أمن الحاسوب من الثغرات التي تهاجم التطبيقات

إعداد المبرمج: عبدالهادي فرحان حربان

أمنية الحاسوب وتشفير المعلومات

علوم الحاسوب صعدة كلية العلوم التطبيقية

تحت إشراف الإستاذ القدير: بكر الزنّي

النوع الأول: ثغرات" Remote File Include "

يعمل هذا النوع على تمكين المهاجم من إدراج ملف خارجي الى ملفات الموقع بشكل غير شرعي. يقوم المهاجم على الأغلب من خلال هذه الثغرة بإدراج ملف Phpshell ويستطيع من خلاله التلاعب بالموقع وقد يصل الى التلاعب بالخادم(server) كاملاً!

لو قمنا بطرح سؤال: عن كيف يتم إصابة البرامج بهذه الثغرة؟

لوجدنا إن الإجابة عليه هي: انه يتم إصابة البرامج عن طريق هذه الثغرة عن طريق إستخدام الدوال التالية بالبرنامج:(Require_once و Require و Include_once و Include) متبوعة بعلامة $ (متغير).

نقوم بكتابة مثال يوضح ذلك وهو عبارة عن كود بسيط مصاب:

```
<?php

$ghost = $_GET['hacked'];

include ($ghost);

?>
```

شرح الكود المصاب (المضروب):

بالسطر الأول من الكود تم وضع متغير بإسم ghost وإعطائه القيمة التالية "hacked"

وبالسطر الثاني من الكود تم إستخدام الدالة include وإستخدام علامة $ قبل إسم المتغير ghost من بين الأقواس.

ولو قمنا بطرح سؤال آخر عن: كيف يمكننا تأمين البرامج من هذا النوع؟

الجواب نقول: التأمين او الترقيع يكون عن طريق تعريف المتغير المصاب ل(/.).

نقوم بمثال يوضح ترقيع الكود السابق من الثغرة فإليكم الشكل التالي:

```
<?php
$ghost = $_GET['hacked'];
$ghost = "./";
include ($ghost);
?>
```

مع إستبدال ghost بإسم المتغير الملحق بالعلامة $.

النوع الثاني: ثغرات "Local File Include"

يعمل هذا النوع على تمكين المهاجم من قراءة أكواد ملفات الموقع المصاب.

لو قمنا بطرح سؤال: عن كيف يتم إصابة البرامج بهذه الثغرة؟

لوجدنا ان الإجابة عليه هي: انه يتم إصابة البرامج بهذه الثغرة عن طريق إستخدام الدوال التالية:

(fread و show_source و readfile و file).

نقوم بمثال يوضح ذلك وهو عبارة عن كود مصاب:

```
<?php

readfile($hacked);

?>
```

شرح الكود المصاب (المضروب):

نلاحظ إستخدام الدالة readfile وعلامة $ مسبوقة بال"hacked" بداخل الأقواس.

ولو قمنا بطرح سؤال آخر عن: كيف يمكننا تأمين البرامج من هذا النوع؟

الجواب نقول: لتأمين او الترقيع يكون عن طريق تعريف المتغير المصاب ل(/.).

كما ثغرات الريموت فايل انكلود.

نقوم بمثال يوضح ترقيع الكود السابق من الثغرة هذه فإليكم شكل المثال التالي:

```
<?php

$hacked = "./";

readfile($hacked);

?>
```

مع إستبدال hacked بإسم المتغير الملحق بعلامة $.

النوع الثالث: ثغرات "XSS"

يعمل هذا النوع على تمكين المهاجم من زرع أكواد (جافا سكريبت واتش تي ام ال) في الملف المصاب.

وينتج عن ذلك في معظم الأوقات تمكين المهاجم من سحب (كوكيز أدمن) الموقع عن طريق ملف وما!.

ويختلف هذا النوع عن بقية الثغرات؛ لأن تنفيذه لا يكون على الموقع نفسه بل يكون على مستخدمين الموقع.

لو قمنا بطرح سؤال: عن كيف يتم إصابة البرامج بهذه الثغرة؟

لوجدنا إن الإجابة عليه هي: انها تتم الإصابة بهذا النوع من الثغرات غالباً عن طريق مربعات البحث(Search) كمربع البحث الموجود ببعض برامج (البي اتش بي).

نقوم بمثال يوضح ذلك وهو عبارة عن كود مصاب:

```
<?php

print $_GET['hacked'];

?>
```

ولو قمنا بطرح سؤال آخر عن: كيف يمكننا تأمين البرامج من هذا النوع؟

الجواب نقول: التأمين او الترقيع يكون عن طريق الدوال التالية:

(htmlentities or htmlspecialchars)

نقوم بمثال يوضح ترقيع الكود السابق من الثغرة هذه فإليكم شكل المثال التالي:

```
<?php
print htmlspecialchars($_GET['hacked']);
?>
```

شرح لعملية ترقيع الكود المصاب(المضروب):

نلاحظ اننا في عملية الترقيع وضعنا الدالة htmlspecialchars بعد print واضفنا قوسين حول $_GET

وبهذا الشكل لن يتم تنفيذ استغلال الثغرة وسيتم عرضه بالصفحة فقط لاغير!