BÀI TẬP CTF

Bảo mật web và ứng dụng – NT213.M21.ANTN

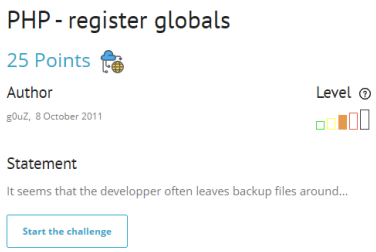
Giảng viên hướng dẫn: *Đỗ Hoàng Hiển*

Sinh viên thực hiện: *19520199 – Lê Tôn Nhân*

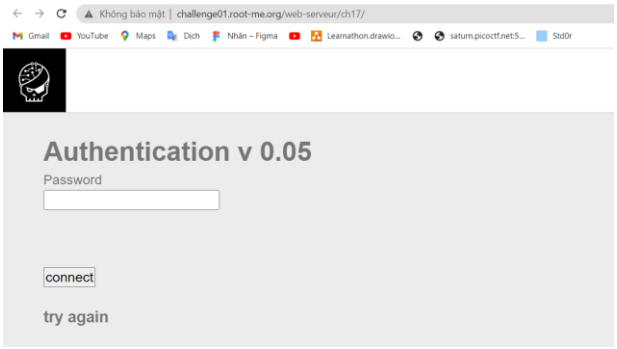
Challenge 11: PHP - register globals (level medium)

Link challenge: https://www.root-me.org/en/Challenges/Web-Server/PHP-register-globals

- Ta nhận được gợi ý ở challenge này là các nhà phát triển thường để lại các tệp sao lưu xung quanh



- Truy cập vào challenge ta được trang web như bên dưới

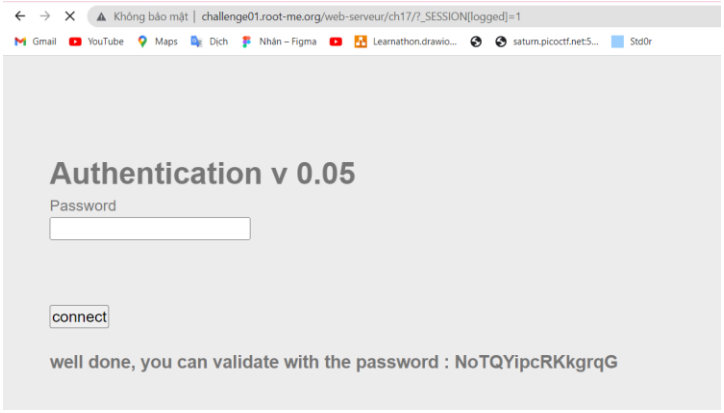


- Trang web yêu cầu ta xác thực với Password
- Dựa vào gợi ý ta biết được việc cần làm là tìm file backup. File backup thường có đuôi là bak. Sau nhiều lần thử cuối cùng cũng tìm ra được file backup là index.php.bak
- Truy cập vào link http://challenge01.root-me.org/web-serveur/ch17/index.php.bak là ta có thể tải file backup này về

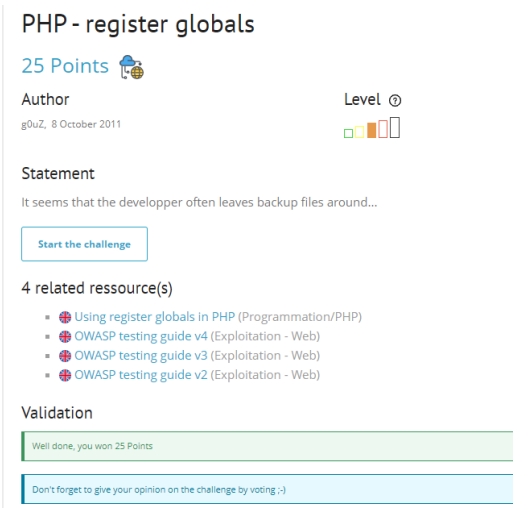
- Đọc code của file backup

```php
if (isset($_POST["password"]))
    $password = $_POST["password"];

if (!ini_get('register_globals')) {
    $superglobals = array($_SERVER, $_ENV,$_FILES, $_COOKIE, $_POST, $_GET);
    if (isset($_SESSION)) {
        array_unshift($superglobals, $_SESSION);
    }
    foreach ($superglobals as $superglobal) {
        extract($superglobal, 0 );
    }
}

if (( isset ($password) && $password!="" && auth($password,$hidden_password)==1) || (is_array($_SESSION) && $_SESSION["logged"]==1 ) ){
    $aff=display("well done, you can validate with the password : $hidden_password");
} else {
    $aff=display("try again");
}

echo $aff;

?>
```

- Ta thấy password sẽ xuất hiện khi **$_SESSION["logged"]==1**. Do đó ta cần thực hiện ghi đè biến này thông qua url như sau: **http://challenge01.root-me.org/web-serveur/ch17/?_SESSION[logged]=1**



- Kết quả cho thấy được password là NoTQYipcRKkgrqG
- Nộp password vừa tìm được và ta vượt qua thử thách thành công



FLAG: NoTQYipcRKkgrqG