

Forum:[Hack Forums](#)

Thread: [\[MEGA\]WEBSITE HACKING\[MEGA\]](#)

BladeCNH - June 11, 2010, 3:15 am

WEBSITE HACKING MEGA THREAD

Well this is my first "serious" thread and I'm going to dedicate it to website hacking (exploiting). This thread will hold threads from other HF members, it will hold those threads I choose, because I thought they were the best explained and easy to understand.

SQL Injection or SQLI

SQL injection is a code injection technique that exploits a security vulnerability occurring in the database layer of an application. The vulnerability is present when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and thereby unexpectedly executed. It is an instance of a more general class of vulnerabilities that can occur whenever one programming or scripting language is embedded inside another. SQL injection attacks are also known as SQL insertion attacks. --[WIKIPEDIA]--

First one is video tutorial created by raahul2008 here is the link to the thread:

<https://hackforums.net/showthread.php?tid=96173&highlight=SQLI+tut>

And here is written tutorial by ADIL:

<https://hackforums.net/showthread.php?tid=469384>

2.XSS

Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications that enables malicious attackers to inject client-side script into web pages viewed by other users. An exploited cross-site scripting vulnerability can be used by attackers to bypass access controls such as the same origin policy. Cross-site scripting carried out on websites were roughly 80% of all security vulnerabilities documented by Symantec as of 2007.[1] Their impact may range from a petty nuisance to a significant security risk, depending on the sensitivity of the data handled by the vulnerable site, and the nature of any security mitigations implemented by the site's owner. --[WIKIPEDIA]--

[img]http://www.mattvirus.net/blog/wp-content/uploads/2008/05/paypal_xss.jpg[/img]

Here is XSS tutorial by #DataBase:

<https://hackforums.net/showthread.php?tid=190627&highlight=xss+tut>

3.RFI and LFI (Remote and Local File Inclusion)

Remote File Inclusion (RFI) is a type of vulnerability most often found on websites, it allows an attacker to include a remote file usually through a script on the web server. The vulnerability occurs due to the use of user supplied input without proper validation. This can lead to something as minimal as outputting the contents of the file, but depending on the severity, to list a few it can lead to:

- Code execution on the web server

- Code execution on the client-side such as Javascript which can lead to other attacks such as cross site scripting (XSS).

- Denial of Service (DoS)

- Data Theft/Manipulation --[WIKIPEDIA]--

Local File Inclusion is ability to execute arbitrary file as a code.(This can be used to gain access to site or steal information)

Here is RFI and LFI tutorial by Loka123:

<https://hackforums.net/showthread.php?tid=208129&highlight=RFI+tut>

4.Rooting

Well everything here is being held in the name.Rooting webserver means using exploits to gain root access to that site, so it can be exploited.

[img]http://aknow.prevx.com/content/blog/c99_owned.jpg[/img]

Here is a rooting tutorial by The 7th Sage:

<https://hackforums.net/showthread.php?tid=192450&highlight=rooting+tut>

5.Metasploit and Nmap

You have all probably heard about Metasploit Framework and Nmap port scanner.Nmap is the best (in my opinion) scanner ever, it doesn't only scan for ports it also has some extra functions, and metasploit is great tool that contains bunch of exploits and it is used to check websites vulnerabilities.

[img]http://maestro-sec.com/blogs/wp-content/uploads/2008/10/metasploit.png[/img]

You can download metasploit here:

<http://www.metasploit.com/framework/download/>

Just choose your OS and when you install metasploit it will ask you to install nmap too.

Here is also a tut on Nmap and Metasploit by VipVince:

<https://hackforums.net/showthread.php?tid=303858>

And here is a detailed tutorial about metasploit:

<http://www.offensive-security.com/metasploit-unleashed/>

5K1DD13 SECTION

OK this is for those guys that loves using tools against their enemy.

1.Havij

Havij is tool created to try all possible SQL (well not exactly ALL) functions and commands to exploit the website, just like SQLI Helper you can use it with Exploit Scanner.

[img]http://redmove.persianguig.com/MyPrograms/havij%201.07%20snap-shot.gif[/img]

You can download Havij here:

<http://www.dl4all.com/software/264965-havij-108-website-hacking-software.html>

2.SQLI Helper

Nothing much to say about this one it has the same purpose as Havij.

[img]http://maxxablog.com/wp-content/uploads/2009/08/ss5-Small-573x332-custom.jpg[/img]

Download SQLI Helper v2.7 here:

<http://www.pccomputerease.com/sql-helper-v2-7-#.html>

3.WVS Scanner

This tool will scan the website for you and show you all vulnerabilities of that website, it will even show you some details about that vulnerability.

[img]http://www.sonicguard.com/images/Acunetix/WVS_v4_Report_Edited_200-lg.jpg[/img]

You can download WVS here:

<http://www.acunetix.com/vulnerability-scanner/vulnerabilityscanner65.exe>

Thats all.Enjoy.

Frank Sinatra - June 11, 2010, 3:29 am

nice but you have forgotten alot of vulnerabilty like xst (cross site tracing) or xsrf (cross site request forgery) and many more but these two are the newest! but great tutorial!

Thug Life - June 11, 2010, 3:30 am

Great tutorial! i love it man. Nice and neat.

LONGRIFLE - June 11, 2010, 3:34 am

nice bro good tut :)

to short

I need yo teach 4.Rooting but I don't have Linux :(can help me ? :?

Moody_KSA - June 11, 2010, 3:43 am

great tutorial,

this thread deserves sticky

BladeCNH - June 11, 2010, 3:56 am

(Jun 11, 2010 03:29 AM)3x0r_\$c0rPi0n Wrote: [\[CITE\]](#) nice but you have forgotten alot of vulnerabilty like xst (cross site tracing) or xsrf (cross site request forgery) and many more but these two are the newest! but great tutorial!

I mentioned only those that are most familliar to most of the users.?

(Jun 11, 2010 03:34 AM)LONGRIFLE Wrote: [\[CITE\]](#) nice bro good tut :)

to short

I need yo teach 4.Rooting but I don't have Linux :(can help me ? :?

You can download linux from the official website of the distro, I recommend you to download Ubuntu 10.04 from

<http://www.ubuntu.com/desktop/get-ubuntu/download>

Cum on guys, anyone else have to say anything????

Vipermakd - June 11, 2010, 4:01 am

Nice and Great work man.. It's a good compilation of great tuts thanks

BladeCNH - June 11, 2010, 4:51 am

Post please!!

ShortyyStillShort

z3pt0seC - June 11, 2010, 5:25 am

<http://www.acunetix.com/vulnerability-scanner/vulnerabilityscanner65.exe>

FOR the last tool to download
--Nice collection--

sami47 - June 11, 2010, 5:26 am

thanks man this will help me alot

texeon - June 11, 2010, 5:29 am

You have done a lovely job, I agree with the others saying you have left things out, but all in all, great job!

BladeCNH - June 11, 2010, 5:39 am

Thank you guys.

Anyone else..

shweetu - June 11, 2010, 6:12 am

cool man !! do it someday

CATMAN - June 11, 2010, 8:18 am

Thanks for great tutorial!!!!

sonicd3f3nc3 - June 11, 2010, 10:34 am

Also missed...Xpath injection...

BladeCNH - June 11, 2010, 10:51 am

(Jun 11, 2010 10:34 AM)sonicd3f3nc3 Wrote: [\[CITE\]](#) Also missed...Xpath injection...
I already wrote this in one of my posts:

I only wrote about those vulnerabilities that are familliar to most of the users.

daneuchar - June 11, 2010, 11:58 am

Nice post With all those thing together !