File Upload Exploitation

pentestlab.blog/category/web-application/page/6

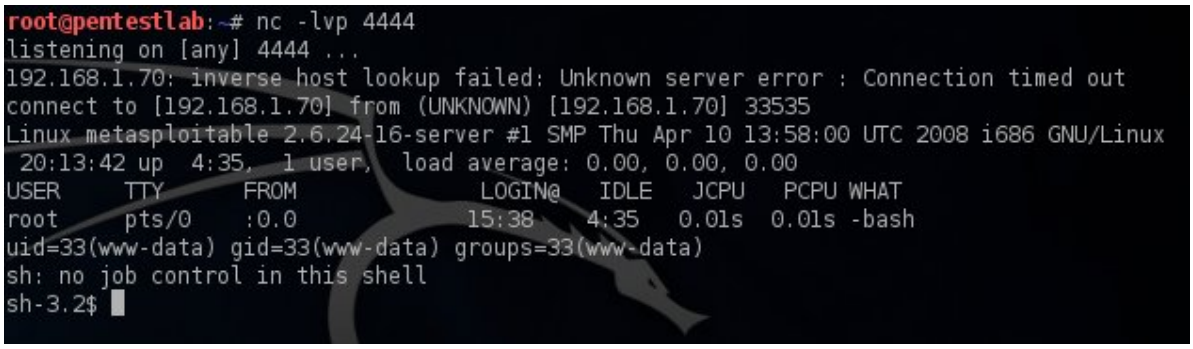
December 23, 2012

File upload vulnerabilities consists a major threat for web applications.A penetration tester can use a file upload form in order to upload different types of files that will allow him to obtain information about the web server or even a shell.Of course shell is always a goal but a good penetration tester must not stop there.Further activities can be performed after the shell.The focus of these activities must be on the database.In this article we will see how we can obtain a shell from the exploitation of file upload on a Linux web server and how we can dump the database that is running on the system.

Backtrack includes a variety of web shells for different technologies like PHP,ASP etc.In our example we will use the damn vulnerable web application which is written in PHP in order to attack the web server through the file upload.The web shell that we will use in our case it will be the php-reverse-shell.

uploading the web shell

Now we have to set our machine to listen on the same port as our web shell.We can do this with netcat and the command nc -lvp 4444.The next step is to go back to the web application and to try to access the URL that the PHP reverse shell exists.We will notice that it will return a shell to our console:



Obtaining a shell

So we have compromise the remote web server and we can execute further commands from our shell-like a simple ls in order to discover directories.

Now it is time to dump the database.We will have to go to the directory with the name uploads because this directory has write permissions and it is visible to the outside world which means that we can access it and we can create a file.Then we can use the following command in order to dump the database to a file.

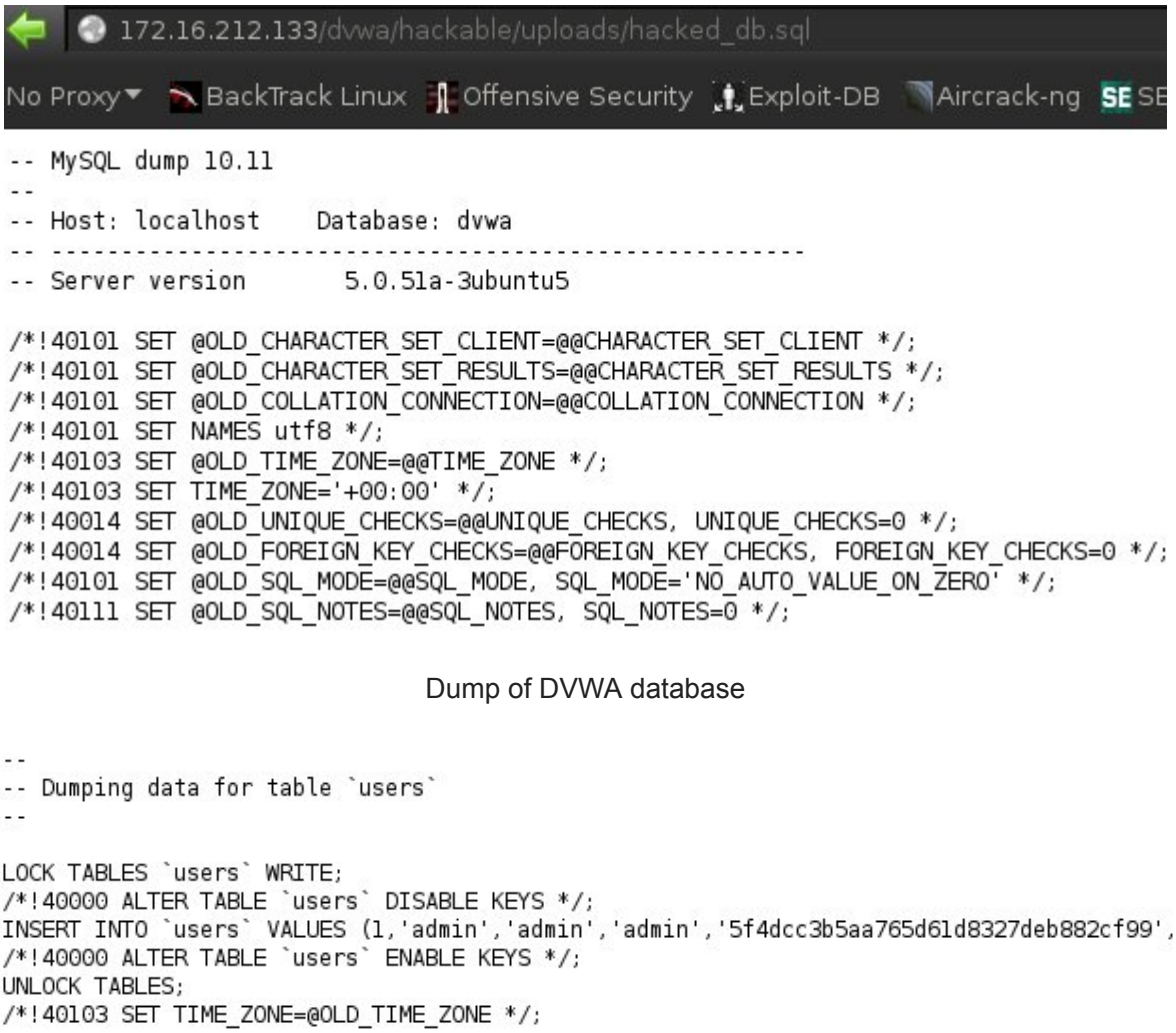
Listing Directories

mysqldump -u root -p dvwa > hacked_db.sql

We already know that the user root exists because it is already logged into the system.Also it is very common the name of the application or of the company to be the database name so we will use the dvwa.The > sign will create a file inside the uploads directory with the name hacked_db.sql.

As we can see from the image above we had to provide a password.In this scenario we just pressed enter without submitting anything.In a real world penetration test it would be much more difficult however it is always a good practice to try some of the common passwords.The next two images are showing the dump of the dvwa database.

Dumping the database to a file



Dump of DVWA database

Dump of DVWA database 2

From the last image we can see that we even obtain the password hash of the admin which it can be cracked by using a tool like john the ripper.This is also important as we may want to have the admin privileges and into the application.

Conclusion

In this article we saw how we can obtain a shell by exploiting a file upload form of an application and how we can dump the database.Of course in a real world scenario it is more likely restrictions to be in place but it good to know the methodology and the technique that we must follow once we have managed to upload our web shell.