



bugcrowd.com

Cross Site Scripting

```
root@kali:~/Desktop/tools/Sublist3r# python sublist3r.py -d tesla.com
```

Sublist3r

Coded By Ahmed Aboul-Ela - @aboul3la

```
[*] Enumerating subdomains now for tesla.com
[*] Searching now in Baidu..
[*] Searching now in Yahooe..
[*] Searching now in Google..
[*] Searching now in Bing..
[*] Searching now in Ask..
[*] Searching now in Netcraft..
[*] Searching now in DNSdumpster..
[*] Searching now in Virustotal..
[*] Searching now in ThreatCrowd..
[*] Searching now in SSL Certificates..
[*] Searching now in PassiveDNS..
[!] Error: Google probably now is blocking our requests
[*] Finished now the Google Enumeration ...
[*] Total Unique Subdomains Found: 36
```


```
www.tesla.com
auth.tesla.com
autodiscover.tesla.com
blog.tesla.com
comparison.tesla.com
dev.tesla.com
eva-origin.tesla.com
forums.tesla.com
imap.tesla.com
ir.tesla.com
lyncdiscover.tesla.com
model3.tesla.com
my.tesla.com
naa-origin.tesla.com
nas-origin.tesla.com
new.tesla.com
new-dev.tesla.com
partners.tesla.com
pop.tesla.com
powerwall.tesla.com
resources.tesla.com
shop.tesla.com
sling.tesla.com
smtp.tesla.com
```

Lab Description

Lab Description

For the Cross Site Scripting Testing module we will be suggesting OSS labs from [bWapp \(an extremely buggy web application\)](#) written by Malik Mesellem.

bWapp hosts several individual XSS challenges for a newcomer including variants of both stored and reflected xss, in several contexts, and input locations.



an extremely buggy web app !

Choose your bug:

----- bWAPP v2.2 ----- ▾

Hack

Set your security level:

low ▾

Set

Current: low

BugsChange PasswordCreate UserSet Security LevelResetCreditsBlogLogoutWelcome Bee





/ XSS - Reflected (POST) /


Enter your first and last name:

First name:

Last name:

Go





an extremely buggy web app !

Choose your bug:

----- bWAPP v2.2 ----- ▾

Hack

Set your security level:

low ▾

Set





Current: low

BugsChange PasswordCreate UserSet Security LevelResetCreditsBlogLogoutWelcome Bee

/ XSS - Reflected (AJAX/JSON) /

Search for a movie:

HINT: our master really loves Marvel movies :)



Lab Description - bwapp

[bWapp \(an extremely buggy web application\)](#) can be quickly stood up by downloading it's virtual machine version on Sourceforge, called bee-box:

- <https://sourceforge.net/projects/bwapp/files/bee-box/>

Use VMware Player to start up this application. The provided INSTALL.txt file will give you credentials to start up the application and administer it from the server side if necessary.

For [bWapp \(an extremely buggy web application\)](#) we suggest you do the following sections:

Bwapp Section - A3 - Cross-Site Scripting (XSS)

Cross-Site Scripting - Reflected (GET)
Cross-Site Scripting - Reflected (POST)
Cross-Site Scripting - Reflected (JSON)
Cross-Site Scripting - Reflected (AJAX/JSON)
Cross-Site Scripting - Reflected (AJAX/XML)
Cross-Site Scripting - Reflected (Back Button)
Cross-Site Scripting - Reflected (Custom Header)
Cross-Site Scripting - Reflected (Eval)
Cross-Site Scripting - Reflected (HREF)
Cross-Site Scripting - Reflected (Login Form)

Cross-Site Scripting - Reflected (phpMyAdmin)
Cross-Site Scripting - Reflected (PHP_SELF)
Cross-Site Scripting - Reflected (Referer)
Cross-Site Scripting - Reflected (User-Agent)
Cross-Site Scripting - Stored (Blog)
Cross-Site Scripting - Stored (Change Secret)
Cross-Site Scripting - Stored (Cookies)
Cross-Site Scripting - Stored (SQLiteManager)
Cross-Site Scripting - Stored (User-Agent)