
ATTACK
DEFENSE
by PentesterAcademy

Name	Vulnerable Nginx X
URL	https://www.attackdefense.com/challengedetails?cid=216
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.

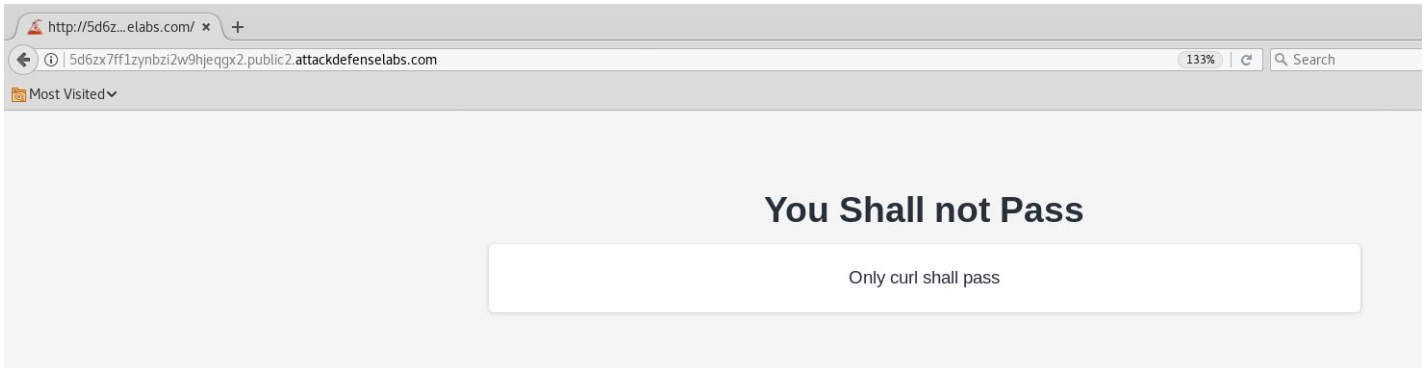
The home page content is protected from the users who are visiting the portal using web browsers. In order to view the full content of the page, the user has to use other tools.

Objective: Your task is to find the correct way to access the complete page content and retrieve the flag!

Solution:

Step 1: Inspect the web application.

URL: http://5d6zx7ff1zynbzi2w9hjeqgx2.public2.attackdefenselabs.com/



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

Command: curl http://5d6zx7ff1zynbzi2w9hjeqgx2.public2.attackdefenselabs.com

```
root@PentesterAcademyLab:~# curl http://5d6zx7ff1zynbzi2w9hjeqgx2.public2.attackdefenselabs.com/
<html>
<head><title>301 Moved Permanently</title></head>
<body bgcolor="white">
<center><h1>301 Moved Permanently</h1></center>
<hr><center>nginx/1.14.0</center>
</body>
</html>
root@PentesterAcademyLab:~#
```

Step 3: Follow the redirect with curl command.

Command: curl -L http://5d6zx7ff1zynbzi2w9hjeqgx2.public2.attackdefenselabs.com/

```
root@PentesterAcademyLab:~# curl -L http://5d6zx7ff1zynbzi2w9hjeqgx2.public2.attackdefenselabs.com/
<!DOCTYPE html>
<html lang="en">
  <head>
    <!-- Required meta tags -->
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
    <!-- End Required meta tags -->
    <!-- Begin SEO tag -->
    <title></title>
    <!-- End SEO tag -->
    <!-- FAVICONS -->
    <link rel="apple-touch-icon-precomposed" sizes="144x144" href="static/apple-touch-icon.png">
    <link rel="shortcut icon" href="static/favicon.ico">
    <meta name="theme-color" content="#3063A0">
    <!-- End FAVICONS -->
    <script src="static/vendor/pace/pace.min.js"></script>
    <!-- BEGIN BASE STYLES -->
    <link rel="stylesheet" href="static/vendor/bootstrap/css/bootstrap.min.css">
    <link rel="stylesheet" href="static/vendor/font-awesome/css/fontawesome-all.min.css">
       <link rel="stylesheet" href="static/vendor/open-iconic/css/open-iconic-bootstrap.min.css">
    <!-- END BASE STYLES -->
    <!-- BEGIN PLUGINS STYLES -->
    <!-- END PLUGINS STYLES -->
    <!-- BEGIN THEME STYLES -->
    <link rel="stylesheet" href="static/stylesheets/main.css">
    <link rel="stylesheet" href="static/stylesheets/custom.css">
    <!-- END THEME STYLES -->
  </head>
  <body>
```

```
        <!-- .wrapper -->
          <!-- .page -->
                <!-- .section-block -->
                <br>
                <br>
                <br>

                  <h3 id="publisher" class="text-center">Congratulations! Your flag is: 699681a51acc2b09ac3fb45d964839cd</h3>

    <script src="static/vendor/jquery/jquery.min.js"></script>
    <script src="static/vendor/bootstrap/js/popper.min.js"></script>
    <script src="static/vendor/bootstrap/js/bootstrap.min.js"></script>
    <script src="static/vendor/perfect-scrollbar/perfect-scrollbar.min.js"></script>
    <script src="static/javascript/main.min.js"></script>
    <script src="static/javascript/custom.js"></script>
    </body>
</html>
root@PentesterAcademyLab:~#
```

Flag: 699681a51acc2b09ac3fb45d964839cd

References:

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