

Homework #2: OSINT

Name: Gilbert Garczynski

UID: 115308718

Honor Pledge: I pledge on my honor that I have not given or received any unauthorized assistance on this assignment/examination.

Assignment Goal: To apply the OSINT techniques discussed in lecture to solve a series of small challenges based around a fake scenario.

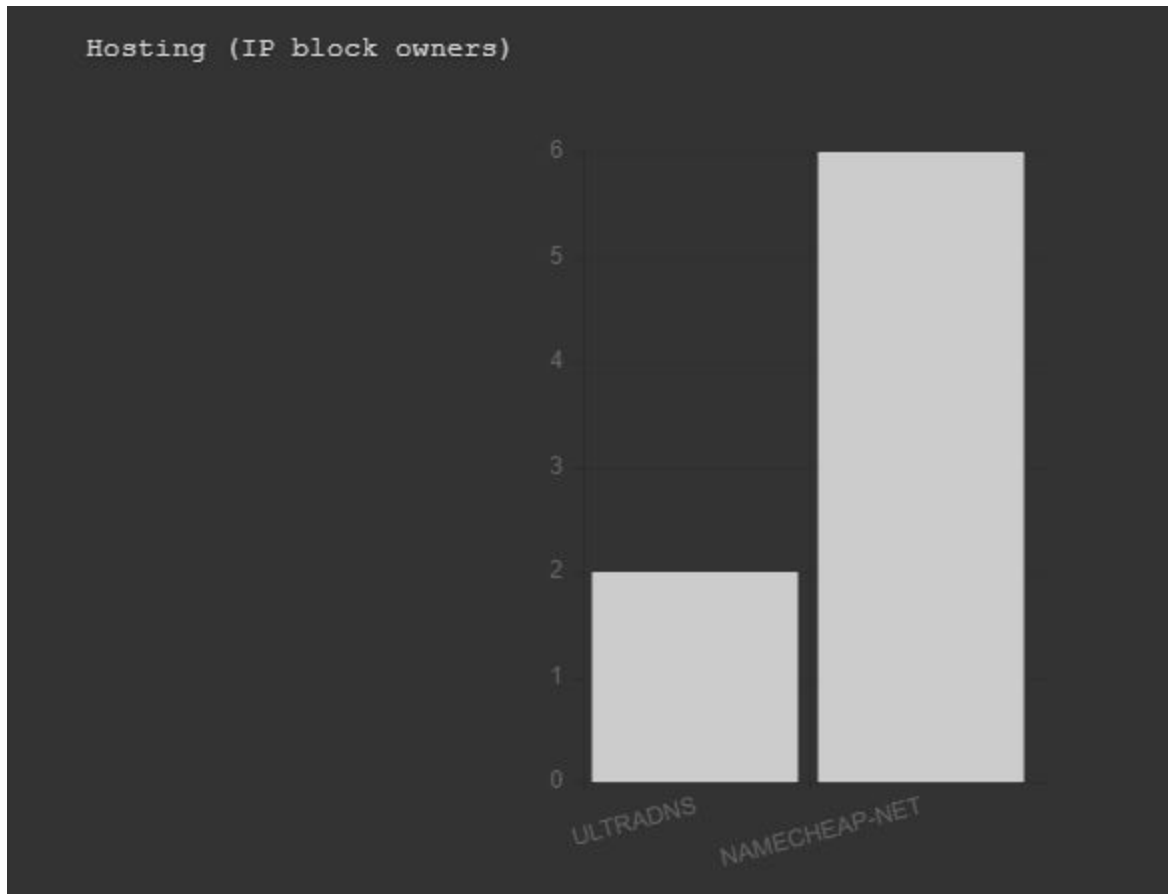
Consider the following scenario: An e-commerce company has suffered an attack by a hacking group. The company <http://supersecure.store>, has had their website defaced and some secret information has been exposed to the internet. You're a security analyst, who's goal is to use some OSINT techniques to discover information about the attackers.

1. Find information about the domain (25 points)

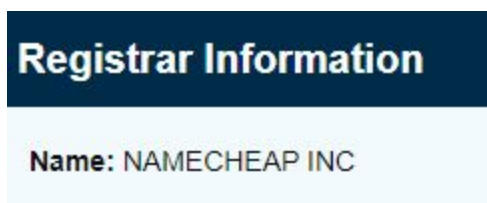
Using [DNSdumpster.com](https://dnsdumpster.com), I can ascertain that the host location is somewhere in the United States.



































The domain is also registered through a registrar named NameCheap Inc.
From DNSDumpster:



From ICANN:



The IP address for the servers is **156.154.132.200** and for the email for the domain is **162.255.118.51**. Source, DNSdumpster

DNS Servers		
dns1.registrar-servers.com.      	156.154.132.200 dns1.registrar-servers.com	ULTRADNS United States
dns2.registrar-servers.com.      	156.154.133.200 dns2.namecheaposting.com	ULTRADNS United States
MX Records ** This is where email for the domain goes...		
20 eforward5.registrar-servers.com.    	162.255.118.51 eforward1.registrar-servers.com	NAMECHEAP-NET United States
15 eforward4.registrar-servers.com.    	162.255.118.52 eforward2.registrar-servers.com	NAMECHEAP-NET United States
10 eforward1.registrar-servers.com.    	162.255.118.51 eforward3.registrar-servers.com	NAMECHEAP-NET United States
10 eforward2.registrar-servers.com.    	162.255.118.52 eforward2.registrar-servers.com	NAMECHEAP-NET United States
10 eforward3.registrar-servers.com.    	162.255.118.51 eforward1.registrar-servers.com	NAMECHEAP-NET United States

A reverse IP lookup on [Reverse IP Lookup - MxToolbox](#) confirms that the DNS server is NameCheap Inc.

2. Check out the web scraper rules (25 points)

Hidden login page <http://supersecure.store:1337/>

Add “robots.txt” to the end of the URL <http://supersecure.store/>. So the URL becomes <http://supersecure.store/robots.txt>.

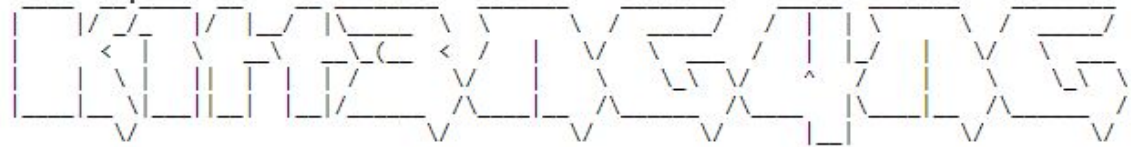
```

User-agent: Googlebot
Disallow: /

User-agent: k1tt3ng4ng
Allow: /

User-agent: *
Disallow: http://supersecure.store:1337/

```



Following the URL under “User-agent: *” will take you to the login screen.

What pages are not allowed to be scrapped? (Hint: 🤖)

The pages that are not allowed to be scrapped are the pages after / at the end of the URL. as you can see in the above screen capture, the User-agent: GoogleBot disallows the ‘/’ to be viewed.

3. Find the credentials for the hidden login panel (25 points)

After finding the secret login page, I right clicked and selected “view source”. This took me to this:

```

1 <head>
2 <link href="//maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.css" rel="stylesheet" id="bootstrap-css">
3 <script src="//maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js"></script>
4 <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/3.2.1/jquery.min.js"></script>
5 <link rel="stylesheet" type="text/css" href="login-styles.css">
6 </head>
7 <script>
8     function validate() {
9         var username = document.getElementById("login").value;
10        var password = document.getElementById("password").value;
11        if(username == "k1tt3ng4ng" && password == "d0gzuck") { // this is secure webdev at its finest
12            alert("CONGRATS... you found my secret... the answer is... CMSC388U{OSINT-IS-FUN}");
13        } else {
14            alert("WRONG PASSWORD");
15        }
16    }
17 </script>
18 <div class="wrapper fadeInDown">
19     <div id="formContent">
20
21         <div class="fadeIn first">
22             <img src="" height=150px>
23             
24         </div>
25
26         <form>
27             <input type="text" id="login" class="fadeIn second" name="login" placeholder="login">
28             <input type="text" id="password" class="fadeIn third" name="login" placeholder="password">
29             <input type="submit" onclick="validate()" class="fadeIn fourth" value="Log In">
30         </form>
31
32         <div id="formFooter">
33             <a class="underlineHover" href="http://www.nyan.cat/cats/pirate.gif">Need a Password?</a>
34         </div>
35     </div>
36 </div>
37 </div>
38

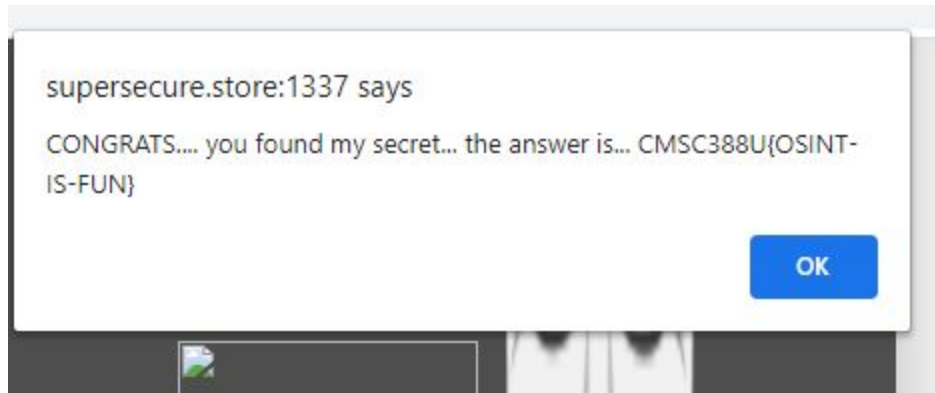
```

As you can see, on line 11, the username and password (credentials) are plainly in view.

Username: k1tt3ng4ng

Password: d0gzsuck

After this login, a JavaScript message pops up



The secret message is : CMSC388U{OSINT-IS_FUN}