ATTACK DEFENSE

by PentesterAcademy

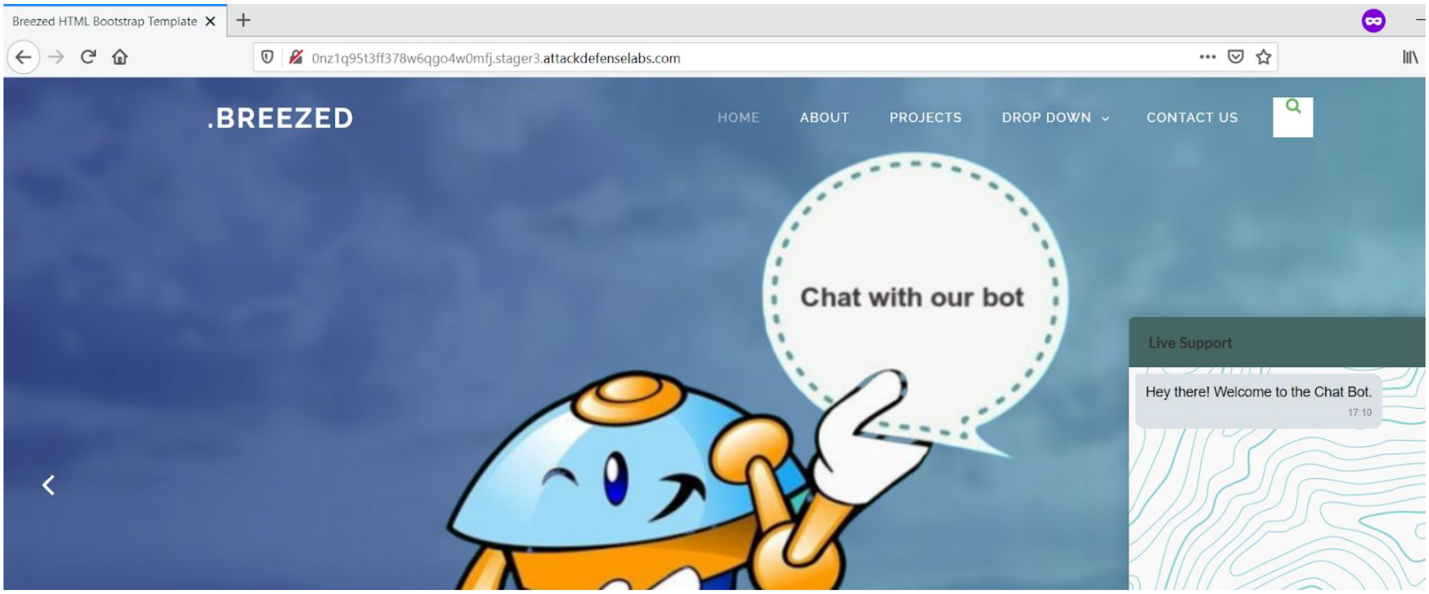
Name	Botman: XSS
URL	https://www.attackdefense.com/challengedetails?cid=2178
Type	Web Technology : Bot Attacks

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:

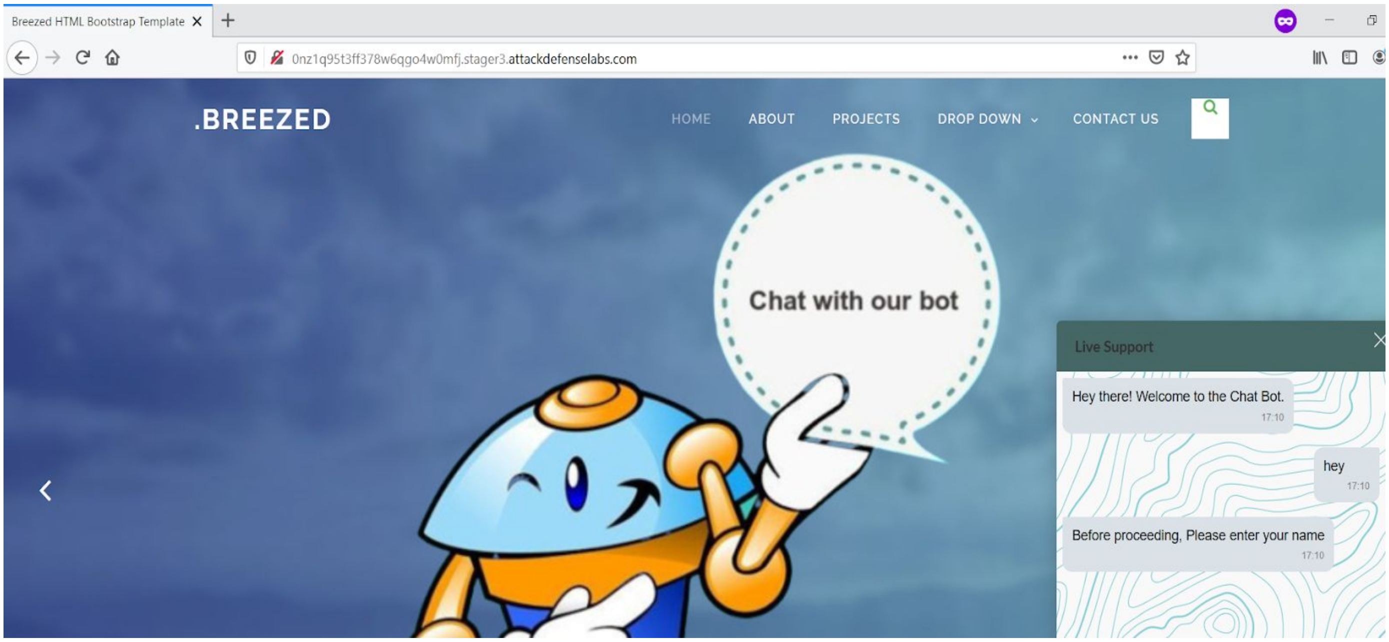
The web application is vulnerable to Stored XSS attack.

Step 1: Inspect the web application.


Breezed HTML Bootstrap Template
0nz1q95t3ff378w6qgo4w0mfj.stager3.attackdefenselabs.com
.BREEZED
HOME
ABOUT
PROJECTS
DROP DOWN
CONTACT US
Chat with our bot
Live Support

Hey there! Welcome to the Chat Bot.
17:10

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


Breezed HTML Bootstrap Template
0nz1q95t3ff378w6qgo4w0mfj.stager3.attackdefenselabs.com
.BREEZED
HOME
ABOUT
PROJECTS
DROP DOWN
CONTACT US
Chat with our bot
Live Support

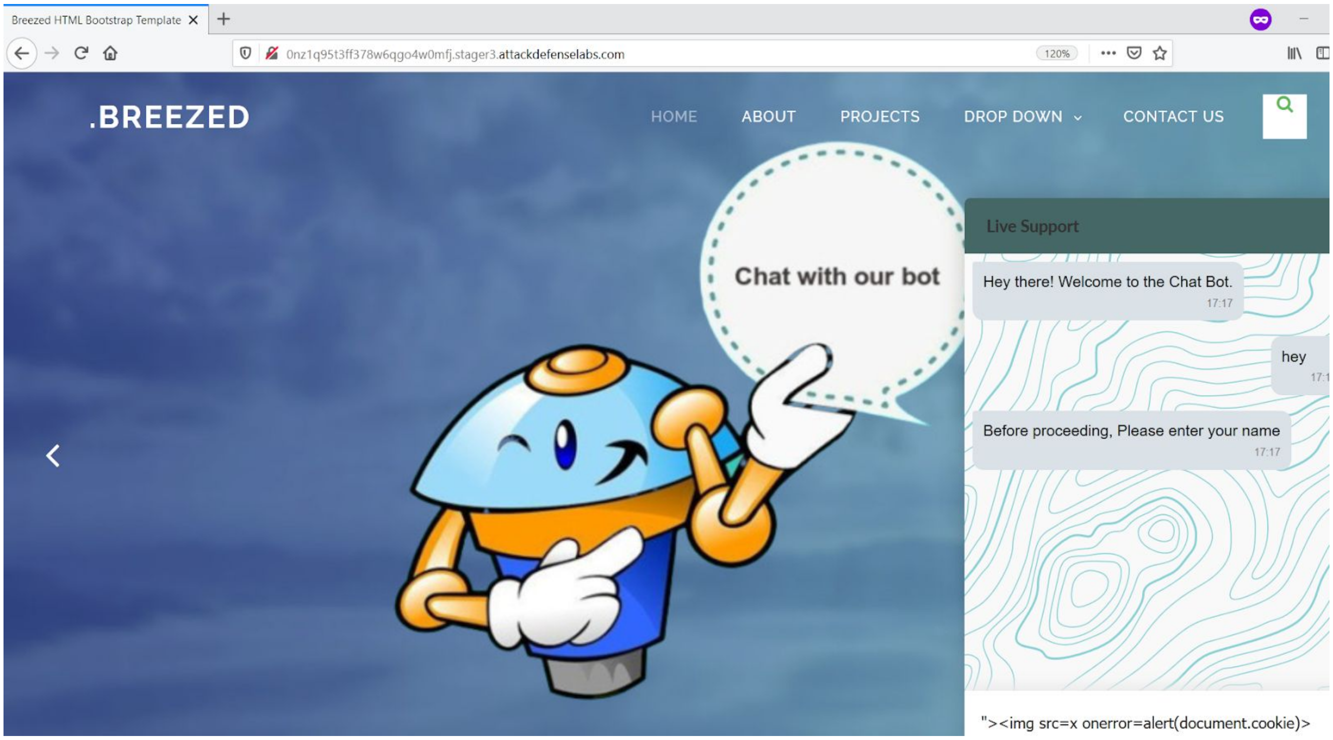
Hey there! Welcome to the Chat Bot. 17:10

hey 17:10

Before proceeding, Please enter your name 17:10

Step 3: Inject the XSS payload in the chat field to retrieve the cookie.

Payload: "><img src=x onerror=alert(document.cookie)>


Breezed HTML Bootstrap Template
0nz1q95t3ff378w6qgo4w0mfj.stager3.attackdefenselabs.com
120%
.BREEZED
HOME
ABOUT
PROJECTS
DROP DOWN
CONTACT US
Chat with our bot
Live Support

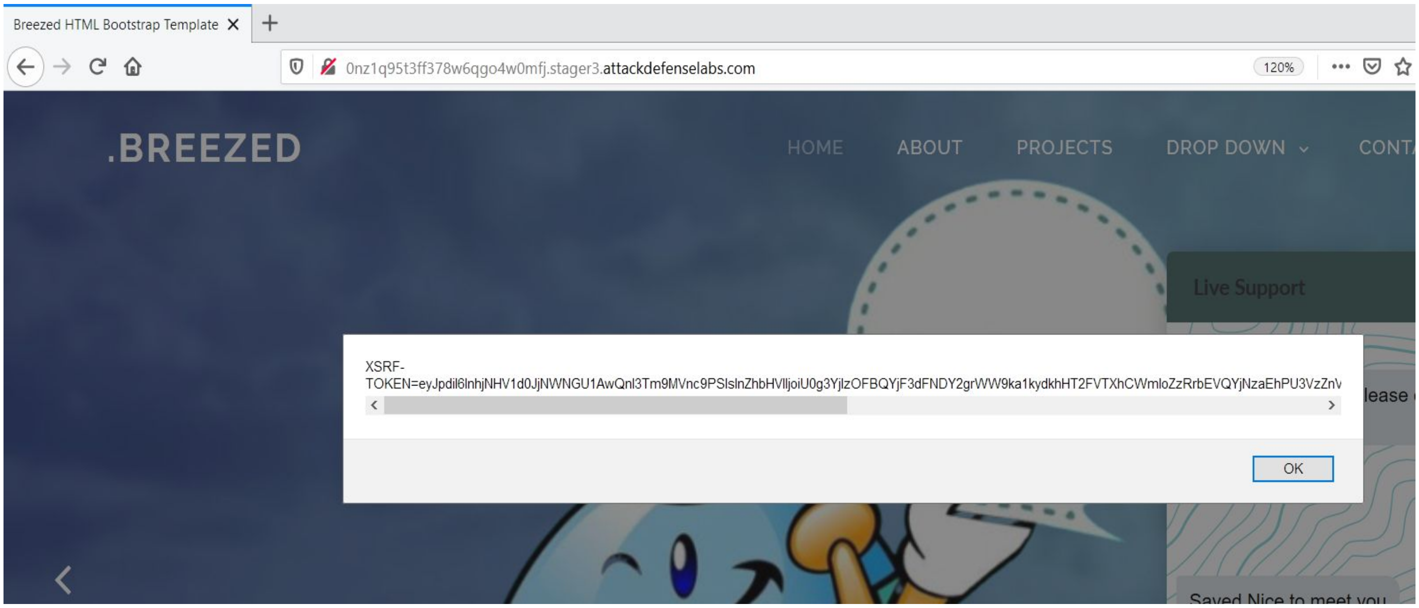
Hey there! Welcome to the Chat Bot. 17:17

hey 17:1

Before proceeding, Please enter your name 17:17

"><img src=x onerror=alert(document.cookie)>

Send the message with the payload.



```
XSRF-
TOKEN=eyJpdil6lnhjNHV1d0JjNWNGU1AwQnl3Tm9MVnc9PSlslnZhbHVlIjoiU0g3YjlzOFBQYjF3dFNDY2grWW9ka1kydkhHT2FVTXhCWmloZzRrbEVQYjNzaEhPU3VzZnV
```

Breezed HTML Bootstrap Template
0nz1q95t3ff378w6qgo4w0mfj.stager3.attackdefenselabs.com
120%
.BREEZED
HOME
ABOUT
PROJECTS
DROP DOWN
CONTA
Live Support
lease
Saved Nice to meet you
OK

The XSS payload has been successfully triggered.

References:

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