OWASP Top 10 Lab Report — TryHackMe
Author: Rishi Bose
College: NMIMS Mumbai
Program: B.Tech Cybersecurity (3rd Year)

Badge

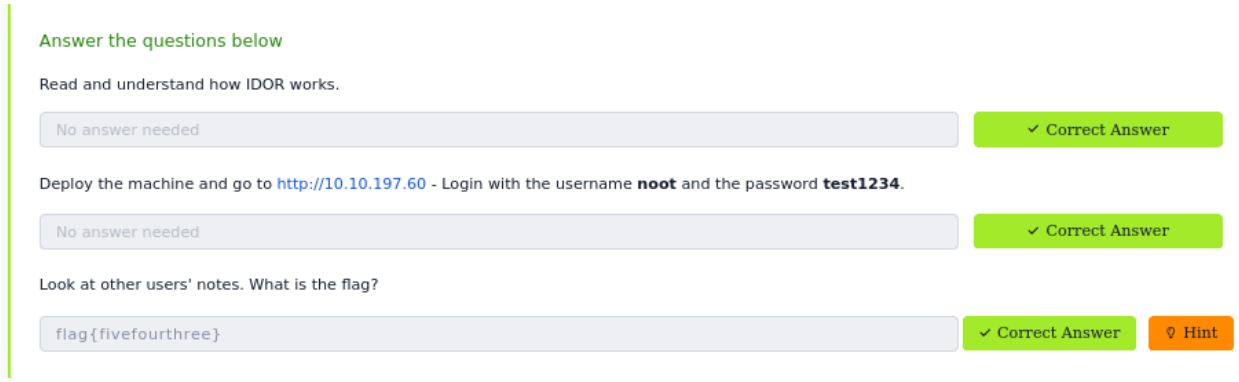
🚀 Overview

This report documents my practical journey through the **OWASP Top 10 Web Application Security Risks**, completed on **TryHackMe**. Each task in the room mimicked a real-world vulnerability, offering a safe and guided environment to practice offensive and defensive security techniques.

---

1. **Broken Access Control**

- **Target URL:** `http://10.10.197.60:81/`
- **Discovery:** Developer note hinted at `/assets/` directory
- **Sensitive File:** `users.bak`
- **Password Hash Extracted:** For user `admin`
- **Password Cracked:** `qwertyuiop`
- **Logged in as Admin:** Flag retrieved successfully.



---

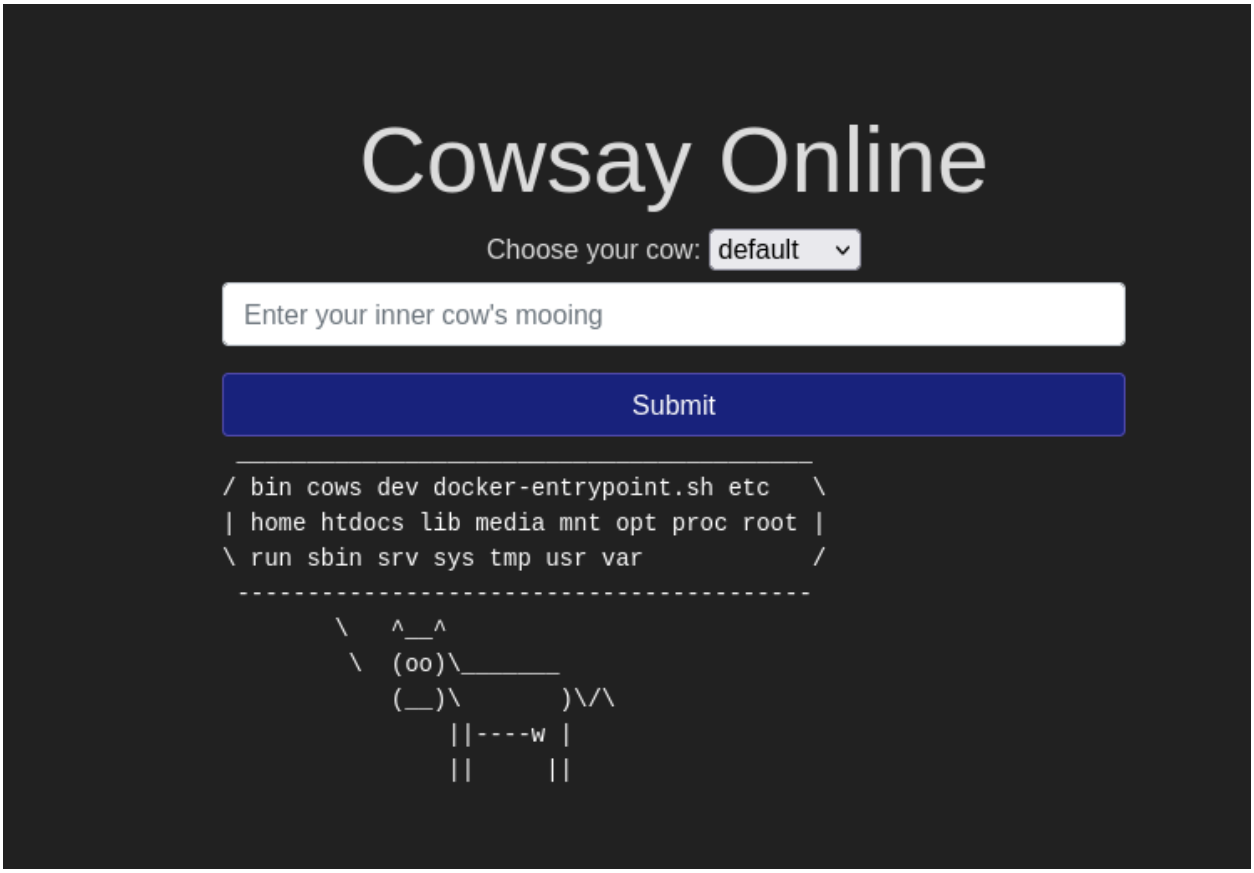
2. Cryptographic Failures

- **Task:** Identify and crack weak password hashes (MD5).
- **Tool Used:** crackstation.net
- **Example:** `6eea9b7ef19179a06954edd0f6c05ceb` → `qwertyuiop`

---

3. Injection (Command Injection)

- **Target URL:** `http://10.10.41.61:82/`
- **Payload Used:** `$(ls /)`
- **Exploited via Field:** `mooing`
- **Outcome:** Listed files, found sensitive data.

- 

---

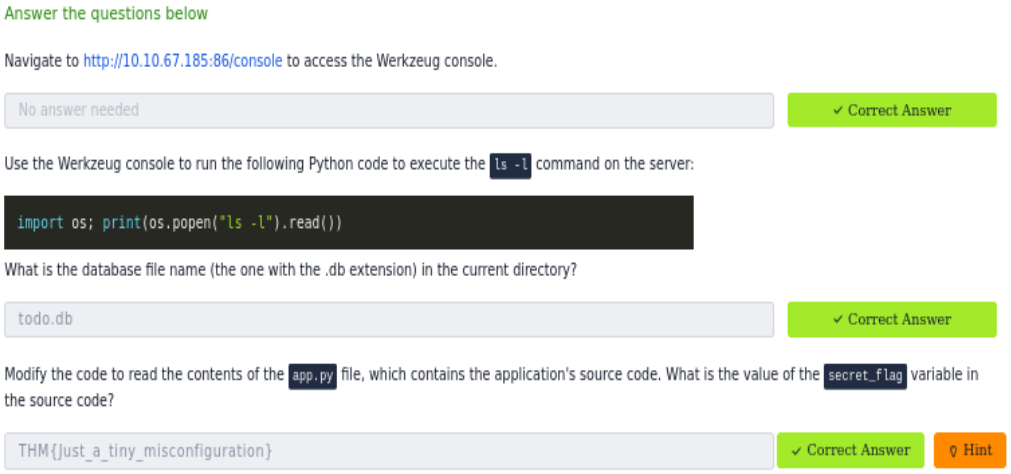
4. Insecure Design

- **Target:** Password reset bypass
- **URL:** `http://10.10.41.61:85/`
- **User Affected:** `joseph`
- **Exploit:** Re-registered using minor space: `joseph`
- **Reset Password To:** `eFqcNZShfzjn5V`
- **Flag:** `THM{Not_3ven_c4tz_c0uld_sav3_U!}`

---

5. Security Misconfiguration

- **Target URL:** `http://10.10.67.185:86/console`
- **Framework:** Werkzeug Debug Console
- **Payload:** `import os; print(os.popen("ls -l").read())`
- **Discovered File:** `site.db`
- **Flag Retrieved From:** `app.py`



---

6. Vulnerable and Outdated Components

- **Target:** Nostromo Web Server v1.9.6
- **Exploit Used:** CVE-2019-16278 (Python exploit script)
- **Command:** `python2 exploit.py 10.10.67.185 84 id`
- **Flag File:** `/opt/flag.txt`
- **Flag:** `THM{But_1ts_n0t_my_f4ult!}`

---

7. Identification and Authentication Failures

- **Re-registration Flaw:** Input sanitization missing
- **Logged in as:** `darren` and `arthur`
- **Accessed Flags:** From both user dashboards

---

8. Software Integrity Failures

- **Concept:** Using external JS libraries (e.g. jQuery) without SRI hash
- **Correct HTML Format:**

```
<script src="https://code.jquery.com/jquery-3.6.1.min.js"
        integrity="sha256-o88AwQnZB+VDvE9tvIXrMQaPlFFSUTR+nldQm1LuPXQ="
        crossorigin="anonymous"></script>
```

---

9. Security Logging and Monitoring Failures

- **Log Review:** Detected brute-force from IP `49.99.13.16`
- **Username Attempts:** `admin`, `administrator`, `root`

- **Impact:** Showcased lack of IP rate-limiting

🔗 Tools Used

- **Recon:** Gobuster, Nmap
- **Exploitation:** Python, Bash, TryHackMe Attack Boxes
- **Hash Cracking:** Crackstation.net
- **Browser Tools:** DevTools, Source Inspection

📊 Summary

This lab helped reinforce both fundamental and advanced offensive techniques related to web vulnerabilities. I strengthened my understanding of real-world attack vectors and how to prevent them in live applications. Each challenge reflected a real-life security risk backed by CVEs and documented exploits.

🚀 Ready for More

Feel free to connect if you're working on real-world cybersecurity problems or building secure applications.

LinkedIn: Rishi Bose
GitHub: github.com/rishi-bose
TryHackMe Rank: ADEPT [0x7]

#OWASP #Cybersecurity #TryHackMe #Pentesting #RCE #WebSecurity #Infosec