

# HOMEWORK 1

Sara Bruzzese - 1648786

## 1. Website: [www.psicologiareba.it](http://www.psicologiareba.it)

1) the command “wget [www.psicologiareba.it](http://www.psicologiareba.it)” allow me to create a local copy of the web page, that I can analyze trying to find some useful comments.

In this case, the comments gave me a brief description of what the code do in that part of the source. An example of the result is shown here:

```
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
<!--[endif]-->
<style type="text/css">
.clear {
    zoom: 1;
    display: block;
}
</style>
<![endif]-->
<script>
(function(i,s,o,g,r,a,m){i['GoogleAnalyticsObject']=r;i[r]=i[r]||function(){
(i[r].q=i[r].q||[]).push(arguments)},i[r].l=1*new Date();a=s.createElement(o),
m=s.getElementsByTagName(o)[0];a.async=1;a.src=g;m.parentNode.insertBefore(a,m)
})(window,document,'script','https://www.google-analytics.com/analytics.js','ga');
ga('create', 'UA-89664632-4', 'auto');
ga('send', 'pageview');
</script>
</head>
<body>
<div class="section" id="page"> <!-- Defining the #page section with the section tag -->
<div class="header"> <!-- Defining the header section of the page with the appropriate tag -->
<h1>Psicologia REBA</h1>
<h3>Psicologia Ambientale</h3>
<div class="nav clear"> <!-- The nav link semantically marks your main site navigation -->
<ul>
<li><a href="#article1">Test REBA</a></li>
<li><a href="#article2">Psicologia Ambientale</a></li>
<li><a href="#article3">Link Siti</a></li>
</ul>
</div>
</div>
<div class="section" id="articles"> <!-- A new section with the articles -->
<!-- Article 1 start -->
```

2) Then, I configured DirBuster to start a sort of “dictionary attack” to the website on port 80 (HTTP). I choose a wordlist from DirBuster and I didn’t used privoxy because I have the permission to perform this operation from the owner of the website, but if I had to do this in an anonymous way, I should have modify the options of DirBuster and set the program to run through a specified proxy (on port 8118 in this case). I show here the partial result of my work.

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing			
File Options About Help			
http://www.psicologiareba.it:80/80/			
Scan Information \ Results - List View: Dirs: 54 Files: 8 \ Results - Tree View \ Errors: 22 \			
Directory Structure	Response Code	Response Size	
/	200	14041	
tmp	403	1542	
img	403	1542	
cgi-bin	403	1542	
php.php	200	183	
status	403	1542	
1	403	1542	
htdocs	200	1712	
2	403	1542	
htdocs	200	1710	
cgi-bin	403	263	
img	403	263	
jquery.scrollTo-1.4.2	403	263	
jquery.scrollTo-min.js	200	2514	
script.js	200	569	
icons	403	1542	
small	403	1542	
webmail	302	477	
cpanel	302	461	

2. In the seminar "how I met your girlfriend" it's shown how certain services are insecure, allowing to take advantage of poorly maintained mechanisms. The example of Facebook is initially presented: it uses a PHP session to authenticate users, which makes use of cookies that maintain the session authentication. Facebook generates a cookie composed by 160 bits, so it's very difficult to force this mechanism without any hint. These 160 bits are composed by: 32 bits for the address IP, 32 bits for the epoche, 32 bits for microseconds and 64 bits for a random value. The goal is to be able to guess the cookie code in order to overcome the authentication phase without really knowing the sensitive data to log in to Facebook. As I've already said, it's not possible to brute force this cookie as it would take too long for our current skills. The presenter of the seminar shows techniques to be able to obtain almost all the 160 bits with some tricks, remaining with only 20 bits to guess. It shows how simple it is to establish the 32 bits of the epoch by keeping track of the user's activity, it can almost certainly establish the value of the epoch simply by observing when the target user connects to the Facebook chat. The 32 bits of the IP address can be discovered by bringing the target user to click on a link under our domain, from whose logs it's easy to trace the desired IP address. The 32-bit microseconds can be reduced because they can take a value between 0 and 999.999 which is expressed with 20 bits. Even 64 random bits can be considerably reduced, because often they are not generated completely randomly. It's possible to identify these bits by discovering some values related to the user and taking advantage of the knowledge of the functions used for random generation. It's shown as with around 500,000 login attempts it was able to find the right cookie to enter the private profile. To improve security, Facebook decided to add more entropy elements, for example you can choose your own randomness seed. Subsequently, the presenter shows how to open a certain port on the target user's router. Using some mechanisms such as cross-protocol scripting (XPS) and NAT pinning, it is possible to confuse the target browser and router. When the target user clicks on a malicious site, some mechanisms are activated that lead the browser to request the server to need to open a specific port on its router. To prevent this type of attack, it's important restrict firewall settings and use tools to know if an application it is attempting to access unknown ports. Finally, the presenter talked about geolocation with the XXXSS attack. If the target visits a malicious site, it activates a mechanism that accesses the local page of its router and detects the MAC address of the devices connected to it, and then sends them to the hacker. The attacker can subsequently send a request to Google to find out the geolocation of the devices, as Google has the association of most of the MAC addresses and their respective geographical addresses.

4. For this exercise I choose the company: Philmark Group. I googled “Philmark group resume firewalls” and I found very interesting information on their website. I found many job roles that they’re searching for the Philmark company.

## SISTEMISTA DI RETE (ROMA)


Full TimeRomaPosted on 30 Gennaio 2020


**Philmark Group**


Cerchiamo un Sistemista di rete con le seguenti competenze tecniche:


- Certificazione Cisco CCNA e CCNP,
- Conoscenza firewall Fortinet e protocollo internet BGP


I found out that they were searching for security specialists 2 years ago, and they were interested in intrusion detection and testing penetration.


**Azienda:** Philmark Informatica S.p.A.


**Aggiornata il:** 23/10/2018


**Impegno:** Full-time

**Compenso lordo:** Da concordare

**Figura ricercata:** Specialisti IT

**Luogo di lavoro:** Emirati Arabi Uniti, Dubai

**Contratto di lavoro:** Da determinare

**Posti disponibili:** 1

### Descrizione

Philmark Informatica S.p.A. ricerca Specialisti IT su Dubai.

Profili ricercati:

**Development Manager**

Responsibilities:

- Supervising the development of several software products on multiple operating systems.

Skills:

- At least 8 years of software engineering experience in the field of IT security (i.e. penetration testing frameworks, **intrusion detection** systems, Antivirus, Firewalls, etc.).
- Hands-on and up to date experience in software development on Windows, Linux, OS X, Android, iOS environments with full understanding of the lifecycle of software products, including design, development, deployment, maintenance.
- Expert knowledge of IP protocol stack and applications.
- Knowledge of security paradigms and models.
- Project and product management experience.
- Practical and familiar with management processes and tools for software engineering.
- Team leading and coaching experience.
- Attitude to problem solving using unconventional and creative methods.

I didn't find out any relevant configuration of the firewall.

5. I used archive.org to analyse the behaviour of the website [www.psicologiareba.it](http://www.psicologiareba.it) during the years and I found out that the first copy of the website dates back to the 2009 and probably had another owner or had another scope.



This is the first result on archive.org.

Then during the years, they added information about some courses.



From 2015 the website became under construction, and the situation doesn't change for a year, until they put up for sale the domain.



From 2017 the website was set up with the contents that it has now.

6. [hackersforcharity.org/ghdb](https://hackersforcharity.org/ghdb) contains the basic listing of many of the best Google search strings that hackers use to dig up information on the Web.

### Index of /railsapp/config

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>	-	-	
<a href="#">application.rb</a>	2018-09-23 05:37	659	
<a href="#">boot.rb</a>	2018-09-23 05:37	207	
<a href="#">cable.yml</a>	2018-09-23 05:37	190	
<a href="#">credentials.yml.enc</a>	2018-09-23 05:37	464	
<a href="#">database.yml</a>	2018-09-23 05:37	594	
<a href="#">environment.rb</a>	2018-09-23 05:37	128	
<a href="#">environments/</a>	2019-01-03 01:17	-	
<a href="#">initializers/</a>	2019-01-03 01:17	-	
<a href="#">locales/</a>	2019-01-03 01:17	-	
<a href="#">master.key</a>	2018-09-23 05:37	32	
<a href="#">puma.rb</a>	2018-09-23 05:37	1.4K	
<a href="#">routes.rb</a>	2018-09-27 02:00	161	
<a href="#">spring.rb</a>	2018-09-23 05:37	111	
<a href="#">storage.yml</a>	2018-09-23 05:37	1.1K	

Apache/2.4.29 (Ubuntu) Server at www.renamon.org Port 443

I choose to search the string: [intitle:"index of" "credentials.yml"](#). This search allows me to find files containing encrypted credentials, I show here my first result where I found out the "credentials.yml.enc" file.

### Index of /\_vti\_pvt

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>	-	-	
<a href="#">access.cnf</a>	2019-04-04 20:28	141	
<a href="#">botinfo.cnf</a>	2019-04-04 20:28	24	
<a href="#">bots.cnf</a>	2019-04-04 20:28	24	
<a href="#">deptodoc.btr</a>	2019-04-04 20:28	324	
<a href="#">doctodep.btr</a>	2019-04-04 20:28	5.5K	
<a href="#">frontpg.lck</a>	2019-04-04 20:28	0	
<a href="#">linkinfo.btr</a>	2019-04-04 20:28	5.5K	
<a href="#">service.cnf</a>	2019-04-04 20:28	1.2K	
<a href="#">service.grp</a>	2019-04-04 20:28	49	
<a href="#">service.lck</a>	2019-04-04 20:28	0	
<a href="#">service.pwd</a>	2019-04-04 20:28	60	
<a href="#">services.cnf</a>	2019-04-04 20:28	2	
<a href="#">svcacl.cnf</a>	2019-04-04 20:28	63	
<a href="#">writeto.cnf</a>	2019-04-04 20:28	24	

Apache Server at www.granvilleislandpublishing.com Port 443

Then, I searched the string: [intitle:"index of" service.grp](#). This string allows me to find admin usernames in plain text. In the picture, in access.cnf I found username and password in plain text.

### Index of /backup/nhocrum.com

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>	-	-	
<a href="#">domain.conf</a>	2018-07-17 13:21	236	
<a href="#">domain.usage</a>	2018-07-17 00:10	50	
<a href="#">email/</a>	2018-07-17 13:59	-	
<a href="#">ftp.conf</a>	2018-07-17 13:21	32	
<a href="#">ftp.passwd</a>	2018-07-17 13:21	84	
<a href="#">nhocrum.com.db</a>	2018-07-17 13:21	731	
<a href="#">subdomain.list</a>	2018-07-17 13:21	0	

Apache/2.4.34 (Win32) OpenSSL/1.0.2o PHP/5.6.38 Server at nhocrum.com Port 80

Finally, I searched the string: [intitle:"index of" share.passwd OR cloud.passwd OR ftp.passwd - public](#). It allows me to find password files, as shown in the picture in [ftp.passwd](#).

7. I did the research for the website [www.psicologiareba.it](http://www.psicologiareba.it). The registry is the owner of the domain extensions. In this case, we have a .it domain, so the **registry** is the CNR of Pisa.

```
refer:      whois.nic.it

domain:     IT

organisation: IIT - CNR
address:    Via Moruzzi, 1
address:    Pisa I-56124
address:    Italy

contact:    administrative
name:       Marco Conti
organisation: IIT - CNR
address:    Via Moruzzi, 1
address:    Pisa I-56124
address:    Italy
phone:      +39 050 315 2123
fax-no:     +39 050 315 2113
e-mail:     direttore@iit.cnr.it

contact:    technical
name:       Maurizio Martinelli
organisation: IIT - CNR
address:    Via Moruzzi, 1
address:    Pisa I-56124
address:    Italy
phone:      +39 050 315 2087
fax-no:     +39 050 315 2207
e-mail:     maurizio.martinelli@iit.cnr.it

nserver:    A.DNS.IT 194.0.16.215 2001:678:12:0:194:0:16:215
nserver:    DNS.NIC.IT 192.12.192.5 2a00:d40:1:1:0:0:0:5
nserver:    M.DNS.IT 2001:1ac0:0:200:0:a5d1:6004:2 217.29.76.4
nserver:    NAMESERVER.CNR.IT 194.119.192.34 2a00:1620:c0:220:194:119:192:34
nserver:    R.DNS.IT 193.206.141.46 2001:760:ffff:ffff:0:0:0:ca
nserver:    S.DNS.IT 194.146.106.30 2001:67c:1010:7:0:0:0:53
ds-rdata:   41901 10 2 47F7F7BA21E48591F6172EED13E35B66B93AD9F2880FC9BADA64F68CE28EBB90

whois:      whois.nic.it

status:     ACTIVE
remarks:    Registration information: http://www.nic.it/

created:    1987-12-23
changed:    2019-09-25
source:     IANA
```

LOCATION		Registrar	
Country	Italy (IT)	Organizzazione:	Seeweb S.r.l.
Continent	Europe (EU)	Nome:	TOPHOST-REG
Coordinates	43.1479 (lat) / 12.1097 (long)	Web:	<a href="https://www.tophost.it">https://www.tophost.it</a>
Time	2020-03-23 13:54:43 (Europe/Rome)	DNSSEC:	no
NETWORK		Nameservers	
IP address	217.64.195.204	ns1.th.seeweb.it ns2.th.seeweb.it	
Hostname	w-11.th.seeweb.it		
Provider	SEEWEB s.r.l.		
ASN	12637		

I did a research on nic.it and I found out the registrar, which is the entity which collaborates with the registry to provide some Internet services to the host. In this case, the **registrar** is Seeweb, who provides even the DNS service.

The registrant is the final user that decides to open a website. In this case, the **registrant** is hidden through anonymous information. This is an option that the registrant could choose when signing the contract.

If I start a “IP location finder” request for the website, I can find the IP address, the location and the owner.



8. I can perform a zone transfer with the command “nslookup”. I can exploit zone transfer to gather useful information about the DNS server, the hostname and the IP address. If the response is from a non-authoritative server, this means that it can be an old information.

Firstly, I performed the query to know the name server of the target domain, using the NS type query:

```
C:\Users\Sara>nslookup -type=ns psicologiareba.it
Server: fritz.box
Address: 192.168.178.1

Risposta da un server non autorevole:
psicologiareba.it      nameserver = ns1.th.seeweb.it
psicologiareba.it      nameserver = ns2.th.seeweb.it

ns1.th.seeweb.it       internet address = 217.64.201.170
ns2.th.seeweb.it       internet address = 95.174.18.147
ns2.th.seeweb.it       AAAA IPv6 address = 2001:4b78:2100:2::1
```

Then, I performed a complete check that gave me a lot more information, using the ANY type query:

```
C:\Users\Sara>nslookup -type=any psicologiareba.it
Server: fritz.box
Address: 192.168.178.1

Risposta da un server non autorevole:
psicologiareba.it      AAAA IPv6 address = 2001:4b78:1001::1101
psicologiareba.it      text =

      "v=spf1 include:_spf.th.seeweb.it ?all"
psicologiareba.it      MX preference = 10, mail exchanger = m-11b.th.seeweb.it
psicologiareba.it      MX preference = 20, mail exchanger = smtp-avas-th.seeweb.it
psicologiareba.it      primary name server = ns1.th.seeweb.it
                        responsible mail addr = hostmaster.seeweb.it
                        serial = 1
                        refresh = 86400 (1 day)
                        retry = 7200 (2 hours)
                        expire = 2592000 (30 days)
                        default TTL = 21600 (6 hours)
psicologiareba.it      internet address = 217.64.195.204
psicologiareba.it      nameserver = ns2.th.seeweb.it
psicologiareba.it      nameserver = ns1.th.seeweb.it

psicologiareba.it      nameserver = ns1.th.seeweb.it
psicologiareba.it      nameserver = ns2.th.seeweb.it
ns1.th.seeweb.it       internet address = 217.64.201.170
ns2.th.seeweb.it       internet address = 95.174.18.147
ns2.th.seeweb.it       AAAA IPv6 address = 2001:4b78:2100:2::1
```

9. If I perform the traceroute, I obtain this result:

```
C:\> Prompt dei comandi

Microsoft Windows [Versione 10.0.18362.720]
(c) 2019 Microsoft Corporation. Tutti i diritti sono riservati.

C:\Users\Sara>tracert www.psicologiareba.it

Traccia instradamento verso www.psicologiareba.it [217.64.195.204]
su un massimo di 30 punti di passaggio:

 1  2 ms    2 ms    2 ms  fritz.box [192.168.178.1]
 2  3 ms    3 ms    3 ms  194.183.16.59
 3  3 ms    3 ms    5 ms  194-183-16-113.uni.it [194.183.16.113]
 4  4 ms    4 ms   21 ms  e5-1.a.nam.uni.net [213.233.30.21]
 5  4 ms    4 ms    3 ms  seeweb-nap.namex.it [193.201.28.23]
 6  6 ms    5 ms    5 ms  xe-2-3-0-45.kirk.fro2.seeweb.it [212.25.170.134]
 7  4 ms    6 ms    8 ms  cloud.fw-15a.fro2.seeweb.it [85.94.213.245]
 8  4 ms    4 ms    5 ms  w-11.th.seeweb.it [217.64.195.204]

Traccia completata.
```

This is the route that the ICMP packet follows to reach the destination from my client. Each row represents a hop in the route. The route could be different every time I perform this action because my packet could take another route, it depends on the best route calculated in that specific moment.