In this room, we will cover the following OWASP top 10 vulnerabilities:

1. Injection

2. Broken Authentication

3. Sensitive Data Exposure

4. XML External Entity

5. Broken Access Control

6. Security Misconfiguration

7. Cross-site Scripting

8. Insecure Deserialization

9. Components with Known Vulnerabilities

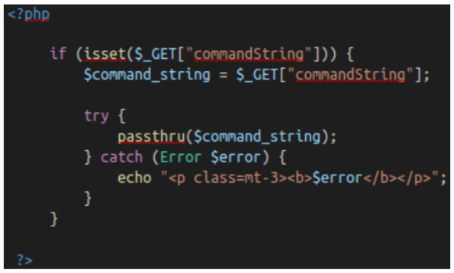
10. Insufficient Logging & Monitoring

Tasks:

Task 1, Task 2, Task 3 & Task 4:

Read all the information provided in these tasks and press "Complete."

EvilShell (evilshell.php) Code Example



```
<?php

    if (isset($_GET["commandString"])) {
        $command_string = $_GET["commandString"];

        try {
            passthru($command_string);
        } catch (Error $error) {
            echo "<p class=mt-3><b>$error</b></p>";
        }
    }

 ?>
```

Task 5:

Deploy the attached virtual machine (VM) and read the information in the task.

5.1 What unusual text file is present in the website's root directory?

To determine the file, access the console and execute the command "ls." Submit your answer as "drpepper.txt."

5.2 How many non-root/non-service/non-daemon users exist?

Execute the command "cat /etc/passwd" in the console. Submit your answer as "0."

5.3 What user is the application running as?

Type the command "whoami" in the console. Submit your answer as "www-data."

5.4 What is the user's shell set as?

Execute the command "cat /etc/passwd" and find the line corresponding to the "www-data" user. Read the same line to determine the directory. Submit your answer as "/usr/sbin/nologin."

5.5 What version of Ubuntu is running?

Type the command "lsb_release -a" in the console. Submit your answer as "18.04.4."

5.6 Print out the MOTD. What favorite beverage is displayed?

Use the command "ls /etc/update-motd.d" to see all the files related to the MOTD (Message of the Day). Locate the "00-header" file and display its contents with the command "cat /etc/update-motd.d/00-header." Submit your answer as "DR PEPPER."

Task 6:

Read the information provided in the task and press "Complete."

Task 7:

Read the information provided in the task and deploy the VM attached to this room.

What is the flag found in Darren's account?

Follow the instructions given in the task, register a new account with the username "darren," and log in using the created credentials. Copy and paste the flag from Darren's account into the answer box.

What is the flag found in Arthur's account?

Repeat the same steps as before, but this time use the username "arthur" to log in. Copy and paste the flag from Arthur's account into the answer box.

Task 8:

Read the information provided in the task and deploy the VM attached to this task.

Task 9:

Read the information provided in the task and press "Complete."

Task 10:

Read the information provided in the task and press "Complete."

Task 11:

What is the name of the mentioned directory?

Open the page in a web browser and navigate to the login page. View the source code to find the name of the directory.

Answer: "/assets"

Navigate to the directory you found in the previous question. Which file is likely to contain sensitive data?

After reaching the directory, look for a file with the ".db" extension.

Answer: "webapp.db"

Use the provided material to access the sensitive data. What is the password hash of the admin user?

Download the "webapp.db" file and execute the following commands in the terminal, assuming you are in the same location as the file:

```
sqlite3 web.db

.tables

PRAGMA table_info(users);

SELECT * FROM users;
```

Look for the password hash in the output.

Answer: (Provide the password hash found)

What is the admin's plaintext password?

Navigate to "crackstation.net" and enter the password hash you found. Follow the instructions to crack the hash and obtain the plaintext password.

Answer: (Provide the admin's plaintext password)

Login as the admin. What is the flag?

Use the obtained admin credentials to log in to the application. The flag will be displayed on the first page after logging in.

Answer: (Provide the flag)

Task 12:

Read the information provided in the task and press "Complete."

Task 13:

Read the information provided in the task. The answers to these questions can be found within the task.

What does XML stand for?

Answer: (Provide the full form of XML)

Is it mandatory to have an XML prolog in XML documents?

Answer: (Choose either "Yes" or "No")

Can XML documents be validated against a schema?

Answer: (Choose either "Yes" or "No")

How can the XML version and encoding be specified in an XML document?

Answer: (Provide the method to specify the XML version and encoding)

Task 14:

Read the information provided in the task. The answers can be found within the task text.

How do you define a new ELEMENT in XML?

Answer: "!ELEMENT"

How do you define a ROOT element in XML?

Answer: "!DOCTYPE"

How do you define a new ENTITY in XML?

Answer: "!ENTITY"

Task 15:

Read the information provided in the task and press "Complete."

Task 16:

Navigate to the website mentioned in the task.

Try to display your own name using any payload.

Attempt to read the "/etc/passwd" file.

What is the name of the user in "/etc/passwd"?

Answer: "flacon"

Where is Falcon's SSH key located?

Answer: "/home/falcon/.ssh/id_rsa"

What are the first 18 characters of Falcon's private key?

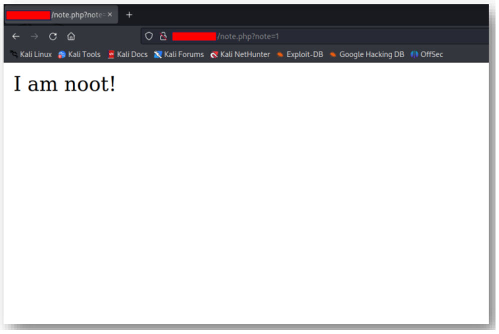
Answer: (Provide the first 18 characters of the private key)

Task 17:

Read the information provided in the task and press "Complete."

Task 18:

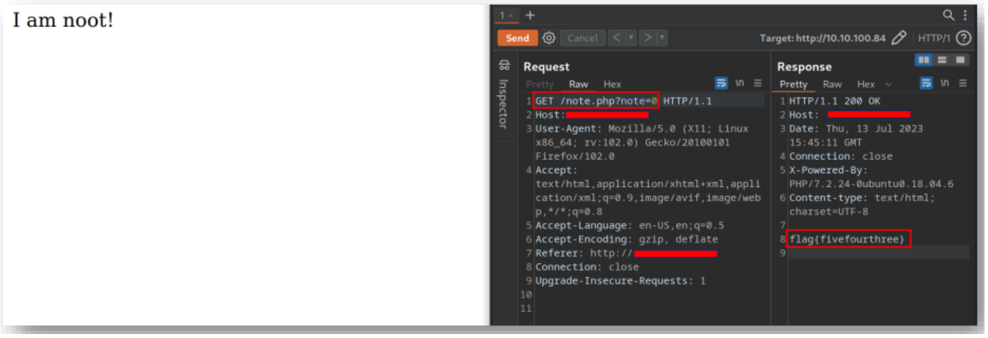
Read and understand how IDOR (Insecure Direct Object Reference) works.



I am noot!

Read the task text and press "Complete."

Deploy the machine and go to "http://MACHINE_IP" in your browser. Log in with the username "noot" and the password "test1234."



I am noot!

```
GET /note.php?note=0 HTTP/1.1
Host:[redacted]
User-Agent: Mozilla/5.0 (X11; Linux
x86_64; rv:102.0) Gecko/20100101
Firefox/102.0
Accept:
text/html,application/xhtml+xml,appli
cation/xml;q=0.9,image/avif,image/web
p,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://[redacted]
Connection: close
Upgrade-Insecure-Requests: 1
```

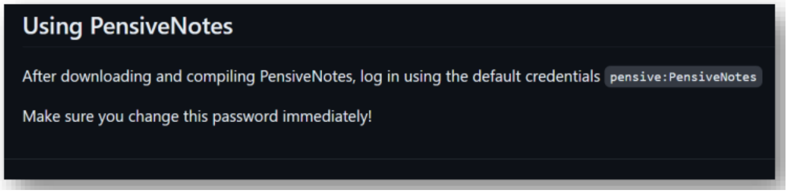
```
HTTP/1.1 200 OK
Host: [redacted]
Date: Thu, 13 Jul 2023
15:45:11 GMT
Connection: close
X-Powered-By:
PHP/7.2.24-0ubuntu0.18.04.6
Content-type: text/html;
charset=UTF-8

flag{fivefourthree}
```

Change the parameter in the URL from "note.php?note=1" to "note.php?note=0" to access another user's note and find the flag.

Task 19:

Read the information provided in the task and then deploy the provided machine.

Hack into the web application and find the flag!



Using PensiveNotes

After downloading and compiling PensiveNotes, log in using the default credentials `pensive:PensiveNotes`

Make sure you change this password immediately!

Search for default credentials for the given application and log in using those credentials. The flag will be displayed.

Task 20:

Read the information provided in the task and deploy the VM attached to the task.

Navigate to "http://MACHINE_IP" in your browser and click on the "Reflected XSS" tab in the navigation bar. Craft a reflected XSS payload that will cause a popup saying "Hello."

Answer: "ThereIsMoreToXSSThanYouThink"

Craft a reflected XSS payload that will cause a popup displaying your machine's IP address.

Answer: "ReflectiveXss4TheWin"

Add a comment and see if you can insert some of your own HTML.

Answer: "HTML_T4gs"

Create an alert popup box on the page displaying your document cookies.

Answer: "W3LL_D0N3_LVL2"

Change the text "XSS Playground" to "I am a hacker" by adding a comment and using JavaScript.

Answer: "websites_can_be_easily_defaced_with_xss"

Task 21:

Read the information provided

in the task.

Who developed the Tomcat application?

Answer: "Apache Software Foundation"

What type of attack that crashes services can be performed with insecure deserialization?

Answer: "Denial of Service"

Task 22:

If a dog was sleeping, would this be:

A) A State

B) A Behavior

Answer: "A Behavior"

Task 23:

What is the name of the base-2 formatting used to send data across a network?

Answer: "binary"

Task 24:

If a cookie has the path "webapp.com/login," what would be the URL that the user has to visit?

Answer: "webapp.com/login"

What is the acronym for the web technology that Secure cookies work over?

Answer: "HTTPS"

Task 25:

Follow the instructions in the task until you reach the "Modify Cookie" section.

1st flag (cookie value):

Copy the session ID and decode it with Base64 using a tool like CyberChef.

Answer: (Provide the decoded value)

2nd flag (admin dashboard):

Modify the cookie as instructed in the task.

Answer: (Provide the flag found on the admin dashboard)

Task 26:

Follow the instructions in the task. Once you have a reverse shell, enter the command "/bin/bash -i" to obtain a better shell. Search for the "flag.txt" file by using the following commands: "cd ..", "ls", and "cat flag.txt."

Tsk 27:a

Read the information provided in the task and press "Complete."

Task 28:

Read the information provided in the task and press "Complete."

Task 29:

How many characters are in "/etc/passwd"? (Use the command "wc -c /etc/passwd" to get the answer)

Search for the given hint "unauthenticated bookstore app RCE's" using a search engine.

Answer: (Provide the character count)

Bonus: Try using default credentials on the admin page to access it. You may also find an exploit by uploading files for books.

Task 30:

Read the information provided in the task. Download the log file and open it.

What IP address is the attacker using?

Look for entries from the same IP address repeatedly in the log file.

Answer: (Provide the attacker's IP address)

What kind of attack is being carried out?

Answer: "brute force"