Web Application Security

An IXP Manager Perspective

Barry O'Donovan

RIPE 92, Edinburgh, Scotland, May 2026

inex

Interconnecting networks
and people since 1996

Why Web Application Security?

The threat model has changed

- **Now your web portal controls your infrastructure**
  - Route server configs, member data, automated provisioning
- **The attack surface has grown**
  - Public web apps, APIs, member self-service, ***and staff***
- **More than "just" a defaced webpage**
  - Path to production systems
  - NIS2 raise the bar and regulatory attention

Web Application Security Fundamentals

- Broken Access Control
- Security Misconfiguration
- Software Supply Chain Failures
- Cryptographic Failures
- Injection
- Insecure Design
- Authentication Failures
- Software or Data Integrity Failures
- Security Logging and Alerting Failures
- Mishandling of Exceptional Conditions

OWASP includes details on how to prevent and examples – essential reading.

- https://owasp.org/Top10/2025/

IXP Manager

IXP Manager

- Free & Open-Source Software Platform for IXPs
  - https://www.ixpmanager.org/
- Teaches and implements best practice
- Mature – created pre-2005, open-sourced 2010

IXP Manager – Community Statistics

14,299	493 Tbps	20,869
Connected Networks	Connected Capacity	Connected Ports

There are at least 262 IXPs Powering Peering using IXP Manager around the world to connect 14,299 networks of which 8,020 are unique. The edge peering capacity of these networks is 493 Tbps over 20,869 connected ports. We aggregate traffic statistics from 154 IXP Manager platforms which show us that the peak traffic exchanged is 114.94 Tbps.

The Challenge of Legacy

- **20 years of accumulated decisions**
  - Past assumptions need regular revisiting. Acceptable 2010; risk in 2026.
  - Technical debt compounds
- **Rewriting isn't realistic**
  - Incremental improvements while keeping production running
- **Framework upgrades are hard**
  - PHP, Laravel, and dependencies must move together
- **Success raises the stakes**
  - 262+ IXPs means higher security expectations

The Challenge of Legacy

2005 - PHP4/Pear/Perl

2007 - ZF1/Doctrine ORM1/Smarty

2012 – ZF1/Doctrine ORM2/Smary

2015-9 - Laravel, Doctrine, Foil

2021 – Laravel, Foil

The Challenge of Legacy – Layer defences

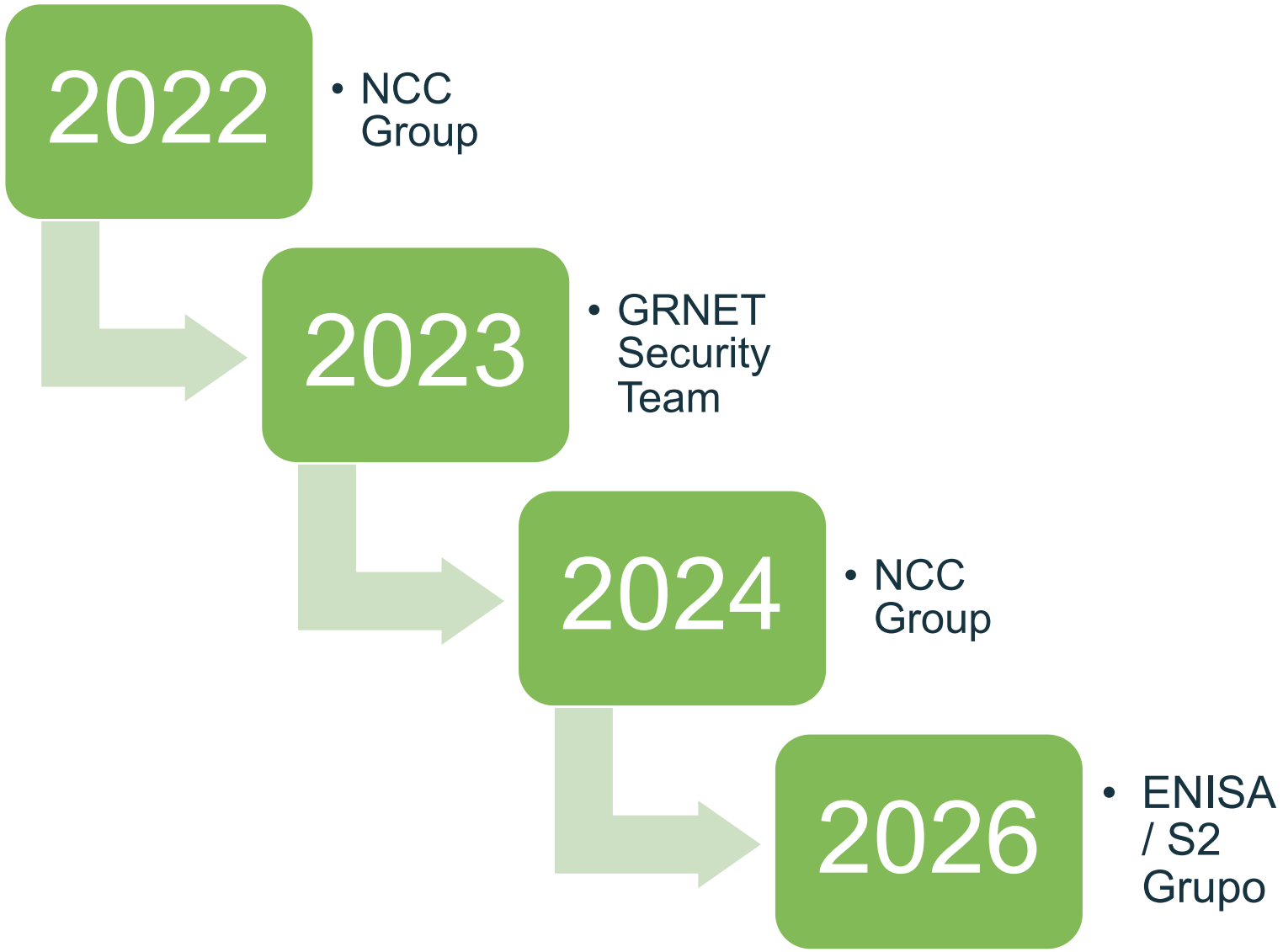
- CI pipeline with static code analysis and unit testing
- Supply chain security via dependency scanning
- Penetration testing
- ISMS: Secure Application Development Policy
- GitHub: 2fa enforced, branch protection, secret scanning

We're not claiming perfection.

We are committed to continuous improvement.

Independent Security Assessments

Web Application Pen Tests of IXP Manager



Pen Test: 2022 NCC Group

v6.3.0 - Security hardening, with various improvements …

Mostly “was grand in the past, not now” issues

Some XSS issues
User enumeration via forgotten password
Enforce a (stronger) password policy
Disable phpinfo() by default

Pen Test: 2023 GRNET

v6.3.1 - XSS Security Fixes, Small Bug Fixes …

Five XSS issues

4 required admin access

1 potentially non-admin user, no PoC

Pen Test: 2024 NCC Group

Mostly advisory / “by design” – some under review

DocStore - uploaded file types not restricted – only admins can upload files.

A couple implementation specific issues – advice provided

2026 ENISA Penetration Test

ENISA Cybersecurity Support Action

- **ENISA** - European Union Agency for Cybersecurity
- 2022 - Cybersecurity Support Action Programme
  - Support Member States reinforce their preparedness (ex-ante), and response (ex-post) capabilities.
- Ireland's NCSC oversaw this program in Ireland
- Invited DigiCORE members to submit applications
- INEX submitted IXP Manager for the web application penetration test service

Beneficiaries

- INEX
- ~60 EU IXPs
- >260 worldwide

The Assessment

- **Seven-day web application pen test**
  - Conducted in February 2026 on v7.0.1
  - Grey-box methodology
  - Combination of AI and human

- Performed by independent professionals
  - S2 Grupo

Results & Remediation

- **3 medium-risk, 1 low-risk vulnerability [CVSS]**
  - Unsecured input – Persistent Cross-Site Scripting (XSS) [6.7]
  - Lack of Headers – X-Frame-Options and CSP [5.3]
  - User Enumeration via Differentiated HTTP Responses [5.3]
  - Information Disclosure – Error messages [2.7]

- **Most issues have been addressed in v7.2**
  - Content Security Policy requires research

[VULN-02] Lack of Headers: X-Frame-Options and Content Security Policy

The X-Frame-Options header allowed specifying whether a frame or iframe was permitted to embed the web content. Websites could use it to prevent clickjacking attacks by ensuring their content was not embedded in other sites.

```
<Directory /srv/ixpmanager/public>
    Header Set X-Frame-Options "DENY"
```

Post Penetration Test Work

V7.1: Securing Administrative Functions

- Publicly accessible by design
  - Creates unique security challenges
  - Probably not feasible in the medium term?

- V7.1 introduced a /admin prefix for admin-only functions.
  - Protect access to at the web server level
  - Reduces the potential attack surface by 72%

Only useful if you implement this!

V7.2: Additional Security Fixes

- ENISA’s work inspired our new developer (Thomas Kerin)
  - Developed an innovative XSS catcher
  - Concentrated on XSS execution rather than injection
  - Updated many templates
  - No known PoCs/exploits

- URL building via string concatenation replaced
  - Laravel's URL builder ensures variable input is sanitised.

Key Takeaways

- **Web application security is everyone's responsibility**
  - Whether you use IXP Manager or your own system
- **Invest in independent security assessments**
  - EU programmes like ENISA's can help fund this
- **Adopt a secure development lifecycle**
  - ISMS, OWASP, CI, responsible disclosure, supply chain security
- **Keep frameworks and dependencies current**
- **Upgrade to IXP Manager v7.2**

Our Sponsors

APNIC FOUNDATION

GOLD

BCIX

Berlin Commercial Internet Exchange

NIX NORWEGIAN INTERNET EXCHANGE

SILVER

ZA INX

LONAP

BRONZE

InterLAN·IX

GRIX

SLIX

Thank you.

Interconnecting networks
and people since 1996