WORDPRESS AND SECURITY

MARK DUBOIS

MARK@WEBPROFESSIONALS.ORG

SECURITY ASPECTS

Security fundamentals (account, password, backups and more)

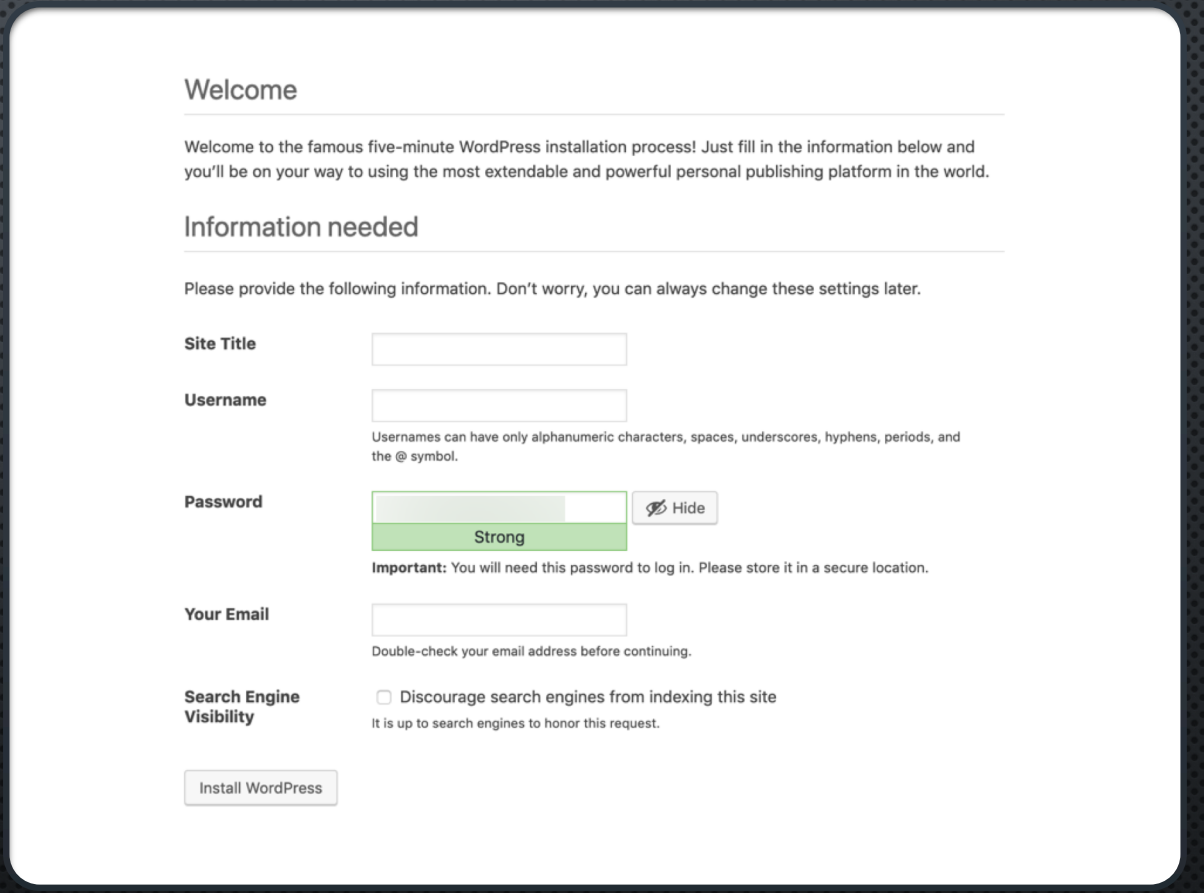
What do attack vectors hope to accomplish

Source: https://imgur.com/gallery/Wegl3Fu

```
$table_prefix  = 'wp_';
```

- wp_commentmeta
- wp_comments
- wp_links
- wp_options
- wp_postmeta
- wp_posts
- wp_termmeta
- wp_terms
- wp_term_relationships
- wp_term_taxonomy
- wp_usermeta
- wp_users

Username ?


Welcome
Welcome to the famous five-minute WordPress installation process! Just fill in the information below and you'll be on your way to using the most extendable and powerful personal publishing platform in the world.
Information needed
Please provide the following information. Don't worry, you can always change these settings later.
Site Title
Username
Usernames can have only alphanumeric characters, spaces, underscores, hyphens, periods, and the @ symbol.
Password
Hide
Strong
Important: You will need this password to log in. Please store it in a secure location.
Your Email
Double-check your email address before continuing.
Search Engine Visibility
Discourage search engines from indexing this site
It is up to search engines to honor this request.
Install WordPress

SECURITY FUNDAMENTALS - USERS

- USERNAMES – NO ADMIN ANY MORE (NO NEED TO USE ONES LIKE ASMITH EITHER)
- PASSWORDS – KEEP LONG AND COMPLEX
  - HTTP://CORRECTHORSEBATTERYSTAPLE.NET/ (FOR EXAMPLE)
- ONLY USE ADMIN ACCOUNT FOR UPDATES (KEEP SEPARATE ACCOUNT FOR POSTS)

2FA WHERE POSSIBLE

Top 10 Failed Logins

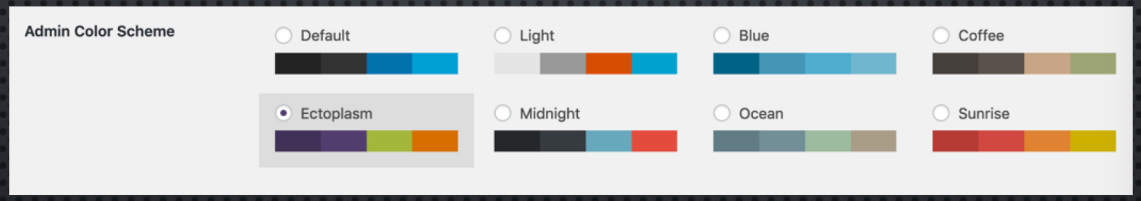
Username	Login Attempts	Existing User
admin	1	No
hahaxx2	1	No

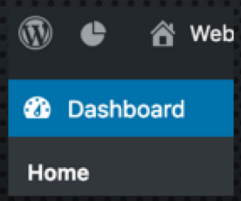
This email was sent from your website '[redacted]' by the Wordfence plugin at Monday [redacted] 2019 at 12:45:43 PM
The Wordfence administrative URL for this site is: [redacted]
A user with username [redacted]' who has administrator access signed in to your WordPress site.
User IP: [redacted]
User hostname: [redacted]
User location: [redacted] United States

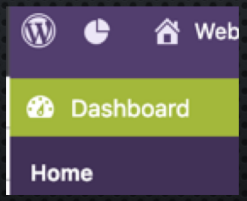
NOTIFY EVERY TIME ADMIN SIGNS IN

SECURITY FUNDAMENTALS – COLOR SCHEMES

- USE DIFFERENT COLOR SCHEMES FOR YOUR ADMIN ACCOUNTS

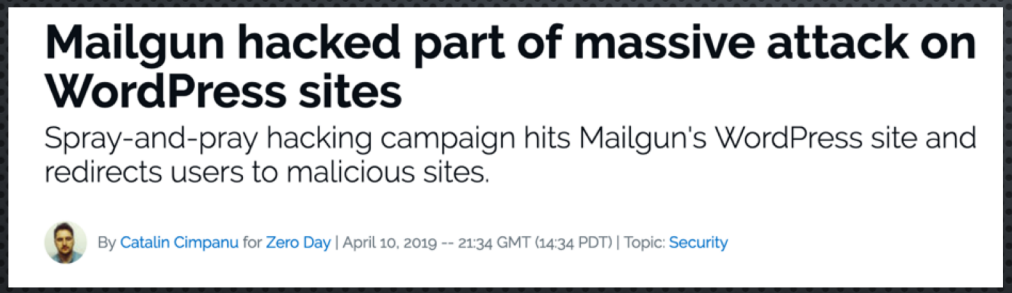






SECURITY FUNDAMENTALS - UPDATES

- PLUGINS AND THEMES – KEEP THEM UP TO DATE



Mailgun hacked part of massive attack on WordPress sites

Spray-and-pray hacking campaign hits Mailgun's WordPress site and redirects users to malicious sites.

By Catalin Cimpanu for Zero Day | April 10, 2019 -- 21:34 GMT (14:34 PDT) | Topic: Security

Email automation and delivery service Mailgun was one of the many companies that have been hacked today as part of a massive coordinated attack against WordPress sites.

The attacks exploited an unpatched cross-site scripting (XSS) vulnerability in a WordPress plugin named Yuzo Related Posts.

The vulnerability allowed hackers to inject code in vulnerable sites, which they later used to redirect incoming visitors to all sorts of nasties, such as tech support scams, sites peddling malware-laced software updates, or plain ol' spammy pages showing ads.

https://www.zdnet.com/article/mailgun-hacked-part-of-massive-attack-on-wordpress-sites/

SECURITY FUNDAMENTALS - BACKUPS

- BACKUPS – THERE ARE MANY ALTERNATIVES – THIS IS ONE I OFTEN USE
- KEEP IN MIND – IT IS NOT A VALID BACKUP UNTIL YOU HAVE RESTORED IT

SECURITY FUNDAMENTALS - PLUGINS

- AntiSpam Bee
- Better Plugin Compatibility Control
- ManageWP
- Two factor Authentication
- WordFence Security
- WordPress Version Info
- WP Statistics

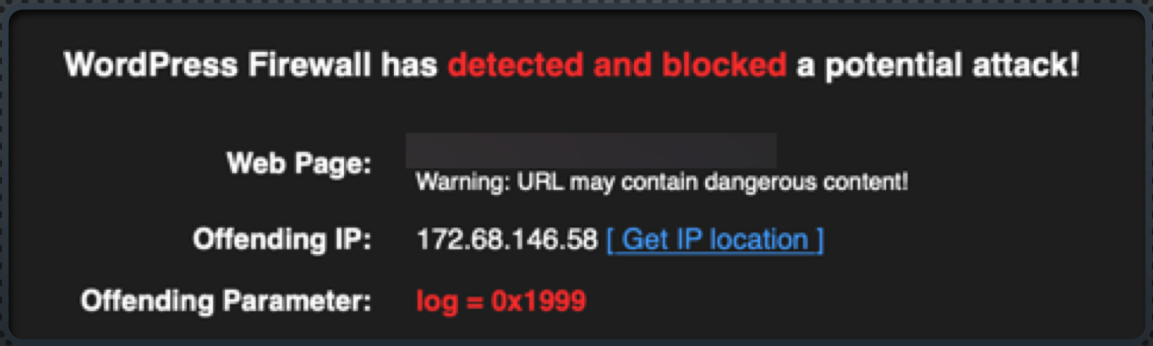
SECURITY ASPECTS

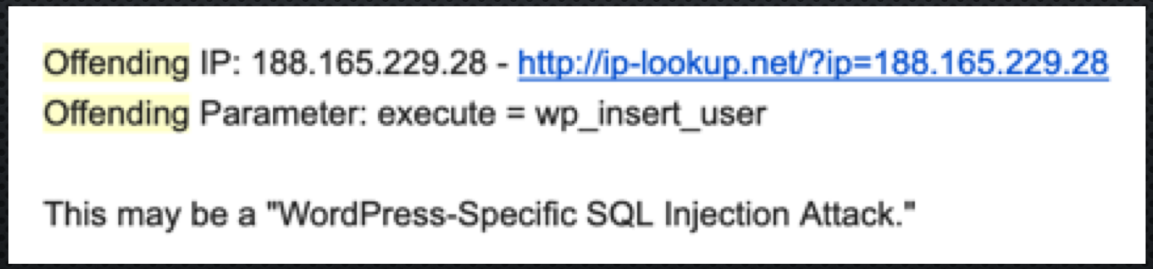
Security fundamentals (account, password, backups and more)

What do attack vectors hope to accomplish

SQL INJECTION

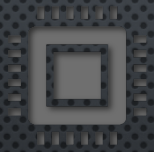
PURPOSE IS TO COMPROMISE DATABASE (OFTEN TO DUMP CONTENTS)





SQL INJECTION EXPLAINED

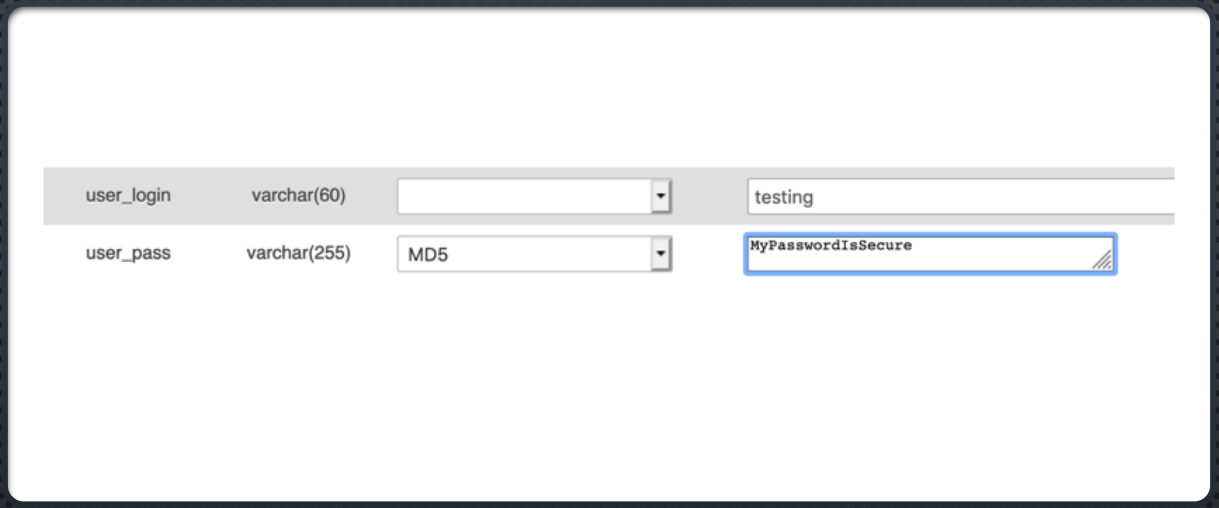
Attacks database layer of application



Using certain words or commands to control or access the database

Contents can then be manipulated or downloaded

Passwords encrypted, but often just MD5 hash (HashCat and similar tools)



IF YOU HAVE PHPMYAMIN ACCESS

DIRECTORY TRAVERSAL

PURPOSE IS TO EXPLOIT USER SUPPLIED FILE NAMES/ CONTENTS

December 3, 2018 12:10pm	**39.104.80.94 (China)** Blocked for Directory Traversal - wp-config.php in query string: file=../wp-config.php
December 3, 2018 9:08am	**39.104.110.131 (China)** Blocked for Directory Traversal - wp-config.php in query string: file=../wp-config.php

MALICIOUS FILE UPLOAD

PURPOSE IS TO UPLOAD EXECUTABLE FILE (.PHP) SO IT CAN BE ACCESSED VIA BROWSER AND EXECUTED (TO GRANT ACCESS TO PROTECTED ITEMS)

December 2, 2018 7:37pm	**139.162.228.61 (United Kingdom)** Blocked for Malicious File Upload (PHP)
December 2, 2018 7:37pm	**176.31.208.193 (Germany)** Blocked for Malicious File Upload (PHP)

CROSS SITE SCRIPTING

- REFERENCE: HTTPS://WWW.OWASP.ORG/INDEX.PHP/CROSS-SITE_SCRIPTING_(XSS)

```
<body onload=alert('test1')>
```

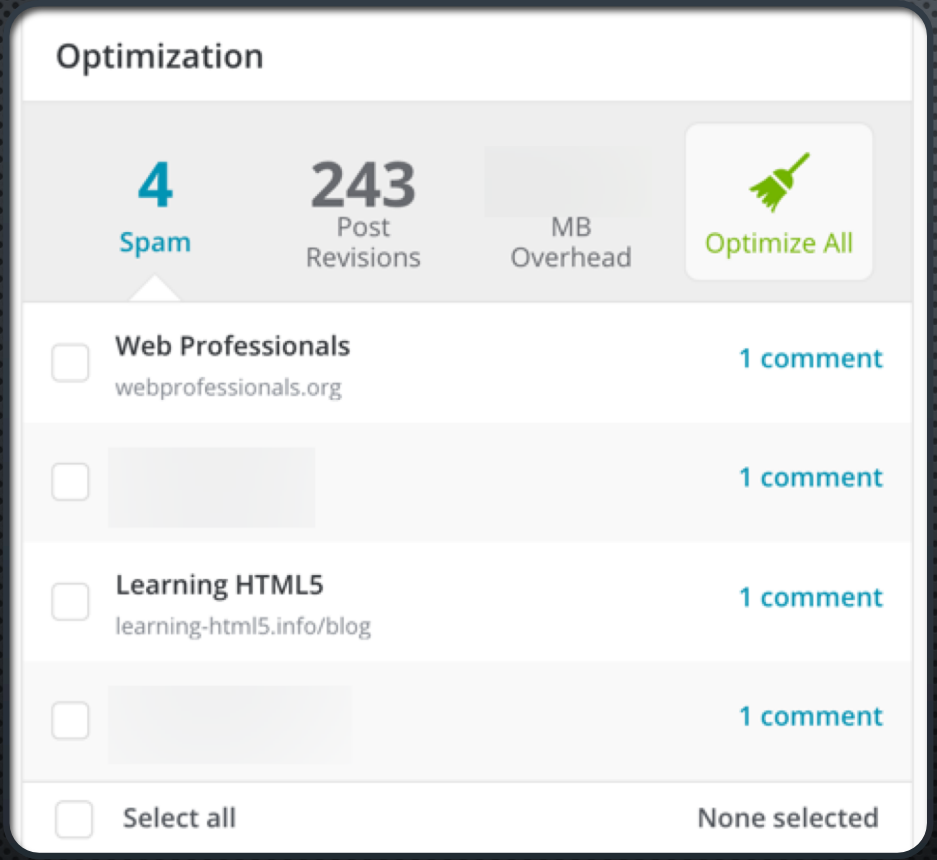
```
<b onmouseover=alert('Wufff!')>click me!</b>
```

```
<img src="http://url.to.file.which/not.exist" onerror=alert(document.cookie);>
```

XSS EXPLAINED

Data enters through untrusted source [form] (and is not sanitized)

Can fully disclose session cookies (allowing one to hijack a user session and take over their account)


Optimization
4
Spam
243
Post
Revisions
MB
Overhead
Optimize All
Web Professionals
webprofessionals.org
1 comment
1 comment
Learning HTML5
learning-html5.info/blog
1 comment
1 comment
Select all
None selected

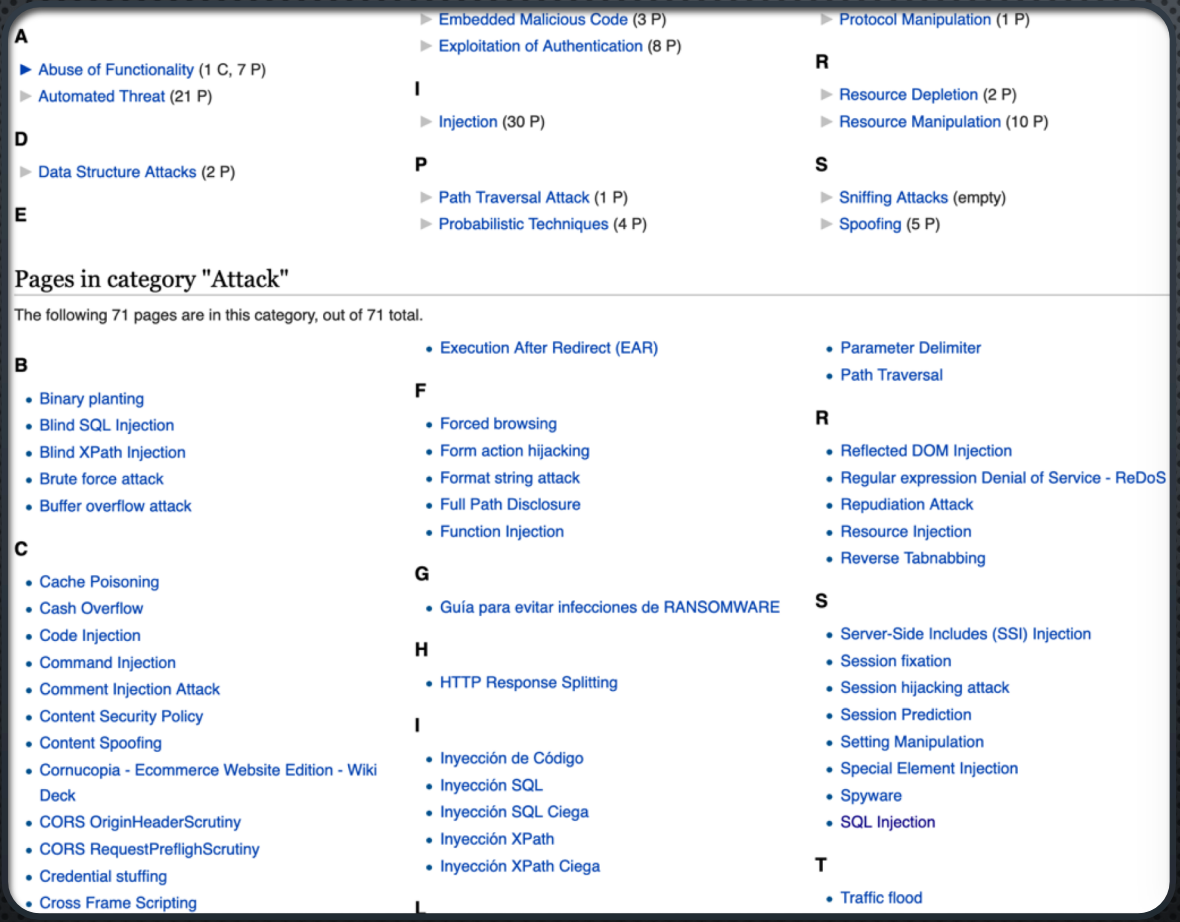
WEBLOG SPAM

SPAM PURPOSE

OFTEN RANDOM COMMENTS
(WITH HYPERLINKS)

GOAL IS TO INCREASE THOSE
SITES SEARCH ENGINE RANKING

MORE POPULAR THE SITE => MORE SPAM



A
- Abuse of Functionality (1 C, 7 P)
- Automated Threat (21 P)

D
- Data Structure Attacks (2 P)

E
- Embedded Malicious Code (3 P)
- Exploitation of Authentication (8 P)

I
- Injection (30 P)

P
- Path Traversal Attack (1 P)
- Probabilistic Techniques (4 P)
- Protocol Manipulation (1 P)

R
- Resource Depletion (2 P)
- Resource Manipulation (10 P)

S
- Sniffing Attacks (empty)
- Spoofing (5 P)

Pages in category "Attack"

The following 71 pages are in this category, out of 71 total.

B
- Binary planting
- Blind SQL Injection
- Blind XPath Injection
- Brute force attack
- Buffer overflow attack

C
- Cache Poisoning
- Cash Overflow
- Code Injection
- Command Injection
- Comment Injection Attack
- Content Security Policy
- Content Spoofing
- Cornucopia - Ecommerce Website Edition - Wiki Deck
- CORS OriginHeaderScrutiny
- CORS RequestPreflighScrutiny
- Credential stuffing
- Cross Frame Scripting

- Execution After Redirect (EAR)

F
- Forced browsing
- Form action hijacking
- Format string attack
- Full Path Disclosure
- Function Injection

G
- Guía para evitar infecciones de RANSOMWARE

H
- HTTP Response Splitting

I
- Inyección de Código
- Inyección SQL
- Inyección SQL Ciega
- Inyección XPath
- Inyección XPath Ciega

- Parameter Delimiter
- Path Traversal

R
- Reflected DOM Injection
- Regular expression Denial of Service - ReDoS
- Repudiation Attack
- Resource Injection
- Reverse Tabnabbing

S
- Server-Side Includes (SSI) Injection
- Session fixation
- Session hijacking attack
- Session Prediction
- Setting Manipulation
- Special Element Injection
- Spyware
- SQL Injection

T
- Traffic flood

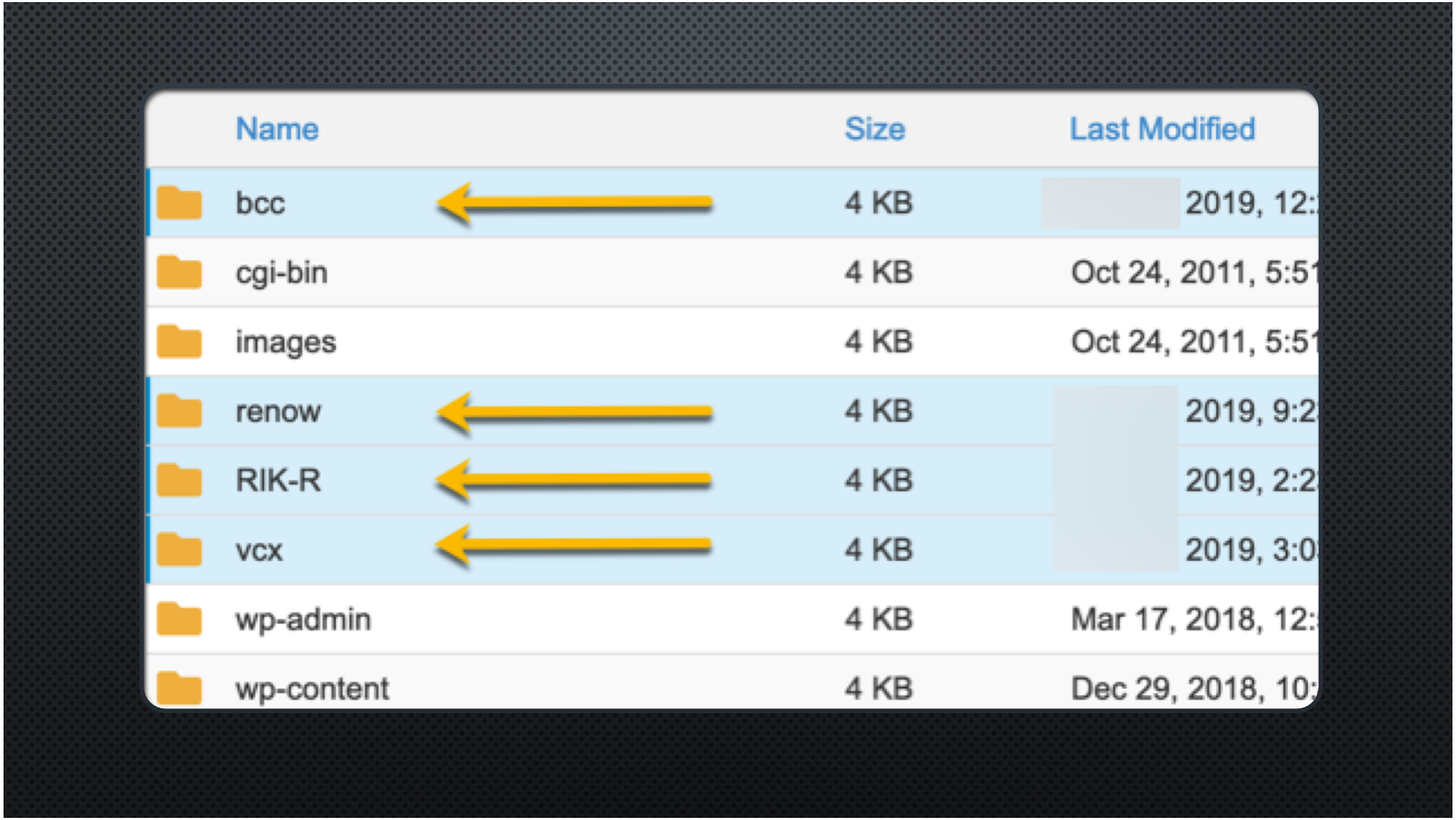
MANY OTHER ATTACK VECTORS

HTTPS://WWW.OWASP.ORG/INDEX.PHP/CATEGORY:ATTACK

NOW WHAT?

NOT LIMITED TO THESE

- Homepage looks different (perhaps you see spam pop-up ads)
- Site performance issues
- Unexplained files/ folders appear
- Changes to admin users (new ones or some removed)


Name
Size
Last Modified
bcc
4 KB
2019, 12:
cgi-bin
4 KB
Oct 24, 2011, 5:51
images
4 KB
Oct 24, 2011, 5:51
renow
4 KB
2019, 9:2
RIK-R
4 KB
2019, 2:2
vcx
4 KB
2019, 3:0
wp-admin
4 KB
Mar 17, 2018, 12:
wp-content
4 KB
Dec 29, 2018, 10:

WORDPRESS AND SECURITY

MARK DUBOIS

MARK@WEBPROFESSIONALS.ORG