bugcrowd.com

Broken Access Control Testing

Bugcrowd Open Source Software Lab Guide

Lab Description

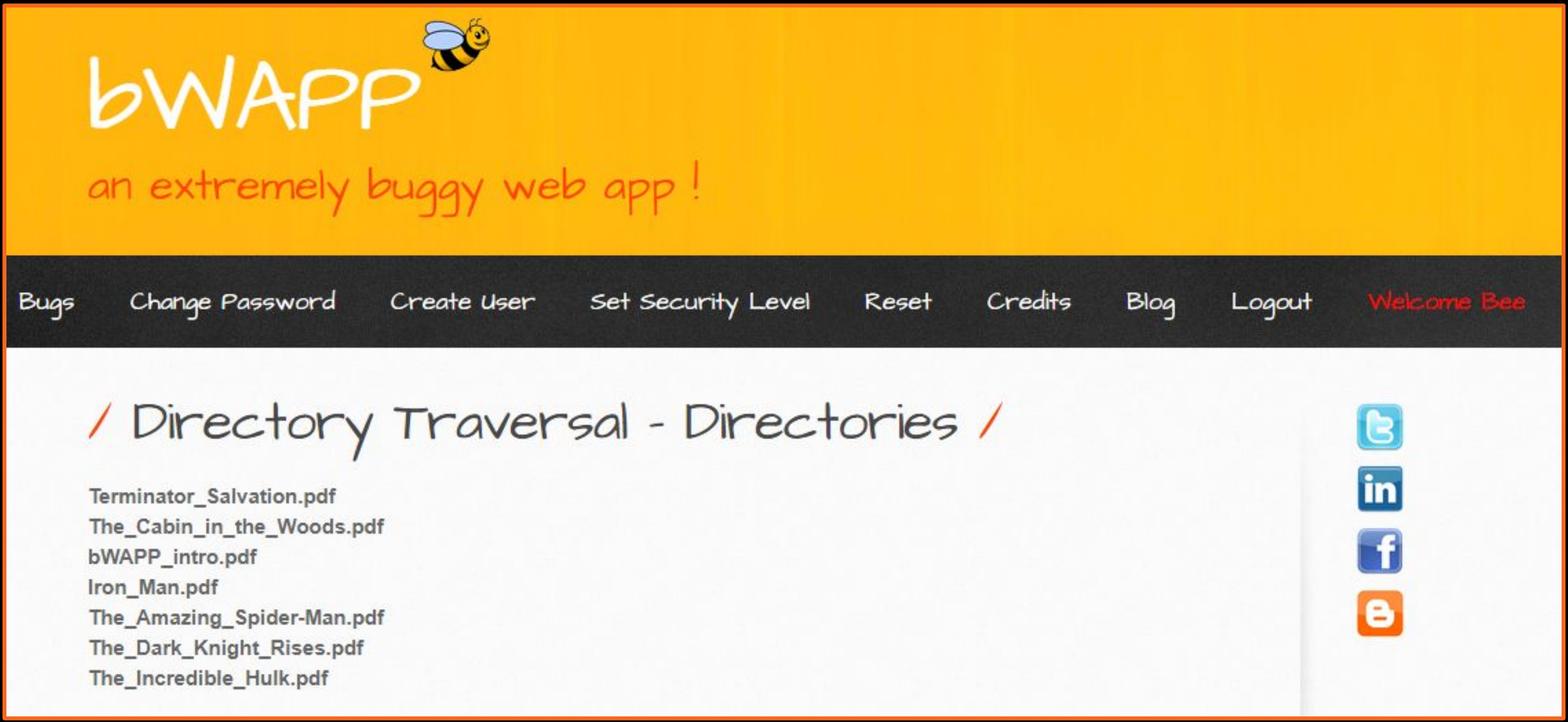
```
root@kali:~/Desktop/tools/Sublist3r# python sublist3r.py -d tesla.com

# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for tesla.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] 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
eua-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
```

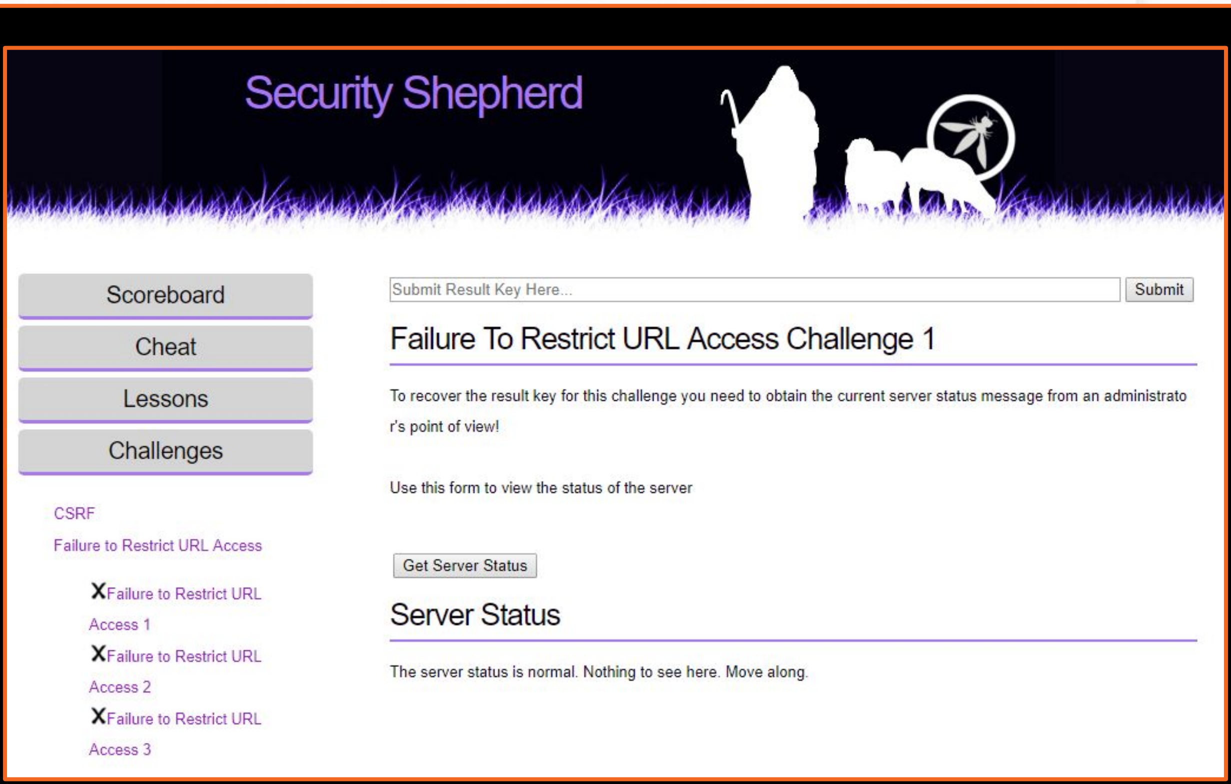
Lab Description

For the Broken Access Controls Testing module we will be suggesting OSS labs from two projects called bWapp (an extremely buggy web application) written by Malik Mesellem and OWASP Security Shepherd by Mark Denihan and Sean Duggan.



/ Directory Traversal - Directories /

Terminator_Salvation.pdf
The_Cabin_in_the_Woods.pdf
bWAPP_intro.pdf
Iron_Man.pdf
The_Amazing_Spider-Man.pdf
The_Dark_Knight_Rises.pdf
The_Incredible_Hulk.pdf


Security Shepherd
Scoreboard
Cheat
Lessons
Challenges
CSRF
Failure to Restrict URL Access
XFailure to Restrict URL Access 1
XFailure to Restrict URL Access 2
XFailure to Restrict URL Access 3
Submit Result Key Here...
Submit
Get Server Status

Failure To Restrict URL Access Challenge 1

To recover the result key for this challenge you need to obtain the current server status message from an administrator's point of view!

Use this form to view the status of the server

Server Status

The server status is normal. Nothing to see here. Move along.

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 - A4 - Insecure Direct Object Reference

Insecure DOR (Change Secret)
Insecure DOR (Reset Secret)
Insecure DOR (Order Tickets)

Bwapp Section - A7 - Missing Functional Level Access Control

Directory Traversal - Directories
Directory Traversal - Files
Local File Inclusion (SQLiteManager)
Remote & Local File Inclusion (RFI/LFI)
Restrict Device Access
Restrict Folder Access

Lab Description - OWASP Security Shepherd

OWASP Security Shepherd can be quickly stood up by downloading it’s virtual machine version on Github. Look for the newest release and file that ends with “Vm”:

- (current)https://github.com/OWASP/SecurityShepherd/releases/download/v3.0/owaspSecurityShepherdVm_V3.0.zip

Use VMware Player to start up this application.

For OWASP Security Shepherd we suggest you do the following sections:

Security Shepherd **Lesson** - Failure To Restrict URL Access
Security Shepherd **Lesson** - Insecure Direct Object References

Security Shepherd **Challenges** - Failure To Restrict URL Access

Failure to Restrict URL Access 1
Failure to Restrict URL Access 2
Failure to Restrict URL Access 3

Security Shepherd **Challenges** - Failure To Restrict URL Access

Insecure Direct Object Reference Bank Challenge
Insecure Direct Object References Challenge One
Insecure Direct Object References Challenge Two

Security Shepherd **Challenges** - Poor Data Validation

Poor Data Validation 1
Poor Data Validation 2