War on WordPress

How bots wage war and
what we can do about it.

Lisa-Marie Karvonen
39/f/Finland

WP-Ensure Oy

Bad Actors & Bots

Why they do what they do.

1. Stealing data to sell or spam.
2. Political or personal agenda.
3. Because they can.

Nicholas Cage is awesome. Just not in all roles.
Happy to discuss it with you.

Case 1: Political Agenda

Trying to bring a site down.

- VPN through Poland.
- Passing Cloudflare bot tests.
- Testing vulnerable plugins.
- xmlrpc.php
- API endpoints.

This person is taking down the site through HTML <img>. Amazing skills :D

Securing Our Sites

DNS Level

Stopping them before they reach our servers.

1. Clean up DNS records.
2. Remove old installations.
3. SPF and DKIM setup.
4. Good DDoS protection.
5. Easy way to monitor traffic and block.

Server Level

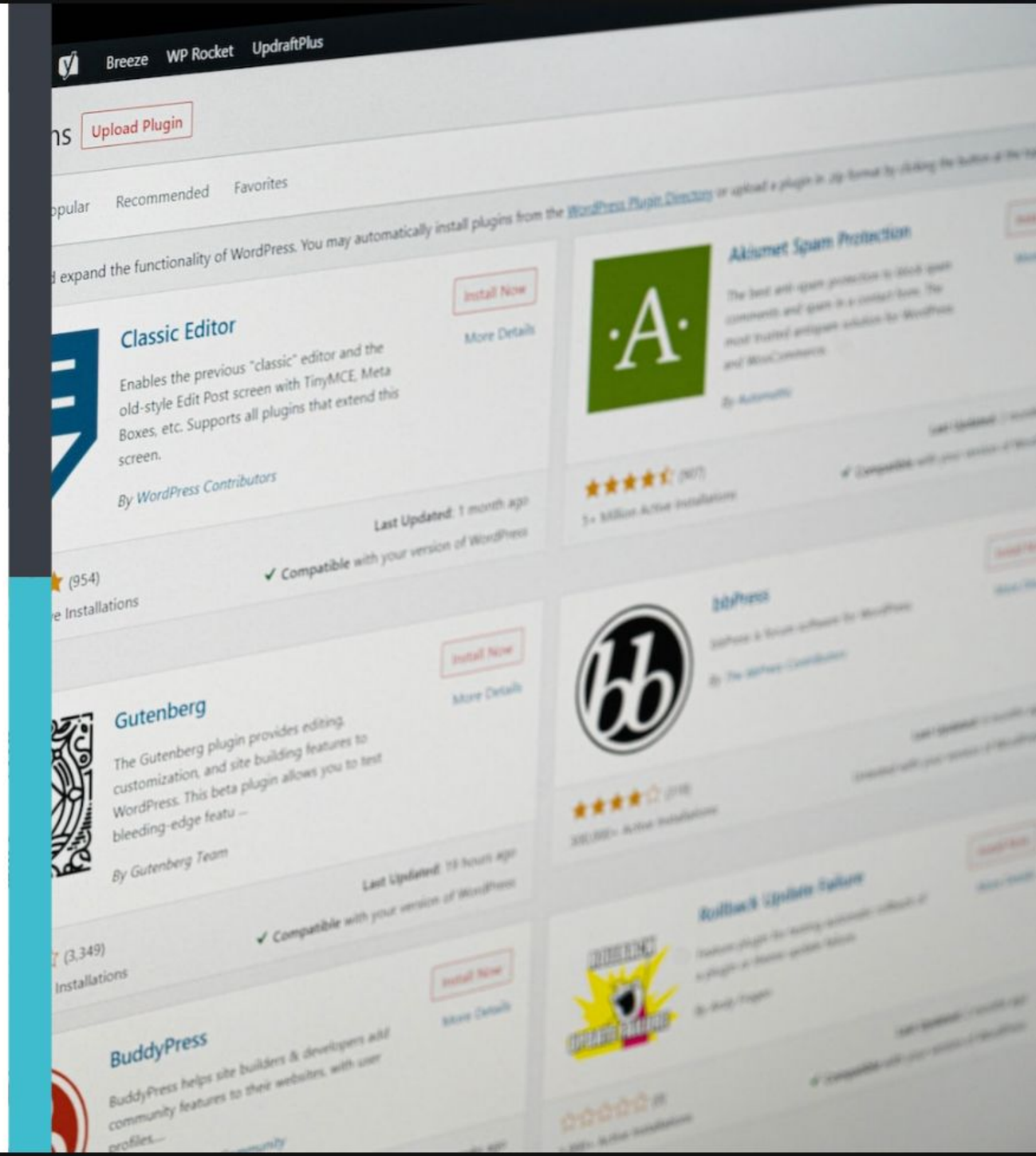
Protecting our server.

1. Security patches installed.
2. Closed ports by default.
3. Fail2ban and other server level protection.
4. No tools like phpMyAdmin installed permanently.

WP Level

Securing our installations.

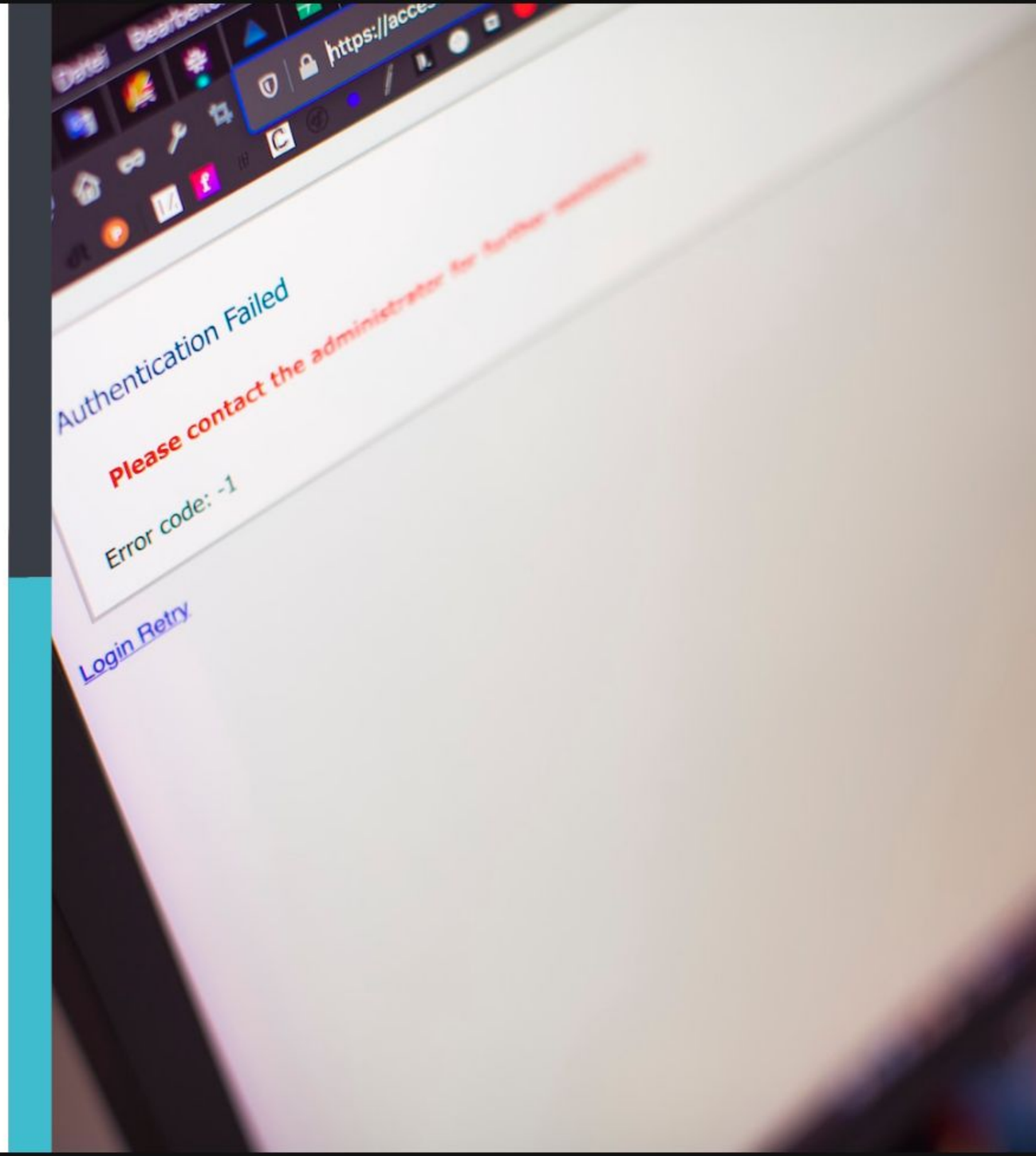
1. Core, plugins and themes kept up to date.
2. Minimize surface attack area (KISS).
3. Custom coded themes with minimal dependencies.
4. Basic pen testing of any endpoints looking for data leakage, new holes.



Case 2: Bad Coding

The bots will find it... eventually.

- Demo code, live to show customer.
- Security through obscurity doesn't work.
- Data stolen, phishing emails sent.



WP Level

Security Plugins & Hardening

1. Login protection, 2FA, usernames and passwords to a good standard. Block unrecognized usernames.
2. Minimize data leakage, WP version, author pages, check sitemaps and endpoints.
3. WAF plugin installation.
4. Avoid free plugins that collect user data. They are getting paid somehow.

GDPR

Not just a headache.

Everyone has a right to privacy.

Thank You!

Contact Info:
Lisa-Marie Karvonen
lisa@wpensure.com
https://wpensure.com

Find me on LinkedIn.

Additional images from Unsplash.