Lab 05: Attacking a Vulnerable Web Application and Database

Author: Joseph Patrick C. Galvez

American Military University

ISSC: Red Team and Blue Team Security

Mr. Brian Burnett

7/27/2025

Hacking Lab Report: Attacking a Vulnerable Web Application and Database

## Introduction

The purpose of this lab is for students to be able to identify the vulnerabilities within web applications and web servers. Students are also instructed on how to perform SQL injection attacks and XSS attacks. Section 1 involves using the Damn Vulnerable Web Application (DVWA) to perform XSS and SQL injection attacks. The final Part of this lab is to execute a command that inserts a .txt file into the target device. Section 2 involves much the same thing as section 1 but with less guidance, a similar type of vulnerability is exploited to insert another .txt file into the target device.

## Section 1:

The lab instructs me to report that running a the command: a' ORDER BY 2;# where the “2” is the number of suspected columns in the database. If there are no error messages then the guess is correct.

A screenshot of a computer

AI-generated content may be incorrect.[[1]](#footnote-1)A screenshot of a computer

AI-generated content may be incorrect.[[2]](#footnote-2)A screenshot of a computer

AI-generated content may be incorrect.[[3]](#footnote-3)A screenshot of a computer

AI-generated content may be incorrect.[[4]](#footnote-4)A screenshot of a computer

AI-generated content may be incorrect.[[5]](#footnote-5)

**Section 2:**

Similarly to section 1 the lab instructs me to report that running the command a' ORDER BY 2;# reveals whether the database has 2 rows. If there is no error message then there are that many rows.

A screenshot of a computer

AI-generated content may be incorrect.[[6]](#footnote-6)A screenshot of a computer

AI-generated content may be incorrect.[[7]](#footnote-7)A screenshot of a computer

AI-generated content may be incorrect.[[8]](#footnote-8)A screenshot of a computer

AI-generated content may be incorrect.[[9]](#footnote-9)

References

Hatsize. (n.d.). *Lab environment: Ethical hacking simulation* [Virtual lab]. JBL Learning. <https://jbl-lti.hatsize.com/labview/?e=4160193>

*For additional information on APA Style formatting, please consult the* [*APA Style Manual, 7th*](https://apastyle.apa.org/style-grammar-guidelines) *Edition.*

1. Figure 1 – an alert is executed from the web service through an SQL injection attack. [↑](#footnote-ref-1)
2. Figure 2 – On a high security setting the web page resists an SQL injection attack. [↑](#footnote-ref-2)
3. Figure 3 – an SQL injection attack reveals the profile running the web service. [↑](#footnote-ref-3)
4. Figure 4 – Displayed the the .txt file resulting from an SQL injection attack. [↑](#footnote-ref-4)
5. Figure 5 – Password hashes are revealed by an SQL injection attack. [↑](#footnote-ref-5)
6. Figure 6 - An XSS attack causes the webpage to show an alert message of my creation. [↑](#footnote-ref-6)
7. Figure 7 – An SQL injection attack reveals the user profile that runs the web service. [↑](#footnote-ref-7)
8. Figure 8 - An SQL Injection attack reveals hashes for stored passwords. [↑](#footnote-ref-8)
9. Figure 9 – An SQL injection attack created a .txt file that is stored on the target device. [↑](#footnote-ref-9)