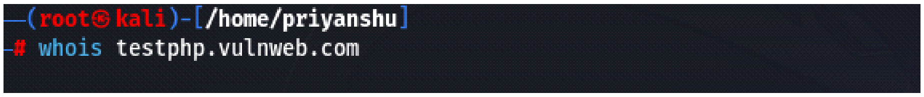
TASK LEVEL(HARD)

Create a detailed report including the information, planning and the attacks initiated and steps involved to analyze and initiate the attack in the website http://testphp.vulnweb.com.

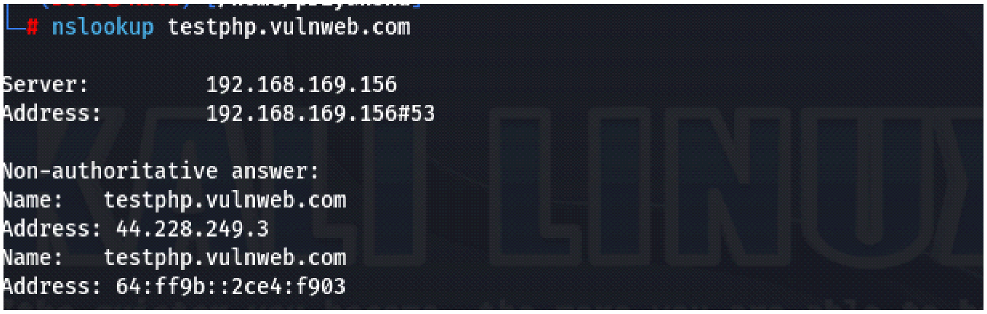
Step-1:- Website Reconnaissance

(i)Identify Domain Information:- Use whois to retrieve domain registration details.



```
┌──(root㉿kali)-[/home/priyanshu]
└─# whois testphp.vulnweb.com
```

(ii)Use nslookup to get DNS information.

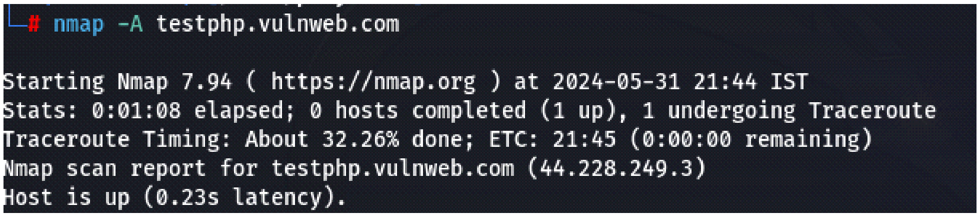


```
└─# nslookup testphp.vulnweb.com

Server:         192.168.169.156
Address:        192.168.169.156#53

Non-authoritative answer:
Name:   testphp.vulnweb.com
Address: 44.228.249.3
Name:   testphp.vulnweb.com
Address: 64:ff9b::2ce4:f903
```

(iii)Scan for Open Ports and Services:-Use Nmap to scan for open ports and identify running services.



```
└─# nmap -A testphp.vulnweb.com

Starting Nmap 7.94 ( https://nmap.org ) at 2024-05-31 21:44 IST
Stats: 0:01:08 elapsed; 0 hosts completed (1 up), 1 undergoing Traceroute
Traceroute Timing: About 32.26% done; ETC: 21:45 (0:00:00 remaining)
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.23s latency).
```

Step-2:-Identify Potential Vulnerabilities

(i)Refer to the OWASP Top 10 list to understand common vulnerabilities and prioritize testing.

(ii)Use Nikto to scan for known vulnerabilities and misconfigurations.

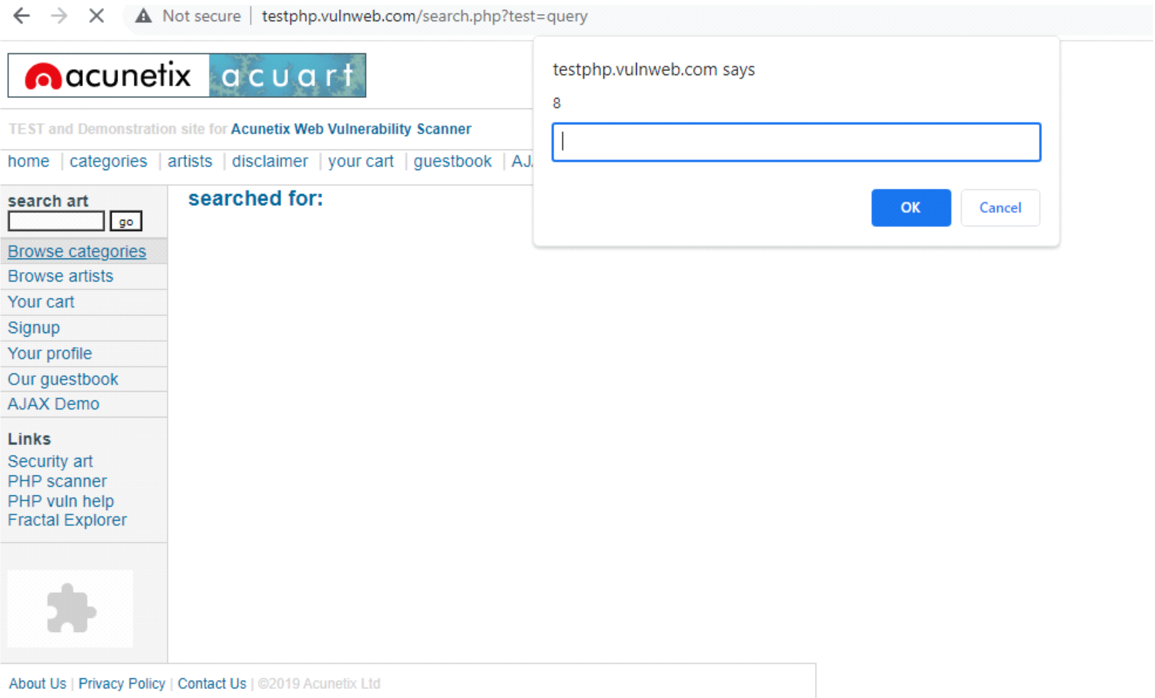
(iii)Use SQLMap to test for SQL injection vulnerabilities.

(iv)Manually inject common XSS payloads into input fields and observe the responses.

(v)Manually inject common XSS payloads into input fields and observe the responses & tests the other vulnerabilities such as Cross-Site Request Forgery(CSRF).

Step-3:-Exploit Identified Vulnerabilities

XSS(Cross-Site Scripting):-



Not secure | testphp.vulnweb.com/search.php?test=query

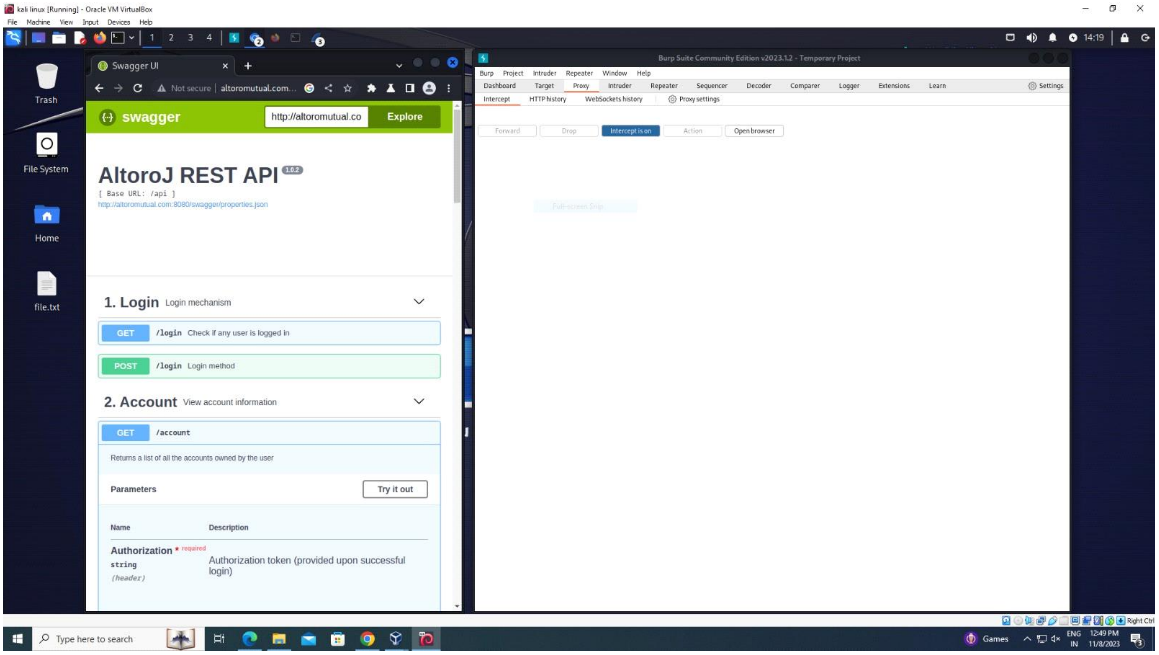
testphp.vulnweb.com says

8

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

searched for:

Default Credential:-



AltoroJ REST API 1.0.2

[Base URL: /api]

http://altoromutual.com:8080/swagger/properties.json

1. Login Login mechanism

GET /login Check if any user is logged in

POST /login Login method

2. Account View account information

GET /account

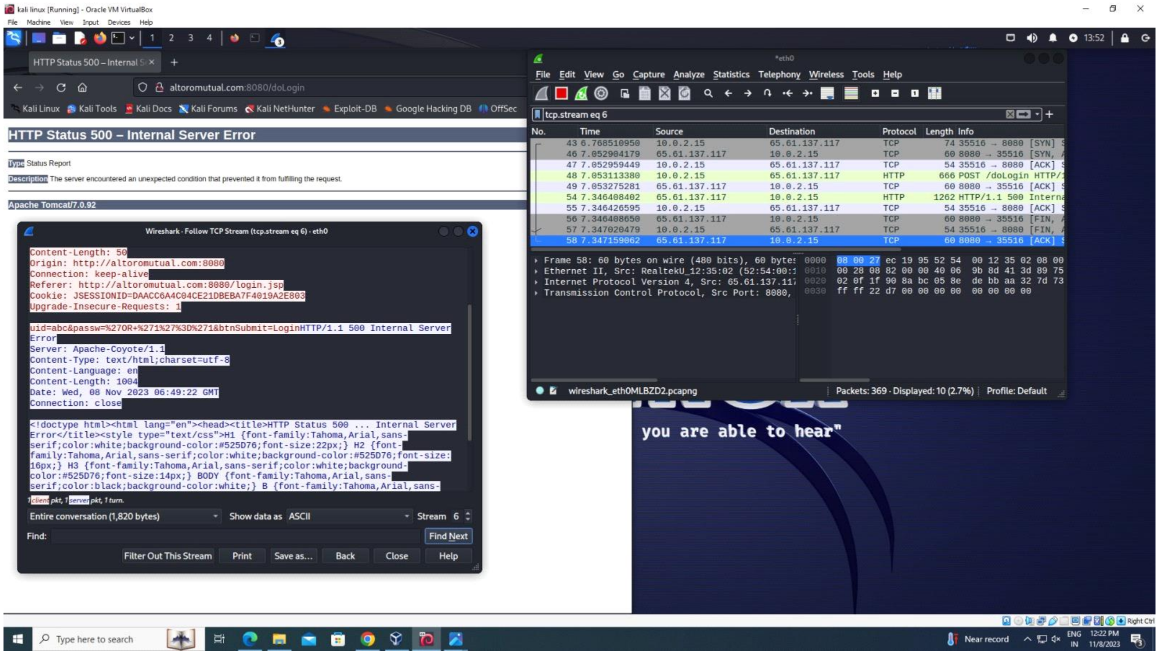
Returns a list of all the accounts owned by the user

Parameters

Name	Description
Authorization * required string (header)	Authorization token (provided upon successful login)

kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Trash
File System
Home
file.txt
14:19
Swagger UI
Not secure | altoromutual.com...
swagger
http://altoromutual.co
Explore
Try it out
Burp Suite Community Edition v2023.1.2 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn
Settings
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is on Action Open browser
Type here to search
Games
ENG IN
12:49 PM 11/8/2023
Right Ctrl

SQL Injection:-



HTTP Status 500 – Internal Server Error

Type Status Report

Description The server encountered an unexpected condition that prevented it from fulfilling the request.

Apache Tomcat/7.0.92

Wireshark · Follow TCP Stream (tcp.stream eq 6) · eth0

```
Content-Length: 50
Origin: http://altoromutual.com:8080
Connection: keep-alive
Referer: http://altoromutual.com:8080/login.jsp
Cookie: JSESSIONID=DAACC6A4C04CE21DBEBA7F4019A2E803
Upgrade-Insecure-Requests: 1

uid=abc&passw=%27OR+%271%27%3D%271&btnSubmit=LoginHTTP/1.1 500 Internal Server
Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Language: en
Content-Length: 1004
Date: Wed, 08 Nov 2023 06:49:22 GMT
Connection: close

<!doctype html><html lang="en"><head><title>HTTP Status 500 ... Internal Server
Error</title><style type="text/css">H1 {font-family:Tahoma,Arial,sans-
serif;color:white;background-color:#525D76;font-size:22px;} H2 {font-
family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:
16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-
color:#525D76;font-size:14px;} BODY {font-family:Tahoma,Arial,sans-
serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-
```

1 client pkt, 1 server pkt, 1 turn.

Entire conversation (1,820 bytes) Show data as ASCII Stream 6

Find:

*eth0

tcp.stream eq 6

```
No.  Time         Source         Destination    Protocol Length Info
  43 6.768510950  10.0.2.15      65.61.137.117  TCP        74 35516 → 8080 [SYN] S
  46 7.052904179  65.61.137.117  10.0.2.15      TCP        60 8080 → 35516 [SYN, A
  47 7.052959449  10.0.2.15      65.61.137.117  TCP        54 35516 → 8080 [ACK] S
  48 7.053113380  10.0.2.15      65.61.137.117  HTTP      666 POST /doLogin HTTP/1
  49 7.053275281  65.61.137.117  10.0.2.15      TCP        60 8080 → 35516 [ACK] S
  54 7.346408402  65.61.137.117  10.0.2.15      HTTP     1262 HTTP/1.1 500 Interna
  55 7.346426595  10.0.2.15      65.61.137.117  TCP        54 35516 → 8080 [ACK] S
  56 7.346408650  65.61.137.117  10.0.2.15      TCP        60 8080 → 35516 [FIN, A
  57 7.347020479  10.0.2.15      65.61.137.117  TCP        54 35516 → 8080 [FIN, A
  58 7.347159062  65.61.137.117  10.0.2.15      TCP        60 8080 → 35516 [ACK] S
```

```
› Frame 58: 60 bytes on wire (480 bits), 60 bytes      0000  08 00 27 ec 19 95 52 54  00 12 35 02 08 00
› Ethernet II, Src: RealtekU_12:35:02 (52:54:00:1      0010  00 28 08 82 00 00 40 06  9b 8d 41 3d 89 75
› Internet Protocol Version 4, Src: 65.61.137.117     0020  02 0f 1f 90 8a bc 05 8e  de bb aa 32 7d 73
› Transmission Control Protocol, Src Port: 8080,      0030  ff ff 22 d7 00 00 00 00  00 00 00 00
```

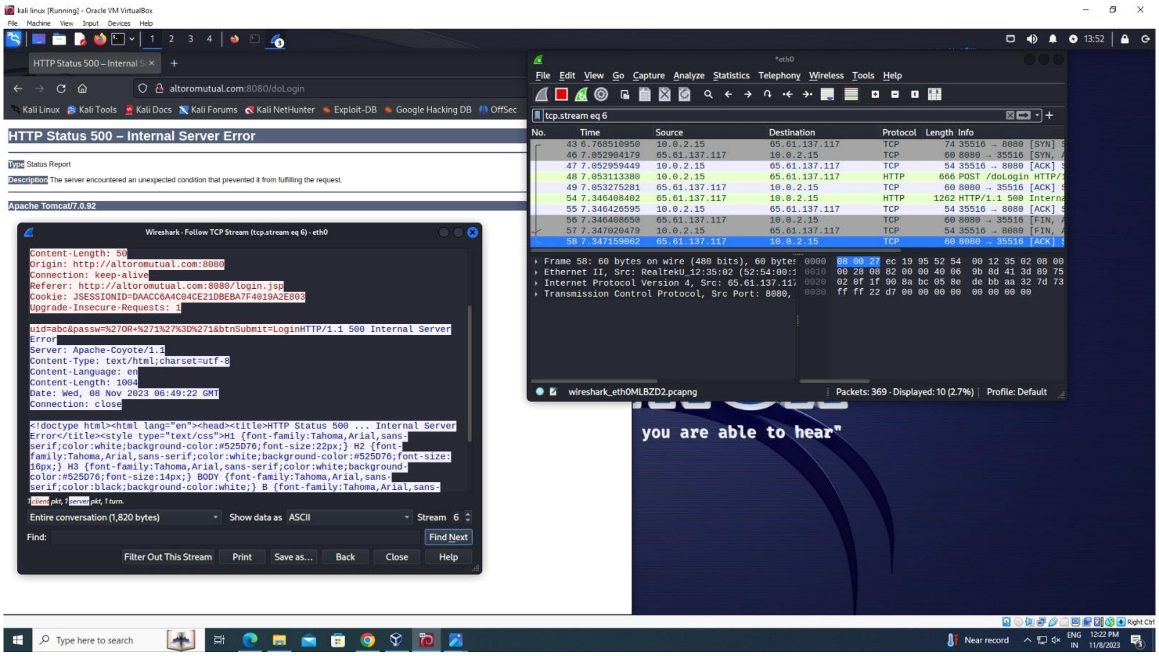
wireshark_eth0MLBZD2.pcapng | Packets: 369 · Displayed: 10 (2.7%) | Profile: Default

Type here to search   Near record   ENG IN 12:22 PM 11/8/2023

Description:-SQL injection occurs when hackers input harmful SQL commands into website forms, allowing them to control databases, access, alter, or delete crucial data. This compromises system integrity and security significantly.

Remediation:-To prevent SQL injection, use prepared statements and parameterized queries, validating and sanitizing user inputs before executing any SQL queries, ensuring a secure way to interact with the database and protecting against potential attacks.

Capturing Passwords With WireShark:-


kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
HTTP Status 500 – Internal S
altoromutual.com:8080/doLogin
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
13:52
you are able to hear"
Type here to search
Near record
ENG IN
12:22 PM 11/8/2023
Right Ctrl

HTTP Status 500 – Internal Server Error

Type Status Report

Description The server encountered an unexpected condition that prevented it from fulfilling the request.

Apache Tomcat/7.0.92

Wireshark · Follow TCP Stream (tcp.stream eq 6) · eth0

```
Content-Length: 50
Origin: http://altoromutual.com:8080
Connection: keep-alive
Referer: http://altoromutual.com:8080/login.jsp
Cookie: JSESSIONID=DAACC6A4C04CE21DBEBA7F4019A2E803
Upgrade-Insecure-Requests: 1

uid=abc&passw=%27OR+%271%27%3D%271&btnSubmit=LoginHTTP/1.1 500 Internal Server
Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Language: en
Content-Length: 1004
Date: Wed, 08 Nov 2023 06:49:22 GMT
Connection: close

<!doctype html><html lang="en"><head><title>HTTP Status 500 ... Internal Server
Error</title><style type="text/css">H1 {font-family:Tahoma,Arial,sans-
serif;color:white;background-color:#525D76;font-size:22px;} H2 {font-
family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:
16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-
color:#525D76;font-size:14px;} BODY {font-family:Tahoma,Arial,sans-
serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-
```

1 client pkt, 1 server pkt, 1 turn.

Entire conversation (1,820 bytes) Show data as ASCII Stream 6

Find: Find Next

Filter Out This Stream | Print | Save as… | Back | Close | Help

*eth0

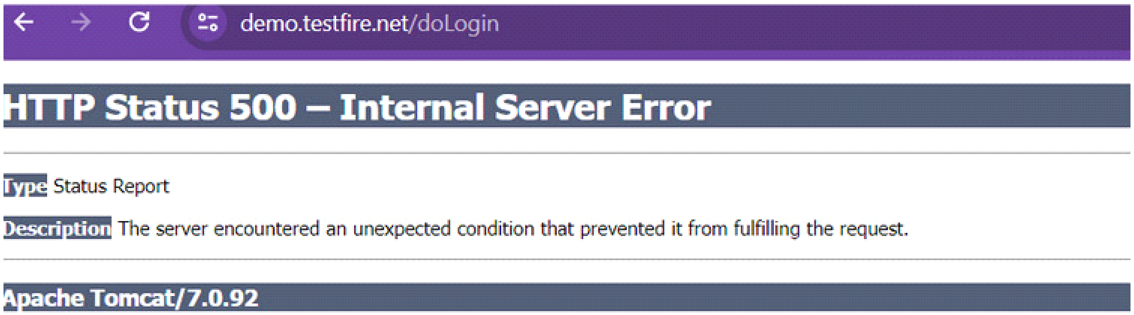
tcp.stream eq 6

```
No.  Time         Source         Destination    Protocol Length Info
  43 6.768510950  10.0.2.15      65.61.137.117  TCP        74 35516 → 8080 [SYN] S
  46 7.052904179  65.61.137.117  10.0.2.15      TCP        60 8080 → 35516 [SYN, A
  47 7.052959449  10.0.2.15      65.61.137.117  TCP        54 35516 → 8080 [ACK] S
  48 7.053113380  10.0.2.15      65.61.137.117  HTTP      666 POST /doLogin HTTP/1
  49 7.053275281  65.61.137.117  10.0.2.15      TCP        60 8080 → 35516 [ACK] S
  54 7.346408402  65.61.137.117  10.0.2.15      HTTP     1262 HTTP/1.1 500 Interna
  55 7.346426595  10.0.2.15      65.61.137.117  TCP        54 35516 → 8080 [ACK] S
  56 7.346408650  65.61.137.117  10.0.2.15      TCP        60 8080 → 35516 [FIN, A
  57 7.347020479  10.0.2.15      65.61.137.117  TCP        54 35516 → 8080 [FIN, A
  58 7.347159062  65.61.137.117  10.0.2.15      TCP        60 8080 → 35516 [ACK] S
```

```
› Frame 58: 60 bytes on wire (480 bits), 60 bytes    0000  08 00 27 ec 19 95 52 54  00 12 35 02 08 00
› Ethernet II, Src: RealtekU_12:35:02 (52:54:00:1    0010  00 28 08 82 00 00 40 06  9b 8d 41 3d 89 75
› Internet Protocol Version 4, Src: 65.61.137.117    0020  02 0f 1f 90 8a bc 05 8e  de bb aa 32 7d 73
› Transmission Control Protocol, Src Port: 8080,     0030  ff ff 22 d7 00 00 00 00  00 00 00 00
```

wireshark_eth0MLBZD2.pcapng | Packets: 369 · Displayed: 10 (2.7%) | Profile: Default

Apache Server Error:-



demo.testfire.net/doLogin

HTTP Status 500 – Internal Server Error

Type Status Report

Description The server encountered an unexpected condition that prevented it from fulfilling the request.

Apache Tomcat/7.0.92

Step-4:-Document Findings and Impacts

XSS(Cross-Site Scripting):-

Description:-Default credentials are pre-configured usernames and passwords provided by manufacturers or developers for initial access to devices or software.

Recommendation:

- Encode all user inputs before displaying them in the browser to prevent the execution of malicious scripts.
- Use Content Security Policy (CSP) to restrict the sources from which scripts can be loaded.
- Validate and sanitize all user inputs to remove any executable script content.

SQL Injection:-

Description:-SQL injection occurs when hackers input harmful SQL commands into website forms, allowing them to control databases, access, alter, or delete crucial data. This compromises system integrity and security significantly.

Recommendation:

- Use parameterized queries or prepared statements to interact with the database.
- Validate and sanitize all user inputs to ensure they do not contain malicious SQL code.
- Implement stored procedures for database operations.

Default Credential:-

Description:-Default credentials are pre-configured usernames and passwords provided by manufacturers or developers for initial access to devices or software.

recommandation:

- Upon first access, change the default credentials to a strong, unique password.
- Use passwords that are long (at least 12 characters) and include a mix of letters (both uppercase and lowercase), numbers, and special characters.
- Regularly monitor the default account for any unauthorized access attempts.

- Regularly use security scanners to check for the presence of default credentials in your network.
- Ensure compliance with internal security policies and industry standards regarding credential management.

Capturing Passwords With WireShark:-

Description:-In this vulnerability the username and password are being stolen by attacker using WireShark Tool.

Recommendations

- Ensure all web traffic uses HTTPS instead of HTTP. HTTPS encrypts data between the client and server, making it difficult for attackers to capture sensitive information.
- Use strong encryption protocols for all communication channels.
- Require MFA for all user logins. This adds an extra layer of security even if passwords are compromised.
- Implement strict access controls to limit who can capture network traffic. Ensure only authorized personnel have access to critical network segments.
- Keep detailed logs of network activity and regularly audit these logs for unusual patterns.

Apache Server Error:-

Description:-An Apache server error occurs when the web server encounters an issue processing a request, leading to error messages displayed on the website, indicating problems with server configurations or client requests.

Recommendations:-

- Check file permissions: Ensure the Apache user has the appropriate permissions to access the files and directories.
- Adjust Apache configuration: Ensure the Require directive or AllowOverride is set correctly in your configuration files.
- Verify file paths: Ensure the file or directory exists at the specified path.

- Review proxy settings: Verify the ProxyPass and ProxyPassReverse directives in your Apache configuration.
- Check backend server: Ensure the backend server is running and accessible.