

Forum:[Hack Forums](#)

Thread: [Vulnerable Forum 3k members](#)

Ooze - March 25, 2015, 3:45 pm

So this isnt a huge forumn but I found a page within the forumn that was vulnerable. I got all the tables and none of them contain columns with username an password or anything like that. I know this site has users and members but I dont see anything. I will leave a link to the site so it will probably be defaced before I can do anything. But thats ok as long as I learn what the problem is.

<http://www.interplay.com/games/support.php?id=263>

That is the vulnerble link. Have fun but make sure to tell me what I did wrong.

Benign - March 25, 2015, 3:57 pm

Did you dump a list of all of the available databases?

What about running a search with sqlmap for column names in case you missed something?

Ooze - March 25, 2015, 5:48 pm

(Mar 25, 2015 03:57 PM)Benign Wrote: [\[CITE\]](#) Did you dump a list of all of the available databases?

What about running a search with sqlmap for column names in case you missed something?To my knowledge the only other database was information schema which is usless and I dont use SQL map but I could try

sluggerz - March 25, 2015, 10:33 pm

Lol dude you're just missing it because that information is definitely in there.

Benign - March 25, 2015, 11:59 pm

(Mar 25, 2015 10:33 PM)sluggerz Wrote: [\[CITE\]](#) Lol dude you're just missing it because that information is definitely in there.

Are you saying this because you've seen it, or just to say something? It could be that the forum authentication data is in a separate database technology that isn't accessible from the injection point we have, or even hosted on another system.

I havnt looked so I'm not saying this is the case, I'm just saying it could be that there is no auth data here.

-zERaIT - March 26, 2015, 1:11 am

Just a basic injection guys.

PHP Code

<?php

http://www.interplay.com/games/support.php?id=-263 union select 1,group_concat(table_name),3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19+from+information_schema.tables+where+table_schema=0x696e7446572706c6179--

PHP Code

<?php

banners,banners_banner_id_seq,careers,careers_career_id_seq,downloads,franchises,

franchises_franchise_id_seq,news,news_news_id_seq,screenshots,
screenshots_screenshot_id_seq,titles,titles_title_id_seq

Have to go to work, so didn't go any further.

Disparity - March 26, 2015, 1:40 am

(Mar 26, 2015 01:11 AM)-zERaIT Wrote: [\[CITE\]](#) PHP Code

```
<?php
```

banners,banners_banner_id_seq,careers,careers_career_id_seq,downloads,franchises,
franchises_franchise_id_seq,news,news_news_id_seq,screenshots,
screenshots_screenshot_id_seq,titles,titles_title_id_seq

Exactly what I got. However, I do have the time to go further, and from what I can tell this vulnerability holds little to no promise. I didn't find any usertables or anything sensitive at all.

Edit: Why the fuck is HF blocking anything under the PHP tag I post? Even when I'm just quoting someone?

Ooze - March 26, 2015, 7:11 am

(Mar 26, 2015 01:40 AM)Disparity Wrote: [\[CITE\]](#) Exactly what I got. However, I do have the time to go further, and from what I can tell this vulnerability holds little to no promise. I didn't find any usertables or anything sensitive at all.

Edit: Why the fuck is HF blocking anything under the PHP tag I post? Even when I'm just quoting someone?Thanks for checking and making sure I'm not crazy, I have no idea why there is no sensitive data, I have never dealt with a site that ended up like that. Thanks again for checking.

sluggerz - March 26, 2015, 10:57 am

I wonder if they are running two DBS. I would try a different parameter.

Ffour1939 - March 30, 2015, 6:14 pm

(Mar 26, 2015 10:57 AM)sluggerz Wrote: [\[CITE\]](#) I wonder if they are running two DBS. I would try a different parameter.

But wouldn't you see the other DB? For the hell of it I ran the link in havij(I know the basics of sqlmap so far but havij was faster while I did other things) and I click get DB at least 5 times and only info_schem and interplay came

Disparity - March 30, 2015, 9:53 pm

(Mar 26, 2015 07:11 AM)C0deZilla Wrote: [\[CITE\]](#) Thanks for checking and making sure I'm not crazy, I have no idea why there is no sensitive data, I have never dealt with a site that ended up like that. Thanks again for checking.

The user tables are simply kept in a separate area. This vulnerability seems to be an a media related area of the site. User tables and other sensitive data simply wouldn't have a place in being there.

sluggerz - March 31, 2015, 11:12 am

(Mar 30, 2015 09:53 PM)Disparity Wrote: [\[CITE\]](#) The user tables are simply kept in a separate area. This vulnerability seems to be an a media related area of the site. User tables and other sensitive data simply wouldn't have a place in being there.

Exactly what I was saying. This site probably run two database and you need to find the correct vuln to get access to the other half.

Casper.zxc - April 2, 2015, 5:43 am

There's no admin or id in that vulnerable site :3