

Forum:[Hack Forums](#)

Thread: [Site completely vulnerable to SQLi but cannot find any links](#)

Eminem? - April 15, 2014, 10:28 am

Hey guys,

So yes I'm using havij like a skid, but I've attempted manual before and it was really tough for me, I want to keep going a bit with havij while learning manual and get a better understanding of manual SQLi so don't worry about that.

I was just wondering, I'm trying to get a DB of a site, I can tell it's vuln. because it has MySQL errors all over the pages and most links don't even work because of that.

But I'm pretty sure havij requires a link that ends with, for example:

website.com/userid=3, notice how the 3 looks like balls lol...

Anyway, I can't find any links of the sorts, so what do I put into havij?

Thanks!!

WayOfTheTitans - April 15, 2014, 10:42 am

skid.com/niggerchess.php?negres=1337

vac33 - April 15, 2014, 10:55 am

You need to find a page that first of all uses sql. Look for userpages and fourm posts. What are the SQL errors? Not all SQL errors mean that the site is venerable. For example the database could be renamed without reconfiguring the site to the new database

Eminem? - April 15, 2014, 11:02 am

Alright, here are some examples of the errors:

Warning: mysql_fetch_row(): supplied argument is not a valid MySQL result resource in /usr/local/home/httpd/vhtdocs/satin/main/config.php on line 33

select bookID,imprint,title,subtitle,author,cover,ISBN,pub_date,price,disc_price,avail,short_blurb from books where bookID=

Warning: mysql_fetch_row(): supplied argument is not a valid MySQL result resource in /usr/local/home/httpd/vhtdocs/satin/main/preorder.php on line 14

Thanks!

vac33 - April 15, 2014, 11:09 am

In my experience that error is usually caused by the wrong host name selected in defining the db or the permission setup for accessing the database being incorrect in. In essence the reason why you're having trouble SQLi'ing the site is because the database isn't even functional with it.

WayOfTheTitans - April 15, 2014, 11:11 am

(Apr 15, 2014 11:09 AM)vac33 Wrote: [\[CITE\]](#) In my experience that error is usually caused by the wrong host name selected in defining the db or the permission setup for accessing the database being incorrect in. In essence the reason why you're having trouble SQLi'ing the site is because the database isn't even functional with it.
this is wrong. Its because the request for information from the database is not formatted using a GET request. use post.

Eminem? - April 15, 2014, 11:11 am

Ohh, I see what you're saying. Shame though, I guess I'll work on another site.

Thanks man!

vac33 - April 15, 2014, 11:19 am

(Apr 15, 2014 11:11 AM)WayOfTheTitans Wrote: [\[CITE\]](#) this is wrong. Its because the request for information from the database is not formatted using a GET request. use post.

That doesn't even make sense. He's getting errors for the website before injecting, not only afterwards. ?

(Apr 15, 2014 11:11 AM)Eminem? Wrote: [\[CITE\]](#) Ohh, I see what you're saying. Shame though, I guess I'll work on another site.

Thanks man!

No worries, you might want to keep that website written down as a possibility for non sqli exploits though

WayOfTheTitans - April 15, 2014, 11:37 am

(Apr 15, 2014 11:19 AM)vac33 Wrote: [\[CITE\]](#) That doesn't even make sense. He's getting errors for the website before injecting, not only afterwards. ?

No worries, you might want to keep that website written down as a possibility for non sqli exploits though

you are so fucking retarded it hurts. You dont understand the principles of why sql errors occur do you?

pwntoken - April 20, 2014, 8:24 am

(Apr 15, 2014 10:28 AM)Eminem? Wrote: [\[CITE\]](#) Hey guys,

So yes I'm using havij like a skid, but I've attempted manual before and it was really tough for me, I want to keep going a bit with havij while learning manual and get a better understanding of manual SQLi so don't worry about that.

I was just wondering, I'm trying to get a DB of a site, I can tell it's vuln. because it has MySQL errors all over the pages and most links don't even work because of that.

But I'm pretty sure havij requires a link that ends with, for example:

website.com/userid=3, notice how the 3 looks like balls lol...

Anyway, I can't find any links of the sorts, so what do I put into havij?

Thanks!!

because the the data is pulled out via a web service called 'REST'.

(Apr 15, 2014 10:28 AM)Eminem? Wrote: [\[CITE\]](#) Hey guys,

So yes I'm using havij like a skid, but I've attempted manual before and it was really tough for me, I want to keep going a bit with havij while learning manual and get a better understanding of manual SQLi so don't worry about that.

I was just wondering, I'm trying to get a DB of a site, I can tell it's vuln. because it has MySQL errors all over the pages and most links don't even work because of that.

But I'm pretty sure havij requires a link that ends with, for example:

website.com/userid=3, notice how the 3 looks like balls lol...

Anyway, I can't find any links of the sorts, so what do I put into havij?

Thanks!!

because the the data is pulled out via a web service called 'REST'.