Task 1: Web Application Security Testing — Security Report

# 1. Introduction

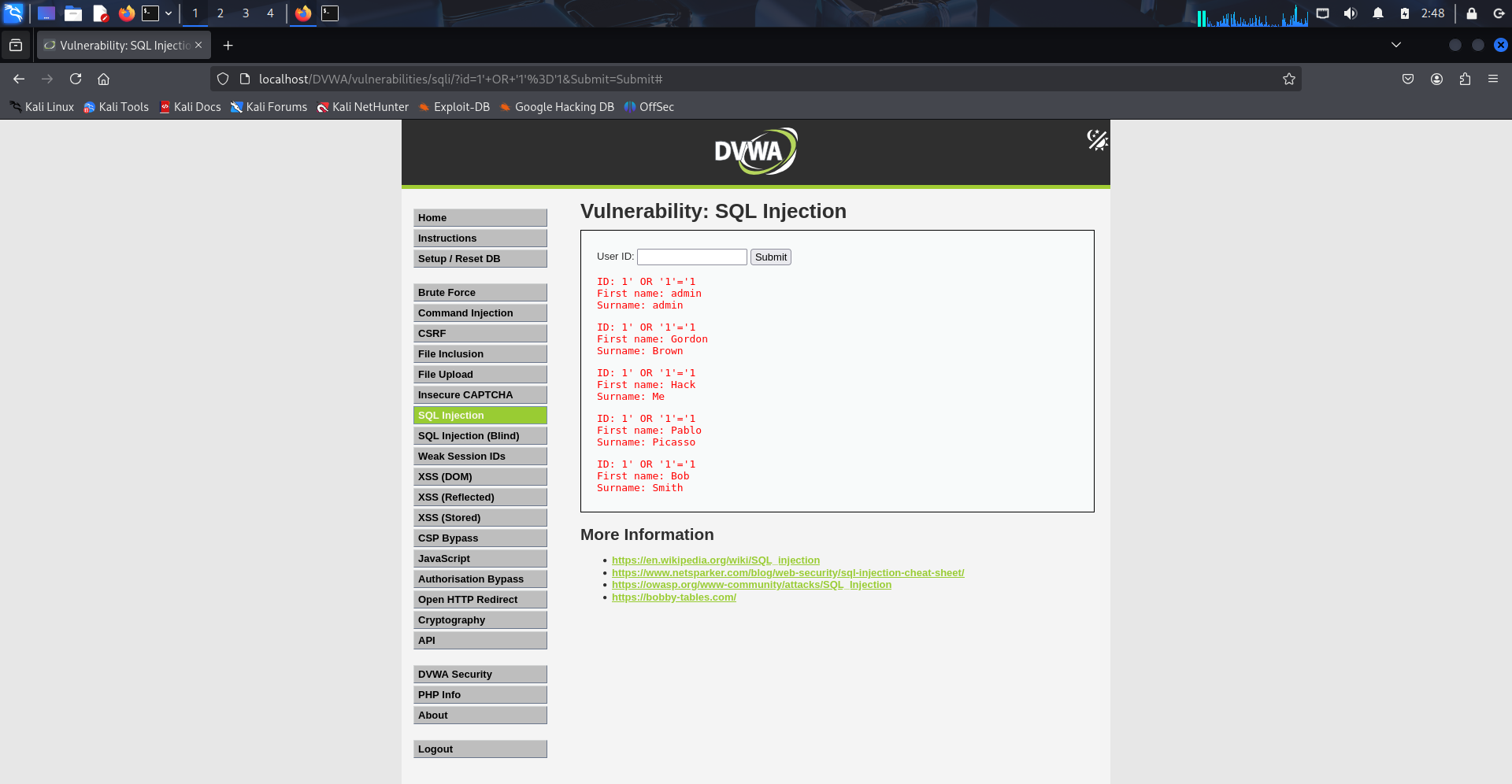
As part of my Cyber Security Internship at Future Interns, I conducted web application security testing on DVWA (Damn Vulnerable Web Application). The goal was to identify common web vulnerabilities — specifically:  
- SQL Injection (SQLi)  
- Cross-Site Scripting (XSS)  
- Brute Force Authentication flaws  
  
This report details my findings, screenshots, and recommended mitigations.

# 2. Tools Used

- DVWA — intentionally vulnerable web app for testing  
- Burp Suite Community Edition  
- SQLMap (optional)  
- Kali Linux

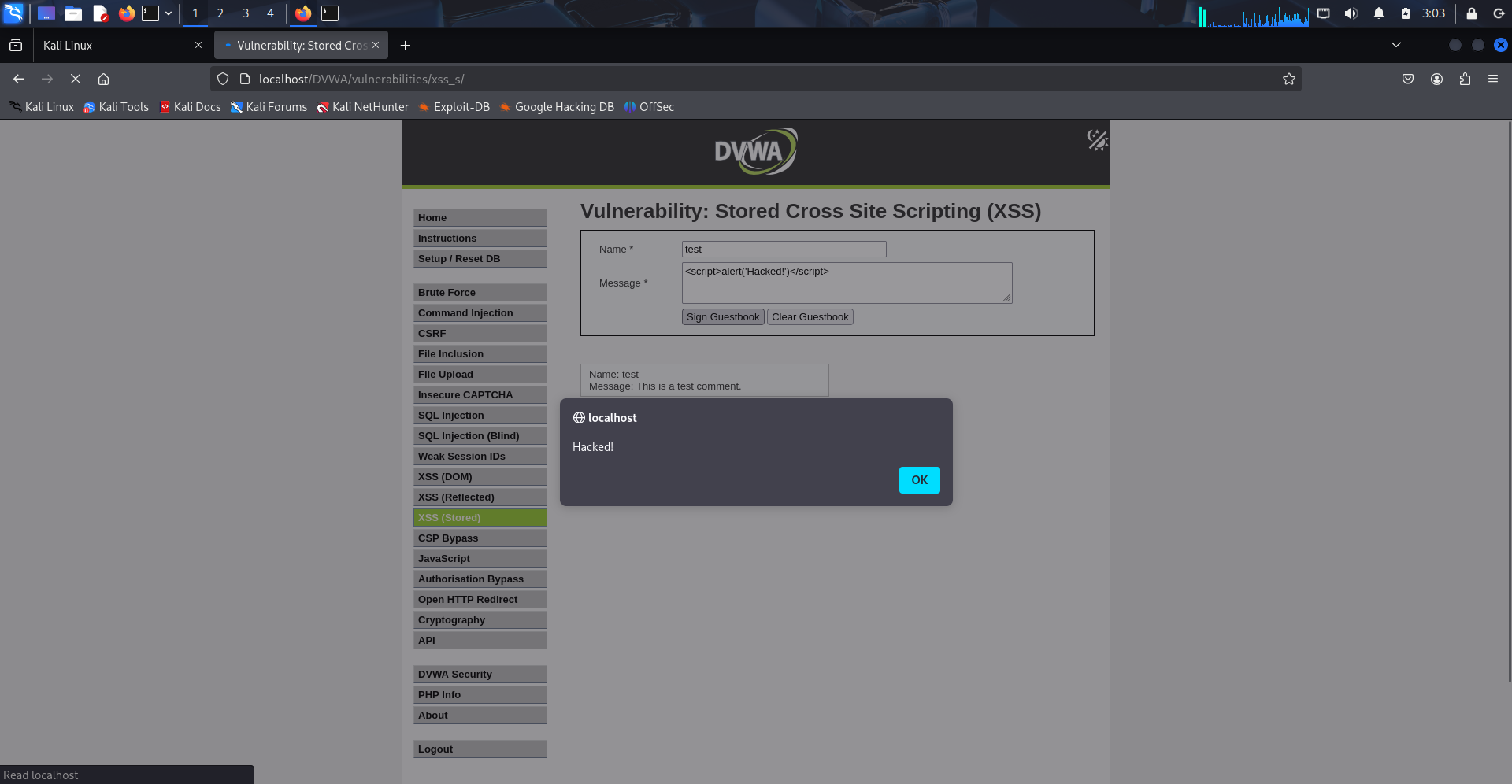
# 3. Findings

## A. SQL Injection

Description: I tested the User ID input in DVWA’s SQL Injection module.  
Payload Used: ' OR '1'='1  
Result: Bypassed intended query logic and dumped multiple user records.  
✅ Screenshot: 

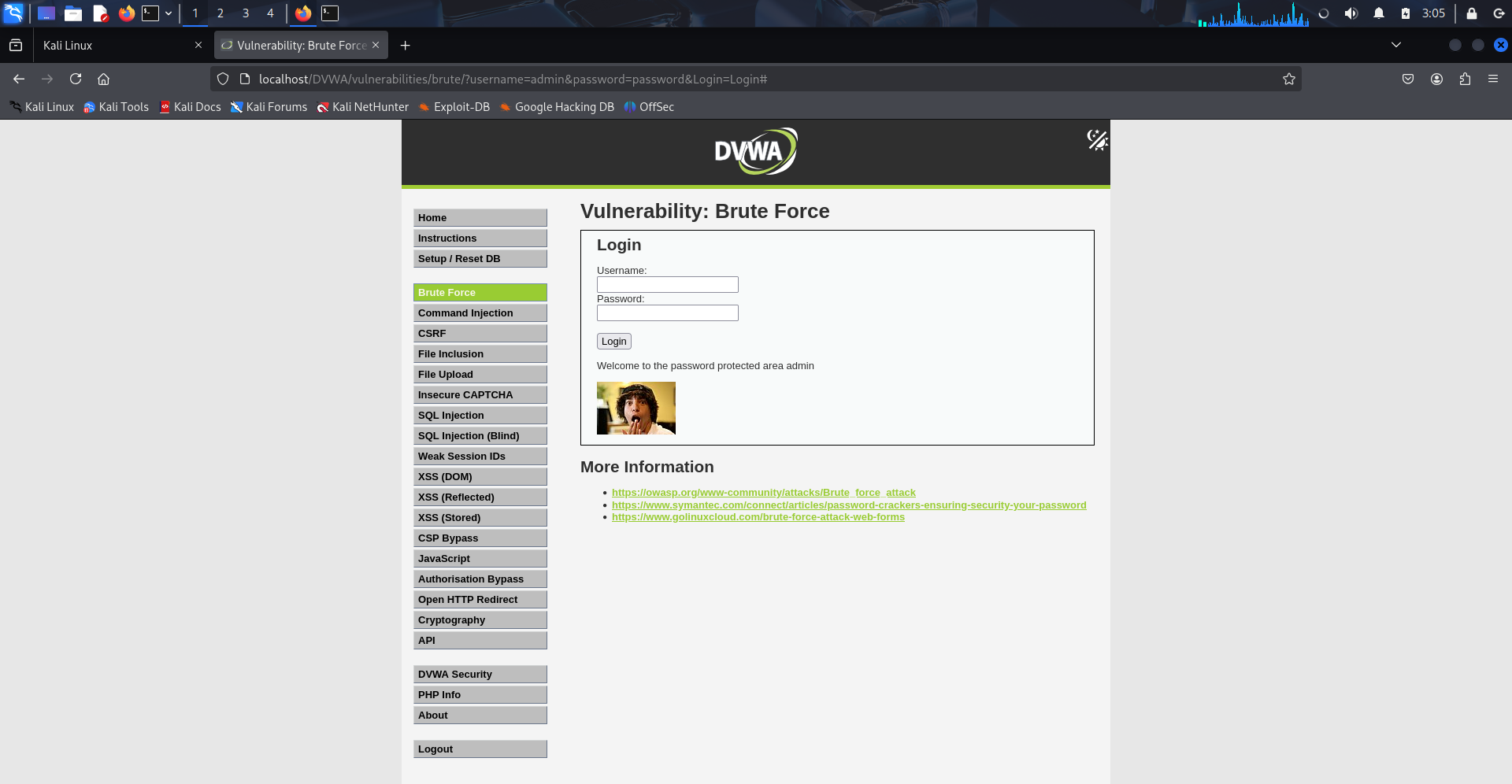
## B. Stored Cross-Site Scripting (XSS)

Description: I tested the Guestbook comment input in DVWA’s Stored XSS module.  
Payload Used: <script>alert('Hacked!')</script>  
Result: Successfully injected malicious JavaScript which triggered an alert pop-up when the page reloaded.  
✅ Screenshot:



## C. Brute Force Attack

Description: Tested login forms for weak credential protection.  
Result: Bypassed login by guessing default credentials (admin / password).  
✅ Screenshot:



# 4. Mitigation Strategies

|  |  |
| --- | --- |
| Vulnerability | Recommended Fix |
| SQL Injection | Use prepared statements (parameterized queries) instead of directly inserting user input into SQL queries. Validate and sanitize input. |
| Stored XSS | Sanitize user input. Use output encoding when displaying user data on web pages. Implement Content Security Policy (CSP). |
| Brute Force | Enforce strong password policies, use CAPTCHA, implement account lockouts after repeated failed attempts, enable multi-factor authentication (MFA). |

# 5. Conclusion

This task strengthened my practical skills in:  
- Web application penetration testing  
- Identifying real-world vulnerabilities  
- Using tools like Burp Suite & DVWA  
- Documenting security flaws and proposing fixes  
  
I now better understand how attackers exploit common weaknesses — and how developers can secure their apps by design.

# Attachments

- Screenshots: SQLi, XSS, Brute Force evidence  
- DVWA Config: Local setup on Kali Linux

Prepared by:

Sagar Singh

Future Interns Cyber Security Intern