

Forum:[Hack Forums](#)

Thread: [The Alchemist's SQLi Vulnerability Scanner](#)

The Alchemist16 - November 19, 2012, 12:11 am

The Alchemist's SQLi Vulnerability Scanner

Hello Hackforums,

I've come up with a new script. I'd like to share this cool script with you.

This script checks if the entered URL is vulnerable to SQL Injection(GET) or not...

Advantage of using this script :

I've given a textbox to enter the URLs. You can enter more than one URL to be checked.

Very often you come across huge lists of URLs and people say that they are all Vulnerable to SQLi. Well, this is what you'll need then...

Enter all the URLs and Scan for SQLi Vulnerability.

The URLs need to be entered in the textbox in this way :

Code `www.example1.com/index.php?id=1`

`www.example2.com/index.php?id=1'`

`http://www.example3.com/index.php?id=1`

`www.example4.com/index.php?id=1'`

`www.example.com/index.php?id=1`

One URL in one line.

Here's the script :

PHP Code

```
<?php
<!DOCTYPE html PUBLIC
"-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta http-equiv="author" content="The Alchemist"/>
<link rel="shortcut icon" href="favicon.ico" />
<title>SQLi Vulnerability Scanner</title>
<style type="text/css">
.text {
    font-family: "Comic Sans MS", cursive;
    color: #999;
}
.box {
    font-family: "Comic Sans MS", cursive;
    font-weight: bold;
    color: #00F;
    background-color: #FF9;
```

```

}
</style>
</head>

<body background=
"http://fc00.deviantart.net/fs70/i/2011/324/9/2/black___purple_textures_by_paralyzinglove-d4gscvx.j
pg">
<p align="center">
</p>
<br /><br />
<p align="center"><font class="text" size="5">SQL Injection Vulnerability Scanner</font>
<br /><br />
<font face="Comic Sans MS, cursive" size="3" color="#FFFFFF">Only post URLs like this : <br />
http://www.example.com/index.php?id=1<br />OR<br />www.example.com/index.php?id=1
</font></p>
<br /><br /><br />
<p align="center">
<form method="post" action="">
<textarea name="url" class="box" cols="80" rows="10"></textarea>
<br /><br /><br />
<input type="submit" name="submit" value="Scan" />
</form>
</p>
<br /><br /><br />
<p align="center">
<?php
//SQL Injection Vulnerability Scanner coded by The Alchemist
function get_content($url)
{
    $ch = curl_init();

    curl_setopt ($ch, CURLOPT_URL, $url);
    curl_setopt ($ch, CURLOPT_HEADER, 0);

    ob_start();

    curl_exec ($ch);
    curl_close ($ch);
    $string = ob_get_contents();

    ob_end_clean();

    return $string;
}
function is_vulnerable($url)
{
    $contents = @get_content($url);
    if(((strpos($contents,"sql") || strpos($contents,"SQL"))
        && strpos($contents,"error")) || (strpos($contents,"mysql_")
        && strpos($contents,"()")))
    {
        echo '<font face="Comic Sans MS, cursive" size="4" color="#00FF00">';
    }
}

```

```
    echo $url." is vulnerable to SQL injection<br>";
}
else
{
    echo '<font face="Comic Sans MS, cursive" size="4" color="#FFFFFF">';
    echo $url." is not vulnerable to SQL injection<br>";
}
echo '</font>';
}
if(isset($_POST['url']) && isset($_POST['submit']))
{
    $arr=explode("\n",strip_tags(htmlentities($_POST['url'])));
    foreach($arr as $ar)
    {
        $ar=trim($ar);
        if(!strstr($ar,"http://") && !strstr($ar,"https://"))
        {
            $ar="http://".$ar;
        }
        if(!strstr($ar,""))
        {
            $ar=$ar."";
        }
        if(strstr($ar,"?") && strstr($ar,"=")
            && filter_var($ar, FILTER_VALIDATE_URL))
        {
            is_vulnerable($ar);
        }
    }
}
?>
</p>
</body>
</html>
```

Save it with .php extension and then surf...

Thats all..
Enjoy..?

PLEASE GIVE FEEDBACK!!!

Swish - November 19, 2012, 7:24 am

Nice release, going to try this out!

The Alchemist16 - November 19, 2012, 7:29 am

Yani Wrote:What if the application doesn't return errors?Application? Where do you see an application here that'll return errors? If you mean to say that the page in the URL does not return errors, then the URL is not vulnerable to SQLi.

RogueXD Wrote:Nice release, going to try this out!Thanks... Do give feedback after trying out...

The Alchemist16 - November 19, 2012, 7:47 am

Yani Wrote:That's a web-application and if it doesn't return errors it can still be vulnerable to blind

SQL injection.Oh. Sorry mate, I misunderstood you.

The script that I made only checks for GET UNION based SQLi Vulnerability..

For checking blind SQLi vulnerability, this script won't work... And I don't think it'll be easy to make a script that checks for blind SQLi because you need to manually type things like this 0'or'0'='0 and click the submit button..

In my script, if the URL ending with ' does not return an error, the URL is not vulnerable to UNION based GET SQLi....

JoinSeventh - November 19, 2012, 8:11 am

(Nov 19, 2012 08:47 AM)The Alchemist16 Wrote: [\[CITE\]](#) Oh. Sorry mate, I misunderstood you.

The script that I made only checks for GET UNION based SQLi Vulnerability..

For checking blind SQLi vulnerability, this script won't work... And I don't think it'll be easy to make a script that checks for blind SQLi because you need to manually type things like this 0'or'0'='0 and click the submit button..

In my script, if the URL ending with ' does not return an error, the URL is not vulnerable to UNION based GET SQLi....

It can still be vulnerable to Union Based SQL Injection even though the app doesn't give you an error.

Very often the indication if a webapp is vulnerable could be something like that images or text dissapears or you can even get redirected.

A test you could do in addition to checking for SQL Errors could be something like the following (Pseudo-code):

```
PHP Code
<?php
url-source = getsource("http://target.com/index.php?id=1")
url-source-true = getsource("http://target.com/index.php?id=1" + "+and+1=1--")
url-source-false = getsource("http://target.com/index.php?id=1" + "+and+1=2--")
if(url-source == url-source-true){
    if(url-source-true != url-source-false)
        output "Target is vulnerable"
}
```

This would be an indication that the target is vulnerable to either Union, Error or Blind SQL Injection.

Ofcourse this test would not be accurate if the website dynamically changes, in that case you could use something like pattern matching to determine if website content disappears or changes.

The Alchemist16 - November 21, 2012, 8:41 pm

Alright.... Thanks for the snippet... And the feedback ofcourse...

ShitTaker99 - November 21, 2012, 9:55 pm

(Nov 19, 2012 09:11 AM)JoinSeventh Wrote: [\[CITE\]](#) A test you could do in addition to checking for SQL Errors could be something like the following (Pseudo-code):

```
PHP Code
<?php
url-source = getsource("http://target.com/index.php?id=1")
url-source-true = getsource("http://target.com/index.php?id=1" + "+and+1=1--")
url-source-false = getsource("http://target.com/index.php?id=1" + "+and+1=2--")
if(url-source == url-source-true){
    if(url-source-true != url-source-false)
        output "Target is vulnerable"
}
```

This would be an indication that the target is vulnerable to either Union, Error or Blind SQL Injection.

Ofcourse this test would not be accurate if the website dynamically changes, in that case you could

use something like pattern matching to determine if website content disappears or changes.
what happens if it gives a 404 page?

The Alchemist16 - *November 23, 2012, 12:46 am*

It wont give 404 error... Chances are very less...