

Forum:[Hack Forums](#)

Thread: [Do SQL injections still work?](#)

Keekboi125 - January 10, 2022, 1:37 pm

I heard a lot of people saying SQL injections don't work anymore, is this true or is it just more difficult or what?

Beladonis - January 10, 2022, 2:37 pm

They still do exist but are becoming rarer over time I guess, as coding practices evolve, example the usage of parameterized queries.

It's just like authentication bypass with SQL injections in login forms, I can imagine back in the days they were prominent, nowadays they are pretty much non-existent because devs learned to sanitize their code. Same goes with RFI/LFI.

Hackers - January 12, 2022, 2:25 pm

It's harder because of frameworks that handle data properly so that everything is fully sanitized. A lot of the web was built on PHP in a time when people didn't understand how user supplied data could break or change queries. Now we have a lot more awareness, so things like prepared statements, data sanitizing, and redundant security measures are used by the majority.

Website generators like Wix, Squarespace, etc have also made it easier for companies to have secure sites. Sure, they could release buggy code or a vulnerability for SQL injection, but the chances are they won't make such a large mistake.

The vulnerable sites are usually made by a junior developer, sometimes a random employee who has "some tech experience". It might be whipped together from a static HTML template, or maybe they'll install an old plugin that has vulns. Either way, this is the most common way that new vulnerable sites come online. Most injectable sites will have been left not updated, or are brought back online after being dead/offline - This can also happen if old software is used by a company, even if updated mostly.

zizoo - January 17, 2022, 7:29 am

i' think its don't work anymore

TramBoarder - January 17, 2022, 7:53 am

I would guess that google dorking for generic vulnerabilities doesn't work very well no matter what it is. The dorks have been used for like a decade or more so any vulnerable site you find is either already hacked and messed up, or the vulnerability can't be exploited at all because the code is broken or something, or already patched. When I started using dorks I pretty much immediately realized this and started making up my own. Still, it seems difficult to find fresh targets.

That being said, just in the last week I found a couple admin login SQL injection vulnerabilities (one of them I later realized you could just login as anything and it would let you in so maybe that doesn't count :P). I also found a couple that seem exploitable because they output code related to the query, but I just couldn't get it to work because I'm still not great at it.

So yeah, As someone who got into hacking pretty recently, it seems like it still works, though I don't know what it was like years ago.

linkinpork - January 17, 2022, 8:29 am

(Jan 10, 2022 02:37 PM)Keekboi125 Wrote: [\[CITE\]](#) I heard a lot of people saying SQL injections don't work anymore, is this true or is it just more difficult or what?

It's still in the OWASP Top 10, but it got demoted to Top 3 in 2021 (from Top 1 in 2017). It falls under Injection, but that also includes other forms of data injection like OS Command Injection and LDAP Injection. Reference: https://owasp.org/Top10/A03_2021-Injection/

SQLMap's bleeding edge update is literally only 4 hours ago so people are obviously still into it.

Cheers!

DevNode - January 25, 2022, 12:01 am

You will always get a new developer who forgets to sanitise the users input.

spidey - February 4, 2022, 5:18 pm

(Jan 25, 2022 01:01 AM)DevNode Wrote: [\[CITE\]](#) You will always get a new developer who forgets to sanitise the users input.

good to know thanks for this^^^

Enzo - February 24, 2022, 4:32 pm

Website attacking in general has decreased in popularity in the Blackhat community over the years for sure. Especially considering how easy it is to paste an SQLi attacks and just most sites having long patched them. Even XSS (Cross Site Scripting) Attacks and Command injections are seldomly used now. Consider the debut of log4j it seems likely there will be a lot of upcoming Java Exploitation in websites. I believe this will become increasingly more popular in the near future.

SIM-5165548 - March 7, 2022, 8:24 am

Yes it is still possible, sometimes it can lead to escalate privileges and make RCE. There is also possibility to make sql injection even if the query is in prepared statement. Unfortunately i can not give link to articles about it because i dont have enough posts. PM me if You are interested.

Sapple - March 9, 2022, 6:29 am

As the first comment quoted, it works, but its very rare now a days. Coding practices have evolved and evolving day by day. Instead look for some other method, that will be easy to do.