

BÀI TẬP CTF

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

Giảng viên hướng dẫn: *Đỗ Hoàng Hiên*

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

PHP - register globals

25 Points 🏆

Author

g0uZ, 8 October 2011

Level 🔒

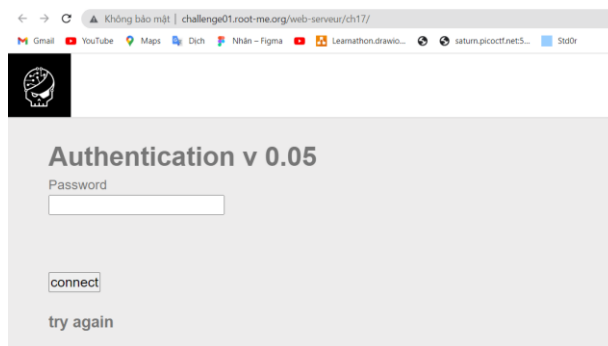


Statement

It seems that the developer often leaves backup files around...

[Start the challenge](#)

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



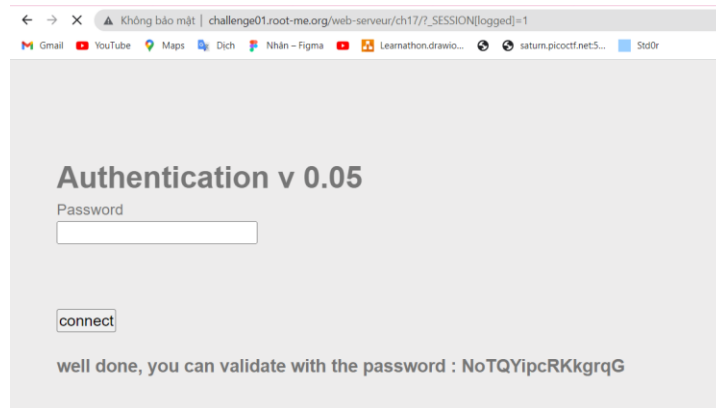
- Trang web yêu cầu ta xác thực với Password
- Dựa vào gợi ý ta biết được việc cần làm là tìm file backup. File backup thường có đuôi là bak. Sau nhiều lần thử cuối cùng cũng tìm ra được file backup là index.php.bak
- Truy cập vào link <http://challenge01.root-me.org/web-serveur/ch17/index.php.bak> là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

- Đọc code của file backup

```
index.php X
F: > HK6 > Bảo mật web và ứng dụng > Bài Tập > Bài tập 6 > index.php
44
45 if (isset($_POST["password"]))
46     $password = $_POST["password"];
47
48 if (ini_get('register_globals')) {
49     $superglobals = array($_SERVER, $_ENV, $_FILES, $_COOKIE, $_POST, $_GET);
50     if (isset($_SESSION)) {
51         array_unshift($superglobals, $_SESSION);
52     }
53     foreach ($superglobals as $superglobal) {
54         extract($superglobal, 0);
55     }
56 }
57
58 if ((isset($password) && $password!="") && auth($password,$hidden_password)==1) || (is_array($_SESSION) && $_SESSION["logged"]==1 ){
59     $aff=display("well done, you can validate with the password : $hidden_password");
60 } else {
61     $aff=display("try again");
62 }
63
64 echo $aff;
65
66 ?>
67
```

- 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

PHP - register globals

25 Points 

Author

g0uZ, 8 October 2011

Level 



Statement

It seems that the developer often leaves backup files around...

[Start the challenge](#)

4 related ressource(s)

-  Using register globals in PHP (Programming/PHP)
-  OWASP testing guide v4 (Exploitation - Web)
-  OWASP testing guide v3 (Exploitation - Web)
-  OWASP testing guide v2 (Exploitation - Web)

Validation

Well done, you won 25 Points

Don't forget to give your opinion on the challenge by voting :)

FLAG: NoTQYipcRKkgrqG