ATTACK DEFENSE

by PentesterAcademy

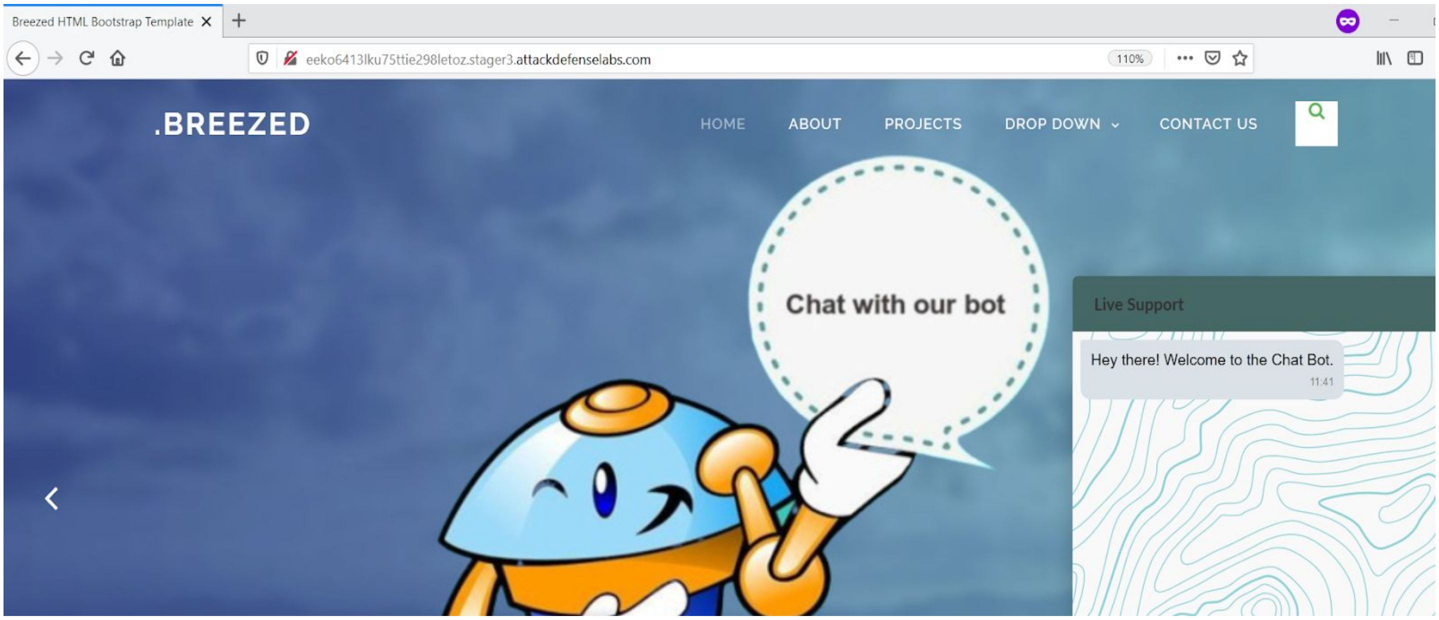
Name	Botman: SSRF
URL	https://www.attackdefense.com/challengedetails?cid=2183
Type	Web Technology : Bot Attacks

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 SSRF attack.

Step 1: Inspect the web application.



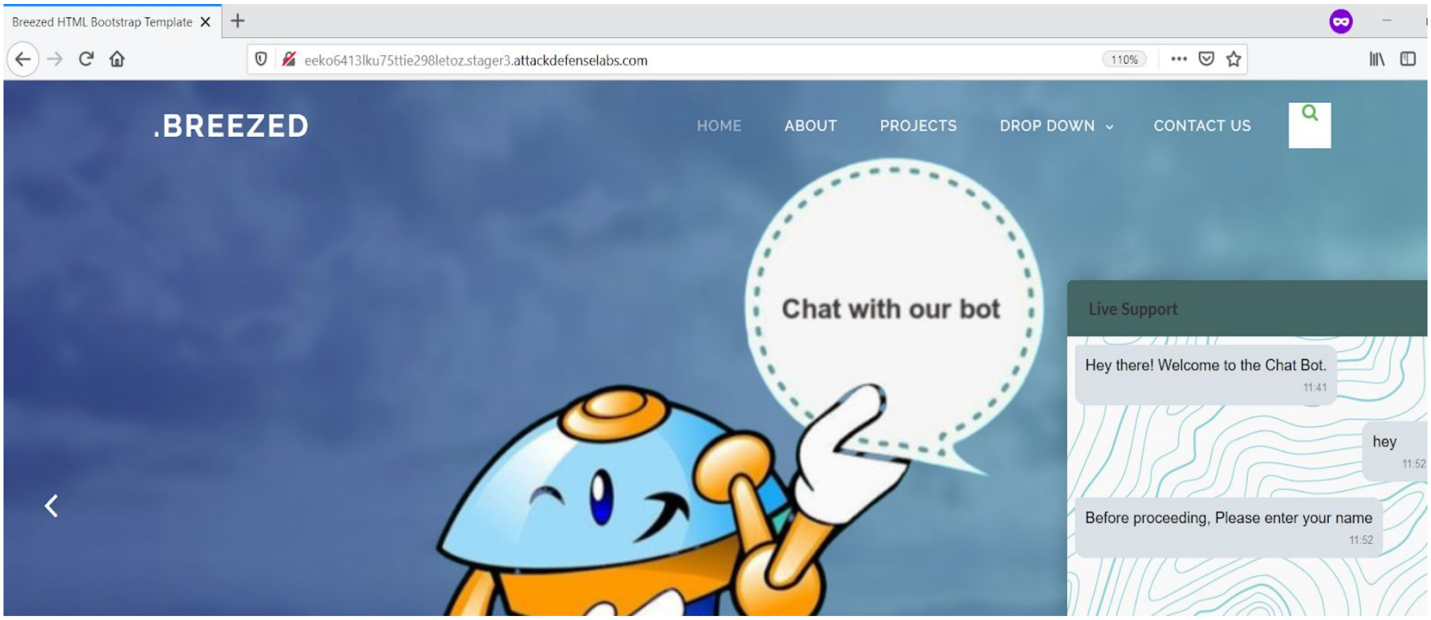
Breezed HTML Bootstrap Template

eeko6413lku75ttie298letoz.stager3.attackdefenselabs.com

Live Support

Hey there! Welcome to the Chat Bot. 11:41

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

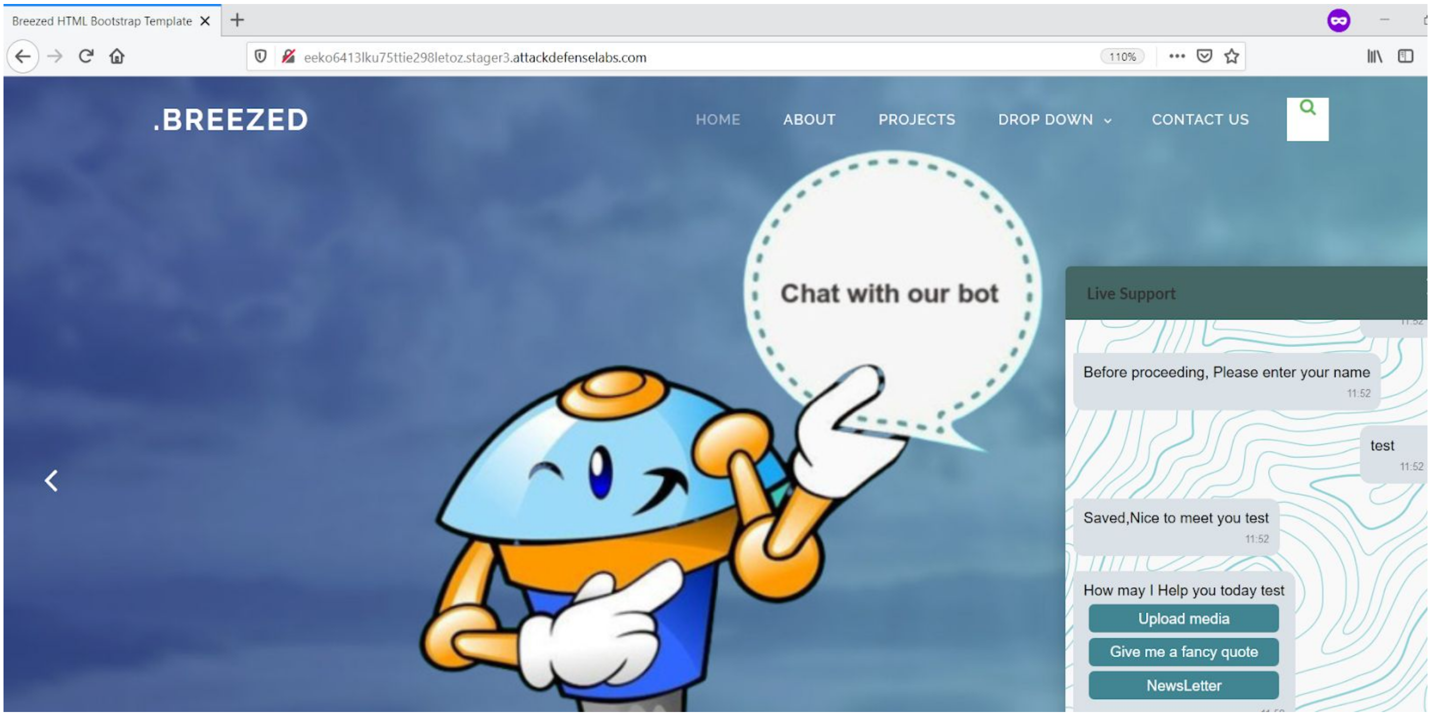

Breezed HTML Bootstrap Template
eeko6413lku75ttie298letoz.stager3.attackdefenselabs.com
110%
.BREEZED
HOME
ABOUT
PROJECTS
DROP DOWN
CONTACT US
Chat with our bot
Live Support

Hey there! Welcome to the Chat Bot. 11:41

hey 11:52

Before proceeding, Please enter your name 11:52

Step 3: Enter a name in the message.



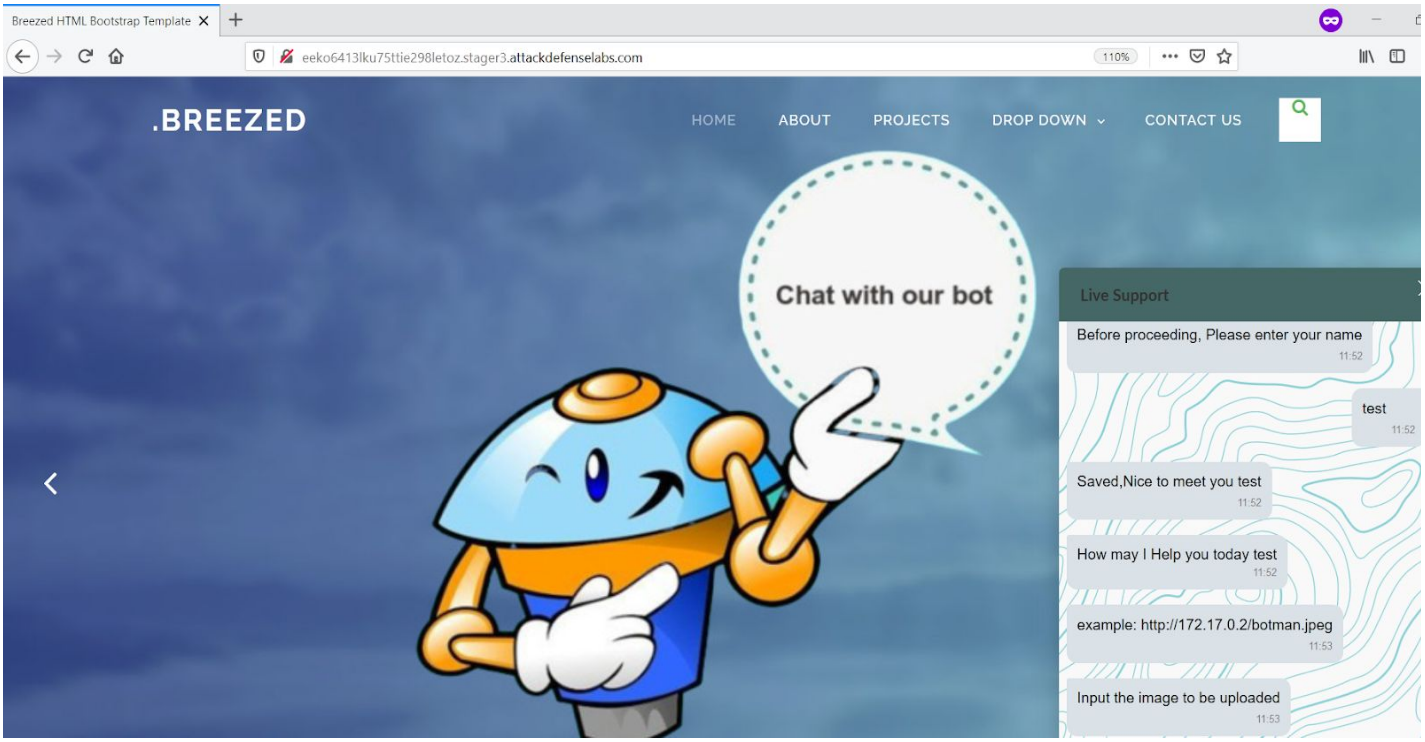
Before proceeding, Please enter your name 11:52

test 11:52

Saved,Nice to meet you test 11:52

How may I Help you today test

Click on the “Upload media” button.


Breezed HTML Bootstrap Template
eeko6413lku75ttie298letoz.stager3.attackdefenselabs.com
110%
.BREEZED
HOME
ABOUT
PROJECTS
DROP DOWN
CONTACT US
Chat with our bot
Live Support

Before proceeding, Please enter your name 11:52

test 11:52

Saved,Nice to meet you test 11:52

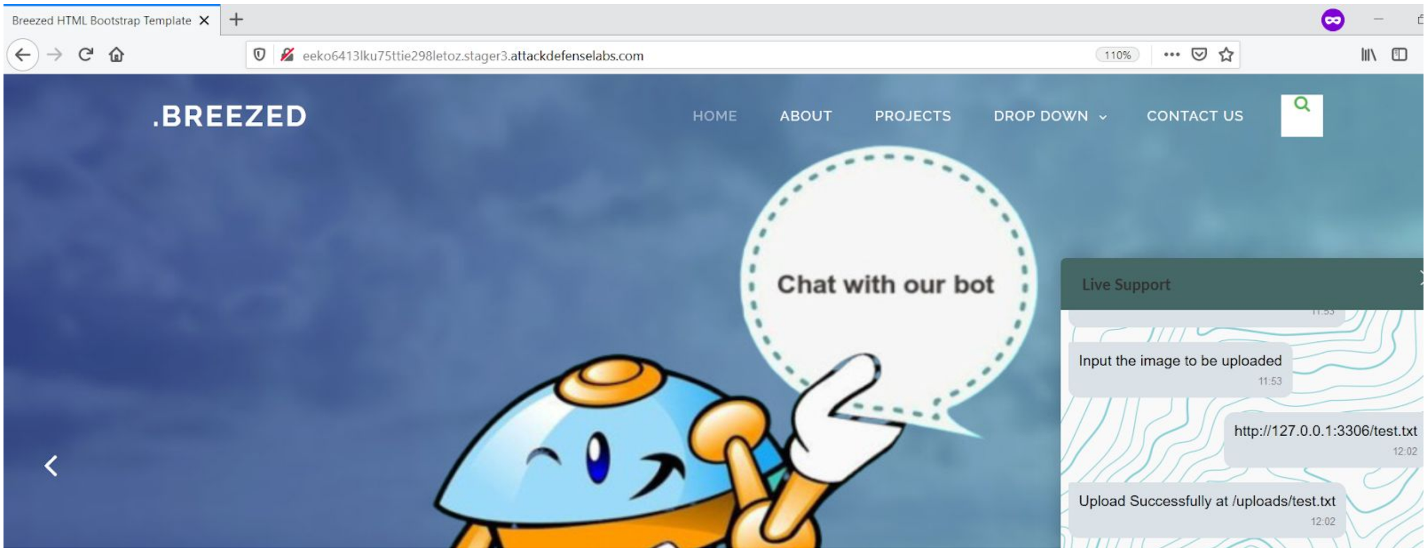
How may I Help you today test 11:52

example: http://172.17.0.2/botman.jpeg 11:53

Input the image to be uploaded 11:53

Step 4: Inject the SSRF payload to retrieve the version of MySQL Server.

Payload: http://127.0.0.1:3306/test.txt


Breezed HTML Bootstrap Template
eeko6413lku75ttie298letoz.stager3.attackdefenselabs.com
110%
.BREEZED
HOME
ABOUT
PROJECTS
DROP DOWN
CONTACT US
Chat with our bot
Live Support

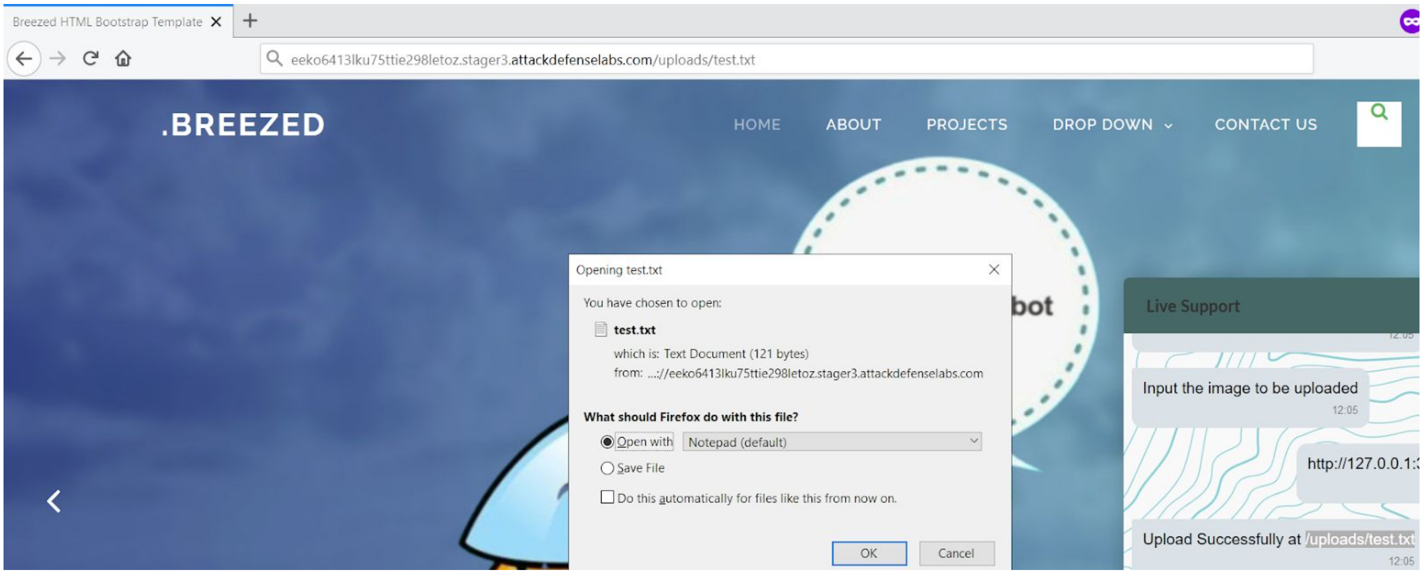
Input the image to be uploaded 11:53

http://127.0.0.1:3306/test.txt 12:02

Upload Successfully at /uploads/test.txt 12:02

Step 5: Navigate to the file path provided.

URL: http://eeko6413lku75ttie298letoz.stager3.attackdefenselabs.com/uploads/test.txt


Breezed HTML Bootstrap Template
eeko6413lku75ttie298letoz.stager3.attackdefenselabs.com/uploads/test.txt
.BREEZED
HOME
ABOUT
PROJECTS
DROP DOWN
CONTACT US
bot
Live Support

Opening test.txt

You have chosen to open:

test.txt

which is: Text Document (121 bytes)

from: ...://eeko6413lku75ttie298letoz.stager3.attackdefenselabs.com

What should Firefox do with this file?

● Open with Notepad (default)

○ Save File

□ Do this automatically for files like this from now on.

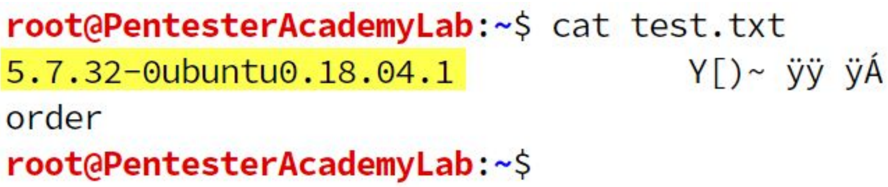
OK Cancel

Input the image to be uploaded 12:05

http://127.0.0.1:

Upload Successfully at /uploads/test.txt 12:05

Step 6: Click on download and check the contents of the file and retrieve the version.



```
root@PentesterAcademyLab:~$ cat test.txt
5.7.32-0ubuntu0.18.04.1          Y[)~ ÿÿ ÿÁ
order
root@PentesterAcademyLab:~$
```

Flag: 5.7.32-0ubuntu0.18.04.1

References:

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