

Forum:[Hack Forums](#)

Thread: [\[havij\] what do i do when this happens \[havij\]](#)

Bag - January 22, 2011, 2:44 am

So it sayd its vulnerable but just stops!? where do i go from there?

[IMG]http://i52.[censored].com/314f5tx.jpg[/IMG]

?

ssihiss - January 22, 2011, 2:52 am

TABLES and colums etc ;;; this is a new version right ? lol mybe it's a bug

Bag - January 22, 2011, 12:58 pm

I CANT Go to tables columns ect it just ends after there and idk what to do :/

yeh im on 1.14 should i go back to 1.13? maybe someone has the full version of that idk?

im really stuck lol

ThankYouAndGoodbye - January 22, 2011, 1:26 pm

Its a bug in havij when it selects an unreliable regex, you would be able to exploit the site if you had taken the time to learn manual injection instead of relying on zero skill skids tools.

Bag - January 22, 2011, 1:31 pm

I have read many manual injections on this site and they are all fine but HARDLY WORK!

WHY? Becuase by the time its been posted everywhere it now is 1. not as good 2. doesnt get a decent site to exploit...

I ONLY use havij to Speed up the process so I dont have to sit there entering in code that may or may not work for four hours...

Could you maybe just point me to a thread that could help me with exploiting if i have a "unreliable regex"

-Thanks!

ThankYouAndGoodbye - January 22, 2011, 1:41 pm

Theres an easy answer to that, dont use havij, if your competant in manual sql injection revert back to that, the site is obviously vulnerable but havij cant determine a column count and thus cant call a group_concat() to pull information from the DB, however if you took a manual approach to it you would notice the changes in the site that havij missed because havij only reliese on the presence of one word in a web page to determine if it has changed.

And your obviously not very good at sql injection if it takes your 4 hours per site.

Bag - January 22, 2011, 2:03 pm

well I am posting in begginer hacking now huh? ^.^

ohokay so your saying i should re-find the column count on my own and go from there?

ThankYouAndGoodbye - January 22, 2011, 2:09 pm

Yes, havij is obviously returning false positives when it comes to the column count. If you want to stick to using skid tools, ill give you a tip: Change havij's "database" option to "mysql blind" - this will force havij to treat any sql injection like a blind injection and instead of relying on a correct column count with the group_concat() call, it will soley rely on llooking for positives when gussing table names letter by letter - it will take longer, but it wont require any skill or brain power on your behalf.

Bag - January 22, 2011, 2:12 pm

Haha! Well thanks a bunch! As much as you sound like and uber dick I get that your probably tired of n00bs on here loocking for the easy way out XP ill go read some more threads and see if i can tackly this without havij

-Thanks

ThankYouAndGoodbye - January 22, 2011, 2:17 pm

When you fully understand manual sql injection, you see why havij is a peice of shit. Im just sick of seeing people relying on it as there only method of sql injection because its piss poor, havij can on only successfully exploit 1 in 5 sql injections that a human could do manually.

I just prefer to make people think before giving them an easy way out.

Happy Hacking