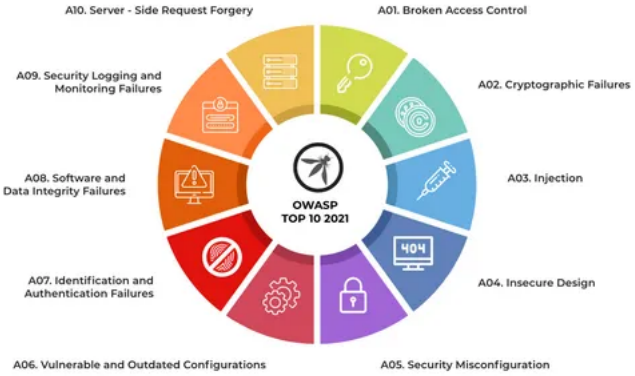
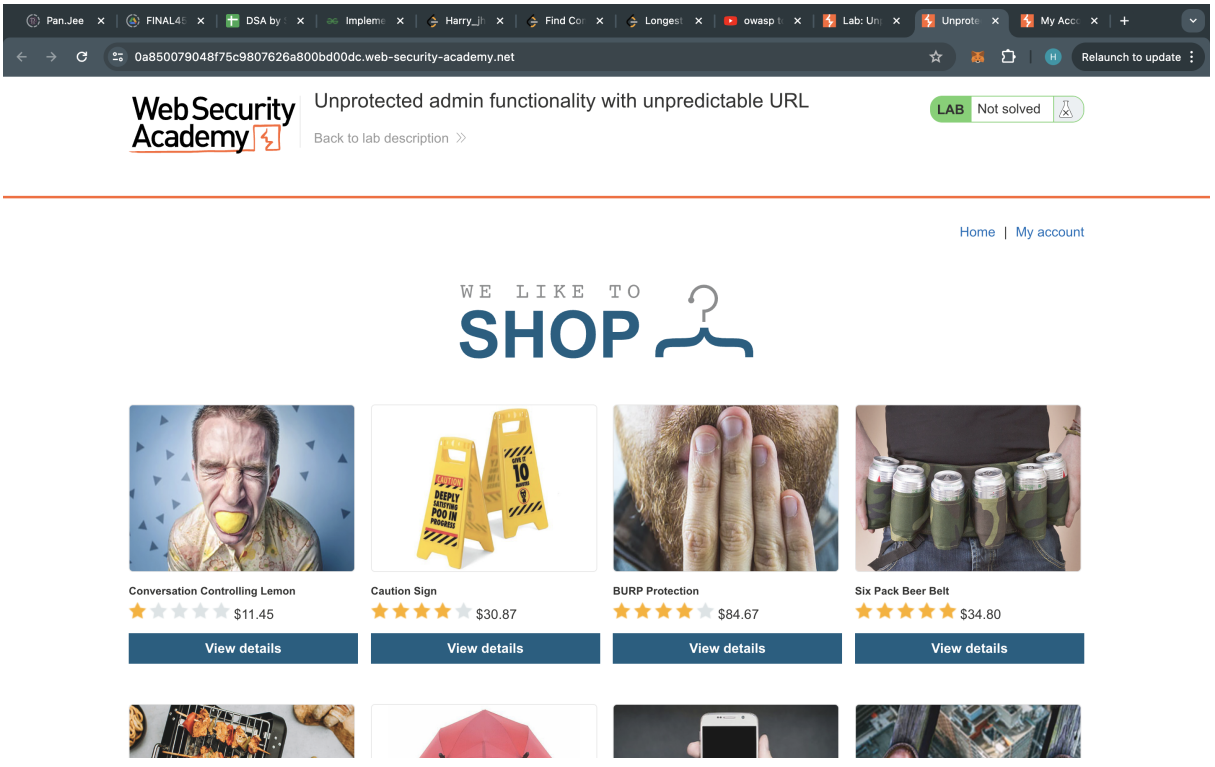
OWASP TESTING



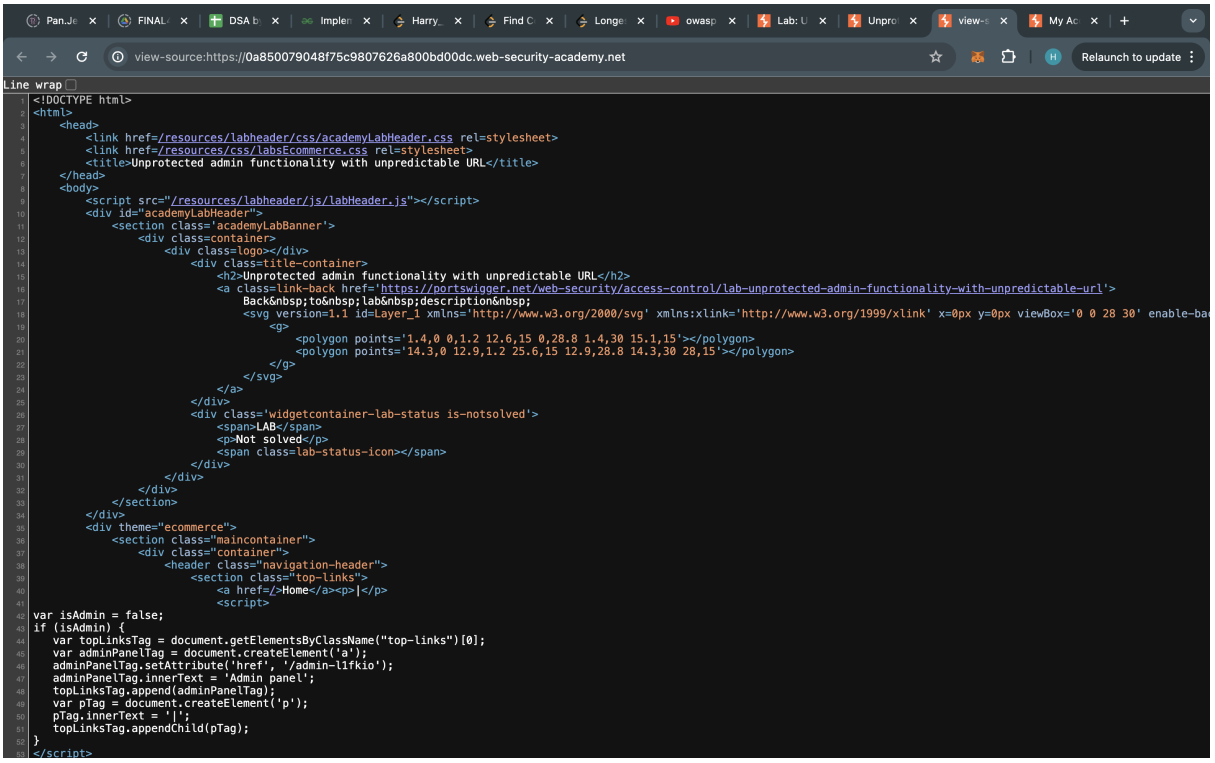
The OWASP Top 10 is a list of the most critical security risks to web applications

1. Broken Access Control (A01:2021)Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data.

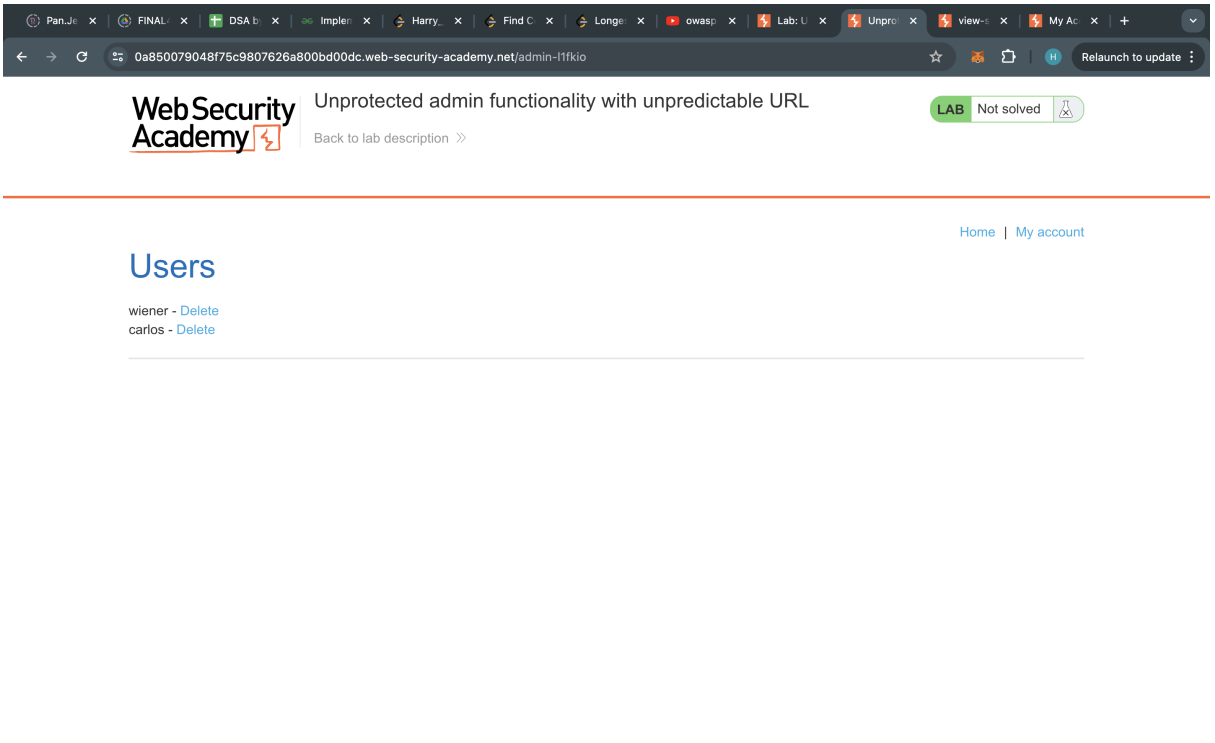
Here, is my the dynamic website



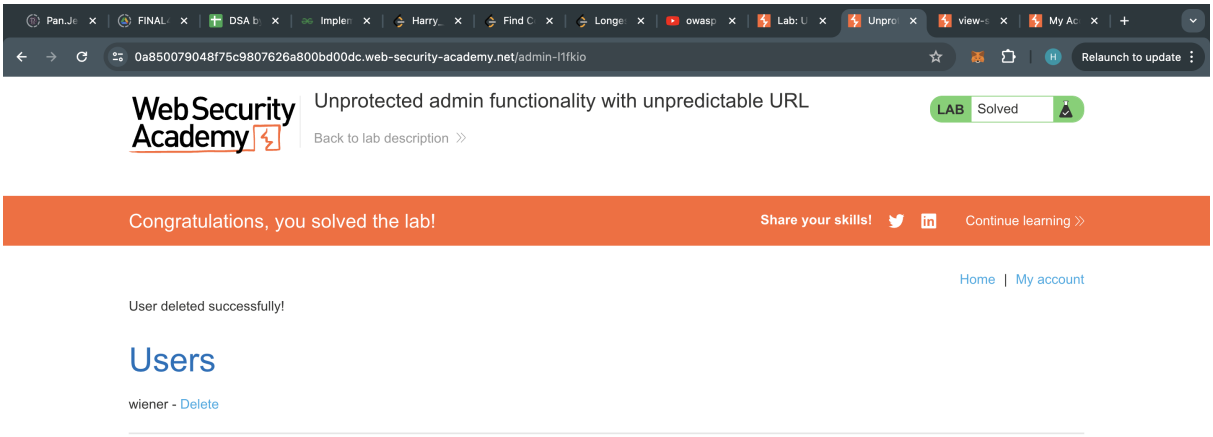
now we will access the admin dash as an unauthorized person using inspect code and we can see the admin code and see the admin dash link :- /admin-o5itnj



now as we access the admin dash now we can del anything from dash ex like carlos



after del carlos from admin dash from outside we can broke access control from the admin



2. Cryptographic Failures (A02:2021)Previously known as "Sensitive Data Exposure," this category focuses on failures related to cryptography, which often lead to exposure of sensitive data.

Firstly, start up the machine once it is booted up open Firefox and head to http://machine-ip:81/. Once there go to the log-in page and view the source code. You can view the source code by using the hotkey combo CTRL + U. This will open a separate page.

Have a look around the web app. The developer has left themselves a note indicating that there is sensitive data in a specific directory.

What is the name of the mentioned directory?

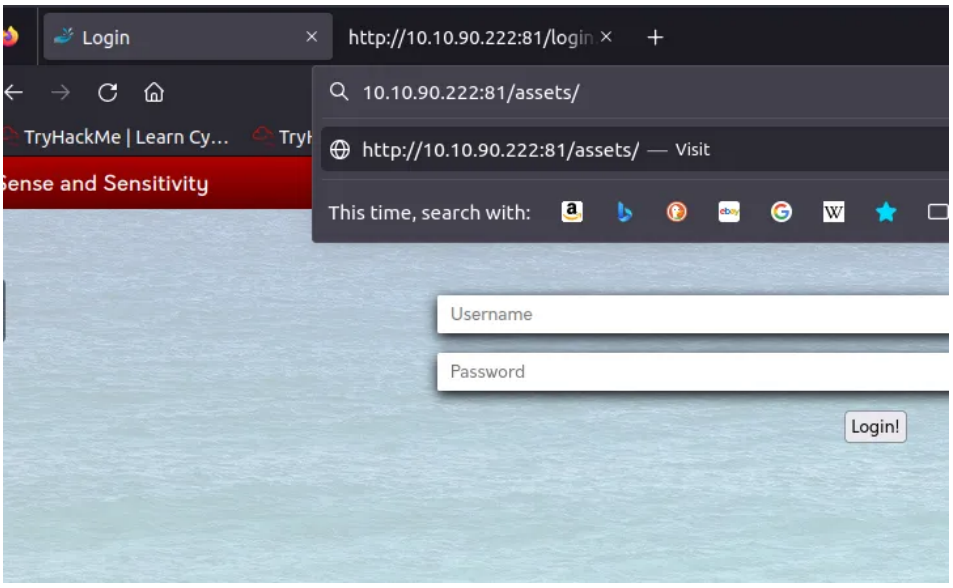
Hint: Have a look at the source code on the /login page.

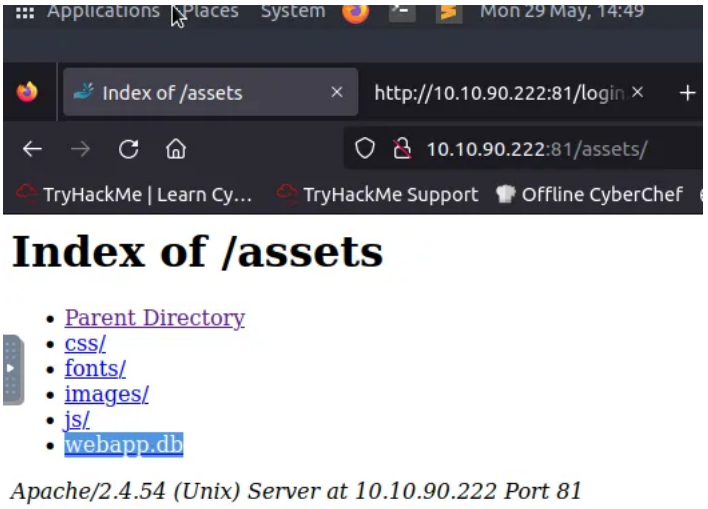
```
<html>
    <head>
        <title>Login</title>
        <meta name="viewport" content="width=device-width, user-scalable=no">
        <meta charset="utf-8">
        <link rel="shortcut icon" type="image/x-icon" href="../favicon.ico">
        <link type="text/css" rel="stylesheet" href="assets/css/style.css">
        <link type="text/css" rel="stylesheet" href="assets/css/loginStyle.css">
        <link type="text/css" rel="stylesheet" href="assets/css/orkney.css">
        <link type="text/css" rel="stylesheet" href="assets/css/icons.css">
        <script src="assets/js/jquery-3.5.1.min.js"></script>
    </head>
    <body>
        <header>
            <a id="home" href="/">Sense and Sensitivity</a>
            <a id="login" href="/login.php">Login</a>
        </header>
        <div class=background></div>
        <!-- Must remember to do something better with the database than store it in /assets... -->
        <main>
            <div class="content">
                <form method="POST">
                    <input type="text" name="user" placeholder="Username"><br>
                    <input type="password" name="pass" placeholder="Password"><br>
                    <input id="loginBtnFunc" type="submit" value="Login!">
                </form>
                        </div>
        </main>
        <footer><span>&copy; Sense and Sensitivity, 2022</span></footer>
    </body>
```

Answer Format: /******

Answer: /assets

Navigate to the directory you found in question one. What file stands out as being likely to contain sensitive data?



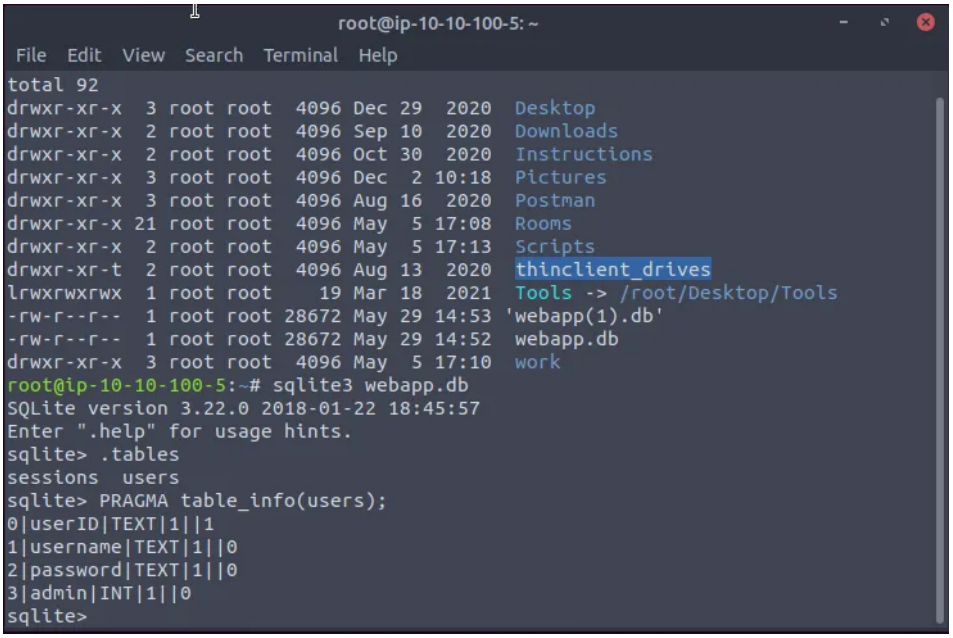


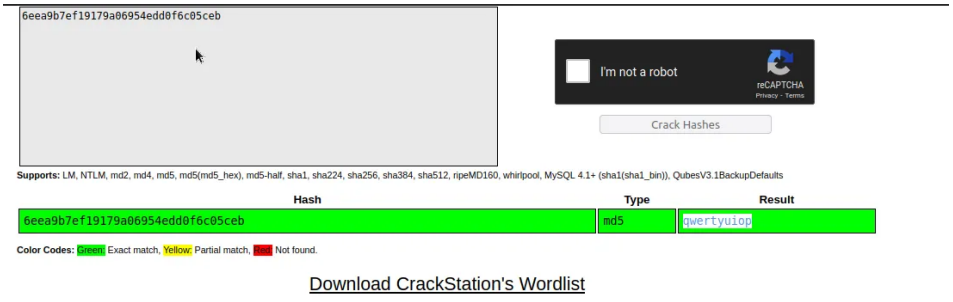
Answer Format: ******.**

Answer: webapp.db

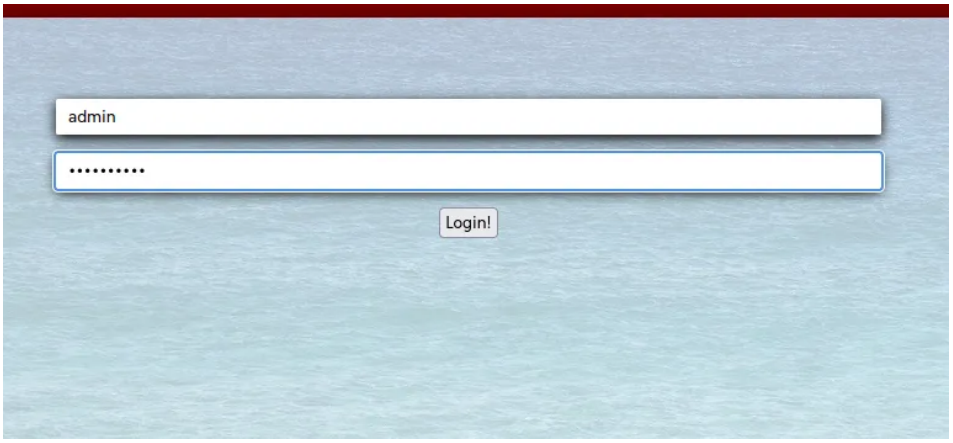
Use the supporting material to access the sensitive data. What is the password hash of the admin user?

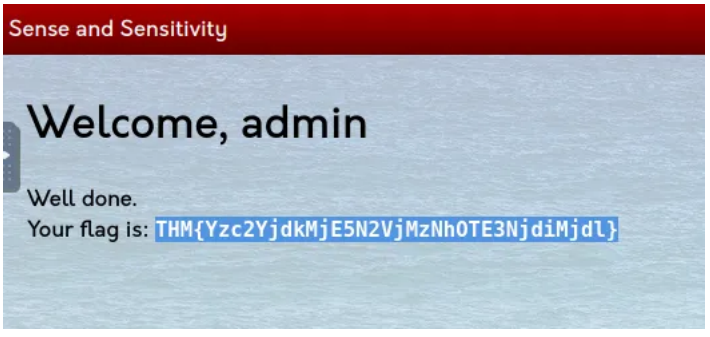
Download the database (.db) and pull up your command line. Now list everything in the folder using the **ls -l.**Next, we need to access the database with SQLite3 using **sqlite3 webapp.db** followed by **.tables** which brings up “users” and finally **PRAGMA table_info (users)**



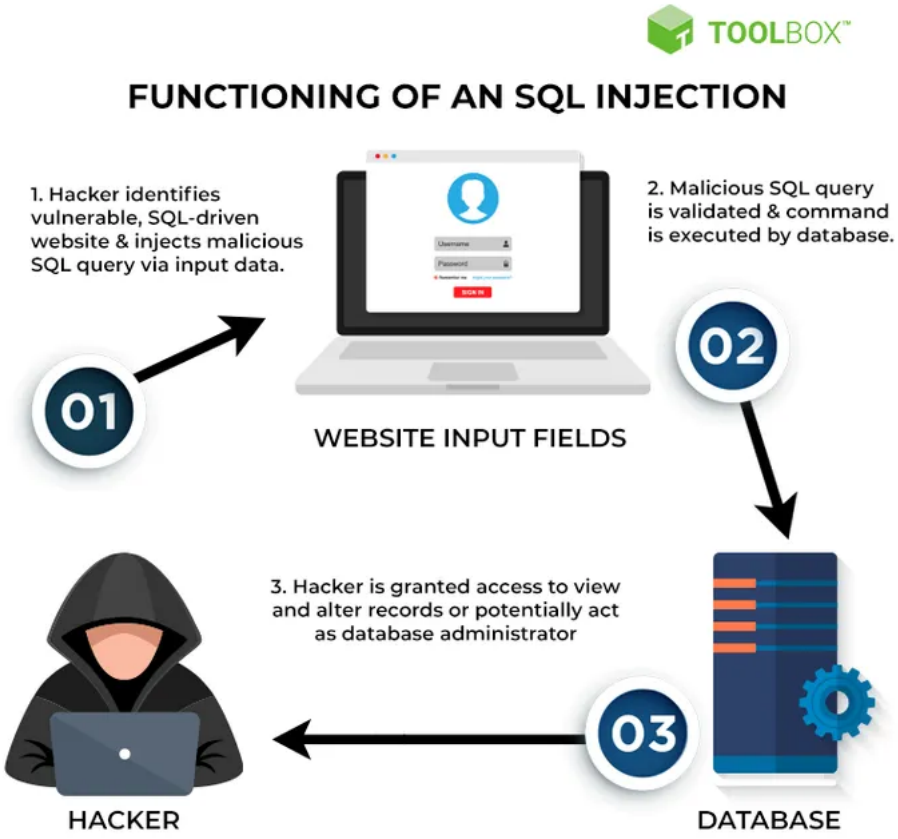


Download CrackStation's Wordlist





3. Injection (A03:2021)Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.



SQL injection - product category filter

SELECT * FROM products WHERE category = 'Gifts' AND released = 1

End goal: display all products both released and unreleased.

Analysis:

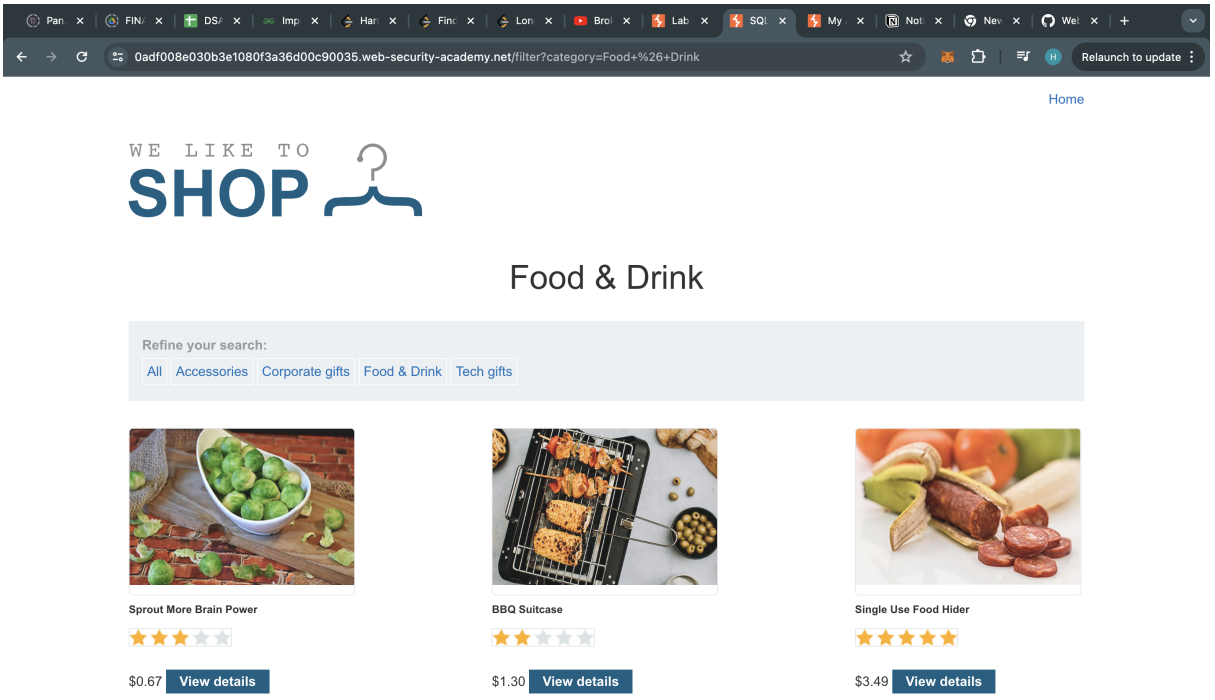
SELECT * FROM products WHERE category = 'Pets' AND released = 1

SELECT * FROM products WHERE category = ''' AND released = 1

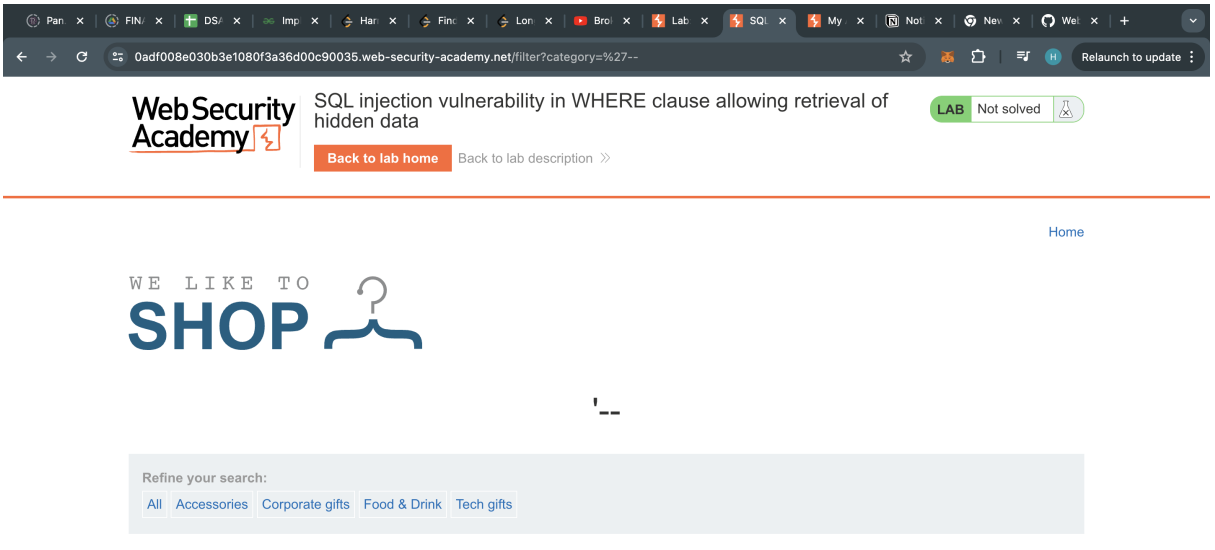
SELECT * FROM products WHERE category = ''--' AND released = 1

SELECT * FROM products WHERE category = ''

SELECT * FROM products WHERE category = '' or 1=1 --' AND released = 1



i am in food and drink section and now i have to remove all product from the page

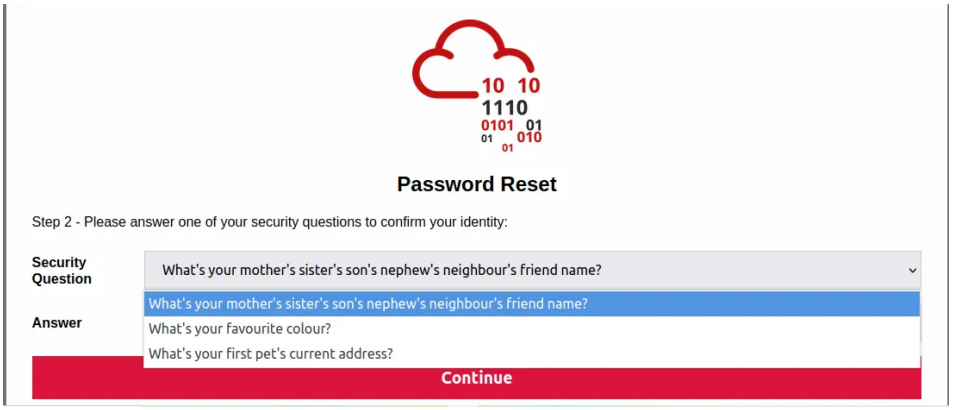


all product get remove from the page

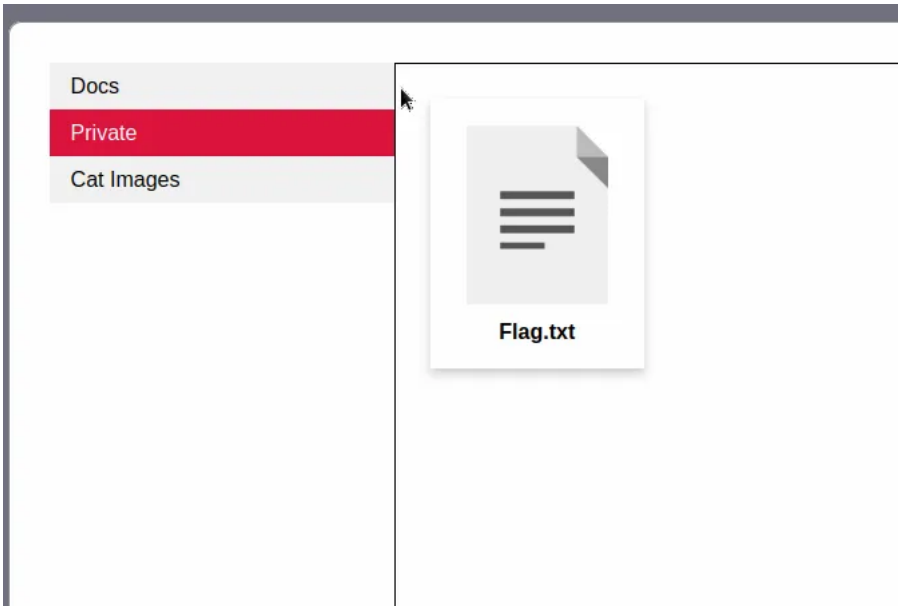
4. Insecure Design (A04:2021)Insecure design is a broad category representing different weaknesses, expressed as “missing or ineffective control design.”\

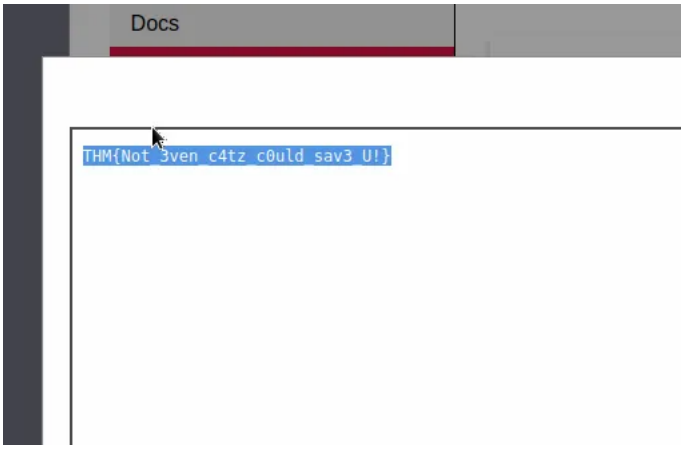
Navigate to http://MACHINE_IP:85 and get into joseph's account. This application also has a design flaw in its password reset mechanism. Can you figure out the weakness in the proposed design and how to abuse it?

Time to once again boot up the VM, open Firefox, and make your way to http://MACHINE_IP:85. Once you get to the page you should notice that it is a login page. We want to use the information that we have so far. THM provided that the person's name is 'joseph", but we don't have a password and we are not sure if that is his username. But there is a button that says "I forgot my password..." Click it and continue on.



It will first ask the user name, "joseph" was supplied, so we are using that. Now, the question's hint asks which is the easiest to guess from the three options. The first is an impossible task within the scope of this task and so is the last question. So we are going to be guessing colors. ROYGBIV (Red, Orange, Yellow, Green, Blue, Indigo, and Violet) is a safe place to start. I tried starting at the spelling variation of Red and finally Bingo! at "green" (it is case-sensitive). The system automatically generates a new temp password. You should write it down and/or copy and paste it. Use the information to log in.





Try to reset joseph's password. Keep in mind the method used by the site to validate if you are indeed joseph.

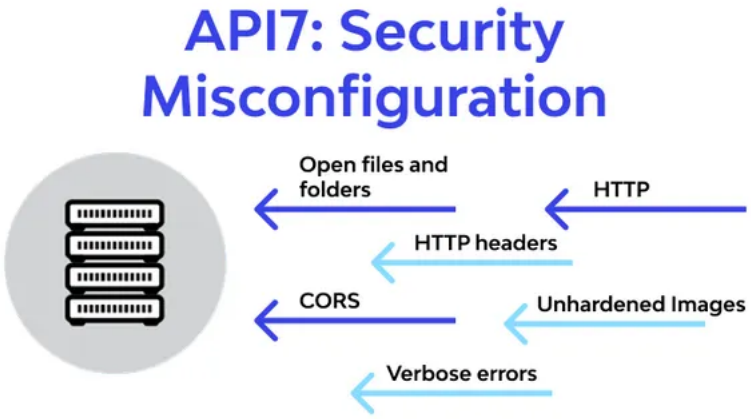
No Answer Needed

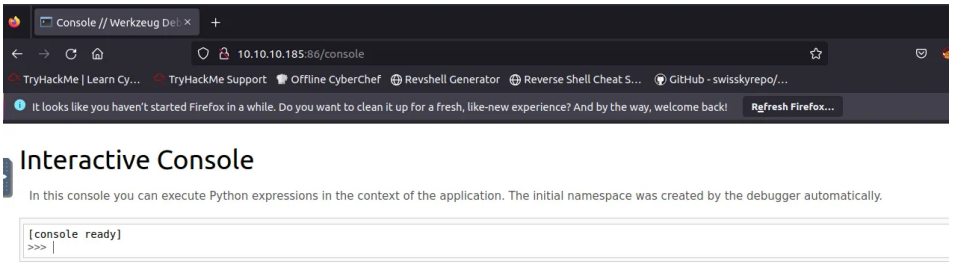
What is the value of the flag in joseph's account?

Hint: Is there any security question that can be easily guessed?

Answer Format: ***{**********}

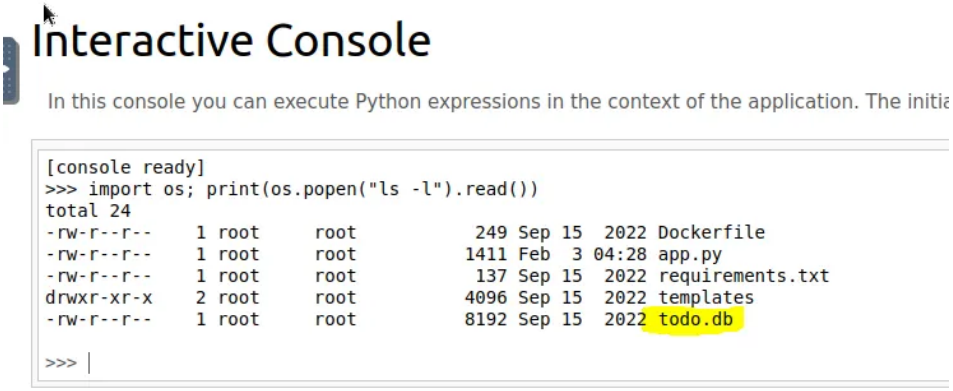
5. Security Misconfiguration (A05:2021)Security misconfiguration is the most commonly seen issue. Misconfiguration can occur at any level of an application stack, including network services, platforms, web servers, application servers, databases, frameworks, custom code, and pre-installed virtual machines.





Once you get there, input the following code:

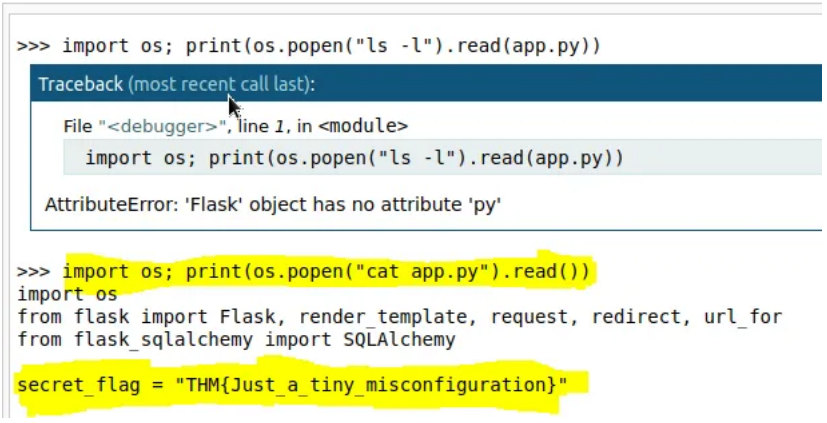
```
import os; print(os.popen("ls -l").read())
```



Once we use the code it will return the database directory. The first question asks for the file name for the database. The easiest way to figure out the answer is to look for the file name ending in [.db].

The next question asks you to modify the code, so you can read the contents of the `app.py.` It should look like this:

`import os; print(os.popen("cat app.py").read())`



Once we enter the altered code the site returns the flag:

THM{Just_a_tiny_misconfiguration}

Navigate to http://MACHINE_IP:86/console to access the Werkzeug console.

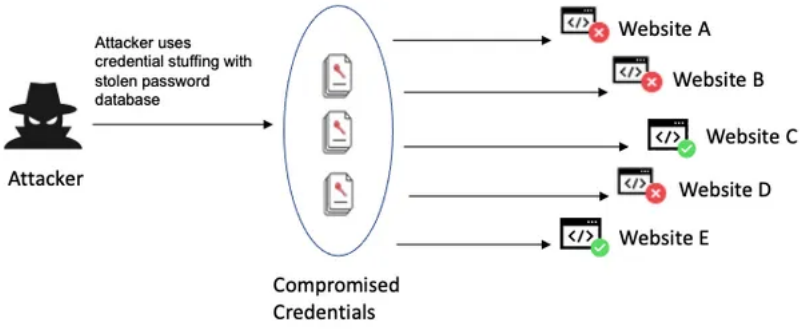
No Answer Needed

Use the Werkzeug console to run the following Python code to execute the `ls -l` command on the server:

\

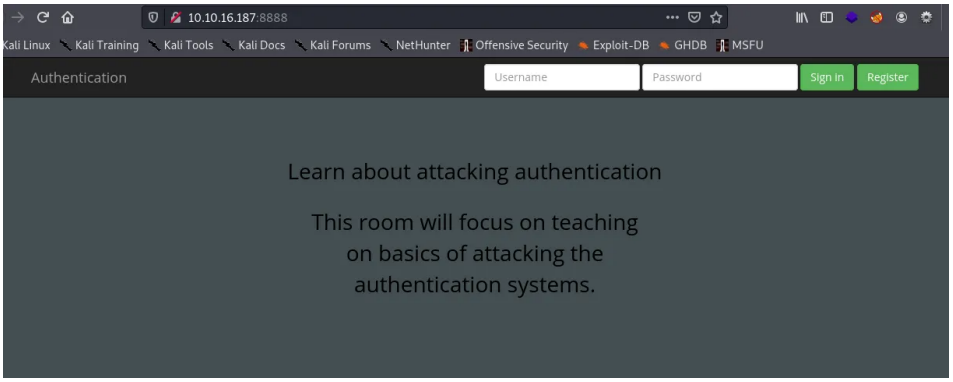
6. Vulnerable and Outdated Components (A06:2021)Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover.

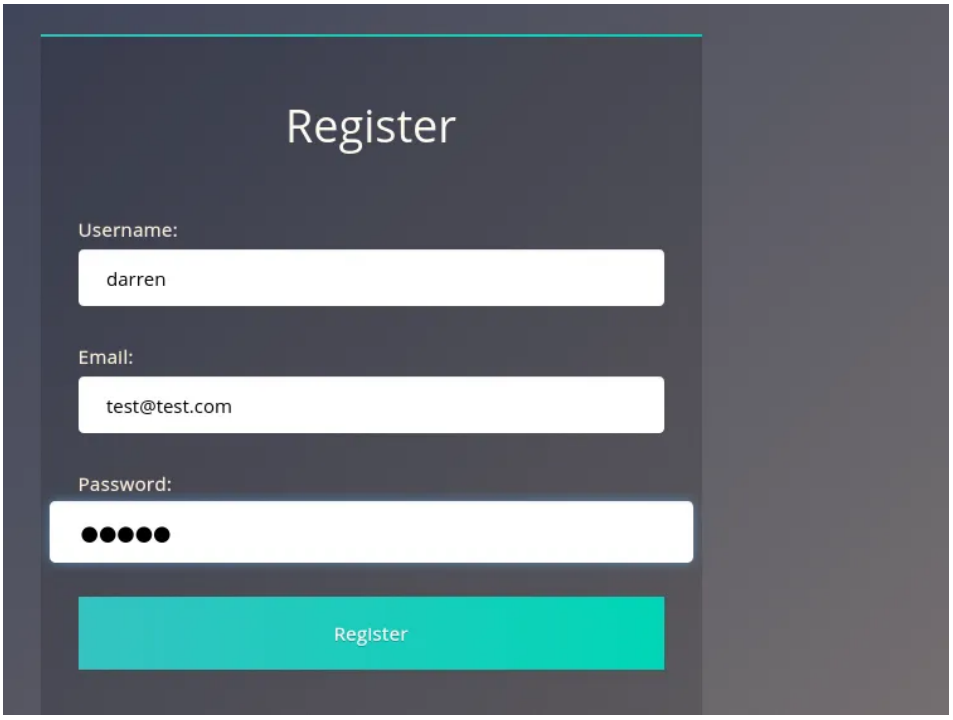
7. Identification and Authentication Failures (A07:2021)Previously "Broken Authentication," this category includes failures related to identification and authentication mechanisms. Functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens.



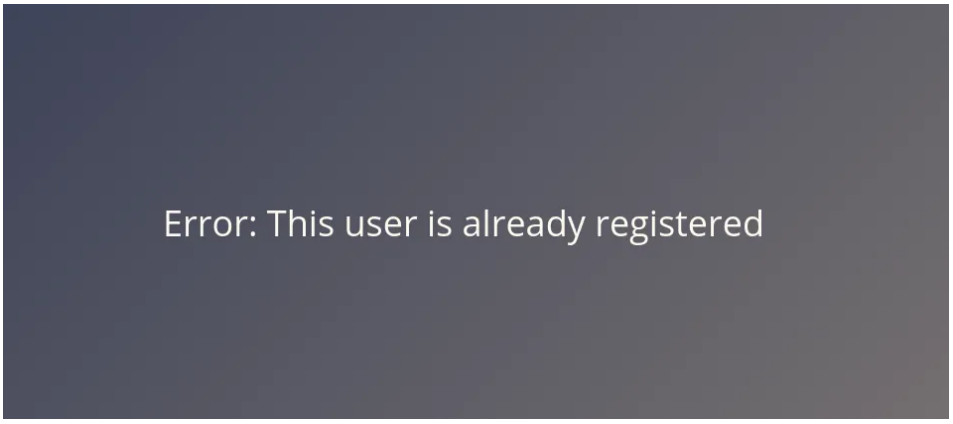
To see this in action go to http://10.10.147.50:8888 and try to register a user name darren, you'll see that the user already exists so then try to register a user " darren" and you'll see that you are now logged in and will be able to see the content present only in Darren's account which in our case is the flag that you need to retrieve.

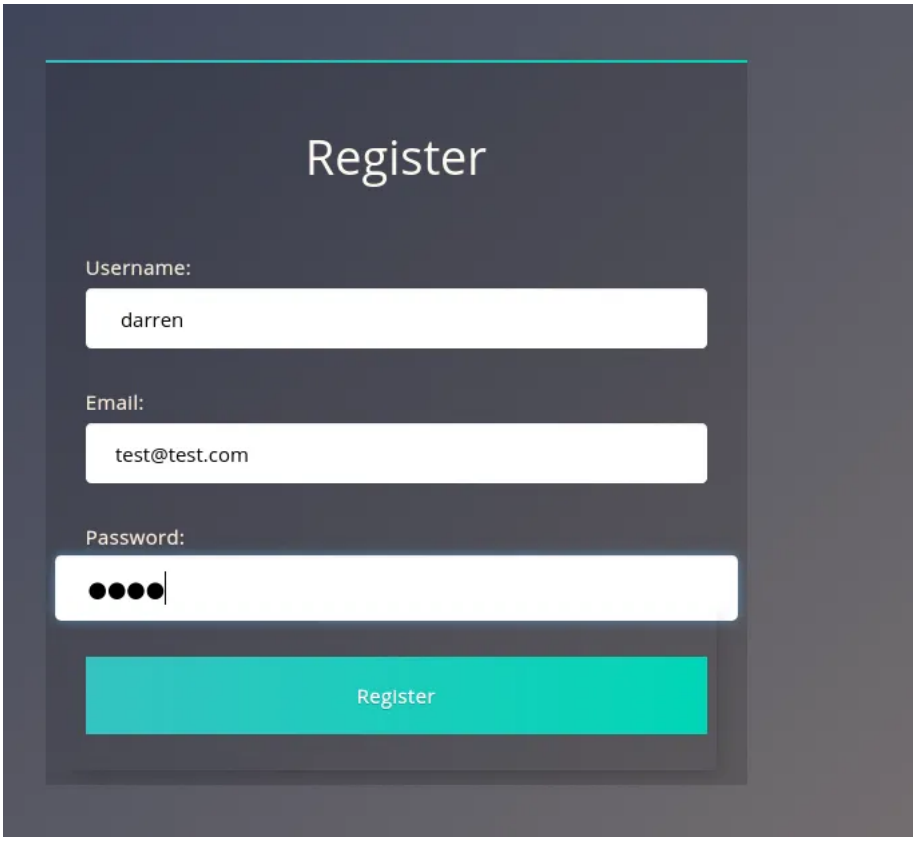
We can visit the website http://MACHINE_IP:8888.

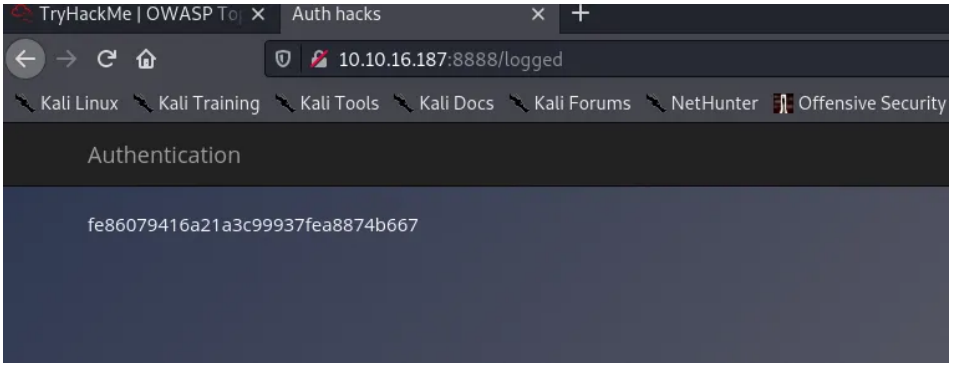


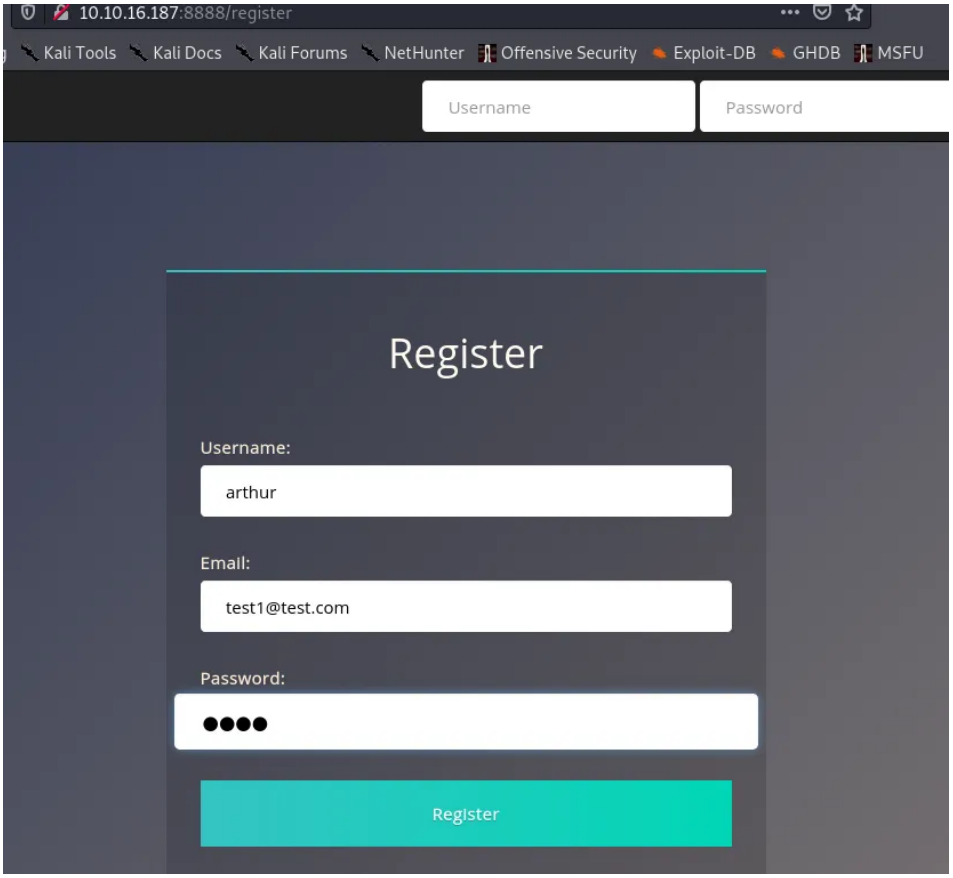


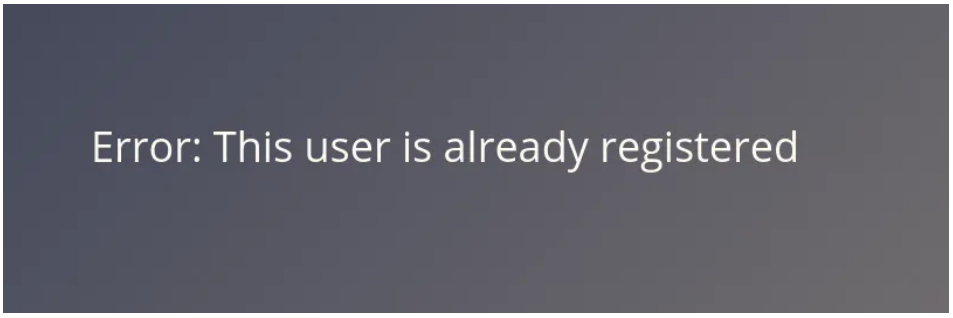
I'm trying to be registered as "darren".

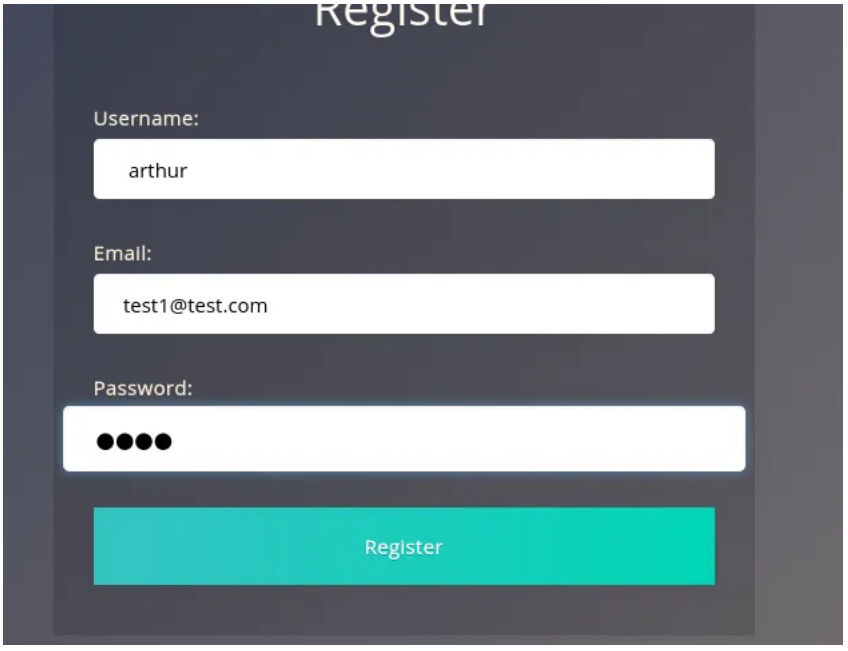


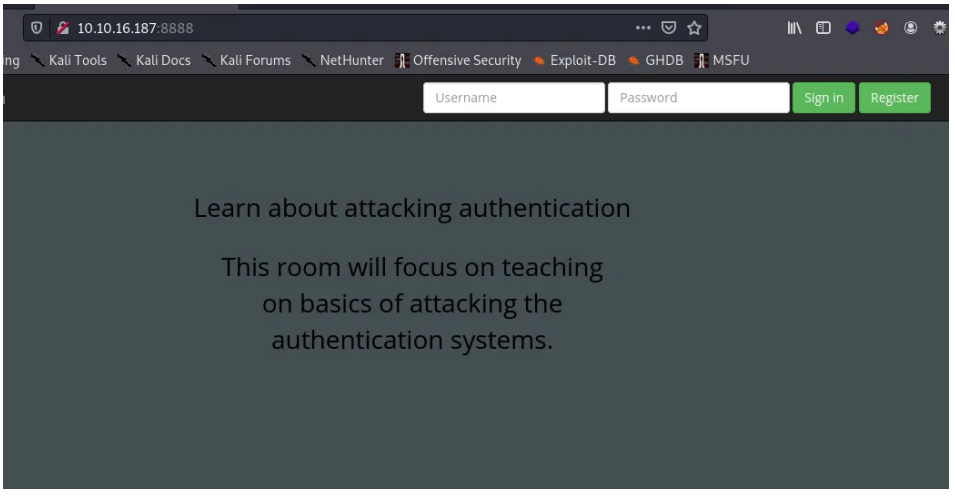

Register
Username:
darren
Email:
test@test.com
Password:
Register

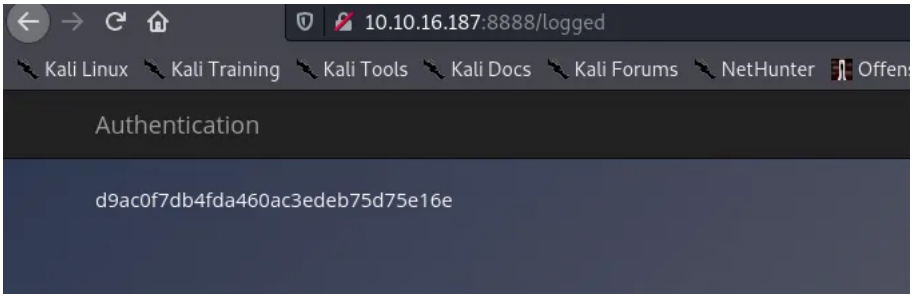

TryHackMe | OWASP To
Auth hacks
10.10.16.187:8888/logged
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Authentication
fe86079416a21a3c99937fea8874b667


10.10.16.187:8888/register
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
Username
Password
Register
Username:
arthur
Email:
test1@test.com
Password:
Register


Error: This user is already registered

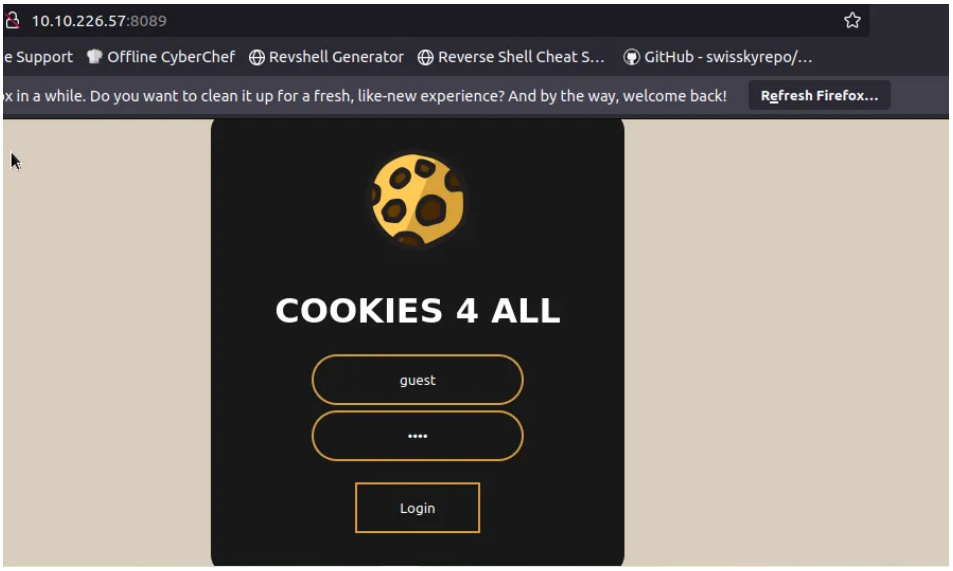


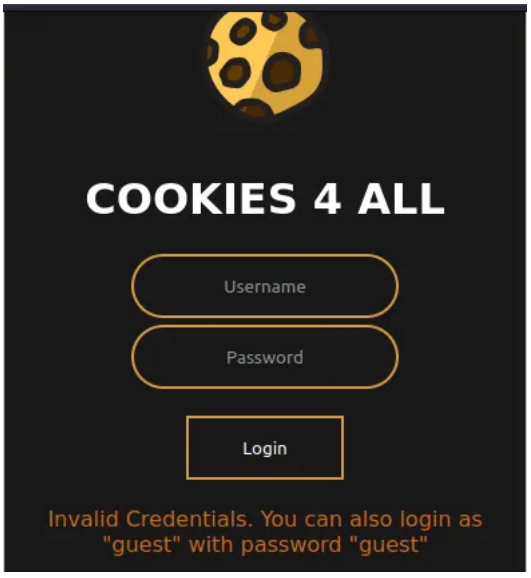


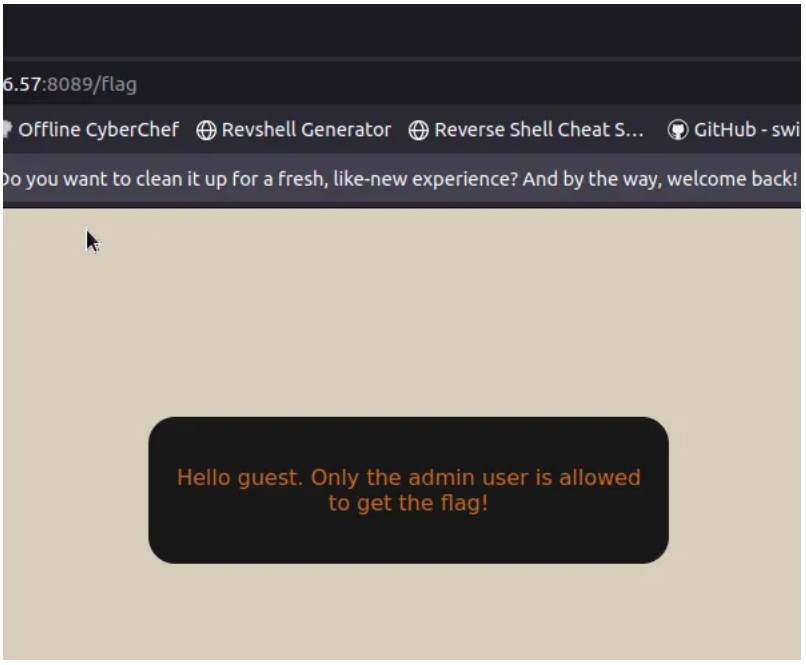


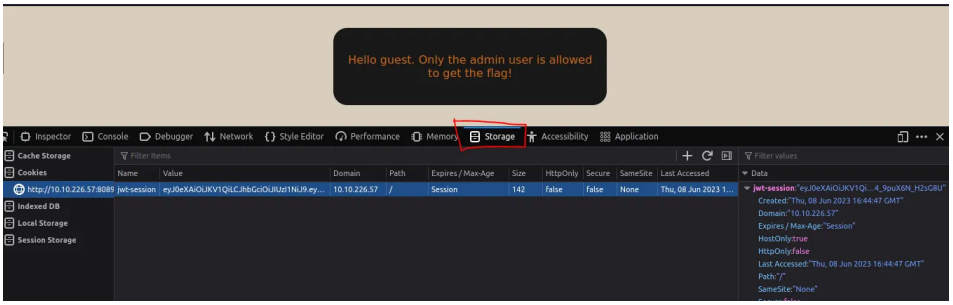
8. Software and Data Integrity Failures (A08:2021)This category is related to code and infrastructure that does not protect against integrity violations. One example is an application that relies on libraries, plugins, or modules from untrusted sources.

Start your machine and attack box, then go to the site that was given http://MACHINE_IP:8089/. Once you get to the screen, attempt to log into the guest account with a random password.


10.10.226.57:8089
e Support
Offline CyberChef
Revshell Generator
Reverse Shell Cheat S...
GitHub - swisskyrepo/...
x in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
COOKIES 4 ALL
guest
....
Login


COOKIES 4 ALL
Username
Password
Login
Invalid Credentials. You can also login as "guest" with password "guest"


6.57:8089/flag
Offline CyberChef
Revshell Generator
Reverse Shell Cheat S...
GitHub - swi
Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Hello guest. Only the admin user is allowed to get the flag!

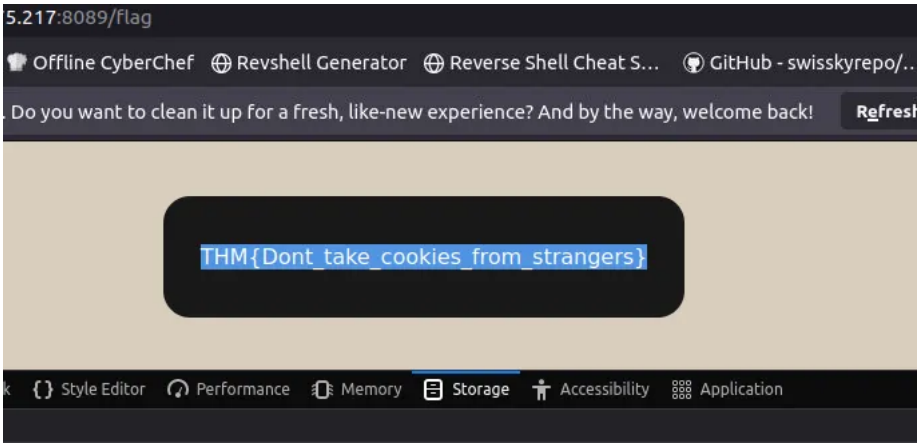


Open a word document. Copy the “Value” and paste the entire code to the document. It should look like this:

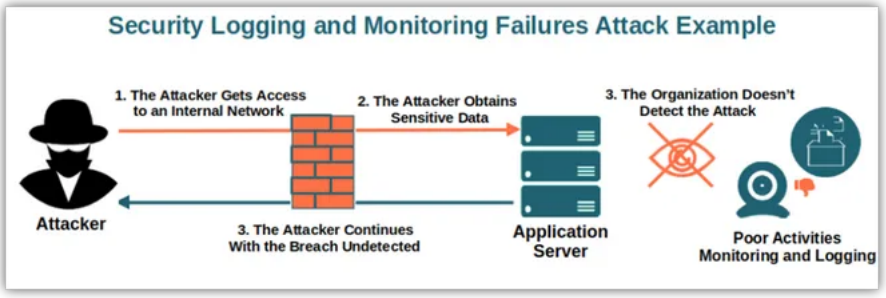
> eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VybmFtZSI6Imd1ZXN0IiwiZXhwIjoxNjg2MzIxzKQF9Xo1uYBVA

Next, you need to use the head and payload. If you recall from the task the header is up to the “.”, then the payload is up to the next “.”, don’t worry the signature we won’t need it.

Go to https://appdevtools.com/base64-encoder-decoder and DECODE the header and payload separately.



9. Security Logging and Monitoring Failures (A09:2021)Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allow attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data.



10. Server-Side Request Forgery (SSRF) (A10:2021)SSRF flaws occur when a web application is fetching a remote resource without validating the user-supplied URL. Even if the application doesn’t return the response to the user, an attacker can still find the HTTP response by analyzing how long it takes to get an answer.

Exploiting Regular / In-Band SSRF

Request:

```
POST /product/stock HTTP/1.0
Content-Type: application/x-www-
form-urlencoded
Content-Length: 118


stockApi=http://stock.weliketoshop
.net:8080/product/stock/check%3Fpr
oductId%3D6%26storeId%3D1
```

Response:

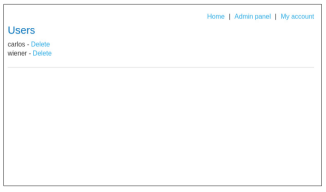
```
HTTP/1.1 200 OK
Content-Type: text/plain;
charset=utf-8
Connection: close
Content-Length: 3



506
```

Exploiting Regular / In-Band SSRF

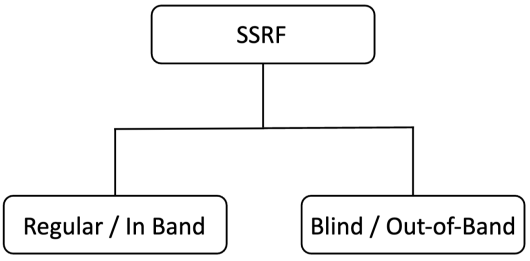
Request:

```
POST /product/stock HTTP/1.0
Content-Type: application/x-www-
form-urlencoded
Content-Length: 118



stockApi=http://localhost/admin
```

Response:



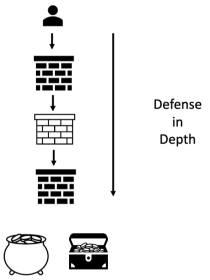
Types of SSRF



Preventing SSRF Vulnerabilities

Defense in depth approach:

- Application Layer defenses
- Network Layer Defenses



Network Layer Defenses

- Segment remote resource access functionality in separate networks to reduce the impact of SSRF
- Enforce “deny by default” firewall policies or network access control rules to block all but essential intranet traffic

OWASP Top Ten 2017 vs. 2021