

Forum:[Hack Forums](#)

Thread: [Malformed Webshells](#)

jolo7 - June 1, 2022, 8:56 am

Whenever I upload a php shell on to a test vm, then access it from the "attacker" vm, it appears as malformed, showing part of the code in fields etc. I've tried with various webshells (all quite old). The attacker machine is a linux vm, while the test target is windows 10 (with defender disabled).

Does anyone know why that might be?

Aside from that, can someone point to an up-to-date resource for webshells?

linkinpork - June 1, 2022, 5:21 pm

(Jun 1, 2022 08:56 AM)jolo7 Wrote: [\[CITE\]](#) Whenever I upload a php shell on to a test vm, then access it from the "attacker" vm, it appears as malformed, showing part of the code in fields etc.

You sure your target has PHP installed?

Here's a quick guide:

Get XAMPP <https://www.apachefriends.org/index.html> when you need a WAMP stack in a pinch.

Get composer <https://getcomposer.org/download/>

Download npm <https://nodejs.org/en/download/>

Laravel installation guide <https://laravel.com/docs/4.2/installation>

How-to:

Assuming you installed XAMPP in C:/xampp and your Laravel project in C:/laravel, go to C:/xampp/apache/conf/extra/httpd-vhosts.conf and replace all contents with something like this:

Code <VirtualHost *:80>

ServerAdmin random-email-address-or-whatever@hackforums.net

DocumentRoot "C:\laravel\public"

ServerName localhost

<Directory "C:\laravel\public">

Options Indexes FollowSymLinks MultiViews

AllowOverride all

Order Deny,Allow

Allow from all

Require all granted

</Directory>

</VirtualHost>

Restart your Apache server using the XAMPP control panel when you're ready

Place the webshell in C:/laravel/public/webshell.php , and you should be able to access it via <http://localhost/webshell.php>

If [Doc](#) has extra time on his hands he might be able to answer some questions. [Lynx](#) knows a thing or two about npm as well (plus the guy keeps a node website) so he might lend help if he's not busy.

Doc - June 2, 2022, 12:44 am

(Jun 1, 2022 08:56 AM)jolo7 Wrote: [\[CITE\]](#) Whenever I upload a php shell on to a test vm, then access it from the "attacker" vm, it appears as malformed, showing part of the code in fields etc. I've tried with various webshells (all quite old). The attacker machine is a linux vm, while the test target is windows 10 (with defender disabled).

Does anyone know why that might be?

Aside from that, can someone point to an up-to-date resource for webshells?
I need some more information from you, if you could be more specific.

When you say it appears as malformed, showing part of the code in fields etc: Can you be more specific? How are you accessing the shell exactly? What do you mean it's showing part of the code in fields? What fields are you referring to?

Keep in mind, the more specific and detailed you are in your responses, the better I'll be able to try and help.

Lynx - June 2, 2022, 12:54 am

(Jun 1, 2022 05:21 PM)linkinpork Wrote: [\[CITE\]](#) You sure your target has PHP installed?

Here's a quick guide:

Get XAMPP <https://www.apachefriends.org/index.html> when you need a WAMP stack in a pinch.

Get composer <https://getcomposer.org/download/>

Download npm <https://nodejs.org/en/download/>

Laravel installation guide <https://laravel.com/docs/4.2/installation>

How-to:

Assuming you installed XAMPP in C:/xampp and your Laravel project in C:/laravel, go to C:/xampp/apache/conf/extra/httpd-vhosts.conf and replace all contents with something like this:

Code <VirtualHost *:80>

```
ServerAdmin random-email-address-or-whatever@hackforums.net
DocumentRoot "C:\laravel\public"
ServerName localhost
```

<Directory "C:\laravel\public">

```
Options Indexes FollowSymLinks MultiViews
AllowOverride all
Order Deny,Allow
Allow from all
```

```
    Require all granted
</Directory>
</VirtualHost>
```

Restart your Apache server using the XAMPP control panel when you're ready

Place the webshell in C:/laravel/public/webshell.php , and you should be able to access it via <http://localhost/webshell.php>

If [Doc](#) has extra time on his hands he might be able to answer some questions. [Lynx](#) knows a thing or two about npm as well (plus the guy keeps a node website) so he might lend help if he's not busy. Wouldn't say I'm good with npm to be honest. Nor do I get why npm is relevant in OP's case.

I'm guessing your "victim" isn't running the php correctly. It's either running the wrong version or it depends on certain plugins to be enabled.

I don't get why you would try to install a webshell on a windows machine in the first place though. You would be dependent on the victim having an open port, running php and have it be running consistently.