INTRODUCTION TO CAPTURE THE FLAG (CTF) AND WEB EXPLOITATION

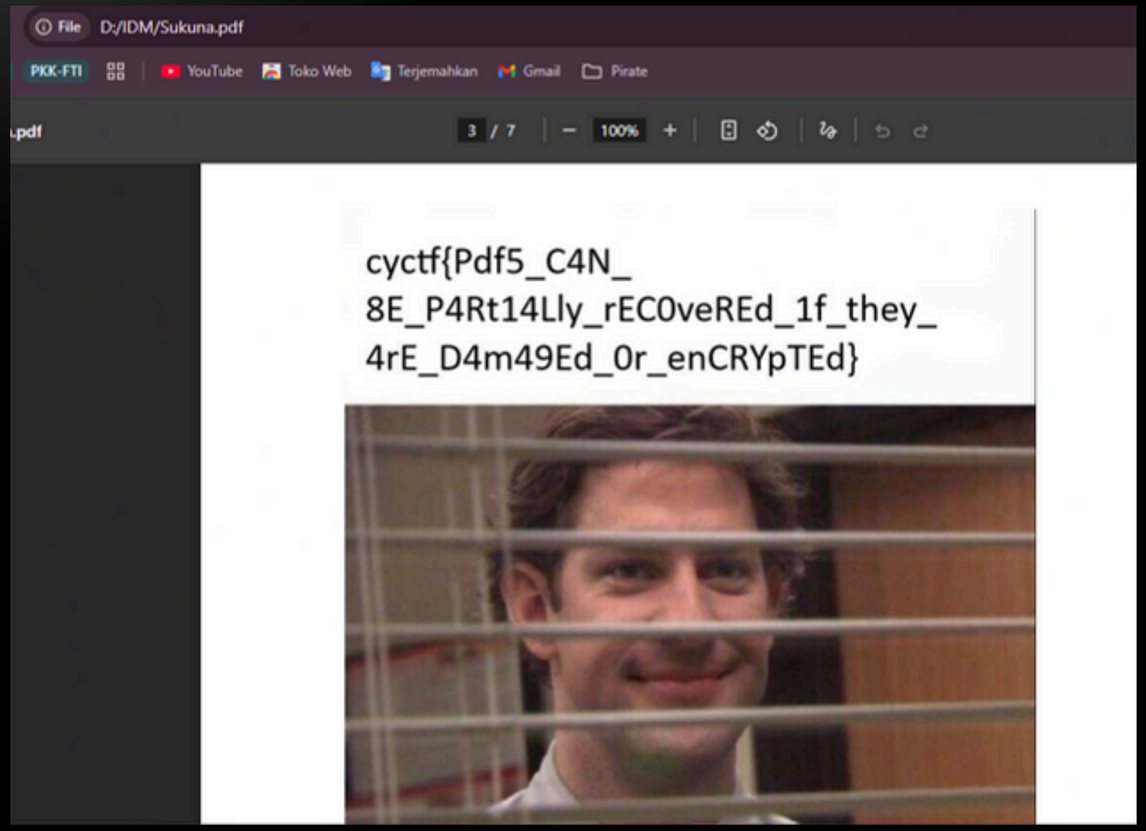
PRESENTATION

CAPTURE THE FLAG (CTF)

CTF adalah lomba di mana peserta menyelesaikan tantangan terkait keamanan komputer untuk menemukan flag (potongan *string* rahasia).

Cocok dimainkan untuk belajar, praktek, dan juga melakukan validasi terhadap kemampuan *cybersecurity* yang dimiliki. Biasanya digunakan sebagai Titik Masuk orang ke bidang Cyber Security.

CONTOH FLAG




```
20
21      <div class="temple-content">
22        <form class="temple-form" action="" method="post">
23          <div class="ritual-text">
24            <span class="mystical-prompt">
                □□Enter the sacred words to unlock ancient wisdom...
              </span>
25          </div>
26          <div class="input-container">
27            <input class="temple-input" type="text" name="text" value="" placeholder="
              your message here...">
28            <input class="temple-button" type="submit" value="□□Transmute">
29          </div>
30        </form>
31
32        <div class="revelation-area">
33          <h2 class="ancient-text">
34            0
35            WRECKIT60{7h3_T3mp7471On_5hOw3d_M3_7h3_W4y_0u7}
36          </h2>
37        </div>
38      </div>
39
40      <footer class="temple-footer">
41        <div class="mystical-symbols">
            □ □ □ □ □
          </div>
42      </footer>
43    </div>
44  </body>
45 </html>
46
```

TIPE CAPTURE THE FLAG

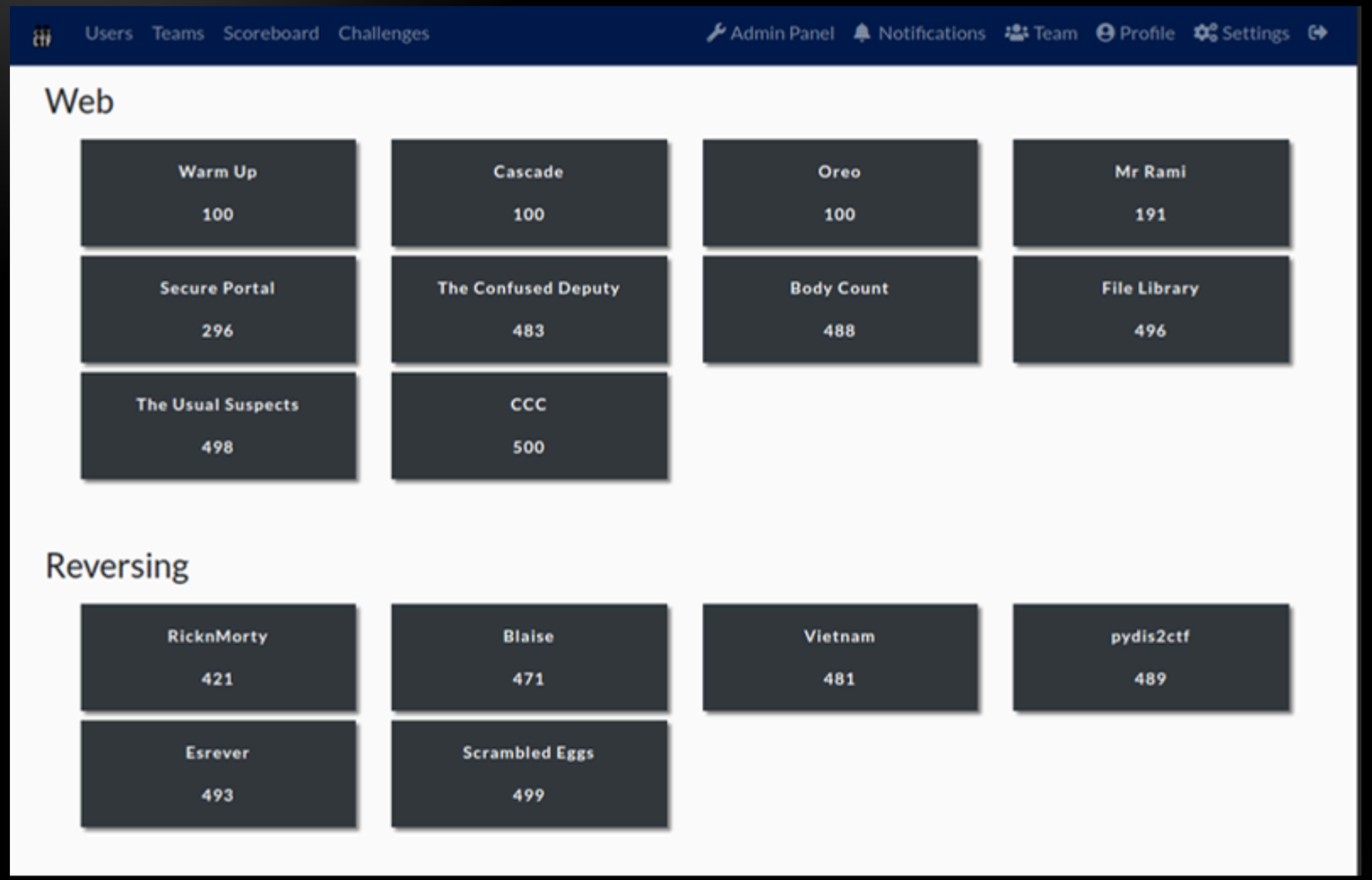
JEOPARDY

ATTACK AND DEFENSE

JEOPARDY

Jeopardy merupakan tipe CTF yang paling umum. Terdiri dari beberapa challenge yang dipisahkan berdasarkan kategori. Terdapat kategori seperti **Web Exploitation**, **Binary Exploitation**, **Forensics**, **Cryptography**, **Reverse Engineering**, dan lain lain.

JEOPARDY


Users
Teams
Scoreboard
Challenges
Admin Panel
Notifications
Team
Profile
Settings
Web
Warm Up
100
Cascade
100
Oreo
100
Mr Rami
191
Secure Portal
296
The Confused Deputy
483
Body Count
488
File Library
496
The Usual Suspects
498
CCC
500
Reversing
RicknMorty
421
Blaise
471
Vietnam
481
pydis2ctf
489
Esrever
493
Scrambled Eggs
499

KATEGORI SOAL CTF JEOPARDY

Web Exploitation

This category focuses on exploiting vulnerabilities in web applications and servers.

Reverse Engineering

This category involves analyzing and understanding the functionality of compiled code or binary files.

Cryptography

This category involves deciphering and breaking encryption techniques and algorithms.

Forensics

This category focuses on analyzing digital evidence and investigating cybercrimes.

Misc

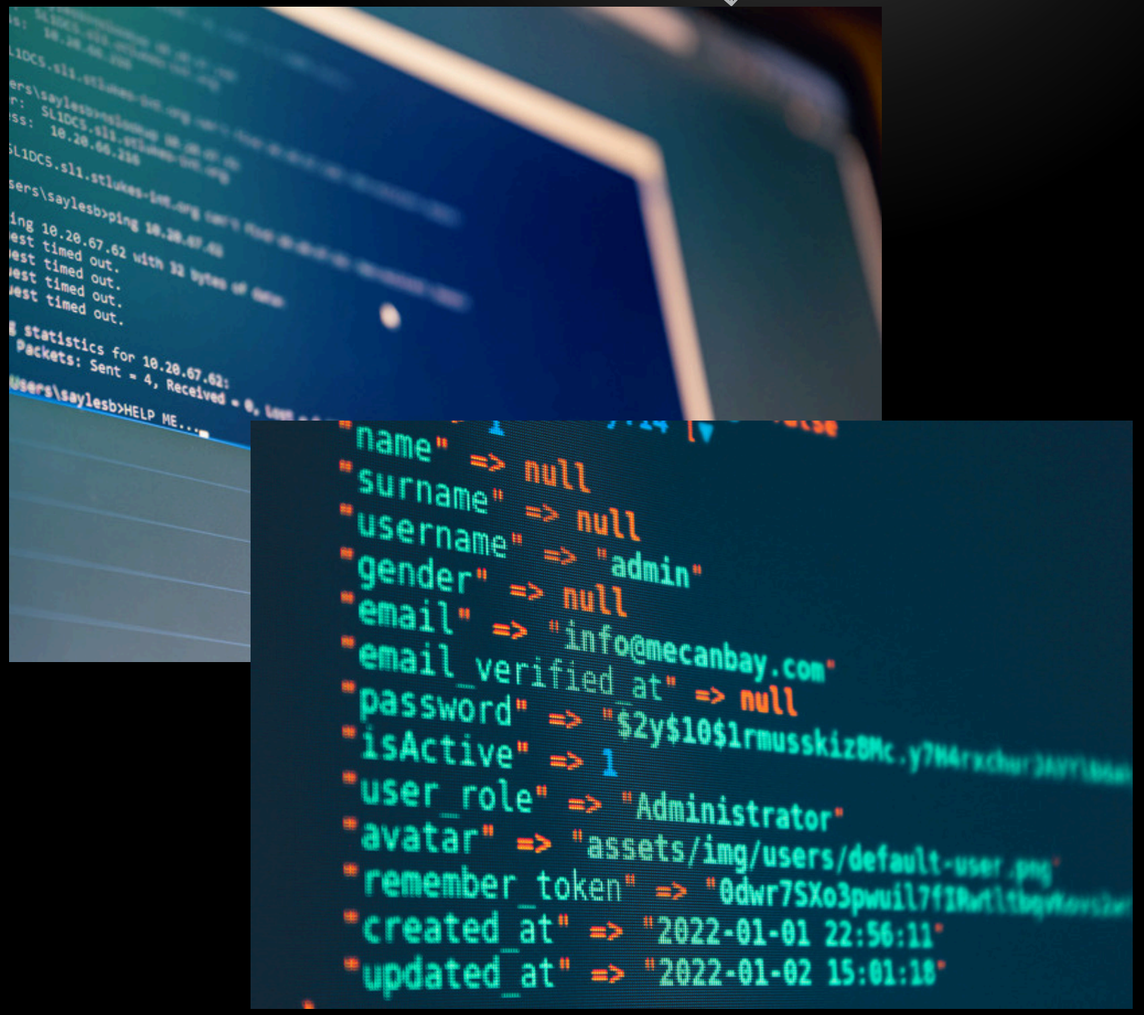
This category covers various challenges that don't fit into specific categories.

Binary Exploitation

This category involves exploiting vulnerabilities in binary programs and systems.

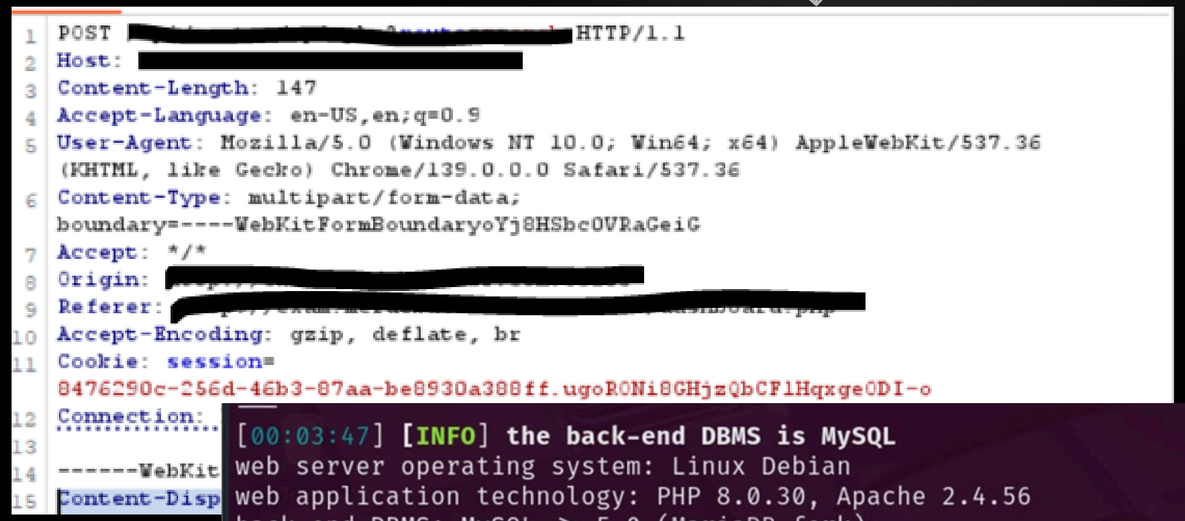
WEB EXPLOITATION

Web exploitation adalah praktik menemukan dan mengeksploitasi kerentanan (vulnerabilities) pada aplikasi web untuk mendapatkan akses, data, atau kontrol yang tidak sah. Dalam konteks / CTF, web exploitation berarti mencari kelemahan di aplikasi web, misalnya web atau API, lalu memanipulasinya untuk menemukan flag atau bukti kompromi.



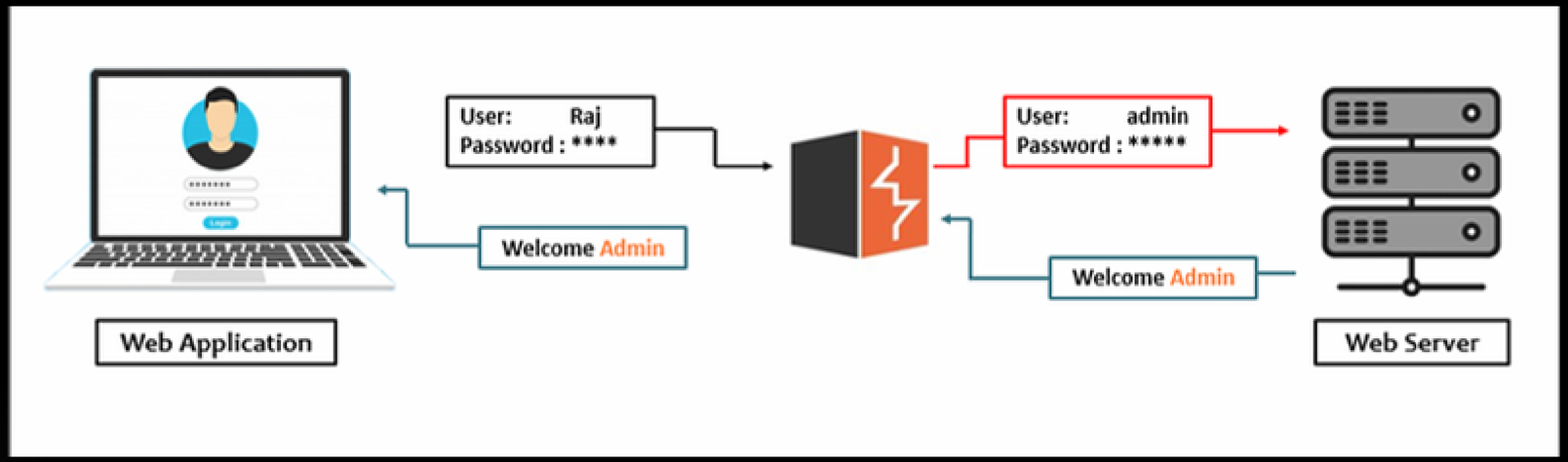
WEB EXPLOITATION

- *HTML, CSS, JAVASCRIPT BASICS*
- ***SQL INJECTION (SQLI)***
- ***CROSS-SITE SCRIPTING (XSS)***
- *CROSS-SITE REQUEST FORGERY (CSRF)*
- *FILE INCLUSION (LFI/RFI)*
- ***COMMAND INJECTION***
- ***SERVER SIDE TEMPLATE INJECTION (SSTI)***
- *AUTHENTICATION BYPASS*
- *SESSION MANAGEMENT*
- *DAN LAIN-LAIN (E.G., SSRF, DIRECTORY TRAVERSAL, INSECURE DESERIALIZATION).*



BURPSUITE

Burpsuite adalah web proxy yang bertindak sebagai perantara antara aplikasi web target dan server web.



LATIHAN BURP SUITE

https://play.picoctf.org/practice/challenge/419?category=1&difficulty=1&page=1

SQL INJECTION (SQLI)

Jenis serangan yang digunakan untuk memanipulasi query ke sebuah database, dimana hal ini dapat dimanfaatkan oleh penyerang untuk melakukan ekstraksi dari database tersebut.

BASIC SQLI

Input

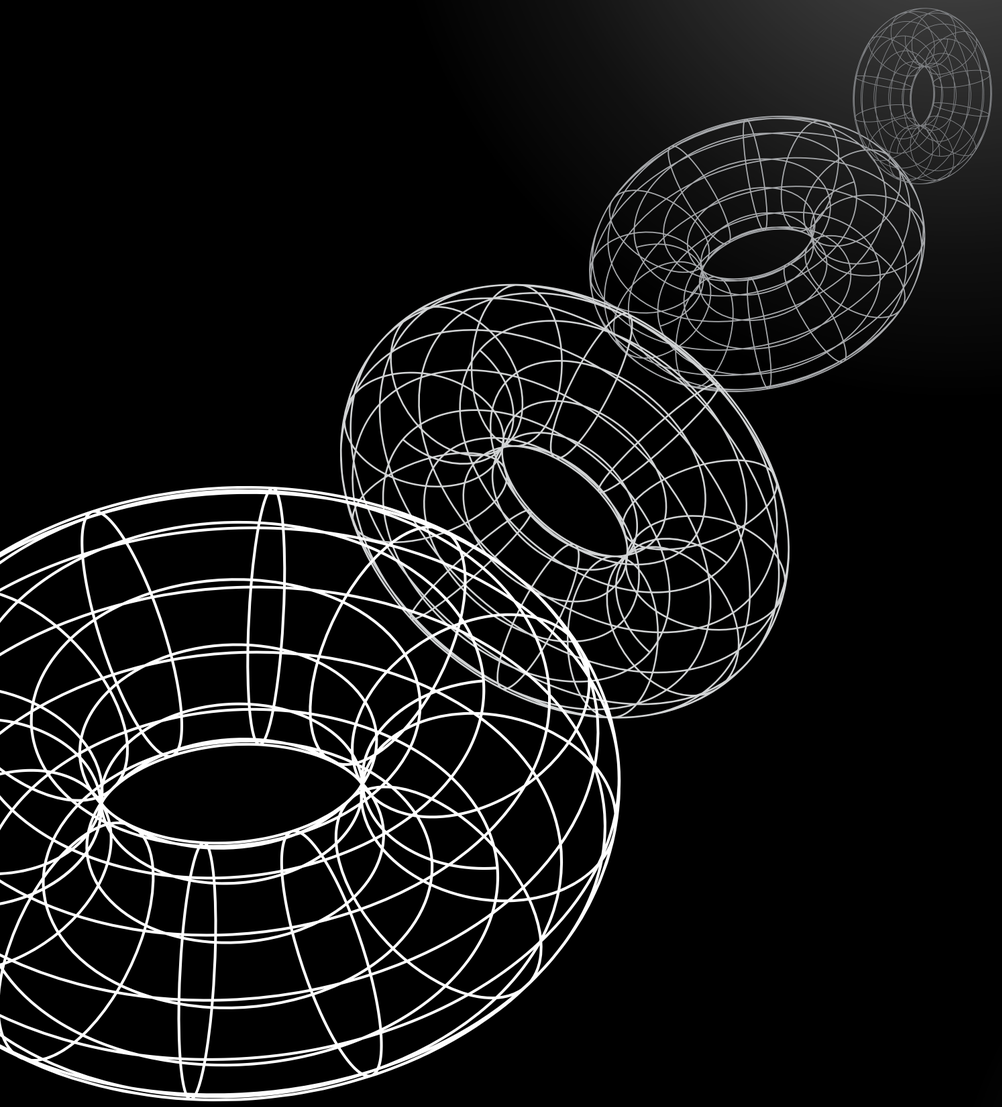
username: ' OR 1=1 --
password: bar

Query

```
SELECT * FROM users WHERE username='' OR '1'='1' -- ' AND password='bar'
```

Result

Login Success (as admin)



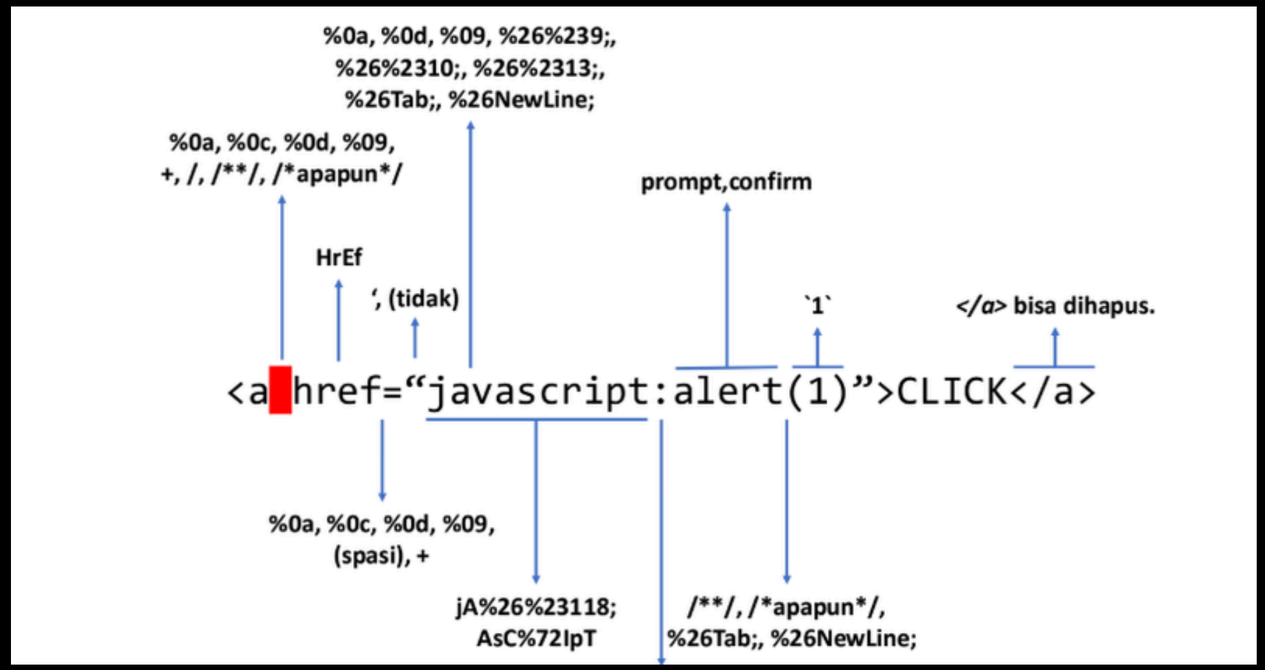
DEMO SQLI

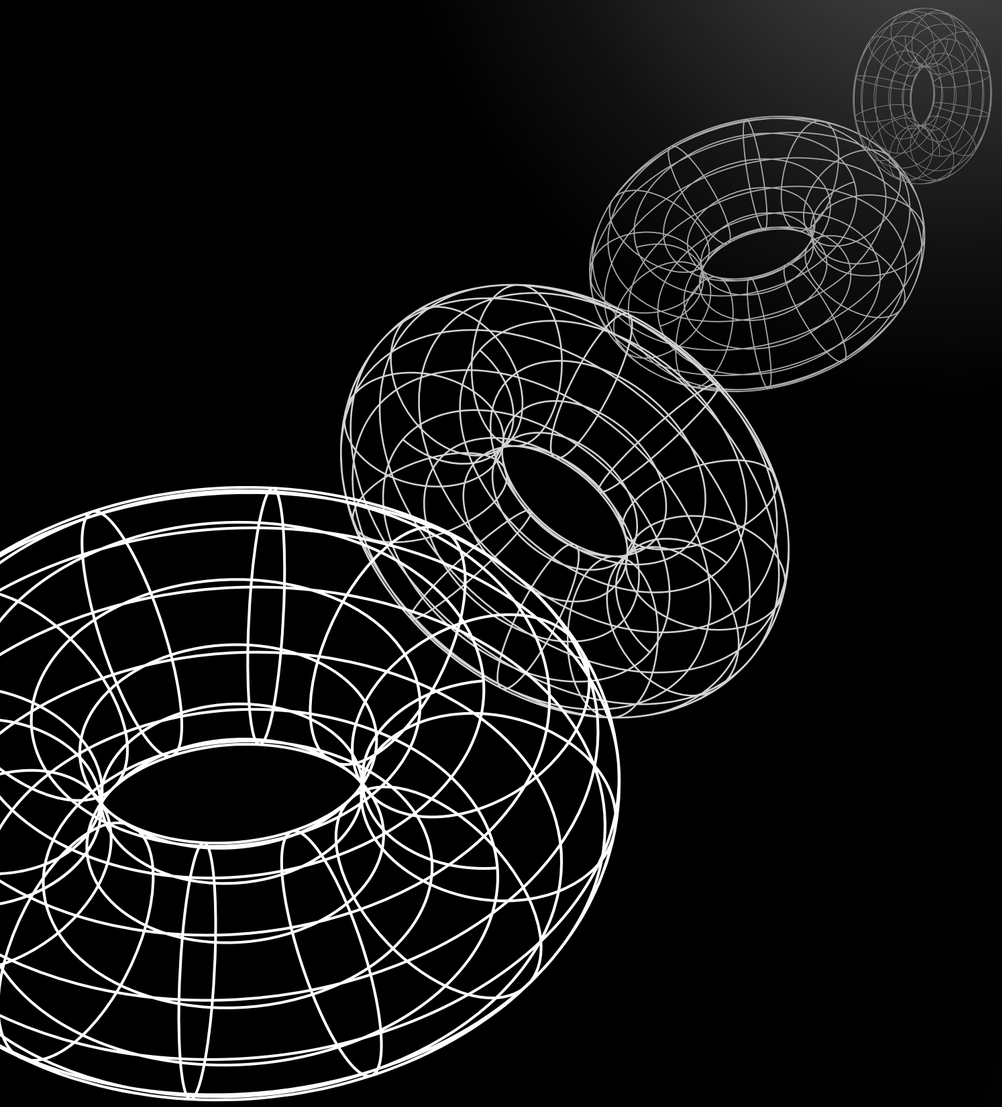
https://play.picoctf.org/practice/challenge/304?category=1&page=1&search=sql

Payload:
username: ' OR 1=1 --
password: bebas

CROSS-SITE SCRIPTING (XSS)

Jenis kerentanan keamanan web di mana aplikasi web memasukkan input dari pengguna ke halaman HTML tanpa sanitizing yang tepat, sehingga penyerang bisa menyisipkan dan menjalankan kode JavaScript di browser korban.





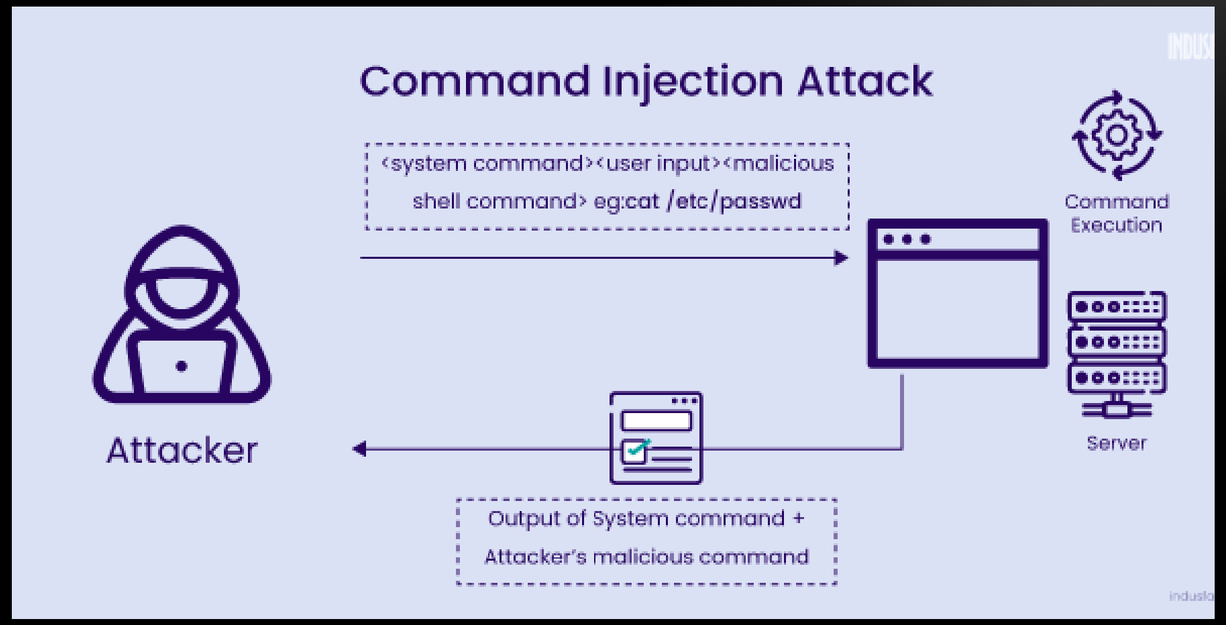
DEMO XSS

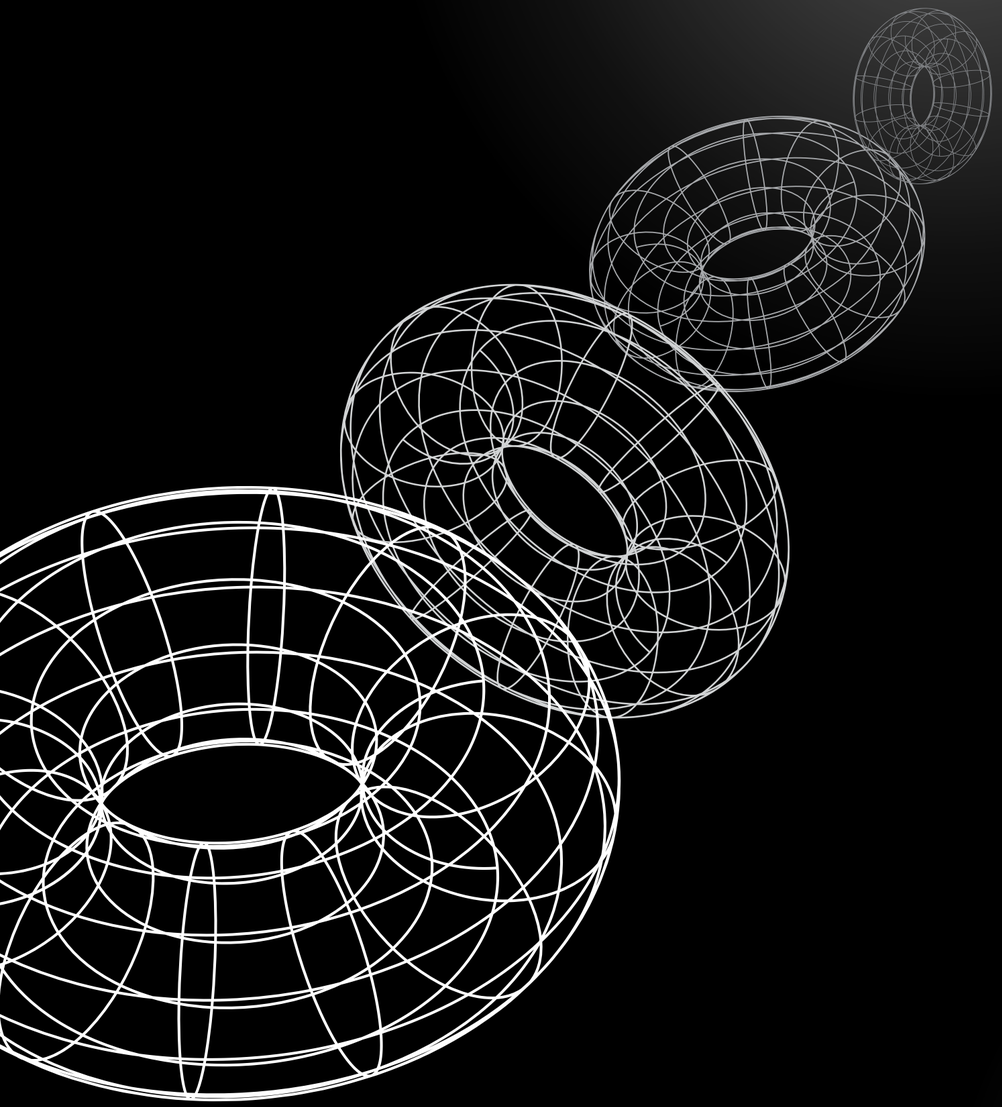
https://portswigger.net/web-security/cross-site-scripting/reflected/lab-html-context-nothing-encoded

Payload:
<script>alert(“bebas isinya apa aja”)</script>

COMMAND INJECTION

Jenis kerentanan keamanan di mana aplikasi web (atau program) menerima input dari pengguna dan — tanpa validasi atau sanitasi yang cukup — memasukkan input itu ke dalam perintah sistem (shell) sehingga penyerang bisa menjalankan perintah-perintah sistem operasi pada server target. Singkatnya: input pengguna di-trusted menjadi bagian dari perintah shell yang dieksekusi server.





DEMO COMMAND INJECTION

https://play.picoctf.org/practice/challenge/202?category=1&difficulty=2&page=1&search=caas

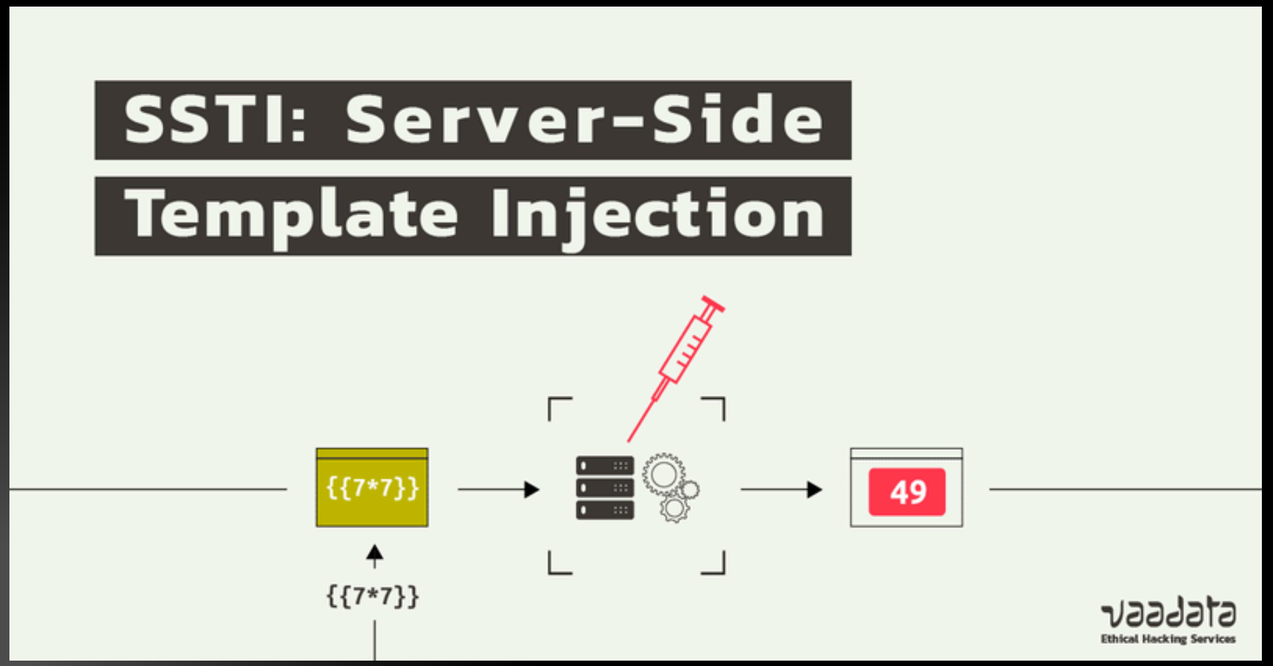
Payload:

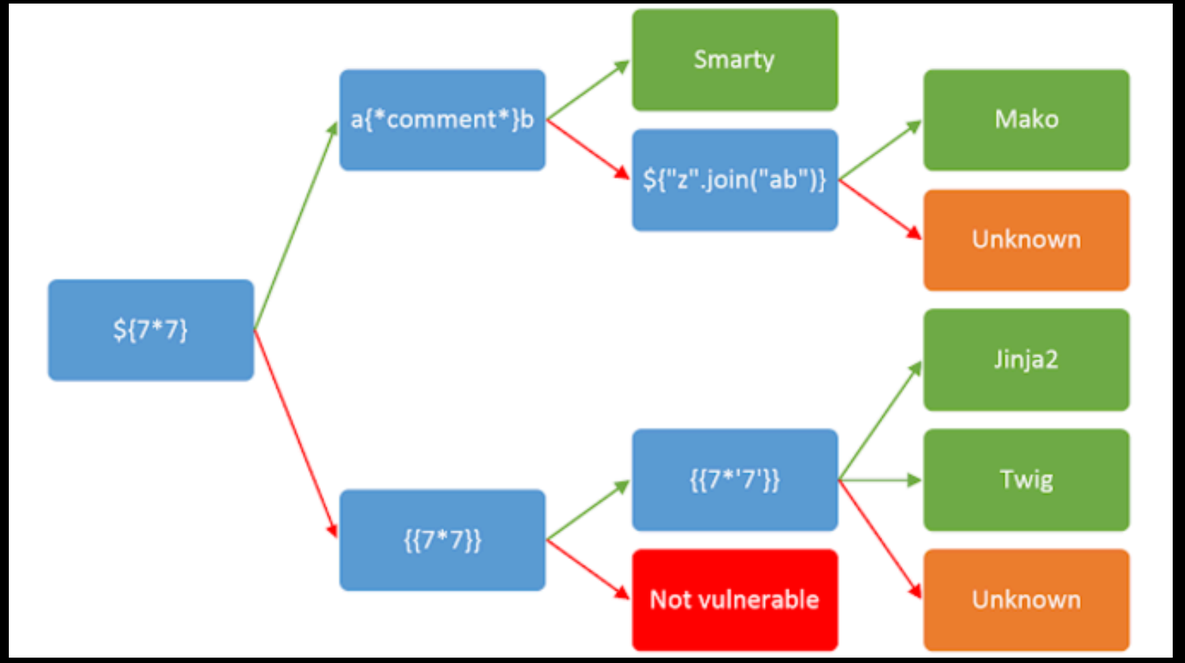
https://caas.mars.picoctf.net/cowsay/tes;%20ls

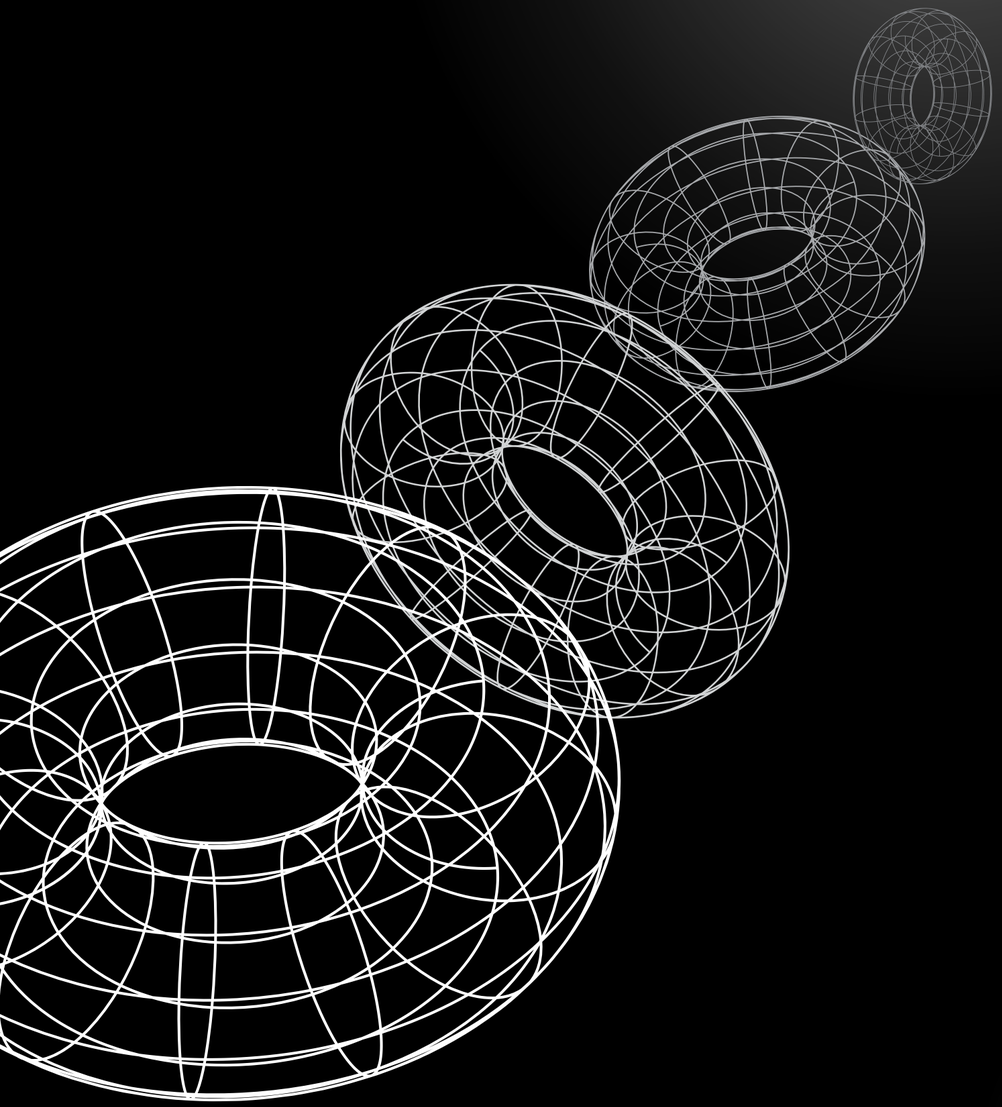
https://caas.mars.picoctf.net/cowsay/tes;%20cat%20falg.txt

SERVER-SIDE TEMPLATE INJECTION

Kerentanan ketika input pengguna disisipkan ke dalam template engine server tanpa sanitasi, sehingga attacker bisa menjalankan kode atau perintah melalui fitur template itu sendiri.







DEMO SSTI

https://play.picoctf.org/practice/challenge/492?category=1&difficulty=1&page=1&search=ssti

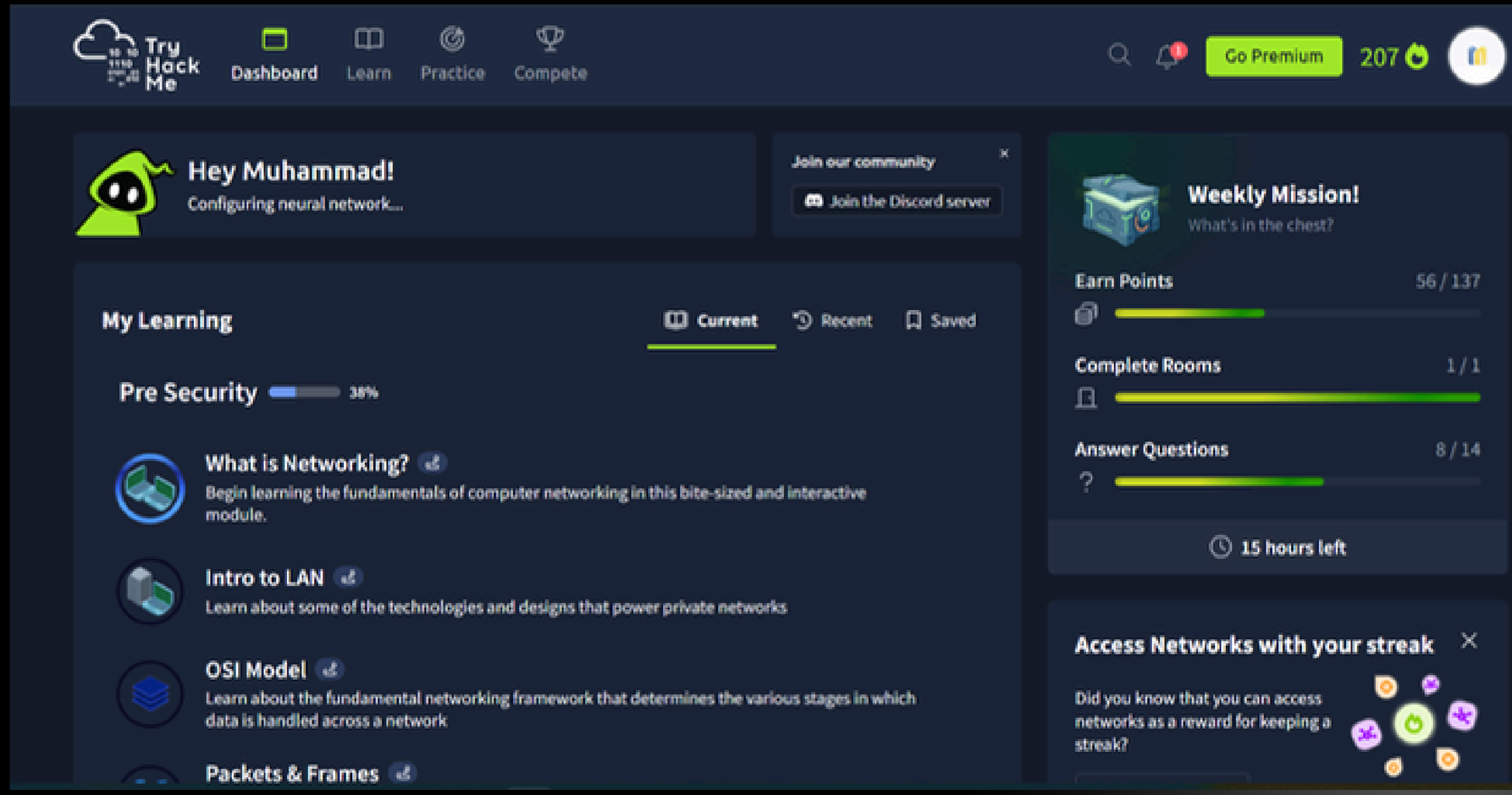
Payload:
{{request.application.__globals__.__builtins__.__import__('os').popen('ls').read()}}

{{request.application.__globals__.__builtins__.__import__('os').popen('cat flag').read()}}

List Payload:
https://github.com/payloadbox/ssti-payloads

PLATFORM CTF/CYBERSECURITY

1. *PICOCTF*
2. *HACKTHEBOX*
3. *TRYHACKME*



THANK YOU