



Perbaikan dan Mitigasi Insiden Web Judi Online

- Direktorat Operasi Keamanan Siber



Gambaran Umum

go.id/public/css/slot-online/

SLOT88 termasuk pilihan

| NAMA SITUS | MIN. DEPOSIT | BONUS | DAFTAR & LOGIN |
|------------|--------------|-----------------------|----------------|
| SLOT DANA | RP 10.000 | SLOT DEPOSIT VIA DANA | DAFTAR |
| SLOT GACOR | RP 10.000 | SLOT DANA | DAFTAR |

OMG! **TELAH HADIR BARU!!**
SLOT DEPOSIT DANA
MINIMAL DEPOSIT
10 RIBU
BONUS DEPOSIT TANPA
POTONGAN 100%!!

go.id/slot-gacor/index.php

Kami adalah salah satu situs judi slot online yang men...

| NAMA SITUS | MIN. DEPOSIT | BONUS | DAFTAR & LOGIN |
|------------|--------------|---------------|----------------|
| SLOT GACOR | RP 10.000 | BONUS GACOR!! | DAFTAR |

DAFTAR DAN MENANGKAN JACKPOTNYA
MAXWIN 500



Penyebab Terjadinya Situs Judi Online

- Menggunakan CMS/Teknologi yang outdated
- File Upload File yang tidak disanitasi
- XSS (Input file yang tidak disanitasi)
- Membuka port remote/shell pada ip publik



Menggunakan CMS/Teknologi yang outdated

exploit-db.com/exploits/50383

EXPLOIT DATABASE

Apache HTTP Server 2.4.49 - Path Traversal & Remote Code Execution (RCE)

| | | | | | |
|-------------------------|---------------------------|-------------------------------|-------------------------|------------------------------|----------------------------|
| EDB-ID: 50383 | CVE: 2021-41773 | Author: LUCAS SOUZA | Type: WEBAPPS | Platform: MULTIPLE | Date: 2021-10-06 |
|-------------------------|---------------------------|-------------------------------|-------------------------|------------------------------|----------------------------|

EDB Verified: ✓

Exploit: ↓ / {}

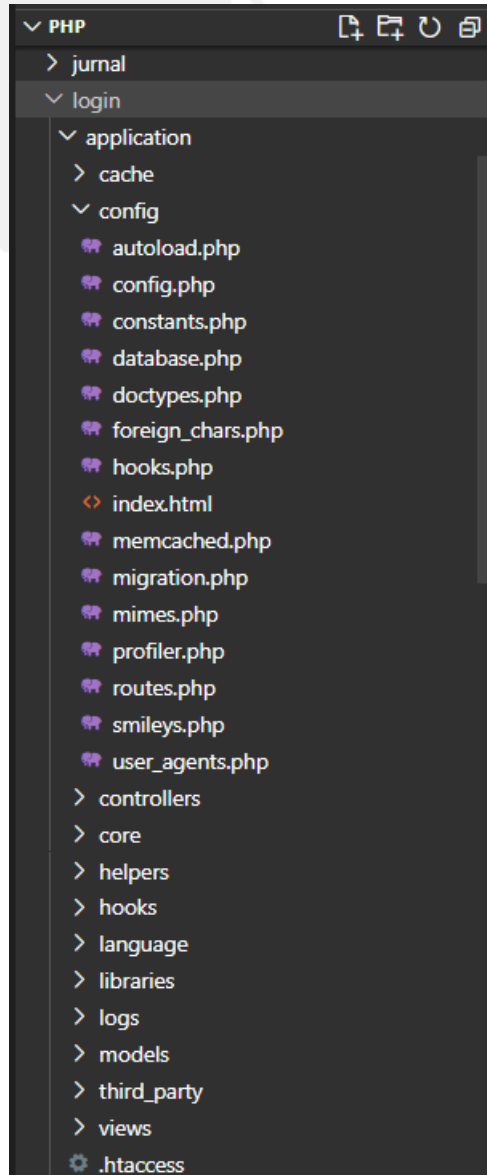
Vulnerable App: ▾

```
# Exploit Title: Apache HTTP Server 2.4.49 - Path Traversal & Remote Code Execution (RCE)
# Date: 10/05/2021
# Exploit Author: Lucas Souza https://lsass.io
# Vendor Homepage: https://apache.org/
# Version: 2.4.49
# Tested on: 2.4.49
# CVE : CVE-2021-41773
# Credits: Ash Daulton and the cPanel Security Team
```

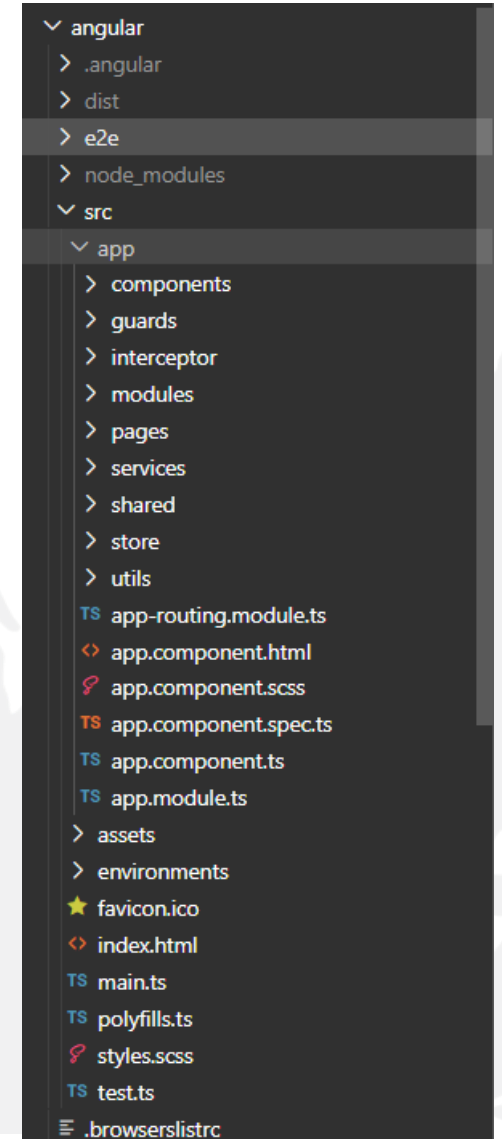


Menggunakan CMS/Teknologi yang outdated

Pada PHP
/var/www/html



Pada Teknologi
yang lebih
modern





File Upload File yang tidak di sanitasi



Drag&Drop files here

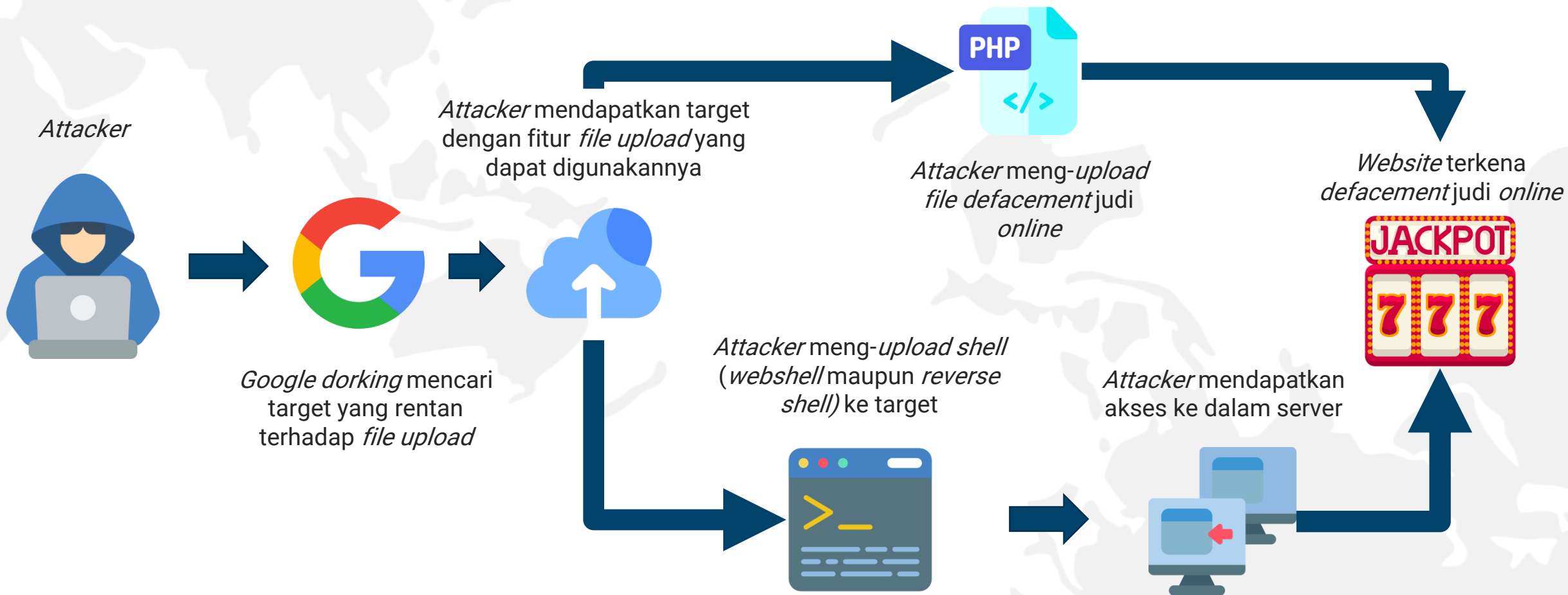
or

[Browse Files](#)

- Pembatasan Ekstensi baik secara front-end, maupun back-end

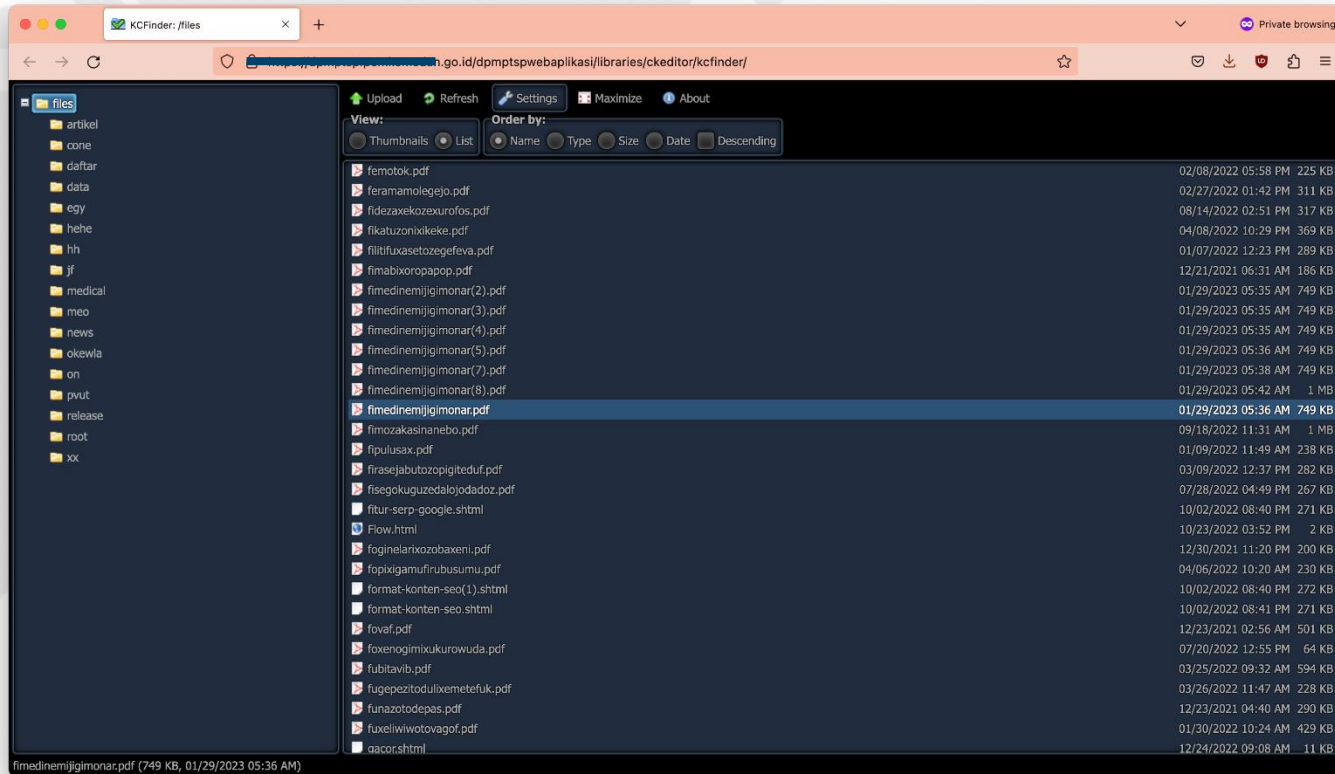


File Upload Yang Tidak disanitasi

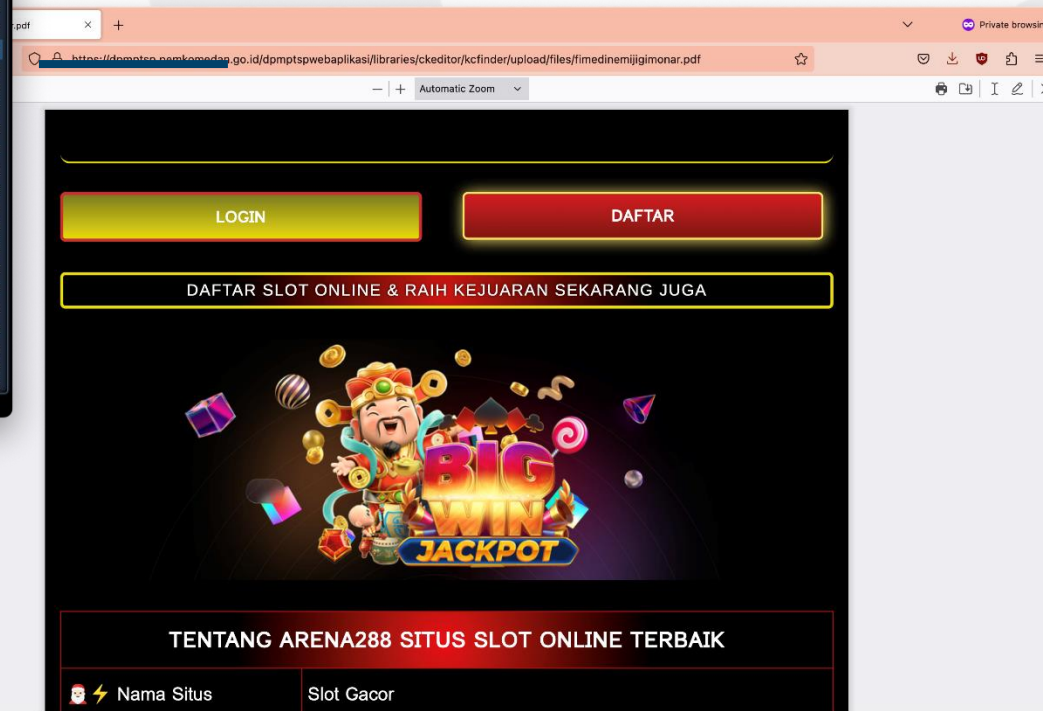




Proof of Concept Web Defacement Judi Online – File Upload



Fitur *file upload* dapat diakses secara publik

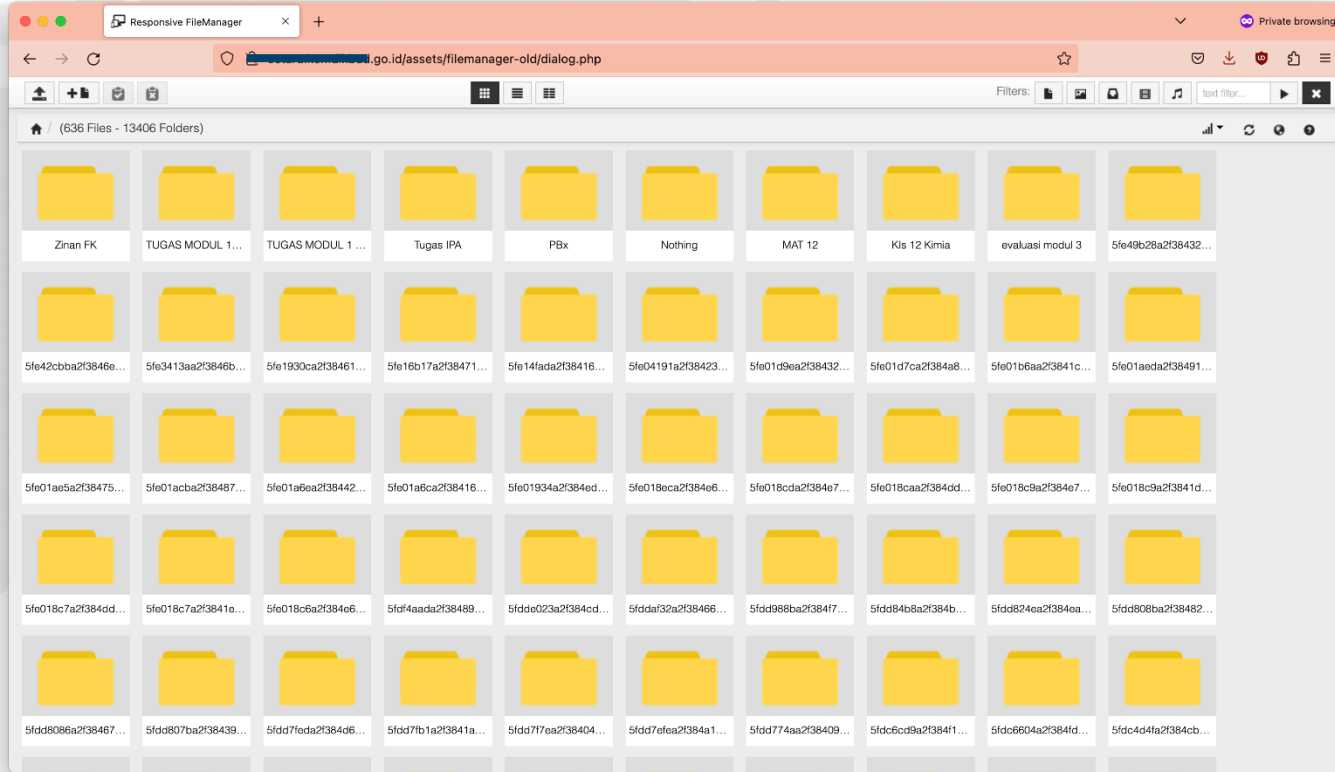


Defacement Judi *Online*

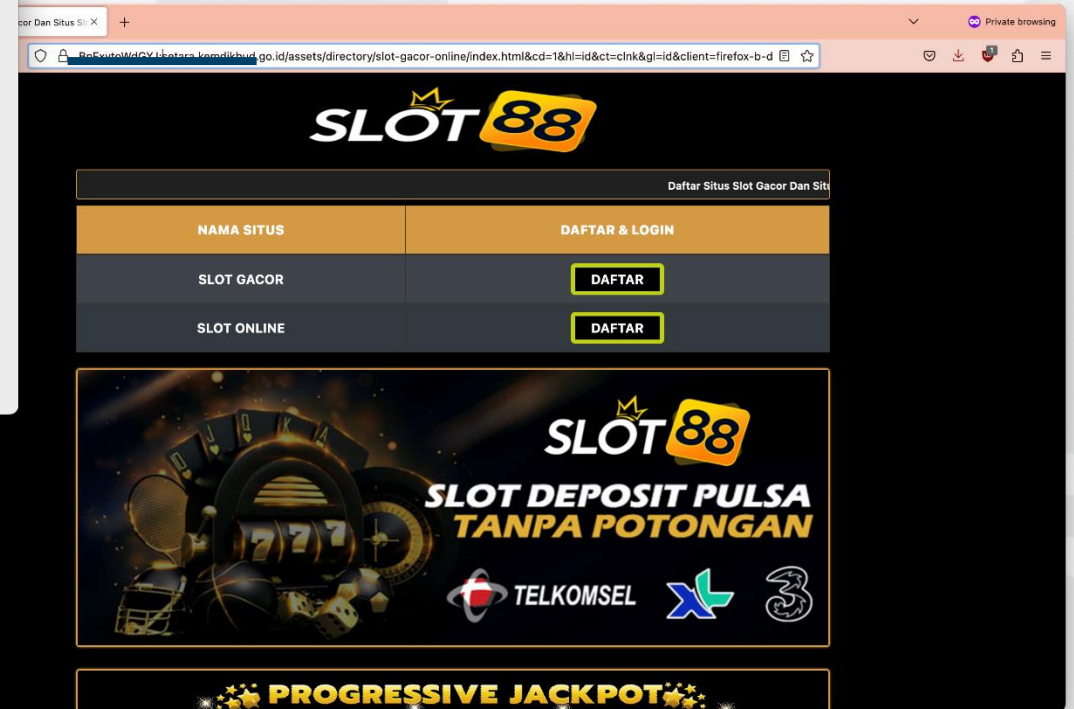




Proof of Concept Web Defacement Judi Online – File Upload



Fitur *file upload* dapat diakses secara publik

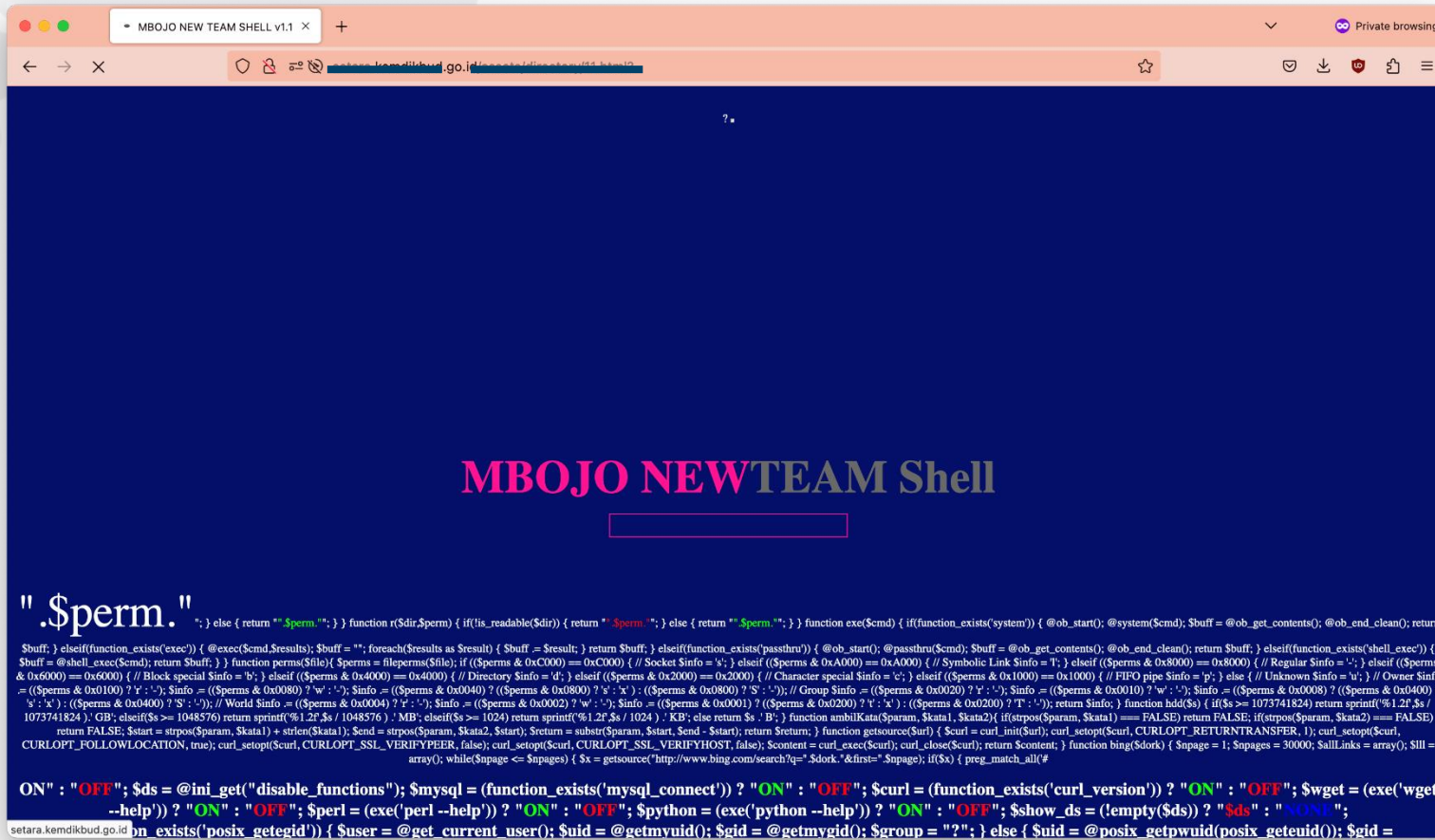


Defacement Judi *Online* (*cache*) – sudah diperbaiki





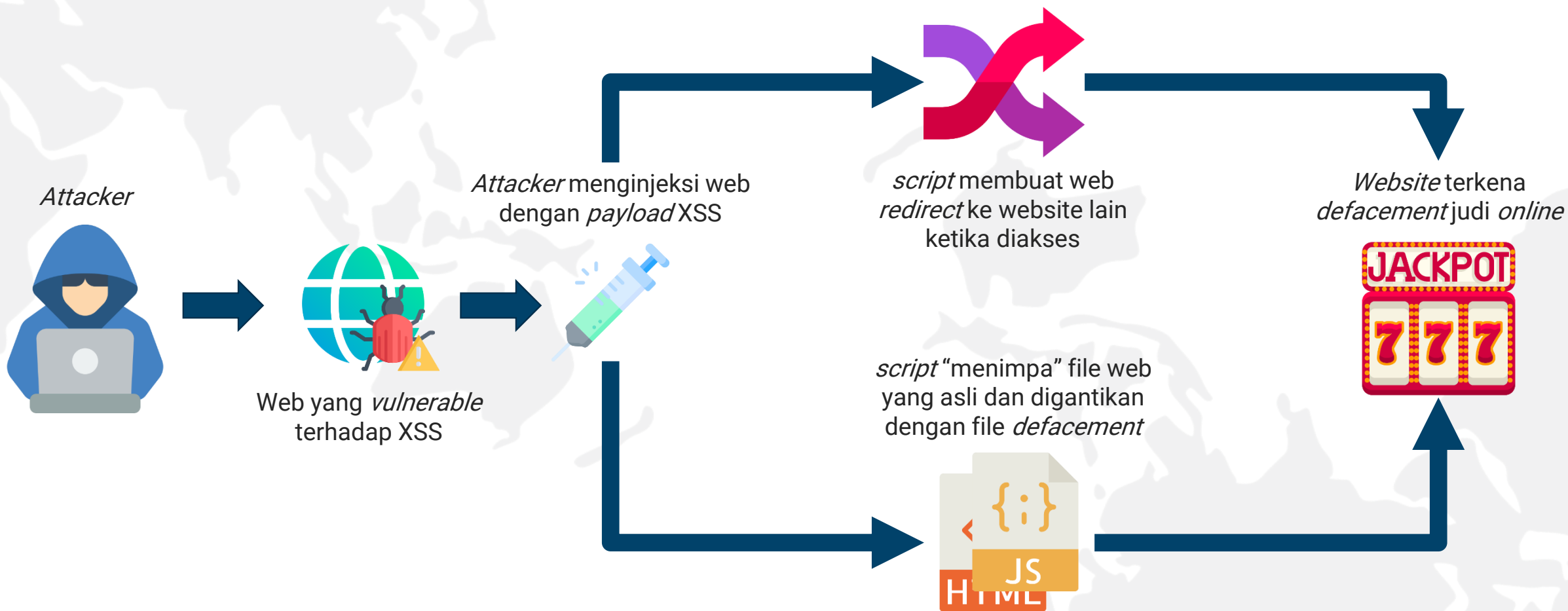
Proof of Concept Web Defacement Judi Online – File Upload



Webshell yang telah di-upload oleh attacker ke dalam server

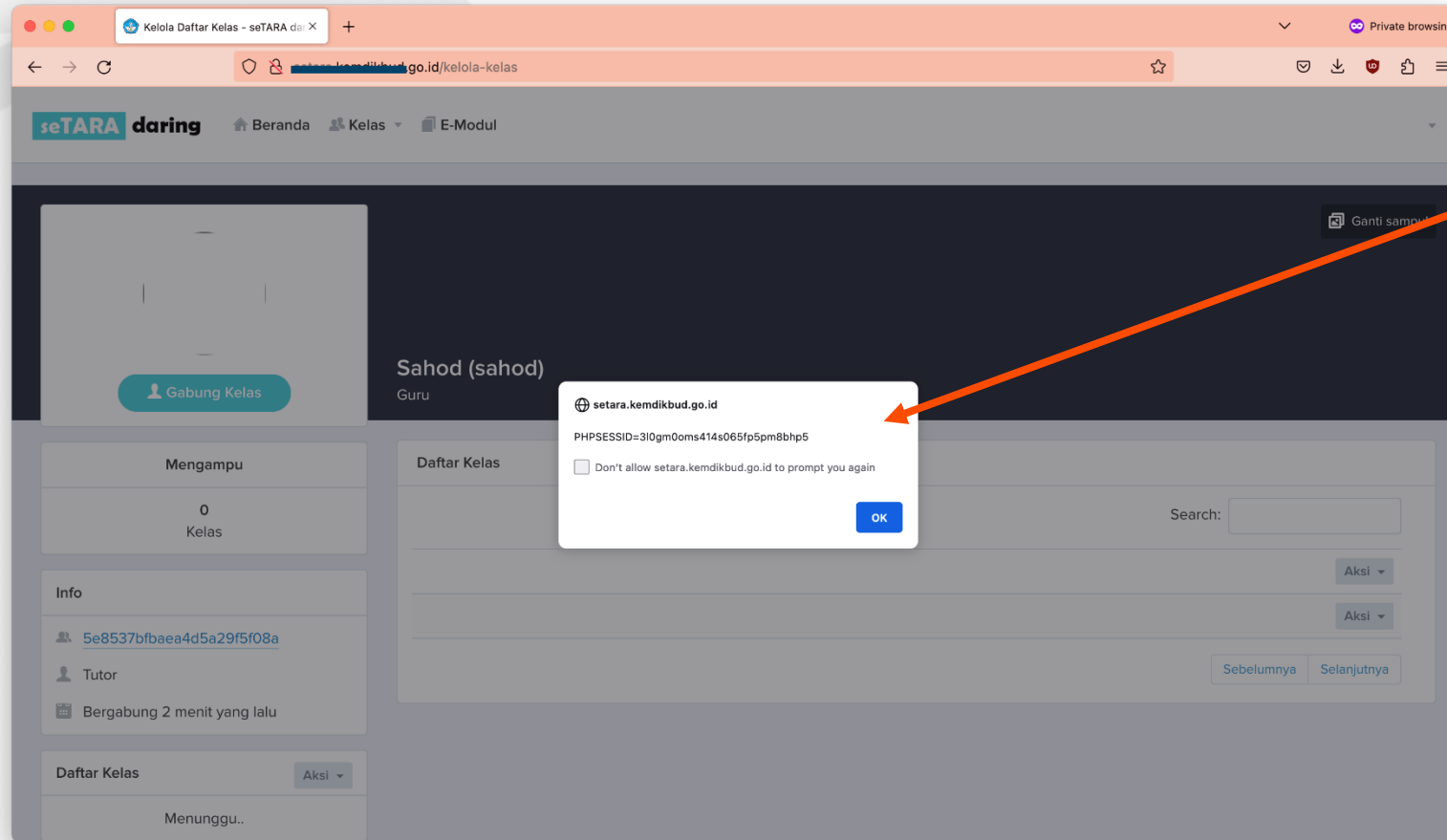


Kemungkinan Penyebab Utama Web Defacement Judi *Online* – XSS





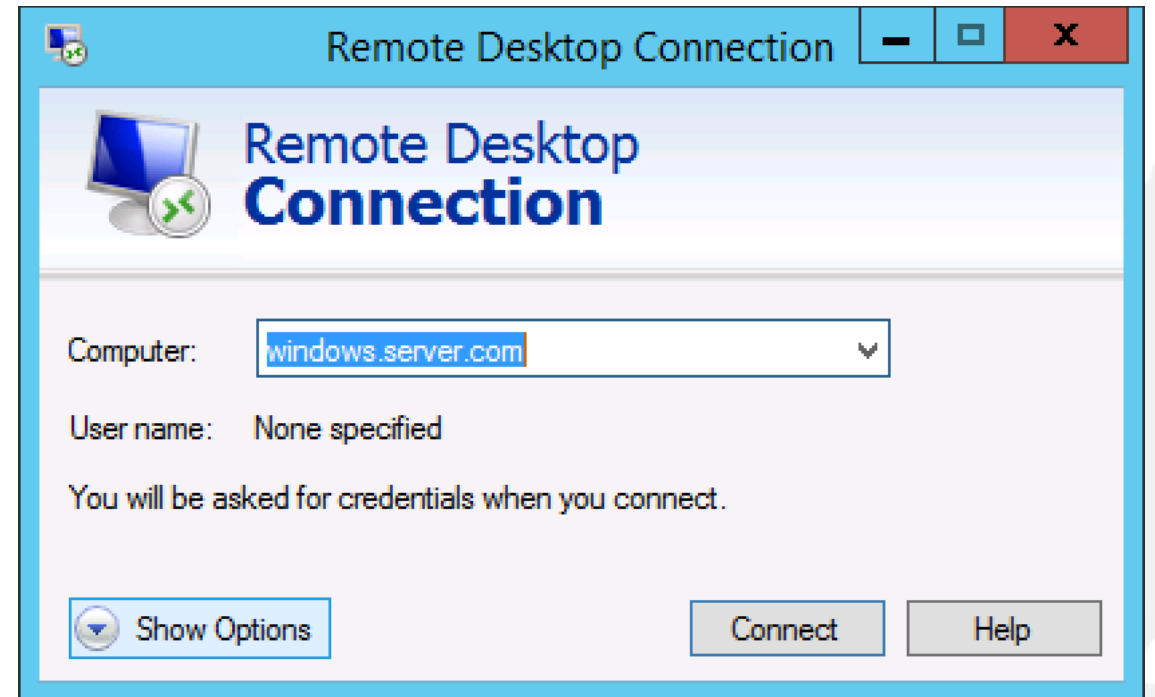
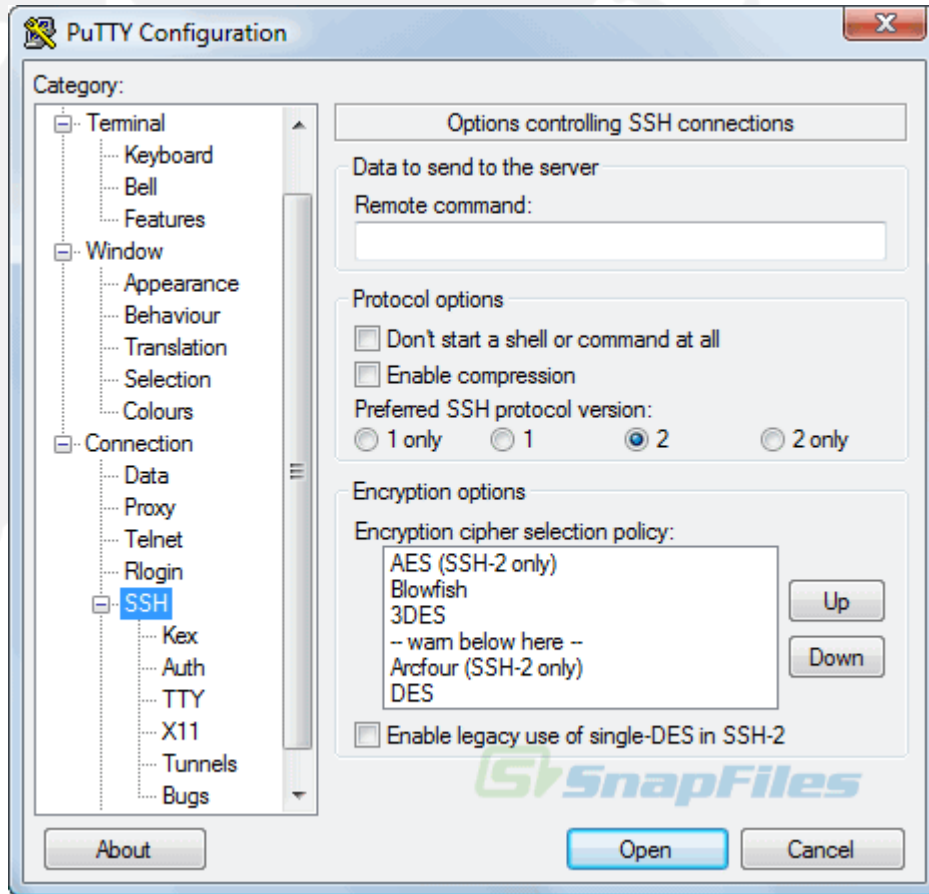
Proof of Concept Web Defacement Judi Online – XSS



script yang diinjeksikan ke dalam web berhasil dieksekusi



Membuka Port SSH/Remote Desktop pada IP Publik





Perbaikan Website Terdampak

 **TOOLBOX**





Perbaikan *Website* Terdampak

| No | Objective | C | Keterangan |
|----|--|---|---|
| 1 | Menentukan sistem yang terdampak dan segera melakukan isolasi terhadap sistem yang terdampak ((e.g Melakukan <i>disconnect</i> melalui jaringan, ataupun pencabutan kabel <i>ethernet</i> dari sistem)) | | |
| 2 | Melakukan pengecekan terhadap <i>Content Management System</i> (CMS) yang digunakan, apakah sudah menggunakan versi terbaru atau belum | | |
| 3 | Melakukan pengecekan terhadap <i>Plugin</i> yang digunakan, apakah sudah menggunakan versi terbaru atau belum | | |
| 4 | Melakukan pengecekan terhadap <i>username</i> dan <i>password</i> yang digunakan, apakah sudah menerapkan metode penggunaan <i>password</i> yang direkomendasikan | | Sudah tidak menggunakan <i>password default</i> , dan sudah menggunakan kombinasi huruf besar dan kecil, angka, simbol, karakter unik |
| 5 | Menerapkan sistem <i>Two Factor Authentication</i> (2FA) pada sistem <i>login</i> | | |

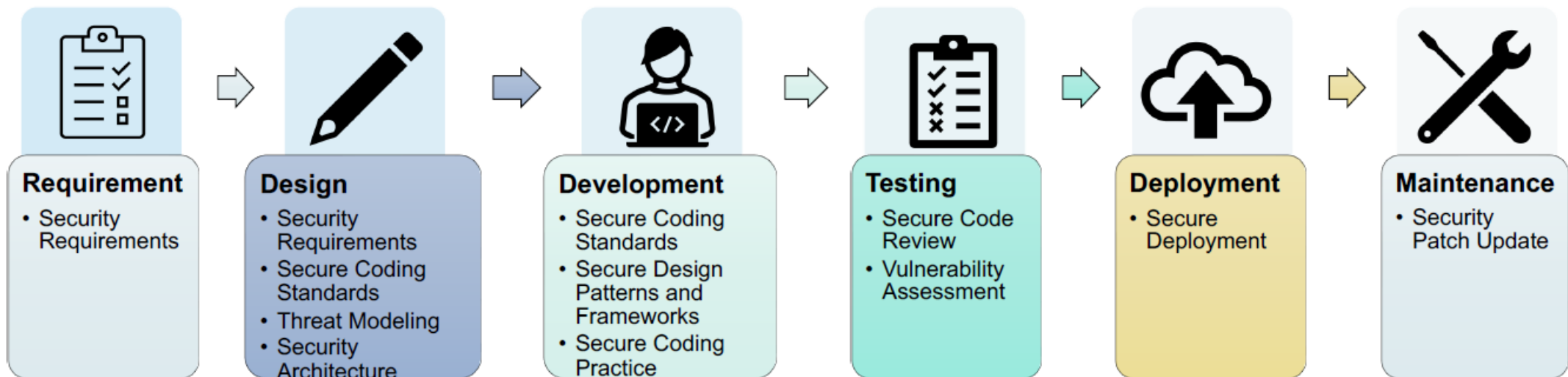


Perbaikan *Website* Terdampak

| No | Objective | C | Keterangan |
|----|--|---|--|
| 6 | Melakukan <i>scanning webshell</i> seperti melakukan pengecekan file-file pada direktori <i>website</i> satu persatu untuk menemukan <i>webshell</i> | | |
| 7 | Melakukan pengecekan konfigurasi <i>website</i> apakah ada perubahan pada konfigurasi atau kesalahan pada konfigurasi (misconfiguration) | | Apakah masih ada yang HTTP, sanitasi input |
| 8 | Melakukan inventarisasi pada <i>website</i> yang masih aktif digunakan dan dikelola, serta menonaktifkan <i>website</i> yang sudah tidak pernah digunakan | | |
| 9 | Memeriksa <i>port</i> internal yang terbuka dan dapat diakses oleh publik | | Linux: netstat -tulpn Windows: netsat -an find "XX" |
| 10 | Melakukan <i>dump</i> atau <i>backup</i> terhadap file <i>website</i> , kemudian dikirimkan ke BSSN secara resmi dengan surat permohonan perbantuan analisis | | Utamakan CSIRT yang sudah dimiliki |
| 11 | Menerapkan Whitelist/VPN ketika domain/subdomain digunakan untuk integrasi data sistem seperti API | | |



Mitigasi



Sumber : EC-Council Secure SDLC



Mitigasi



Update ke
CMS/Teknologi
Terbaru



Menguji keamanan aplikasi,
Kemudian perbaikan



Menerapkan sistem
keamanan seperti WAF/EDR



File Integrity Monitoring

/var/www/html (file web)

