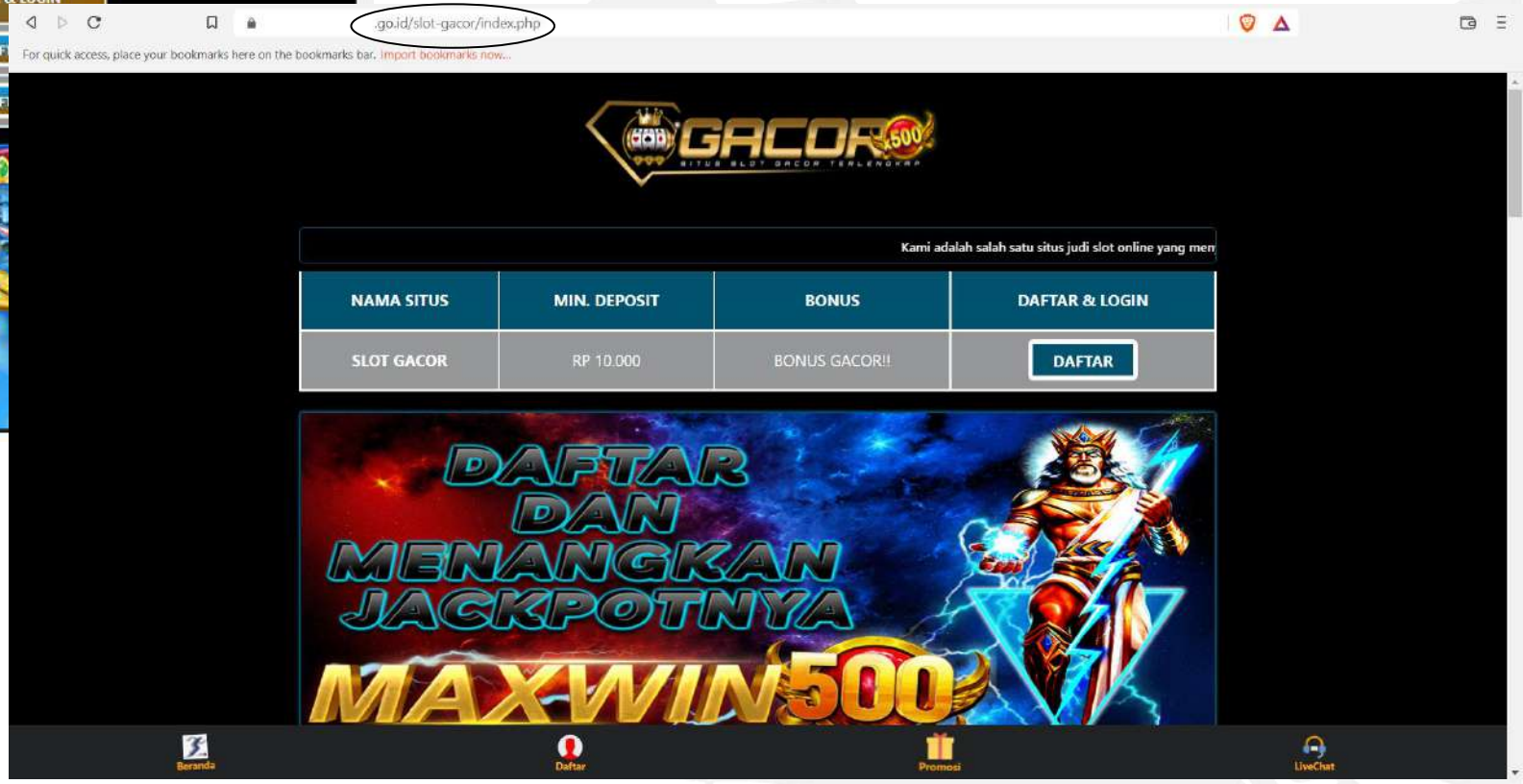
Perbaikan dan Mitigasi Insiden Web Judi Online

- Direktorat Operasi Keamanan Siber

BERSAMA BSSN NEGARA AMAN SEJAHTERA | 8 FEBRUARI 2023

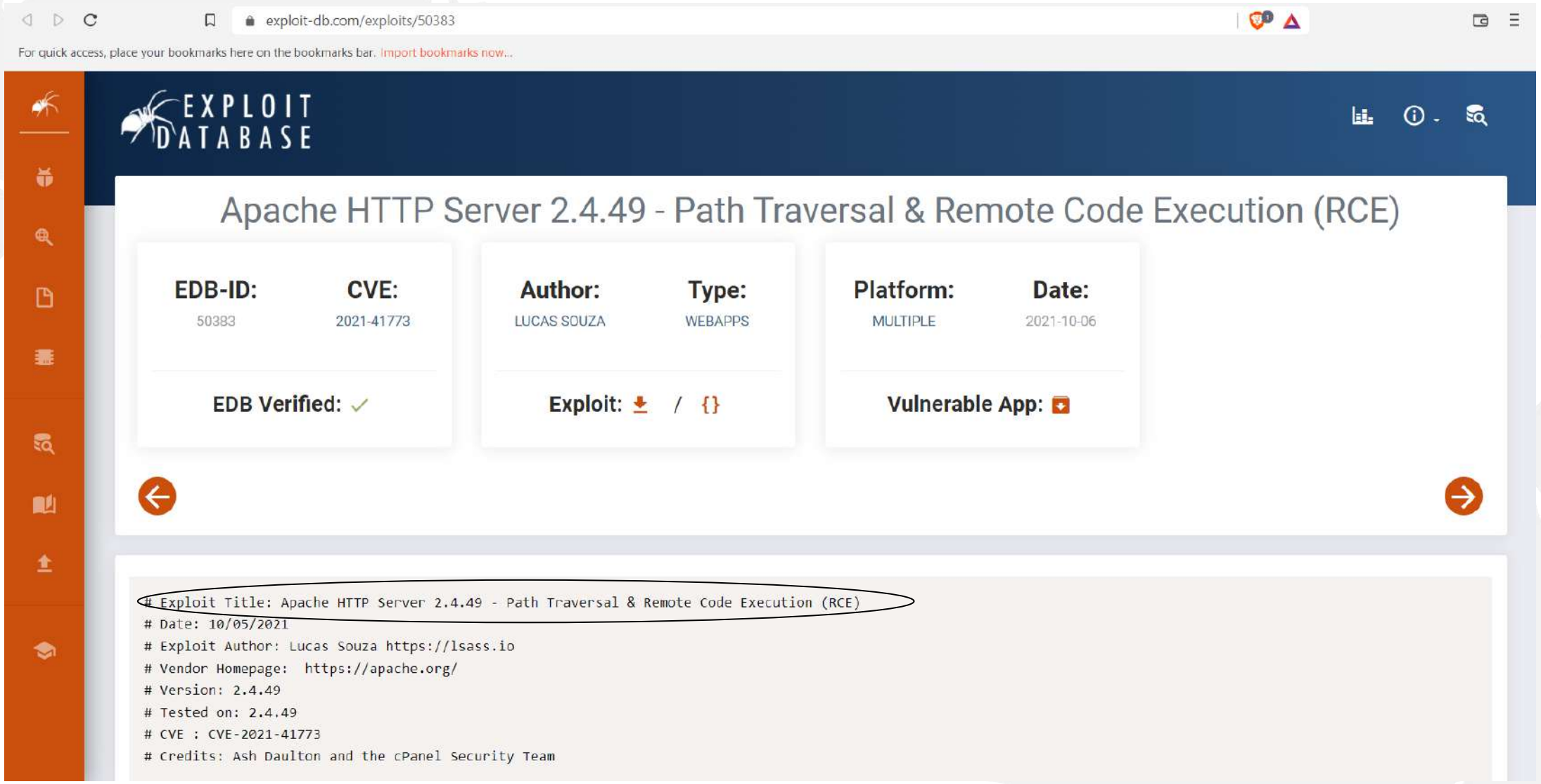
Gambaran Umum



Penyebab Terjadinya Situs Judi Online

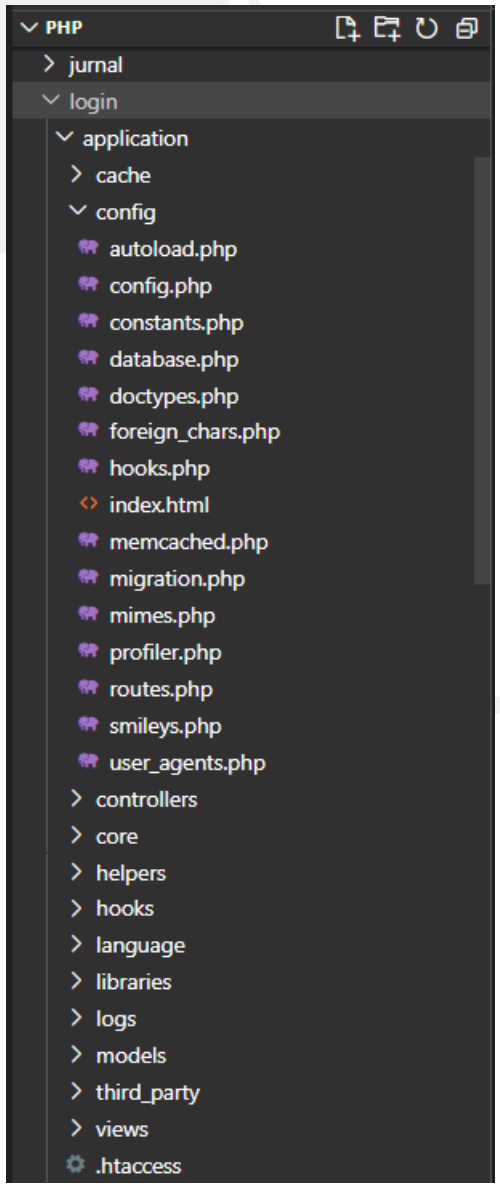
- Menggunakan CMS/Teknologi yang outdated
- File Upload File yang tidak disanitasi
- XSS (Input file yang tidak disanitasi)
- Membuka port remote/shell pada ip publik

Menggunakan CMS/Teknologi yang outdated

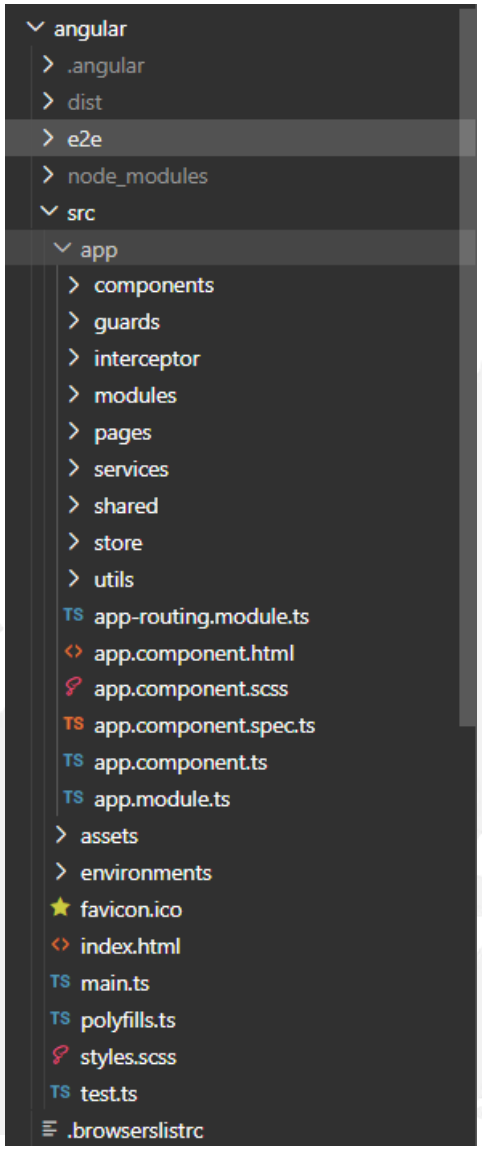


Menggunakan CMS/Teknologi yang outdated

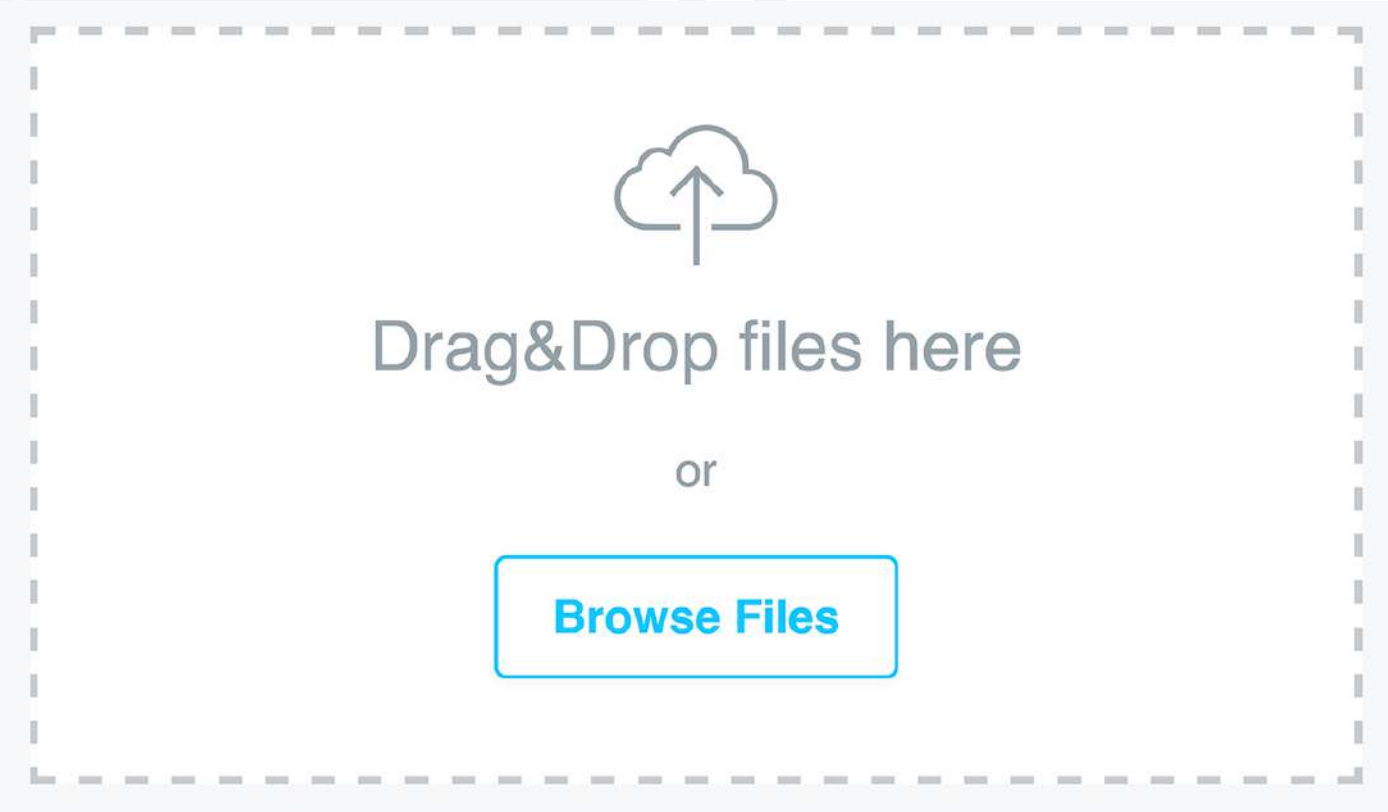
Pada PHP
/var/www/html



Pada Teknologi yang lebih modern



File Upload File yang tidak di sanitasi



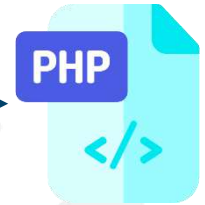
- Pembatasan Ekstensi baik secara front-end, maupun back-end

File Upload Yang Tidak disanitasi

Attacker

Google dorking mencari target yang rentan terhadap *file upload*

Attacker mendapatkan target dengan fitur *file upload* yang dapat digunakannya

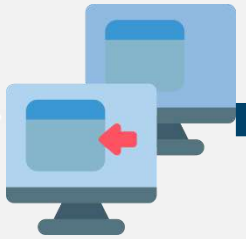


Attacker meng-*upload file defacement* judi *online*

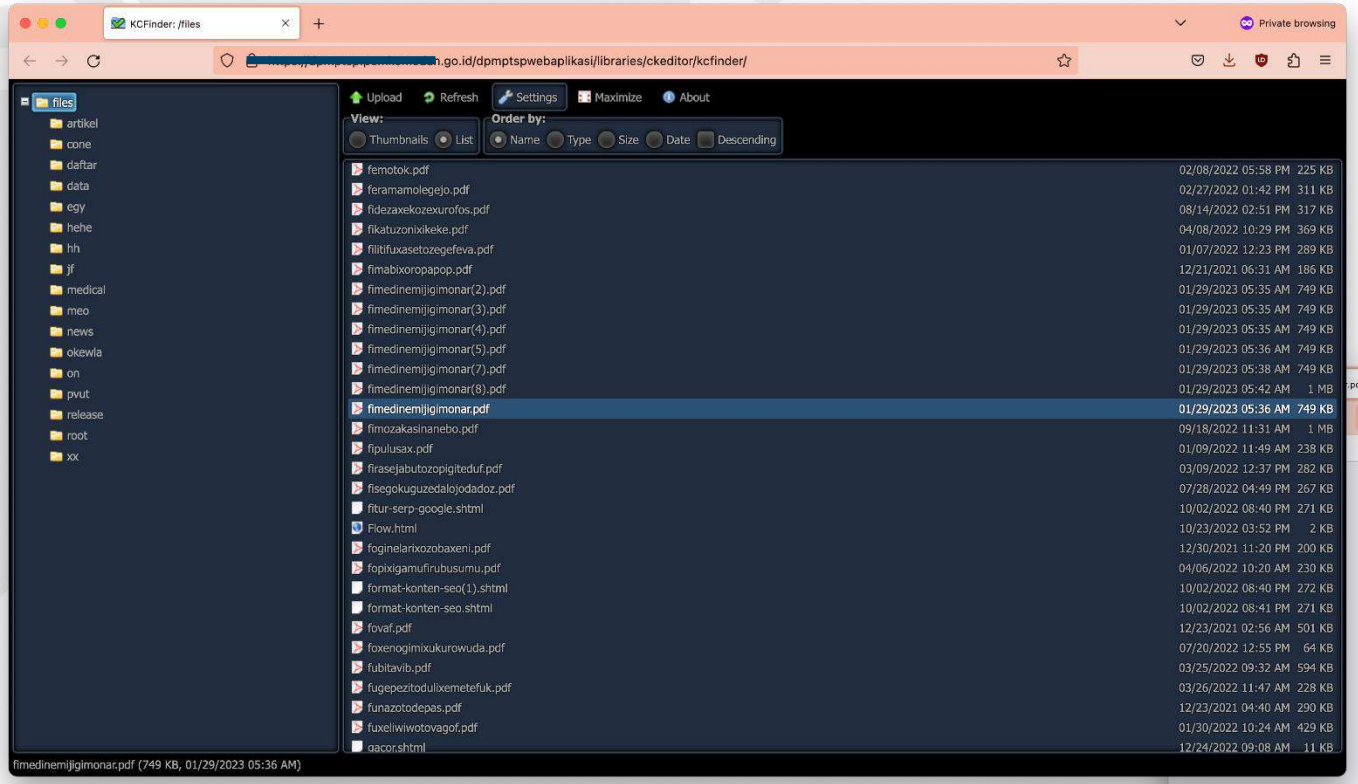
Website terkena *defacement* judi *online*

Attacker meng-*upload shell* (*webshell* maupun *reverse shell)* ke target

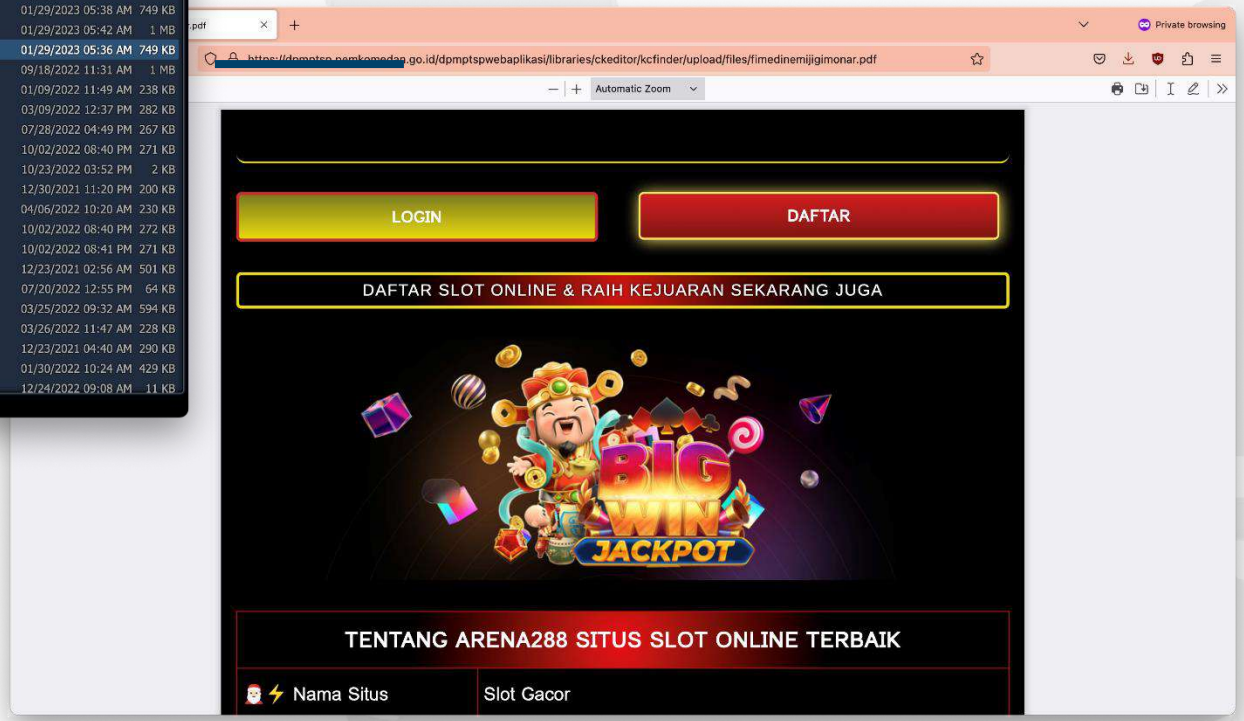
Attacker mendapatkan akses ke dalam server



Proof of Concept Web Defacement Judi *Online – File Upload*

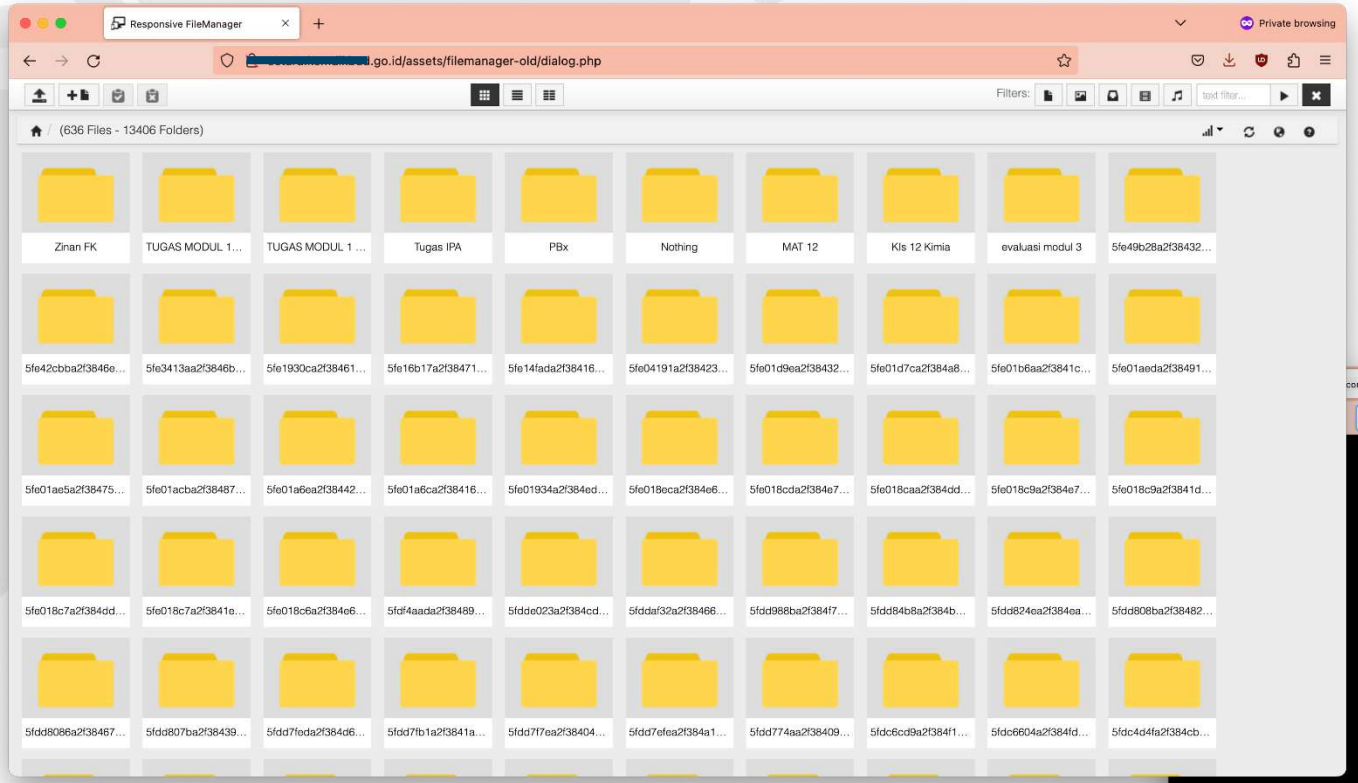


Fitur *file upload* dapat diakses secara publik

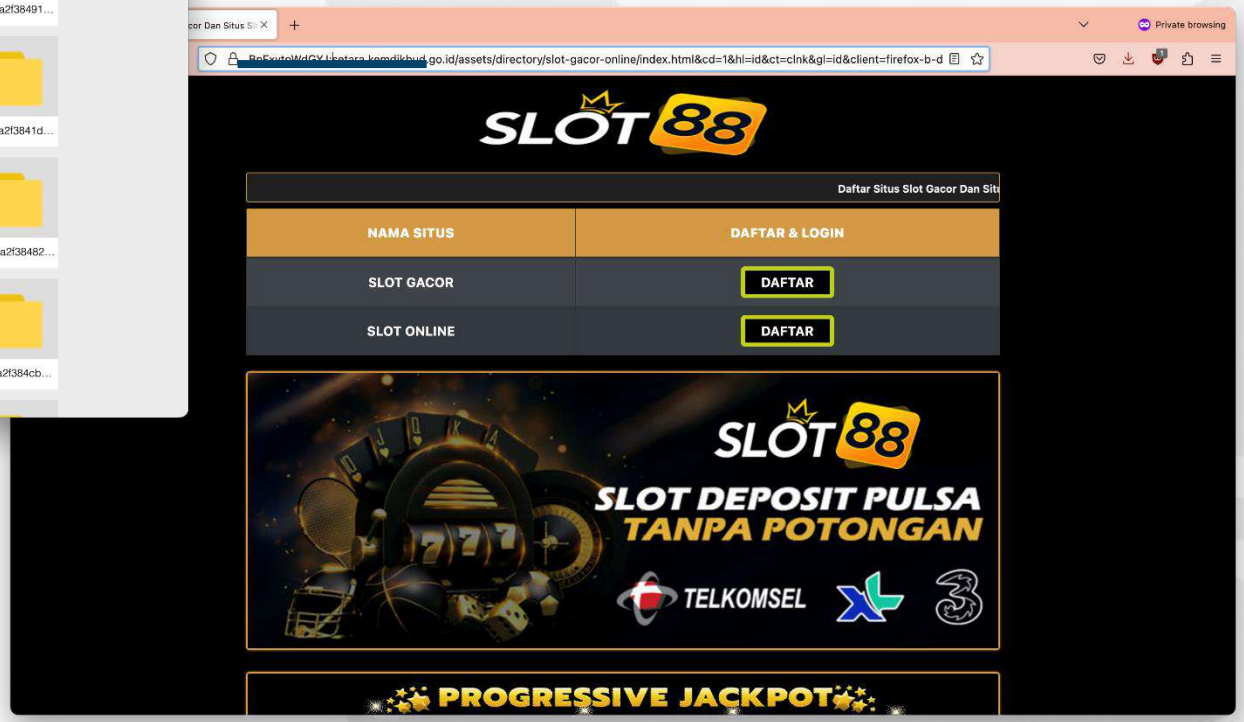


Defacement Judi *Online*

Proof of Concept Web Defacement Judi Online – *File Upload*

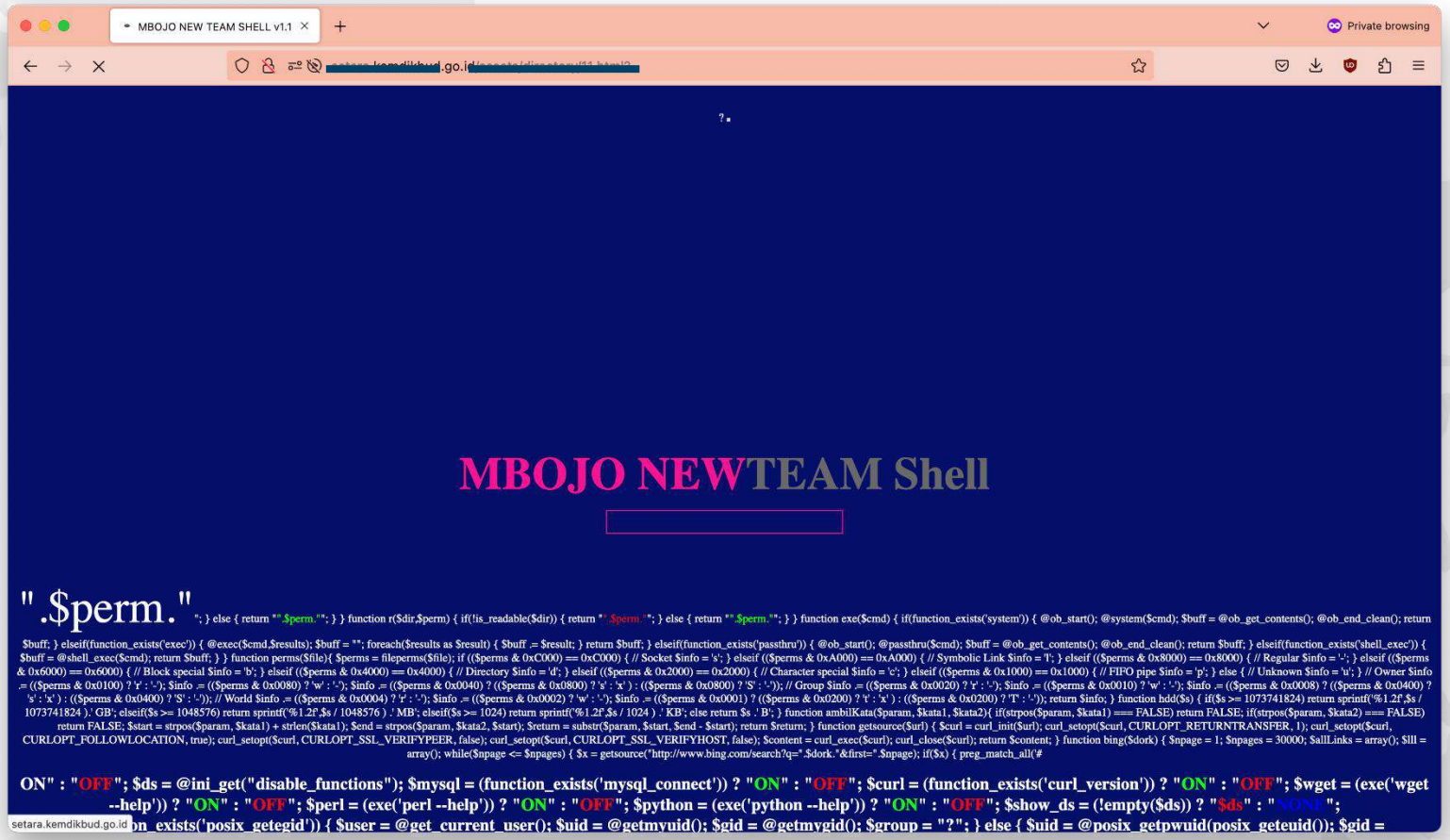


Fitur *file upload* dapat diakses secara publik



Defacement Judi *Online (cache)* – sudah diperbaiki

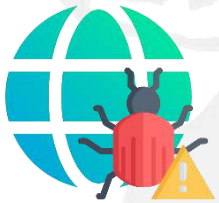
Proof of Concept Web Defacement Judi Online – *File Upload*



Webshell yang telah di-*upload* oleh *attacker* ke dalam server

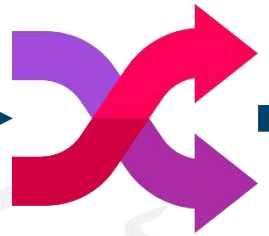
Kemungkinan Penyebab Utama Web Defacement Judi *Online* – *XSS*

Attacker



Web yang *vulnerable* terhadap XSS

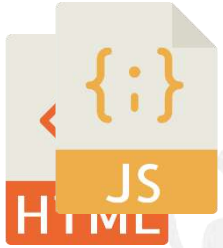
Attacker menginjeksi web dengan *payload* XSS



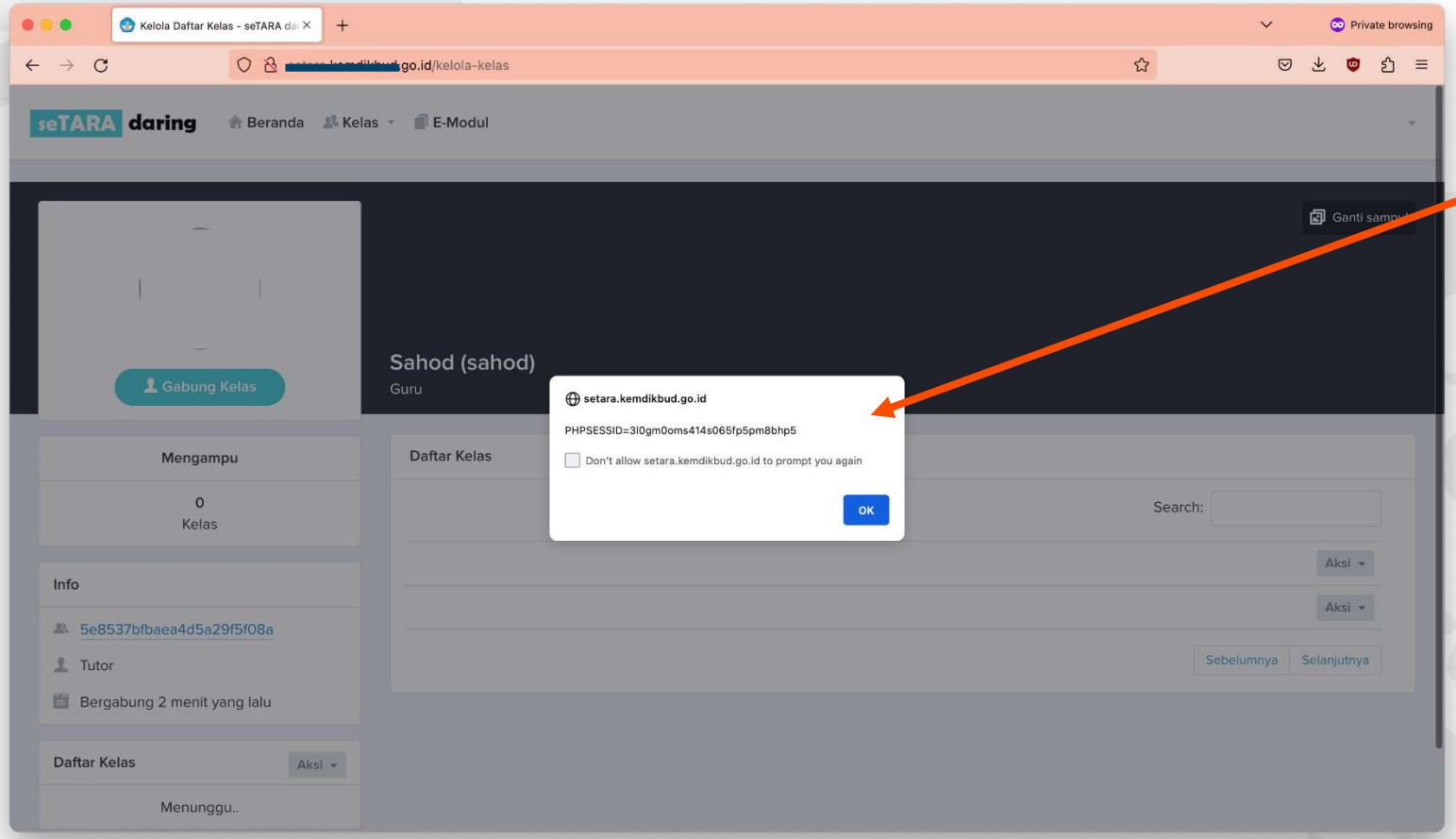
script membuat web *redirect* ke website lain ketika diakses

Website terkena *defacement* judi *online*

script "menimpa" file web yang asli dan digantikan dengan file *defacement*

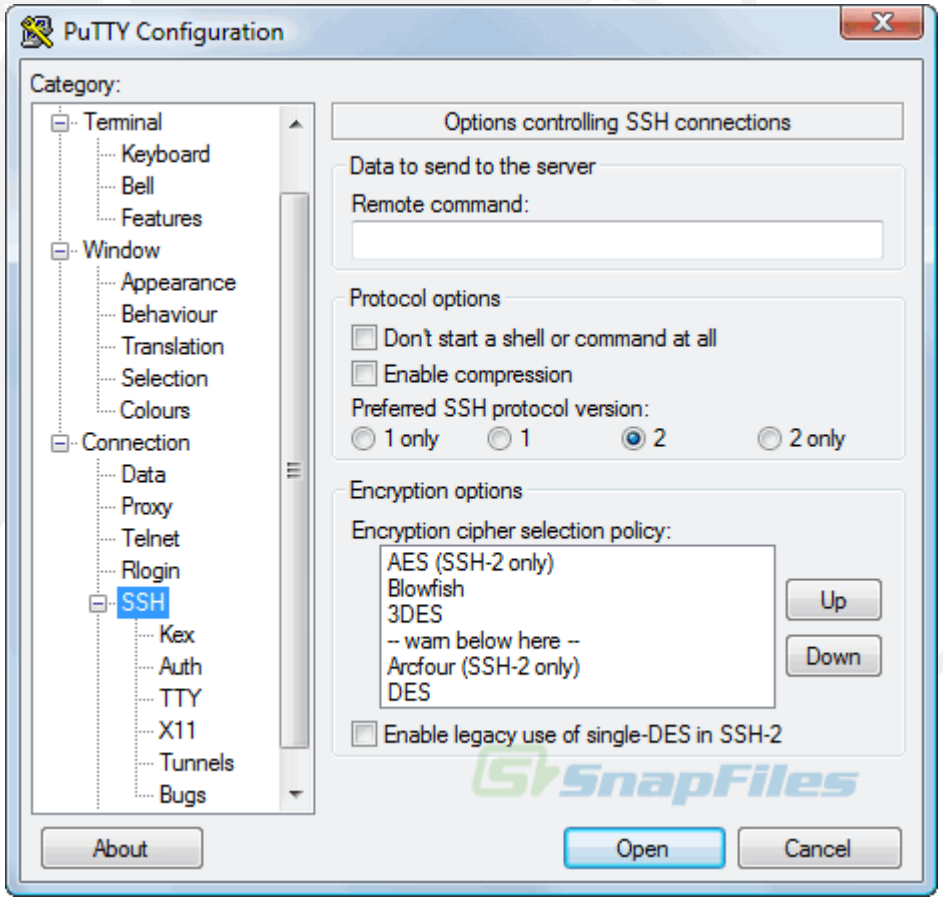


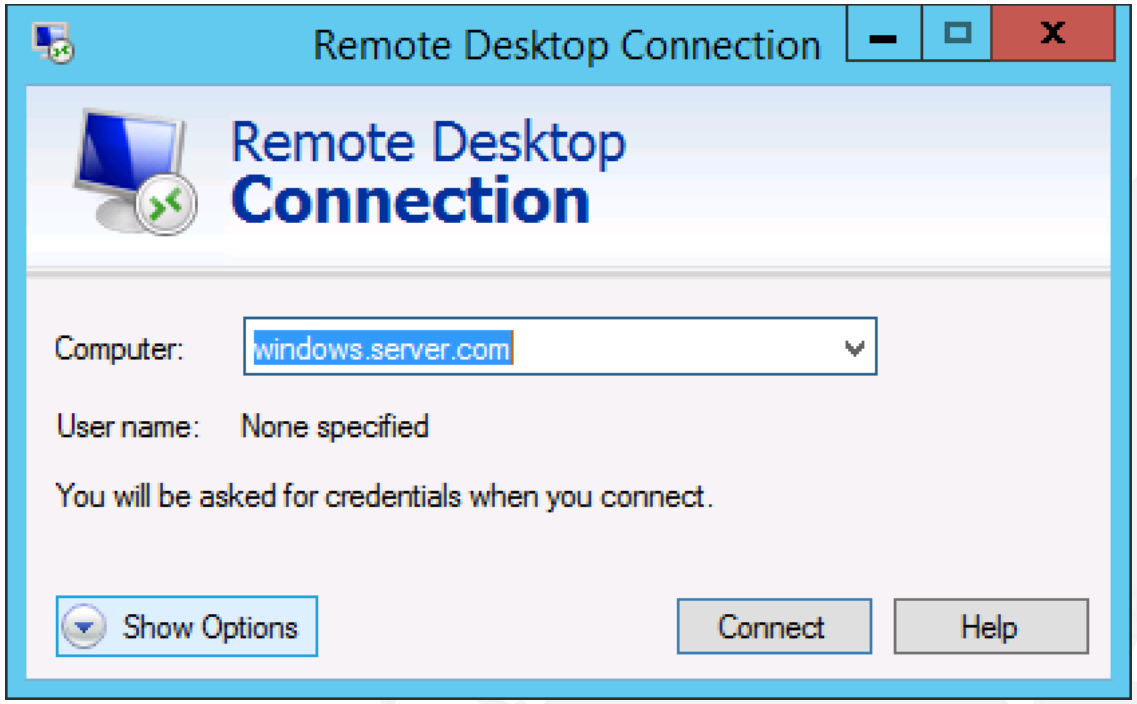
Proof of Concept Web Defacement Judi Online – XSS



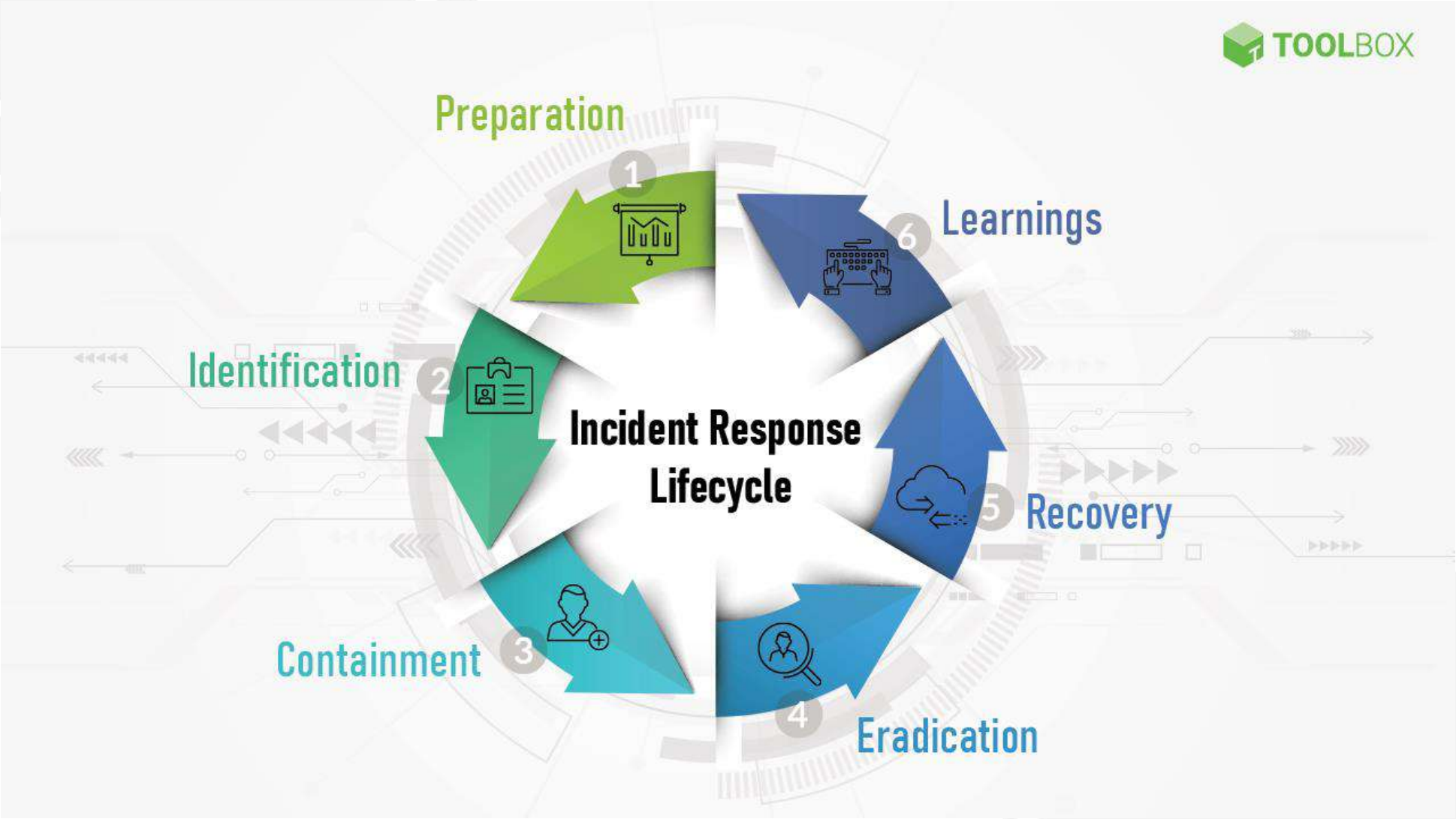
script yang diinjeksikan ke dalam web berhasil dieksekusi

Membuka Port SSH/Remote Desktop pada IP Publik





Perbaikan Website Terdampak



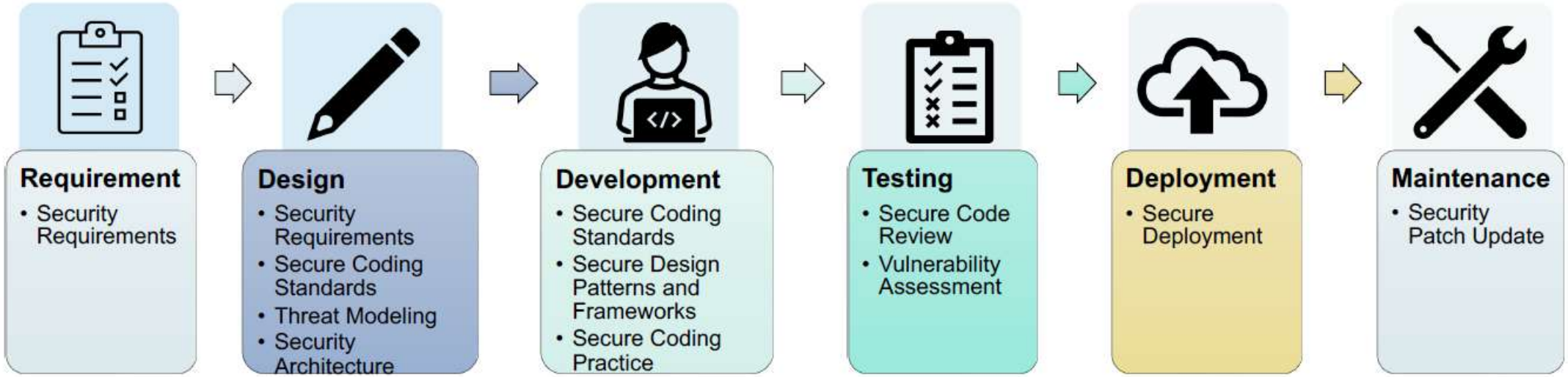
Perbaikan *Website* Terdampak

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

Perbaikan *Website* Terdampak

No	Objective	C	Keterangan
6	Melakukan *scanning webshell* seperti melakukan pengecekan file-file pada direktori *website* satu persatu untuk menemukan *webshell*		
7	Melakukan pengecekan konfigurasi *website* apakah ada perubahan pada konfigurasi atau kesalahan pada konfigurasi (missconfiguration)		Apakah masih ada yang HTTP, sanitasi input
8	Melakukan inventarisasi pada *website* yang masih aktif digunakan dan dikelola, serta menonaktifkan *website* yang sudah tidak pernah digunakan		
9	Memeriksa *port* internal yang terbuka dan dapat diakses oleh publik		Linux: netstat –tutlpn Windows: netsat –an | find "XX"
10	Melakukan *dump* atau *backup* terhadap file *website*, 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		

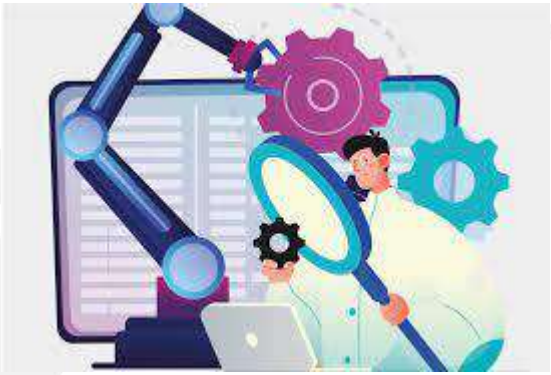
Mitigasi



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)