

Forum:[Hack Forums](#)

Thread: [SQL INJ Bild - xss](#)

A Data - July 12, 2017, 4:27 am

Hello

Can you help me

I want to hack this site .scom.au/gpStudent

I scanned web site with the program

And there are security problems

Blind SQL Injection

POST (multipart) input username was set to

```
if(now()=sysdate(),sleep(0),0)/*XOR(if(now()=sysdate(),sleep(0),0))OR""XOR(if(now()=sysdate(),sleep(0),0))OR""*/
```

krlo-s - July 12, 2017, 7:30 am

Time based SQLi, a pain in the arse imo. It might be vulnerable to other technique tho

andmuchmore - July 12, 2017, 5:19 pm

That looks like an Acunetix payload.

Sometime acunetix time based sql injections are a false positive. Try injecting with sqlmap something along the lines of

Code `./sqlmap.py -u "url.here" --data "postdatahere" -p username --random-agent`

Alot of the time blind injections are vulnerable to both time based and boolean based, if it is vulnerable to boolean based injection, crank up the threads in sqlmap which will increase the speed of the injection.

If sqlmap doesn't find the vuln, try testing if it is vuln yourself manually. Change the sleep() function in the query to different numbers (ie sleep(5)) the page could pause loading for 5 seconds or how every long you specify. If the page successfully sleeps, then you can move onto manual injection. If that is the case, I can give you a script that will automate the injection if you give me the injection syntax.

If you have any problems, hmu and I will help you

Gardener Jim - July 13, 2017, 12:23 am

I cannot even locate that site..

andmuchmore - July 13, 2017, 9:57 pm

I found the site he was referring too.. I am pretty sure its a false positive. I couldn't replicate the vulnerability (even though acunetix detected it)

A Data - July 18, 2017, 2:14 am

@andmuchmore i'm not pm for u

(Jul 12, 2017 05:19 PM)andmuchmore Wrote: [\[CITE\]](#) That looks like an Acunetix payload.

Sometime acunetix time based sql injections are a false positive. Try injecting with sqlmap something along the lines of

```
Code ./sqlmap.py -u "url.here" --data "postdatahere" -p username --random-agent
```

Alot of the time blind injections are vulnerable to both time based and boolean based, if it is vulnerable to boolean based injection, crank up the threads in sqlmap which will increase the speed of the injection.

If sqlmap doesn't find the vuln, try testing if it is vuln yourself manually. Change the sleep() function in the query to different numbers (ie sleep(5)) the page could pause loading for 5 seconds or how every long you specify. If the page successfully sleeps, then you can move onto manual injection. If that is the case, I can give you a script that will automate the injection if you give me the injection syntax.

If you have any problems, hmu and I will help you

is not work

please Help

login site is method post

not attack from sql map