

Laporan Hasil Pengujian Penetration Test

ngflask.pokdartik.or.id

https://ngflask.pokdartik.or.id

Target	ngflask.pokdartik.or.id (https://)
Jenis Aplikasi	Python / Flask (indikasi cookie session)
Tanggal Pengujian	28 July 2026
Jenis Pengujian	Black-box, Read-only, Non-destructive
Lingkup	Transport, Security Headers, Cookie, CORS, Eksposur, Debug, Methods
Penyusun	Tim Pentest POKDARTIK
Klasifikasi	Rahasia — Hanya untuk pihak berwenang

RAHASIA

Dokumen ini menyajikan hasil tinjauan keamanan secara pasif (read-only). Tidak ada perubahan data, penghapusan, brute-force, atau eksploitasi aktif yang dilakukan.

1. Ringkasan Eksekutif

Pengujian keamanan (penetration test) terhadap <https://ngflask.pokdartik.or.id> dilakukan secara black-box, read-only, dan non-destructive pada 28 July 2026 oleh **Tim Pentest POKDARTIK**. Dari 12 area pengujian: **11 berstatus TERATASI** dan **1 berstatus MASIH TERBUKA** (0 MEDIUM, 0 LOW, sisanya INFO).

Catatan CMS: Situs ini terdeteksi sebagai **Python / Flask (indikasi cookie session)**. Rencana perubahan/migrasi platform harus menargetkan instalasi yang sesungguhnya.

Tabel Status Pengujian

No	Area Pengujian	Hasil	Status
F-01	Enkripsi Transport (HTTPS wajib / HSTS)	AMAN	TERATASI
F-02	Validitas & Kekuatan Sertifikat TLS	AMAN	TERATASI
F-03	Cookie & Session Flags	AMAN	TERATASI
F-04	Content Security Policy (CSP)	AMAN	TERATASI
F-05	Clickjacking Protection (X-Frame-Options)	AMAN	TERATASI
F-06	MIME Sniffing Protection	AMAN	TERATASI
F-07	Referrer Policy	AMAN	TERATASI
F-08	CORS Policy	AMAN	TERATASI
F-09	Debug Mode (Werkzeug)	AMAN	TERATASI
F-10	Eksposur Source / File Sensitif	AMAN	TERATASI
F-11	HTTP Methods (TRACE/PUT/DELETE)	AMAN	TERATASI
F-12	Header X-XSS-Protection (usang)	LEMAH	MASIH TERBUKA

Status "TERATASI" = kontrol diterapkan dengan benar saat pengujian. "MASIH TERBUKA" = temuan yang disarankan diperbaiki.

2. Apa yang Dilakukan dalam Pengujian Ini

- **Rekon pasif:** header HTTP, identifikasi teknologi (Server, CMS), metadata TLS via openssl.
- **Security headers:** HSTS, CSP, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, CORS, X-XSS-Protection.
- **Transport:** perbandingan HTTP vs HTTPS (plaintext leak).
- **Cookie/session:** flag Secure, HttpOnly, SameSite.
- **Eksposur endpoint:** pemindaian path source/file sensitif (status only).
- **Debug mode:** POST JSON, cek traceback vs respons generik.
- **HTTP methods & CORS:** verifikasi metode berbahaya & kebijakan cross-origin.

Alat

- curl 8.x — header, status, body.
- openssl — sertifikat TLS.
- Python 3 — orkestrasi & pelaporan.

Yang TIDAK Dilakukan

- Tidak brute-force, tidak ubah data, tidak eksploitasi aktif, tidak DoS.
- Tidak menyimpan kredensial.

3. Temuan & Verdict

F-01 — Enkripsi Transport (HTTPS wajib / HSTS)

TERATASI

Tingkat: INFO

Bukti:

```
HTTP -> 301 redirect ke HTTPS, tidak ada plaintext body.
```

Dampak: Risiko MITM/session hijack via plaintext dapat diabaikan.

Rekomendasi: Pertahankan redirect 301 + HSTS.

F-02 — Validitas & Kekuatan Sertifikat TLS

TERATASI

Tingkat: INFO

Bukti:

```
Issuer: -; berlaku: - s.d. -
```

Dampak: Enkripsi transport tersertifikasi.

Rekomendasi: Pantau masa berlaku & perpanjang sebelum kadaluarsa.

F-03 — Cookie & Session Flags

TERATASI

Tingkat: INFO

Bukti:

```
Cookie:
mastergalery_session=eyJjc3JmX3Rva2VuIjo1YTJlMTA1YzkyMDY3MDRmOTZjZTIyMjliM2NmMWQ3
ZTBhMWZlODkyZCJ9.ameakg.78-QHBaXOM_9ItaSWYlYQSh2Itc -> Secure; HttpOnly;
SameSite=Lax
```

Dampak: Cookie terlindungi dari XSS theft & plaintext leak.

Rekomendasi: Pertahankan konfigurasi SESSION_COOKIE_SECURE=True.

F-04 — Content Security Policy (CSP)

TERATASI

Tingkat: INFO

Bukti:

```
CSP kuat dengan script-src + nonce/self.
```

Dampak: MITIGASI XSS kuat.

Rekomendasi: Pertahankan; tambahkan object-src 'none', base-uri 'self'.

F-05 — Clickjacking Protection (X-Frame-Options)

TERATASI

Tingkat: INFO

Bukti:

```
X-Frame-Options: DENY
```

Dampak: Terlindungi dari clickjacking.

Rekomendasi: Pertahankan; tambahkan CSP frame-ancestors 'none'.

F-06 — MIME Sniffing Protection

TERATASI

Tingkat: INFO

Bukti:

```
X-Content-Type-Options: nosniff
```

Dampak: Mencegah MIME sniffing.

Rekomendasi: Tambahkan header X-Content-Type-Options: nosniff.

F-07 — Referrer Policy

TERATASI

Tingkat: INFO

Bukti:

```
Referrer-Policy: no-referrer
```

Dampak: Mencegah kebocoran URL ke pihak ketiga.

Rekomendasi: Set Referrer-Policy: no-referrer / same-origin.

F-08 — CORS Policy

TERATASI

Tingkat: INFO

Bukti:

```
Tidak ada header CORS (aman default).
```

Dampak: Tidak ada risiko CORS.

Rekomendasi: Tidak ada tindakan.

F-09 — Debug Mode (Werkzeug)

TERATASI

Tingkat: INFO

Bukti:

```
Tidak ada traceback; respons generik (400/404).
```

Dampak: Tidak ada kebocoran stack trace.

Rekomendasi: Pastikan DEBUG=False di produksi.

F-10 — Eksposur Source / File Sensitif

TERATASI

Tingkat: INFO

Bukti:

```
.git/HEAD, .env, phpinfo.php, backup.sql -> 404/403.
```

Dampak: Tidak ada kebocoran source.

Rekomendasi: Tidak ada tindakan.

F-11 — HTTP Methods (TRACE/PUT/DELETE)

TERATASI

Tingkat: INFO

Bukti:

```
Metode berbahaya (405/403).
```

Dampak: Tidak ada metode berbahaya terbuka.

Rekomendasi: Tidak ada tindakan.

F-12 — Header X-XSS-Protection (usang)

MASIH TERBUKA

Tingkat: INFO

Bukti:

```
X-XSS-Protection masih disajikan.
```

Dampak: Header deprecated; pada kasus tertentu justru memperkenalkan XSS sekunder.

Rekomendasi: Hapus (andalkan CSP) atau set '0'.

4. Rekomendasi

No	Prioritas	Aksi	Detail
R-1	LOW	Perbaiki temuan MEDIUM	Terapkan rekomendasi per-finding (CORS, cookie flag, dll).
R-2	LOW	Perketat CSP	CSP berbasis nonce + frame-src 'self' + object-src 'none'.
R-3	INFO	Pertahankan kontrol aman	Lanjutkan HSTS, debug off, install guard, header dasar.
R-4	INFO	Re-test berkala	Ulangi pentest setelah perubahan config/kadaluarsa TLS.

4.1 Contoh Konfigurasi (nginx / origin)

```
# Hapus CORS wildcard bila tidak diperlukan
# add_header Access-Control-Allow-Origin "" always;

# CSP ketat (ganti nonce di runtime)
add_header Content-Security-Policy "default-src 'self'; script-src 'self' 'nonce-%
(nonce)s'; style-src 'self' 'nonce-%(nonce)s'; img-src 'self' data: https;; frame-src
'self'; object-src 'none'; base-uri 'self'; form-action 'self';" always;
add_header X-Frame-Options "DENY" always;
add_header X-XSS-Protection "0" always;
add_header X-Content-Type-Options "nosniff" always;
add_header Referrer-Policy "same-origin" always;
add_header Strict-Transport-Security "max-age=31536000; includeSubDomains" always;
```

5. Kesimpulan & Lampiran

Aplikasi <https://ngflask.pokdartik.or.id> (Python / Flask (indikasi cookie session)) memiliki **11 kontrol TERATASI** dan **1 temuan MASIH TERBUKA**. Postur secara keseluruhan sudah cukup baik; perbaiki temuan terbuka untuk mencapai hardening optimal.

Rekomendasi migrasi: karena CMS terdeteksi **Python / Flask (indikasi cookie session)**, pastikan platform pengganti menargetkan instalasi yang sesungguhnya, dan terapkan hardening (CORS, cookie flag, CSP) sejak awal, lalu pentest ulang.

6. Lampiran A — Bukti Pengujian

ID	Area	Status	Bukti
F-01	Enkripsi Transport (HTTPS wajib / HSTS)	TERATASI	HTTP -> 301 redirect ke HTTPS, tidak ada plaintext body.
F-02	Validitas & Kekuatan Sertifikat TLS	TERATASI	Issuer: -; berlaku: - s.d. -
F-03	Cookie & Session Flags	TERATASI	Cookie: mastergalery_session=eyJjc3JmX3Rva2VuljoiYTJIMTA1Yzk
F-04	Content Security Policy (CSP)	TERATASI	CSP kuat dengan script-src + nonce/self.
F-05	Clickjacking Protection (X-Frame-Options)	TERATASI	X-Frame-Options: DENY
F-06	MIME Sniffing Protection	TERATASI	X-Content-Type-Options: nosniff
F-07	Referrer Policy	TERATASI	Referrer-Policy: no-referrer
F-08	CORS Policy	TERATASI	Tidak ada header CORS (aman default).
F-09	Debug Mode (Werkzeug)	TERATASI	Tidak ada traceback; respons generik (400/404).
F-10	Eksposur Source / File Sensitif	TERATASI	.git/HEAD, .env, phpinfo.php, backup.sql -> 404/403.
F-11	HTTP Methods (TRACE/PUT/DELETE)	TERATASI	Metode berbahaya (405/403).
F-12	Header X-XSS-Protection (usang)	TERBUKA	X-XSS-Protection masih disajikan.