WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

PenLab Vulnerable Web Application

[1]Ms. Rajvee Sakariya, [2]Mr. Keshav Singh

[1] Department of Computer Science, Parul University Vadodara, Gujarat, India rajvee.sakariya34114@paruluniversity.ac.in

[2] Department of Computer Science, Parul University Vadodara, Gujarat, India 210303105529@paruluniversity.ac.in

ABSTRACT :

PenLab is a dedicated penetration testing lab designed for cybersecurity professionals and students to enhance their practical skills in ethical hacking, vulnerability assessment, and exploit development. The lab provides a controlled and legally compliant environment where users can perform penetration testing on various systems, mimicking real-world scenarios. Built with virtualized environments, automated vulnerability assessments, and guided exploitation techniques, PenLab serves as a powerful tool for learning and research. This paper details the architecture, functionalities, and use cases of PenLab.

Keywords: Penetration testing, ethical hacking, cybersecurity training, vulnerability assessment, exploit development

1.0 INTRODUCTION:

With the rise in cyber threats and attacks, there is an increasing demand for skilled cybersecurity professionals.

"Traditional classroom-based training often lacks hands-on experience, making it difficult for learners to grasp real-world hacking techniques."

PenLab bridges this gap by providing an interactive environment where cybersecurity enthusiasts can practice penetration testing legally and safely. PenLab enables users to work on simulated vulnerabilities and real-world security challenges in a sandboxed environment. The lab includes various operating systems, vulnerable web applications, and misconfigured networks to help users understand and exploit security weaknesses. Automated vulnerability assessments and guided exploitation modules assist beginners in developing their penetration testing skills. To enhance the learning experience, PenLab offers real-time attack simulations, live debugging sessions, and forensic analysis tasks. Unlike conventional training platforms, PenLab integrates machine learning-based vulnerability detection, adaptive learning modules, and collaborative team-based challenges.

2.0 Methodology:

The penetration testing methodology followed during the PenLab project included:

- **Information Gathering** Using OSINT techniques and reconnaissance tools like WHOIS, Shodan, and subdomain enumeration.

- **Scanning and Enumeration** Active and passive scanning with tools such as Nmap, Nikto, and Burp Suite.

- **Exploitation** Validation of security flaws using SQLmap, Metasploit, and custom scripts.

- **Post-Exploitation Analysis** Evaluating the impact of successful attacks and privilege escalation possibilities.

- **Reporting and Mitigation** Documenting findings, proof-of-concept (PoC) exploits, and recommending security improvements.

3.0 PROBLEM AND SOLUTION DESCRIPTION:

The cybersecurity industry faces a skills gap where professionals lack practical penetration testing experience. Many aspiring ethical hackers struggle to find legally compliant environments to practice offensive security techniques. Existing labs either focus on static challenges or lack guided learning support, making it difficult for beginners to advance. PenLab addresses these gaps by offering an adaptive, real-time, and legally compliant penetration testing environment.

Problem Statement and Choice of Solution

Conventional cybersecurity training lacks hands-on practice, real-world attack scenarios, and adaptive learning mechanisms. Many learners struggle with understanding complex vulnerabilities without proper guidance. PenLab solves this by:

1. Offering a legally compliant environment with diverse security challenges.
2. Providing automated vulnerability scanning and guided exploitation.
3. Allowing real-time collaboration between learners and mentors.

4.0 APPLICATION DEVELOPMENT:

Software Development Process Model

PenLab follows an agile development approach, allowing iterative improvements based on user feedback. This ensures that new attack vectors, vulnerabilities, and security techniques are constantly updated.

Technologies Used

1. Vulnerability Scanners: Integration with tools like OpenVAS and Nessus ensures real-time security assessments.
2. Exploitation Frameworks: Metasploit, Burp Suite, and custom exploit scripts enhance the penetration testing experience.

5.0 USE CASE FOR THE APPLICATION:

User Dashboard

The dashboard provides access to various security labs, progress tracking.

Virtual Machines and Challenges

Users can select vulnerable systems, practice exploits, and receive automated feedback.

6.0 Findings and Analysis:

During the project, multiple vulnerabilities were identified, including:

6.1 SQL Injection (SQLi)

- **Tested Using** SQLmap and manual payload insertion.
- **Payload Used** `1' OR '1'='1 --`
- **Impact** Allowed unauthorized database access, data retrieval, and potential administrative takeover.
- **Mitigation** Implement **prepared statements**, **input validation**, and **Web Application Firewall (WAF)**.

6.2 Cross-Site Scripting (XSS)

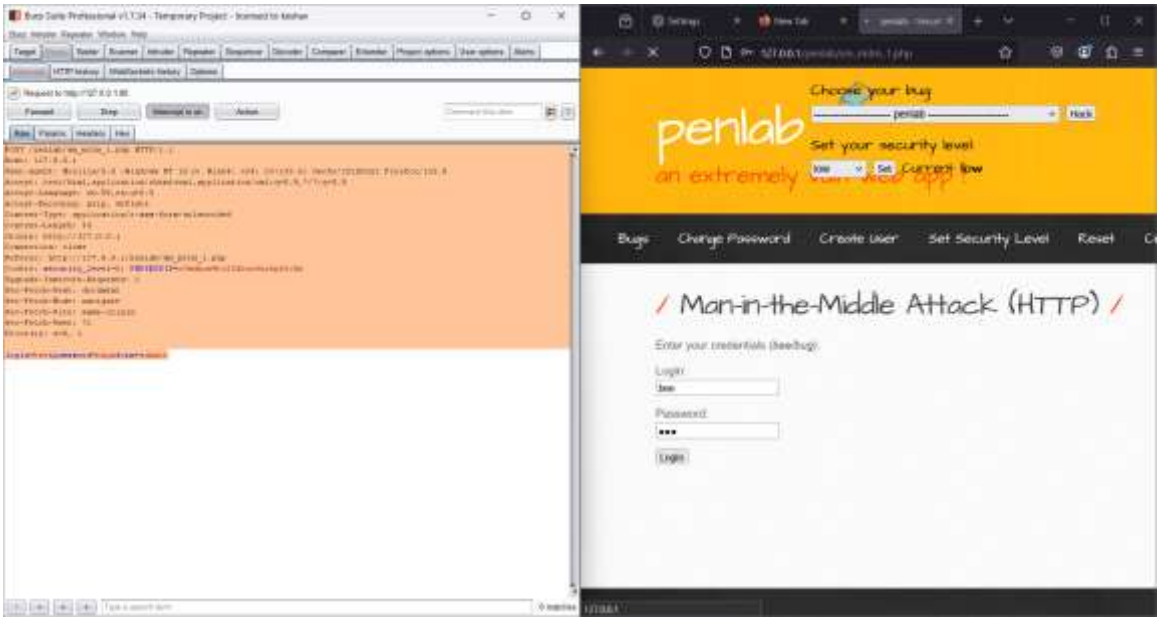
- **Tested Using** Burp Suite and manual script injection.
- **Payload Used** `<script>alert('XSS')</script>`
- **Impact** Allowed session hijacking and data theft via malicious JavaScript execution.
- **Mitigation** Implement **input sanitization**, **Content Security Policy (CSP)**, and **secure cookie attributes**.

7.0 Proof of Findings (Screenshots) :

The following sections contain proof-of-concept (PoC) evidence for vulnerabilities identified in the PenLab project.

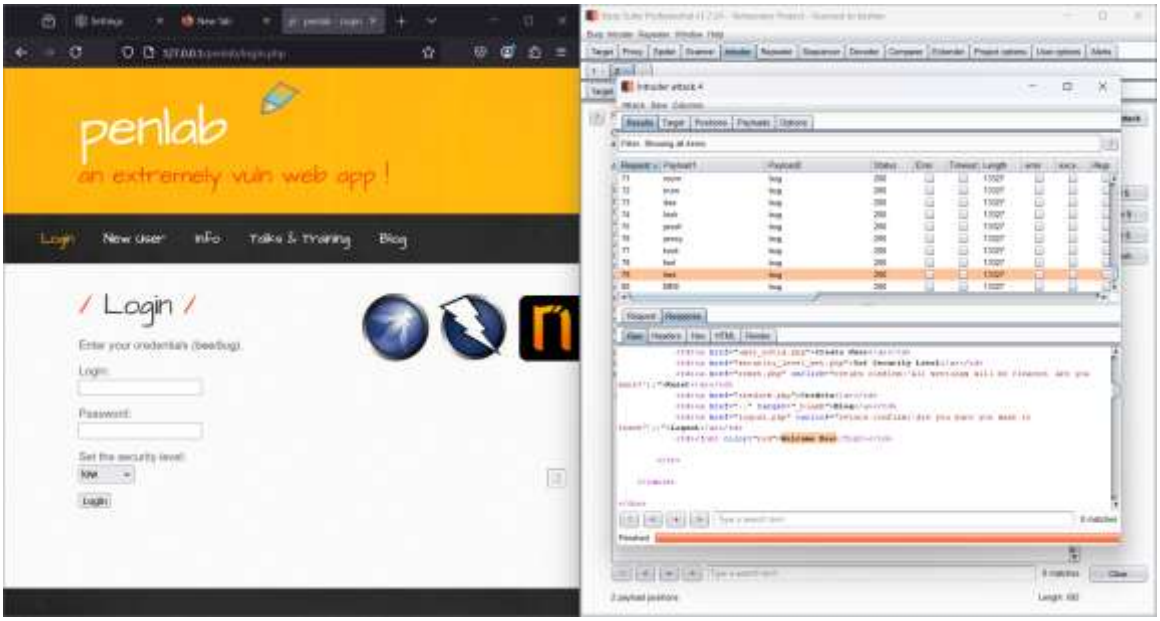
7.1 MITM Attack using Burpsuite

This screenshot will show the results of an MITM Attack performed to capturing user credentials.



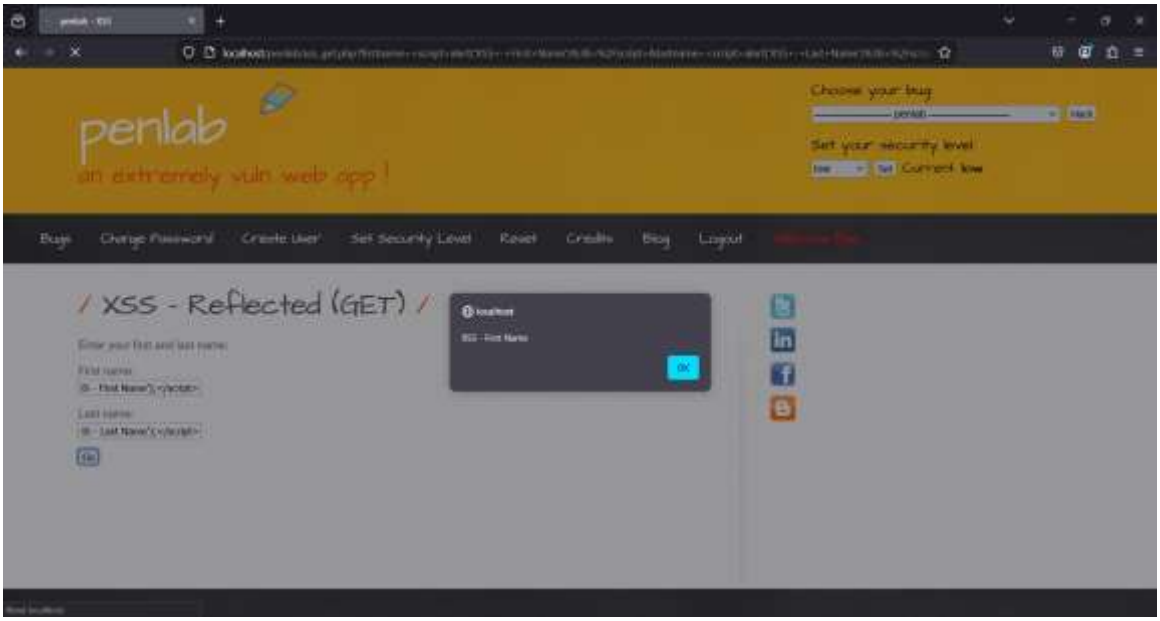
7.2 Password Brute-force Attack using Burpsuite Intruder

This screenshot will demonstrate a successful Bruteforce attack that retrieved Login information.



7.3 Cross-Site Scripting (XSS) Attack

This screenshot will display an XSS vulnerability.



8.0 CONCLUSION:

PenLab provides a hands-on cybersecurity training platform, bridging the gap between theoretical learning and real-world penetration testing. By integrating automated vulnerability assessments, guided exploit execution, and collaborative learning, it ensures that users develop essential cybersecurity skills in a safe environment.

9.0 FUTURE WORK:

Future enhancements for PenLab include:

1. AI-based attack simulations.
2. Cloud-based machine learning analytics for threat detection.
3. Enhancing intrusion detection systems with machine learning

10.0 References:

[1] Linhart, C., Klein, A., Heled, R., & Orrin, S. (2005). HTTP request smuggling. Proceedings of the 14th International Conference on World Wide Web, 768-769.

[2] Bortz, A., & Boneh, D. (2007). Exploring timing attacks on the web. Proceedings of the 16th International Conference on World Wide Web, 621-629.

[3] Gelernter, N., & Herzberg, A. (2015). Cross-site search attacks. Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, 1394-1405.

[4] Rautenstrauch, C., Pellegrino, G., & Stock, B. (2023). A comprehensive study of cross-site leaks: Attacks and defenses. IEEE Symposium on Security and Privacy, 2754-2771.

[5] Knittel, J., Mainka, C., Niemietz, M., & Noß, B. (2021). Attacking websites using HTTP request smuggling: Empirical testing of servers and proxies. IEEE European Symposium on Security and Privacy, 1772-1786.

[6] Van Goethem, T., Franken, J., Sanchez-Rola, R., & Dworken, A. (2022). Evaluating defenses against cross-site leaks: A comprehensive analysis. USENIX Security Symposium, 787-804.

[7] Sudhodanan, S., Khodayari, E., & Caballero, J. (2020). BASTA-COSI: A tool for detecting cross-site leaks in web applications. Proceedings of the 29th USENIX Security Symposium, 1-18.