**CyberForge CTF: Hands-On Evaluation of Practical Cybersecurity Skills in Learning Management Systems| A Comprehensive Walkthrough**

.

**Task 01 – Introduction**

* Explore our customized TryHackMe area built for studying cybersecurity inside educational environments. Dive into a simulated environment to find weaknesses in a Learning Management System (LMS). Engage in hands-on challenges to grasp real-world assault techniques and defense measures. Improve security awareness and defense abilities by engaging in interactive activities that imitate prevalent cyber attacks. Compete with peers to safeguard the LMS against potential threats and boost your cybersecurity expertise. Join us in boosting cybersecurity awareness and preserving educational systems from digital hazards.

A screenshot of a computer

Description automatically generated

**Task 02 – Recon**

* The opening assignment in our Capture The Flag (CTF) challenge involves performing reconnaissance using Nmap, a sophisticated network scanning tool. The purpose is to detect open ports on a target system, which is vital for understanding the network topology and potential entry points for exploitation. This activity establishes the framework for succeeding tasks, enabling participants to obtain crucial knowledge about the target system's services and vulnerabilities.

A screenshot of a computer

Description automatically generated

* A hint is given to the player, saying to scan all ports with Nmap.
* The user has to perform a Nmap scan on the target. All the ports should be scanned, otherwise non- standard ports may not be displayed in the scan results.

A screen shot of a computer

Description automatically generated

From the Nmap scan results, the player can understand that the following ports are open,

* FTP
* SSH
* HTTP
* Blackice-icecap 8081

How many ports are open?: 4

What is special open port - 8081

**Task 03 – FTP Enumeration**

* The introductory task in our Capture The Flag (CTF) challenge involves undertaking reconnaissance using Nmap, a powerful network scanning tool. The objective is to discover open ports on a target machine, which is crucial for understanding the network topology and potential entry points for exploitation. This activity creates the framework for subsequent activities, enabling participants to gather critical knowledge about the target system's services and vulnerabilities.

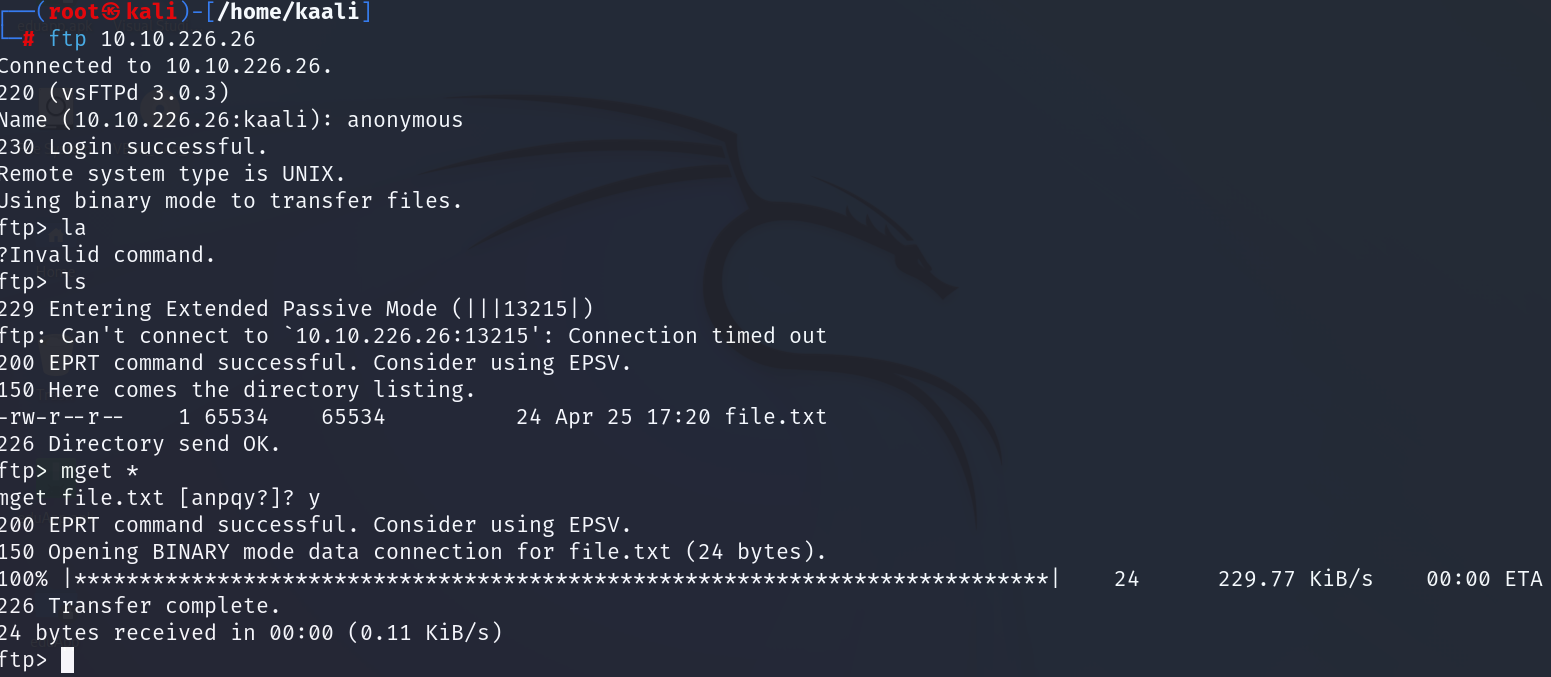
A screenshot of a computer

Description automatically generated

* The first step in penetrating the FTP server is to test for the anonymous login.
* Anonymous login is enabled in the FTP server and player can find the text file.

Steps for FTP Enumeration:

1. Identify FTP Server: Obtain the FTP server's IP address or hostname that you intend to enumerate.
2. Connect to FTP Server: Use an FTP client like ftp or FileZilla to connect to the FTP server.
3. Log in Anonymously: Once connected, attempt to log in anonymously. If prompted for a username, use anonymous as the username and provide your email address (e.g., user@example.com) as the password.



* How can you log to the FTP server - anonymous
* What is contain inside it – use the command ls the is file.txt
* File.txt
* What is the Flag? – download the file using mget and read it.

FLAG{F7P\_L0gin\_Succ3ss}

**Task 04 – Source Code Review**

* There is web service operating on port 80. So Need to go for that and, In this work, your purpose is to study the source code of a particular program to reveal a secret flag. Source code review is a key ability in cybersecurity, as it helps you to uncover vulnerabilities and secret information encoded inside the code.

A screenshot of a computer

Description automatically generated

So, in order to view the source code, player should enter “view-source” command in the URL. Player will come across some suspicious lines of comments as follows.

A computer screen shot of a program

Description automatically generated

What is the flag?

FLAG{X3r0\_1s\_4\_7r34s0r\_70\_1n\_t3h\_70\_7r34s0r}

**Task 05 – Hidden Directory Discovery**

* In this job, your purpose is to discover and access a hidden directory . These files are widely used to inform web spiders about which portions of the website should not be crawled or indexed.
* Discovering hidden folders can disclose useful information about the web server's setup and perhaps unearth sensitive data. Use your investigation abilities to explore through the secret routes and finish the task successfully.

A screenshot of a computer

Description automatically generated

What is the name of the secret directory? – maintain

Scan with gobuster tool use big.txt

A screen shot of a computer

Description automatically generated

What txt commonly used to instruct web crawlers – robots.txt

A screenshot of a computer

Description automatically generated

This is like encrypted need to decrypt so use cyberchef decode with base 64

What is the Flag on that text in file - FLAG{B4s3\_643n73d\_7h3\_7r34s0r\_70\_7h3\_7r34s0r}

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

What is the Flag

* Flag{D!rec7ory\_enm\_Don

**Task 06 – Play with cookie**

* In this challenge, participants will employ a Cross-Site Scripting (XSS) attack to exploit a vulnerability in a web application and steal a user's cookie data. XSS attacks include inserting malicious scripts into web pages seen by other users, allowing attackers to take illegal activities on behalf of the victim.   
  The purpose of this job is to illustrate how XSS may be used to extract sensitive information, such as session cookies, which can subsequently be used for session hijacking or other malicious activities. By learning and implementing this attack, participants will get insights into the severity of XSS vulnerabilities and the relevance of safe coding standards in web development.
* In this task, your objective is to leverage a Cross-Site Scripting (XSS) vulnerability to steal a user's cookie from a target web application. XSS allows attackers to inject malicious scripts into web pages, which can be executed by unsuspecting users' browsers.

Follow these steps:

1. Identify a vulnerable input field or parameter on the target web application.
2. Craft a malicious XSS payload designed to capture the victim's cookie when executed.
3. Inject the XSS payload into the vulnerable input field or URL parameter.
4. Execute the attack by triggering the XSS payload (e.g., by visiting a manipulated URL or interacting with the vulnerable input).

Use can use automated tools.(PwnXss,Dalfox,Xsser)

A screenshot of a computer

Description automatically generated

For Xss attack we need input field. In search we can input a paloyd

A screen shot of a computer

Description automatically generated

A black rectangular object with white border

Description automatically generated

Lets try to get cookie by <script>alert(document.cookie)</script>

A close up of a logo

Description automatically generated

A screenshot of a computer

Description automatically generated

This like encrypted lets decrypt.

A screenshot of a computer

Description automatically generated

* what is Vulnerable parameter - name
* What payload can be used to steal the cookie? <script>alert(document.cookie)</script>
* What is the flag?

Top of Form

FLAG{XSS\_1nj3c7\_7h3\_7r34s0r\_70\_7h3\_7r34s0r}

**Task 07 – Brute-Force Attack**

* In this challenge, participants will conduct a brute-force assault aiming at gaining unauthorized access to a target system or application. This attack approach includes systematically testing different combinations of users and passwords until the proper credentials are discovered. By employing tools like Hydra or John the Ripper, participants will receive practical experience in understanding the efficacy of brute-force assaults and the need of setting strong password rules and security measures to counteract such threats. This exercise underlines the need of robust authentication procedures and gives participants with vital skills to fight against brute-force attacks in real-world cybersecurity scenarios

A screenshot of a computer

Description automatically generated

In this work, you will show a brute-force assault targeting the password field on a login page to obtain unauthorized access.  
  
Follow these steps:

1. Identify the target login page where you have a known valid username.   
2. Use a brute-force tool (e.g., Hydra, Burp Suite Intruder) to automate password guessing for the discovered account.   
3. Configure the brute-force tool to create and test alternative password combinations (e.g., dictionary-based attack, incremental attack) against the login form.   
4. Monitor the brute-force operation and wait for a successful password guess

* We can get the username of this institute b recon the web page

A close-up of a contact us

Description automatically generated

* You can use burp,hydra to get the password hint os book so grep the word book form rockyou.txt

A close up of a black background

Description automatically generated

* I am using burp to brute force so first capture the request

A screenshot of a computer

Description automatically generated

* Send to intruder, add parameters.

A screenshot of a computer

Description automatically generatedTop of Form

* Set the paylod, copy or text upload

A screenshot of a computer

Description automatically generated

* Start he attack, chek the length of response

A screenshot of a computer

Description automatically generated

Blackbook has different length use it and try to log

A screenshot of a confirmation form

Description automatically generated

Done.

1. What is the username - james.carom@edu.com
2. What is the password - blackbook
3. What is the Flag after Success login- flag{You\_have\_logged\_sucessfully}

**Task 07 – OTP Bypass**

* In this exercise, you will conduct an OTP bypass attack by recording and altering HTTP requests to authenticate without a valid OTP code.   
    
  Follow these steps:   
  Use a proxy tool (e.g., Burp Suite, OWASP ZAP) to intercept and collect HTTP traffic between the client and server during OTP authentication.   
  Navigate to the login page needing OTP authentication and commence the login procedure.   
  Capture the HTTP request containing the OTP code (usually found in the request headers or parameters).   
  Use the proxy tool to edit the captured request and delete or change the OTP code argument.   
  Forward the amended request to the server and examine the server's response.   
  Alternatively, attempt to undertake brute-force assaults on the OTP parameter by making repeated requests with various OTP codes.

A screenshot of a computer

Description automatically generated

* Check the response headers

A screenshot of a computer

Description automatically generated

A screenshot of a confirmation form

Description automatically generated

A computer screen shot of a message

Description automatically generated

* What is the Header name pass OTP - X-OTP
* What is the Flag - FLAG{07P\_Bypassed}

**Task 08 – SQL Injection on Admin Login**

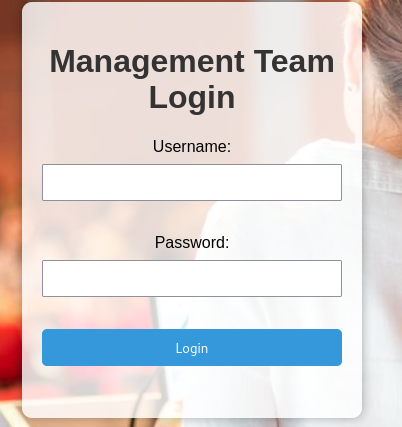
* Participants will employ the SQLmap tool to perform a SQL injection attack, seeking to expose weaknesses in a web application's database backend. This challenge will highlight the potential effect of SQL injection, allowing participants to automate the identification and exploitation of such vulnerabilities. By obtaining real experience with SQLmap, participants will expand their awareness of SQL injection threats and discover effective mitigation measures to defend online applications against this ubiquitous security issue.

In this challenge, you will show a SQL Injection (SQLi) attack to overcome authentication and get unauthorized access to the admin dashboard.   
  
Follow these steps:   
1. Identify the login form or endpoint for the admin team login on the website.   
2. Use Burp can collect the request   
3. Sqlmap may use to automate sql injection

A screenshot of a computer

Description automatically generated

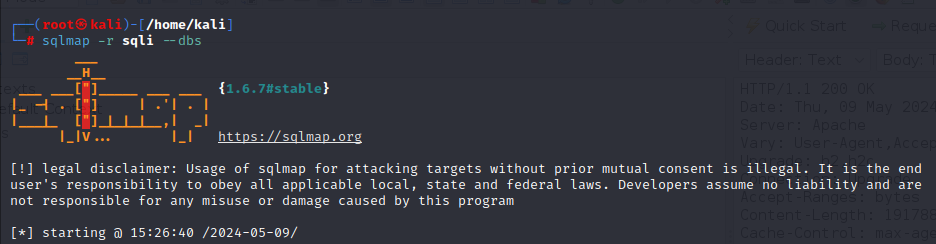
* Then we have admin dashboard. Check some link to login.
* Adman team can login. Lets do sql injection by using sqlmap

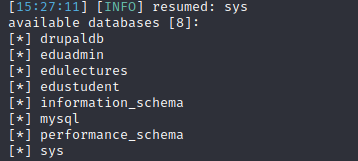


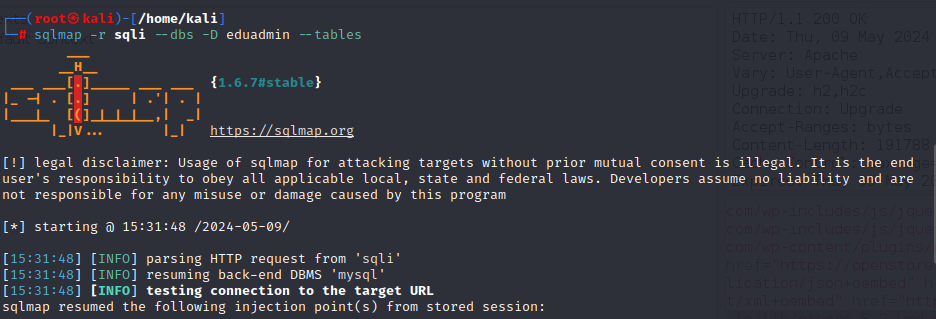
1. Capture the login request with burp

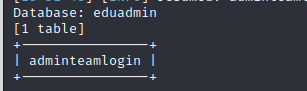


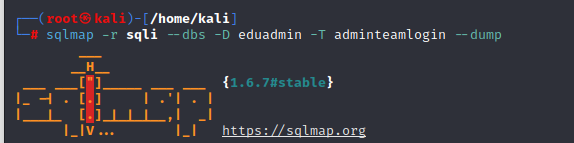
1. Save the file and attack with sqlmap.













What database contain Admin credentials – eduadmin

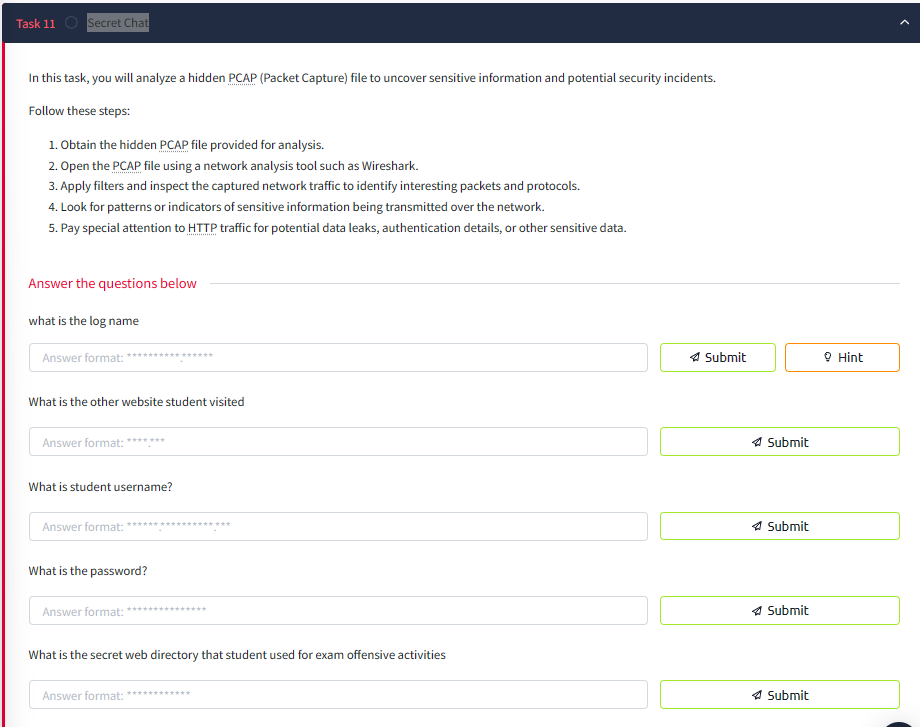
What is the admin name - Michael

What is the password  - 482c811da5d5b4bc6d497ffa98491e38

What is the password in clear text - password123

**Task 08 – Secret Chat**

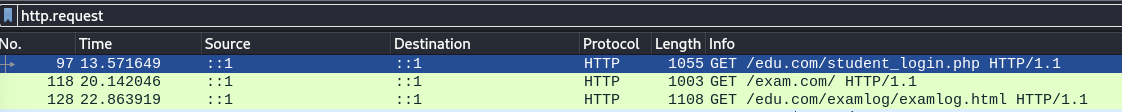
* Participants will engage in packet analysis using tools like Wireshark or tcpdump to intercept and analyze network traffic during a chat discussion. This experiment attempts to show how sensitive information, such as login passwords or personal messages, might be exposed through unencrypted network traffic. By examining intercepted packets, participants will receive practical insights into network-based dangers and the need of deploying encryption and secure communication protocols to safeguard sensitive data from interception. This hands-on exercise will strengthen participants' skills in identifying and mitigating network vulnerabilities, stressing proactive security methods to defend against unwanted access and data breaches in real-world cybersecurity scenarios.



A screenshot of a computer

Description automatically generated

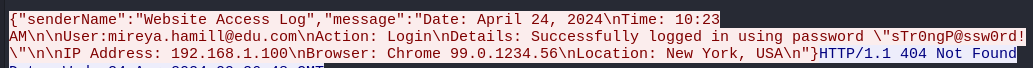
* There is file in examplog download it .
* Open the pcap file with wire shark and chck http requst



* There are some post req lets see.



* Follow http stream



* We can get student login name and password
* There is another GET request



* what is the log name - eduexamlog.pcapng
* What is the other website student visited - exam.com
* What is student username? - mireya.hamill@edu.com
* What is the password? - sTr0ngP@ssw0rd!
* What is the secret web directory that student used for exam offensive activities - secret\_share

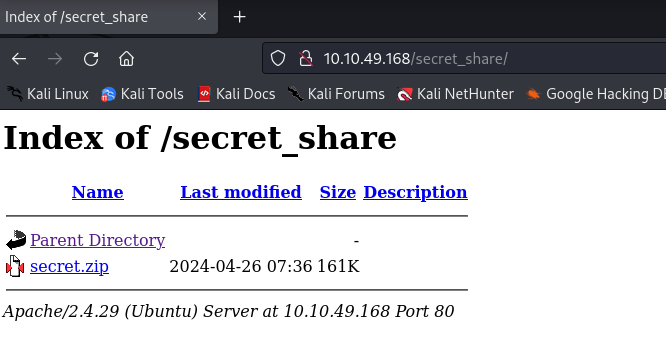
**Task 09 - Forencis Investigation**

* Students try to trade the exam answers in secret way you have to uncover the mechanism.   
  In this job, you will exhibit abilities in password cracking and steganography by extracting secret material from a password-protected ZIP file including audio, picture, and text files.

Follow these steps:

1. Download the ZIP File: Obtain the password-protected ZIP file supplied for the challenge.
2. Initiate Brute-Force assault: Use a password-cracking program (e.g., John the Ripper, Hashcat) to execute a brute-force assault on the ZIP file's password. Generate a password list (e.g., rockyou.txt) or use predetermined criteria to guess probable passwords.

1. Extract Files from ZIP: Once the password is cracked, extract the contents of the ZIP file to reveal the hidden files (music, image, text).
2. Analyze Steganography in Files: Examine the extracted files (music, picture, text) for hidden information using steganography tools (e.g., Steghide, StegCracker): For images: Use steganography techniques to find hidden messages or data buried within the image pixels.For audio: Analyze audio files for hidden messages or signals encoded using steganography techniques. For text: Look for hidden content within plaintext files using steganography analysis tools.



* Zip file is protected with password we need to crack it.

A screenshot of a computer

Description automatically generated

* Crack using fcrackzip

A black background with white text

Description automatically generated

A screenshot of a computer

Description automatically generated

1. **Image**

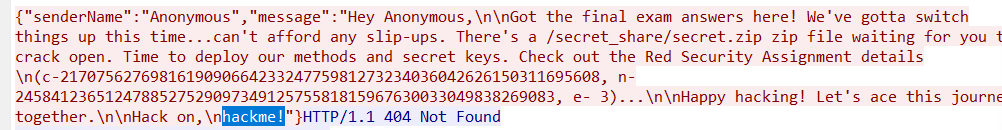
* Use stegnogrphy technique

1. steghide

A screenshot of a computer

Description automatically generated

1. Protected with password, first need to get password. In pcap here was password hackme!



A computer screen shot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

1. Text file has song but these can be hidden message in spaces.

A close up of a black background

Description automatically generated

1. There is audio. When listing it I realized that it is mose code. Capture the code by hearing to us.

Flag{S0und\_lik3\_m3ssage}



**Task 10 - Cryptography challenges**

In this challenge, you will decrypt parameters (c, n, e) extracted from a PCAP file to obtain the flag. The PCAP file likely contains network traffic with encrypted data, and you need to recover the plaintext message

A screenshot of a computer

Description automatically generated

* I have c,n,e then I use
* Make python program for decrpt

A screenshot of a computer

Description automatically generated

A close up of a computer screen

Description automatically generated

What is the Encryption algorithm used – RSA

What is the flag - Flag{4ll\_!nf0\_D3cryped}

**Task 11 – Reverse Engineering Challenges**

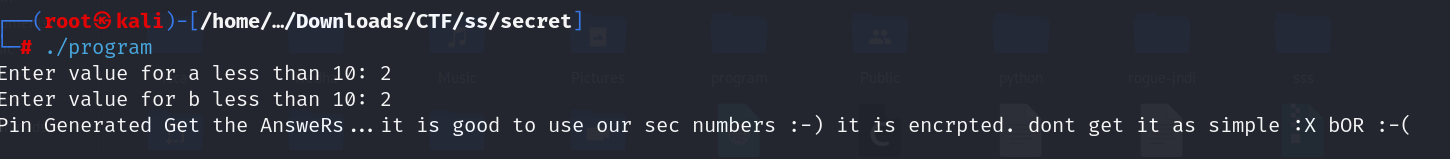
* In this challenge, you will reverse engineer a software to identify the process utilized for generating a PIN. Once you understand the mathematical process, your aim is to produce the proper PIN and use it to extract the flag contained in a file entitled answers.txt.

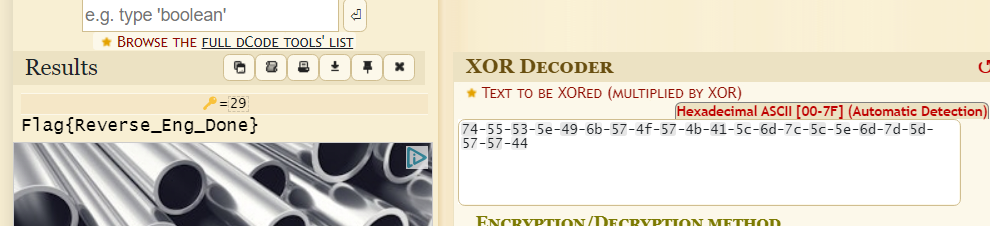
1. Obtain the Program: Get the software or executable that creates the PIN.   
2. Analyze the Program: Use tools like Ghidra, IDA Pro, or GDB to learn how the software generates the PIN from provided input.   
3. Identify the PIN Calculation Method: Look for patterns or activities in the program's code that determine how the PIN is produced.   
4. Generate the right PIN: Implement the stated calculation procedure in a script or program to generate the right PIN using the input data.   
5. Retrieve the Flag: Use the created PIN to access and get the flag from the answers.txt file. The flag may be encrypted or concealed using the PIN.

A screenshot of a computer

Description automatically generated

* There is program first try to run





What are the Secret numbers 5,6

What is the pin 29

What is the flag Flag Flag{Reverse\_Eng\_Done}

**Task 12 - Mobile Pen testing**

In this assignment, you will undertake mobile penetration testing by reverse engineering a mobile application to identify critical information or secrets buried inside the app.



1. Set Up the Mobile Testing Environment: Set up a testing environment using tools like Android Studio, APKTool, or jadx to decompile the APK file and investigate its contents.   
2. Decompile the APK File: Use APK decompilation tools (e.g., jadx, APKTool) to decompile the APK file into its matching source code and resources.

What is the file contain sensitive information hardcord - strings.xml

What is AWS\_ID - MOBILEP3N735T!N6

What is AWS Secret Key - wJalrXUtnFEMIK7MDENG

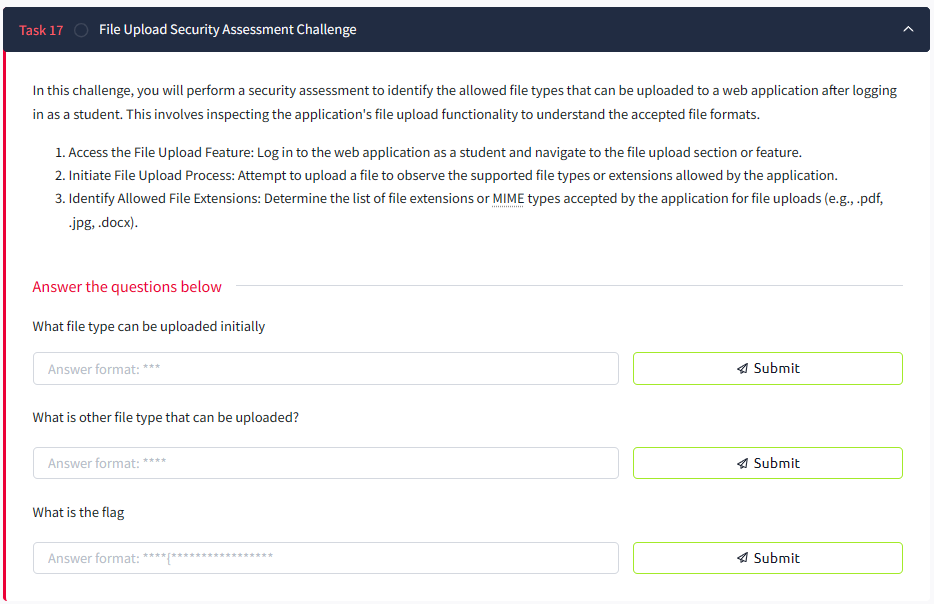
Who is android authorities - com.mycompany.myhh.provider

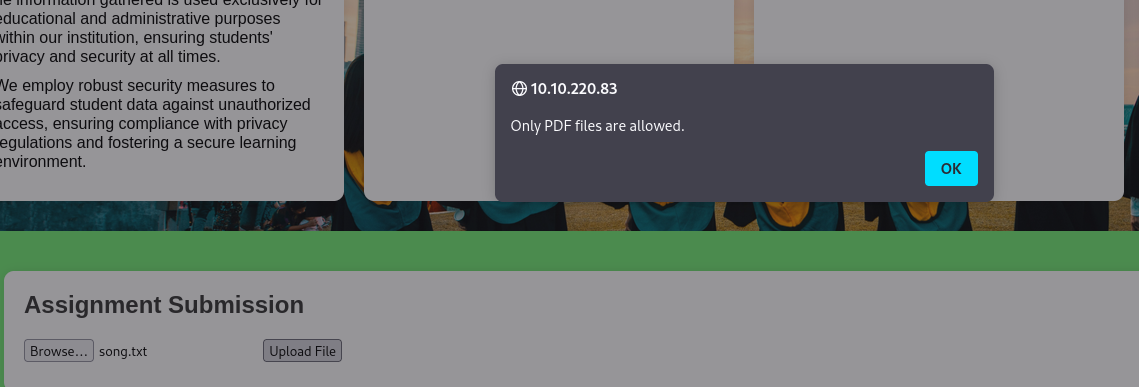


**Task 13 - File Upload Security Assessment Challenge**

* In this task, you will undertake a security assessment to determine the acceptable file types that can be uploaded to a web application after logging in as a student. This requires evaluating the application's file upload capability to understand the allowed file types.

1. Access the File Upload Feature: Log in to the online application as a student and click to the file upload area or feature.   
2. Initiate File Upload Process: Attempt to upload a file to observe the supported file types or extensions allowed by the program.   
3. Identify Allowed File Extensions: Determine the list of file extensions or MIME types accepted by the program for file uploads (e.g., .pdf, .jpeg, .docx).





A grey rectangular sign with white text

Description automatically generated

A screenshot of a video chat

Description automatically generated

What file type can be uploaded initially pdf

What is other file type that can be uploaded? html

What is the flag - Flag{Upload\_vulnerable}.

**Tsask 14 - Cookie Manipulation Challenge**

In this assignment, you will locate and enable a secret upload button on a web application by manipulating cookies. The upload feature is restricted to individuals with administrator access .

1. view Cookies: Use browser developer tools to view cookies linked with your session. Look for cookies relating to user rights or settings (e.g., admin cookie).   
2. Manipulate the Admin Cookie: Modify the value of the admin cookie from 0 to 1 using browser developer tools or a cookie-editing plugin.   
3. Enable the Upload Functionality: After adjusting the admin cookie setting, return the upload area to enable the hidden upload button.   
4. Upload a File: Use the now-enabled upload option to upload a file and complete the challenge.

A screenshot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated

A screenshot of a computer program

Description automatically generated

A white rectangular object with black lines

Description automatically generated

A close-up of a computer screen

Description automatically generated

What is the initial cookie value – 0

What is the flag - Flag{4dm!n\_53curi7y\_Byp4ss3d}

**Task 15 Insecure Direct Object Reference (IDOR) Challenge**

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

A screenshot of a computer

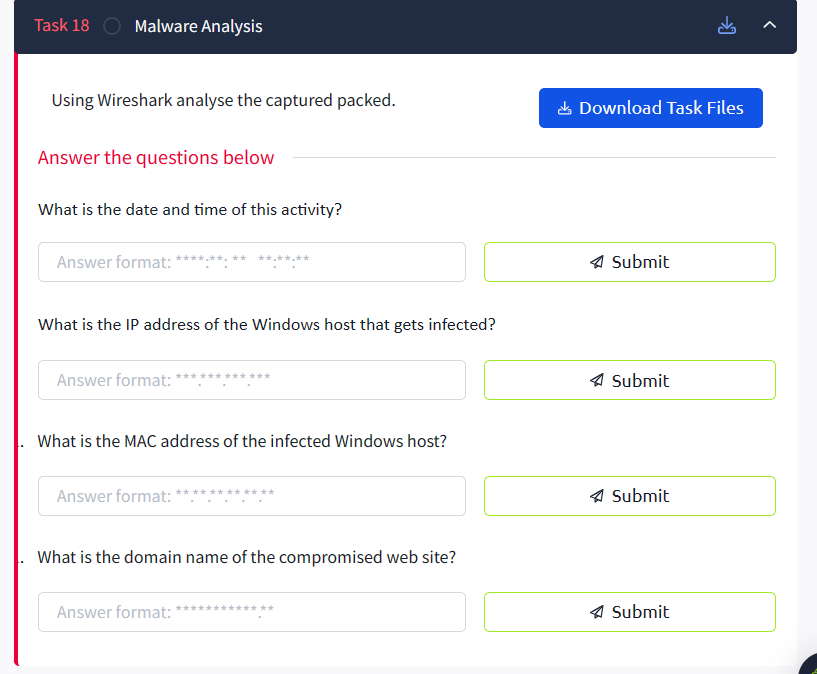
Description automatically generated

What is the vulnerable ID contain flag – 0009

What is the Flag - Flag{IDOR\_exploited}

**Task 16 Malware Analysis**

* In this task, participants will investigate suspected malware using a mix of Wireshark, Flare VM, and VirusTotal. First, they will use Wireshark to capture and study network traffic created by the virus, discovering any dangerous communication patterns. Next, participants will employ Flare VM to study the malware in a controlled environment, doing static and dynamic analysis to understand its behavior and extract indications of compromise (IOCs). Finally, participants will submit the suspicious file to VirusTotal for complete analysis using several antivirus engines, getting insights into the malware's detection rate and accompanying threat intelligence. This exercise teaches participants with practical skills in malware analysis, boosting their capacity to recognize and respond to malware events efficiently.



1. What is the date and time of this activity? –

2014:12: 09 04:48:41

**Text, table

Description automatically generated**

1. What is the IP address of the Windows host that gets infected?

192.168.204.137

Text

Description automatically generated

1. What is the MAC address of the infected Windows host?

00.50.56.f8.ec.99

Text

Description automatically generated

1. What is the host name of the infected Windows host?

38NTRGDFFQKR-PC<00>

Graphical user interface

Description automatically generated with medium confidence

1. What is the domain name of the compromised web site?

Digiwebname.in

A screen shot of a computer

Description automatically generated

1. What is the IP address of the compromised web site?

205.234.186.111

A picture containing calendar

Description automatically generated

**Task 17 - Server Exploitation**

* In this challenge, you will undertake reconnaissance and information gathering on a target server to discover services operating on specified ports. By enumerating open ports and identifying associated services, you will acquire vital information for later phases in the server exploitation process.   
    
  Follow these procedures to accomplish the reconnaissance phase of the server exploitation challenge:   
  1. Identify Target Server: Obtain the IP address or domain name of the target server you will be examining.   
  2. Perform Port Scanning: Use tools like Nmap or Masscan to scan the target server for open ports and services.

A screenshot of a computer

Description automatically generated

A computer screen shot of white text

Description automatically generated

A screenshot of a computer

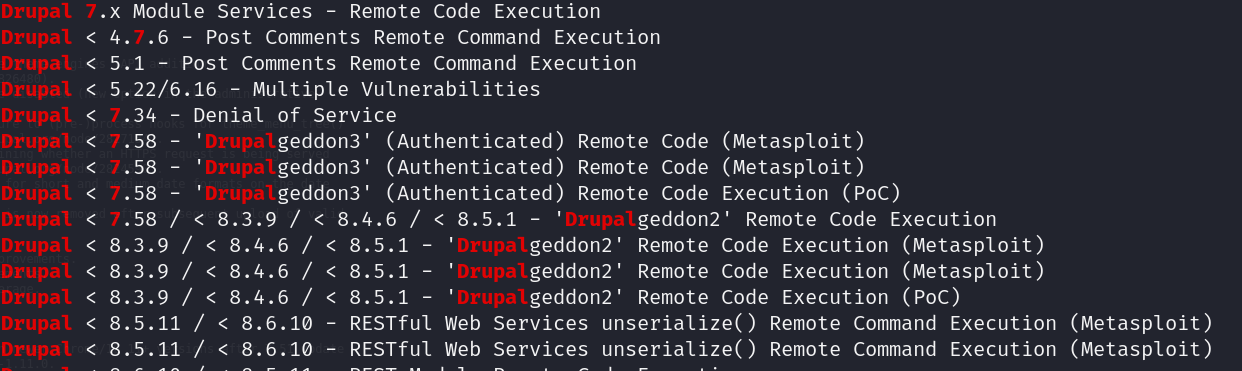
Description automatically generated

A screenshot of a computer

Description automatically generated

A screen shot of a black background

Description automatically generated



What is the service running on port 8081 – blackice-icecap

What is the Drupal version running - Drupal 7.54

What is the website name running – eduweb

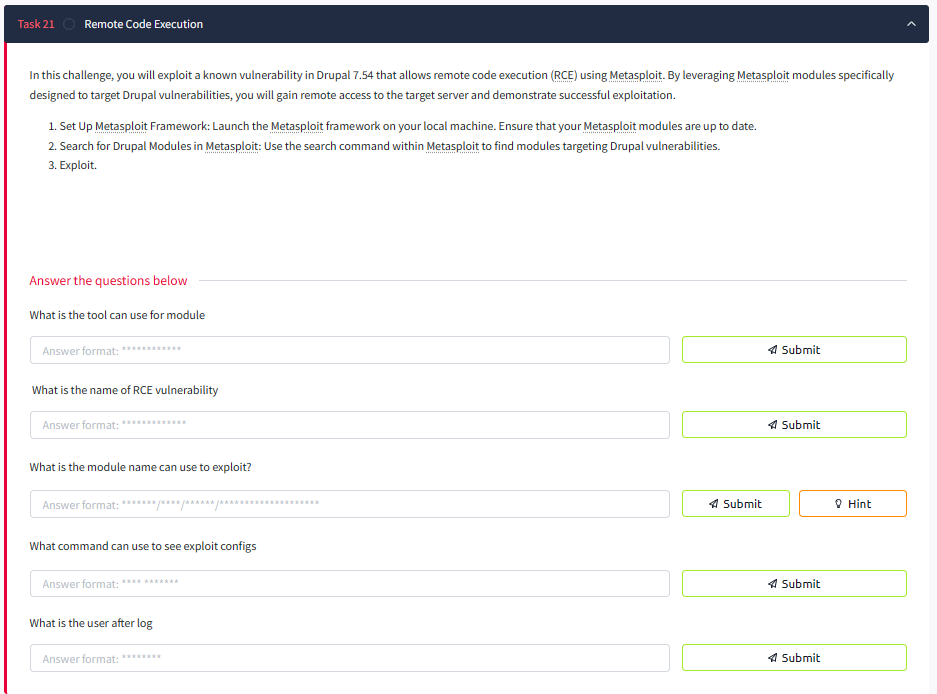
What Text file helpful for find version details – CHANGELOG.txt

What is the vulnerability of that version - Remote Code Execution

In this challenge, you will attack a known vulnerability in Drupal 7.54 that permits remote code execution (RCE) using Metasploit. By employing Metasploit modules particularly built to target Drupal vulnerabilities, you will get remote access to the target server and show successful exploitation.

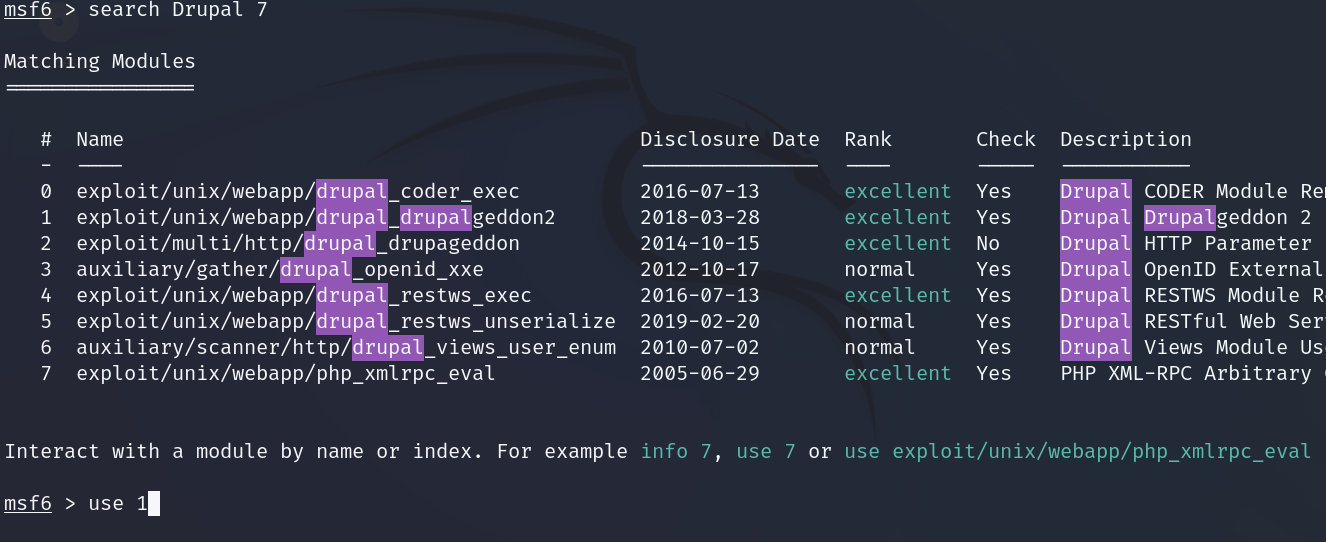
1. Set Up Metasploit Framework: Launch the Metasploit framework on your local PC. Ensure that your Metasploit modules are up to date.   
2. Search for Drupal Modules in Metasploit: Use the search command within Metasploit to identify modules targeting Drupal vulnerabilities.   
3. Exploit.

**Task 18 Remote Code Execution**



What is the tool can use for module – searchsploit

 What is the name of RCE vulnerability - Drupalgeddon2



What is the module name can use to exploit? - exploit/unix/webapp/drupal\_drupalgeddon2



What command can use to see exploit configs - Show options

A screenshot of a computer screen

Description automatically generated

What is the user after log - www-data

A screenshot of a computer program

Description automatically generated

A close-up of a computer screen

Description automatically generated

**Task 19 User Enumeration**

1. Identify Target System : Determine the system or directory where you suspect backup files (\*.bak) might be stored.
2. Search for Backup Files: Use the find command to locate all backup files (\*.bak) within the specified directory:

A screenshot of a computer

Description automatically generated

A close-up of a computer code

Description automatically generated

A close up of a blue background

Description automatically generated”

A screen shot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A computer screen shot of white text

Description automatically generated

A screenshot of a computer

Description automatically generated

**Task 20 Privilege Escalation**

A screenshot of a computer

Description automatically generated

* In this challenge, you'll perform privilege escalation by leveraging sudo -l to identify a misconfigured command and then using GTFOBins to exploit it for root access.



A close-up of a white background

Description automatically generated

A close up of a text

Description automatically generated

A black background with white text

Description automatically generated

A screenshot of a computer program

Description automatically generated