

Hacking the Cookie: Privilege Escalation via Cookie Manipulation

Introduction

Welcome to this detailed writeup for the "Hack the Cookie" lab on HackerDNA. This challenge demonstrates a common web vulnerability: insecure session management through client-side cookie tampering. By manipulating a Base64-encoded cookie, we can escalate our privileges from a guest user to an admin role, bypassing authentication controls.

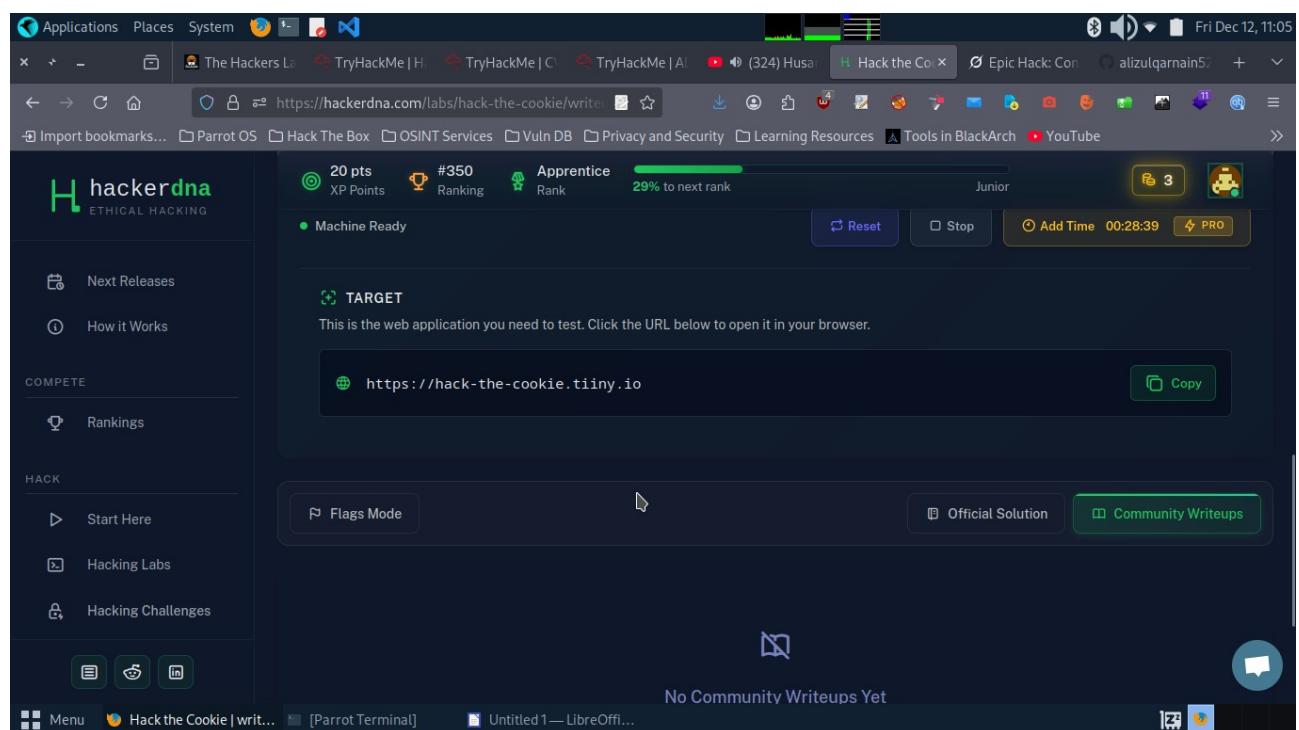
The lab simulates a corporate internal portal where user roles are stored in a tamperable cookie. We'll walk through the process step by step, including logging in with provided credentials, inspecting and decoding the cookie, modifying it, and re-encoding it to gain admin access.

Firstly when lab started

Prerequisites:

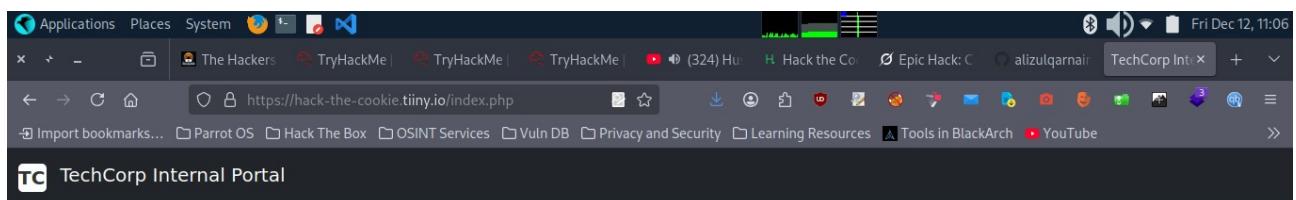
- A web browser with developer tools (e.g., Chrome DevTools).
- Access to a terminal for Base64 encoding/decoding.
- The lab URL: <https://hack-the-cookie.tiny.io>

Note: This is for educational purposes only in a controlled lab environment. Never apply these techniques to real systems without authorization.



Step 1: Access the Lab and Log In

1. Navigate to the lab URL: <https://hack-the-cookie.tiny.io>.
2. You'll be presented with a login page for the TechCorp Internal Portal.
3. Use the pre-filled credentials:
 - Username: guest
 - Password: password
4. Click "Login" to access the guest dashboard. You'll see a restricted view with limited options like Employee Resources and IT Support Ticket System.



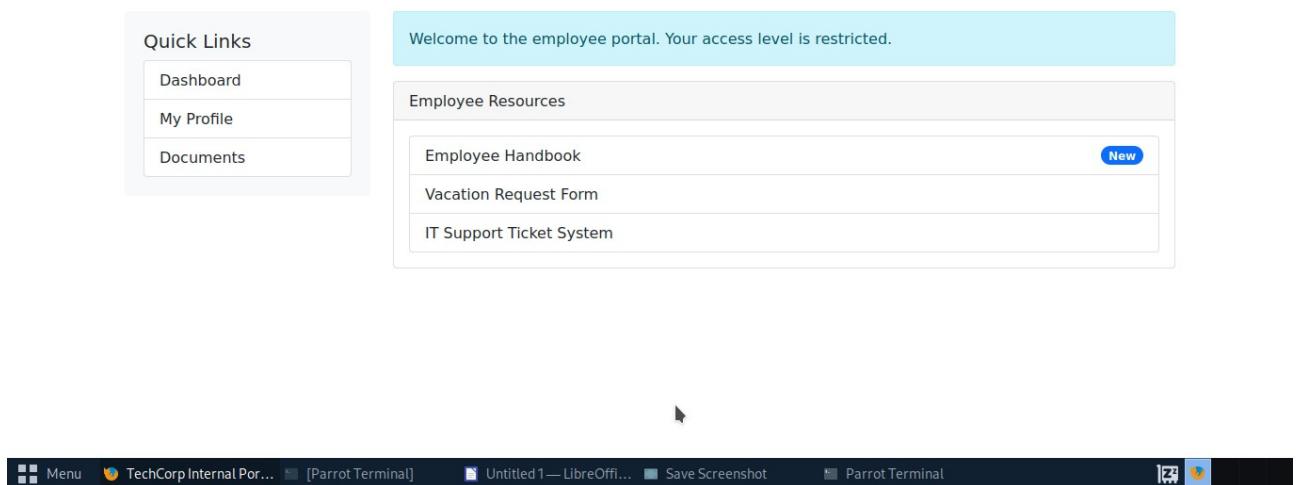
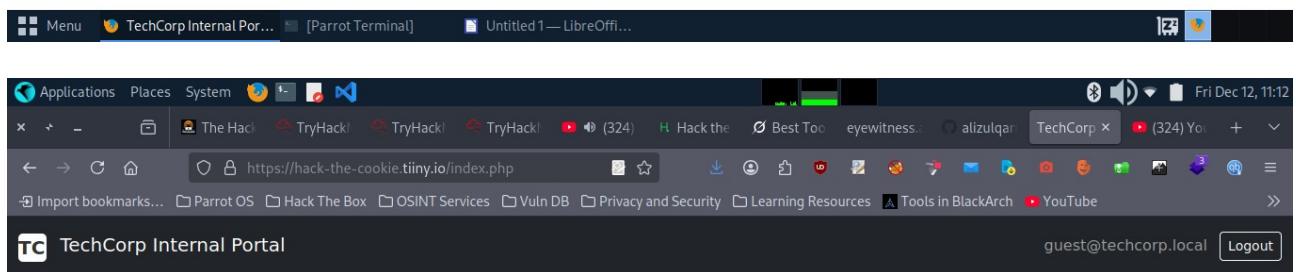
TechCorp

Employee Login

Username

Password

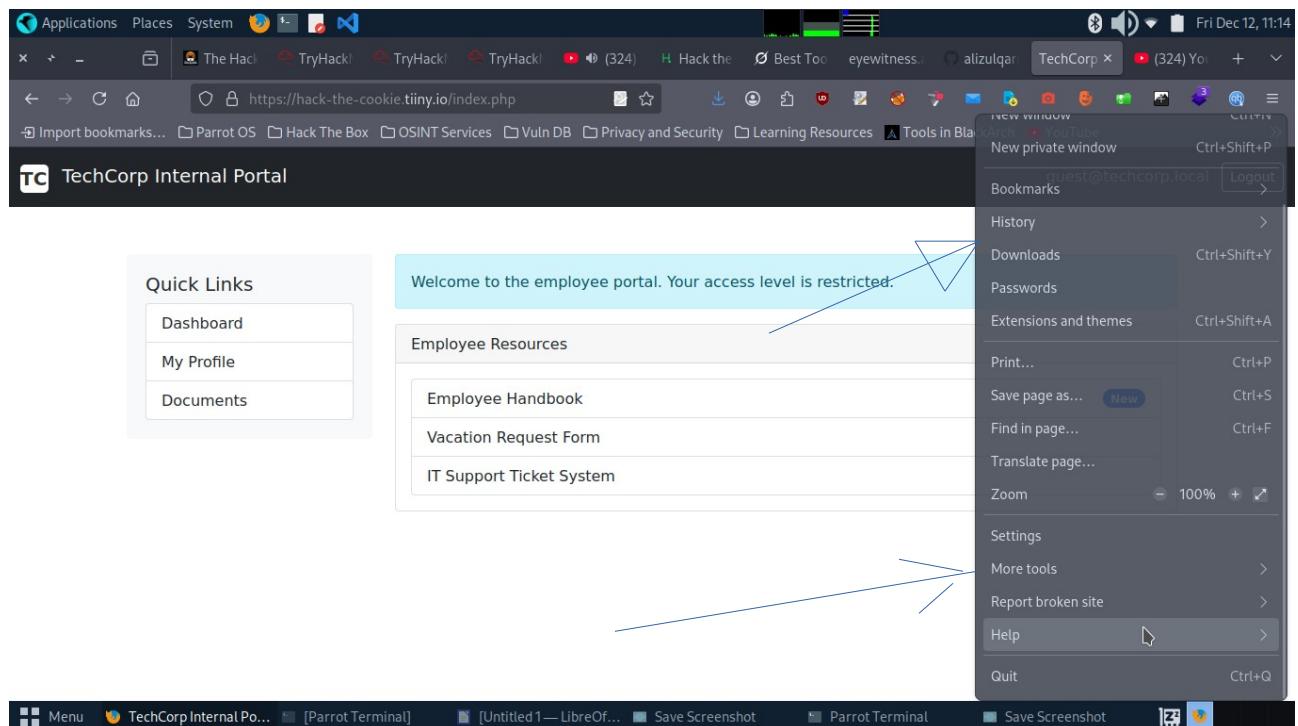
Login

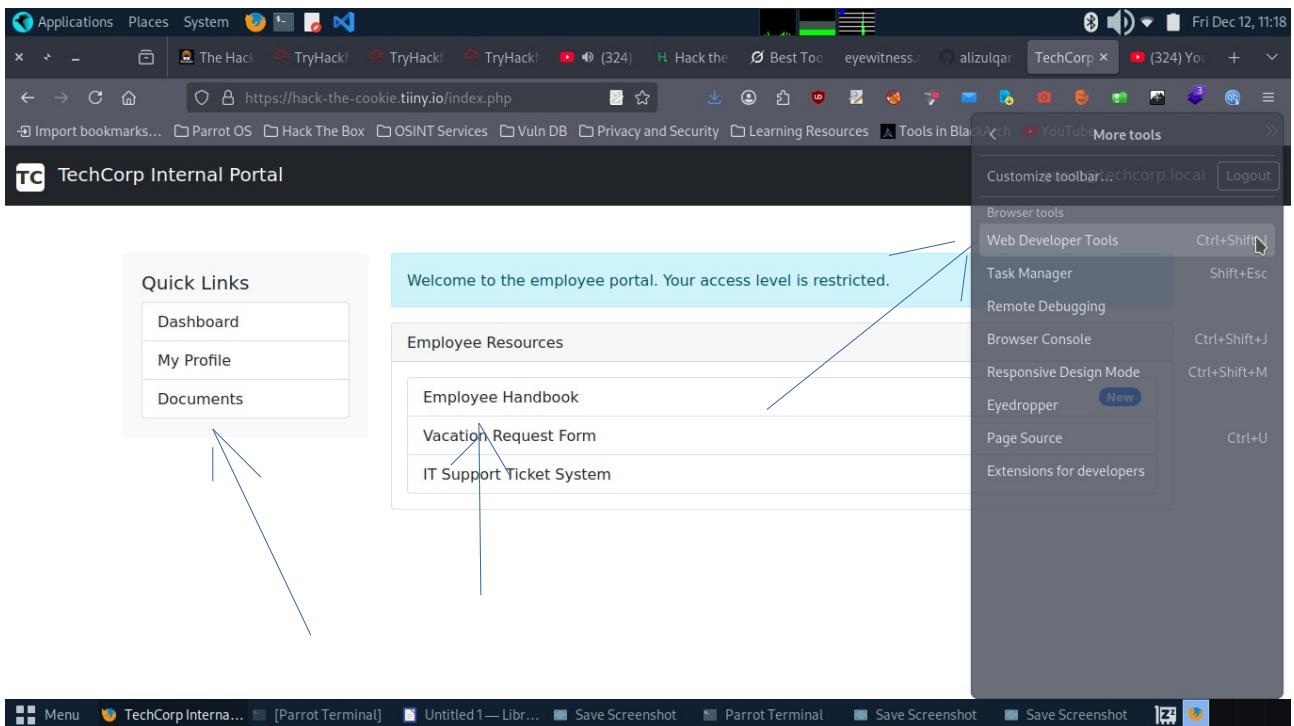


Step 2: Inspect the Session Cookie Using Developer Tools

1. With the dashboard loaded, open your browser's developer tools (press F12 or right-click > Inspect).
2. Navigate to the "Application" tab (or "Storage" in some browsers).
3. Under "Cookies," locate the domain's cookies and find the one named user_session.
4. Copy the value of user_session. It should look something like this (example value):

eyJ1c2VyX2lkIjoxLCJ1c2VybmFtZSI6Imd1ZXN0Iiwicm9sZSI6Imd1ZXN0IwiZW1haWwiOiJndWVzdEB0ZWNoY29ycC5sb2NhBCJ9





Step 3: Decode the Cookie

1. Open a terminal or command prompt.
2. Use the base64 command to decode the copied cookie value:
text

```
echo  
"eyJ1c2VyX2lkIjoxLCJ1c2VybmFtZSI6Imd1ZXN0Iiwicm9sZSI6Imd1ZXN0IwiZW1haWwi  
OiJndWVzdEB0ZWNoY29ycC5sb2NhbcJ9" | base64 -d
```

3. The output will be a JSON object revealing the session details:

```
{"user_id":1,"username":"guest","role":"guest","email":"guest@techcorp.local"}
```

This confirms the cookie stores user data in plain text after Base64 decoding, making it vulnerable to tampering.

Step 4: Modify and Re-Encode the Cookie

1. Edit the JSON object to change the "role" from "guest" to "admin":

```
{"user_id":1,"username":"guest","role":"admin","email":"guest@techcorp.local"}
```

2. Re-encode the modified JSON back to Base64:

```
echo '{"user_id":1,"username":"guest","role":"admin","email":"guest@techcorp.local"}' | base64
```

3. The new encoded value will be:

```
eyJ1c2VyX2lkIjoxLCJ1c2VybmFtZSI6Imd1ZXN0Iiwicm9sZSI6ImFkbWluIwiZW1haWwiOiJnd  
WVzdEB0ZWNoY29ycC5sb2NhbcJ9
```

Step 5: Replace the Cookie and Reload

Return to the browser's developer tools and the Cookies section.

- Edit the user_session cookie by pasting the new Base64-encoded value.

- Save the changes and reload the page (F5 or refresh button).
- The dashboard should now reflect admin privileges, granting access to additional features and revealing the flag

Congratulations you got your flag

