

Forum:[Hack Forums](#)

Thread: [Bypassing PHP code filter.](#)

?M???????? - October 12, 2012, 3:50 am

Im trying to execute a shell on a vBulletin site via a vBa CMPS html module as the account I am using does not have permissions to the plugin system. My problem being that any php tags are phrased and commented out like this:

Code [b]<!--[/b]?php code here ?-->

Just wondering if there is an easy way to bypass this filter or any other way I could execute the php.

Thanks in advance,
-Matt

Psyman - October 12, 2012, 3:53 am

Try canceling it out by re-ordering this "--".

Will probably cancel out the comment but not sure if it'll work out for you.

?M???????? - October 12, 2012, 4:29 am

(Oct 12, 2012 03:53 AM)Psyman Wrote: [\[CITE\]](#) Try canceling it out by re-ordering this "--".

Will probably cancel out the comment but not sure if it'll work out for you.

Not 100% sure what you mean, the "--" is inserted automatically by the phrasing script.

For example:

Code Input:

<?php code here ?>

Output:

<--?php code here ?-->

Th3PonyWizard - October 12, 2012, 4:38 am

Code %3C%3Fphp

//code goes here

%3F%3EAlso try ASP tags.

Code <%

%>

Psyman - October 12, 2012, 4:39 am

(Oct 12, 2012 04:29 AM)?M???????? Wrote: [\[CITE\]](#) Not 100% sure what you mean, the "--" is inserted automatically by the phrasing script.

For example:

Code Input:

<?php code here ?>

Output:

<--?php code here ?-->

You're clearly clueless with basic HTML, -- cancels out HTML comments.

?M??????? - October 12, 2012, 5:07 am

(Oct 12, 2012 04:38 AM)Th3PonyWizard Wrote: [\[CITE\]](#) Code %3C%3Fphp
//code goes here
%3F%3EAlso try ASP tags.
Code <%
%>
Both cause the code to be shown as plaintext.

(Oct 12, 2012 04:39 AM)Psyman Wrote: [\[CITE\]](#) You're clearly clueless with basic HTML, -- cancels out HTML comments.

I do not know much at all about HTML, if I add -- to close the comment made I am still going to be unable to run the script, right?

Psyman - October 12, 2012, 3:34 pm

(Oct 12, 2012 05:07 AM)?M??????? Wrote: [\[CITE\]](#) Both cause the code to be shown as plaintext.

I do not know much at all about HTML, if I add -- to close the comment made I am still going to be unable to run the script, right?

As long as it's not within the PHP tags, hopefully.

Phizo - October 12, 2012, 5:10 pm

(Oct 12, 2012 04:38 AM)Th3PonyWizard Wrote: [\[CITE\]](#) Code %3C%3Fphp
//code goes here
%3F%3EAlso try ASP tags.
Code <%
%>

I don't see how URL encoding is going to help since it won't ever get decoded.

As far as I can see there's no way around it, it blocks all variations of PHP opening tags since all variations require at least <?.

Not even a short echo tag would work (<?=) since, assuming they're matching just <?, it will just be filtered and replaced with HTML comment tags.

If it were simple to bypass then it most likely would've been discussed somewhere already.

?asp3r - October 12, 2012, 8:17 pm

(Oct 12, 2012 05:10 PM)Phizo Wrote: [\[CITE\]](#) I don't see how URL encoding is going to help since it won't ever get decoded.

As far as I can see there's no way around it, it blocks all variations of PHP opening tags since all variations require at least <?.

Not even a short echo tag would work (<?=) since, assuming they're matching just <?, it will just be filtered and replaced with HTML comment tags.

If it were simple to bypass then it most likely would've been discussed somewhere already.

OffTopic: have not seen you on in a bit :D

OnTopic: Phizo knows what he's doing. Trust this guy. If he says it wont help, it wont help.

dofawa - *October 13, 2012, 12:25 am*

Thank you alot I Mp as soon as I bit!