

Forum:[Hack Forums](#)

Thread: [\[INFO\] MOST USED HACKING METHODS \[INFO\]](#)

Red Dragon_al - September 3, 2012, 11:49 am

Here u have some of the most used website hacking methods. This are just for info if u want to know more about just use google

1-Blind Structured Query Language Injection (blind SQLi):

Method of once again insufficient security validation and sanitization of user-input.

2-Basic SQLi

This is the easiest method of SQLi. This method allows you to enter codes such as ' or '1'='1 into the username and password fields to gain access. E.g. you find the admin login on a site and you may enter the correct username admin and the password as: ' or '1'='1.

3-Cross Site Scripting (XSS):

A method of injection html/javascript into a website. The XSS can be both persistent attacks, and non-persistent.

4-Remote File Inclusion (RFI):

A method of uploading a shell in to a site

5-Local File Inclusion (LFI) AKA Directory traversal attack:

A method of pulling usernames and passwords off a website vulnerable to the exploit of insufficient security validation / sanitization of user-supplied input file names.

6-Cross site request forgery (CSRF):

An attack that is commonly sent by e-mail or other means and often tricks a user.

Icon_charly_link_greens given to a target may include HTML, something like this:

Code:

Code ``And this will be activated through the victims browser and the site will think it was a valid and intentional move.

7-Public Exploits:

Public exploits are just scripts that people have released for others to use. Such as this exploit which exploits a webserver

running this program on one of its open ports. I suggest you have a quick look through the script to see how/why it works. The way of finding which software you target is using by using Nmap or the GUI Zenmap

8-DNS hijacking:

This is the method or redirecting the domain name to a rouge domain name. This method is used particually in phishing attacks.

9-Bruteforcing:

This method is the practise of running a program to keep guessing the password and username of a site. This method is fastly going out of fashion as the max login attempts are added and even without this obstical, it can take weeks to gain the correct password. Programs commonly used for this are hydra and Brutus.

10-Password Guessing:

Yes, just as it sounds. This is the method of just guessing common passwords such as:

Code:

```
admin
admin123
321admin123
password
toor
thesitesname
```

11-Packet Sniffing:

If you find a site with FTP access, there may be a chance you can use a tool such as cain and abel to sniff their password and username when the login. Not a very easy task as the traffic is sometimes encrypted.

12-RCE (Remote Command Execution):

This is the method of making the server read command that you have entered for it to.

E.g.

Code:

```
index.php?cmd=whoami
index.php?cmd=net user
```

13-Social Engineering:

A common method used to gain information. This can be a long process, but an effective one. They can patch software, but it will always be people's ignorance that will let you/your target down.

14-Cookie poisoning:

This is a method of editing cookies you have already gained, to gain extra privileges. Not a very common method now as of cookies being encrypted, and having to be signed. This exploit can work on some surprising sites, take a look, you may be surprised.

15-Parameter tampering:

An attack usual done by moderfying values in the url. E.g. changing a value to decrease the amount you have to pay on something.

Code:

```
<input type="hidden" id="1008" name="cost" value="70.00">
```

In this example, an attacker can modify the "value" information of a specific item, thus lowering its cost.

source: http://www.owasp.org/index.php/Web_Parameter_Tampering

16-Tamper Data:

A very nifty Firefox addon which is used to modify http/https headers and post parameters.

17-Admin Auth bypass:

This exploit can be as simple as adding:

Code:

```
?action=edit
```

To a URL. This exploit when a server/application allows you to edit by having the valid URL, instead of by cookies. Another method of admin auth bypass is editing the html to proceed even if the

password is wrong.

this is a collection from google results so i give credits to google :p :p

THANKS FOR READING & REPLY

Desmolicious - September 3, 2012, 2:09 pm

CRLF Injection plz? I'm not sure if its a Hacking method but It's pretty useful.

robife - September 3, 2012, 2:12 pm

Thanks for this Red Dragon_al nice post
FLM

VipVince - September 3, 2012, 2:52 pm

Pretty nice list you have made there.

HeXagone - September 3, 2012, 5:05 pm

10-Password Guessing:

YEAh this is a good methode lol

Starfall - September 3, 2012, 5:15 pm

RFI's nearly dead. Great list, though. I'm sure it'll help someone out.

Zixem - September 3, 2012, 8:01 pm

>Your topic is "MOST USED HACKING METHODS" and the first one is Remote File Inclusion...this method is almost extinct.

>I think you should put the XSS first, then SQLi.

Back to the topic: nice list you did there (:

TheNeutron - September 4, 2012, 2:48 am

Nice list, Helpful for learners like me... You should add some more in the list. THanks! :)

Jae? - September 4, 2012, 2:57 am

Great list. Will seriously help the beginners. Although, I don't understand why RFI is first considering it's almost dead. Swap it with something more popular and used today.

Red Dragon_al - September 4, 2012, 3:21 am

(Sep 4, 2012 02:57 AM)Jewel Wrote: [\[CITE\]](#) Great list. Will seriously help the beginners. Although, I don't understand

why RFI is first considering it's almost dead. Swap it with something more popular and used today.

the numbers are not to reveal wich is the most used. just random. I know that RFI it's almost dead but i put it first cuz its the easy one that i have learn and the first one that i have learned but anyway now changed.. its not first anymore

thnx all for the reply

Jae? - September 4, 2012, 3:44 am

(Sep 4, 2012 03:21 AM)Red Dragon_al Wrote: [\[CITE\]](#) the numbers are not to reveal wich is the most used. just random. I know that RFI it's almost dead but i put it first cuz its the easy one that i have learn and the first one that i have learned but anyway now changed.. its not first anymore

thnx all for the reply

Well, judging by your title "MOST USED HACKING METHODS", I think they have to sort of reveal which is the most used, but I'm not going to argue about it. Good job on this once again, amazing collection.

Red Dragon_al - September 5, 2012, 10:31 am

(Sep 4, 2012 03:44 AM)Jewel Wrote: [\[CITE\]](#) Well, judging by your title "MOST USED HACKING METHODS", I think they have to sort of reveal which is the most used, but I'm not going to argue about it. Good job on this once again, amazing collection.
yeah ur right man, thnx for the good reply ? ?

toniohawk2 - September 5, 2012, 10:48 am

Good to see an enumeration like this, thanks for this post :)

Red Dragon_al - September 6, 2012, 11:31 am

(Sep 5, 2012 10:48 AM)toniohawk2 Wrote: [\[CITE\]](#) Good to see an enumeration like this, thanks for this post :)
welcome man thnx for the reply ? ?