

Forum:[Hack Forums](#)

Thread: [XAMPP, PHP, SQLi, and MySQL](#)

jj1972 - September 2, 2013, 12:22 pm

Hi,

I'm an XAMPP user and after all this practicing of SQL injection on other sites for two months and learning a bit, I've decided I need to spend some quality 'defensive' time building a test site on my localhost. I intend to build a MySQL database and a PHP interface.

As an exercise I would like to build various interfaces, with each one providing a bit more security than the previous one. The lowest protected site would be vulnerable to SQLi and XSS.

Have any of you done this before? If so, do you have any suggestions? Lessons learned? I imagine you became better in attacking sites.

Here are some goals of mine.

1. Block all regular SQL injections. Duh!
2. Without using WAF, use regular expressions to detect/filter obfuscated SQLi attacks.
3. Decrease security so blind injections will work.
4. Write tools.
 - a. Brute force blind injection tool.
 - b. Analyzer that detects attacks and logs to a file.
5. Upload database and code to a host online, and invite others to give it a go.

Regards,
JJ

Blockchain - September 2, 2013, 10:37 pm

Simple prevention to SQL injection - prepared statements.

SHADOW REALM - September 2, 2013, 10:40 pm

Look over DVWA, That's the exact same thing your thinking of

jamesWonka - September 2, 2013, 10:40 pm

As user above said, use prepared statements and filter any and all user input that may or may not be displayed on the site (htmlspecialchars()) it's really not too hard to protect your site from these things. The servers security should be much more worry some if you're a good developer.

PigBacon - September 3, 2013, 6:20 am

(Sep 2, 2013 10:40 PM)jamesWonka Wrote: [\[CITE\]](#) As user above said, use prepared statements and filter any and all user input that may or may not be displayed on the site (htmlspecialchars()) it's really not too hard to protect your site from these things. The servers security should be much more worry some if you're a good developer.

But only filter information with something like htmlspecialchars when you're required to - e.g. displaying it. Keep your data pure when it's stored.

cull980ssbsgu - September 3, 2013, 10:44 am

(Sep 3, 2013 06:20 AM)plausibility Wrote: [\[CITE\]](#) But only filter information with something like htmlspecialchars when you're required to - e.g. displaying it.

Keep your data pure when it's stored.

I m satisfied with u , if we are saving a secure data into database when any data is entered no chance for sql injection

jj1972 - September 5, 2013, 2:30 pm

Hi,

Thanks for your thoughts.

One goal is to build a system that is secure...as secure as I can make it. And then "reduce security" so a blind SQLi scenario is presented. I'm really curious about creating this through 'improper/incomplete' coding.

You mention saving secure data. I had only thought about 'reading' data with SQLi. I'll add a form for a user to upload a comment or conduct a search. That will need protecting too.

Thanks again,
JJ

Ego Inc - September 5, 2013, 10:08 pm

<http://www.hackthissite.org/> Have fun :)