

Forum:[Hack Forums](#)

Thread: [Wha tutorial should I follow if I'd like to get download PHP files from a website?](#)

xCaptainNutz - August 5, 2017, 4:17 pm

Wha tutorial should I follow if I'd like to get download PHP files from a website?

Charger - August 5, 2017, 4:19 pm

You can't unless you find an RFI vuln or login to the file manager.

xCaptainNutz - August 5, 2017, 4:26 pm

(Aug 5, 2017 04:19 PM)Charger Wrote: [\[CITE\]](#) You can't unless you find an RFI vuln or login to the file manager.

Any tut?

webdev77 - August 5, 2017, 4:28 pm

(Aug 5, 2017 04:26 PM)xCaptainNutz Wrote: [\[CITE\]](#) Any tut?

That's not something you can just follow a tutorial and guarantee results for. Take 2 minutes and google search it. You will find several thousand pages with helpful information on the topics mentioned.

xCaptainNutz - August 5, 2017, 4:31 pm

(Aug 5, 2017 04:28 PM)webdev77 Wrote: [\[CITE\]](#) That's not something you can just follow a tutorial and guarantee results for. Take 2 minutes and google search it. You will find several thousand pages with helpful information on the topics mentioned.

I have googled a bit and understood it's an injection of a shell/php script into the url where the url expects a page.

I assume this isn't possible when for instance the page expects an ID
for example:

website.com/search?uid=837 right?

The ID is then forwarded to an SQL command.

webdev77 - August 5, 2017, 4:39 pm

(Aug 5, 2017 04:31 PM)xCaptainNutz Wrote: [\[CITE\]](#) I have googled a bit and understood it's an injection of a shell/php script into the url where the url expects a page.

I assume this isn't possible when for instance the page expects an ID
for example:

website.com/search?uid=837 right?

The ID is then forwarded to an SQL command.

Get/post requests are generally filtered by the website backend to prevent malicious injections. Your goal is to find a mistake in the filtering process that allows a malicious request to get through and perform the intended command.

xCaptainNutz - August 5, 2017, 5:20 pm

(Aug 5, 2017 04:39 PM)webdev77 Wrote: [\[CITE\]](#) Get/post requests are generally filtered by the website backend to prevent malicious injections. Your goal is to find a mistake in the filtering process that allows a malicious request to get through and perform the intended command.

What method would you prefer, hacking into the file manager or this?