

Forum:[Hack Forums](#)

Thread: [PHP | Webdav | scanner | Coded by me.](#)

radde94 - February 21, 2013, 10:11 pm

Hello,

So I was bored, I looked for some webdav exploiter, but I had no time to wait for friends to come online so they could give me it. So I started thinking, at first I did php code for search for random IPs and see if they was up using socket on ip:port, got a lot of IPs and working.

After a while I added a function that scanned for ip:port + the folder webdav. The script is very simple to use.

Version 1

You need 2 files to get this working.

.php file

.txt file

Code <?php

```
$rand1 = rand(0, 300);
```

```
$rand2 = rand(0, 300);
```

```
$rand3 = rand(0, 300);
```

```
$rand4 = rand(0, 300);
```

```
$ip = ($rand1 . "." . $rand2 . "." . $rand3 . "." . $rand4);
```

```
$port = "80";
```

```
$output = @fsockopen($ip, $port, $errno, $errstr, 1);
```

```
if (!$output) { echo 'Offline' . '<meta http-equiv="refresh" content="0">'; }
```

```
else {
```

```
    $fileUrl = "http://$ip/webdav/";
```

```
    $AgetHeaders = @get_headers($fileUrl);
```

```
    if (preg_match("[200]", $AgetHeaders[0])) {
```

```
        echo 'Success: http://' . $ip . '/webdav/';
```

```
        $invoegen = $ip . '/webdav/' . "\n";
```

```
        $fopen = fopen("logg.txt", "a");
```

```
        fwrite($fopen, $invoegen);
```

```
        fclose($fopen);
```

```
        echo '<meta http-equiv="refresh" content="0">';
```

```
    } else {
```

```
        echo 'Failed: http://' . $ip . '/webdav/';
```

```
        echo '<meta http-equiv="refresh" content="0">';
```

```
    }
```

```
}
```

```
@fclose($output);
```

```
echo '<br>';
```

```
$rand5 = rand(0, 100);
```

```
$rand6 = rand(0, 100);  
$rand7 = rand(0, 100);  
$rand8 = rand(0, 100);
```

```
$ip2 = ($rand5 . "." . $rand6 . "." . $rand7 . "." . $rand8);
```

```
$output = @fsockopen($ip2, $port, $errno, $errstr, 1);
```

```
if (!$output) { echo 'Offline' . '<meta http-equiv="refresh" content="0">'; }  
else {  
    $fileUrl = "http://$ip2/webdav/";  
    $aGetHeaders = @get_headers($fileUrl);  
    if (preg_match("|200|", $aGetHeaders[0])) {  
        echo 'Success: http://' . $ip2 . "/webdav/";  
        $invoegen = $ip2 . "/webdav/" . "\n";  
        $fopen = fopen("logg.txt", "a");  
        fwrite($fopen, $invoegen);  
        fclose($fopen);  
        echo '<meta http-equiv="refresh" content="0">';  
    } else {  
        echo 'Failed: http://' . $ip2 . "/webdav/";  
        echo '<meta http-equiv="refresh" content="0">';  
    }  
}  
@fclose($output);
```

?>This method is scanning 2 options, random IPs from 0,100 and random IPs from 0,300 to find more IPs and faster.

Version 2 - PHP

You need 2 files to get this working, and 1 database.

.php file

.txt file

Code <?php

```
if(isset($_GET['range']) && ($_GET['end'])) {  
    $random =  
    rand($_GET['range'], $_GET['end']) .'.  
    rand($_GET['range2'], $_GET['end2']) .'.  
    rand($_GET['range3'], $_GET['end3']) .'.  
    rand($_GET['range4'], $_GET['end4']);
```

```
mysql_connect("HOST", "USER", "PASSWORD") or die("Canno't connect to mysql server");  
mysql_select_db("DATABASE") or die("Canno't select database");
```

```
$result = mysql_query("SELECT * FROM up WHERE ip='$random'") or die("Canno't select from  
database");  
$row = mysql_fetch_array($result);  
if($random == $row['ip']) {  
    die('<meta http-equiv="refresh" content="0">');  
} // Die, Refresh.
```

```
$output = @fsockopen($random, "80", $errno, $errstr, $_GET['delay']);  
if (!$output) {
```

```

echo 'Failed: <a href="http://'.$random.':80' target="_BLANK">http://' . $random . ':80</a> No
webserver on this IP';
echo '<meta http-equiv="refresh" content="0">';
// Refresh
} else {
if($_GET['folder'] == "") {
mysql_query("INSERT INTO up (ip) VALUES('$random')");
echo 'Success: <a href="http://'.$random.':80' target="_BLANK">http://' . $random . ':80</a> No
webserver on this IP';
echo '<meta http-equiv="refresh" content="0">';
// Refresh
} // Else.
else {
$fileUrl = "http://$random/webdav/";
$AgetHeaders = @get_headers($fileUrl);
if (preg_match("|200|", $AgetHeaders[0])) {
$invoegen = "http://" . $random . "/webdav/" . "\n";
$fopen = fopen("webdav.txt", "a");
fwrite($fopen, $invoegen);
fclose($fopen);
echo 'Success: <a href="http://'.$random.'/'.$_GET['folder'].'" target="_BLANK">http://' . $random .
.'/'.$_GET['folder'].'"</a> Webserver+Folder on this IP<br>';
echo 'Adding to webdav.txt, <b>Done</b>';
echo '<meta http-equiv="refresh" content="0">';
// Refresh
} // End if (preg_match("|200|", $AgetHeaders[0])) {
} // End if(isset($_GET['folder'] == "")) {}
mysql_query("INSERT INTO up (ip) VALUES('$random')");
echo 'Success: <a href="http://'.$random.':80' target="_BLANK">http://' . $random . ':80</a> No
webserver on this IP';
echo '<meta http-equiv="refresh" content="0">';
// Refresh
} // End if (!$output) {
@fclose($output); // Close $output

} // Else end if(isset($_GET['range']) && ($_GET['end'])) {
else {
?>
<form method="get" action="">
<b>->Random->
<input type="text" name="range" value="0" size="1" />.
<input type="text" name="range2" value="0" size="1" />.
<input type="text" name="range3" value="0" size="1" />.
<input type="text" name="range4" value="0" size="1" />
<-This to This->
<input type="text" name="end" value="255" size="1" />.
<input type="text" name="end2" value="255" size="1" />.
<input type="text" name="end3" value="255" size="1" />.
<input type="text" name="end4" value="255" size="1" />
<-End random<-<br>
<font color="red">Leave blank if you don't now what you are doing.</font>
<br><br>
->Folder->

```

<input type="text" name="folder" value="webdav" /><-Folder to search, leave blank for no folder<-

->Delay->

<input type="text" name="delay" value="1" /><-In seconds of the ping<-

<input type="submit" value="->Search<-" />

</form>

<i><center>Si coded by | Michi on HackForums</center></i>

<?php

} // End if(isset(\$_GET['range']) && (\$_GET['end'])) {

?>For this you need a .txt file called webdav.txt

Version 2 - Database

Make a database named "anything", do the code below into the database.

Code CREATE TABLE `up` (

`id` INT(255) NOT NULL AUTO_INCREMENT PRIMARY KEY ,

`ip` VARCHAR(255) NOT NULL

) ENGINE = MYISAM ;

For the .txt just make a empty text document. If running linux don't forget to chmod the .txt file.

Enjoy ?

MrPaxio - February 23, 2013, 11:34 am

Thanks man :P I've been looking for soooo long.

Paradigm. - February 23, 2013, 11:41 am

Doesn't look to bad however the \$rand1,\$rand2,\$rand3 and \$rand4 variables should only go up to 255.

CarrotMilk - February 23, 2013, 11:42 am

Mannn, indent your code properly, that's an eye-sore ?

Pillows - February 23, 2013, 12:52 pm

You should make sure that the script doesn't scan into local IP's (10, 127, 192, etc), military IPs, and gateways (255). If you're doing this more than once isn't a for loop good for repetitive code?

radde94 - February 23, 2013, 7:45 pm

(Feb 23, 2013 01:52 PM)Pillows Wrote: [\[CITE\]](#) You should make sure that the script doesn't scan into local IP's (10, 127, 192, etc), military IPs, and gateways (255). If you're doing this more than once isn't a for loop good for repetitive code?

Well, you could recode it for Mysql : Database and use if IP -> Scanned already, skip.

If you need that just PM me and I'll help you out.

Regards,

| Michi

MrPaxio - February 23, 2013, 10:31 pm

Mine won't output to the logg.txt

Ideas?

csrx - February 23, 2013, 10:32 pm

Thanks for this man very useful i need to try this

radde94 - February 23, 2013, 11:38 pm

(Feb 23, 2013 11:31 PM)MrPaxio Wrote: [\[CITE\]](#) Mine won't output to the logg.txt
Ideas?
Running linux?
chmod it.

Also, it need to be in the same folder.

It only add to logg.txt if IP is online and folder webdav exist.

--

EDIT:

Working on a more advanced script, will be 2-3 versions soon enough :)

1 With .txt file
1 With database

You can choose between them, also adding a form so you can choose which folder you are going to scan on and what ip ranges :)

MrPaxio - February 23, 2013, 11:44 pm

(Feb 24, 2013 12:38 AM)| Michi Wrote: [\[CITE\]](#) Running linux?
chmod it.

Also, it need to be in the same folder.

It only add to logg.txt if IP is online and folder webdav exist.

--

EDIT:

Working on a more advanced script, will be 2-3 versions soon enough :)

1 With .txt file
1 With database

You can choose between them, also adding a form so you can choose which folder you are going to scan on and what ip ranges :)

Really nice :) and I'm on a webhost(Is that alright?) and I chmoded it already to 777. I visit the URL and it rapidly refreshes. but the logg.txt doesn't change even after a hour or so.

radde94 - February 24, 2013, 12:33 am

(Feb 24, 2013 12:44 AM)MrPaxio Wrote: [\[CITE\]](#) Really nice :) and I'm on a webhost(Is that alright?) and I chmoded it already to 777. I visit the URL and it rapidly refreshes. but the logg.txt doesn't change even after a hour or so.

It's looking for many ranges, it takes a while before it find a web server with webdav.

?

DAVEologist - February 24, 2013, 1:03 am

(Feb 24, 2013 01:33 AM)| Michi Wrote: [\[CITE\]](#) It's looking for many ranges, it takes a while before it find a web server with webdav.

?

I think your code might have some chances pinging the same IP for a brief period of time. Why don't you try storing what you already pinged using MySQL, or NoSQL so that there will be no repetition of pinging IPs.

radde94 - February 24, 2013, 1:09 am

I just release version 2,

Have fun guys, took like 5-15 minutes to code it for all of you!

It's working good ?

(Feb 24, 2013 02:03 AM)DAVEologist Wrote: [\[CITE\]](#) I think your code might have some chances pinging the same IP for a brief period of time. Why don't you try storing what you already pinged using MySQL, or NoSQL so that there will be no repetition of pinging IPs.

Yeah, I fixed it in version 2, It's released on first page, enjoy :)

Wait, don't use version 2, found an error.

Sorry :(

Fixed it,

Forgot to add the
\$result and \$row.

Should not look for same ip, that is online twice now.

Enjoy ?

ManDoR - February 24, 2013, 2:50 am

To be honest, even if you're saying you coded it in like 10min, I hope nobody will learn from it. God, you're still using `mysql_*` or `die()`, you're not indenting your code... Please at least put some effort in the releases you make.

DAVEologist - February 24, 2013, 3:05 am

(Feb 24, 2013 03:50 AM)ManDoR Wrote: [\[CITE\]](#) To be honest, even if you're saying you coded it in like 10min, I hope nobody will learn from it. God, you're still using `mysql_*` or `die()`, you're not indenting your code... Please at least put some effort in the releases you make.

I totally agree. Someone could even make this better. (*cough* *cough*)

This is a good idea, so please add some effort in your code.

radde94 - February 24, 2013, 5:07 am

(Feb 24, 2013 03:50 AM)ManDoR Wrote: [\[CITE\]](#) To be honest, even if you're saying you coded it in like 10min, I hope nobody will learn from it. God, you're still using `mysql_*` or `die()`, you're not indenting your code... Please at least put some effort in the releases you make.

So if you are going to bitch about it code it self?

And why should I indent my code when it's for private hosting and not public?

ManDoR - February 24, 2013, 6:23 am

(Feb 24, 2013 06:07 AM) Michi Wrote: [\[CITE\]](#) So if you are going to bitch about it code it self?

And why should I indent my code when it's for private hosting and not public?
Can't you take advice instead of acting like a jerk?

What you did is absolutly one of the easiest to do in webdevelopment. I won't make this because it's absolutly not challenging or anything. If you think I can't make it, then you're free to think that.

Indenting your code will make your release better, more readable, and will look more professional. On top on that, you're sharing your code with us, so yes indead, it's public and not private.

radde94 - February 24, 2013, 9:15 pm

(Feb 24, 2013 07:23 AM)ManDoR Wrote: [\[CITE\]](#) Can't you take advice instead of acting like a jerk?

What you did is absolutly one of the easiest to do in webdevelopment. I won't make this because it's absolutly not challenging or anything. If you think I can't make it, then you're free to think that.

Indenting your code will make your release better, more readable, and will look more professional. On top on that, you're sharing your code with us, so yes indead, it's public and not private.
Well as allways,

Haters gonna hate ?

Haters make you famous ?

The version 2 was way faster then the first one,

So recommending using version 2 for faster scans, also do not forget to add delay if your internet connection is bad.

Otherwise it's self DDoS :)

Regards,
Michi

ManDoR - February 24, 2013, 11:10 pm

PHP Code

```
<?php
if($random == $row['ip']) { }
// Do nothing.
else {
```

Woot.

radde94 - February 24, 2013, 11:37 pm

(Feb 25, 2013 12:10 AM)ManDoR Wrote: [\[CITE\]](#) PHP Code

```
<?php
if($random == $row['ip']) { }
// Do nothing.
else {
```

Woot.

If random(rand) ip numbers is equal to ip in mysql database
// Do nothing,

Else run the code.

This is to skip pinging same ip twice.

Funny do, calling yourself a PHP developer and that my code is to simple, gosh you don't even now if or else statements funny, you made my day sir.

Regards,
Michi ?

ManDoR - February 25, 2013, 7:27 am

(Feb 25, 2013 12:37 AM)| Michi Wrote: [\[CITE\]](#) If random(rand) ip numbers is equal to ip in mysql database
// Do nothing,

Else run the code.

This is to skip pinging same ip twice.

Funny do, calling yourself a PHP developer and that my code is to simple, gosh you don't even now if or else statements funny, you made my day sir.

Regards,
Michi ?
Using an empty if statement to make an else? Ah!

fobber - February 25, 2013, 8:02 am

(Feb 25, 2013 08:27 AM)ManDoR Wrote: [\[CITE\]](#) Using an empty if statement to make an else? Ah!
"if not" is so overrated! haha :D
Lorem ipsum

ManDoR - February 25, 2013, 8:08 am

(Feb 25, 2013 09:02 AM)fobber Wrote: [\[CITE\]](#) "if not" is so overrated! haha :D
Lorem ipsum
Yeah that must be it

Spoiler ([Click to View](#))

PHP Code

```
<?php
if("Michi" == "Know what he's doing") {
    // Do nothing
} else {
    die("swaggy = shitty"); // No other possible way, you must die.
}
```

CarrotMilk - February 25, 2013, 9:12 am

Fuck you OP. He was just giving you some advice; no need to be just a cunt about it.

radde94 - February 25, 2013, 9:51 am

Thanks for keeping my thread alive,

As always, Haters make you famous <3

Regards,
Michi.

CarrotMilk - February 25, 2013, 10:23 am

(Feb 25, 2013 10:51 AM)| Michi Wrote: [\[CITE\]](#) Thanks for keeping my thread alive,

As always, Haters make you famous <3

Regards,
Michi.

Yes, they make ME famous. They make YOU look like a tool.

ManDoR - February 25, 2013, 10:26 am

(Feb 25, 2013 11:23 AM)CarrotMilk Wrote: [\[CITE\]](#) Yes, they make ME famous. They make YOU look like a tool.

Then it's a pretty bad tool. Like one from the stone age.

radde94 - February 26, 2013, 10:53 pm

Old tools is way better then new tools :)

Updated the code, not using empty statement any more.

Open for more suggestions,

Regards,
Michi