



WP FUTURE
CONCLAVE 2026
KOZHIKODE

September 5, 2026

Kerala Govt. CyberPark Auditorium - Kozhikode

Nestor Angulo de Ugarte

We Built an AI That Finds Vulnerabilities in Plugins. So Can Everyone Else.

OR

WordPress security
when discovery stops being the bottleneck



WP FUTURE
CONCLAVE 2026
KOZHIKODE



Nestor Angulo

CISSP

Head of Technology
@ ISC2 Spain Chapter

Who's talking

- Former Head of Security @ **Patchstack**.
- 8 years @ **Sucuri** / **GoDaddy** cleaning hacked sites and hunting card skimmers.
- CISSP.
- Computer Science Engineer.
- Board member, **ISC2 Spain Chapter**.
- WordCamp speaker since 2018.

nestorangulo.pro

linkedin.com/in/pharar



WP FUTURE
CONCLAVE 2026
KOZHIKODE

01

The old question

"Is my plugin/site secure?"



WP FUTURE
CONCLAVE 2026
KOZHIKODE

Finding bugs was the hard part

Slow

Someone reads the code. Line by line.

Rare

Few people can do it well. Fewer do it for free.

Silent

Most plugins were never looked at. Ever.

**Security by obscurity was never a strategy.
It was just the default.**



WP FUTURE
CONCLAVE 2026
KOZHIKODE

02

The field report

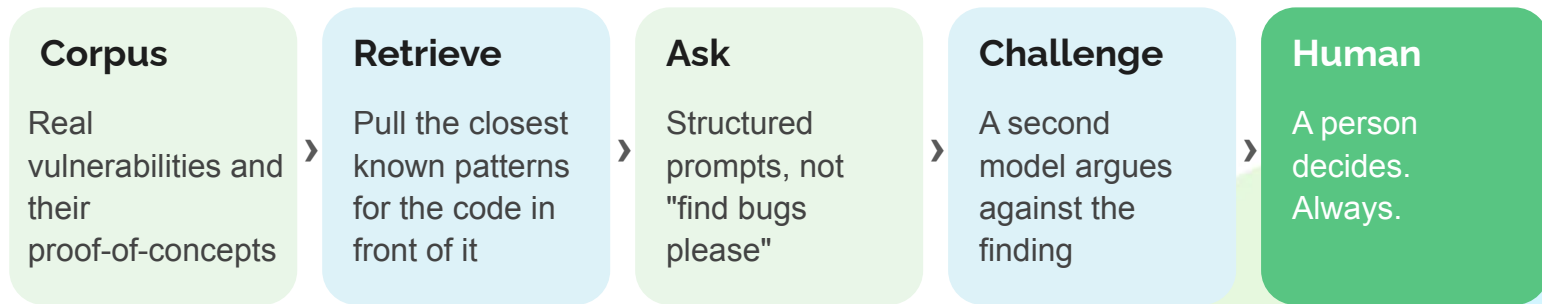
What we built, what worked,
what it got wrong



WP FUTURE
CONCLAVE 2026
KOZHIKODE

The idea, in one line

Teach a system what real vulnerabilities look like, then let it look everywhere.



WP FUTURE
CONCLAVE 2026
KOZHIKODE

What worked

Variants

One known bug became a search across thousands of plugins.

Speed

Triage that took a day took an hour. Reviewers looked at candidates, not haystacks.

Cheap

Commodity parts. No research lab. No big budget.

The same bug, copy-pasted into fifty plugins, stopped hiding.



WP FUTURE
CONCLAVE 2026
KOZHIKODE

What it got wrong

It only finds what it already knows

Variants of known bugs, yes.
Something new, no.

Confidence is not correctness

Beautifully argued findings that
were simply false.

The work moved, it did not vanish

Less reading code, more verifying
claims.

**Human-in-the-loop is a design, not a
disclaimer**

Remove the human and the
output is a liability.



WP FUTURE
CONCLAVE 2026
KOZHIKODE

So can everyone else

An LLM API

A vector
database

Public
vuln data

Public PoCs

A few
weeks

Nothing on this list is secret.
Nothing on this list is expensive.
Nothing on this list checks who is
asking.



WP FUTURE
CONCLAVE 2026
KOZHIKODE

03

The consequence

When discovery gets cheap,
volume follows



WP FUTURE
CONCLAVE 2026
KOZHIKODE

One year

7,966

CVEs disclosed in 2024 for the WordPress ecosystem

Before AI-assisted discovery went mainstream.



WP FUTURE
CONCLAVE 2026
KOZHIKODE

One year

11,334 (42% increase YoY)

CVEs disclosed in 2025 for the WordPress ecosystem

Highly exploitable vulnerabilities increased 113% YoY

patchstack

By risk: Low Medium High



Discovery is no longer the bottleneck.

Response is.

- Someone will find something in your code.
- Probably not you. Possibly not a friend.
- The only variable left is what happens next.



WP FUTURE
CONCLAVE 2026
KOZHIKODE

04

The new question

"When someone finds something,
how fast do I know, decide and ship?"



WP FUTURE
CONCLAVE 2026
KOZHIKODE

Three clocks

1

Know

From "bug exists" to
"I have been told".
Hours, or years?

2

Decide

From "I have been
told" to "I know what
to do". Who calls it?

3

Ship

From "fix exists" to
"every site has it".
Days, or never?

**Your security posture is the
slowest of the three.**



WP FUTURE
CONCLAVE 2026
KOZHIKODE

05

The short list

Five practices that make the clocks run



WP FUTURE
CONCLAVE 2026
KOZHIKODE

1 · Know what you ship

If you cannot list what is inside your plugin,
you cannot know when it breaks.

Clock: KNOW

Terminology

SBOM = Software Bill of Materials (the artifact)

SCA = Software Composition Analysis (the activity)



WP FUTURE
CONCLAVE 2026
KOZHIKODE

2 · Give people a way to tell you

A researcher with a finding and no door will use a window.

Clock: KNOW

First-hand

The findings that hurt most were never the worst bugs. They were the ones reported to a contact form nobody read, then published anyway three months later.



WP FUTURE
CONCLAVE 2026
KOZHIKODE

3 · Watch what you depend on

Most of your vulnerabilities will be published under somebody else's name.

Clock: KNOW

First-hand

A large share of plugin advisories we processed traced back to a shared library or a copied snippet. The plugin author usually found out from us, not from the upstream.



WP FUTURE
CONCLAVE 2026
KOZHIKODE

4 · Say how long you will support it

An abandoned plugin with 50,000 installs is a vulnerability with a countdown.

Clock: DECIDE

First-hand

Many of the "critical, unpatched" advisories we published had the same root cause: the author had moved on years ago and never said so. The bug was not the failure. The silence was.



WP FUTURE
CONCLAVE 2026
KOZHIKODE

5 · Ship fixes to everyone, fast

A patch nobody installs is a blog post.

Clock: SHIP

First-hand

Sites I cleaned at Sucuri were routinely running plugin versions patched a year earlier. The fix existed. It never arrived. From the attacker's side, that is the same as no fix.



WP FUTURE
CONCLAVE 2026
KOZHIKODE

06

Why this stops being optional

Someone got tired of asking nicely



WP FUTURE
CONCLAVE 2026
KOZHIKODE

Six days from today

11 September 2026

EU Cyber Resilience Act, Article 14:

reporting obligations start to ENISA and the national CSIRT.

24h

early warning

72h

full notification

1m

final report

Severe incidents

14d

final report
after a fix

Actively exploited vulns



WP FUTURE
CONCLAVE 2026
KOZHIKODE

Who is in scope?

Probably out

- A free plugin on WordPress.org
- No paid tier, no paying customers
- Contributing code you do not own

Probably in

- A freemium or premium plugin
- A theme or SaaS sold to EU customers
- An agency shipping products to Europe

Disclaimer: *"Probably" is doing real work in this slide. Check with someone who reads law for a living.*



WP FUTURE
CONCLAVE 2026
KOZHIKODE

It travels by contract, not by law

**GDPR
2018**



**Every vendor
with EU clients**



**DPDP Act
2023**

Your European customers will ask for an ingredient list and a disclosure policy long before your parliament does.



**WP FUTURE
CONCLAVE 2026**
KOZHIKODE

07

Monday

Three things that fit in one morning



WP FUTURE
CONCLAVE 2026
KOZHIKODE

Monday morning

1

Write down what you ship

One file. Every third-party thing, with a version.

2

Publish a door

SECURITY.md, security.txt, an inbox a human reads.

3

Time your last fix

Report received to update shipped. Write the number down.

**None of these needs a budget.
All of them need a decision.**



**WP FUTURE
CONCLAVE 2026
KOZHIKODE**

If you remember three things...

1. Discovery is cheap now. Response is the product.
2. Know what you ship. Have a door. Keep a clock.
3. The regulation is not the point. It is proof someone stopped asking nicely.



WP FUTURE
CONCLAVE 2026
KOZHIKODE

Let's get in Touch!

Nestor Angulo de Ugarte

✉ **Email**
nestor@nestorangulo.pro

🌐 **Web**
nestorangulo.pro

🌐 **LinkedIn**
linkedin.com/in/pharar



Thank You



Questions?