

Forum:[Hack Forums](#)

Thread: [PHP unserialized parameter help](#)

itazy - October 5, 2019, 5:18 pm

Hi everyone, it's my first time using HF although I have been snooping around here a couple of times.

To keep this post on topic - I've stumbled across a website that takes an unserialized parameter when sending a GET or POST request to /getDataWinners/<date parameter> returning simple JSON of the winners.

The unserialized part of course comes when you enter a ' as the parameter or the part of the parameter - calling /getDataWinners/test'), PHP throws a fatal error:

"Uncaught Error: Call to member function fetch_object() on boolean in ... Model->getAllDataWinners('test')..."

I am new to hacking in general but I have experience in object oriented programming, however I've never used or learnt PHP. The most information I have been able to gather is basic Googling.

As far as my gut tells me, if I am able to somehow "form" the parameter to not throw the error and insert my own code I would be able to achieve RCE, but since I don't have an idea of how PHP code is usually typed nor the syntax, my attempts of combining parentheses, brackets, semicolons and comments were in vain.

So, two questions are:

If I successfully form the parameter and insert my code will it work/is it worth the bother or am I just delusional and wasting my time?

If I'm correct in my assumptions can anybody give me some pointers on how to do it?

I respect your time and I'm not expecting anyone to hack sites for me, I just think this is a great learning opportunity for me.

Thanks in advance.

compalabee - October 6, 2019, 5:34 am

(Oct 5, 2019 05:18 PM)itazy Wrote: [\[CITE\]](#) "Uncaught Error: Call to member function fetch_object() on boolean in ... Model->getAllDataWinners('test')..."

What's in the triple dots? Is it really just that, or did you snip some things out? Cos the way I see it (from this point at least), you should put a bool var there, and it's reading "test" as a string and not a bool or int.

While you're at it, have you tried smacking it with SQLi before anything else? If you have bad IDS you might be able to use an automation like sqlmap, delayed by a few hundred milliseconds for evasion. If you manage that, inject a backdoor into the database, bind to it, bam, you get RCE.

itazy - October 7, 2019, 4:05 am

(Oct 6, 2019 05:34 AM)compalabee Wrote: [\[CITE\]](#) What's in the triple dots? Is it really just that, or did you snip some things out?

Yea I took out the server paths, the full error is:

Code Fatal error: Uncaught Error: Call to a member function fetch_object() on boolean in /home/alex/web/site/public_html/application/model/model.php:139 Stack trace: #0 /home/alex/web/site/public_html/application/controller/home.php(156): Model->getAllDataWinners('test') #1 /home/alex/web/site/public_html/application/core/application.php(39): Home->getDataWinners('test') #2 /home/alex/web/site/public_html/public/index.php(30): Application->__construct() #3 {main} thrown in /home/alex/web/site/public_html/application/model/model.php on line 139

(Oct 6, 2019 05:34 AM)compalabee Wrote: [\[CITE\]](#) Cos the way I see it (from this point at least), you should put a bool var there, and it's reading "test" as a string and not a bool or int.

It's actually taking a date string as the parameter in the yyyy-m-d format, but entering a string that isn't a date doesn't return an error, just an empty json array.

(Oct 6, 2019 05:34 AM)compalabee Wrote: [\[CITE\]](#) While you're at it, have you tried smacking it with SQLi before anything else? If you have bad IDS you might be able to use an automation like sqlmap, delayed by a few hundred milliseconds for evasion. If you manage that, inject a backdoor into the database, bind to it, bam, you get RCE.

Tried doing the SQLi manually but it doesn't seem possible since the ' escapes the function string parameter before getting to the actual query. As for sqlmap, can't get it to work with the URL since the parameter isn't in the format ?var=value but rather /value. Any ideas?

compalabee - October 7, 2019, 9:14 am

(Oct 7, 2019 04:05 AM)itazy Wrote: [\[CITE\]](#) Code Fatal error: Uncaught Error: Call to a member function fetch_object() on boolean in /home/alex/web/site/public_html/application/model/model.php:139 Stack trace: #0 /home/alex/web/site/public_html/application/controller/home.php(156): Model->getAllDataWinners('test') #1 /home/alex/web/site/public_html/application/core/application.php(39): Home->getDataWinners('test') #2 /home/alex/web/site/public_html/public/index.php(30): Application->__construct() #3 {main} thrown in /home/alex/web/site/public_html/application/model/model.php on line 139

Congrats, you just saw an injection vector ? Try to write it down on paper first, then visualize it.

How about you make the getAllDataWinners var properly put together, then start a new line of code? From there, comment everything out?

Here's an example:

Code getAllDataWinners('[b]INPUTCODE[/b])
can be exploited as:

getAllDataWinners('DATA+FORGED CLOSE BRACKET;INSERT COMMAND -->comment
everything past that

Also, didn't you notice the file inclusion there?

Code /home/alex/web/site/public_html/application/controller/home.php

You now have some idea of the directory of the website! If you're not too familiar with Linux, best you refresh yourself on basic bash commands ?

(Oct 7, 2019 04:05 AM)itazy Wrote: [\[CITE\]](#) Tried doing the SQLi manually but it doesn't seem possible since the ' escapes the function string parameter before getting to the actual query. As for sqlmap, can't get it to work with the URL since the parameter isn't in the format ?var=value but rather /value. Any ideas?

Try to catch your HTTP request with something like Zaproxy, then input that file into the -r argument of sqlmap. Place a \$ in the area that you designate to have the SQLi. Hopefully that would work.

itazy - October 7, 2019, 12:25 pm

(Oct 7, 2019 09:14 AM)compalabee Wrote: [\[CITE\]](#) Congrats, you just saw an injection vector ? Try to write it down on paper first, then visualize it.

How about you make the getAllDataWinners var properly put together, then start a new line of code? From there, comment everything out?

Here's an example:

Code getAllDataWinners('[b]INPUTCODE[/b])
can be exploited as:

getAllDataWinners('DATA+FORGED CLOSE BRACKET;INSERT COMMAND -->comment
everything past that

First of thanks for all the tips, it really helps out ?

That's one of the things I tried, sadly it looks like it filters out the comment characters like #, /, * since they don't appear in the error message, for example, sending a GET or POST request to:

Code /getDataWinners/a');echo('b');#/*returns:

Code Fatal error: Uncaught Error: Call to a member function fetch_object() on boolean in
/home/alex/web/site/public_html/application/model/model.php:139 Stack trace: #0

/home/alex/web/site/public_html/application/controller/home.php(156):

Model->getAllDataWinners('a');echo('b');') #1

/home/alex/web/site/public_html/application/core/application.php(39):

Home->getDataWinners('a');echo('b');') #2 /home/alex/web/site/public_html/public/index.php(30):

Application->__construct() #3 {main} thrown in

/home/alex/web/site/public_html/application/model/model.php on line 139

(Oct 7, 2019 09:14 AM)compalabee Wrote: [\[CITE\]](#) Also, didn't you notice the file inclusion there?

Code /home/alex/web/site/public_html/application/controller/home.php

You now have some idea of the directory of the website! If you're not too familiar with Linux, best you refresh yourself on basic bash commands ?

Even though I used Windows my whole life I know Linux enough, at least I hope ? Knowing the directory will come in handy, but I can't do much with it till I get to RCE, unless I am mistaken?

(Oct 7, 2019 09:14 AM)compalabee Wrote: [\[CITE\]](#) Try to catch your HTTP request with something like Zaproxy, then input that file into the -r argument of sqlmap. Place a \$ in the area that you designate to have the SQLi. Hopefully that would work.

Caught the request with burp and passed it to sqlmap, but no luck, sqlmap doesn't think it's injectable. Although it's no wonder it didn't work since comments don't work and the only way of making PHP not crash is somehow magically finishing that line of code.

I want to thank you for the effort you put in to explain things to me and try and help me, I would really appreciate if you have anymore ideas.