الفصل السابع عشر
ثغرة ال RCE

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

ثغرة ال RCE

- في البداية تعالو نتعرف على معنى و اختصار هده الثغرة REC اختصار لكلمة remote code execution
- هدا النوع من الثغرات لا يصيب المواقع و حسب لا بل حتى انضمة التشغيل و تطبيقات الهواتف سواء android او ios
- و لا يمكن الكشف على مثل هده الثغرات الى اذا كنت تجيب لغة البرمجة المستعملة في التطبيق او الموقع الدي تقوم ب اختبار الاختراق عليه لان ثغرة RCE ليست مثل باقي الثغرات.
- على سبيل المثال في ثغرة SQLI يمكن لاي مبتدئ استغلال هده الثغرة و لكن عكس ثغرة RCE لانها تحتاج الى مهارات في لغات برمجة معينة
- و نحن هنا نتكلم على اختراق المواقع بكل تاكيد لهذا ما يهمنا في لغات البرمجة هي اللغات الدينامكية Dynamic programming language و منها php و asp و عن قريب JavaScript لان لغة الجافا سكربت سوف تعمل نفس عمل لغة php و هاذا ما يقوله خبراء البرمجة "الجافا سكربت هي المستقبل "

ثغرة ال RCE (تكمله...)

- كيف تحدث ثغرة RCE
- ثغرة RCE تحدث بسبب واحد الا و هو الخطأ من المبرمج نفسه و احيانا تكون الثغرة ب سبب لغة البرمجة نفسها .
- ثغرة RCE بسبب الخطأ من المبرمج :
- لغات البرمجة الدينامكية تتيح للمبرمجين عدة functions جاهزة دون الحاجة الى كتابتها و لكن هذه ال functions تمتلك صلاحيات على النظام او الموقع بحيث تتمكن من التحكم او اعطاء اوامر على النظام مثال على هذا

```
$dz = "varname";

$o = $_GET['arg'];

eval("$dz = $o;");
?>
```

ثغرة ال RCE (تكمله...)

- في الاعلى كود php بسيط بدون فلترة و هذا الخطأ من المبرمج لانه يسمح للمستخدم ب استعمال اي شيء او اي كود على الموقع
- نشوف الاستغلال كيف يكون
- نقوم ب استعراض الرابط على المتصفح 127.0.0.1/index.php?arg=1; phpinfo()
- و نلاحض انه قد قدم لنا phpinfo الخاصة ب السيرفر

127.0.0.1/index.php?arg=1; system('id')

- و الان نلاحض انه قد تم اعطائنا ال id الخاص بنا على السيرفر بكل بساطة و هذا امر خطير جدا

ثغرة ال RCE (تكمله...)

- ثغرة RCE بسبب لغة البرمجة :
- كما تكلمنا في الاعلى انه احيانا تنتج ثغرة rce بسبب خطأ ما في لغات البرمجة .
- و انا هنا لا اتلكم على فراغ لان من كتب لغات البرمجة نفسه الانسان و الانسان غير معصوم من الخطأ و لكن ان تكتشف ثغرة ما في لغة برمجة فهذا يتطلب منك مهارات عاالية جدا
- كمثال على هادا سوف نتكلم على ثغرة
- https://exploitbox.io/vuln/WordPress-Exploit-4-6-RCE-CODE-EXEC-CVE-2016-10033.html
- و هذه الثغرة كانت ب سبب مشكل في دالة mail() في PHP حيث تمكن المخترق من حقن كود في ال Header و الحصول على Shell Session
- و هادا الخطأ من لغة البرمجة نفسها

ثغرة ال RCE (تكمله...)

- الخلاصة :
- ثغرة remote code execution ثغرة كبيرة جدا و تحتاج الى مهارات كبيرة في لغات البرمجة لهذا انت بحاجة الى وقت كبير لاحتراف هذا النوع من الثغرات لهذا لا تياس ابدا و أقرا كثيرااااااااااا

تم بحمد الله انتهاء الفصل السابع عشر