MushroomNepal — External Web Security Assessment

Target: `mushroomnepal.com` / `www.mushroomnepal.com`
Assessment date: 2025-10-15
Tooling: nmap (HTTP/HTTPS NSE scripts), gobuster (enumeration), curl (manual checks) — passive / non-destructive techniques only.
Author: Prayush Hada (testing performed with owner's verbal consent — ensure written scope is retained).

Executive summary

A low-impact external scan of `mushroomnepal.com` found **no immediate critical remote code execution or publicly exploitable SQLi** from surface analysis, but several configuration and hardening issues were detected that raise the site's attack surface and operational risk:

- Missing/inconsistent **security headers** (HSTS, CSP, X-Frame-Options, X-Content-Type-Options).
- A scanner-flagged **Slowloris** DoS detection (likely a false positive on the Vercel platform — verify settings).
- Strange redirect/404 behavior that exposes deployment error messages and odd internal paths.
- Site is hosted on **Vercel** (Cloudflare DNS) — confirm WAF/rate-limit settings.
- Next.js image optimizer returned validation errors (additional details available separately).

Findings summary (copy-ready table)

#	Finding	Evidence (excerpt)	Severity
1	Missing / inconsistent security headers (HSTS, CSP, X-Frame-Options, X-Content-Type-Options)	`http-security-headers: HSTS not configured in HTTPS Server` + `http-headers` lacked CSP/X-Frame/X-Content-Type	**Low → Medium**
2	Slowloris DoS detection (likely false positive)	`http-slowloris-check: VULNERABLE: Slowloris DOS attack` (CVE-2007-6750)	**Medium (report, verify)**
3	Strange redirects / 308 + 404 responses to odd paths	`Location: https:///nice%20ports%2C/Tri%6Eity.txt%2ebak` and `X-Vercel-Error: DEPLOYMENT_NOT_FOUND` in 404 body	**Low → Medium (investigat**
4	Edge/hosting fingerprint + proxy behavior (Vercel, Cloudflare DNS)	`Name Server: lee.ns.cloudflare.com, val.ns.cloudflare.com` + `Server: Vercel` + ASN/netname VERCEL-05	**Info**
5	TLS certificate validity window (short lifetime)	`Not valid before: 2025-09-18 ... Not valid after: 2025-12-17`	**Info**

#	Finding	Evidence (excerpt)	Severity
6	User-agent restrictions & automated scan blocking on HTTP	`http-useragent-tester: Status for browser useragent: 308` and allowed UA list	**Low**

Detailed findings, evidence & remediation

1 — Missing / inconsistent security headers

Severity: Low → Medium
Evidence:

```
http-security-headers: HSTS not configured in HTTPS Server
# http-headers snippet (443)
Cache-Control: private, no-store, max-age=0
Content-Type: text/html; charset=utf-8
Server: Vercel
X-Vercel-Challenge-Token: <redacted>
X-Vercel-Id: <redacted>
X-Vercel-Mitigated: challenge
Date: Wed, 15 Oct 2025 14:07:50 GMT
```

Impact: Missing headers increase risk of protocol downgrade, MIME sniffing, clickjacking and make XSS exploitation easier in some contexts.

Remediation (concrete):

- Add/ensure on all HTTPS responses:

```
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
Content-Security-Policy: default-src 'self'; script-src 'self'
https://trusted.cdn.com; object-src 'none';
```curl -I https://www.mushroomnepal.com
```
```

```
HTTP/2 200
age: 109
cache-control: public, max-age=0, must-revalidate
content-type: text/html; charset=utf-8
date: Wed, 15 Oct 2025 05:24:07 GMT
etag: "10boc5edde833p9"
server: Vercel
strict-transport-security: max-age=63072000
vary: rsc, next-router-state-tree, next-router-prefetch, next-router-
segment-prefetch
x-matched-path: /
x-nextjs-prerender: 1
x-nextjs-stale-time: 300
x-powered-by: Next.js
x-vercel-cache: HIT
x-vercel-id: bom1::iad1::p7bbt-1760544347359-0e6cff7b519a
content-length: 144935
```

- Implement via Vercel headers, a reverse proxy (Cloudflare workers), or application middleware (`helmet` for Node/Express or Next.js headers).
  Verification:
- After deploy, run: `curl -I https://www.mushroomnepal.com` and check for the headers. Re-run the `http-security-headers` nmap script.

---

2 — Slowloris DoS detection (scanner flagged)

Severity: Medium (requires verification)
Evidence:

```
http-slowloris-check: VULNERABLE: Slowloris DOS attack (CVE-2007-6750)
State: LIKELY VULNERABLE
```

Notes: On managed edge platforms like Vercel/Cloudflare this is commonly a false positive because the scanner checks for behavior that older Apache/nginx setups exhibited.
Remediation / Verification steps:

1. Confirm platform limits: verify Vercel/Cloudflare connection/keepalive, maximum concurrent connections, timeouts.
2. If running any origin servers, ensure their keepalive limits and worker timeouts are configured defensively.

3. Enable rate limiting and WAF rules at the edge to block slow/partial requests.
4. If desired, schedule a controlled, low-impact verification test (owner approval required) to confirm whether partial-request behavior can exhaust workers.
   Verification: Monitor server metrics (connections, CPU, response time) while performing a safe simulation in a controlled window.

---

3 — Strange redirects & DEPLOYMENT_NOT_FOUND 404s

Severity: Low → Medium (investigate)
Evidence: redirect map and 404 text:

```
Location: https:///nice%20ports%2C/Tri%6Eity.txt%2ebak
X-Vercel-Error: DEPLOYMENT_NOT_FOUND
```

Proof of Concept (PoC)

Below is an abbreviated, sanitized excerpt of the nmap HTTP/HTTPS script output demonstrating the findings. (Full raw output is stored in the private appendix.)

```
# Port 80 (HTTP) - redirect to HTTPS
80/tcp  open  http  Vercel
  Content-Type: text/plain
  Location: https://mushroomnepal.com/
  Refresh: 0;url=https://mushroomnepal.com/
  server: Vercel

# Port 443 (HTTPS)
443/tcp open  ssl/http Golang net/http server
  http-slowloris-check: VULNERABLE: Slowloris DOS attack (CVE-2007-6750)
  ssl-cert: Subject CN=mushroomnepal.com (valid 2025-09-18 → 2025-12-17)
  http-security-headers:
    Strict_Transport_Security:
      HSTS not configured in HTTPS Server
  http-headers:
    Cache-Control: private, no-store, max-age=0
    Content-Type: text/html; charset=utf-8
    Server: Vercel
```

```
    X-Vercel-Mitigated: challenge
    X-Vercel-Id: bom1::...
    X-Vercel-Challenge-Token: <redacted>
  FourOhFourRequest:
    Strict-Transport-Security: max-age=63072000
    X-Vercel-Error: DEPLOYMENT_NOT_FOUND
```

Suggested next actions :

1. Implement the headers (HSTS, X-Content-Type-Options, X-Frame-Options) this week.