

Forum:[Hack Forums](#)

Thread: [Blind SQL injection help](#)

wattseat - January 15, 2020, 7:58 pm

Hi

I'm putting some effort on getting access to username and password of an .aspx page.

I've been trying blind sql injection since the page isn't amenable to classic injection.

My question is: Am I still able to perform a blind sql attack if the page responds to true statements by not loading (progress bar just keeps spinning)? If a false statement is inserted, for instance id=1 and 1=2, the page produces a custom error.

Any help is appreciated
Thanks.

ropslide - January 15, 2020, 8:05 pm

Quote:Am I still able to perform a blind sql attack if the page responds to true statements by not loading (progress bar just keeps spinning)?

Definetly. That is the point of a blind SQL injection.

wattseat - January 15, 2020, 8:10 pm

I have almost no experience, except what i've been reading and trying over the last like 36 hours.

sqlmap couldn't find ejection points (assuming I did everything right), and every page I looked into explaining how to perform the process manually, assumes that true statements are going to follow through and are based on a delay command for verification. But in my case, the page just won't load, and I can't seem to find a comprehensive tutorial for m situation.

Tyr - January 15, 2020, 8:13 pm

(Jan 15, 2020 09:10 PM)wattseat Wrote: [\[CITE\]](#) I have almost no experience, except what i've been reading and trying over the last like 36 hours.

sqlmap couldn't find ejection points (assuming I did everything right), and every page I looked into explaining how to perform the process manually, assumes that true statements are going to follow through and are based on a delay command for verification. But in my case, the page just won't load, and I can't seem to find a comprehensive tutorial for m situation.

Don't rely too much on SQLmap. Always scan, then if this fails, manually look for a vuln. If you do not know how to find vulns manually, send me a PM. Also, it's injection* haha.

Teferi - January 16, 2020, 3:45 am

You can get the response time with python using the total_seconds method:

```
Code response = requests.post(url, data=post_fields, timeout=timeout)
print(response.elapsed.total_seconds())
```

You say it keeps loading, maybe you can write your own program to dump the database and use the total_seconds method to see if it's either TRUE or FALSE.

Kitty - May 5, 2020, 4:06 pm

I've encountered a problem with blind inj. cause the results that come up with the ascii table are one letter before the actual letter but I can't get the final results out.

For example I get "fqnto_hc" instead of group_id or "oarrvnqc" instead of password.. -_- Could someone please check what's happening, thanks !!

sinclairKali - May 7, 2024, 11:27 am

why is blind sql injection so hard?