

Forum:[Hack Forums](#)

Thread: [SQLi pentesting question](#)

gjariolg1657 - May 25, 2020, 4:41 am

Hi,
I am pentesting sqli using sqlmap.
Sqlmap sometimes detects 'it looks like the back-end DBMS is 'CrateDB'', sometimes detects 'it looks like the back-end DBMS is 'Mysql'.
And always detects any one dbms.
Of course, no result.
Is this WAF problem? Is it impossible sqli?

And I am looking for other good sqli pentest tool than sqlmap, which one is better than sqlmap?
Thank you.

gjariolg1657 - May 25, 2020, 6:17 am

(May 25, 2020 05:07 AM)James! Wrote: [\[CITE\]](#) Could you share some of the log please?

And in answer to your second question, sqlmap is one of the best options for CLI tools. There is SQLi Dumper and Havij that are both GUI based.
Thank you for your reply.
there isn't useful log during test, it says "the parameter is not injectable"
I think there is a WAF, so I tested with all tamper script,
Do u think is it impossible to sqli?

gjariolg1657 - May 25, 2020, 6:46 am

(May 25, 2020 06:20 AM)James! Wrote: [\[CITE\]](#) Don't you have your answer then? The parameter isn't injectable.

I want to know how to you use tamper for WAF bypass, if you know about sqlmap well.
My test dbms is mysql and php site.
I tested with all tamper scripts, do u make tamper yourself for sqli test ? or giveup?
Thanks

pizza500 - May 25, 2020, 6:57 am

sqlmap is not good for pentest, its especially for automated database dump
sqlmap alternatives
<https://linuxsecurity.expert/tools/sqlmap/alternatives/>

gjariolg1657 - May 25, 2020, 7:57 am

(May 25, 2020 06:57 AM)pizza500 Wrote: [\[CITE\]](#) sqlmap is not good for pentest, its especially for automated database dump
sqlmap alternatives
Thank you for your good answer.
I'd like to use sqlmap for tamper scripts, sqlmap alternatives also have WAF bypassing functions,too?

pizza500 - May 25, 2020, 8:57 am

waf bypassing need do manually, you dont really will have success with script
shoot me your target

(May 25, 2020 07:57 AM)gjariolg1657 Wrote: [\[CITE\]](#) Thank you for your good answer.
I'd like to use sqlmap for tamper scripts, sqlmap alternatives also have WAF bypassing functions,too?

xBlackMax - May 25, 2020, 10:08 am

If you use scripts for WAF you probably have no idea what occurs behind the scenes and you'll never get better this way.

You may hit me up with additional details and I'll solve it to you and explain you the process step by step.

gjariolg1657 - May 25, 2020, 7:25 pm

I think WAF bypassing is the most important problem in sqli, so I'd like to use tamper with sqlmap.
So is there any other important option for sqli success?

Thanks

kuramiqnko - May 27, 2020, 2:12 am

Whenever I have the same error, finding the backend, but cannot fetch any database I try with --random-agent and/or --hex, sometimes when the injections are plain text they are detected, but when is used with --hex you have better chance not getting detected.

Try it out !