

Forum:[Hack Forums](#)

Thread: [\[MyBB\] Fixing the Avatar IP Grabbing Exploit](#)

Stapleton - December 1, 2013, 7:30 pm

This is a very basic tutorial and I'm sure some of you may know how to this.

Now, MyBB has a Avatar Vuln, allowing to grab server IP's when uploading Avatar. Such a method can be a threat to your forum, if you want to keep your IP protected.

Now, there're 2 ways of doing this:

1. Using a Proxy
2. Removing the ability to use URL Avatar Linking

Using a Proxy:

1. First, open the path in FTP public_html/inc/ and open up the following file: functions.php
2. Search for line 5584. The code will look like:

PHP Code

```
<?php
curl_setopt($ch, CURLOPT_PROXY, "127.0.0.1");
curl_setopt($ch, CURLOPT_PROXYPORT, "8080");
curl_setopt($ch, CURLOPT_PROXYTYPE, CURLPROXY_SOCKS5);
```

3. We have to replace the 127.0.0.1 IP address with our proxy's IP address. If you're using a HTTP proxy, replace CURLPROXY_SOCKS5 with CURLPROXY_HTTP. By default, it is set to be a socket type proxy.

Removing URL Upload via Template:

1. Login to your Admin and go to AdminCP > Templates & Themes > Templates > Your Theme > User Control Panel > usercp_avatar and then replace it with this code:

PHP Code

```
<?php
<html>
<head>
<title>{$mybb->settings['bbname']} - {$lang->change_avatar}</title>
{$headerinclude}
</head>
<body id="forums">
{$header}
<table width="100%" border="0" align="center">
<tr>
{$usercpnav}
<td valign="top">
```

```

{$avatar_error}
<table border="0" cellspacing="{ $theme['borderwidth']}" cellpadding="{ $theme['tablespace']}" class=
"theadborder">
<tr>
<td class="thead" colspan="2">{$lang->change_avatar}</td>
</tr>
</table>
<table border="0" cellspacing="{ $theme['borderwidth']}" cellpadding="{ $theme['tablespace']}" class=
"tbodyborder">
<tr>
<td class="tbody1" colspan="2">
<table cellpadding="0" cellspacing="0" width="100%"><tr>
<td>{$lang->avatar_note}{$$avataarmsg}
</td>
{$currentavatar}
</tr></table>
</td>
</tr>
<tr>
<td class="tbody2" colspan="2">{$lang->local_galleries}</td>
</tr>
<tr>
<td class="tbody3">{$lang->gallery}</td>
<td class="tbody4">
<form method="post" action="usercp.php">
<input type="hidden" name="my_post_key" value="{ $mybb->post_code}" /><input type="hidden"
name="action" value="avatar" />
<select name="gallery">
{$galleries}
</select>
&nbsp;{$gobutton}
</form>
</td>
</tr>
<tr>
<td class="tbody5" colspan="2">{$lang->custom_avatar}</td>
</tr>
<tr>
<td class="tbody6" width="40%">{$lang->avatar_upload}</td>
<td class="tbody7" width="60%">
<form enctype="multipart/form-data" action="usercp.php" method="post">
<input type="hidden" name="my_post_key" value="{ $mybb->post_code}" />
<input type="file" name="avatarupload" size="25" class="fileupload" />
{$auto_resize}
</td>
</tr>
[ b]<!--[ /b] DeleteAvatarButton -->
</div>
</td>
</tr>
</table>
</form>
{$footer}

```

</body>
</html>

And, you're done. Now, you can enjoy being safe.

Regards,

Stapleton ?

PA?ADOX - December 2, 2013, 10:41 am

Nice tutorial, but there are many simple other ways to grab a server's IP address.

Stapleton - December 2, 2013, 7:09 pm

Thanks Johnny. I know there are several ways. This just fixes of them.

Crypto™ - December 2, 2013, 7:35 pm

The thing about this exploit is it grabs every IP of every person that sees the image ? Theoretically, it could also possibly be used to include a drive by exploit of some sort, if you could add on code after the image while still keeping it valid. [/speculation]

Thanks for the fix Stapleton!

There's also a needlessly complicated and slow solution :) You could grab all images, render them serverside, and push the rendered image to the clients, effectively serving as a reverse image proxy :)