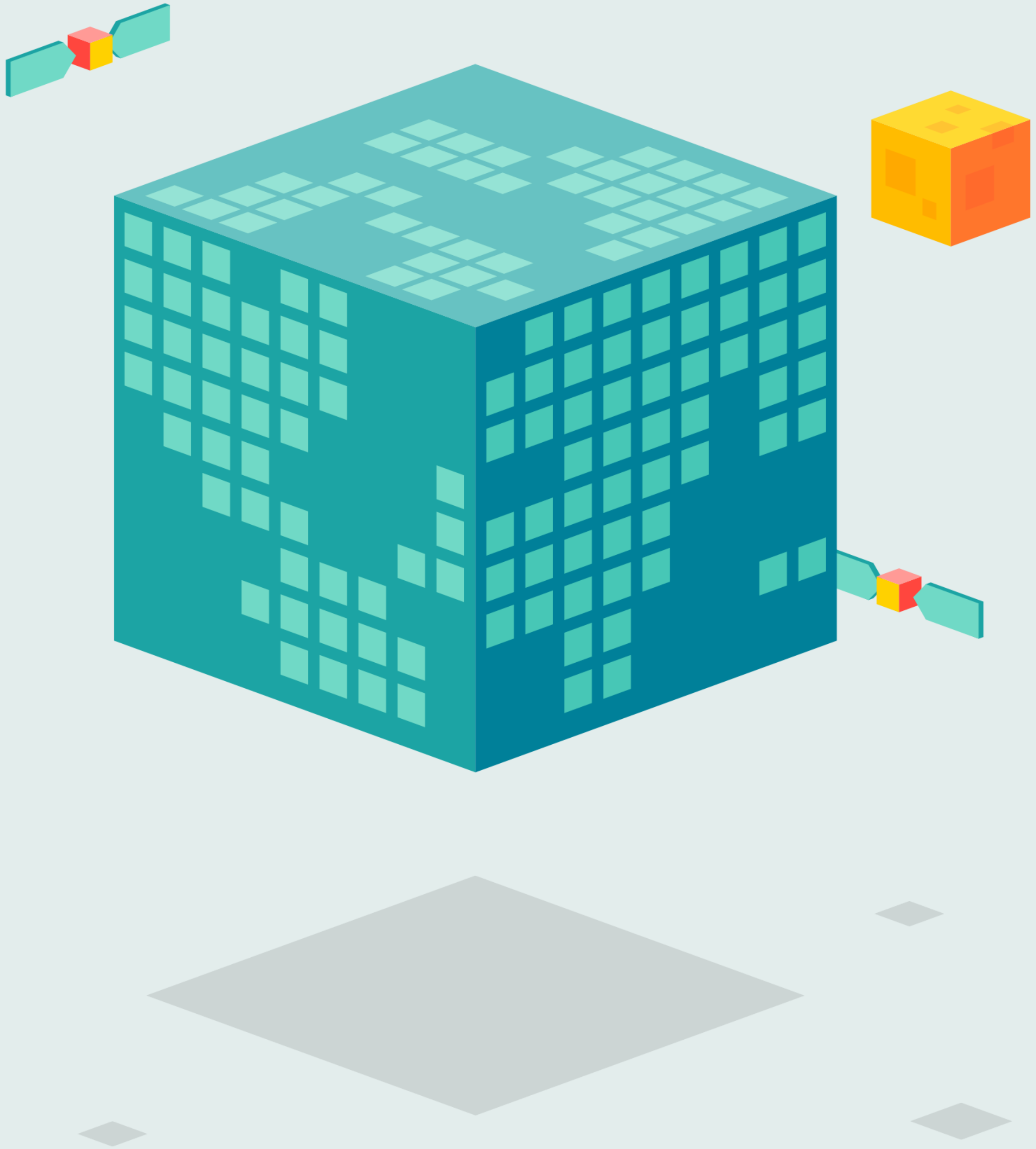
ATTACKING WORDPRESS

LOOKING BACK



Presentator
Eddie Bijnen
Security Engineer

TRUE

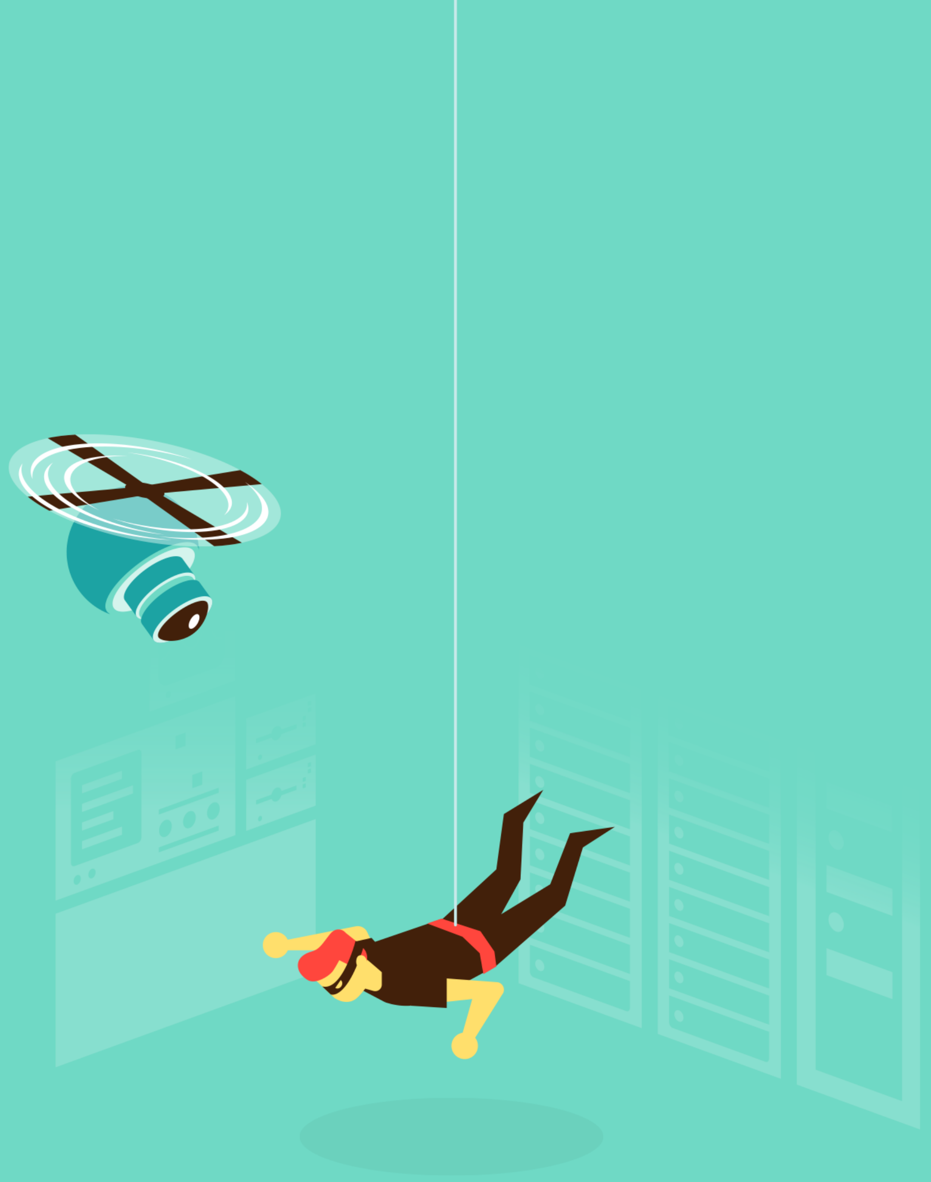
Security engineer¿?!!

→ Penetratie testen

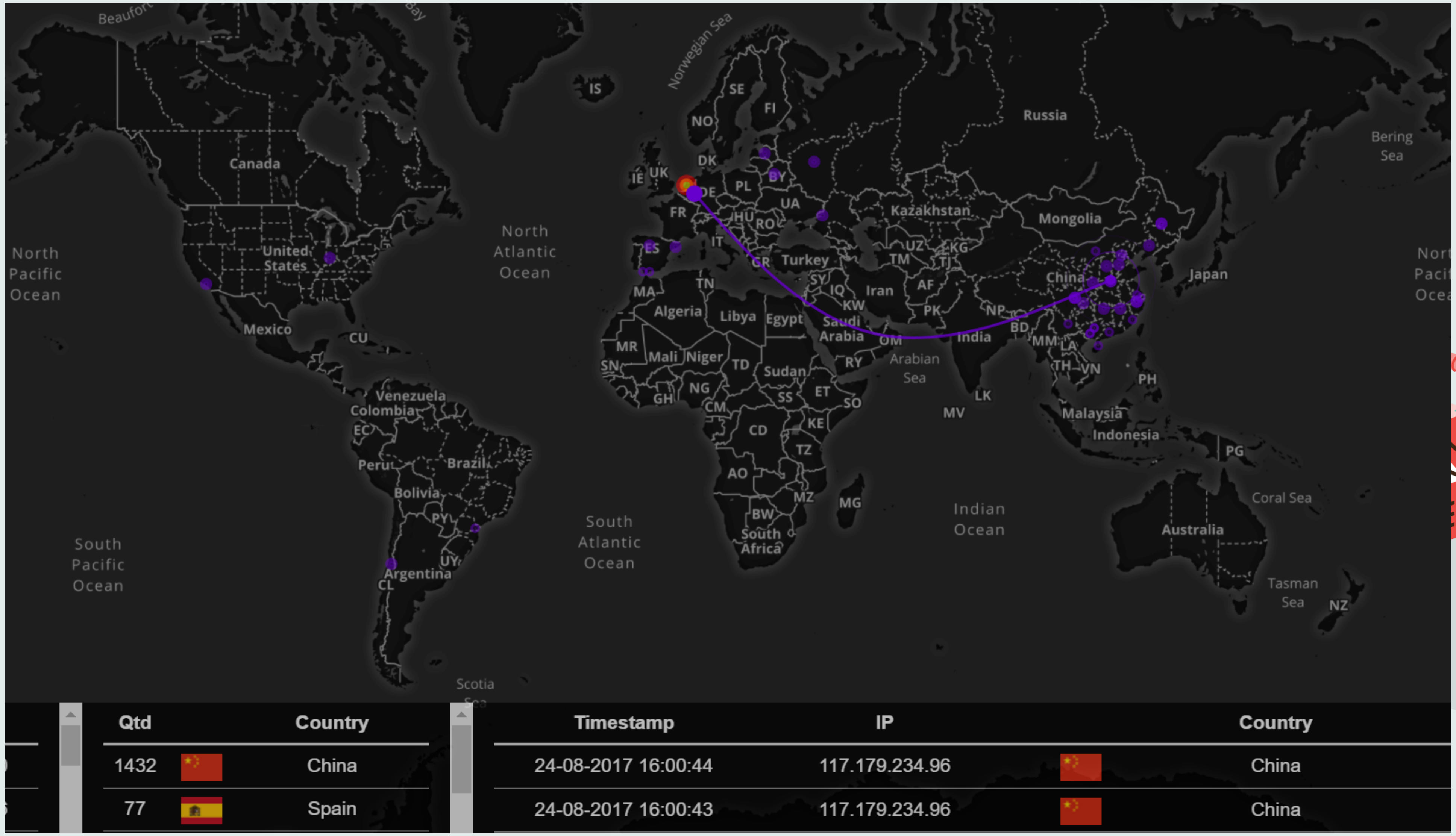
→ Ontwikkelen van security oplossingen

→ Opsporen van hacks

→ Abuse meldingen



My website isn’t that interesting



Qtd		Country
1432	🟥	China
77	🟥	Spain

Timestamp	IP		Country
24-08-2017 16:00:44	117.179.234.96	🟥	China
24-08-2017 16:00:43	117.179.234.96	🟥	China

My website isn’t that interesting

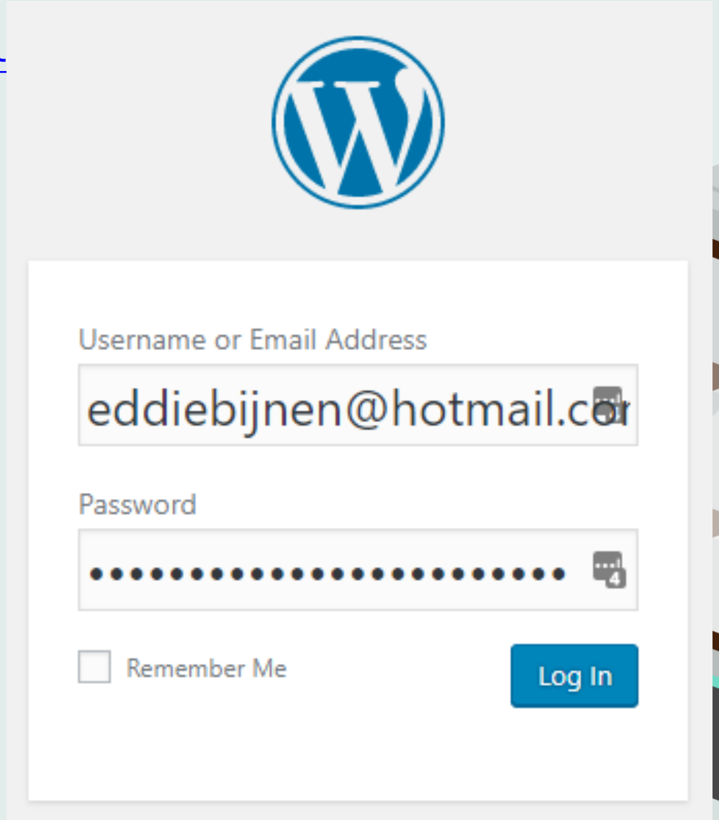
- → DDoS
- → Cryptocoin-mining
- → Spam
- → Randsom

Admin Panel Available

→ https://www.my-website.nl/wp-login.php

→ Unlimited login attempts

→ Lack of HTTPS



Username or Email Address

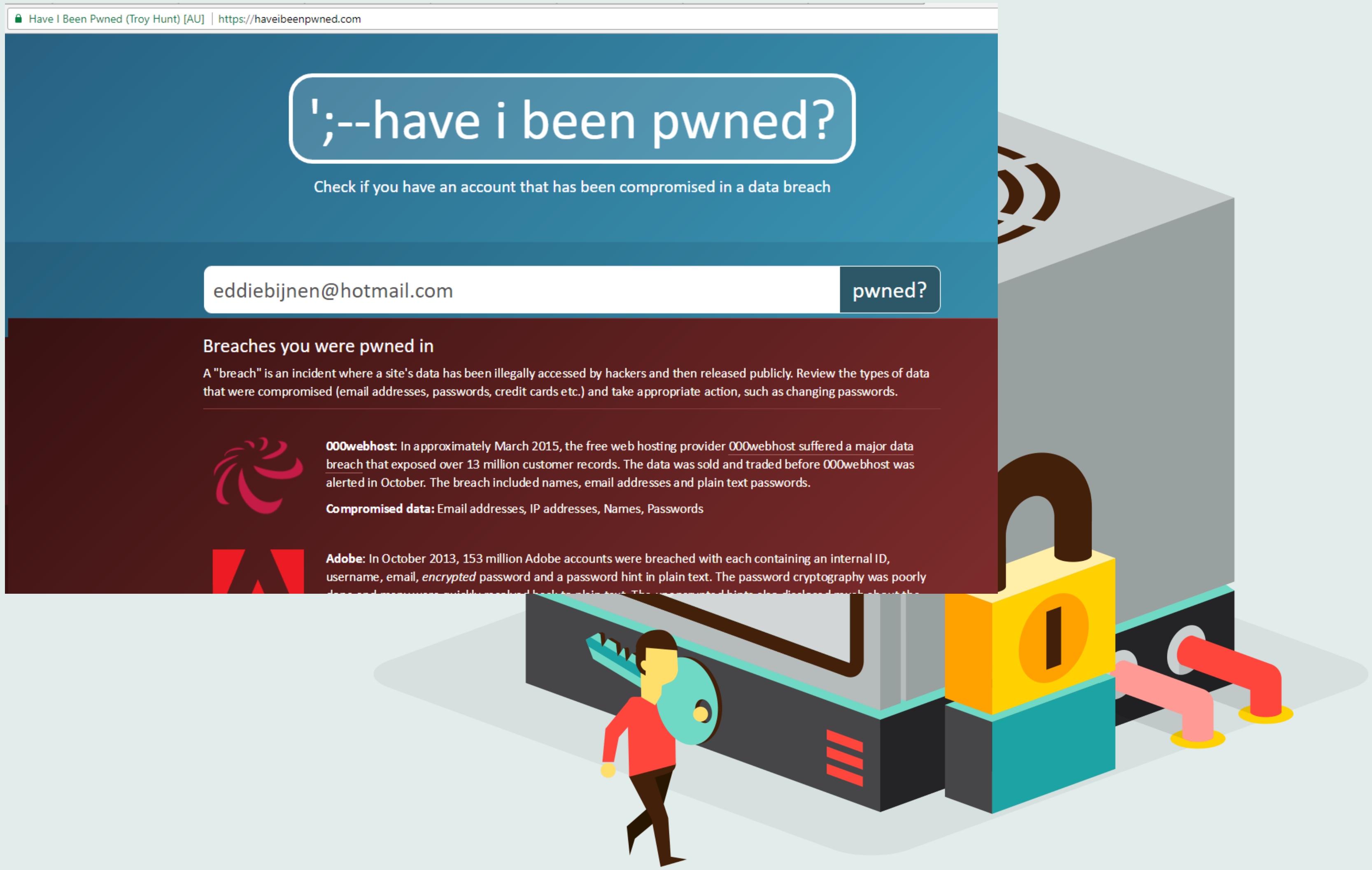
eddiebijnen@hotmail.co

Password

••••••••••••••••••••••••

Password Reuse

- → Myspace
- → Linked-In
- → Adobe
- → Dropbox
- → 220+ andere websites



Have I Been Pwned (Troy Hunt) [AU] | https://haveibeenpwned.com

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

eddiebijnen@hotmail.com

Breaches you were pwned in

A "breach" is an incident where a site's data has been illegally accessed by hackers and then released publicly. Review the types of data that were compromised (email addresses, passwords, credit cards etc.) and take appropriate action, such as changing passwords.

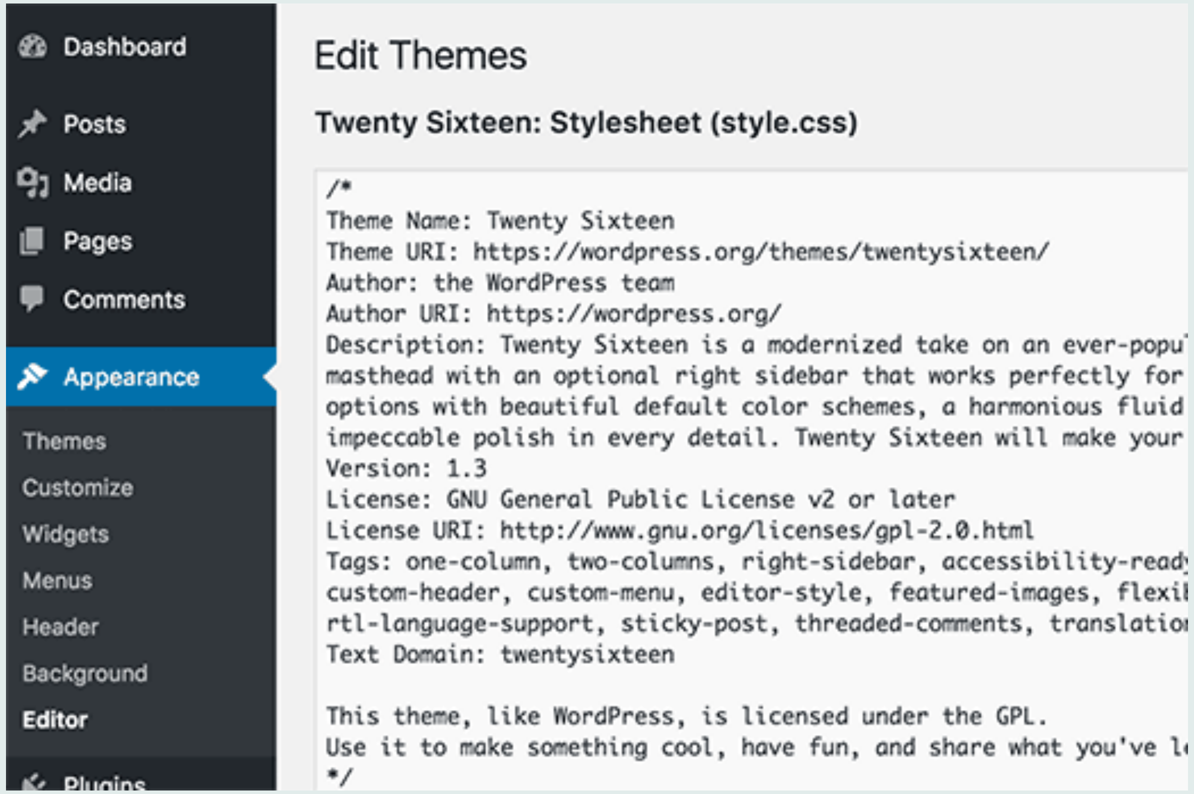
000webhost: In approximately March 2015, the free web hosting provider 000webhost suffered a major data breach that exposed over 13 million customer records. The data was sold and traded before 000webhost was alerted in October. The breach included names, email addresses and plain text passwords.

Compromised data: Email addresses, IP addresses, Names, Passwords

Adobe: In October 2013, 153 million Adobe accounts were breached with each containing an internal ID, username, email, *encrypted* password and a password hint in plain text. The password cryptography was poorly

Am In Now What?

- → A valid admin is by default allowed to change files on disk.

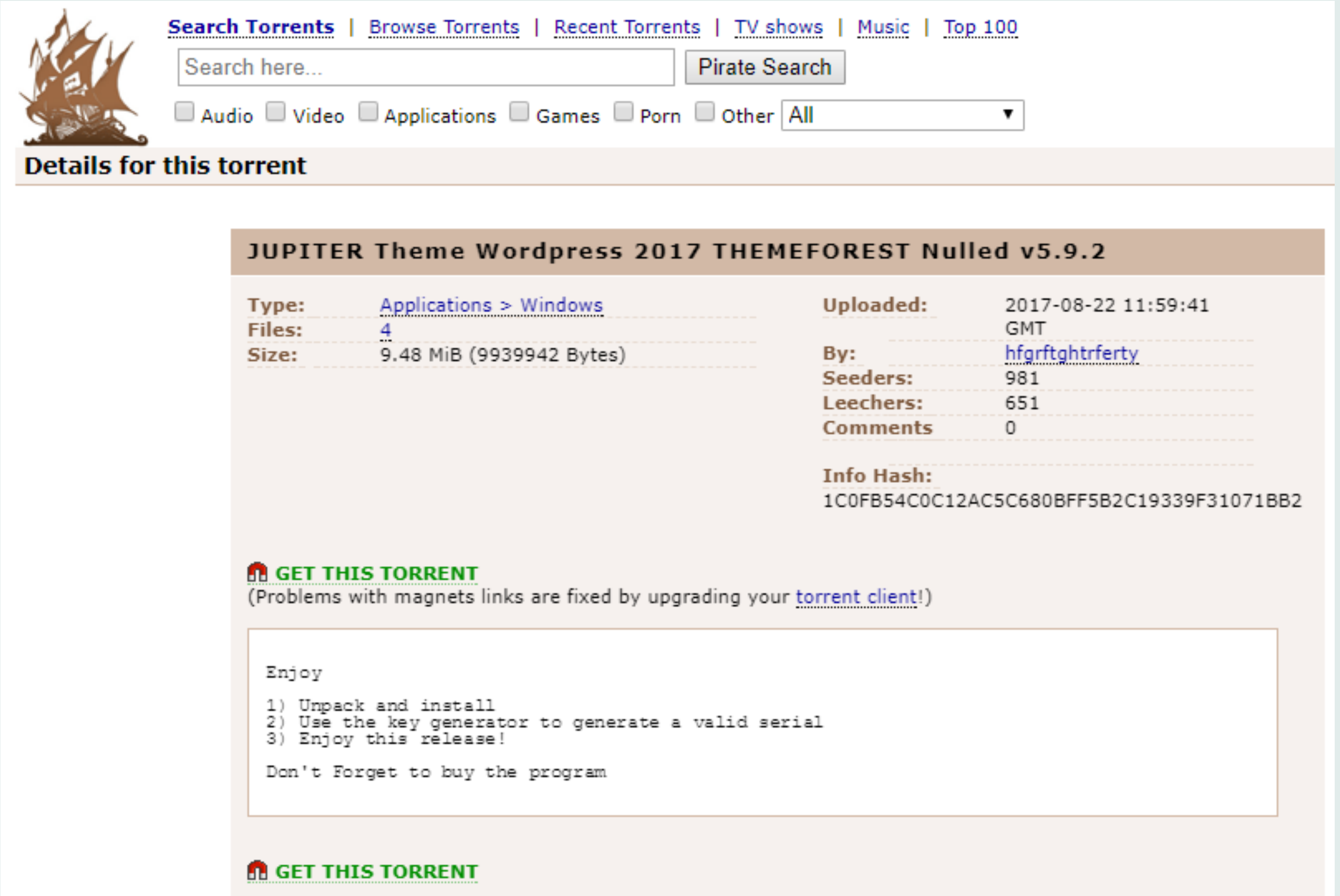


Edit Themes

Twenty Sixteen: Stylesheet (style.css)

```
/*
Theme Name: Twenty Sixteen
Theme URI: https://wordpress.org/themes/twentysixteen/
Author: the WordPress team
Author URI: https://wordpress.org/
Description: Twenty Sixteen is a modernized take on an ever-popu
masthead with an optional right sidebar that works perfectly for
options with beautiful default color schemes, a harmonious fluid
impeccable polish in every detail. Twenty Sixteen will make your
Version: 1.3
License: GNU General Public License v2 or later
License URI: http://www.gnu.org/licenses/gpl-2.0.html
Tags: one-column, two-columns, right-sidebar, accessibility-ready
custom-header, custom-menu, editor-style, featured-images, flexi
rtl-language-support, sticky-post, threaded-comments, translatio
Text Domain: twentysixteen

This theme, like WordPress, is licensed under the GPL.
Use it to make something cool, have fun, and share what you've l
*/
```

Backdoor in pirated software



Search Torrents | Browse Torrents | Recent Torrents | TV shows | Music | Top 100
Search here...
Pirate Search
□ Audio □ Video □ Applications □ Games □ Porn □ Other All ▼

Details for this torrent

JUPITER Theme Wordpress 2017 THEMEFOREST Nulled v5.9.2

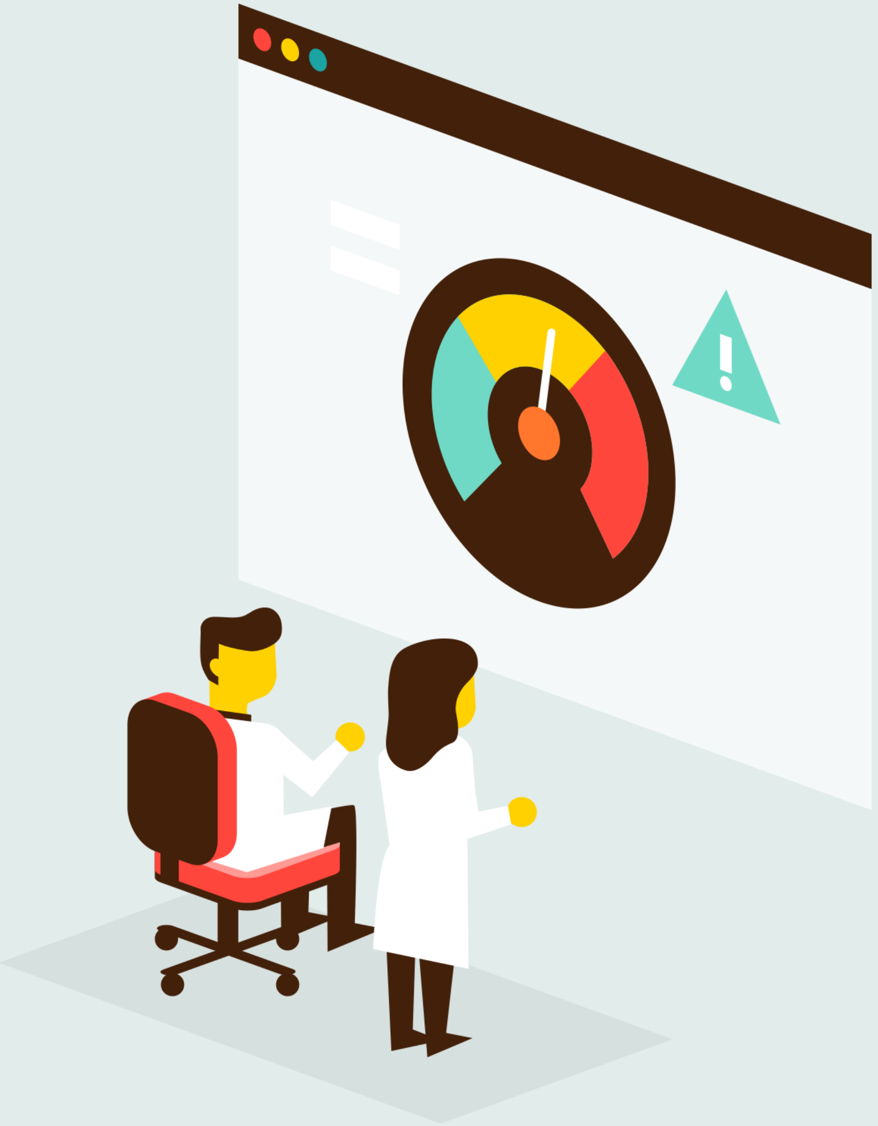
Type:	Applications > Windows
Files:	4
Size:	9.48 MiB (9939942 Bytes)
Uploaded:	2017-08-22 11:59:41 GMT
By:	hfgrftghtrferty
Seeders:	981
Leechers:	651
Comments	0

Info Hash:
1C0FB54C0C12AC5C680BFF5B2C19339F31071BB2

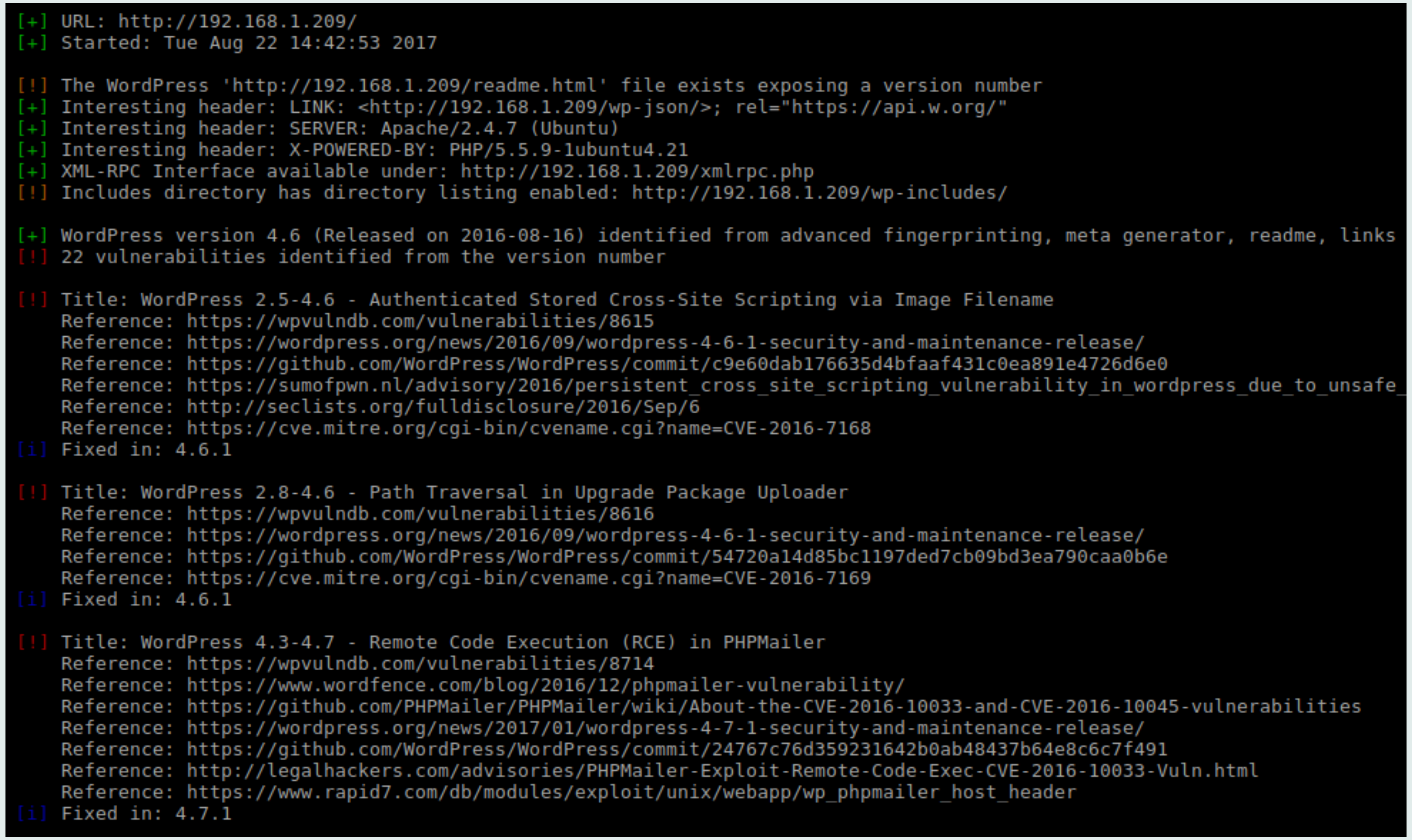
GET THIS TORRENT
(Problems with magnets links are fixed by upgrading your torrent client!)

```
Enjoy

1) Unpack and install
2) Use the key generator to generate a valid serial
3) Enjoy this release!

Don't Forget to buy the program
```

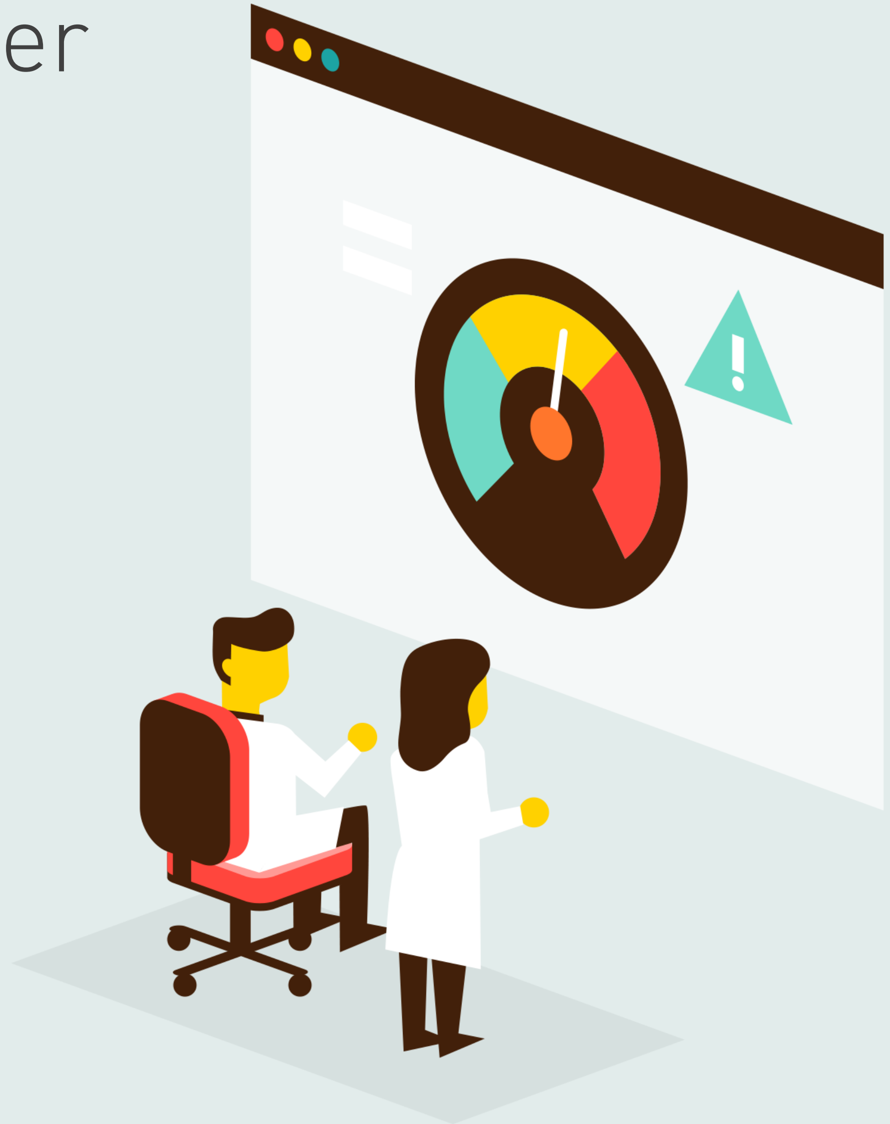
GET THIS TORRENT



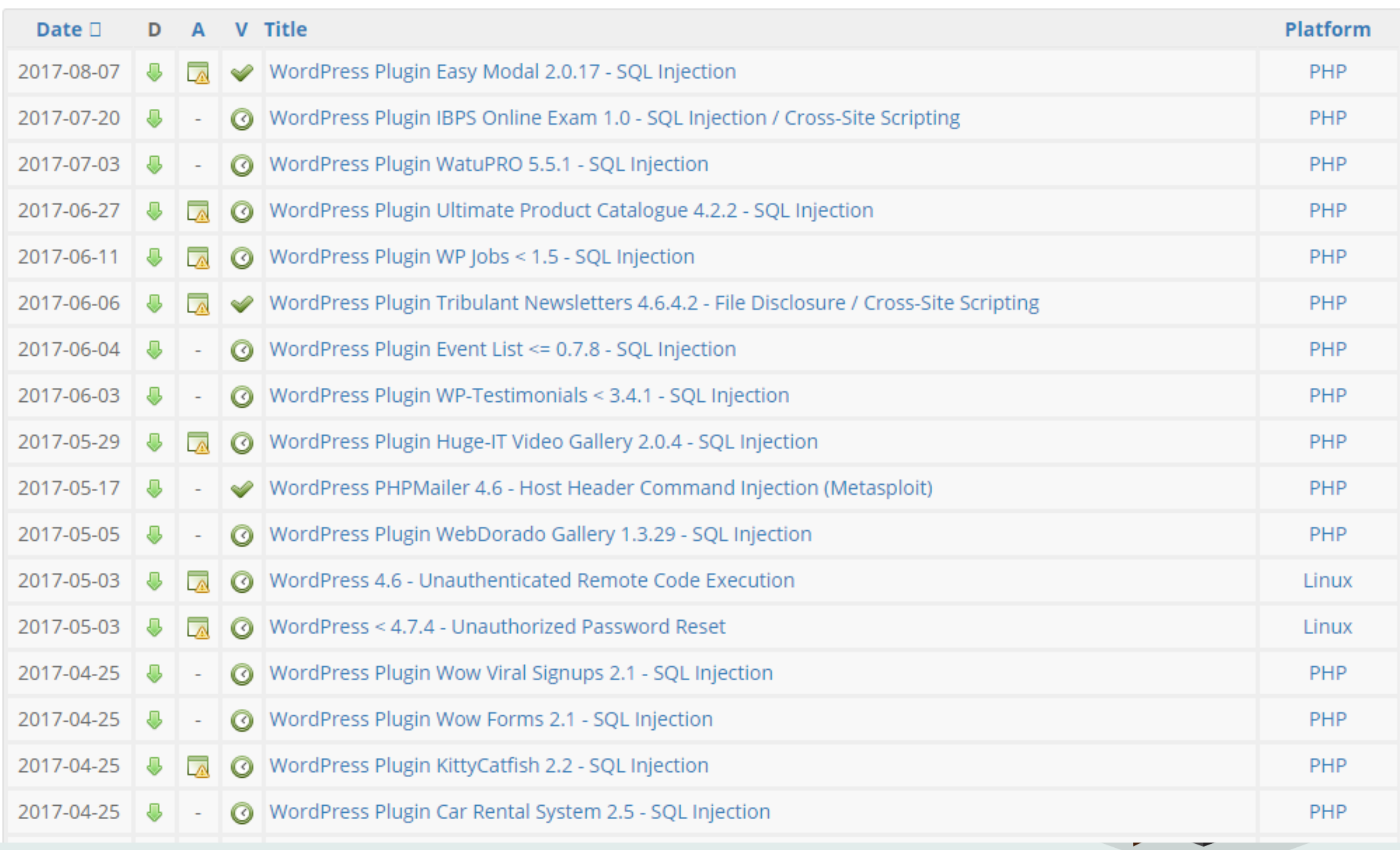
I know what you didn't do last summer



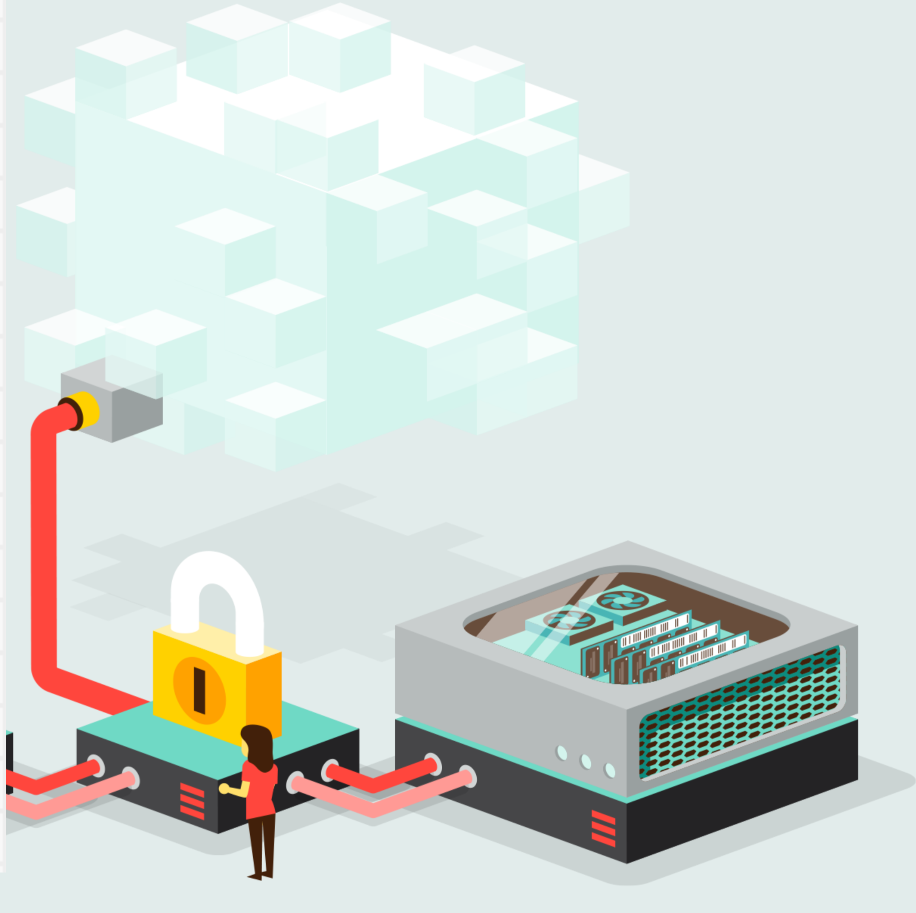
```
[+] URL: http://192.168.1.209/
[+] Started: Tue Aug 22 14:42:53 2017

[!] The WordPress 'http://192.168.1.209/readme.html' file exists exposing a version number
[+] Interesting header: LINK: <http://192.168.1.209/wp-json/>; rel="https://api.w.org/"
[+] Interesting header: SERVER: Apache/2.4.7 (Ubuntu)
[+] Interesting header: X-POWERED-BY: PHP/5.5.9-1ubuntu4.21
[+] XML-RPC Interface available under: http://192.168.1.209/xmlrpc.php
[!] Includes directory has directory listing enabled: http://192.168.1.209/wp-includes/

[+] WordPress version 4.6 (Released on 2016-08-16) identified from advanced fingerprinting, meta generator, readme, links
[!] 22 vulnerabilities identified from the version number

[!] Title: WordPress 2.5-4.6 - Authenticated Stored Cross-Site Scripting via Image Filename
    Reference: https://wpvulndb.com/vulnerabilities/8615
    Reference: https://wordpress.org/news/2016/09/wordpress-4-6-1-security-and-maintenance-release/
    Reference: https://github.com/WordPress/WordPress/commit/c9e60dab176635d4bfaaf431c0ea891e4726d6e0
    Reference: https://sumofpwn.nl/advisory/2016/persistent_cross_site_scripting_vulnerability_in_wordpress_due_to_unsafe_
    Reference: http://seclists.org/fulldisclosure/2016/Sep/6
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7168
[i] Fixed in: 4.6.1

[!] Title: WordPress 2.8-4.6 - Path Traversal in Upgrade Package Uploader
    Reference: https://wpvulndb.com/vulnerabilities/8616
    Reference: https://wordpress.org/news/2016/09/wordpress-4-6-1-security-and-maintenance-release/
    Reference: https://github.com/WordPress/WordPress/commit/54720a14d85bc1197ded7cb09bd3ea790caa0b6e
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7169
[i] Fixed in: 4.6.1

[!] Title: WordPress 4.3-4.7 - Remote Code Execution (RCE) in PHPMailer
    Reference: https://wpvulndb.com/vulnerabilities/8714
    Reference: https://www.wordfence.com/blog/2016/12/phpmailer-vulnerability/
    Reference: https://github.com/PHPMailer/PHPMailer/wiki/About-the-CVE-2016-10033-and-CVE-2016-10045-vulnerabilities
    Reference: https://wordpress.org/news/2017/01/wordpress-4-7-1-security-and-maintenance-release/
    Reference: https://github.com/WordPress/WordPress/commit/24767c76d359231642b0ab48437b64e8c6c7f491
    Reference: http://legalhackers.com/advisories/PHPMailer-Exploit-Remote-Code-Exec-CVE-2016-10033-Vuln.html
    Reference: https://www.rapid7.com/db/modules/exploit/unix/webapp/wp_phpmailer_host_header
[i] Fixed in: 4.7.1
```



Vulnerable Plugins



Date	D	A	V	Title	Platform
2017-08-07	⇩	▣	✓	WordPress Plugin Easy Modal 2.0.17 - SQL Injection	PHP
2017-07-20	⇩	-	◷	WordPress Plugin IBPS Online Exam 1.0 - SQL Injection / Cross-Site Scripting	PHP
2017-07-03	⇩	-	◷	WordPress Plugin WatuPRO 5.5.1 - SQL Injection	PHP
2017-06-27	⇩	▣	◷	WordPress Plugin Ultimate Product Catalogue 4.2.2 - SQL Injection	PHP
2017-06-11	⇩	▣	◷	WordPress Plugin WP Jobs < 1.5 - SQL Injection	PHP
2017-06-06	⇩	▣	✓	WordPress Plugin Tribulant Newsletters 4.6.4.2 - File Disclosure / Cross-Site Scripting	PHP
2017-06-04	⇩	-	◷	WordPress Plugin Event List <= 0.7.8 - SQL Injection	PHP
2017-06-03	⇩	-	◷	WordPress Plugin WP-Testimonials < 3.4.1 - SQL Injection	PHP
2017-05-29	⇩	▣	◷	WordPress Plugin Huge-IT Video Gallery 2.0.4 - SQL Injection	PHP
2017-05-17	⇩	-	✓	WordPress PHPMailer 4.6 - Host Header Command Injection (Metasploit)	PHP
2017-05-05	⇩	-	◷	WordPress Plugin WebDorado Gallery 1.3.29 - SQL Injection	PHP
2017-05-03	⇩	▣	◷	WordPress 4.6 - Unauthenticated Remote Code Execution	Linux
2017-05-03	⇩	▣	◷	WordPress < 4.7.4 - Unauthorized Password Reset	Linux
2017-04-25	⇩	-	◷	WordPress Plugin Wow Viral Signups 2.1 - SQL Injection	PHP
2017-04-25	⇩	-	◷	WordPress Plugin Wow Forms 2.1 - SQL Injection	PHP
2017-04-25	⇩	▣	◷	WordPress Plugin KittyCatfish 2.2 - SQL Injection	PHP
2017-04-25	⇩	-	◷	WordPress Plugin Car Rental System 2.5 - SQL Injection	PHP



What are the risks

- “Meldplicht” and possible fine from the Dutch Autoriteit persoonsgegevens
- Brand reputation
- Additional data cost
- Blacklisting of domains

Homework & Questions

- → https://haveibeenpwned.com/
- → https://premium.wpmudev.org/wp-checkup/
- → https://premium.wpmudev.org/blog/ultimate-wordpress-security-checklist/