

# WEBSITE ENUMERATION & SCANNING





SERVER



LOGIN PAGE



SQL



89.173.11.111



NMAP  
NIKTO  
DIRB  
GOOGLE  
BURPSUITE  
...

TESLA



## Sign In

Email Address ⓘ

Password

SIGN IN

[Forgot email?](#) | [Forgot password?](#)

OR

CREATE ACCOUNT

Око 2.900 резултата (0,21 секунде/и)

www.tesla.com › Powerwall\_2\_Order\_NO\_Norway PDF

## Tesla Model S Reservation Agreement

28.10.2016. — Innkjøpsavtale. Etter gjennomført besøk i ditt lokale, vil du motta en Kjøpsavtale som angir de endelige spesifikasjonene for din. Powerwall ...

www.tesla.com › files › Powerwall\_2\_Order\_NL\_Dutch PDF

## Tesla Model S Reservation Agreement

Bezoek locatie. Uw Powerwall moet worden geïnstalleerd door een getrainde en gecertificeerde installateur. Een vertegenwoordiger van Tesla of van één van ...



www.tesla.com › sites › files › Powerwall\_2\_Order\_CA\_fr PDF

## Tesla Model S Reservation Agreement

Convention d'achat. Après la visite de site, vous recevrez la convention d'achat dans laquelle sont indiqués les spécifications définitives de votre installation de ...

www.tesla.com › files › Powerwall\_2\_Order\_SE\_Sweden PDF

## Tesla Model S Reservation Agreement

Око 1.050.000 резултата (0,47 секунде/и)

elearning.rcub.bg.ac.rs > ... > Elektrotehnički fakultet ▼

## ETF.PORT-2019-2020

Predmet: Praktikum iz osnova računarske tehnike. Nastavnik: prof. dr Zaharije Radivojević, zaki@etf.bg.ac.rs. Asistenti: Filip Hadžić, [hadzic.filip@etf.bg.ac.rs](mailto:hadzic.filip@etf.bg.ac.rs)

med.bg.ac.rs > 2020/06 > online-predprijava-uputstvo ▼ PDF

## Уласком на линк <https://upis-bgmed.etf.bg.ac.rs> кандидат ...

Уласком на линк <https://upis-bgmed.etf.bg.ac.rs> кандидат приступа онлајн веб предпријави. Први корак је регистрација кандидата. Кандидат прави налог ...

it-it.facebook.com > BG.ETF > posts > <https://www.etfbg.ac.rs>...

## <https://www.etf.bg.ac.rs/sr/vesti/2018/09...> - Facebook

<https://www.etf.bg.ac.rs/sr/vesti/2018/09/konkurs-za-upis-na-master-akademske-studije-u-skolskoj-2018-2019-godini>.

www.facebook.com > ETFEES > posts > <https://www.etfbg.ac.rs>...

## <https://www.etf.bg.ac.rs/sr/konkursi/2019...> - Facebook

Око 1.050.000 резултата (0,47 секунде/и)

elearning.rcub.bg.ac.rs > ... > Elektrotehnički fakultet ▼

## ETF.PORT-2019-2020

Predmet: Praktikum iz osnova računarske tehnike. Nastavnik: prof. dr Zaharije Radivojević, zaki@etf.bg.ac.rs. Asistenti: Filip Hadžić, hadzic.filip@etf.bg.ac.rs

med.bg.ac.rs > 2020/06 > online-predprijava-uputstvo ▼ PDF

## Уласком на линк <https://upis-bgmed.etf.bg.ac.rs> кандидат ...

Уласком на линк <https://upis-bgmed.etf.bg.ac.rs> кандидат приступа онлајн веб предпријави. Први корак је регистрација кандидата. Кандидат прави налог ...

it-it.facebook.com > BG.ETF > posts > <https://www.etfbg.ac.rs>...

## <https://www.etf.bg.ac.rs/sr/vesti/2018/09...> - Facebook

<https://www.etf.bg.ac.rs/sr/vesti/2018/09/konkurs-za-upis-na-master-akademske-studije-u-skolskoj-2018-2019-godini>.



Око 205 резултата (0,25 секунде/и)

**Да ли сте мислили:** **intitle:admin OR inurl:admin site:etf.bg.ac.rs**

lists.etf.bg.ac.rs › wws › subscribe · Преведи ову страницу

**rc-admin - RC-Admin - Mailing lists service**

email address : password : First login ? Lost password ? Subscribers: 4. Owners vladimir

lists.etf.bg.ac.rs › sigrequest › rc... ▾ Преведи ову страницу

**rc-admin - RC-Admin - Mailing lists service**

Please provide your email address for your unsubscription request from list rc-admin. Your e-mail address : §. Powered by Sympa 5.3.4.

admin.etf.bg.ac.rs › section-blog · Преведи ову страницу

**Example of Section Blog layout (FAQ section)**

The FTP Layer allows file operations (such as installing Extensions or updating the main configuration file) without having to make all the folders and files writable.

lists.etf.bg.ac.rs › help › admin · Преведи ову страницу





```
(mrhacker@kali) - [~]
```

```
$ ping 192.168.1.4
```

```
PING 192.168.1.4 (192.168.1.4) 56(84) bytes of data.
```

```
64 bytes from 192.168.1.4: icmp_seq=1 ttl=64 time=5.41 ms
```

```
64 bytes from 192.168.1.4: icmp_seq=2 ttl=64 time=0.745 ms
```

```
64 bytes from 192.168.1.4: icmp_seq=3 ttl=64 time=0.617 ms
```

```
64 bytes from 192.168.1.4: icmp_seq=4 ttl=64 time=0.501 ms
```

```
64 bytes from 192.168.1.4: icmp_seq=5 ttl=64 time=0.820 ms
```

```
64 bytes from 192.168.1.4: icmp_seq=6 ttl=64 time=0.783 ms
```

```
64 bytes from 192.168.1.4: icmp_seq=7 ttl=64 time=0.573 ms
```

```
64 bytes from 192.168.1.4: icmp_seq=8 ttl=64 time=0.818 ms
```

```
64 bytes from 192.168.1.4: icmp_seq=9 ttl=64 time=0.597 ms
```

```
64 bytes from 192.168.1.4: icmp_seq=10 ttl=64 time=0.785 ms
```

(mrhacker@kali) - [~]

\$ ping google.com

PING google.com (216.58.214.206) 56(84) bytes of data.

64 bytes from bud02s23-in-f206.1e100.net (216.58.214.206): icmp\_seq=1 ttl=118 time=34.6 ms

64 bytes from 206.214.58.216.in-addr.arpa (216.58.214.206): icmp\_seq=2 ttl=118 time=35.1 ms

64 bytes from 206.214.58.216.in-addr.arpa (216.58.214.206): icmp\_seq=3 ttl=118 time=40.1 ms

64 bytes from 206.214.58.216.in-addr.arpa (216.58.214.206): icmp\_seq=4 ttl=118 time=34.7 ms

64 bytes from 206.214.58.216.in-addr.arpa (216.58.214.206): icmp\_seq=5 ttl=118 time=35.0 ms

64 bytes from 206.214.58.216.in-addr.arpa (216.58.214.206): icmp\_seq=6 ttl=118 time=34.8 ms

64 bytes from 206.214.58.216.in-addr.arpa (216.58.214.206): icmp\_seq=7 ttl=118 time=34.7 ms

64 bytes from 206.214.58.216.in-addr.arpa (216.58.214.206): icmp\_seq=8 ttl=118 time=34.8 ms

^C

--- google.com ping statistics ---

8 packets transmitted, 8 received, 0% packet loss, time 7009ms

rtt min/avg/max/mdev = 34.560/35.457/40.071/1.750 ms

(mrhacker@kali) - [~]

```
(mrhacker@kali) - [~]
```

```
$ host tesla.com
```

```
tesla.com has address 199.66.11.62
```

```
tesla.com mail is handled by 10 us-smtp-inbound-1.mimecast.com.
```

```
tesla.com mail is handled by 10 us-smtp-inbound-2.mimecast.com.
```

```
(mrhacker@kali) - [~]
```

```
$ nslookup tesla.com
```

```
Server:          192.168.1.1
```

```
Address:         192.168.1.1#53
```

```
Non-authoritative answer:
```

```
Name:   tesla.com
```

```
Address: 199.66.11.62
```

```
;; Got recursion not available from 192.168.1.1, trying next server
```

```
(mrhacker@kali) - [~]
```

```
$ █
```



(mrhacker@kali)-[~]

\$ whois tesla.com

Domain Name: TESLA.COM

Registry Domain ID: 187902\_DOMAIN\_COM-VRSN

Registrar WHOIS Server: whois.markmonitor.com

Registrar URL: <http://www.markmonitor.com>

Updated Date: 2020-10-02T09:07:57Z

Creation Date: 1992-11-04T05:00:00Z

Registry Expiry Date: 2022-11-03T05:00:00Z

Registrar: MarkMonitor Inc.

Registrar IANA ID: 292

Registrar Abuse Contact Email: [abusecomplaints@markmonitor.com](mailto:abusecomplaints@markmonitor.com)

Registrar Abuse Contact Phone: +1.2083895740

Domain Status: clientDeleteProhibited <https://icann.org/epp#clientDeleteProhibited>

Domain Status: clientTransferProhibited <https://icann.org/epp#clientTransferProhibited>

Domain Status: clientUpdateProhibited <https://icann.org/epp#clientUpdateProhibited>

Domain Status: serverDeleteProhibited <https://icann.org/epp#serverDeleteProhibited>

Domain Status: serverTransferProhibited <https://icann.org/epp#serverTransferProhibited>

Domain Status: serverUpdateProhibited <https://icann.org/epp#serverUpdateProhibited>

Name Server: A1-12.AKAM.NET

Name Server: A10-67.AKAM.NET

Name Server: A12-64.AKAM.NET

Name Server: A28-65.AKAM.NET

Name Server: A7-66.AKAM.NET

Name Server: A9-67.AKAM.NET

Name Server: EDNS69.ULTRADNS.BIZ

Name Server: EDNS69.ULTRADNS.COM

Name Server: EDNS69.ULTRADNS.NET

Name Server: EDNS69.ULTRADNS.ORG

DNSSEC: unsigned

I

URL of the ICANN Whois Inaccuracy Complaint Form: <https://www.icann.org/wicf/>

>>> last update of whois database: 2021-03-01T08:47:34Z <<<

## Name Server Performance

Server	Resolved IP	TTL	Response Time (ms)	Status
ns2.google.com. [2001:4860:4802:34::a]	172.217.3.164	300	12	NOTICE
ns1.google.com. [2001:4860:4802:32::a]	172.217.3.164	300	44	NOTICE
ns3.google.com. [2001:4860:4802:36::a]	172.217.3.164	300	12	NOTICE
ns4.google.com. [2001:4860:4802:38::a]	172.217.3.164	300	45	NOTICE

## Namespace Server delegation

Root Server Glue IP mapping	Name Server mapping		Status
Root Server Glue IP	ns2.google.com.	216.239.34.10	OK
	ns1.google.com.	216.239.32.10	
	ns3.google.com.	216.239.36.10	
	ns4.google.com.	216.239.38.10	
216.239.34.10 [ns2.google.com.]	-		Possible DNS forwarding issue.
216.239.32.10 [ns1.google.com.]	-		Possible DNS forwarding issue.
216.239.36.10 [ns3.google.com.]	-		Possible DNS forwarding issue.
216.239.38.10 [ns4.google.com.]	-		Possible DNS forwarding issue.

## DNS Traversal - performed using b.root-servers.net.

Server	Name Servers	Response Time (ms)	Status
a.gtld-servers.net. [192.5.6.30]	ns2.google.com. ns1.google.com. ns3.google.com. ns4.google.com. ns2.google.com.	6	OK



File Actions Edit View Help

(mrhacker@kali) - [~]

\$ whatweb 192.168.1.4

http://192.168.1.4 [200 OK] Apache[2.2.14][mod\_mono/2.4.3,mod\_perl/2.0.4,mod\_python/3.3.1,mod\_ssl/2.2.14,proxy\_html/3.0.1], Country[RESERVED][ZZ], Email[admin@metacorp.com,admin@owaspbwa.org,bob@ateliergraphique.com,cycloneuser-3@cyclonetransfers.com,jack@metacorp.com,test@thebodgeitstore.com], HTML5, HTTPServer[Ubuntu Linux][Apache/2.2.14 (Ubuntu) mod\_mono/2.4.3 PHP/5.3.2-lubuntu4.30 with Suhosin-Patch proxy\_html/3.0.1 mod\_python/3.3.1 Python/2.6.5 mod\_ssl/2.2.14 OpenSSL/0.9.8k Phusion Passenger/4.0.38 mod\_perl/2.0.4 Perl/v5.10.1], IP[192.168.1.4], JQuery[1.3.2], OpenSSL[0.9.8k], PHP[5.3.2-lubuntu4.30][Suhosin-Patch], Passenger[4.0.38], Perl[5.10.1], Python[2.6.5], Script[text/javascript], Title[owaspbwa OWASP Broken Web Applications]

(mrhacker@kali) - [~]

\$



```
(mrhacker@kali) - [~]
$ whatweb --aggression 3 -v 192.168.1.4
WhatWeb report for http://192.168.1.4
Status      : 200 OK
Title       : owaspbwa OWASP Broken Web Applications
IP          : 192.168.1.4
Country     : RESERVED, ZZ

Summary     : HTTPServer[Ubuntu Linux][Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-lubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1], Python[2.6.5], OpenSSL[0.9.8k], Email[admin@metacorp.com,admin@owaspbwa.org,bob@ateliergraphique.com,cycloneuser-3@cyclonetransfers.com,jack@metacorp.com,test@thebodgeitstore.com], Perl[5.10.1], Passenger[4.0.38], HTML5, JQuery[1.3.2], PHP[5.3.2-lubuntu4.30][Suhosin-Patch], Apache[2.2.14][mod_mono/2.4.3,mod_perl/2.0.4,mod_python/3.3.1,mod_ssl/2.2.14,proxy_html/3.0.1], Script[text/javascript]

Detected Plugins:
[ Apache ]
The Apache HTTP Server Project is an effort to develop and maintain an open-source HTTP server for modern operating systems including UNIX and Windows NT. The goal of this project is to provide a secure, efficient and extensible server that provides HTTP services in sync with the current HTTP standards.

Version      : 2.2.14 (from HTTP Server Header)
Module       : mod_mono/2.4.3,mod_perl/2.0.4,mod_python/3.3.1,mod_ssl/2.2.14
Module       : proxy_html/3.0.1
Google Dorks : (3)
Website      : http://httpd.apache.org/

[ Email ]
Extract email addresses. Find valid email address and syntactically invalid email addresses from mailto: link tags. We match syntactically invalid links containing
```

File Actions Edit View Help

(mrhacker@kali) - [~]

\$ whatweb --aggression 3 -v 192.168.1.1/24 --no-errors

```
(mrhacker@kali) - [~]  
$ dirb http://192.168.1.4
```

```
-----  
DIRB v2.22  
By The Dark Raver  
-----
```

```
START_TIME: Wed Mar 3 03:40:41 2021  
URL_BASE: http://192.168.1.4/  
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
```

```
-----  
GENERATED WORDS: 4612
```

```
---- Scanning URL: http://192.168.1.4/ ----  
+ http://192.168.1.4/.bash_history (CODE:200|SIZE:302)  
-> Testing: http://192.168.1.4/abstract
```



---- Entering directory: http://192.168.1.4/evil/ ----  
(!) WARNING: Directory IS LISTABLE. No need to scan it.  
(Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.4/gallery2/ ----  
+ http://192.168.1.4/gallery2/config (CODE:500|SIZE:0)  
+ http://192.168.1.4/gallery2/embed (CODE:200|SIZE:0)  
==> DIRECTORY: http://192.168.1.4/gallery2/images/  
+ http://192.168.1.4/gallery2/index (CODE:302|SIZE:0)  
+ http://192.168.1.4/gallery2/index.php (CODE:302|SIZE:0)  
==> DIRECTORY: http://192.168.1.4/gallery2/lib/  
+ http://192.168.1.4/gallery2/LICENSE (CODE:200|SIZE:18011)  
+ http://192.168.1.4/gallery2/login (CODE:200|SIZE:33)  
+ http://192.168.1.4/gallery2/main (CODE:200|SIZE:5887)  
==> DIRECTORY: http://192.168.1.4/gallery2/modules/  
+ http://192.168.1.4/gallery2/README (CODE:200|SIZE:73808)  
==> DIRECTORY: http://192.168.1.4/gallery2/themes/

---- Entering directory: http://192.168.1.4/icon/ ----  
==> DIRECTORY: http://192.168.1.4/icon/browser/  
==> DIRECTORY: http://192.168.1.4/icon/clock/  
==> DIRECTORY: http://192.168.1.4/icon/flags/  
==> DIRECTORY: http://192.168.1.4/icon/os/



```
(mrhacker@kali) - [~]  
$ dirb http://192.168.1.4 /usr/share/wordlists/dirb/common.txt
```

```
-----  
DIRB v2.22  
By The Dark Raver  
-----
```

```
START_TIME: Wed Mar 3 03:44:33 2021  
URL_BASE: http://192.168.1.4/  
WORDLIST_FILES: /usr/share/wordlists/dirb/common.txt
```

```
-----  
GENERATED WORDS: 4612
```

```
---- Scanning URL: http://192.168.1.4/ ----  
+ http://192.168.1.4/.bash_history (CODE:200|SIZE:302)  
==> DIRECTORY: http://192.168.1.4/assets/  
-> Testing: http://192.168.1.4/cfc
```

# Index of /images

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
-------------	----------------------	-------------	--------------------

---

 <a href="#">Parent Directory</a>		-	
 <a href="#">Knob_Add.png</a>	01-May-2011 23:07	4.2K	
 <a href="#">Knob_Attention.png</a>	16-Apr-2011 15:57	4.5K	
 <a href="#">mandiant.png</a>	18-Jun-2015 21:57	1.8K	
 <a href="#">owasp.png</a>	22-Apr-2011 16:43	70K	

---



## Welcome to phpMyAdmin

Language


English

Log in

Username:

Password:

Go

 Cookies must be enabled past this point.

## Nmap Reference Guide

nmap - Network exploration tool and security / port scanner

```
nmap [Scan Type...] [Options] {target specification}
```

Nmap ("Network Mapper") is an open source tool for network exploration and security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they're running, what type of packet filters/firewalls are in use, and dozens of other characteristics. While Nmap is commonly used for security audits, many systems and network administrators find it useful for routine tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

The output from Nmap is a list of scanned targets, with supplemental information on each depending on the options used. Key information is the "interesting ports table". That table lists the port number and protocol, service name, and state. The state is either open, filtered, closed, or unfiltered. Open means that an application on the target machine is listening for connections/packets on that port. Filtered means that a firewall, filter, or other network obstacle is blocking the port so that Nmap cannot tell whether it is open or closed. Closed ports have no application listening on them, though they could open up at any time. Ports are classified as unfiltered when they are responsive to Nmap's probes, but Nmap cannot determine whether they are open or closed. Nmap reports the state combinations open|filtered and closed|filtered when it cannot determine which of the two states describe a port. The port table may also include software version details when version detection has been requested. When an IP protocol scan is requested (`-s0`), Nmap provides information on supported IP protocols rather than listening ports.

In addition to the interesting ports table, Nmap can provide further information on targets, including reverse DNS names, operating system guesses, device types, and MAC addresses.

A typical Nmap scan is shown in Example 1. The only Nmap arguments used in this example are **-A**, to enable OS and version detect script scanning, and **traceroute**; **-T4** for faster execution; and then the hostname.

### Example 1. A representative Nmap scan



```
(mrhacker@kali) - [~]  
$ nmap 192.168.1.4  
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-03 03:53 EST  
Nmap scan report for owaspbwa (192.168.1.4)  
Host is up (0.0013s latency).  
Not shown: 991 closed ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
80/tcp    open  http  
139/tcp   open  netbios-ssn  
143/tcp   open  imap  
443/tcp   open  https  
445/tcp   open  microsoft-ds  
5001/tcp  open  complex-link  
8080/tcp  open  http-proxy  
8081/tcp  open  blackice-icecap  
  
Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
```



(mrhacker@kali) - [~]

\$ nmap -sV 192.168.1.4

Starting Nmap 7.91 ( <https://nmap.org> ) at 2021-03-03 03:55 EST

Nmap scan report for owaspbwa (192.168.1.4)

Host is up (0.00100s latency).

Not shown: 991 closed ports

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

22/tcp	open	ssh	OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol 2.0)
--------	------	-----	--

80/tcp	open	http	Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL...)
--------	------	------	---

139/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
---------	------	-------------	---

143/tcp	open	imap	Courier Imapd (released 2008)
---------	------	------	-------------------------------

443/tcp	open	ssl/https?	
---------	------	------------	--

445/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
---------	------	-------------	---

5001/tcp	open	java-object	Java Object Serialization
----------	------	-------------	---------------------------

8080/tcp	open	http	Apache Tomcat/Coyote JSP engine 1.1
----------	------	------	-------------------------------------

8081/tcp	open	http	Jetty 6.1.25
----------	------	------	--------------

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-Port5001-TCP:V=7.91%I=7%D=3/3%Time=603F4EF4%P=x86\_64-pc-linux-gnu%r(NUL

SF:L,4,"\xac\xed\0\x05");

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

File Actions Edit View Help

(mrhacker@kali) - [~]

\$ nmap --script vuln 192.168.1.4

Starting Nmap 7.91 ( <https://nmap.org> ) at 2021-03-03 03:58 EST

Pre-scan script results:

| broadcast-avahi-dos:

| Discovered hosts:

| 224.0.0.251

| After NULL UDP avahi packet DoS (CVE-2011-1002).

| Hosts are all up (not vulnerable).

Stats: 0:00:50 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan

NSE Timing: About 83.57% done; ETC: 03:59 (0:00:03 remaining)

Stats: 0:00:52 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan

NSE Timing: About 83.57% done; ETC: 03:59 (0:00:03 remaining)



NSE Timing: About 99.76% done; ETC: 04:04 (0:00:01 remaining)  
Stats: 0:06:43 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan  
NSE Timing: About 99.76% done; ETC: 04:04 (0:00:01 remaining)  
Stats: 0:06:44 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan  
NSE Timing: About 99.76% done; ETC: 04:04 (0:00:01 remaining)  
Stats: 0:06:44 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan  
NSE Timing: About 99.76% done; ETC: 04:04 (0:00:01 remaining)  
Stats: 0:06:47 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan  
NSE Timing: About 99.88% done; ETC: 04:05 (0:00:00 remaining)  
Nmap scan report for owaspbwa (192.168.1.4)  
Host is up (0.0018s latency).

Not shown: 991 closed ports

PORT STATE SERVICE

22/tcp open ssh

80/tcp open http

http-cross-domain-policy:

VULNERABLE:

Cross-domain and Client Access policies.

State: VULNERABLE

A cross-domain policy file specifies the permissions that a web client such as Java, Adobe Flash, Adobe Reader, etc. use to access data across different domains. A client access policy file is similar to cross-domain policy but is used for M\$ Silverlight applications. Overly permissive configurations enables Cross-site Request Forgery attacks, and may allow third parties to access sensitive data meant for the user.

Check results:

/crossdomain.xml:

```
<?xml version="1.0"?>
<!DOCTYPE cross-domain-policy SYSTEM "http://www.macromedia.com/xml/dtds/cross-domain-policy.dtd">
<cross-domain-policy>
  <allow-access-from domain="*" />
</cross-domain-policy>
```

Extra information:

Extra information:  
Trusted domains:\*

## References:

[https://www.owasp.org/index.php/Test\\_RIA\\_cross\\_domain\\_policy\\_%28TG-CONFIG-008%29](https://www.owasp.org/index.php/Test_RIA_cross_domain_policy_%28TG-CONFIG-008%29)  
<http://sethsec.blogspot.com/2014/03/exploiting-misconfigured-crossdomainxml.html>  
<http://acunetix.com/vulnerabilities/web/insecure-clientaccesspolicy-xml-file>  
[https://www.adobe.com/devnet-docs/acrobatetk/tools/AppSec/CrossDomain\\_PolicyFile\\_Specification](https://www.adobe.com/devnet-docs/acrobatetk/tools/AppSec/CrossDomain_PolicyFile_Specification)  
[https://www.adobe.com/devnet/articles/crossdomain\\_policy\\_file\\_spec.html](https://www.adobe.com/devnet/articles/crossdomain_policy_file_spec.html)  
<http://gursevkalra.blogspot.com/2013/08/bypassing-same-origin-policy-with-flash.html>

http-csrf:

Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=owaspbwa

Found the following possible CSRF vulnerabilities:

Path: <http://owaspbwa:80/shepherd/login.jsp>

Form id:

Form action: login

Path: <http://owaspbwa:80/dom-xss-example.html>

Form id:

Form action: '+location.href+'

Path: <http://owaspbwa:80/ghost/>

Form id:

Form action: submit.php

Path: <http://owaspbwa:80/gallery2/main.php>

Form id: search searchblock



```
(mrhacker@kali) - [~]
```

```
$ nikto
```

```
- Nikto v2.1.6
```

```
+ ERROR: No host or URL specified
```

```
-config+      Use this config file
-Display+     Turn on/off display outputs
-dbcheck      check database and other key files for syntax errors
-Format+      save file (-o) format
-Help         Extended help information
-host+        target host/URL
-id+          Host authentication to use, format is id:pass or id:pass:realm
-list-plugins List all available plugins
-output+      Write output to this file
-nossl        Disables using SSL
-no404        Disables 404 checks
-Plugins+     List of plugins to run (default: ALL)
-port+        Port to use (default 80)
-root+        Prepend root value to all requests, format is /directory
-ssl          Force ssl mode on port
-Tuning+      Scan tuning
-timeout+     Timeout for requests (default 10 seconds)
-update       Update databases and plugins from CIRT.net
-Version      Print plugin and database versions
-vhost+       Virtual host (for Host header)
```

```
+ requires a value
```

Note: This is the short help output. Use -H for full help text.

```
(mrhacker@kali) - [~]
```



```
File Actions Edit View Help

(mrhacker@kali)-[~]
$ nikto -host 192.168.1.5
- Nikto v2.1.6
-----
+ Target IP: 192.168.1.5
+ Target Hostname: 192.168.1.5
+ Target Port: 80
+ Start Time: 2021-03-06 05:52:07 (GMT-5)
-----
+ Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-lubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
+ Server may leak inodes via ETags, header found with file /, inode: 286483, size: 28067, mtime: Thu Jul 30 22:55:52 2015
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ OSVDB-3268: /cgi-bin/: Directory indexing found.
+ /crossdomain.xml contains a full wildcard entry. See http://jeremiahgrossman.blogspot.com/2008/05/crossdomainxml-invites-cross-site.html
+ Apache/2.2.14 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ PHP/5.3.2-lubuntu4.30 appears to be outdated (current is at least 7.2.12). PHP 5.6.33, 7.0.27, 7.1.13, 7.2.1 may also current release for each branch.
+ mod_ssl/2.2.14 appears to be outdated (current is at least 2.8.31) (may depend on server version)
+ OpenSSL/0.9.8k appears to be outdated (current is at least 1.1.1). OpenSSL 1.0.0o and 0.9.8zc are also current.
+ Perl/v5.10.1 appears to be outdated (current is at least v5.20.0)
+ Phusion_Passenger/4.0.38 appears to be outdated (current is at least 4.0.53)
+ mod_mono/2.4.3 appears to be outdated (current is at least 2.8)
+ proxy_html/3.0.1 appears to be outdated (current is at least 3.1.2)
+ mod_perl/2.0.4 appears to be outdated (current is at least 2.0.8)
+ Python/2.6.5 appears to be outdated (current is at least 2.7.8)
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: index.css, index.html
+ OSVDB-39272: /favicon.ico file identifies this app/server as: owasp.org
+ IP address found in the 'location' header. The IP is "127.0.1.1".
```