

Forum:[Hack Forums](#)

Thread: [SQL Injections website http - https](#)

Kulls - January 25, 2016, 12:55 pm

Hello,

I have some questions as :

How SQL injections into a website or there are no variables in the URL (

<http://www.exemple.com/id=5>), here is the variable "id =" ?

And, to a secure website (https) ?

Greating ! ?

Frosteh - January 26, 2016, 7:22 am

You can inject anywhere that takes user input or any kind of external data and puts into the database, the different injection points depend on how the website is built, you need to investigate and experiment or use tools to scan.

A lot of the time page parameters are no longer written as ?variable1=value1&variable2=value2 but can be part of the a (virtual) directory structure such as /news/group/date/headline-news, here the "date" part may be re-written into a parameter used to query a database.

You can inject into the body of posts which post back user data, normally you'd proxy your browser traffic through something like burp suite or ZAP to intercept and modify the post request to include your injection, or use browser add ons to modify it.

Another injection point that is more rare is through cookie values, if for whatever reason the website takes users cookies and stuffs them into a database that's a possible injection point. Websites may be built to collect any kind of user information and put it into a database such as browser name and version, your location, etc. Many of those things can be spoofed and so have the potential for injection.

There's many others, too many for me to list. Some can be very hard to find if it's not obvious the page is collecting that information.

HTTPS can be injected in the same way that HTTP is, if you want to proxy the traffic through a proxy then you'll need to generate a valid SSL certificate for the proxy and install that cert into your browser.

Kulls - January 26, 2016, 11:30 am

Hey !

Thank you for the response !

You've cleared me of my thoughts about them (https) ?, you say that SQL injections are the same as for the http protocol I already tried on sites with havij, and each time the log there was written "Moved Permanently" or "404 forbidden" or something! I do not understand ! Especially havij trouverles BDD is renowned for a site with more than 95% success rate! :\$

I had already tried by hand, and it did nothing.

Do you have any examples to offer me of advanced SQL injections at sites that do not have variables?

Also, I have another question to ask you, (for I see that you are immersed in the field of computer security ?), why servers and web sites use "?", Not "" or another symbol in the URL?

Great ! ?

?Anubis - January 26, 2016, 2:14 pm

You need to have a variable for sql.

And HTTPS has nothing to do with sql, it only encrypts the request to block MITM attacks.

s3cr3t - January 27, 2016, 3:16 pm

hello there,

when you trying to inject https website using havij , you have to change " h t t p s : / / " to "h t t p : / /"

deleting "s" from "https"
and it will work.

Saint - January 27, 2016, 3:19 pm

(Jan 27, 2016 04:16 PM)s3cr3t Wrote: [\[CITE\]](#) hello there,

when you trying to inject https website using havij , you have to change " h t t p s : / / " to "h t t p : / /"

deleting "s" from "https"
and it will work.
Don't use Havij.

?Anubis - January 27, 2016, 3:56 pm

(Jan 27, 2016 04:16 PM)s3cr3t Wrote: [\[CITE\]](#) hello there,

when you trying to inject https website using havij , you have to change " h t t p s : / / " to "h t t p : / /"

deleting "s" from "https"
and it will work.
WTF? OMFG! You're saing we can't inject https websites? ?

Disparity - January 27, 2016, 6:53 pm

(Jan 26, 2016 03:14 PM)?Anubis Wrote: [\[CITE\]](#) You need to have a variable for sql.
No you don't.

?Anubis - January 27, 2016, 11:48 pm

(Jan 27, 2016 07:53 PM)Disparity Wrote: [\[CITE\]](#) No you don't.
You need something.

Kulls - January 28, 2016, 1:10 am

(Jan 27, 2016 04:16 PM)s3cr3t Wrote: [\[CITE\]](#) hello there,

when you trying to inject https website using havij , you have to change " h t t p s : / / " to "h t t p : / /"

deleting "s" from "https"
and it will work.I know I had already tried without success

Thanks for all responses !

you can not use automated software as havij poutmr https sites ?
They are therefore , not hackable except leaks in cryptography https (ssl , tls , etc ...)
another question how Russian hackers were able to hack over 4 billion addresses mail and password ?
I think they should be https sites ...
Great ! ?

Kulls - January 30, 2016, 4:46 am

Nobody knows?
Nobody to answer me ?
? ? ?

JaNuS18 - January 30, 2016, 5:47 am

(Jan 28, 2016 02:10 AM)Kulls Wrote: [\[CITE\]](#) ..
you can not use automated software as havij poutmr https sites ?
They are therefore , not hackable except leaks in cryptography https (ssl , tls , etc ...)
Where is you statement (such sites are not hackable if havij can't inject https sites) coming from? ?

You don't need automated software like Havij to inject a site. Manual injection is more powerful.

Tools are good only for time consuming tasks (blind injection)

Kulls - January 30, 2016, 9:47 am

Hey !
Thanks for answer ! ?
He's an automated software like Havij to make SQL injections on https websites ?
Is it possible to avoid redirects with Havij ?

Can you give me an example of SQL injection in the URL (http), but variable (exemple: "http://www.exemple.com/index.php?id=5").
When we enter a URL in havij, which symbol can we put at the end of the URL? (- Or / / or / * or something else), which could help Havij ?

Great !

JaNuS18 - January 30, 2016, 11:09 am

My message was: Don't use Havij.

Otherwise you will never understand what is going on when you inject some site. Beside in most cases Havij can't bypass WAF...

You can manually inject on many sites where tools fail.

Kulls - January 30, 2016, 1:10 pm

Thank you, but can you give me an example of SQL injection in the URL (http), but variable (exemple: "http://www.exemple.com/index.php?id=5").
When we enter a URL in havij, which symbol can we put at the end of the URL? (- Or / / or / * or something else), which could help Havij or another soft ?
I can't found example on the net, so...

Frosteh - February 1, 2016, 1:53 am

How do you mean help Havij? You're talking about comments which for MySQL

Single line comment --

Multi line comment /* start and */ stop

Single line comments are used to make sites vulnerable to SQLi ignore everything after the injection point, multi-line comments can't be used outside of some very specific circumstances because they require the closing comment */ symbols to be valid SQL.

JaNuS18 is right, don't use Havij, if you want to get really good at SQLi then you'll want to learn how to write it by hand and practice doing that, applications like Havij will never be able to inject everything for you. There's a huge number of resources to learn SQLi manually, hundreds of tutorials including some really in depth ones on my blog.

I think the general consensus in the hacking communities is that running apps like Havij isn't really hacking, if you want to be a real hacker then learn the knowledge and do it yourself.