



Perbaikan dan Mitigasi Insiden Web Judi Online

- Direktorat Operasi Keamanan Siber

BERSAMA BSSN NEGARA AMAN SEJAHTERA | 8 FEBRUARI 2023



Gambaran Umum

The image displays two screenshots of online slot websites, both featuring a dark theme with blue and yellow accents.

Screenshot 1: SLOT DANA

URL: [.go.id/public/css/slot-online/](http://go.id/public/css/slot-online/)

Content:

- SLOT DANA** (NAMA SITUS)
- MIN. DEPOSIT: RP 10.000
- BONUS: SLOT DEPOSIT VIA DANA
- DAFTAR & LOGIN**

Screenshot 2: SLOT GACOR

URL: [.go.id/slot-gacor/index.php](http://go.id/slot-gacor/index.php)

Content:

- GACOR** (NAMA SITUS)
- MIN. DEPOSIT: RP 10.000
- BONUS: BONUS GACOR!!
- DAFTAR**

Banners:

- SLOT DANA**: TELAH HADIR BARU!! SLOT DEPOSIT DANA MINIMAL DEPOSIT 10 RIBU BONUS DEPOSIT TANPA POTONGAN 100%!!
- SLOT GACOR**: 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- Menggunakan CMS/Teknologi yang outdated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Menggunakan CMS/Teknologi yang outdated

The screenshot shows a web browser displaying the Exploit Database at exploit-db.com/exploits/50383. The page title is "Apache HTTP Server 2.4.49 - Path Traversal & Remote Code Execution (RCE)". Key details listed include:

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

Status indicators: EDB Verified: ✓, Exploit: [Download](#) / { }, Vulnerable App: [Details](#).

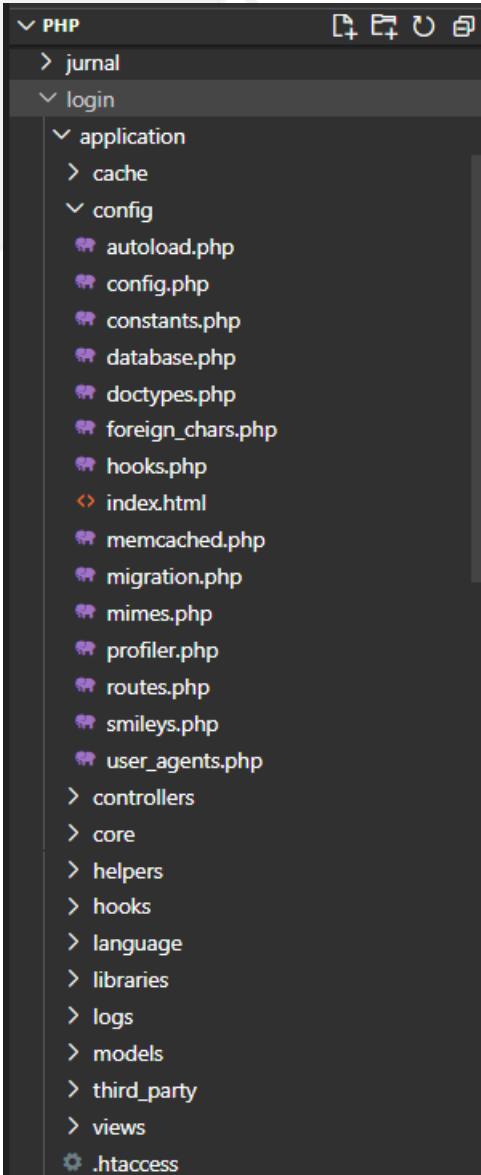
A code block at the bottom contains the exploit script, with the first few lines highlighted:

```
# 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
```

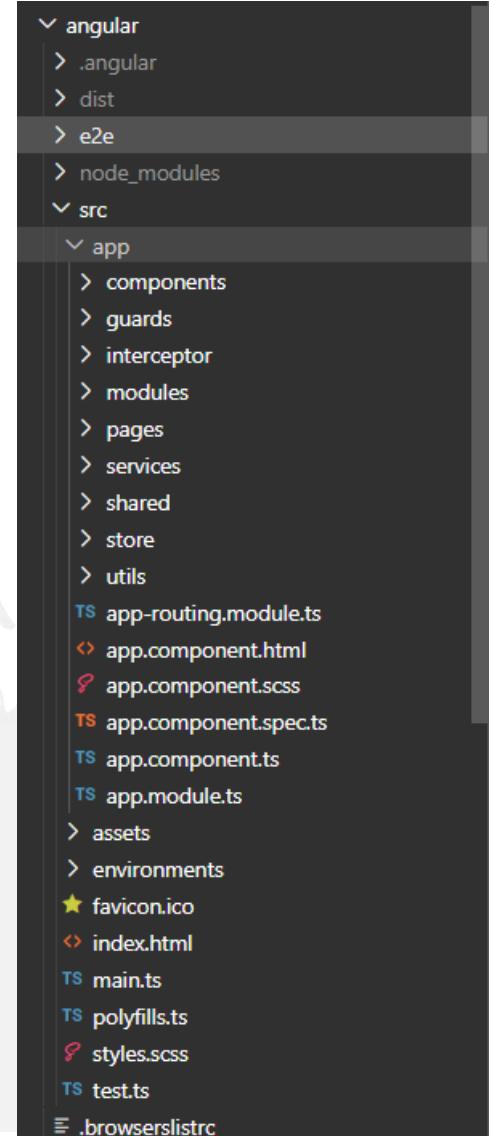


Menggunakan CMS/Teknologi yang outdated

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

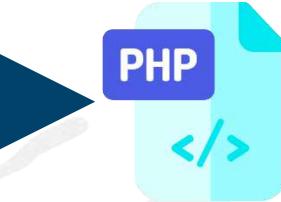
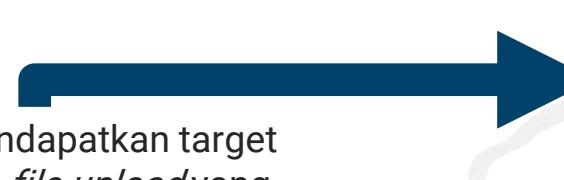
Attacker



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



Google dorking mencari target yang rentan terhadap *file upload*



Attacker meng-upload file defacement judi online



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



Attacker mendapatkan akses ke dalam server



Website terkena defacement judi online



Proof of Concept Web Defacement Judi Online – File Upload

KCFinder: /files

http://192.168.1.100/n.go.id/dpmptspwebaplikasi/libraries/ckeditor/kcfinder/

Upload Refresh Settings Maximize About

View: Order by:

Thumbnails List Name Type Size Date Descending

1	femotok.pdf	02/08/2022 05:58 PM	225 KB
2	feramamolegejo.pdf	02/27/2022 01:42 PM	311 KB
3	fidezaxekozexurofos.pdf	08/14/2022 02:51 PM	317 KB
4	fikatuzonikike.pdf	04/08/2022 10:29 PM	369 KB
5	fiitifuxasetozegefeva.pdf	01/07/2022 12:23 PM	289 KB
6	fimabixoropap.pdf	12/21/2021 06:31 AM	186 KB
7	fimedinemijigimonar(2).pdf	01/29/2023 05:35 AM	749 KB
8	fimedinemijigimonar(3).pdf	01/29/2023 05:35 AM	749 KB
9	fimedinemijigimonar(4).pdf	01/29/2023 05:35 AM	749 KB
10	fimedinemijigimonar(5).pdf	01/29/2023 05:36 AM	749 KB
11	fimedinemijigimonar(7).pdf	01/29/2023 05:38 AM	749 KB
12	fimedinemijigimonar(8).pdf	01/29/2023 05:42 AM	1 MB
13	fimedinemijigimonar.pdf	01/29/2023 05:36 AM	749 KB
14	fimozakasinanabebo.pdf	09/18/2022 11:31 AM	1 MB
15	fipulusax.pdf	01/09/2022 11:49 AM	238 KB
16	firsejabutozopigitduf.pdf	03/09/2022 12:37 PM	282 KB
17	sisegokugugedalojodadzo.pdf	07/28/2022 04:49 PM	267 KB
18	fitr-serp-google.shtml	10/02/2022 08:40 PM	271 KB
19	flow.html	10/23/2022 03:52 PM	2 KB
20	foginelarikozobabeni.pdf	12/30/2021 11:20 PM	200 KB
21	fopixigamufirubusumu.pdf	04/06/2022 10:20 AM	230 KB
22	format-konten-seo(1).shtml	10/02/2022 08:40 PM	272 KB
23	format-konten-seo.shtml	10/02/2022 08:41 PM	271 KB
24	fovaf.pdf	12/23/2021 02:56 AM	501 KB
25	foxenogimixukuronwuda.pdf	07/20/2022 12:55 PM	64 KB
26	fubitavib.pdf	03/25/2022 09:32 AM	594 KB
27	fugepezeitodulixemeteufuk.pdf	03/26/2022 11:47 AM	228 KB
28	funazotodepas.pdf	12/23/2021 04:40 AM	290 KB
29	fuxeliwiwotovagof.pdf	01/30/2022 10:24 AM	429 KB
30	gacor.shtml	12/24/2022 09:08 AM	11 KB

fimedinemijigimonar.pdf (749 KB, 01/29/2023 05:36 AM)

Defacement Judi *Online*

Fitur *file upload* dapat diakses secara publik

A screenshot of a web browser window titled 'pdf' showing a malicious login page. The URL is https://dompetn.pemkomedap.go.id/dpmptspwebaplikasi/libraries/ckeditor/kcfinder/upload/files/fimedinemijigimonar.pdf. The page features a black background with yellow and red accents. It includes two large buttons: 'LOGIN' on the left and 'DAFTAR' on the right. Below these buttons is a yellow banner with the text 'DAFTAR SLOT ONLINE & RAIH KEJUARAN SEKARANG JUGA'. The central focus is a cartoon illustration of a smiling character surrounded by floating coins, diamonds, and a lollipop, with the text 'BIG WIN JACKPOT' overlaid. At the bottom, there is a red banner with the text 'TENTANG ARENA288 SITUS SLOT ONLINE TERBAIK'. The browser interface shows standard navigation controls and a tab bar.



Proof of Concept Web Defacement Judi Online – File Upload

A screenshot of a web-based file manager titled "Responsive FileManager". The interface shows a grid of folder icons and their names. The names include "Zinan FK", "TUGAS MODUL 1...", "TUGAS MODUL 1...", "Tugas IPA", "PBx", "Nothing", "MAT 12", "Kls 12 Kimia", "evaluasi modul 3", and many other randomly generated names like "5fe42cb0a2f3846e...", "5fe341aa2f3846b...", etc. The browser title bar shows the URL "ReExecuteWdGY Lembaga Kependidikan.go.id/assets/filemanager-old/dialog.php".

Defacement Judi *Online*
(cache) – sudah diperbaiki

Fitur *file upload* dapat
diakses secara publik

A screenshot of a defaced website for "SLOT88". The page features a large "SLOT 88" logo at the top. Below it is a registration form with fields for "NAMA SITUS" and "DAFTAR & LOGIN", and buttons for "DAFTAR" under "SLOT GACOR" and "SLOT ONLINE". The main content area features a banner for "SLOT DEPOSIT PULSA TANPA POTONGAN" with a "PROGRESSIVE JACKPOT" banner below it. Logos for "TELKOMSEL", "XL", and "3" are visible. The browser title bar shows the URL "ReExecuteWdGY Lembaga Kependidikan.go.id/assets/directory/slot-gacor-online/index.html&cd=1&hl=id&ct=clnk&gl=id&client=firefox-b-d".

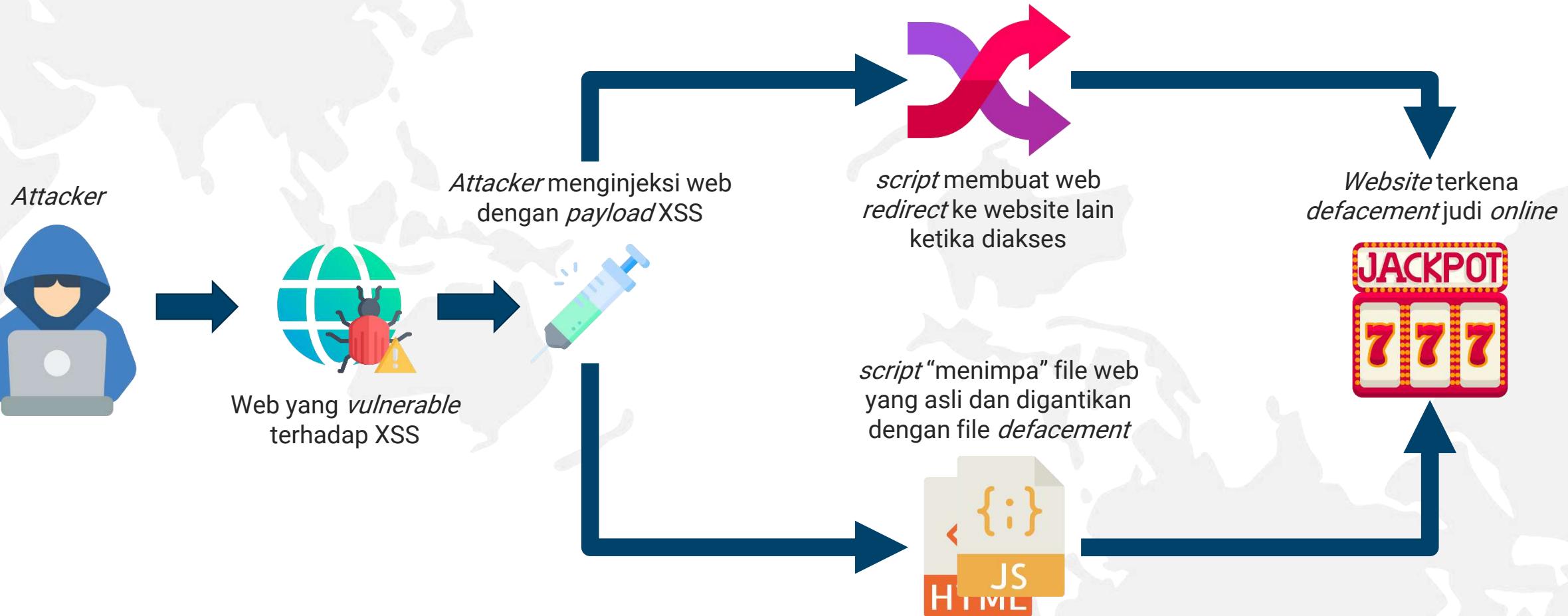


Proof of Concept Web Defacement Judi Online – File Upload

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



Kemungkinan Penyebab Utama Web Defacement Judi Online – XSS





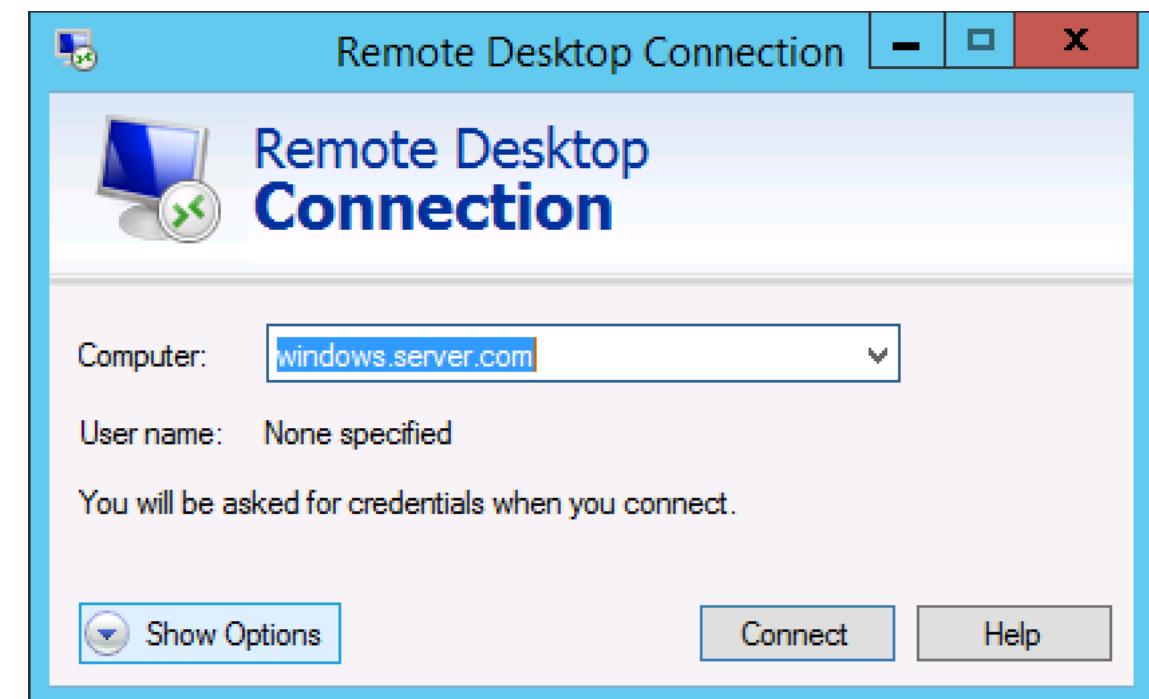
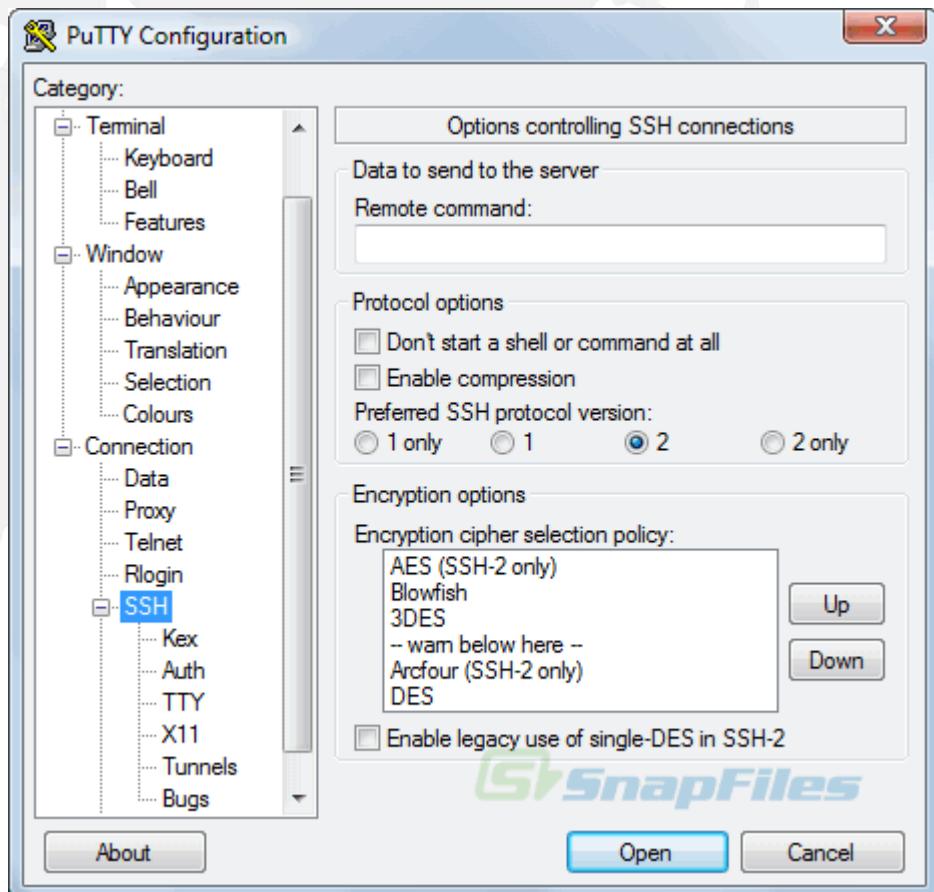
Proof of Concept Web Defacement Judi Online – XSS

The screenshot shows a web browser window with the URL `setara.kemdikbud.go.id/kelola-kelas`. The page is titled "seTARA daring" and displays a user profile for "Sahod (sahod)" under the "Guru" section. On the left, there's a sidebar with "Mengampu" (0 Kelas) and "Info" (User ID: 5e8537bfbaea4d5a29f5f08a). A modal dialog box is overlaid on the page, prompting the user with the message: "setara.kemdikbud.go.id" followed by a PHPSESSID value: "PHPSESSID=3l0gm0oms414s065fp5pm8bhp5". Below the message is a checkbox labeled "Don't allow setara.kemdikbud.go.id to prompt you again" and a blue "OK" button. An orange arrow points from the text "script yang diinjeksikan ke dalam web berhasil dieksekusi" to the modal dialog.

*script yang
diinjeksikan ke
dalam web berhasil
dieksekusi*

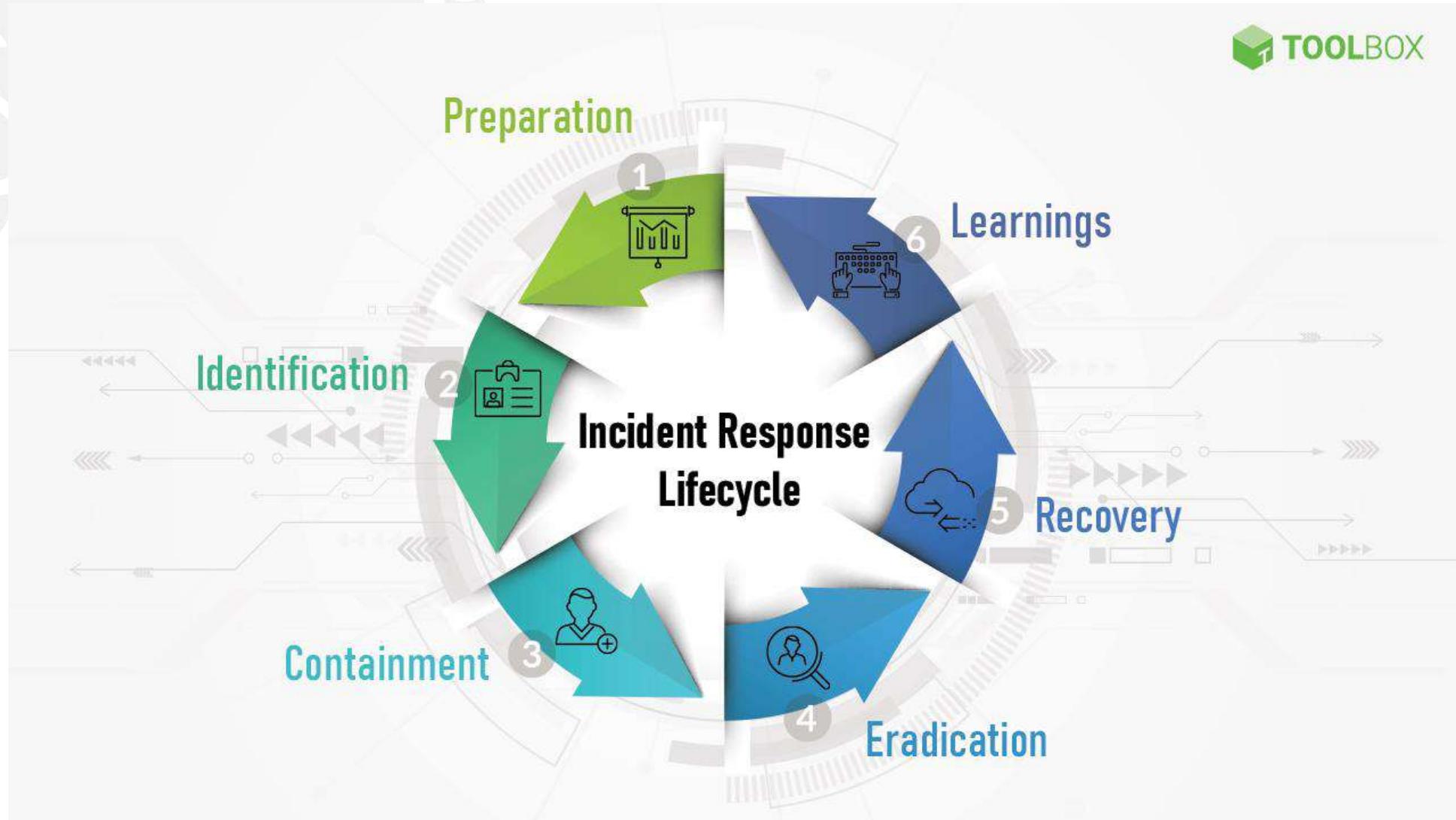


Membuka Port SSH/Remote Desktop pada IP Publik





■ 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 <i>disconect</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>		

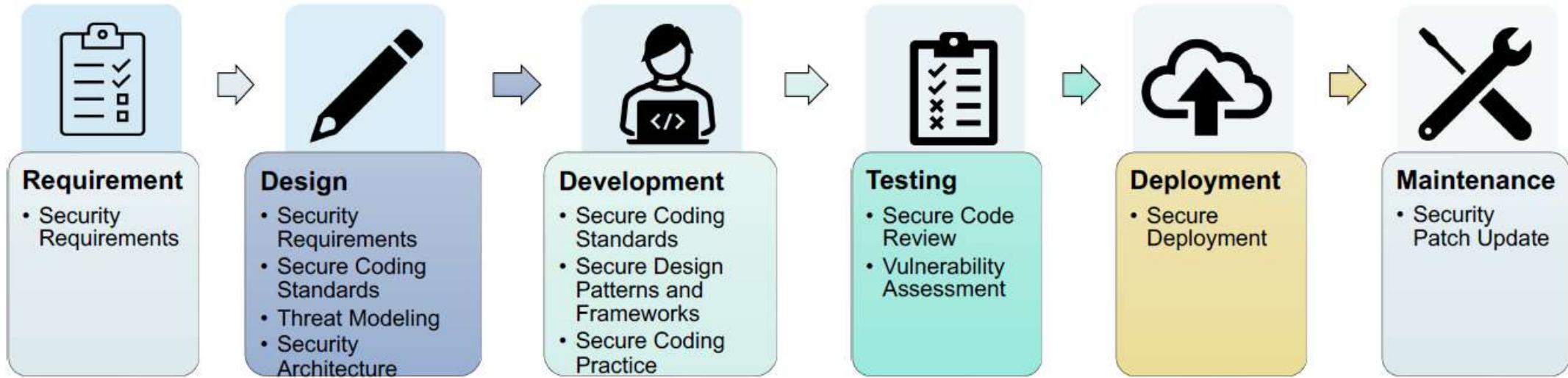


■ Perbaikan Website Terdampak

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 (missconfiguration)		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 -tutlpn 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 pertambuan 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)

