

Forum:[Hack Forums](#)

Thread: [\[PHP Audit Challenge\] Wordpress Plugin - HDW Player](#)

JoinSeventh - February 1, 2014, 3:12 pm

Sup HF.

Back in the days I posted a 0day in a Wordpress plugin:

<http://joinse7en.blogspot.se/2012/08/wordpress-hd-webplayer-11-sql-injection.html>

<https://hackforums.net/showthread.php?tid=2820225>

They've released a new project under the new name HDWPlayer:

<http://hdwebplayer.com/> -> <http://www.hdwplayer.com/>

After all this time, they've still not learned how to sanitize user input.

This vulnerability is pretty useless since you need to be logged in and have access to the admin panel.

So I thought I'd make a little challenge from this instead of publishing it.

Note: There are several SQL Injection vulnerabilities existing in the plugin.

Vulnerable plugin:

HDW Player Plugin for Wordpress Websites Version 2.4.2

Code <http://wordpress.org/plugins/hdw-player-video-player-video-gallery/>

Challenge:

Find one (or all) of the SQL Injection vulnerabilities in the plugin.

0x01 - Find the vulnerable code and where it's located. (I want the code, which file it's in and line number)

0x02 - Do a successful SQL Injection and receive the "version()". (I want the URL + Full Injection Query)

PoC:

It's kind of hard to show a PoC without ruining the challenge but here's a simple one:

Code Receiving user_login:user_pass from wp_users

[!] Do not disclose anything in this thread.

[!] PM me all the answers.

This is not published yet, please let it stay that way for the sake of the challenge.

Good luck.

Spoiler ([Click to View](#))

If you don't know where to begin, here are 2 tutorials I've written on the subject:

Solvers:

[huji](#)

BeggFoMercy - February 1, 2014, 3:37 pm

Uhh I'm too lazy to install a wordpress on my server -.- .

DJ Khale?d - February 1, 2014, 6:20 pm

Post-auth sqli, best cero dia evar. I might make a challenge with a similar concept except with a 0day that's actually practical.

JoinSeventh - February 1, 2014, 6:25 pm

(Feb 1, 2014 07:20 PM)DJ Khale?d Wrote: [\[CITE\]](#) Post-auth sqli, best cero dia evar. I might make a challenge with a similar concept except with a 0day that's actually practical.

Like I said in the OP, I made this because it wasn't useful to me and thought it would be fun to make a little challenge instead of publishing a useless vulnerability.

It wasn't mean to be an awsum 0day release, it was meant to be PHP Code Auditing Challenge.

How is this not practical? It's not useful but still very much practical.

DJ Khale?d - February 1, 2014, 6:39 pm

(Feb 1, 2014 07:25 PM)JoinSeventh Wrote: [\[CITE\]](#) Like I said in the OP, I made this because it wasn't useful to me and thought it would be fun to make a little challenge instead of publishing a useless vulnerability.

It wasn't mean to be an awsum 0day release, it was meant to be PHP Code Auditing Challenge.

No I read that and completely understood your intent. I'm just saying that it would be better to use an example that would actually be practical as far as vulnerability severity and usefulness. Post-auth sqli (SELECT) is pretty much disregarded all together in terms of practicality.

(Feb 1, 2014 07:25 PM)JoinSeventh Wrote: [\[CITE\]](#) How is this not practical? It's not useful but still very much practical.

JoinSeventh - February 1, 2014, 6:52 pm

(Feb 1, 2014 07:39 PM)DJ Khale?d Wrote: [\[CITE\]](#) No I read that and completely understood your intent. I'm just saying that it would be better to use an example that would actually be practical as far as vulnerability severity and usefulness. Post-auth sqli (SELECT) is pretty much disregarded all together in terms of practicality.

This is exploitable which also makes it practical. This is not just theory.

Just because the vulnerability is only exploitable if you're logged in as an admin doesn't mean the means to find and exploit it is any different.

Although I agree that it would be better to use a more useful vulnerability I didn't feel like publishing one.

I'm looking forward to any similar challenge with more real-world applicable content from you.

huji - February 2, 2014, 6:36 am

i found it.the sql vuln.nice challenge

