

Authentication v 0.00

Login

Password

connect

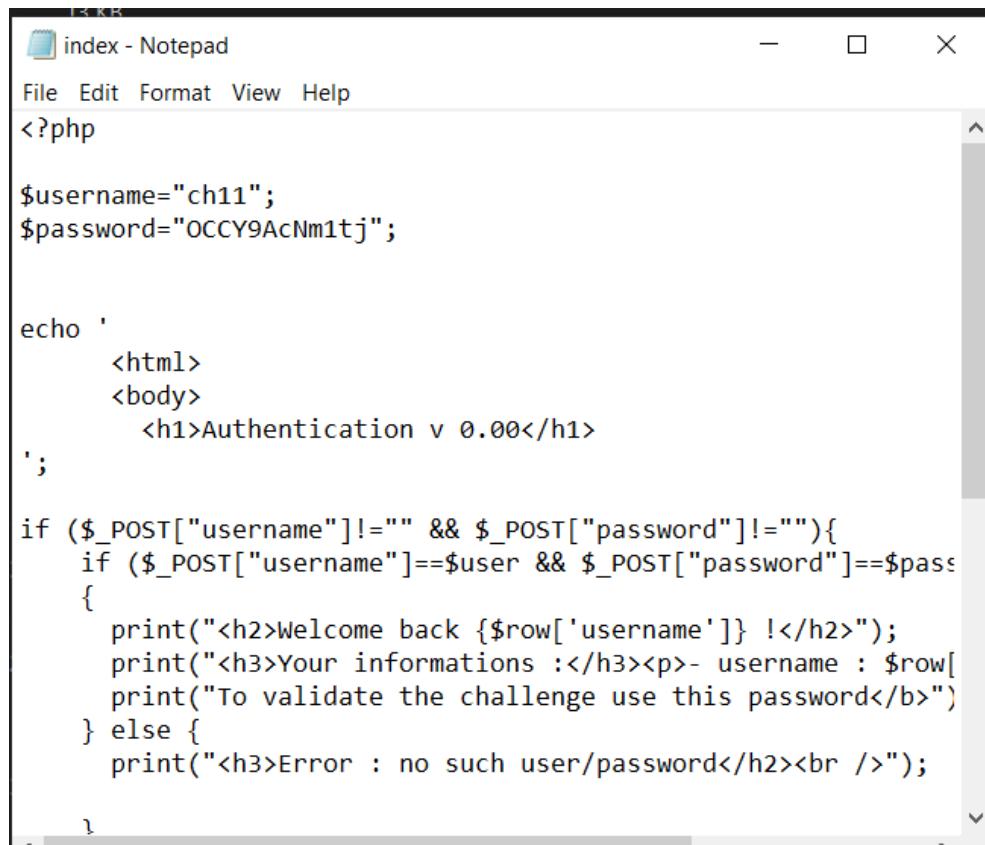
Giao diện trang web cho phép nhập vào username và password như hình. Vì tên challenge là backup file nên ta cần tìm xem file đó ở đâu.

Sau khi research thì server có một vài cách để lưu backup file như là file~, hoặc file.old.

Ta thử tìm cách truy cập các trang đó bằng cách ghi vào URL:

<http://challenge01.root-me.org/web-serveur/ch11/index.php~>.

Kết quả tải được file backup về. Mở lên xem thì thấy như hình dưới.



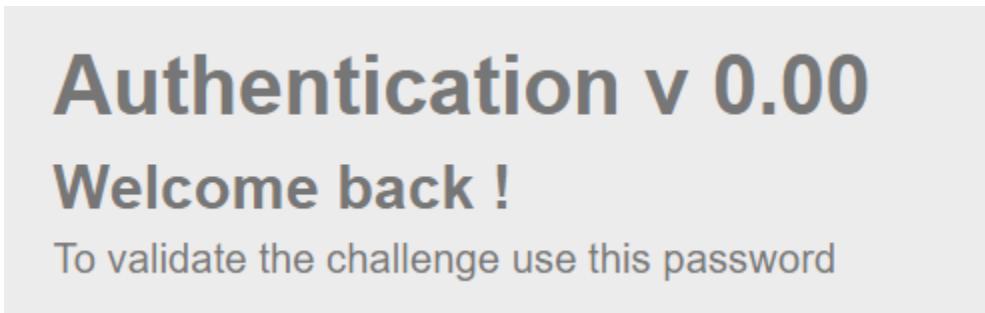
```
index - Notepad
File Edit Format View Help
<?php

$username="ch11";
$password="OCCY9AcNm1tj";

echo '
    <html>
    <body>
        <h1>Authentication v 0.00</h1>
';

if ($_POST["username"]!="" && $_POST["password"]!=""){
    if ($_POST["username"]==$user && $_POST["password"]==$pass){
        print("<h2>Welcome back {$row['username']} !</h2>");
        print("<h3>Your informations :</h3><p>- username : $row[");
        print("To validate the challenge use this password</b>");
    } else {
        print("<h3>Error : no such user/password</h2><br />");
    }
}
```

Ta sẽ có username và mật khẩu như hình trên.



Đăng nhập với username và mật khẩu đã tìm thấy và bypass challenge thành công.