Modern Tools for Web Security to Data Protection

Shreya pardeshi Ankita Deshpande

Student Student

Symbiosis Skills and Professional University Symbiosis Skills and Professional University

Maharashtra, India Maharashtra, India

[**shreyapardeshi227@gmail.com**](mailto:shreyapardeshi227@gmail.com)[**ankitadeshpande2004@gmail.com**](mailto:ankitadeshpande2004@gmail.com)

Aditya Mane

Student

Symbiosis Skills and Professional University

Maharashtra, India

[**adityamane0411@gmail.com**](mailto:adityamane0411@gmail.com)

**ABSTRACT**

In an age of increasing cyber threats, this research paper addresses the importance of tools in strengthening cybersecurity measures in today's organizations. This study examines a variety of cyber security tools, including threat detection, vulnerability management, security information and event management (SIEM), encryption, identity and access management (IAM), incident response, and continuous monitoring.

It would emphasize the significance of leveraging advanced technologies to enhance security measures, detect vulnerabilities, and respond to cyber-attacks effectively. The abstract might delve into the diverse categories of cybersecurity tools, including network monitoring, intrusion detection and prevention, vulnerability assessment, and incident response tools. Additionally, it may touch upon the critical need for automation and artificial intelligence in cybersecurity tools to keep pace with the sophisticated tactics employed by cyber adversaries.

Overall, it aims to provide a concise overview of the pivotal role that cybersecurity tools play in safeguarding organizations and individuals from cyber risks in the contemporary digital landscape.

**Keywords:** Wireshark, Cybersecurity, Nmap, Information, SIEM

1. **INTRODUCTION**

In response to the escalating frequency and sophistication of cyber threats, this research paper delves into the imperative for cybersecurity education and training, emphasizing their role in cultivating a secure and privacy-conscious digital landscape. Acknowledging the lack of comprehensive guides and tools for designing effective cybersecurity curricula, the paper presents practical strategies from analysing existing study programs globally and collecting recommendations from renowned institutions [1].

Introducing the SPARTA Cybersecurity Skills Framework [1], the paper bridges the gap between the job market requirements and educational offerings, facilitating the development of curricula aligned with industry needs. Additionally, it discusses the role of technology transition in deploying cutting-edge cybersecurity solutions to address the evolving threat landscape, emphasizing the importance of synergy among government agencies, private enterprises, and academia [2].

Furthermore, the paper explores the real-life applications of Generative AI (GAI) in cybersecurity [3], highlighting its potential to automate threat detection and enhance system robustness while addressing limitations such as periodic inaccuracies and susceptibility to misuse by malicious actors. Through these insights, the paper aims to contribute to advancing cybersecurity education and technology deployment practices in tackling emerging cyber threats effectively.

1. **Burp Suite**

* Burp Suite, a pivotal tool in cybersecurity, particularly web application security testing, offers robust solutions developed by PortSwigger.Its flagship feature, Burp Intruder, facilitates automated attacks on web applications, enabling security professionals to assess payload effectiveness against injection points [4].
* Here are some key aspects and features of Burp Suite [7]:

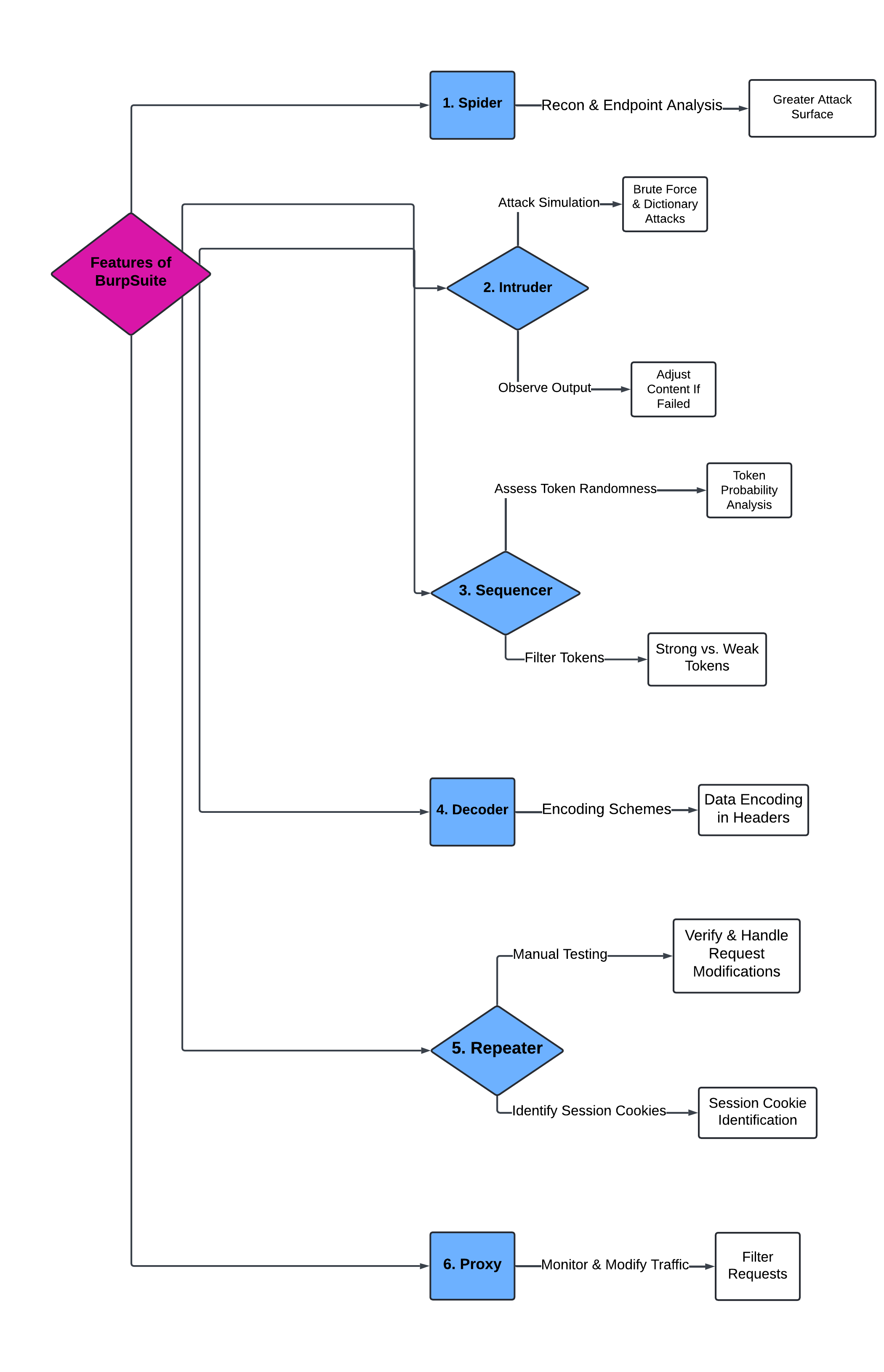


Figure 1: Features of Burp Suite

* Equipped with comprehensive analysis features like site maps and content discovery tools, Burp Suite aids in understanding application structures and pinpointing vulnerabilities.
* The below paper explores the utilization of Burp Suite in enhancing software security testing efficiency, emphasizing its ease of use, high efficient, and flexibility [4].
* Experimental findings underscore its capability to bolster accuracy and safeguard software systems from potential threats, making it an indispensable asset in realm of cybersecurity [4].

**B. Wireshark**

* Wireshark is a network protocol analyser that is embedded with powerful feature set.
* It was formerly known as Ethereal.
* Wireshark is a powerful network protocol analyser with capabilities for sniffing and logging network traffic.
* The potential of Wireshark is such that it can be developed into a robust Intrusion Detection System (IDS).
* It is an open-source tool that allows the developers to add functionalities according to their requirements.
* The utility of Wireshark as packet sniffing, logging and analysis helps the administrators to intercept and log traffic, decode and analyse packet content along with being equipped with sophisticated wireless protocol analysis.
* Wireshark is also equipped with user interface tools like capture and logging tools, prefiltering and analysis features, and post-sniffing analysis capabilities. These tools aid in filtering, monitoring and analysing network traffic.
* The full capabilities of Wireshark can be useful particularly in alert generation and heuristic development to further establish it as comprehensive intrusion detection software[5].

**C. Nmap**

* Nmap has been used by network administrators to detect server vulnerabilities and evaluate the performance of intrusion detection systems and firewalls. But at the same time, Nmap can be used as the scanning tool for the collection of information by attackers. So, some research has been done to utilize and detect Nmap.
* As a scanning tool, Nmap is very useful to collect information of remote hosts or verify the validity of the IDS. In, the authors focus on the operating system detection function of Nmap. They work with the Nmap tool for gathering information about the target operating system by matching the IP/TCP stacks with its built-in fingerprint database.
* The authors in use Nmap to complete specific tasks during the reconnaissance phase active scanning with the Nmap tool. Its port scan operation is used to find the open ports and services of the hosts on the internet to deal with the increase of massive Internet-connected devices.
* Some scholars also use Nmap as a penetration tool to verify the IDS’s performance and detect effects.
* Like most tools used for network security, Nmap is also a tool used to collect the network settings of the target computer to plan attacks by many hackers.
* So, it is necessary to detect Nmap scanning behaviour in the network. The detection approaches of such scanning tools mainly have two types: the novel detection methods and the comprehensive intrusion detection systems such as Snort and Suricata [6].

|  |  |  |  |
| --- | --- | --- | --- |
| Sr. No | Nmap Scan | Description | Keyword |
| 1. | TCP Connect Scan | Establishes a full TCP connection with the target ports to determine whether they are open, closed, or filtered by a firewall. | -sT |
| 2. | Syn Scan (Half-open Scan) | Sends SYN packets to the target ports without completing the TCP handshake. | -sS |
| 3. | UDP Scan | Sends UDP packets to the target ports to determine whether they are open or filtered. | -sU |
| 4. | ACK Scan | Sends ACK packets to the target ports and analyses the responses to determine whether the ports are filtered by a firewall. | -sA |
| 5. | Window Scan | Examines the TCP window size of the target ports to determine their state. | -sW |
| 6. | FIN Scan | Sends FIN packets to the target ports and analyses the responses to determine their state. | -sF |
| 7. | Null Scan | Sends TCP packets with no flags set to the target ports. | -sN |
| 8, | Idle Scan | Leverages a third-party system (idle zombie) to perform the scan, making it difficult to trace back to the original source. | -sI |
| 9, | Version Detection | Attempts to determine the versions of services running on the target ports by analysing their responses. | -sV |
| 10. | Script Scan | Utilizes Nmap scripts (NSE scripts) to perform various tasks such as vulnerability detection, service enumeration, and information gathering. | -sC |

1. **DISCUSSION ON SECURITY TOOLS**

**Table 1: Pros and Cons of Burp suite**

|  |  |  |
| --- | --- | --- |
| Sr. No | Advantages | Disadvantages |
|  | Comprehensive Testing Capabilities | Learning Curve |
| 1. | Offers a wide range of features for testing | Requires familiarity with HTTP protocols and web technologies |
| 2. | Supports both manual and automated testing | Free version has limited functionality |
| 3. | Proxy tool facilitates intercepting requests | Pro version can be expensive for some users |
| 4. | Allows for dynamic scanning of web applications | May generate false positives |
| 5. | Constant updates to keep up with new threats | Limited support for some less common web technologies |

**Table 2: Pros and Cons of Wireshark**

|  |  |  |
| --- | --- | --- |
| Sr. No | Advantages | Disadvantages |
| 1. | Powerful packet analysis capabilities | Steep learning curve for beginners |
| 2. | Comprehensive protocol support | May capture sensitive or private data |
| 3. | Open-source and free to use | Potential legal and privacy concerns |
| 4. | Active community support and updates | Can generate large capture files |
| 5. | Cross-platform compati |  |

**Table 3: Pros and Cons of Nmap**

|  |  |  |
| --- | --- | --- |
| Sr. No | Advantages | Disadvantages |
| 1. | Versatile, customizable | Requires technical expertise |
| 2. | Supports various protocols | May raise security alerts |
| 3. | Free, open-source | Illegal without authorization |
| 4. | Detailed scan reports | Network congestion potential |
| 5. | Active community, updates | Evasion and obfuscation vulnerabilities |
| 6. | Cross-platform compatibility | Limited OS and service detection |
| 7. | Integration with security tools | Time-consuming for large networks |

1. **RESULT**

In the context of modern cybersecurity, the utilization of sophisticated tools is imperative to fortify defenses against evolving cyber threats. Three prominent tools, namely Burp Suite, Wireshark, and Nmap, were investigated to showcase their integral roles in enhancing cybersecurity measures.

**A. Burp Suite**

A comprehensive web application security testing tool, demonstrated its prowess in identifying and mitigating vulnerabilities within web applications. Through the advanced features, such as automated scanning and real-time analysis of HTTP traffic, etc.

Step1: Manipulating Parameters with the Proxy Module for performing the Sniffing Attack

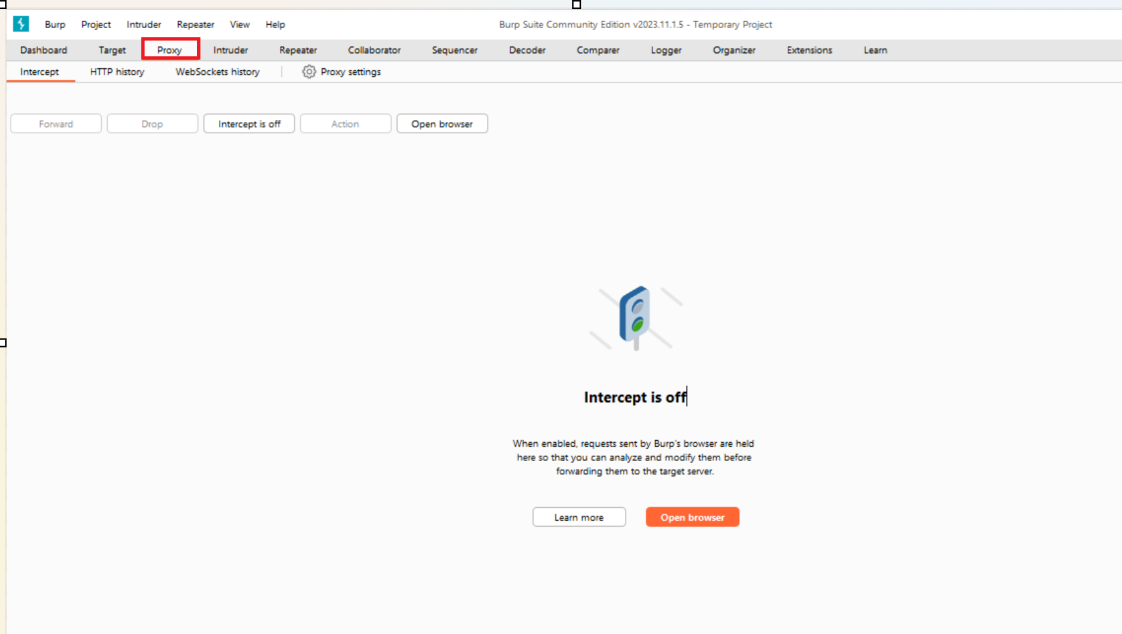


Figure 1**:** The Proxy Module is currently in a non-intercepting mode & not intercepting traffic.

Step 2: Launch the Firefox web browser

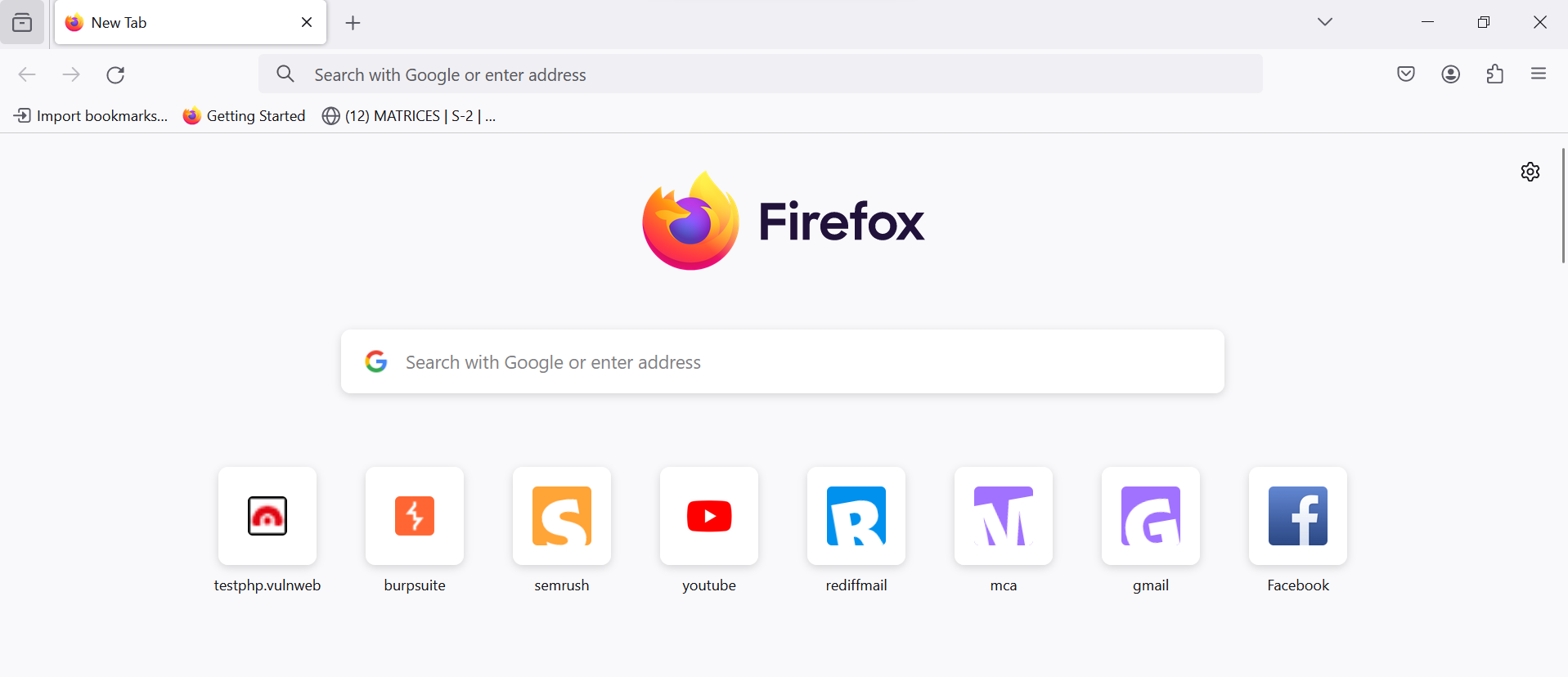


Figure 2: Firefox web browser

Step 3: Open the website through this link “<http://testphp.vulnweb.com/>”

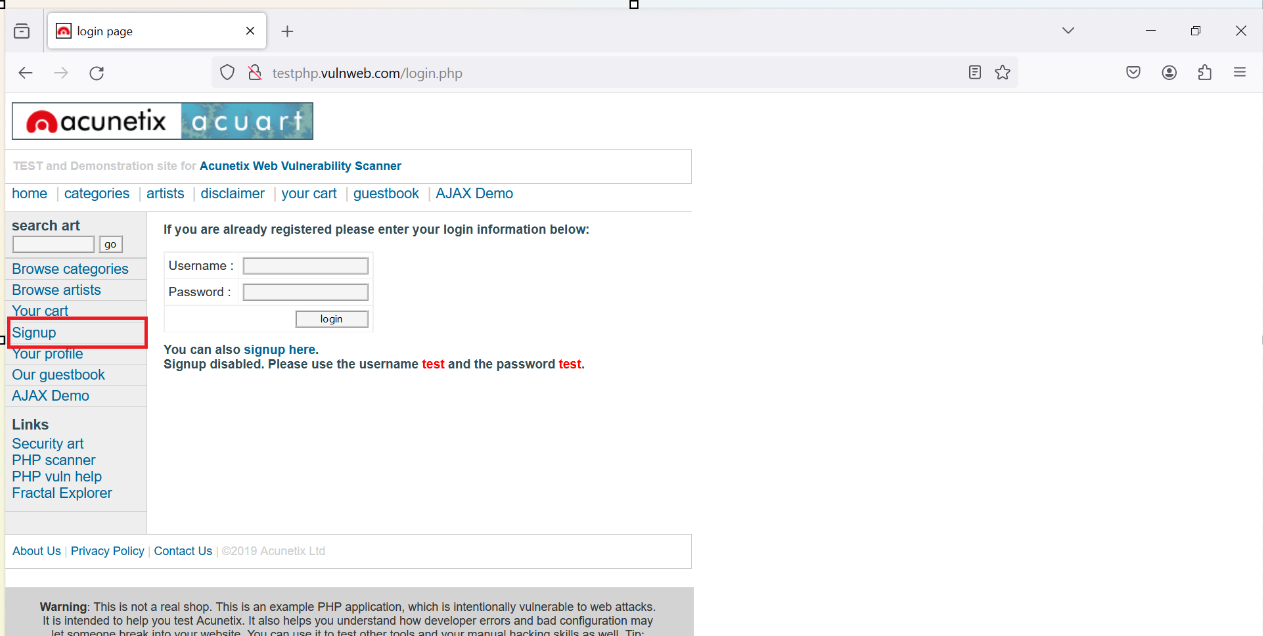
****

Figure 3: Navigate to a website that has known security vulnerabilities and then click on Signup option.

Step 4: Give the login credentials.

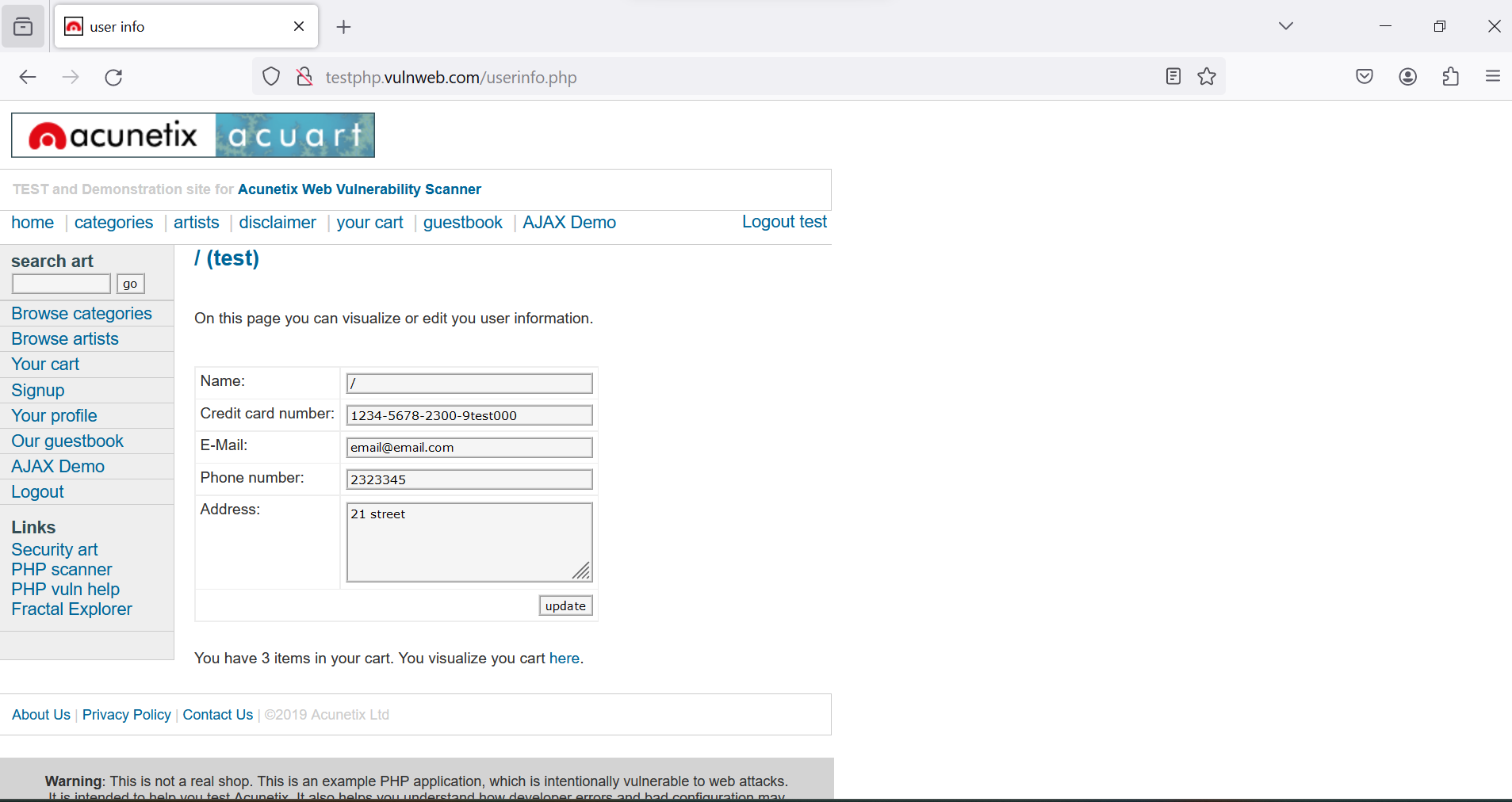


Figure 4: "Enter 'Test' into both the username and password fields on the login form, ensuring the intercept feature remains disabled.

Step 5: Click on “login”

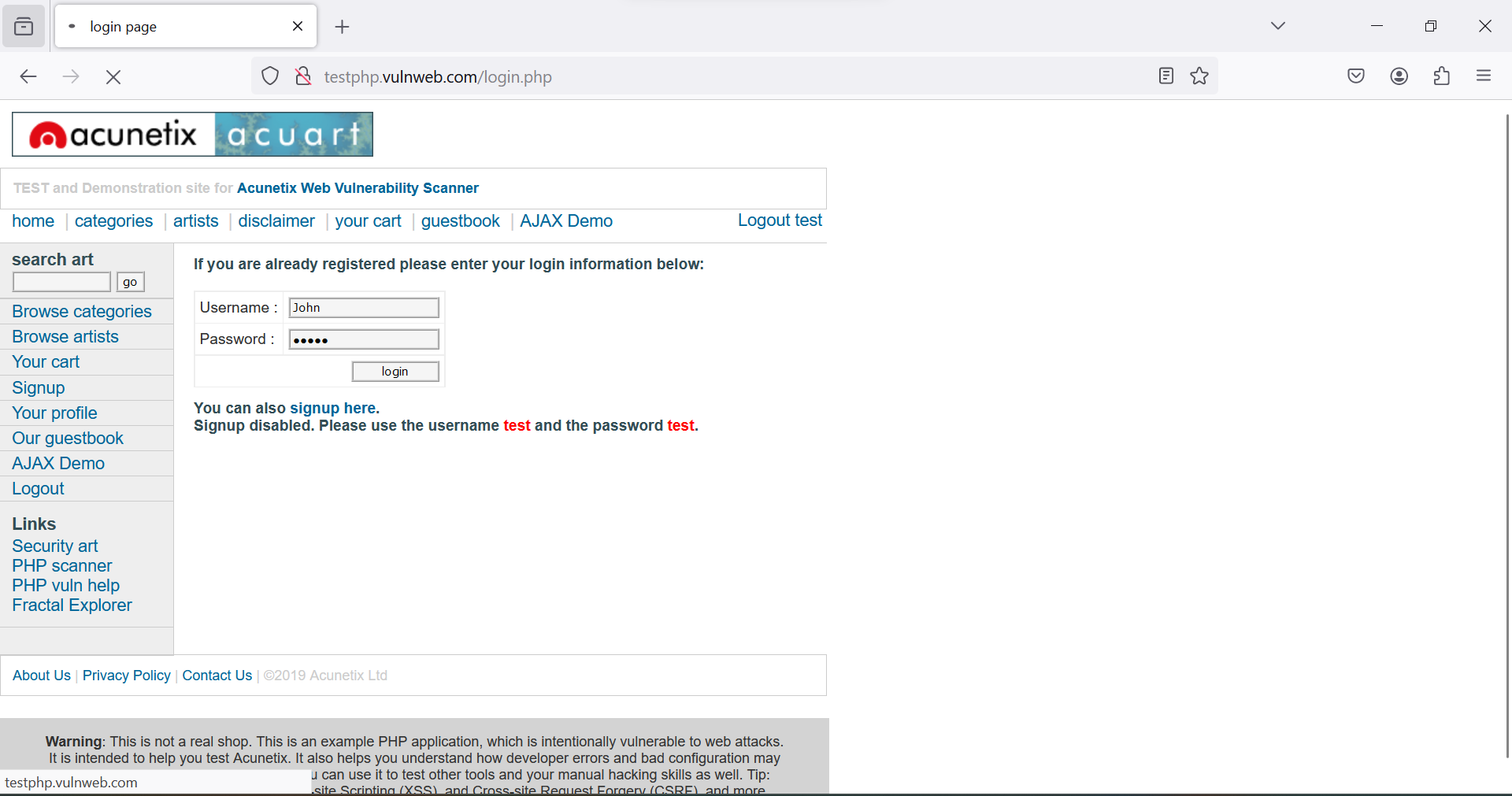


Figure 5: Type "John" into the username field and "12345" into the password field and on the intercept.

Step 6: Now go back to Burp Suite

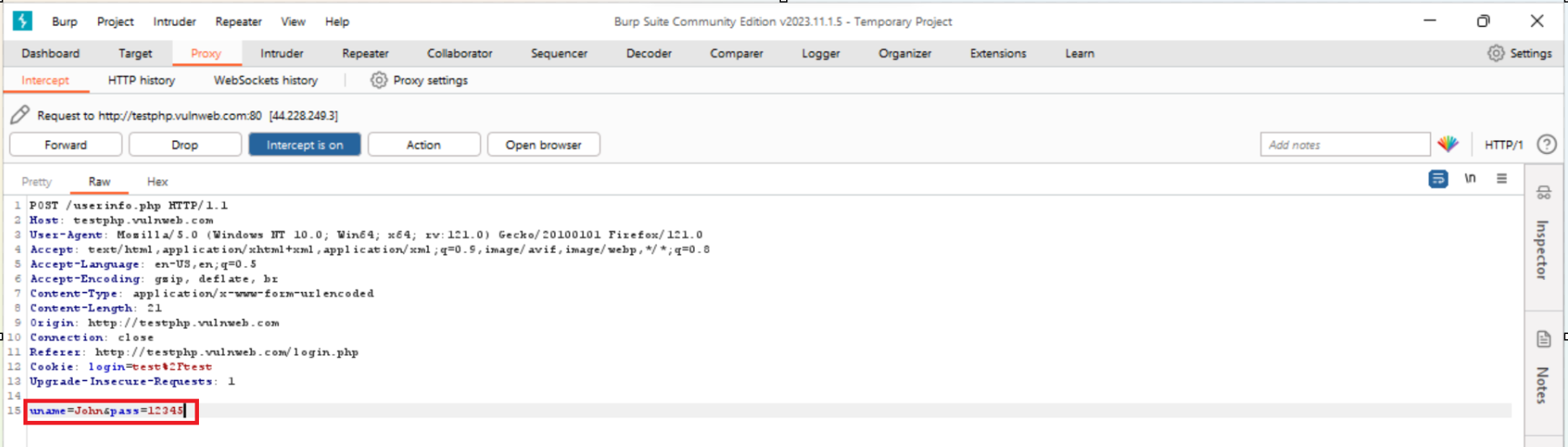


Figure 6: Burp Suite captured the following output after intercept was activated

Step 7: Go to Proxy section and select “Forward”.

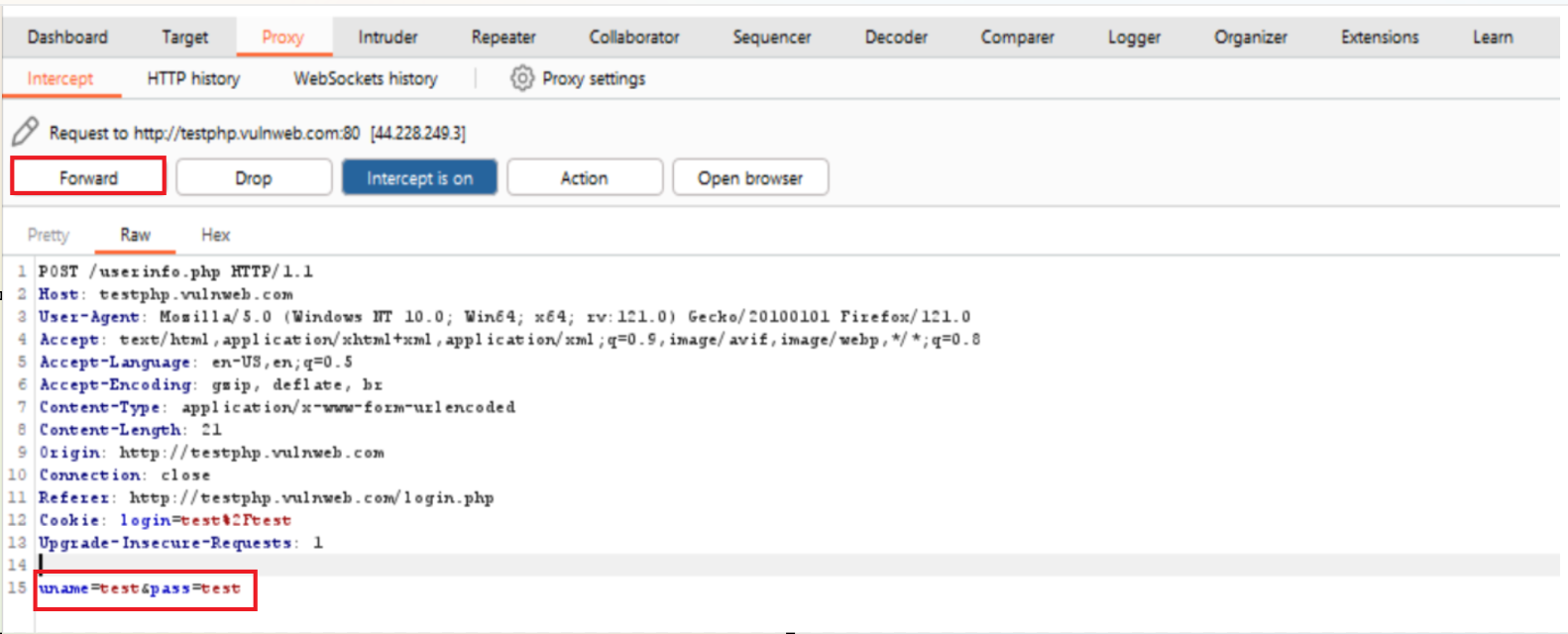


Figure 7: Locate the username and password fields within the intercepted request in Burp Suite's Intercept tab & then overwrite the existing values with "Test" in both fields. Click on the "Forward" button within Burp Suite to send the request with the altered credentials to the server

Step 8: After clicking on “Forward”.

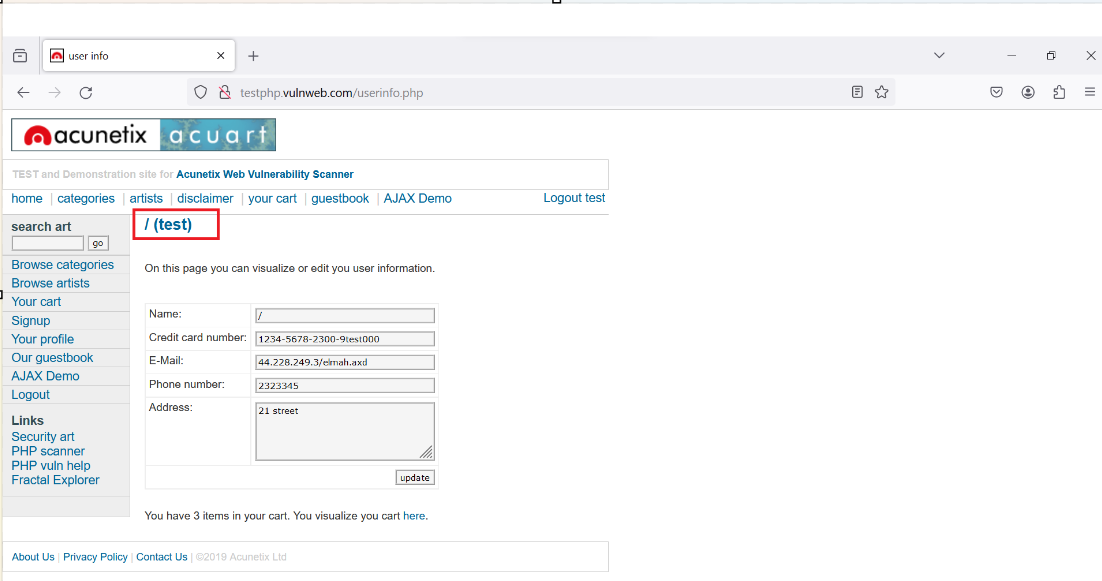
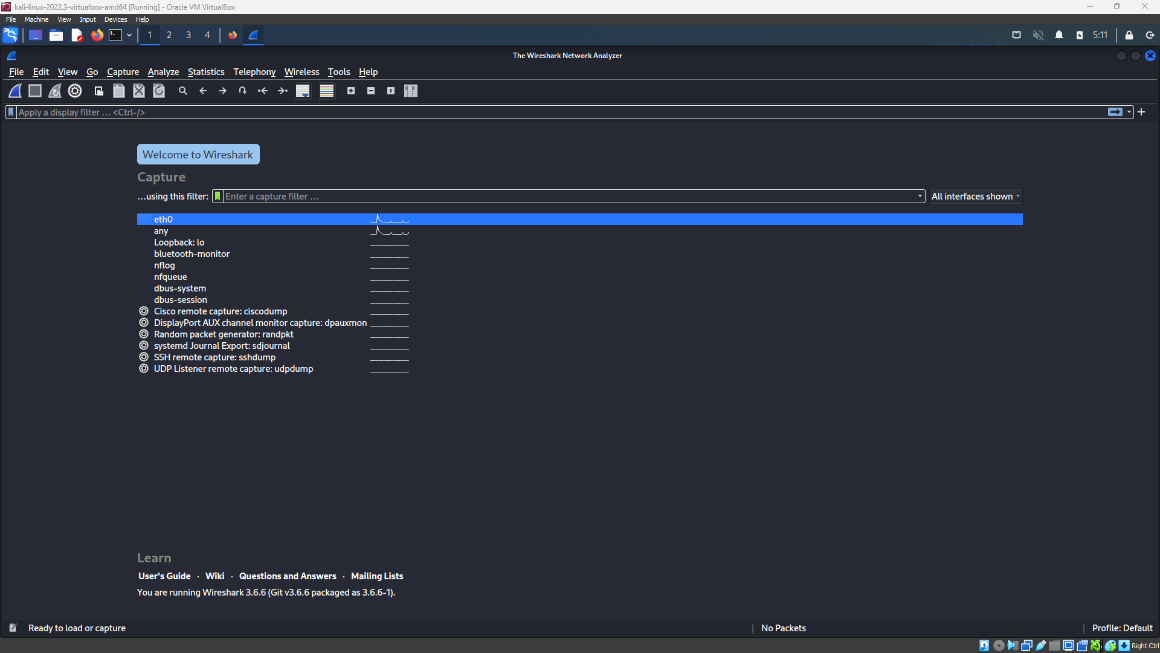


Figure 8: The modified request with the username 'Test' and password 'Test' resulted in a successful login

**B. Wireshark**

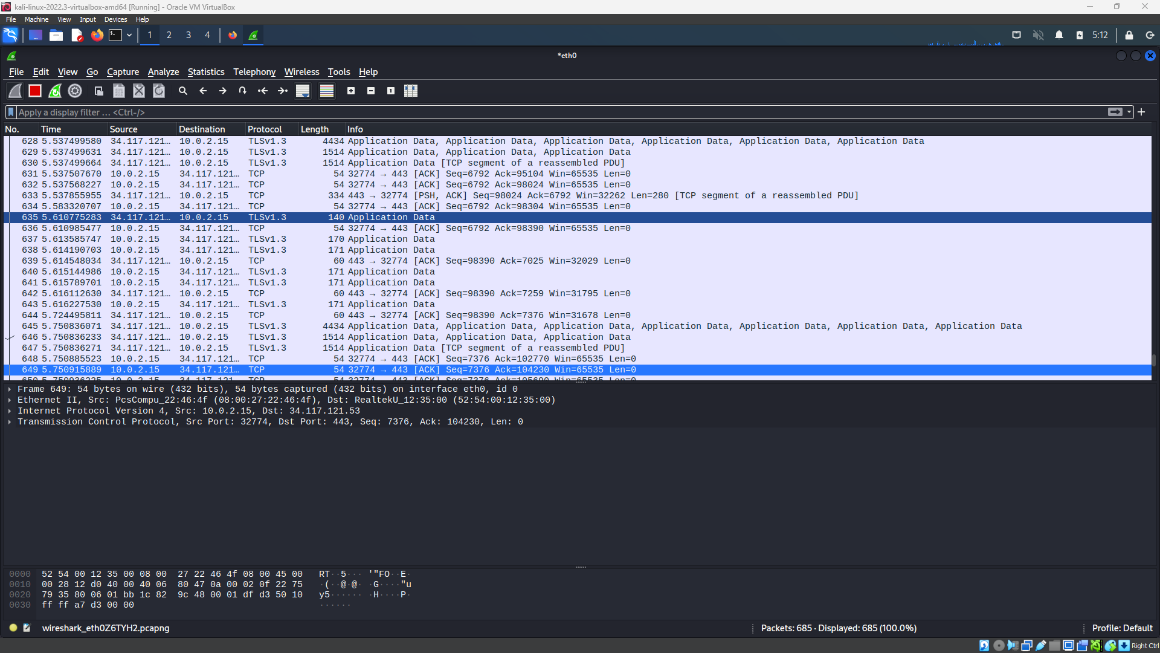
Wireshark, a powerful network protocol analyser, was employed to capture, dissect, and analyse network traffic. It’s real-time analysis capabilities provide deep insights into the communication patterns between network entities. The examination of captured packets, allows cybersecurity professionals to identify anomalies, potential security breaches, and unauthorized access attempts.

Step 1: Open Wireshark and select the eth0 option to capture packets over Wi-Fi or ethernet.



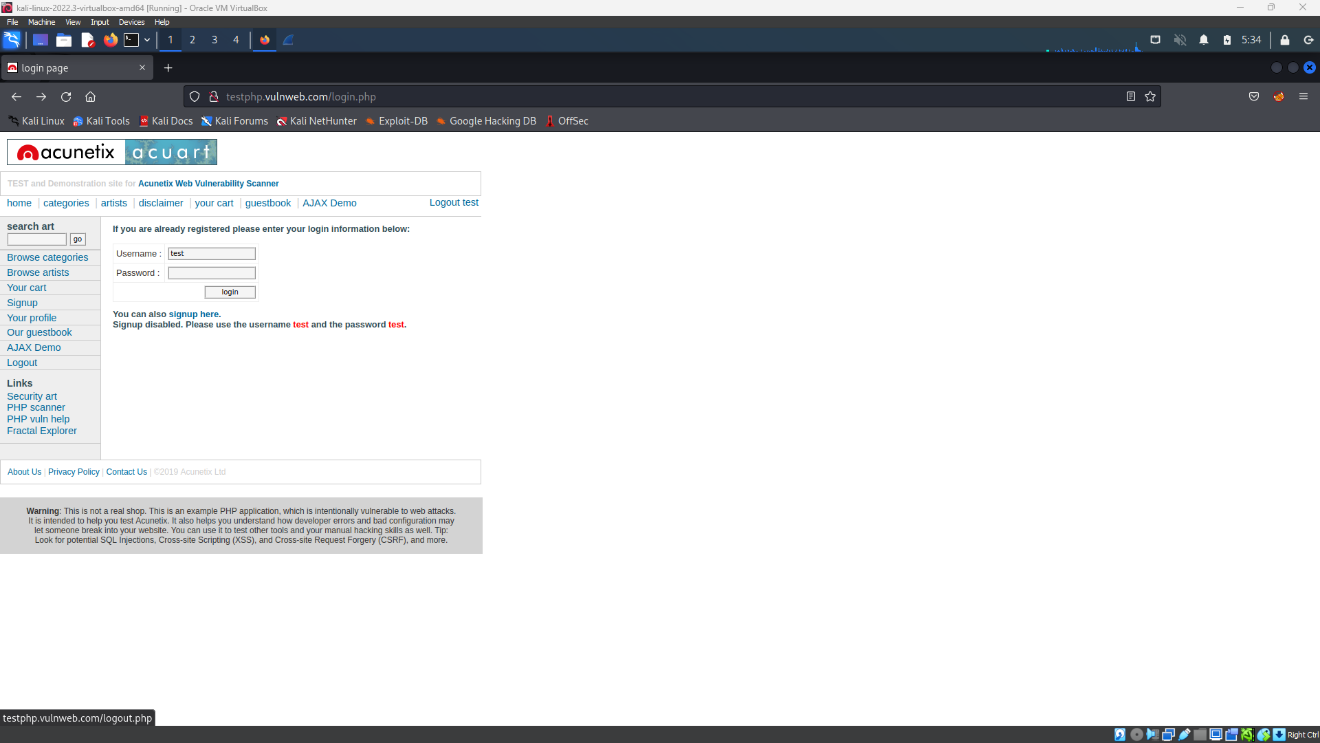
**Figure 9:** Opted for “eth0” option to start packet capturing

Step 2: Enter the interface and a list of network packets will be displayed



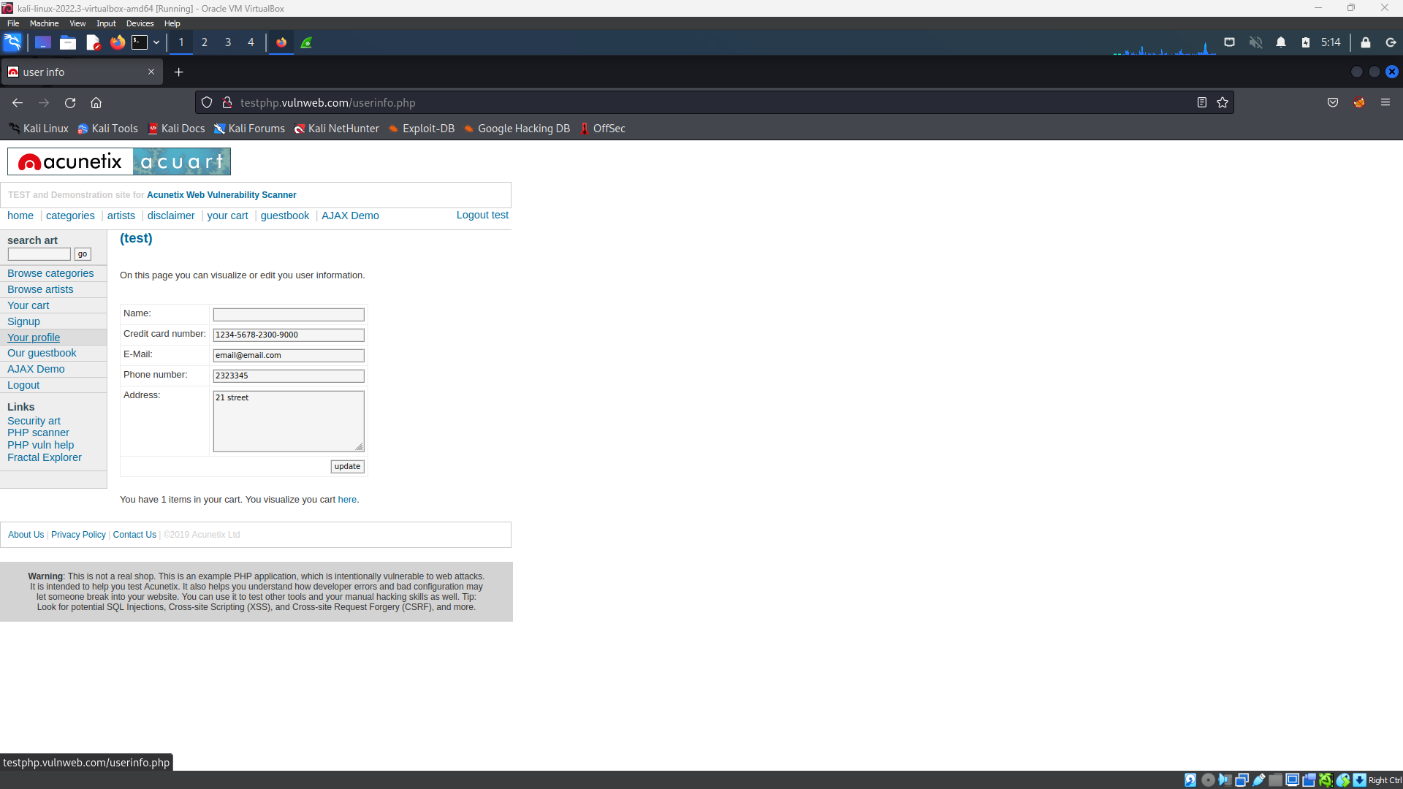
**Figure 10:** List of network packets is being displayed.

Step 3: While the Wireshark is capturing packets open the browser and search for <http://testphp.vulnweb.com/login.php>



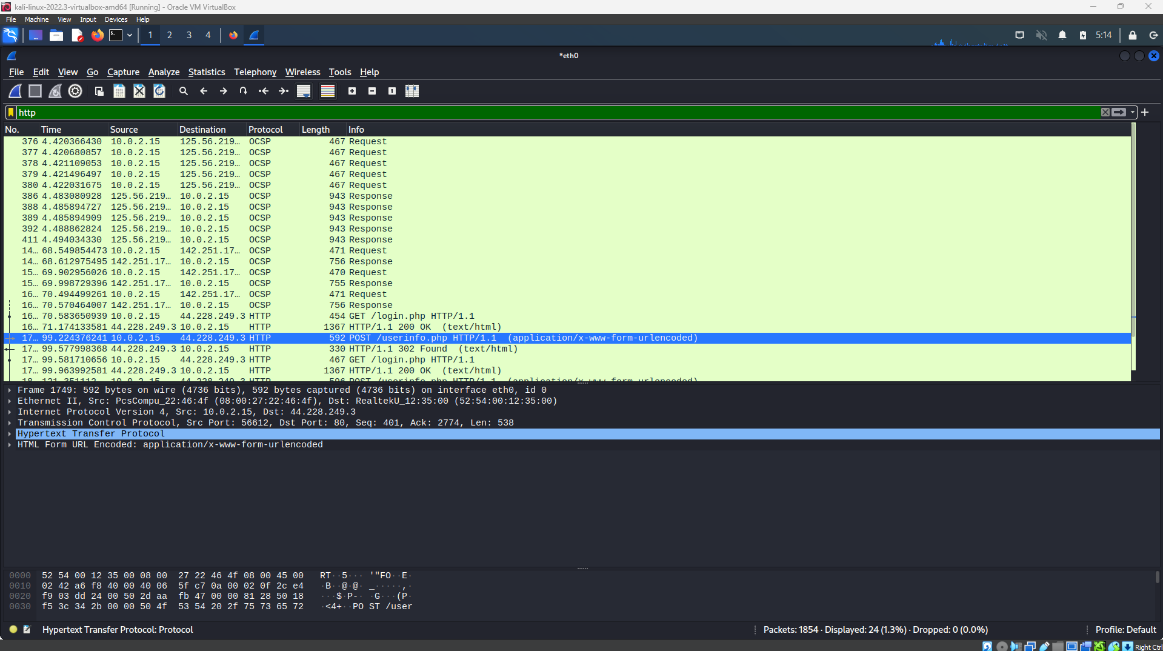
**Figure 11:** Interface of the test website

Step 4: Enter the login credentials given in the website and login



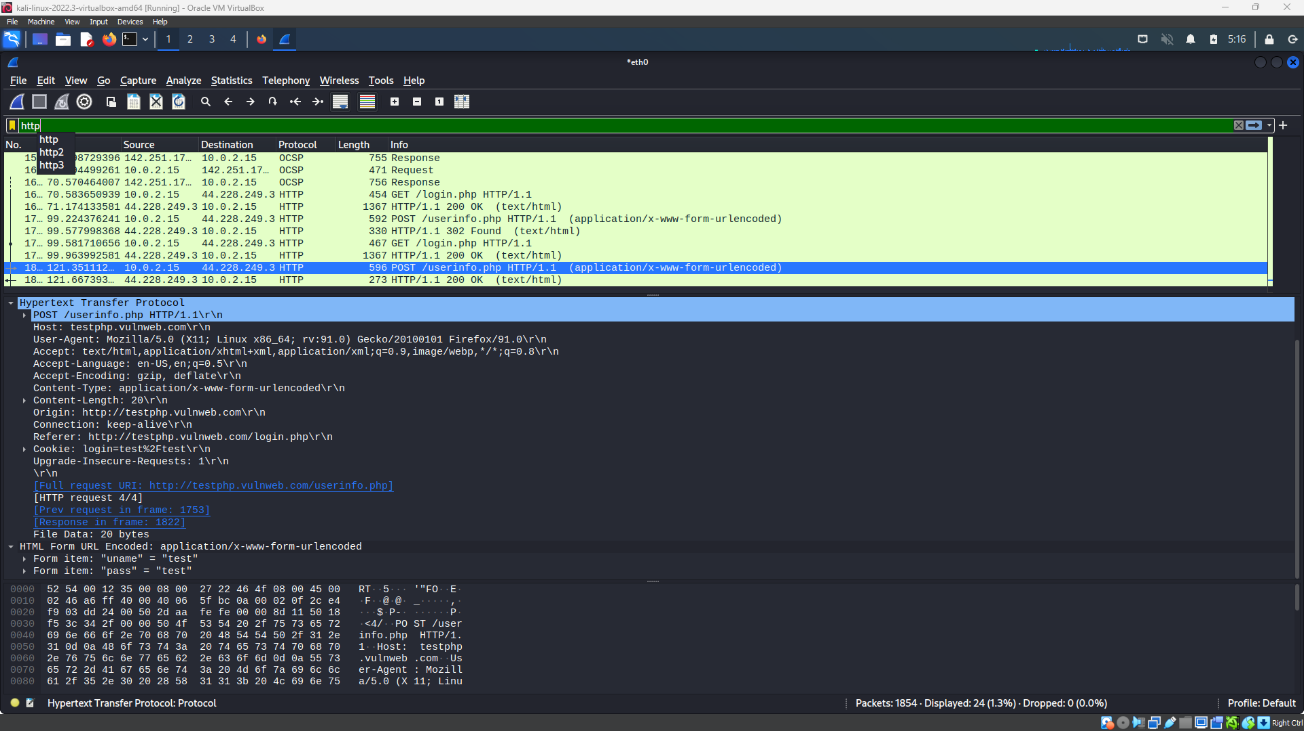
**Figure 12:** After login

Step 5: Go to Wireshark and search for “http” filter in the display packet search box



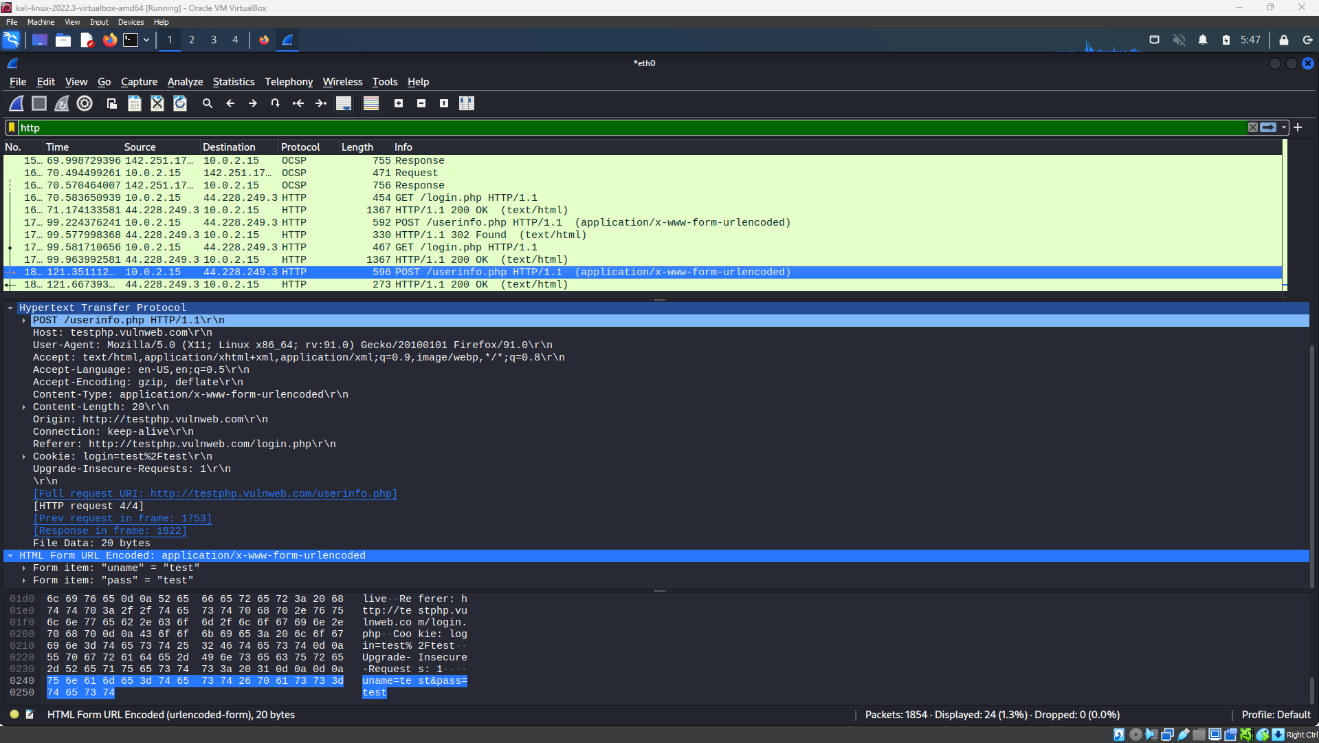
**Figure 13:** List of http packets is displayed

Step 6: Select the “userinfo.php” packet from the packets with http filter.



**Figure 14:** Details of the selected packet is displayed below the list of http packets.

Step 7: Then select “Hypertext Transfer Protocol” and “HTML Form URL Encoded” tab from the bottom menu. The selected tabs show the website from the which the packet is captured and also the username and password entered by the user.



**Figure 15:** The username and password of the user is displayed

**C.Nmap**

Step 1: Open Nmap and scan for IP address

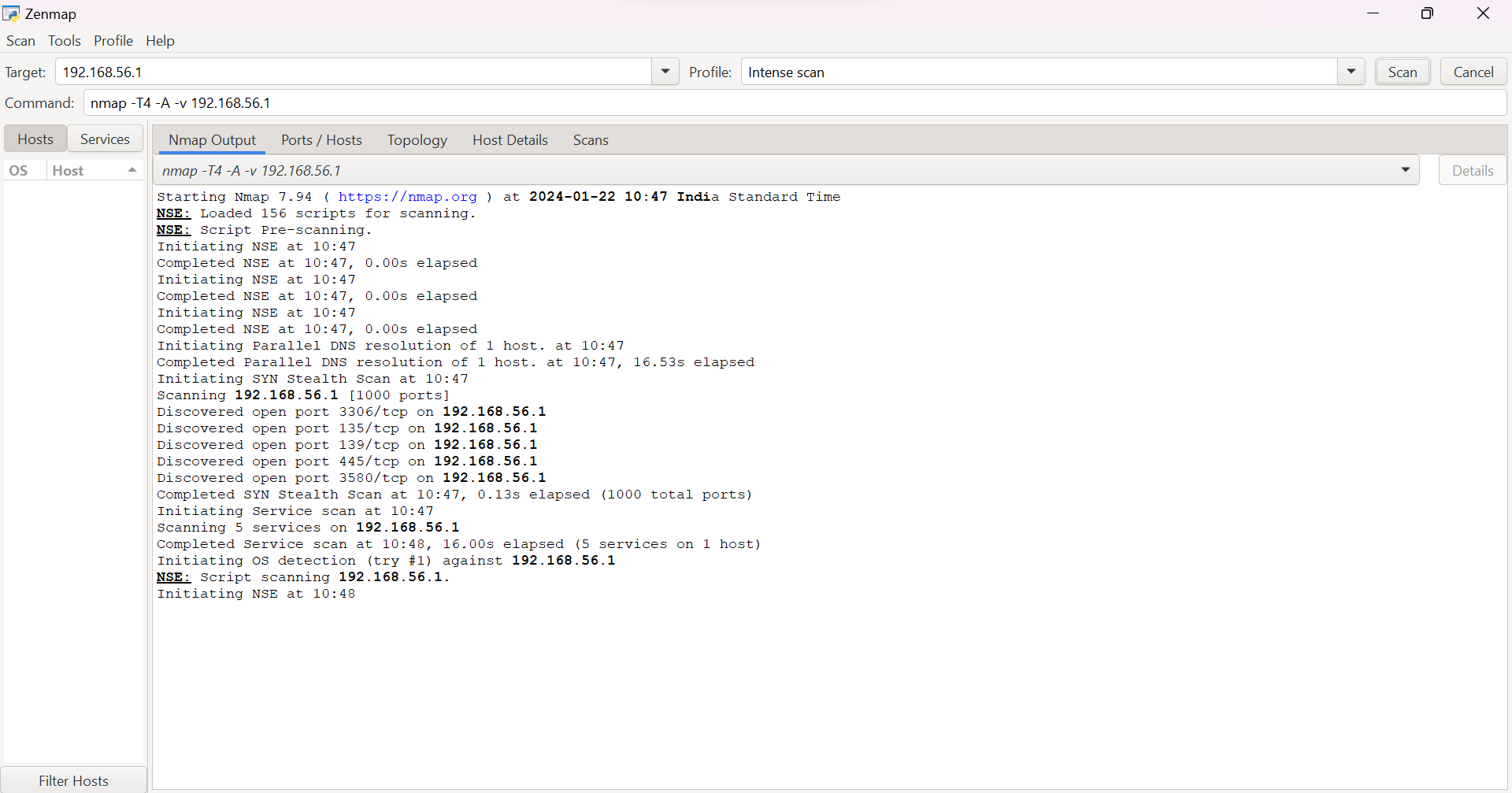
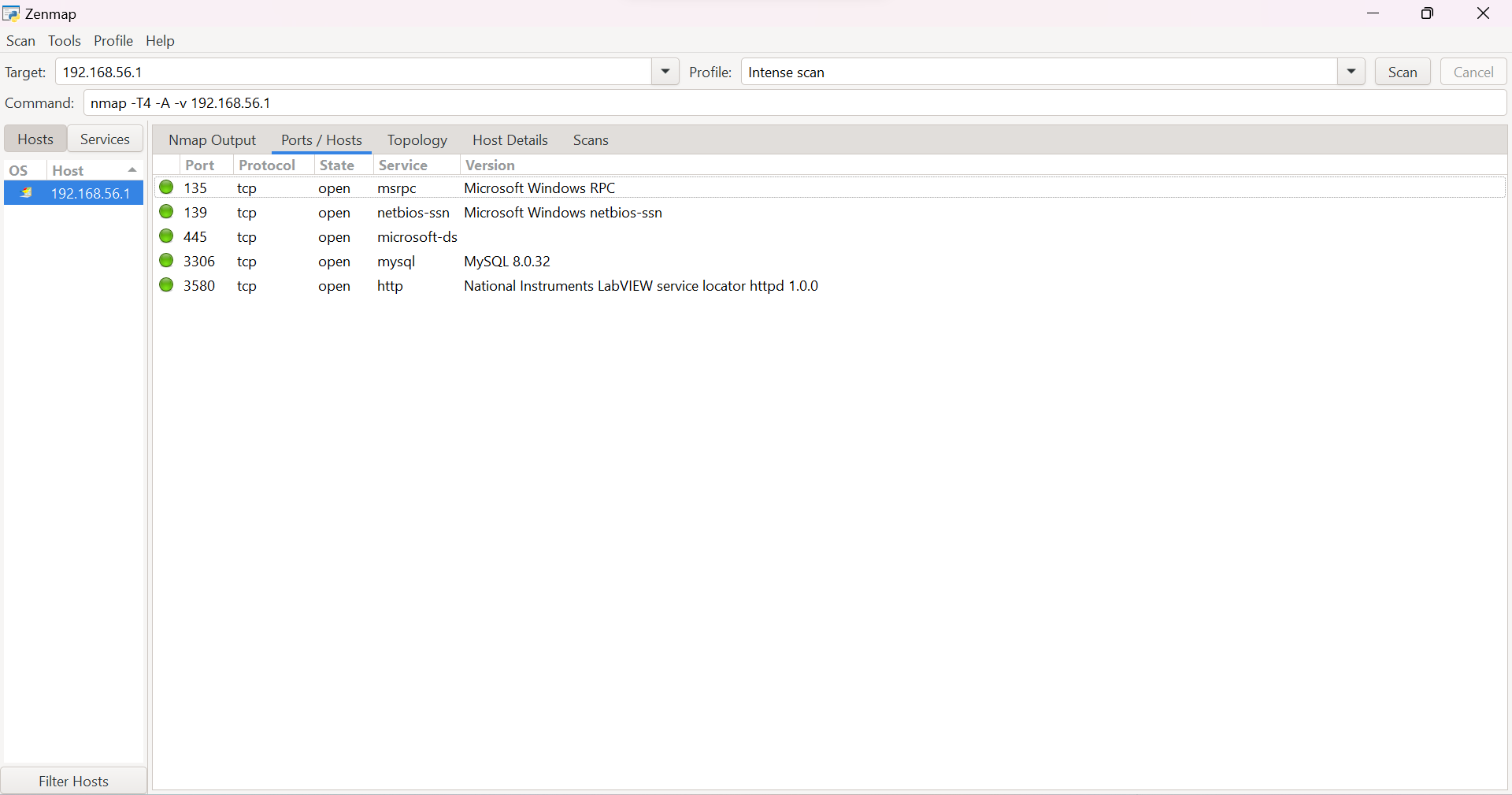


Figure 17: Used Nmap to scan a particular IP address

Step 2: Now we can observe the different port numbers



Step 3: Can also check topology

Figure 18: We can check port number on nmap

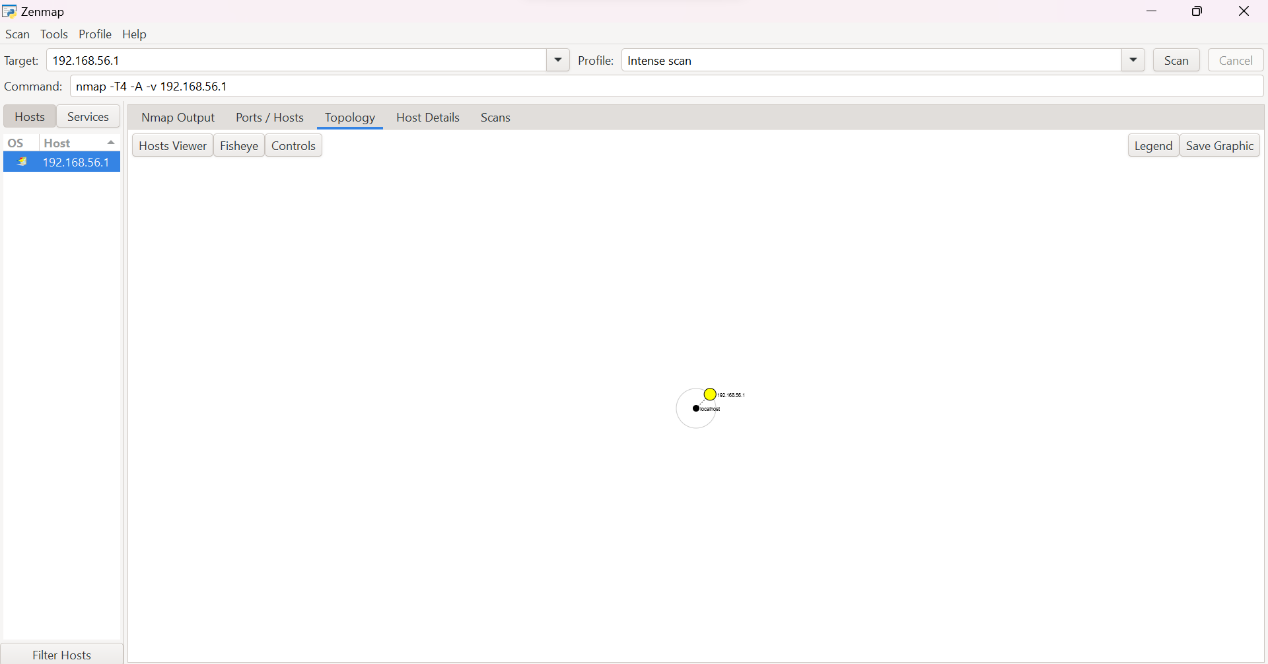


Figure 19: Can check topology

Step 4: Can also check host details

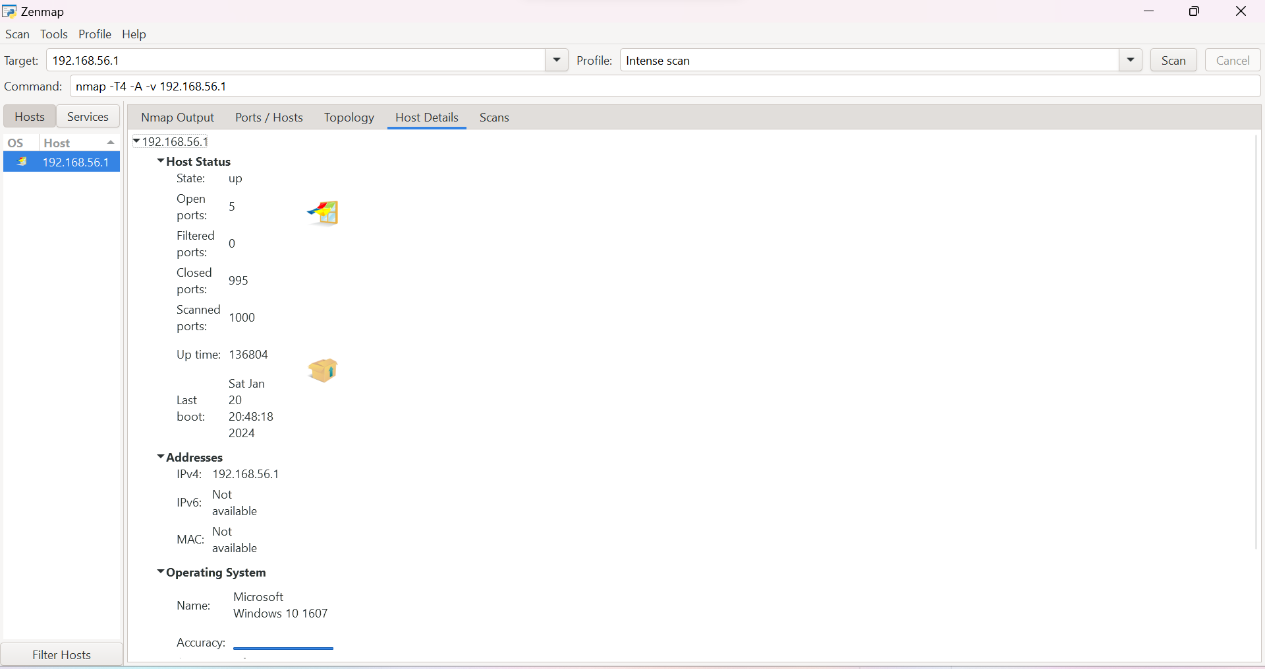


Figure 20: Can check host details also

Step 5: Can also check for previous scans

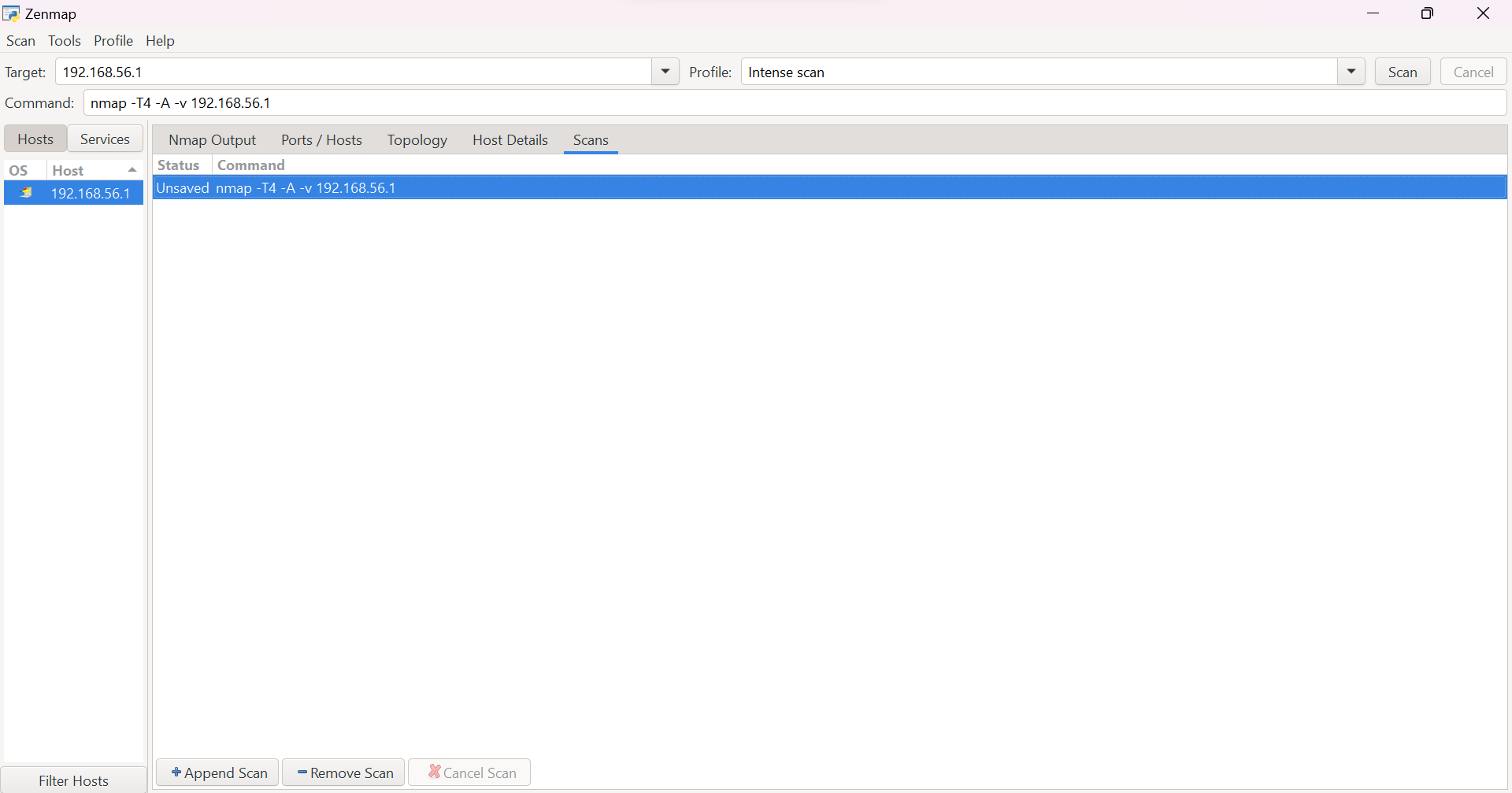


Figure 21: Check for the previous scans

Above figure we can see that we can see some terminologies as follows:

1. Target: Enter the target IP address
2. Profile: Enter the type of scan to be performed
3. The blank space will provide all the information of the scan
4. Nest image shows the information about ports and hosts

**VI. COMPARATIVE ANALYSIS**

1. **Wireshark Vs Burpsuite**

The fundamental difference between Wireshark and Burp Suite lies in their scope and purpose. Wireshark focuses on network protocol analysis, allowing users to capture and analyze network traffic across all protocols and applications. It provides a broad view of network communications, making it suitable for network administrators and security professionals.

Burp Suite, on the other hand, is specifically tailored for web application security testing. It specializes in analyzing HTTP/S traffic, intercepting and manipulating requests and responses to identify vulnerabilities. Burp Suite’s tools enable in-depth web application testing, making it valuable for penetration testers and web security professionals.

Wireshark and Burp Suite are indispensable tools in the domains of network analysis and web application security. Wireshark empowers users with comprehensive network traffic analysis capabilities, aiding network troubleshooting and monitoring. On the other hand, Burp Suite focuses on fortifying web applications by detecting vulnerabilities and ensuring their security. Understanding the differences and applications of these tools allows professionals to leverage their strengths, ensuring robust network infrastructure and secure web applications in today’s ever-evolving digital landscape.[4]

1. **Nmap Vs Wireshark**

While Nmap and Wireshark are both essential tools in the network security and analysis domain, they serve different purposes. Nmap primarily focuses on scanning and discovering network hosts and services, whereas Wireshark specializes in deep packet analysis. Nmap is ideal for conducting port scans, host discovery, and vulnerability assessments, whereas Wireshark excels in capturing and analyzing network traffic for detailed protocol-level inspection.

Certifications for Network Security Engineers: For individuals pursuing a career in network security, certifications play a vital role in validating their skills and knowledge. Some notable certifications in the field of network security include Certified Ethical Hacker (CEH), Certified Information Systems Security Professional (CISSP), Certified Network Defense Architect (CNDA), and Certified Network Security Engineer (CNSE). These certifications provide comprehensive coverage of network security concepts, tools, and practices, and demonstrate an individual's expertise in the field [5].

**VII. CONCLUSION**

In conclusion, this research paper has shed light on the critical role of cybersecurity tools in fortifying defences against the ever-evolving landscape of cyber threats. By delving into various tools such as Burp Suite, Wireshark, and Nmap, we've highlighted their integral contributions to enhancing cybersecurity measures in modern organizations.

The significance of leveraging advanced technologies, including automation and artificial intelligence, cannot be overstated in the realm of cybersecurity. These technologies not only bolster security measures but also enable effective detection of vulnerabilities and prompt responses to cyber-attacks.

Moreover, the paper has emphasized the imperative for cybersecurity education and training, addressing the gap between industry demands and educational offerings. Strategies such as the SPARTA Cybersecurity Skills Framework and the integration of generative AI showcase the ongoing efforts to align educational curricula with industry requirements and deploy cutting-edge solutions.

As organizations continue to navigate the complex cybersecurity landscape, it's crucial to recognize the diverse categories of cybersecurity tools and their real-life applications. Whether it's network monitoring, intrusion detection, vulnerability assessment, or incident response, these tools play a pivotal role in safeguarding organizations and individuals from cyber risks.

In essence, this paper serves as a concise overview of the pivotal role that cybersecurity tools play in safeguarding organizations and individuals in today's digital landscape. By embracing advanced technologies and fostering collaboration among stakeholders, we can effectively mitigate emerging cyber threats and cultivate a secure and privacy-conscious digital environment.

This conclusion summarizes the key findings and contributions of the research paper, providing a comprehensive overview of the importance of cybersecurity tools in today's cybersecurity landscape.

**REFERENCES**

1. J. Hajny, S. Ricci, E. Piesarskas, O. Levillain, L. Galletta and R. De Nicola, "Framework, Tools and Good Practices for Cybersecurity Curricula," in IEEE Access, vol. 9, pp. 94723-94747, 2021, doi: 10.1109/ACCESS.2021.3093952.
2. S. C. Paladino and J. E. Fingerman, "Cybersecurity Technology Transition: A Practical Approach," 2009 Cybersecurity Applications & Technology Conference for Homeland Security, Washington, DC, USA, 2009, pp. 325-330, doi: 10.1109/CATCH.2009.32
3. S. Sai, U. Yashvardhan, V. Chamola and B. Sikdar, "Generative AI for Cyber Security: Analyzing the Potential of ChatGPT, DALL-E and Other Models for Enhancing the Security Space," in IEEE Access, doi: 10.1109/ACCESS.2024.3385107.
4. W. Junmei and Y. Chengkang, "Automation Testing of Software Security Based on BurpSuite," 2021 International Conference of Social Computing and Digital Economy (ICSCDE), Chongqing, China, 2021, pp. 71-74, doi: 10.1109/ICSCDE54196.2021.00025.
5. Banerjee, Usha & Vashishtha, Ashutosh & Mukul, Saxena. (2010). Evaluation of the Capabilities of WireShark as a tool for Intrusion Detection. International Journal of Computer Applications. 6. 10.5120/1092-1427.
6. S. Liao et al., "A Comprehensive Detection Approach of Nmap: Principles, Rules and Experiments," 2020 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), Chongqing, China, 2020, pp. 64-71, doi: 10.1109/CyberC49757.2020.00020.  
   keywords: {Operating systems;Intrusion detection;Telecommunication traffic;Tools;Reconnaissance;Knowledge discovery;Software;Nmap;ET OPEN;CNDR;Intrusion detection},
7. <https://www.javatpoint.com/what-is-burp-suite>
8. N. Bacanin and H. Shaker (Eds.): ICIITB 2022, ACSR 104, pp. 114–135, 2023. <https://doi.org/10.2991/978-94-6463-110-4_10>
9. Goldschmidt, P., Kuˇcera, J.: Defense against syn flood dos attacksˇ using network-based mitigation techniques. In: 2021 IFIP/IEEE International Symposium on Integrated Network Management (IM). pp. 772–777. IEEE (2021)
10. Goyal, P., Goyal, A.: Comparative study of two most popular packet sniffing tools-tcpdump and wireshark. In: 2017 9th International Conference on Computational Intelligence and Communication Networks (CICN). pp. 77–81. IEEE (2017). doi: https://doi.org/10.1109/ cicn.2017.8319360