
10. https://osintframework.com/

Plagiarism Report



ORIGINALITY REPORT

11 %	10%	1 %	%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.juit.ac.in Internet Source	2%
2	www.matthewdevaney.com Internet Source	2%
3	ir.juit.ac.in:8080 Internet Source	1 %
4	www.ir.juit.ac.in:8080 Internet Source	1 %
5	dspace.daffodilvarsity.edu.bd:8080 Internet Source	1 %
6	www.coursehero.com Internet Source	1 %
7	www.mdpi.com Internet Source	<1 %
8	www.sec.gov Internet Source	<1 %
9	mininglink.com.au Internet Source	<1 %

10	www.careerpower.in Internet Source	<1 %
11	acikbilim.yok.gov.tr Internet Source	<1 %
12	Thomas Fend, Gary Jorgensen, Harald Küster. "Applicability of highly reflective aluminium coil for solar concentrators", Solar Energy, 2000 Publication	<1 %
13	www.apraca.org Internet Source	<1 %
14	www.marketunited.com Internet Source	<1 %
15	itweb.co.za Internet Source	<1 %
16	www.cio.com Internet Source	<1 %
17	Keyur Patel. "A Survey on Vulnerability Assessment & Penetration Testing for Secure Communication", 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), 2019 Publication	<1 %
18	Nguyễn Việt Hùng, Nguyễn Thành Công. "Áp dụng học tăng cường trong kiểm thử xâm	<1 %

	nhập tự động", Journal of Science and Technology on Information security, 2023 Publication	
19	resources.infosecinstitute.com Internet Source	<1 %
20	ecuc.ac.ae Internet Source	<1 %
21	pdfs.semanticscholar.org Internet Source	<1 %
22	zen.taozero.net Internet Source	<1 %
23	cifz.ginnasticabutterfly.it Internet Source	<1 %
24	indianexpress.com Internet Source	<1 %
25	wwartimes.blogspot.com Internet Source	<1 %
26	docshare.tips Internet Source	<1 %
27	en.wikipedia.org Internet Source	<1 %
28	www.iilsindia.com Internet Source	<1 %

29	Claudia Greco, Giancarlo Fortino, Bruno Crispo, Kim-Kwang Raymond Choo. "AI-enabled IoT penetration testing: state-of-the-art and research challenges", Enterprise Information Systems, 2022 Publication	<1 %
30	capedge.com Internet Source	<1 %
31	link.springer.com Internet Source	<1 %
32	www.holmsecurity.com Internet Source	<1 %

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		