

Forum:[Hack Forums](#)

Thread: [SQL injection by hand \(without tools like sqlmap\)](#)

quintet4887 - July 9, 2024, 1:14 am

Hey,

I'm new to the topic of SQL Injections. Reading through some threads, many people recommended to use tools like sqlmap. I was wondering whether SQL Injections by hand (without tools like sqlmap) are still a thing? Is it even realistic today to find a vulnerability without the help of such tools (as a beginner)? What is the learning curve for learning about SQLi when using these tools? I just want to avoid learning more about the tool than the vulnerability.

I am learning about SQLi with the help of PortSwigger Academy. While I'm having little trouble with the labs so far, the websites in the wild seem to be a whole different matter. Most seem to use well tested frameworks which implement countermeasures like input validation, prepared statements, etc. I just want to be sure that I'm on the right track.

G33K - July 10, 2024, 12:28 am

It is possible but use a cheat sheet and go after webpages that has lower security that's vulnerable, there is way to scan this or find list that people share here on the forum..

quintet4887 - July 10, 2024, 2:04 am

(Jul 10, 2024 12:28 AM)hackerg33k Wrote: [\[CITE\]](#) It is possible but use a cheat sheet
Thanks for your reply! That's a good one, I will definitely to that.

(Jul 10, 2024 12:28 AM)hackerg33k Wrote: [\[CITE\]](#) and go after webpages that has lower security that's vulnerable, there is way to scan this or find list that people share here on the forum..

Are Bug Bounty programs are good starting point for that? I looked on HackerOne and even the websites without a payout and less tested usually rely on systems like WordPress, use Cloudflare's security products or implement prepared statements themselves, making it virtually impossible to find anything (for me). Or should I search for possible websites on other ways (outside bug bounty programs)?

DenkiGishi - July 11, 2024, 4:04 pm

I'll reply here to follow this as I'm also interested to learn more about SQL injections without tools, especially if anyone has any recommendations on whether or not SQLi may be viable from a mobile device, but I'll assume it has largely to do with whether or not the target website has existing vulnerabilities

Py_Dev - July 13, 2024, 5:10 am

owasp-zap is a good tool. Give it a shot.