

هذا الكتاب عبارة عن نسخة مصغرة ومعدلة مُجبرين لكي تتوافق بكونها كـ [ كتاب الكتروني ] لتصفح الدراسة بأريحية كاملة وبجودة الصور العالية بإمكانك زيارة القسم الخاص بها .

<http://www.d99y.com/vb/forumdisplay.php?f=108>

# بِسْمِ اللّٰهِ الرَّحْمٰنِ الرَّحِیْمِ

## السَّلَامُ عَلَیْكُمْ وَرَحْمَةُ اللّٰهِ وَبَرَكَاتُهُ

www.d99y.com

ساحة التطوير

### مقدمة

تمنياتي لكم احبتي دائماً بالصحة والعافية .

عدنا من جديد لاكمال الدورة الاولى من نوعها على مستوى العالم ، واليوم مع ثغرة جديدة وطريفة وجميلة .

الثغرة تسمى **Remote File Disclosure** ومن الاسم اي اظهار الملفات او كشف الملفات في السيرفر ، الثغرة تختصر بالشكل التالي .. **rfd**

كما ذكرت سابقاً الثغرة بسيطة وهي تقوم على اساس كشف الملفات ، قد يسأل شخص هل يعتبر **Local File Inclusion** كشف ملفات ؟ وماذا تختلف بينها وبين هذه الثغرة

كما تعلمنا في دراسة **Local File Inclusion** ان الثغرة تقوم بدوال الانكلود الطبيعيه **include** وكذلك **require** وخواصها للجلب مره واحدة **include\_once + require\_once !**

ولكن قام المبرمج بعمل بعض التعديلات التي جعلتها فقط **local** ولكن هنا الثغرة تختلف بالدوال وكذلك هي تسمح بكشف الملفات بعكس **Local File Inclusion** التي تجلب الملف وتنفذه بالصفحة!!

يعني مثلاً حين اقوم بثغرة **Local File Inclusion** تجلب ملف الاتصال **config.php** كمثال ، هنا الكونفك سينفذ في الصفحة دون امكانية مشاهدة محتواه لانه عبارة عن ملف **php** ولكن في ثغرة **Remote File Disclosure** سنشاهد محتوى الملف وبذلك يمكن وبشكل كبير اختراق السيرفر بسهولة ..

اتمنى اني وضحت الفرق لكي لا يحدث خلط ، كما ذكرت اختلاف بالدوال وكذلك بالتنفيذ ، في **Local File Inclusion** لايمكن مشاهدة محتويات الملف اذا كان **php** لانه سينفذ في الصفحة ولكن تشكل خطر الثغرة السابقة في قراءة ملفات النظام لانها باي حال لن تنفذ ، ولكن هنا في هذه الثغرة بإمكاننا تصفح الملفات وقراءة محتوياتها بكل اريحية سواء ملفات نظام او ملفات **php**

بالنسبة للدوال التي تنسب الي **Remote File Disclosure** لدينا عشرات الدوال التي تقوم بوظائف بشكل او باخر بقراءة الملفات وتحميلها ، الان الجميع يعلم ان اي دالة تقوم بقراءة محتويات الملفات او تنزيلها دون تحديد هي عبارة عن ثغرة **Remote File Disclosure** ولكن هناك دوال اساسيه وسنقوم بالتطبيق عليها وهي **readfile - show\_source** وهناك عشرات الدوال الاخرى ، ولكن انت كمبرمج تعرفت ان في حالة سمحت للزوار بقراءة الملفات او تحميلها " دون تحديد الملفات " هنا تعتبر ثغرة **Remote File Disclosure** بلاشك مادامت بعيدة عن دوال الانكلود لكي لا تعتبر **LFI** والدالتين السابقتين هي احدهم وانا ذكرتهم على وجه التحديد لاننا سنطبق عليهم في السكربت!

سبب تكون الثغرة كالعاده المبرمج لا يحدد ملفات معينه يتصفحها المستخدم او يحملها ، او يضع ملف واحد بل وضع الدالة في متغير بشكل او باخر وقام باعطاء الزوار صلاحيات خطيره ومضره .

تم معرفة سبب تكون الثغرة ، وخطورتها تمكن باختراق السيرفر في حالة وصول المُتحرِّق الي معلومات هامة كـ ملف الاتصال بقاعدة البيانات او ملفات النظام ، والكثير من الطرق والاساليب الاخرى ، وتم التعرف على اختلافها عن **LFI** اما الانواع هو نوع واحد ، ومن دالة الى اخرى يمكنك جلب رابط معين ولكن لا فائدة من جلب الملفات الخارجية ، لانها ستعرضها من مصدرها ، ويمكنك الجلب من خارج السيرفر ولكن لايمكنك التنفيذ او ماشابه على اية حال وهذا يختلف طبعا من دالة الى اخرى ، واخيراً وكما ذكرت ان الثغرة لا تنقسم الى اي انواع اخرى .

www.d99y.com

ساحة التطوير

### اكتشاف واستغلال

اهلاً وسهلاً بكم احبتي من جديد في اكتشاف الخطأ البرمجي والاستغلال لثغرة **Remote File Disclosure - rfd** التي تكلمنا عنها سابقاً في موضوع المقدمة .

تعلمنا جميعاً سبب تكون الثغرة وانها بنوع وحيد ، وكذلك تعلمنا ان الدوال التي سنقوم بالتطبيق عليها هي **readfile - show\_source** ويوجد الكثير غيرها ، وكذلك تعرفنا على الاختلاف بينها وبين ثغرة **LFI** التي قمنا بدراستها سابقاً ، وكذلك ذكرنا اننا سنقوم باختراق السيرفر باحد طرق استغلال الثغرة .

العادة قمت في برمجة السكربت بشكل سريع على الدالتين السابقتين لكي نقوم بالتطبيق عليها والتعرف على طرق الاستغلال.

تحميل السكريت



والتعليق على ملفات السكريت .

```
<!-----  
////////////////////////////////////  
// [ 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 تحرموني دائماً من دعائكم //  
// وتذكروا ان ساحة التطوير للهكر الاخلاقي //  
////////////////////////////////////  
----->
```

هو لكم ولانكم وانا لم اقم باي جهود الا لكي نرتقي سوياً بالمحتوى العربي .

والسكريت لايحتاج الى تنصيب قم بنقل مجلد السكريت **rfd** الى سيرفرك المحلي **www** او اي كان .

واستعرضه في المتصفح .

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

## قم باختيار القسم المطلوب :

Remote File Disclosure

قراءة  
الملفات

# show\_source

Remote File Disclosure

قراءة  
الملفات

# readfile

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

 coded by NassRawI D99Y team || d99y.com

وكما تشاهد قمت بوضع الدالتين واتحت فرصة التجربة والتطبيق ..

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

## قم باختيار القسم المطلوب :

Remote File Disclosure

قراءة  
الملفات


# show\_source

Remote File Disclosure

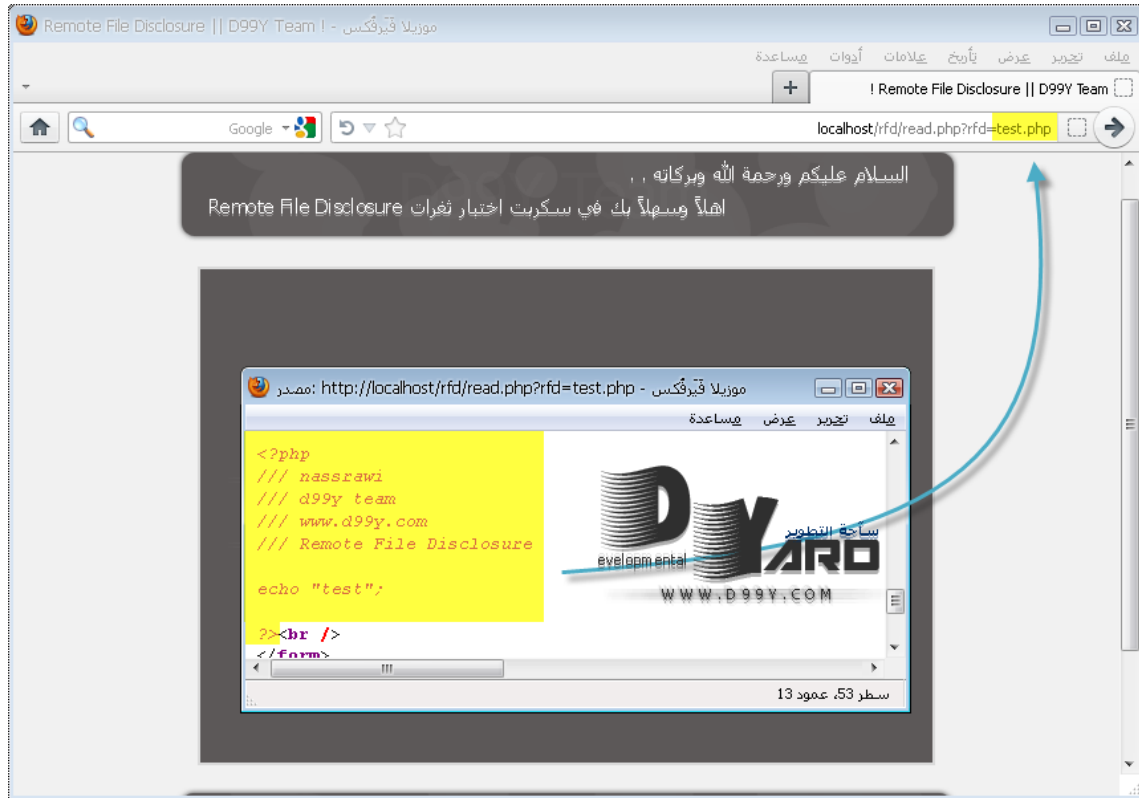
قراءة  
الملفات

# readfile

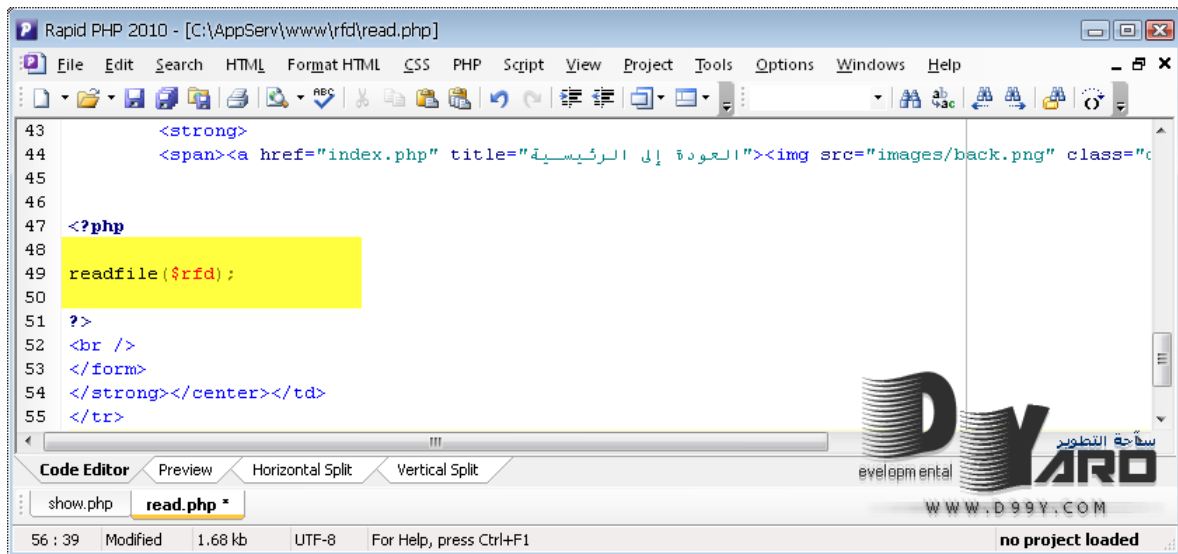
أحذر!  
السكربت مصاب , والهدف من طرحه عمل الاختبارات الأمنية عليه , لذلك اجذر  
من رُفعه على استضافة خاصة , و الاكتفاء بالاختبارات الأمنية داخل السيرفر  
المحلي "وجب التنويه للأهمية"

 coded by NassRawI D99Y team || d99y.com

نقوم باختيار الدالة الاولى ! **readfile**



وكما تشاهد ان الدالة تم تعريفها بمتغير **rfd** وهي تقوم بقراءة ملف **test.php** الموجود في نفس المجلد , وبإمكانك مشاهدة الكود البرمجي لملف **test.php** في سورس الصفحة وفي هذه الدالة ملفات الـ **php** ستجدها في السورس كما ذكرت .



وكما تشاهد الخطأ البرمجي في سطر **49** كما تعلمنا تم تعريف الدالة **readfile** بمتغير **rfd** والمتغير غير محدد للملفات المسموحة .


السلام عليكم ورحمة الله وبركاته , ,  
اهلاً وسهلاً بك في سكرت اختبار ثغرات Remote File Disclosure

## قم باختيار القسم المطلوب :

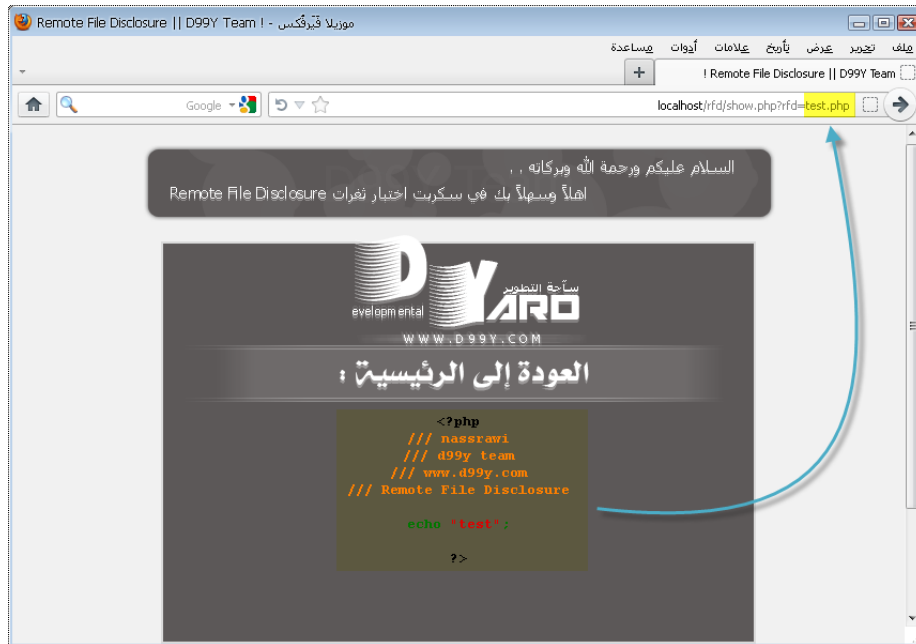


السكرت مصاب , والهدف من طرحه عمل الاختبارات الأمنية عليه , لذلك اجنر من رفعة على استضافة خاصة , و الاكتفاء بالاختبارات الأمنية داخل السيرفر المحلي "وجب التنويه للأهمية"

# أحذرو!

 coded by NassRawI D99Y team || d99y.com

نقوم باختيار الدالة الاخرى ! **show\_source**



الدالة تقوم بعرض محتوى الملف وملونه وجميله ، وطبعاً كما هو حال السابقة الدالة معرفة على متغير **rfd** وتقوم بقراءة ملف **test.php** (المقروء سابقاً) والموجود في نفس المجلد .

```

Rapid PHP 2010 - [C:\AppServ\www\rfd\show.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"><img src="images/back.pn
45
46
47 <?php
48
49 show_source($rfd);
50
51 ?>
52 <br />
53 </form>
54 </strong></center></td>
55 </tr>
Code Editor Preview Horizontal Split Vertical Split
show.php
57 : 57 Modified 1.68 kb UTF-8 no project loaded

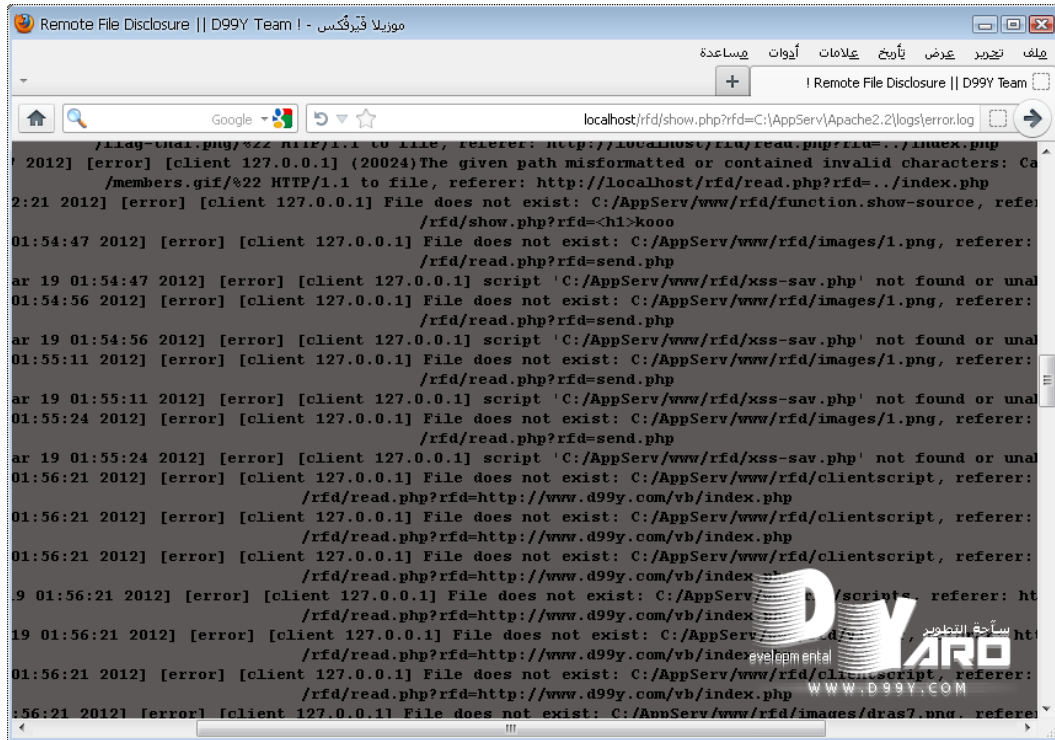
```

والخطأ كما ذكرت سابقاً في سطر 49 تم تعريف الدالة `show_source` على متغير `rfd` وهو غير محمي..

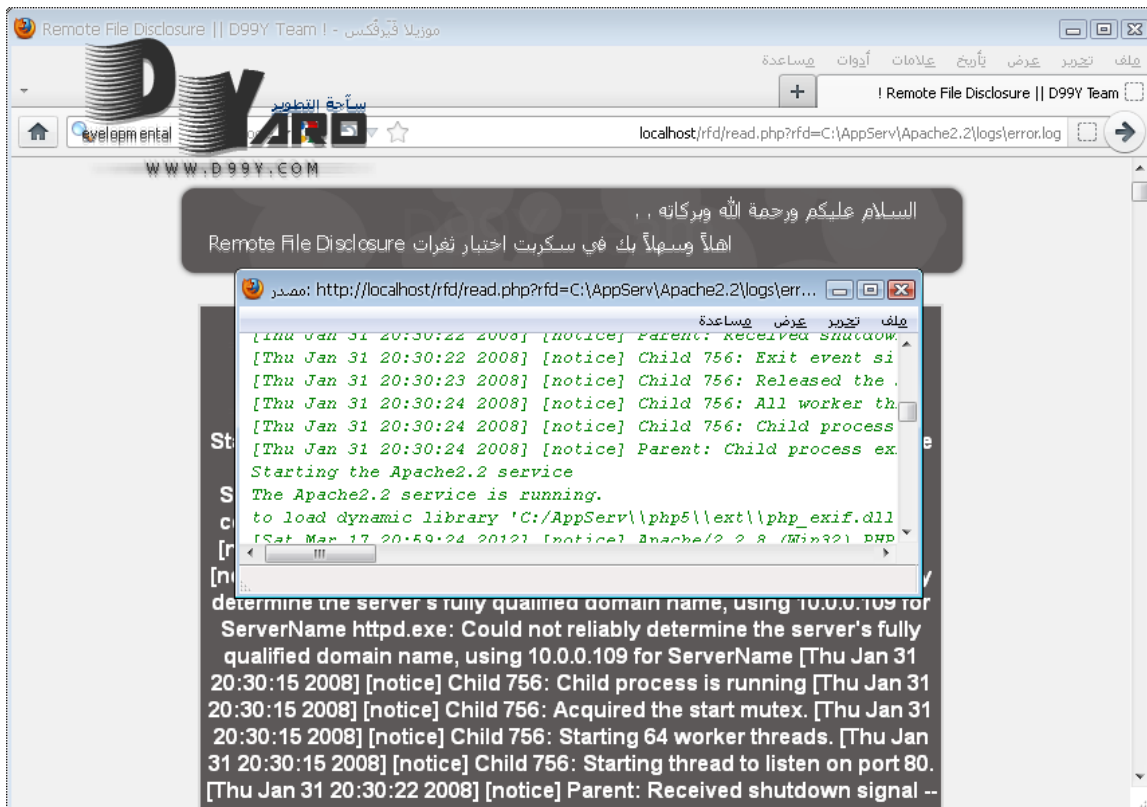
سنقوم بقراءة احد ملفات النظام للتطبيق ، والمسار قد يخذل البعض ويحتاج الي تخمين ، ولكن كما تعودنا لمعرفة المسارات الغالبية من المبرمجين لن يخفي الاخطاء للدوال @ وبذلك نضع ملف غير موجود ليظهر لنا المسار .



وكما نشاهد تم اظهار المسار بشكل واضح ، الان نعرفنا ان النظام منصب على `c` وتعرفنا على مجلد السيرفر ، نقوم بقراءة ملف `logs` للباتشي كمثل ..



كما تشاهد تم استعراض محتواه ..



وكذلك الدالة الاخرى تم استعراض محتواه ..

وطبعاً بالنسبة للدالتين يمكنك مشاهدة محتويات الملفات الاخرى ، كمثل نقوم بقراءة محتوى ملف index.php الخاص بالاباشي ..



كما تشاهد انا عدت خطوة **../** وقمت باستعراض محتوى ملف **index.php** وفعلاً تم استعراضه بنجاح وبامكانك التطبيق على الدالة الأخرى وستجد المحتوى في السورس !

والان بإمكانك استغلال صلاحياتك حالياً في تصفح ملفات النظام والتعرف على البرامج والإصدارات والخ ..

وطبعاً الاستغلال الذي خطر في بالي كـ **مُخترق** في هذه الثغرة ، هو أولاً البحث عن السكريبتات المنصبة في السيرفر ومحاولة البحث عن ملف للاتصال بالقاعدة ، لكي نحصل على بيانات الاتصال في القاعده ..

وهنا فيديو تطبيقي للتوضيح بشكل سريع ..

<http://www.youtube.com/watch?v=SXiCq6x4deo>

بإمكانك المشاهدة بوضوح **HD** وكذلك يمكنك تنزيل الفيديو **mediafire** بوضوح عالي وبحجم صغير!

كما تشاهد أخي العزيز انا متعمد على عدم استخدام اي اداة اختراق لكي اوضح مدى خطورة الثغرة ، وكان التطبيق في نظام ويندوز دون تدخل اي اداة ..

في الاول كما يشاهد الجميع استغلّيت سكرت **XSS** الذي كنا نعمل عليه سابقاً ، بقراءة ملف **config.php** الخاص في قاعدة البيانات ، وفعلاً حصلت على معلومات قاعدة البيانات ، ثانياً اتصلت بالقاعدة عن طريق **phpmyadmin** وعملت قاعده بيانات جديده وجدول وحقل جديد وعملت على تنفيذ امر **SQL** وهو يعمل ملف بمحتوى معين ، وعملت ملف مصاب بثغرة تطبيق الاوامر ، وقمت بتطبيق اولاً امر عرض الملفات ثانياً انشاء ملف وتمكنت من وضع تعليق على السيرفر ، وقمت بعمل يوزر جديد **لسطح المكتب البعيد** وقمت بمنحه صلاحيات المدير ، واتصلت في السيرفر واصبح لدي تحكم كامل في النظام وبصلاحيات المدير كما ذكرت .

هنا استغلال وبشكل سريع عملته وهذا اول استغلال قد يخطر لـ **مُخترق** ان كان يملك عقل **مُخترق** طبعاً سيتمكن من خلق الكثير من الاستغلالات والوصول الى هذا النظام ..

اتمنى ان الشرح كان واضح على الجميع ، وتم بحمد الله استغلال الثغرة واكتشاف الخطأ البرمجي لها ..

[www.d99y.com](http://www.d99y.com)

ساحة التطوير

الترقيع

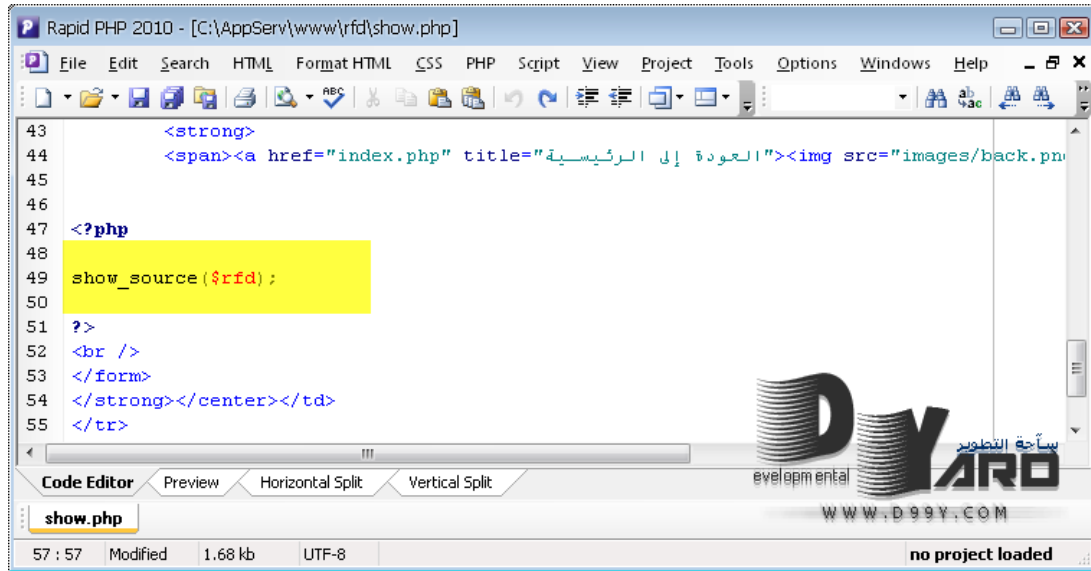
اهلاً وسهلاً بكم يا احبتي في درس ترقيع ثغرة **! Remote File Disclosure - rfd**

تعلمنا جميعاً سبب تكون الثغرة وانها بنوع وحيد ، وكذلك تعلمنا ان الدوال التي قمنا بالتطبيق عليها هي **readfile - show\_source** ويوجد الكثير غيرها ، وكذلك تعرفنا على الاختلاف بينها وبين ثغرة **LFI** التي قمنا بدراستها سابقاً ، وكذلك تمكنا من اختراق السيرفر باحد طرق الاستغلال البسيطة ..

والان حان وقت الترقيع ، الترقيع يا احبتي بسيط ولا يحتاج لوقت وهو بوضع ملفات معينه يسمح للمتغير تصفحها ، كما فعلنا بترقيع **! File Inclusion - FI**

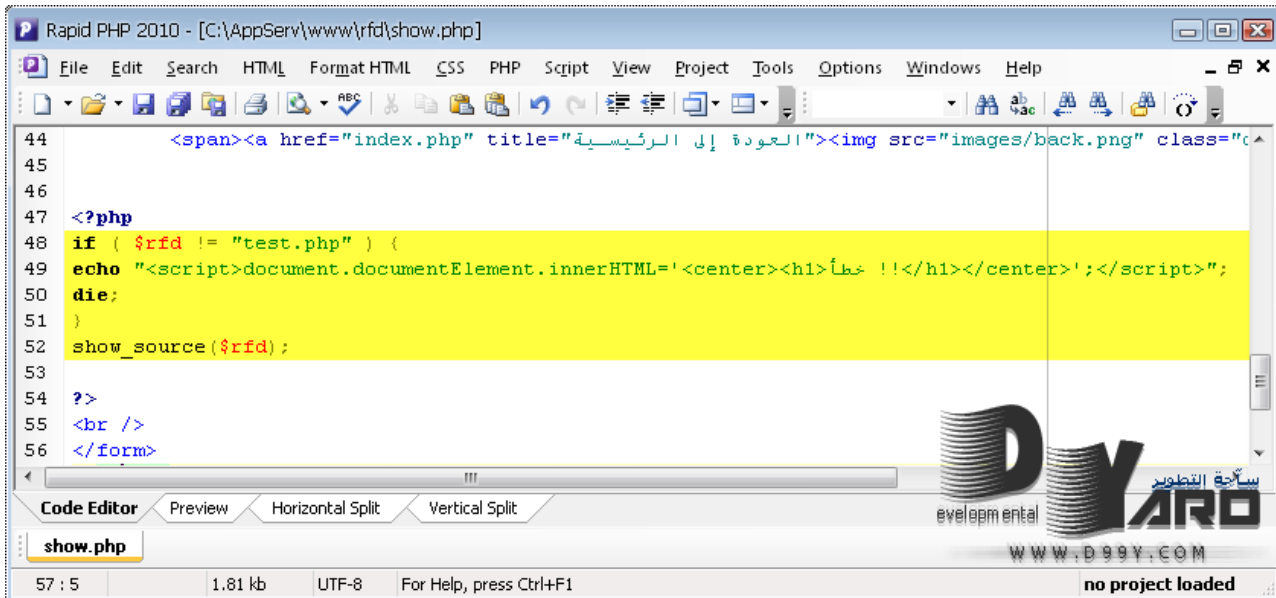
اولاً الخطأ البرمجي لدالة **! show\_source**





```
43 <strong>
44 <span><a href="index.php" title="العودة إلى الرئيسية">
52 <br />
53 </form>
54 </strong></center></td>
55 </tr>
```

في سطر 49 كما نلاحظ تم تعريف الدالة بمتغير دون حمايته ..  
والترقيع ..



```
44 <span><a href="index.php" title="العودة إلى الرئيسية">document.documentElement.innerHTML='<center><h1>خطأ !!</h1></center>';</script>";
50 die;
51 }
52 show_source($rfd);
53
54 ?>
55 <br />
56 </form>
```

بواسطة if الشرطية المتغير rfd اذا كان لايساوي != الملف test.php اطبع echo رسالة الخطأ ، واقتل البرمجية die لكي لا يتم تنفيذ الثغرة من جديد ..

ويجب وضعها فوق المتغير كما تعلمنا لكي يتم التحقق وبعد ذلك الجلب ..



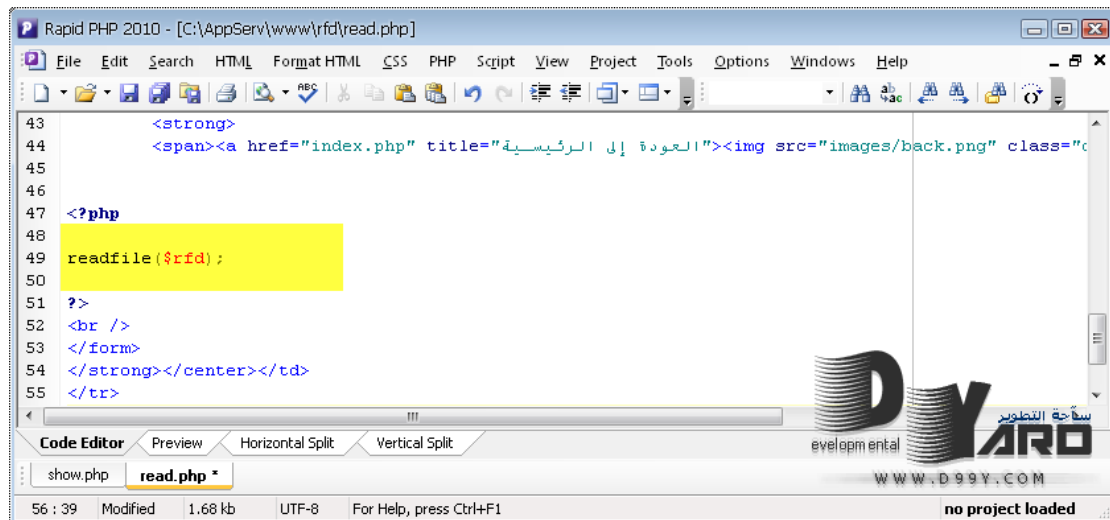
في حالة فتح اي ملف اخر غير الموجود في الشرط ستظهر الرسالة الموضوعه داخل . `echo`

```

Rapid PHP 2010 - [C:\AppServ\www\rfd\show.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>";
50 die;
51 }
52 show_source($rfd);
53
54 ?>
55 <br />
Code Editor Preview Horizontal Split Vertical Split
show.php
57 : 55 1.84 kb UTF-8 For Help, press Ctrl+F1 no project loaded

```

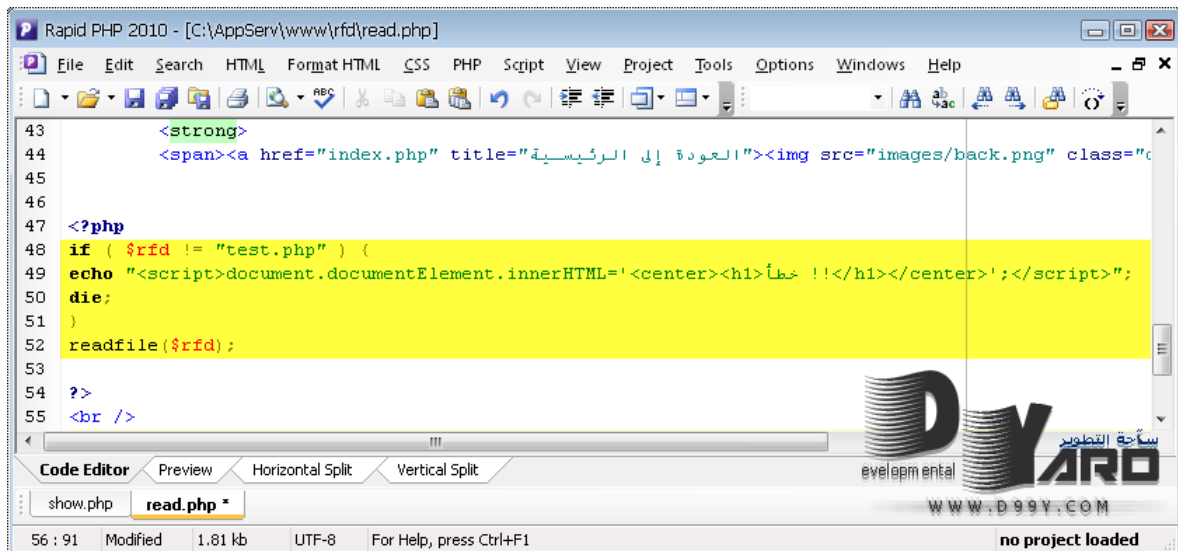
طبعاً بإمكانك وضع اكثر من ملف بواسطة " و `and` او `&&` لاي ملف اخر او بإمكانك وضع الملفات المسموحة داخل مصفوفة `Array` ولك الحرية كمبرمج بالاختيار ..



```
43 <strong>
44 <span><a href="index.php" title="العودة إلى الرئيسية">
52 <br />
53 </form>
54 </strong></center></td>
55 </tr>
```

Code Editor Preview Horizontal Split Vertical Split  
show.php read.php \*  
56 : 39 Modified 1.68 kb UTF-8 For Help, press Ctrl+F1 no project loaded

وكذلك الدالة الاخرى ، في السطر 49 تم تعريف الدالة بمتغير rfd دون الحماية ..



```
43 <strong>
44 <span><a href="index.php" title="العودة إلى الرئيسية">document.documentElement.innerHTML='<center><h1>خطأ !!</h1></center>';</script>";
50 die;
51 }
52 readfile($rfd);
53
54 ?>
55 <br />
```

Code Editor Preview Horizontal Split Vertical Split  
show.php read.php \*  
56 : 91 Modified 1.81 kb UTF-8 For Help, press Ctrl+F1 no project loaded

والحماية كما تعلمنا بواسطة الشرط if وبسهولة ..



و فعلاً تمّ الترفيع ..



تم بحمد الله دراسة ثغرة **Remote File Disclosure - rfd** من جميع النواحي **اكتشاف - توضيح - استغلال - ترفيع** وهذا بفضل الله سبحانه قبل كل شيء

اخواني دائماً ما اعيد واكرر ان الشروحات المطروحة تأخذ وقت كبير جداً مني خصوصاً في اني اعاني من ضيق الوقت ، باسمي لا اريد منكم سوى دعواتكم لي ولوالدي بالتوفيق وحسن الخاتمه وهذا من اكبر الدوافع التي تقوي الشخص للاستمرار وتقديم المزيد ، وكذلك جميع طروحاتي هي موجهه للمبرمجين لطرح برمجيات سليمة والهكر الاخلاقي لتعلم طرق الاختراق والحماية منها ..

اخوكم

**NassRawl**

