



**VISHWAKARMA**  
**UNIVERSITY**  
*Maximising Human Potential*

**[Application  
Security]**

**S. Y. B. Tech Computer Engineering  
Project 1**

**By  
Shivprasad  
Chavan  
202201623**

**2023-2024**

**Pursued in  
Department of Computer Engineering  
Faculty of Science & Technology  
Vishwakarma University, Pune**

## **PROBLEM STATEMENT:**

- Demonstrate a session replay attacks on Global Bank is seeking a skilled developer to create a web application that offers a comprehensive understanding of session management, utilizing the latest technologies and techniques using Man IN the Middle Attack.

## **Introduction:**

- A man-in-the-middle (MITM) attack in the context of session management is a form of cyber attack where a malicious actor intercepts and possibly alters communication between two parties, such as a user and a server, during a session. In this attack, the attacker positions themselves between the communicating parties, secretly monitoring and potentially modifying the data exchanged.
- In the realm of session management, MITM attacks often target sessions established between a user and a server, such as during online banking, shopping, or accessing sensitive information. The attacker aims to gain unauthorized access to the session by eavesdropping on the communication, hijacking the session, or injecting malicious code to steal credentials or manipulate data. This breach compromises the confidentiality and integrity of the session, posing significant risks to both users and service providers. Effective encryption, secure protocols, and robust authentication mechanisms are essential defenses against MITM attacks in session management.

## **Objectives:**

The objective of a man-in-the-middle (MITM) attack in session management is to intercept and manipulate communication between two parties, such as a user and a server, during a session. By positioning themselves covertly between the communicating entities, the attacker seeks to eavesdrop on the data exchanged, hijack the session, or inject malicious code to compromise the confidentiality and integrity of the session. This attack aims to gain unauthorized access to sensitive information, such as login credentials or financial transactions, posing significant risks to both users and service providers. Preventative measures include implementing encryption, secure protocols, and robust authentication mechanisms to thwart MITM attacks and ensure the security of sessions.

## **TECHNOLOGY Used:**

**Packet Sniffing Tools:** Attackers may use packet sniffing software like Wireshark or tcpdump to intercept and analyze data packets passing through the network. Packet sniffing tools are software applications designed to intercept and analyze data packets traveling over a network. These tools work by capturing packets as they pass through network interfaces, allowing users to inspect the contents of the packets, including their headers and payloads. Packet sniffers are commonly used for network troubleshooting, security analysis, and performance monitoring.

## **ALGORITHM:**

**Wireshark** is a widely-used packet sniffing and network analysis tool that allows users to capture, analyze, and troubleshoot network traffic in real-time. Developed as an open-source project, Wireshark is available for various operating systems, including Windows, macOS, and Linux.

### **Key features of Wireshark include:**

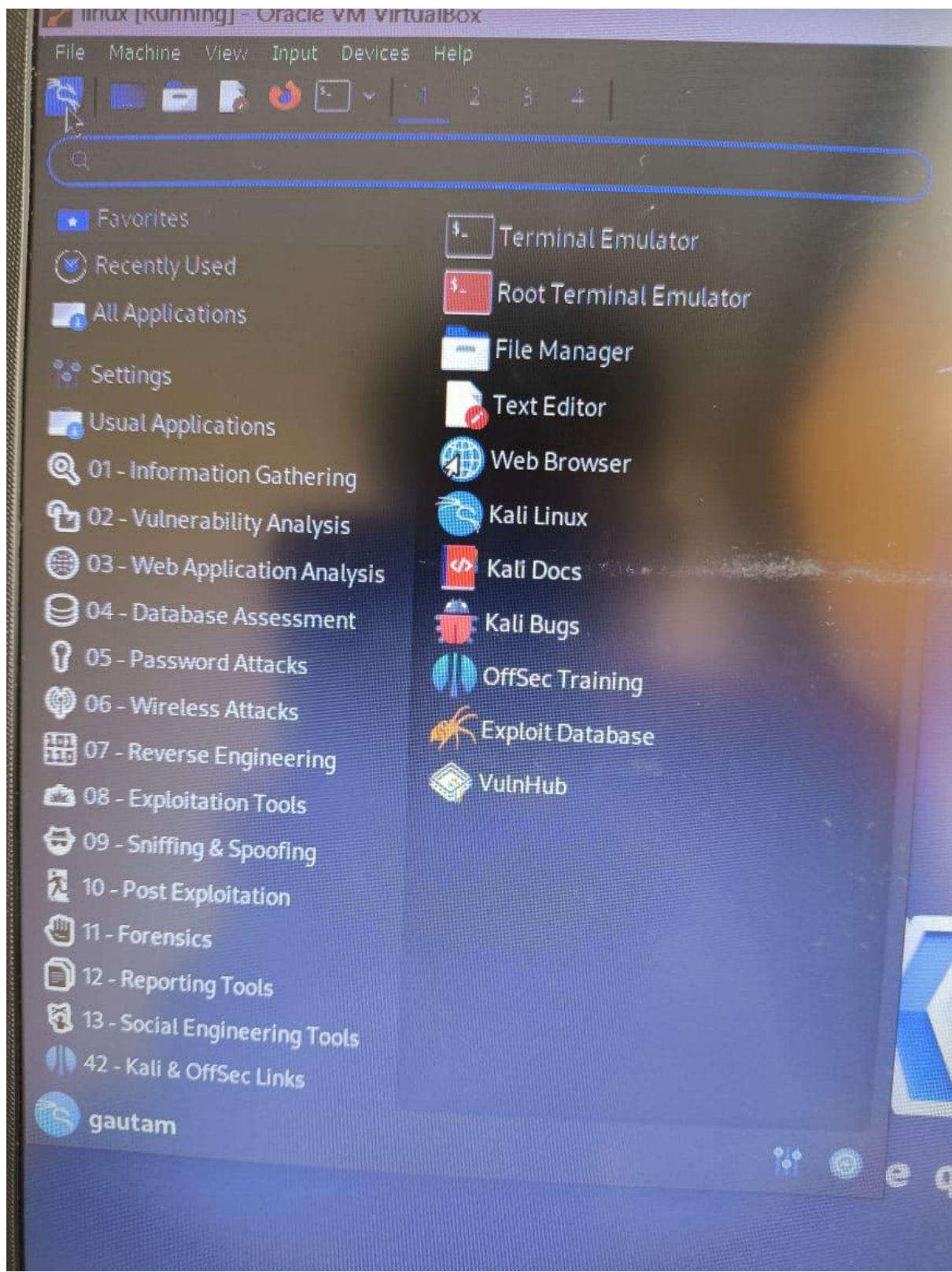
- **Packet Capture:** Wireshark can capture live network traffic from Ethernet, Wi-Fi, Bluetooth, USB, and other network interfaces. It can also read captured files from other packet capture utilities.
- **Protocol Support:** Wireshark supports a vast array of network protocols, ranging from common ones like TCP, UDP, and HTTP to more specialized protocols used in industrial control systems and telecommunications.
- **Deep Packet Inspection:** Wireshark provides detailed information about each captured packet, including its source and destination addresses, packet type, protocol, and payload data.
- **Packet Filtering and Search:** Users can apply filters to focus on specific types of traffic or search for packets containing particular data patterns.
- **Packet Analysis:** Wireshark offers powerful analysis tools, such as packet decoders, flow graphs, and statistics, to help users understand network behavior, identify performance issues, and troubleshoot connectivity problems.
- **Exporting Data:** Users can export captured packets or analysis results in various formats for further investigation or reporting.

## Attack Explanation:

- Set-up Kali Linux

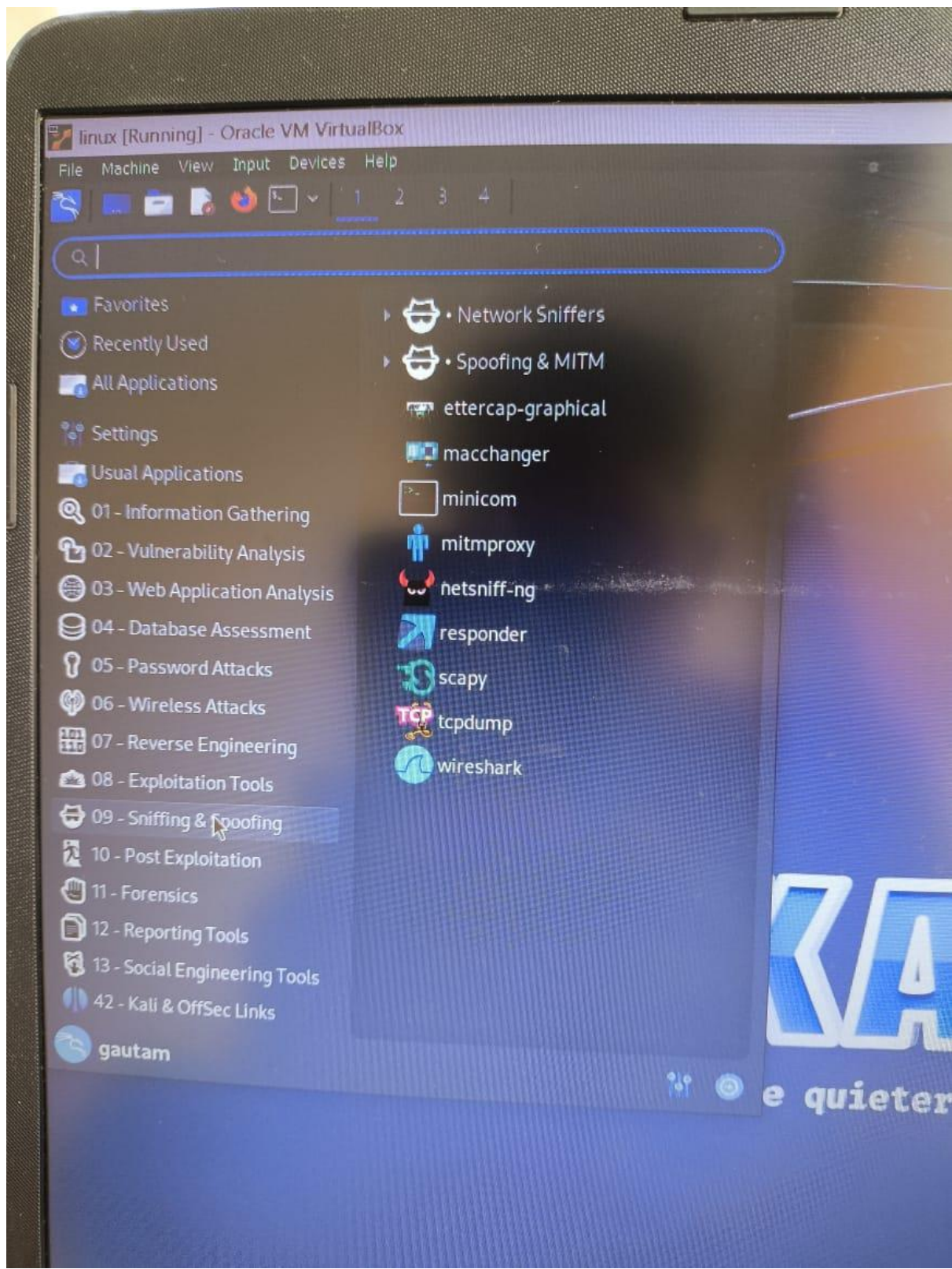


- Go to Applications and Search for a sniffing and spoofing tool

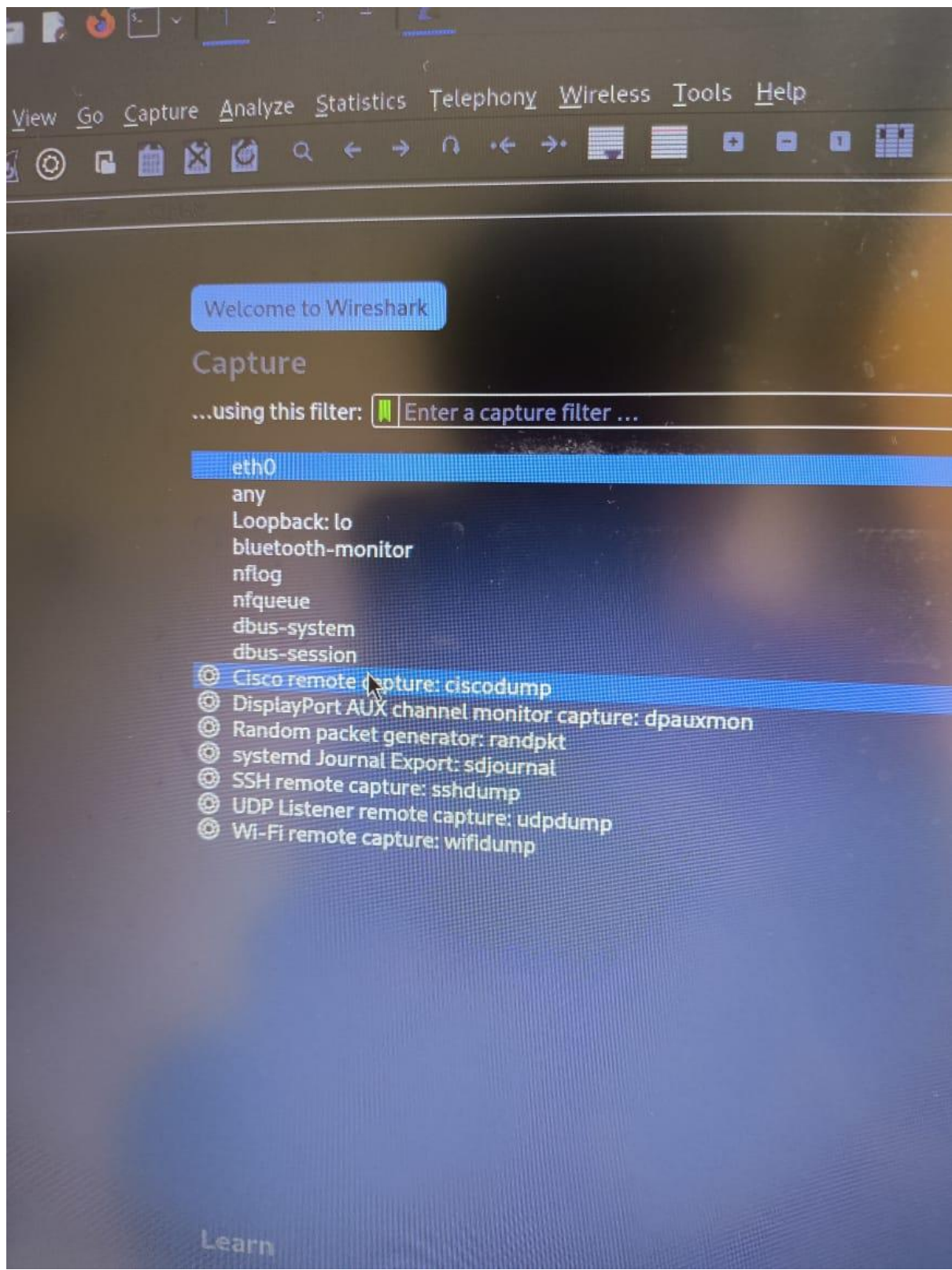


- We will use WireShark



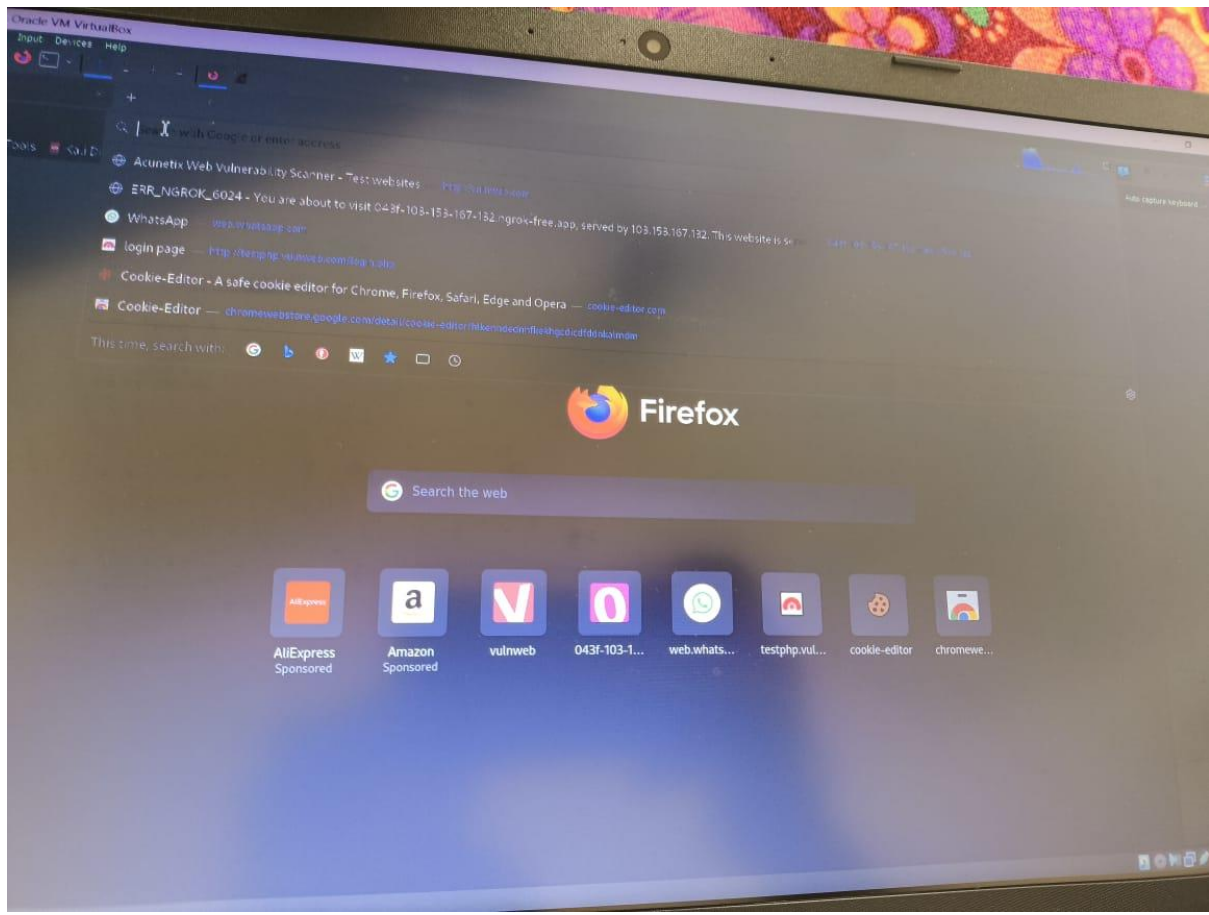


- Start wireshark



- Open your Firefox Browser in another tab





- Search for a vulnerable website to attack ... We will go with [vulnweb.com](http://vulnweb.com)

| Name           | URL   | Technologies                       | Resources   |
|----------------|---|------------------------------------|---|
| SecurityTweets | <a href="http://testhtml5.vulnweb.com">http://testhtml5.vulnweb.com</a>   | nginx, Python, Flask, CouchDB      | <a href="#">Review</a> Acunetix HTML5 scanner or <a href="#">learn more</a> on the topic.   |
| Acuart         | <a href="http://testphp.vulnweb.com">http://testphp.vulnweb.com</a>       | Apache, PHP, MySQL                 | <a href="#">Review</a> Acunetix PHP scanner or <a href="#">learn more</a> on the topic.     |
| Acuforum       | <a href="http://testasp.vulnweb.com">http://testasp.vulnweb.com</a>       | IIS, ASP, Microsoft SQL Server     | <a href="#">Review</a> Acunetix SQL scanner or <a href="#">learn more</a> on the topic.     |
| Acublog        | <a href="http://testaspnet.vulnweb.com">http://testaspnet.vulnweb.com</a> | IIS, ASP.NET, Microsoft SQL Server | <a href="#">Review</a> Acunetix network scanner or <a href="#">learn more</a> on the topic. |
| REST API       | <a href="http://rest.vulnweb.com/">http://rest.vulnweb.com/</a>           | Apache, PHP, MySQL                 | <a href="#">Review</a> Acunetix scanner or <a href="#">learn more</a> on the topic.         |

**Warning:** This site hosts intentionally vulnerable web applications. You can use these applications to understand how programming and configuration errors lead to security breaches. We created the site to help you test Acunetix but you may also use it for manual penetration testing or for educational purposes. It will help you learn about vulnerabilities such as SQL Injection, Cross-site Scripting (XSS), Cross-site Request Forgery (CSRF), and many more.

- Open the second link

← → ↻ 🏠 testphp.vulnweb.com/login.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

**acunetix** **acuart**

TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)

**search art**

[Browse categories](#)  
[Browse artists](#)  
[Your cart](#)  
[Signup](#)  
[Your profile](#)  
[Our guestbook](#)  
[AJAX Demo](#)

**Links**  
[Security art](#)  
[PHP scanner](#)  
[PHP vuln help](#)  
[Privacy policy](#)

If you are already registered please enter your login information below:

Username :   
 Password :

You can also [signup here](#).  
 Signup disabled. Please use the username **test** and the password **test**.

**Warning:** This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how Acunetix works and how it can be used to find vulnerabilities in your web sites. You can use it to test your web sites for vulnerabilities. Look for potential SQL injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

Personal information:  
 Username:   
 Password:



You can also [signup here](#).  
 Signup disabled. Please use the username **test** and the password **test**.

[your cart](#)  
[Signup](#)  
[Your profile](#)  
[Our guestbook](#)

- Signup with any id pass or you can use by-default one “test”.. I have used “**gautam**” as id and “**gautam**” as password

← → ↻ 🏠 testphp.vulnweb.com/login.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

TEST and Demonstration site for [Acunetix Web Vulnerability Scanner](#)

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#) [Logout test](#)

search art

[Browse categories](#)  
[Browse artists](#)  
[Your cart](#)  
[Signup](#)  
[Your profile](#)  
[Our guestbook](#)  
[AJAX Demo](#)  
[Logout](#)

Links

[Security art](#)  
[PHP scanner](#)  
[PHP vuln help](#)  
[Fractal Explorer](#)

If you are already registered please enter your login information below:

Username :

Password :

You can also [signup here](#).  
Signup disabled. Please use the username **test** and the password **test**.

[About Us](#) | [Privacy Policy](#) | [Contact Us](#) | ©2019 Acunetix Ltd

**Warning:** This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

- After login, It will show you Welcome Page





| No.  | Time         | Source        | Destination   | Protocol | Len  | Info                   |
|------|--------------|---------------|---------------|----------|------|------------------------|
| 38   | 2.162169474  | 10.0.2.15     | 34.107.221.82 | HTTP     | 3... | GET /success.txt?ip=4  |
| 42   | 2.253746808  | 34.107.221.82 | 10.0.2.15     | HTTP     | 2... | HTTP/1.1 200 OK (text) |
| 59   | 2.970400569  | 10.0.2.15     | 23.212.50.219 | OCSP     | 4... | Request                |
| 61   | 3.186112683  | 23.212.50.219 | 10.0.2.15     | OCSP     | 9... | Response               |
| 116  | 4.733905634  | 10.0.2.15     | 23.212.50.219 | OCSP     | 4... | Request                |
| 128  | 4.998111498  | 10.0.2.15     | 142.250.70.99 | OCSP     | 4... | Request                |
| 138  | 5.225608758  | 142.250.70.99 | 10.0.2.15     | OCSP     | 7... | Response               |
| 172  | 5.399228913  | 23.212.50.219 | 10.0.2.15     | OCSP     | 9... | Response               |
| 184  | 5.779608097  | 10.0.2.15     | 23.212.50.219 | OCSP     | 4... | Request                |
| 203  | 5.951464352  | 23.212.50.219 | 10.0.2.15     | OCSP     | 9... | Response               |
| 207  | 5.959891846  | 10.0.2.15     | 23.212.50.219 | OCSP     | 4... | Request                |
| 209  | 5.970098242  | 10.0.2.15     | 23.212.50.234 | OCSP     | 4... | Request                |
| 225  | 6.162213513  | 23.212.50.219 | 10.0.2.15     | OCSP     | 9... | Response               |
| 226  | 6.162213985  | 23.212.50.234 | 10.0.2.15     | OCSP     | 9... | Response               |
| 869  | 10.537850100 | 10.0.2.15     | 23.212.50.219 | OCSP     | 4... | Request                |
| 871  | 10.539037880 | 10.0.2.15     | 23.212.50.234 | OCSP     | 4... | Request                |
| 977  | 10.753592503 | 10.0.2.15     | 23.212.50.234 | OCSP     | 4... | Request                |
| 1043 | 10.847916261 | 23.212.50.234 | 10.0.2.15     | OCSP     | 9... | Response               |
| 1104 | 11.141159480 | 23.212.50.219 | 10.0.2.15     | OCSP     | 9... | Response               |
| 1132 | 11.228958739 | 23.212.50.234 | 10.0.2.15     | OCSP     | 9... | Response               |

- After http filter you will get a list of few requests, inside that go for the one with post method

| No. | Time         | Source        | Destination   | Protocol | Len  | Info  |
|-----|--------------|---------------|---------------|----------|------|---|
| 629 | 9.928350666  | 10.0.2.15     | 104.18.5.159  | TCP      | 54   | 49248 → 443 [ACK] Seq=7235 Ack=277746 Win=65535 Len=0                 |
| 630 | 9.929103965  | 10.0.2.15     | 104.18.5.159  | TCP      | 54   | 49248 → 443 [ACK] Seq=7235 Ack=279198 Win=65535 Len=0                 |
| 631 | 10.047807153 | 10.0.2.15     | 142.250.70.99 | TCP      | 54   | 44900 → 80 [FIN, ACK] Seq=1 Ack=1 Win=64240 Len=0                     |
| 632 | 10.049344696 | 142.250.70.99 | 10.0.2.15     | TCP      | 60   | 80 → 44900 [ACK] Seq=1 Ack=2 Win=65535 Len=0                          |
| 633 | 10.089538453 | 10.0.2.15     | 8.8.8.8       | DNS      | 87   | Standard query 0xe0b2 A shavar.services.mozilla.com                   |
| 634 | 10.089986914 | 10.0.2.15     | 8.8.8.8       | DNS      | 87   | Standard query 0x82b0 AAAA shavar.services.mozilla.com                |
| 635 | 10.113898347 | 104.18.5.159  | 10.0.2.15     | TCP      | 2... | 443 → 49248 [PSH, ACK] Seq=279198 Ack=7235 Win=65535 Len=2904 [TCP se |

- Open the post method request

```

Frame 1757: 613 bytes on wire (4904 bits), 613 bytes captured (4904 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_98:f0:91 (08:00:27:98:f0:91), Dst: 52:54:00:12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 44.228.249.3
Transmission Control Protocol, Src Port: 33988, Dst Port: 80, Seq: 958, Ack: 5694, Len: 559
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
  Form item: "uname" = "gautam"
  Form item: "pass" = "gautam"

```

- As you can see it is the username and password that we have used