Software Vulnerabilities:
Exploitation and Mitigation
–
Lab 8

Prof. Jacques Klein & Pedro Jesús Ruiz Jiménez
(inspired from Prof. Alexandre Bartel's course)

8 Injection Attack (42 P.)

In this lab you will exploit an SQL injection vulnerability to dump the database containing user names and passwords.

8.1 Shell Injection

The following program uses the `system` function:

```c
// example from OWASP
// https://www.owasp.org/index.php/Command_injection

#include <stdio.h>
#include <unistd.h>

int main(int argc, char **argv) {
 char cat[] = "cat ";
 char *command;
 size_t commandLength;

 commandLength = strlen(cat) + strlen(argv[1]) + 1;
 command = (char *) malloc(commandLength);
 strncpy(command, cat, commandLength);
 strncat(command, argv[1], (commandLength - strlen(cat)) );

 system(command);
 return (0);
}
```

Question 8.1 Show how to change the C code to prevent any shell command injection. 5 P.

8.2 Setup Labs Environment

8.2.1 Download resources

Download the Debian virtual image here (user:user, password:user).

8.3 Launch Emulated Environment

On your host machine, go to the directory where `Debian.qcow2` is located. Then, create the virtual machine by using the following command:

```
$ qemu-system-x86_64 -hda Debian.qcow2 -m 1024
```

use 4096

You can change the resolution to make the image run faster!

8.4 SQL Injection

The vulnerable website is running at the following URL:

`http://localhost/lab09/`.

Parameters are passed using the GET method:

Ex: `http://localhost/lab09/login.php?u=toto&p=tata`

8.4.1 Vulnerable Code

The target server use the following code to check the validity of users:

```
<? php
[...]
 $username = $_REQUEST["u"];
 $password = $_REQUEST["p"];

 $result = $conn->query("SELECT * FROM users WHERE username = \"$username\" AND password =
 ↪  \"$password\"");
 if ($result->num_rows > 0) {
   # ok
   [...]
 } else {
   # not ok
   [...]
 }
 [...]
?>
```

Question 8.2 Where is the injection vulnerability in the code? 2 P.

Question 8.3 What input should the attacker give for `username` and `password` to bypass the authorisation check of the password? 3 P.

8.4.2 User Name Brute Force

Question 8.4 You quickly want to know a valid user name. Using the above input structure to bypass the authorization check, try user names from the list of most used user names for ssh brute for attacks below. What is one valid user name? 3 P.

```
root
test
oracle
admin
info
user
postgres
mysql
backup
guest
web
tomcat
michael
r00t
upload
alex
sales
linux
bin
ftp
support
temp
nagios
user1
www
test1
nobody
```

8.4.3 Blind

Question 8.5 What is the difference on the html page for a successful authentication and for a failed authentication? 3 P.

Question 8.6 Using this difference, you can know when your SQL query succeeds or not. Build a script/program with the language of your choice to perform a blind SQL attack to dump the 100 rows of the `users` database (100 pairs username/password). Usernames and passwords consist of ascii characters. If you use the GET method to pass parameters, do not forget to convert special characters (ex: space is %20). 15 P.

8.4.4 Patch

Question 8.7 Show how you can patch the code to prevent SQL injection. code from 8.4.1 5 P.

Question 8.8 Is/Are there any other security problem(s) with this website (PHP code / SQL request / information stored in the database / etc.)? If yes, how would you fix it/them? 5 P.

8.5 Bonus

Question 8.9 There is a reference to a movie when the authentication does not succeed. Which movie? 1 P.

Note on plagiarism

Plagiarism is the misrepresentation of the work of another as your own. It is a serious infraction. Instances of plagiarism or any other cheating will at the very least result in failure of this course. To avoid plagiarism, always cite the source from which you obtained the text.