Sri Lanka Institute of Information Technology

Module:

Year 2, Semester 2

Introduction to Cyber Security

S.M.F Hana IT23255142

B.Sc. (Hons) in Information Technology

Specialized in Cyber Security

1 Room Overview

1.1 Title

Authentication Failures

1.2 Objective

The TryHackMe room is designed to provide cybersecurity learners and beginners with both theoretical and hands-on experience in exploiting authentication mechanism. The goal is to simulate real-world web authentication vulnerabilities frequently encountered in bug bounty programs and to demonstrate how these flaws can lead to unauthorized access, information disclosure or privilege escalation.

1.3 Key Vulnerabilities

- User enumeration
- SQL Injection (Authentication Bypass)
- Brute Force Attack
- Insecure Direct Object References (IDOR)
- Sensitive file disclosure
- Directory Traversal

2 Learning Objectives

By completing this room, participants will be able to:

- Understand how weak authentication leads to security flaws
- Identify and exploit user enumeration vulnerabilities
- Preform SQL injection to bypass authentication
- Execute brute force attacks
- Detect and exploit IDRO vulnerabilities to gain unauthorized access to user accounts
- Explore and utilize unauthorized information disclosure and directory traversal to uncover hidden panels

3 Room Structure

3.1 Task 1: Introduction

3.1.1 Description

A brief overview of the room, its educational purpose, and an outline of the challenge flow

3.1.2 Outcome

User understands the rooms learning objectives and engagement structure.

3.2 Task 2: Authentication Failures

3.2.1 Description

Provides a concise explanation of what authentication failure means and how it can impact web application security. The room also include a multiple-choice question to reinforce the concept

3.2.2 Outcome

Learners gains basic theoretical knowledge on authentication failure

3.3 Task 3: User Enumeration

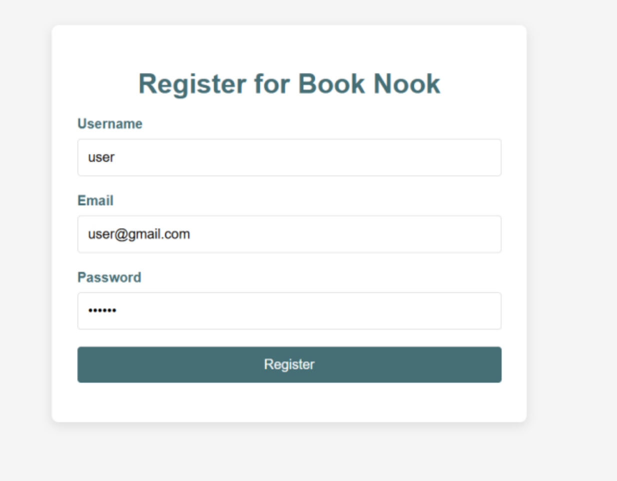
3.3.1 Description

The concept of user enumeration and how it could be done, is included, directing user to the vulnerable website created. User has to find valid usernames existing in the website

website link - http://hana-saleed.ct.ws/

3.3.2 Exploit Scenario

The user has to attempt to perform user enumeration in the registration page. If a username already exists, an error is shown letting the user know if the username already exists. The user has to attempt common usernames.

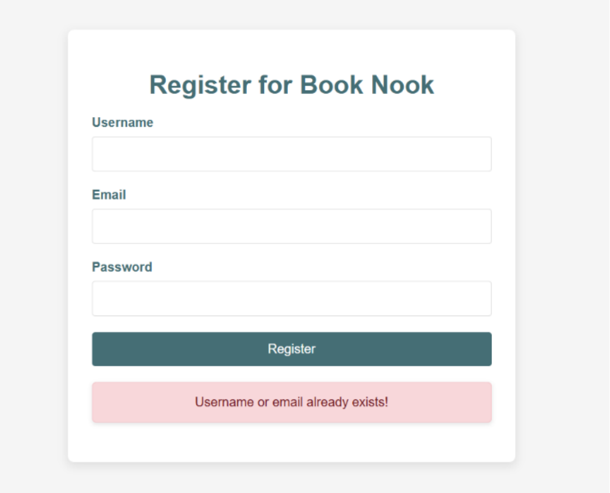


Register for Book Nook

Username: user

Email: user@gmail.com

Password: ••••••



Register for Book Nook

Username:

Email:

Password:

Username or email already exists!

3.3.3 Answer Required

Admin,user

3.3.4 Outcome

Participants learn to perform user enumeration and how registration response can leak information about valid users

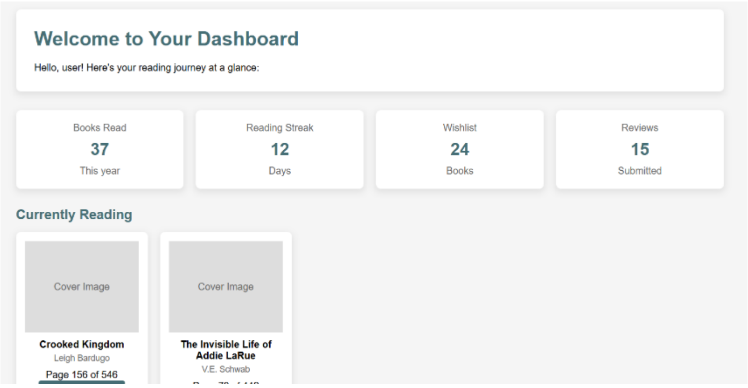
3.4 Task 4: SQL Injection

3.4.1 Description

This task describes the concept of SQL injection and how it can be used to exploit in the login form.

3.4.2 Exploit Scenario

The user has to navigate to login from and enter the username obtained from the previous user enumeration (“user”). Thereafter, the user has to enter ' OR '1'='1 in the to bypass login as the user account.



Welcome to Your Dashboard

Hello, user! Here's your reading journey at a glance:

Books Read 37 This year

Reading Streak 12 Days

Wishlist 24 Books

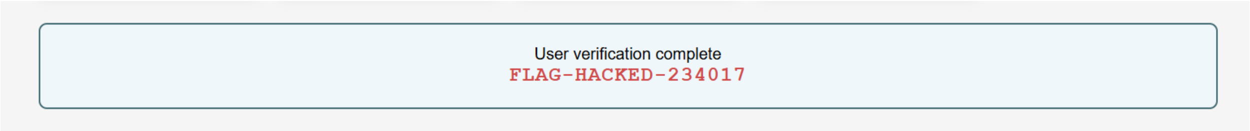
Reviews 15 Submitted

Currently Reading

Crooked Kingdom
Leigh Bardugo
Page 156 of 546

The Invisible Life of Addie LaRue
V.E. Schwab

3.4.3 Answer Required



User verification complete
FLAG-HACKED-234017

3.4.4 Outcome

Learners perform basic SQL injection and understand the importance of input sanitization.

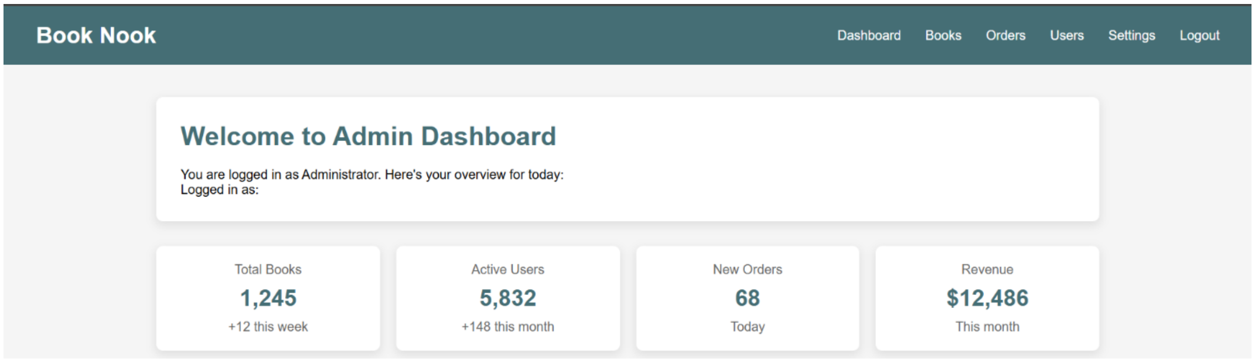
3.5 Task 5: Brute Force

3.5.1 Description

This challenge introduces brute-force attacks where an attacker attempts to gain unauthorized access by systematically guessing passwords. The login page does not implement rate-limiting, lockouts or CAPTCHA

3.5.2 Exploit Scenario

Users are instructed to use tools such as Hydra, Burp Suite intruder, or custom scripts to brute-force admin accounts password. Once successful they gain access to admin dashboard and retrieve the flag.

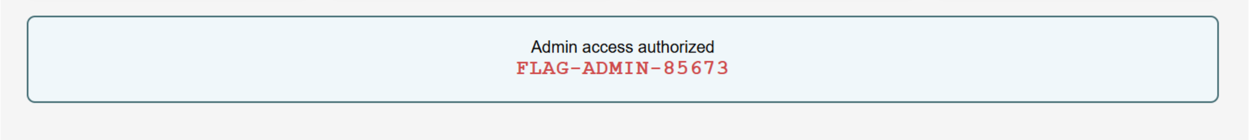


Welcome to Admin Dashboard

You are logged in as Administrator. Here's your overview for today:
Logged in as:

Total Books	Active Users	New Orders	Revenue
1,245	5,832	68	$12,486
+12 this week	+148 this month	Today	This month

3.5.3 Answer Required



Admin access authorized
FLAG-ADMIN-85673

3.5.4 Outcome

Participants learn the significance of implementing rate-limiting, account lockout policies, and password complexity requirements to prevent brute-force attacks.

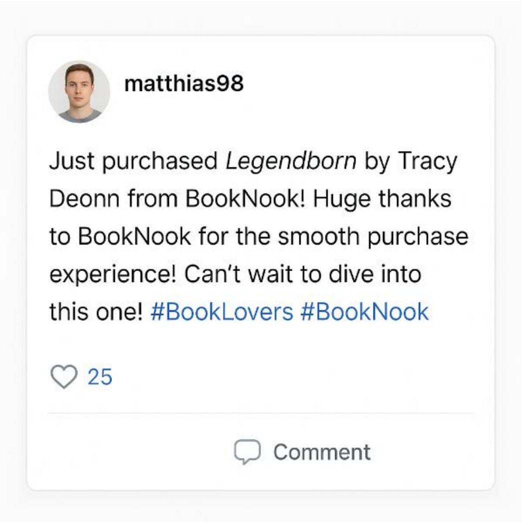
3.6 Task 5: IDOR

3.6.1 Description

This task demonstrates IDOR, how it works and internal implementations like user IDs are exposed in URLs. Additionally, the user gets get a brief idea about information gathering or open-source intelligence (OSINT).

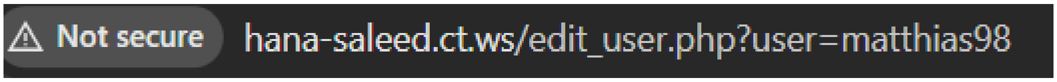
3.6.2 Exploit Scenario

The participants are given an image which they will be able to retrieve a legit username using OSINT. The participants have to log in as a regular user, with the previous user credentials and has to navigate to edit user page. Thereafter. they have to edit the URLs in such a way it can navigate to another users edit user page and modify the user profile.



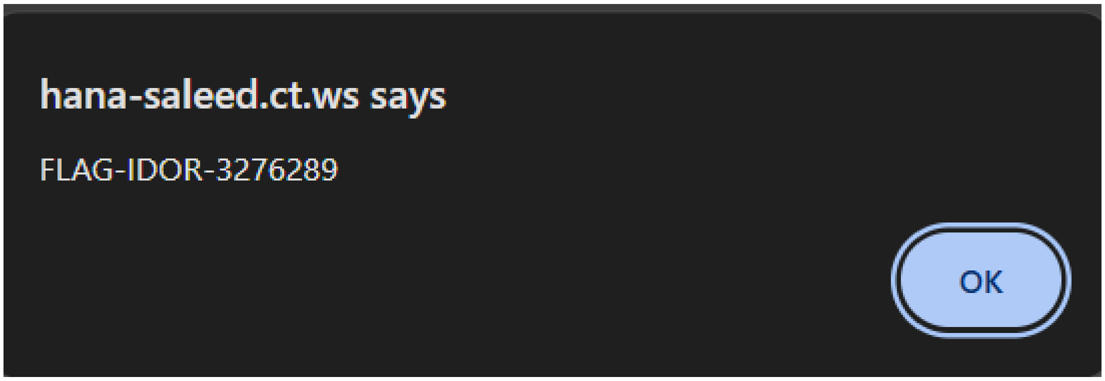
matthias98

Just purchased *Legendborn* by Tracy Deonn from BookNook! Huge thanks to BookNook for the smooth purchase experience! Can't wait to dive into this one! #BookLovers #BookNook



hana-saleed.ct.ws/edit_user.php?user=matthias98

3.6.3 Answer Required



hana-saleed.ct.ws says

FLAG-IDOR-3276289

3.6.4 Outcome

Learners understand the risks of exposing identifiers in client-side input and the importance of server-side access control checks.

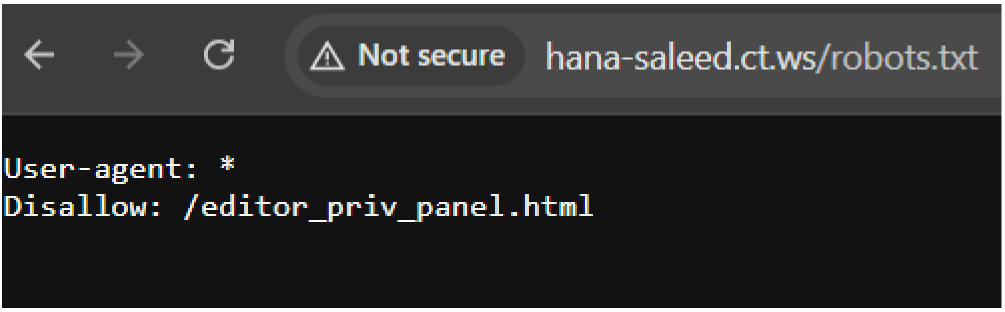
3.7 Task 5: Directory Traversal

3.7.1 Description

This final task illustrates how sensitive files and poorly secured directory structures can reveal unintended access points.

3.7.2 Exploit Scenario

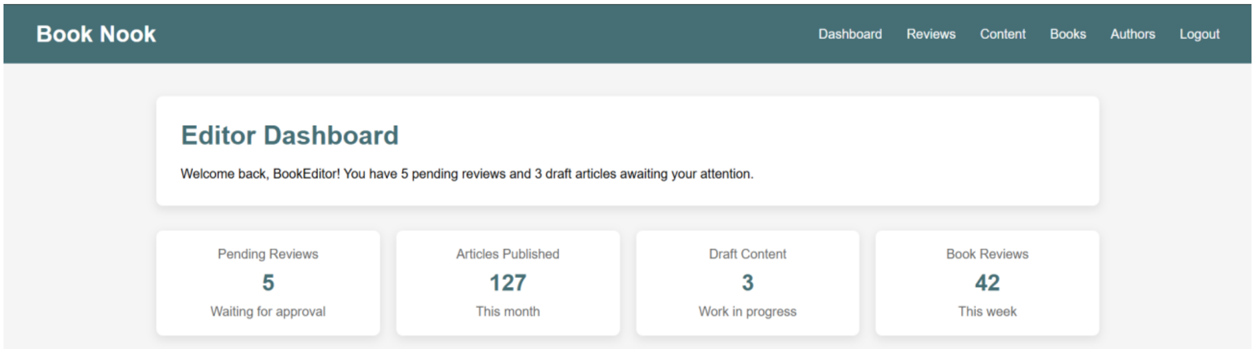
Participants have to explore the robots.txt and have to inspect disapproved directories and have to perform a directory travel by manipulating the URL. The user will find the editors panel path displayed in robots.txt and navigate to editor panel to retrieve the flag



hana-saleed.ct.ws/robots.txt

```
User-agent: *
Disallow: /editor_priv_panel.html
```

.

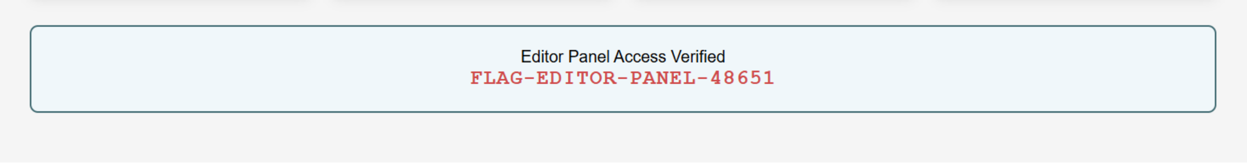


Editor Dashboard

Welcome back, BookEditor! You have 5 pending reviews and 3 draft articles awaiting your attention.

Pending Reviews	Articles Published	Draft Content	Book Reviews
5	127	3	42
Waiting for approval	This month	Work in progress	This week

3.7.3 Answer Required



Editor Panel Access Verified
FLAG-EDITOR-PANEL-48651

3.7.4 Outcome

Participants learn how seemingly harmless files like robots.txt can leak sensitive information and how weak file structure security enables privilege escalation through traversal.

4 Room Link - https://tryhackme.com/jr/authenticationfailures

5 Conclusion

The "Authentication Failures" TryHackMe room provides practical experience in exploiting common web security flaws such as user enumeration, SQL injection, brute-force attacks, IDOR, and directory traversal. By completing this room, participants gain valuable insights into how weak authentication mechanisms can lead to unauthorized access and security breaches. The exercises emphasize the importance of secure coding practices, input validation, and access controls to prevent these vulnerabilities in real-world applications.