

Forum:[Hack Forums](#)

Thread: [Remote File Inclusion vulnerability scanner](#)

-zERaIT - March 19, 2015, 12:34 pm

Hello,

Lately I've been working on writing a script which checks a website if it's vulnerable for Remote File Inclusion attacks.

It basically includes the facebook homepage (<http://www.facebook.com>) and from there I can see if it's vulnerable or not.

If you don't know what Remote File Inclusion is, then below some explanation.

Quote:Remote File Inclusion requires allow_url_fopen and allow_url_include to be enabled.

In most cases allow_url_include is disabled by default.

If allow_url_include is disabled RFI could still occur through functions like file_get_contents and fopen if allow_url_fopen is enabled (and the developer is dun goofd, this takes some extremely bad coding).

As you may have noticed, RFI is quite an uncommon vulnerability these days and thats the reason why I wrote the script.

My source

PHP Code

```
<?php
<html>
<head>
<title>RFI Vulnerability Scanner</title>
<style>
body {
background-color: grey;
text-align: center;
color: black;
}
</style>
</head>

<body>
<h1>RFI Vulnerability Scanner</h1>
<form method="POST" action="">
Website:
<input type="text" name="url" value="http://www.site.com/index.php?id=" size="55" />
<input type="submit" name="submit" value="Scan" />
</form>

<?php
class rfivulnscanner
{
    private $rfiinclude = array("http://www.facebook.com");
    private $rfierrors = array("Welcome to Facebook - Log In, Sign Up or Learn More");
```

```

function valid($website){
if(filter_var($website,FILTER_VALIDATE_URL) && strstr($website,"="))
return true;
return false;
}

```

```

function contents($website) {
$agent= 'Mozilla/5.0 (Windows NT 6.1; WOW64; rv:23.0) Gecko/20100101 Firefox/23.0';
$sche = curl_init();
curl_setopt($sche, CURLOPT_SSL_VERIFYPEER, false);
curl_setopt($sche, CURLOPT_VERBOSE, true);
curl_setopt($sche, CURLOPT_RETURNTRANSFER, true);
curl_setopt($sche, CURLOPT_USERAGENT, $agent);
curl_setopt($sche, CURLOPT_URL,$website);
$result=@curl_exec($sche);
return $result;
}

```

```

function checkerror($url,$add,$errorar) {
foreach($add as $val)
{
$website = $url.$val;
$contents = $this->contents($website);
foreach($errorar as $err)
{
if(strstr($contents, $err))
return true;
}
}
return false;
}

```

```

function rfivulnerable($website) {
$web = $website;
$website = substr($website,0,strpos($website,'=')+1);
if($this->checkerror($website,$this->rfiinclude,$this->rfierrors))
echo htmlentities($web) .
" <span style=\"color: green;\">might</span> be vulnerable to RFI.<br />";
else
echo htmlentities($web) .
" is probably <span style=\"color: red;\">NOT</span> vulnerable to RFI.<br />";
}
}

```

```

if(isset($_POST['url']) && isset($_POST['submit']))
{
$obs = new rfivulnscanner();
$website = $_POST['url'];
if($obs->valid($website)) {
$obs->rfivulnerable($website);
}
else {
echo "<span style=\"color: red;\">". htmlentities($website) ." is not a valid website.</span>";
}
}

```

```
}  
}  
?>  
</body>  
</html>
```

Eitherway, use it as you want. If you have any questions, feel free to ask.

MineSQL - March 19, 2015, 12:51 pm

I've only glanced at it, but you shouldn't be suppressing cURL errors, catch them instead. Perhaps create a bulk site function, since this tool is pretty useless by manually inputting one website at a time.

-zERaIT - March 19, 2015, 2:14 pm

(Mar 19, 2015 12:51 PM)MineSQL Wrote: [\[CITE\]](#) I've only glanced at it, but you shouldn't be suppressing cURL errors, catch them instead. Perhaps create a bulk site function, since this tool is pretty useless by manually inputting one website at a time.

Allright, I'll try to catch them instead of supressing and I'll look into your bulk site function aswell. Thought about it myself aswell but first wanted to let it work for only 1 website.

Thanks for the tips tho.

-zERaIT - March 20, 2015, 1:28 am

(Mar 19, 2015 03:06 PM)Yani Wrote: [\[CITE\]](#) LFI has a bigger successrate. You could try focusing on LFI and adding RFI as an extra?

True, I wanted to first create an RFI script first and then move on to LFI. Also thought about creating something for Cross Site Scripting but we'll see that in the future.

As for now, I'm working on optimizing this script and will move on the LFI after this is done.

notM9 - March 29, 2015, 3:12 pm

If you create any sort've LFI & RFI vuln checker. You should PM me. I would love it. I'll keep updated on your posts. But yes, add bulk checking from a text file or something.