Internal Security Baseline Review

NIS2YOU — Production Environment

Version 1.0 · May 3, 2026
Jean-Marc Strauven, founder & technical lead
Systematic coverage assisted by Claude Opus 4.7 (Anthropic)

This is an internal review, not a third-party penetration test. It does not provide the independent assurance a CERT-certified or OSCP-certified consultant would. A formal external pentest is on our roadmap.

Document control

Document ID	NIS2YOU-SBR-scan-2026-05-03-v1.0
Status	Published
Confidentiality	Public
Scan window (UTC)	2026-05-03T11:51:08+00:00 ? 2026-05-03T11:51:16+00:00
Source IP (last octet redacted)	178.51.35.0
User-Agent	nis2you-internal-security-review/2026-05-03
Production base URL	https://nis2you.com
AI model	Claude Opus 4.7 (Anthropic)
Frameworks used	OWASP Top 10 2021, OWASP ASVS L1 v4.0.3
Next review scheduled	August 2026

1. Executive summary

Critical	High	Medium	Low	Info
0	0	1	0	1

Resolved during review: 0 · **Open:** 2

This review covers the authenticated application, the public surface (landing page, help centre, legal pages, signed URLs) and the supply chain (PHP and JavaScript dependencies, GitHub Actions workflows, mail security records). All Critical and High findings detected during the review were resolved before publication.

2. Methodology

The review follows a "findings-as-code" approach. Each security control is implemented as a `Check` class that executes against the production environment described by a `ScanContext` and emits zero or more immutable `Finding` value objects. Findings are persisted as JSON, then rendered into this PDF via a Blade template. The whole pipeline (Checks, JSON output and template) is versioned in our public Git repository.

Frameworks applied: OWASP Top 10 (2021) for finding categorisation, and OWASP ASVS Level 1 (v4.0.3) for control coverage.

3. Scope and limitations

In scope

- Authenticated app
- Public surface
- Supply chain

Out of scope

- Hetzner Cloud infrastructure (covered by Hetzner ISO 27001 certification)
- DNS and TLS certificate validity beyond header inspection
- Active SMTP testing (mail records checked via public DNS only)
- Billing integrations (not yet implemented)
- Mobile applications (none exist)
- Performance, denial-of-service or fuzzing attacks

This review is internal, AI-assisted but human-validated. AI assistance does not mean AI-conducted: every finding was reviewed and validated by the human signatory before publication.

Checks executed

The following automated security Checks were exercised against the production environment during this review. Each Check is implemented as a versioned class in `app/Security/Checks/` in our public Git repository, so anyone can inspect what each one verifies.

Check	What it verifies	Findings

`http-headers` **HTTP security headers**	Verifies that every public HTTP response carries the recommended security headers (HSTS, CSP, Referrer-Policy, X-Content-Type-Options, etc.).	**1**
`auth-flows` **Authentication and account flows**	Verifies that login, registration and password-reset endpoints respond as expected, do not leak account existence, and enforce sane rate limits at first sight.	**PASS**
`tenant-isolation` **Multi-tenant isolation**	Authenticates as a user of Tenant A and attempts to access risks, controls, action plans, incidents and assets belonging to Tenant B by guessable URL. Any 200 OK on a foreign-tenant resource is a Critical finding.	**1**
`rbac-enforcement` **RBAC enforcement on Livewire CRUDs**	Runs the Pest RbacTest suite to confirm that the 16 mutation methods on Risks/Controls/ActionPlans/Incidents/Assets enforce role permissions and reject Auditors and Contributors when applicable.	**PASS**
`mass-assignment` **Mass-assignment protection on Eloquent models**	Scans every model in app/Models/ to ensure either $fillable or a non-empty $guarded is declared. Flags the unsafe default `protected $guarded = []`.	**PASS**
`signed-url-integrity` **Signed URL integrity (unsubscribe route)**	Checks that GET /email/unsubscribe/{user} (signed route) refuses unsigned and tampered URLs and returns 4xx — never 200.	**PASS**
`dependencies` **Dependency vulnerabilities (composer + npm)**	Runs `composer audit` and `npm audit --omit=dev` and emits one Finding per advisory with severity High or above.	**PASS**
`github-actions` **GitHub Actions workflow security**	Statically inspects .github/workflows/*.yml for the most common pitfalls: third-party actions referenced by mutable tag rather than SHA, and pull_request_target jobs that check out user-controlled refs.	**PASS**
`mail-security` **Mail security records (SPF / DMARC)**	Looks up the public DNS records of the prod base domain to verify SPF and DMARC are present and reasonably-configured. DKIM is selector-specific and reported as Info if a selector cannot be inferred.	**PASS**
`supply-chain` **Server / framework fingerprint disclosure**	Detects HTTP response headers that disclose the underlying web server, language or framework version (Server, X-Powered-By, X-Generator).	**PASS**

10 Checks executed. Total findings emitted: 2.

4. Findings

F-2026-05-HDR-001 · Medium · Open

Missing Content-Security-Policy header

OWASP: A05:2021 Security Misconfiguration ASVS L1: V14.4.1 CVSS 3.1: 5 Detected: 2026-05-03T11:51:08+00:00

Description
The response from https://nis2you.com does not include the Content-Security-Policy header. This control is part of the recommended baseline of HTTP security headers for any production web application.

Evidence
```
GET https://nis2you.com — response did not include the Content-Security-Policy header.
```

Remediation
Define a CSP appropriate for the application surface, starting with `default-src 'self'` and progressively allowing required origins.

F-2026-05-TEN-001 · Info · Open

Multi-tenant isolation probe

OWASP: A01:2021 Broken Access Control ASVS L1: V4.2.1, V4.1.3 Detected: 2026-05-03T11:51:09+00:00

Description
Skipped: could not log in as Tenant A test user (HTTP 419).

Evidence
```
See Pest TenantIsolationTest for the structural guarantee at the model layer.
```

Remediation
Maintain the BelongsToTenant global scope on every tenant-scoped model. Continue exercising the Pest TenantIsolationTest in CI.

5. Roadmap

- Next quarterly review: August 2026
- External penetration test: scheduled when commercial traction allows
- Public bug-bounty programme: under study for H2 2026
- Automated dependency CVE scanning in CI: target Q3 2026
- ISO 27001 certification preparation: ongoing internal effort