Writeup -Kinderriegel

Areeb Hussain
Mtr. 3133658

Questions:

1. Gain access to the "Kinderriegel" backend. There are two flags: The first is hidden in the database and the second is displayed on the main page.
2. Compromise the system. The flag can be found in the root directory of the server. Write down your actions.
3. Can you discover a way to bypass the authentication and exploit the vulnerability even if the password has been changed?
4. Show your l33t sk1llz: Can you extract the flag file on the root system without accessing the admin backend? Write down your actions.

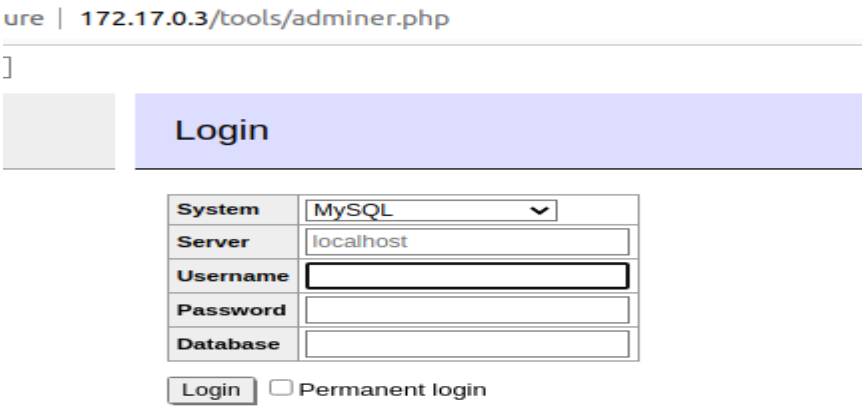
Start and compile the container like the previous tasks
$ sudo docker compose up -d in the container's directory and get the ip address
Ip addr: **172.17.0.3**

Put it into the web, we literally get a picture of animated kinderriegel chocolate nothing more
Lets do a nikto with the command **nikto -h 173.17.0.3** and see what directories are inside

```
---------------------------------------------------------------------------
+ Server: Apache/2.4.29 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/e8z01xdh%28VS.80
+ Cookie PHPSESSID created without the httponly flag
+ OSVDB-3092: /admin/: This might be interesting...
+ Server leaks inodes via ETags, header found with file /tools/, fields: 0x7c 0x574284e7ecd00
+ OSVDB-3092: /tools/: This might be interesting...
+ OSVDB-3093: /admin/index.php: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3268: /images/: Directory indexing found.
+ OSVDB-3268: /images/?pattern=/etc/*&sort=name: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 6544 items checked: 0 error(s) and 10 item(s) reported on remote host
+ End Time:           2022-12-01 06:23:32 (GMT1) (22 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

1. **Gain access to the "Kinderriegel" backend. There are two flags: The first is hidden in the database and the second is displayed on the main page.**

Lets look at ***tools****, it opens a webpage with dbfrontend which leads to a adminer.php. This page looks exactly like a the adminer.php from the sql injection slides. Interesting lets try to manually brute force with commonly used/*default credentials



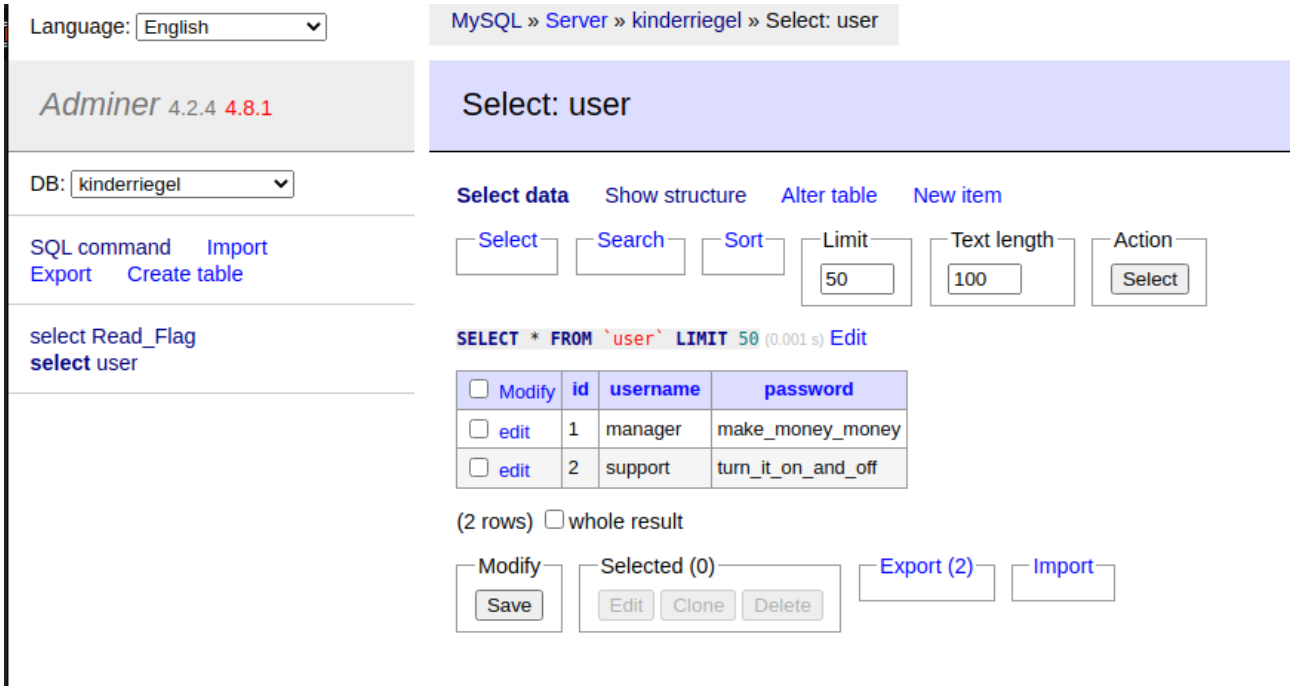
As I remember from sql injection, the adminer.php is used to look into the actual databse. After a couple of tries then going back to the slides I tried
username: root
password: root
database: kinderriegel

And I was in
got the flag from the table Read_flag

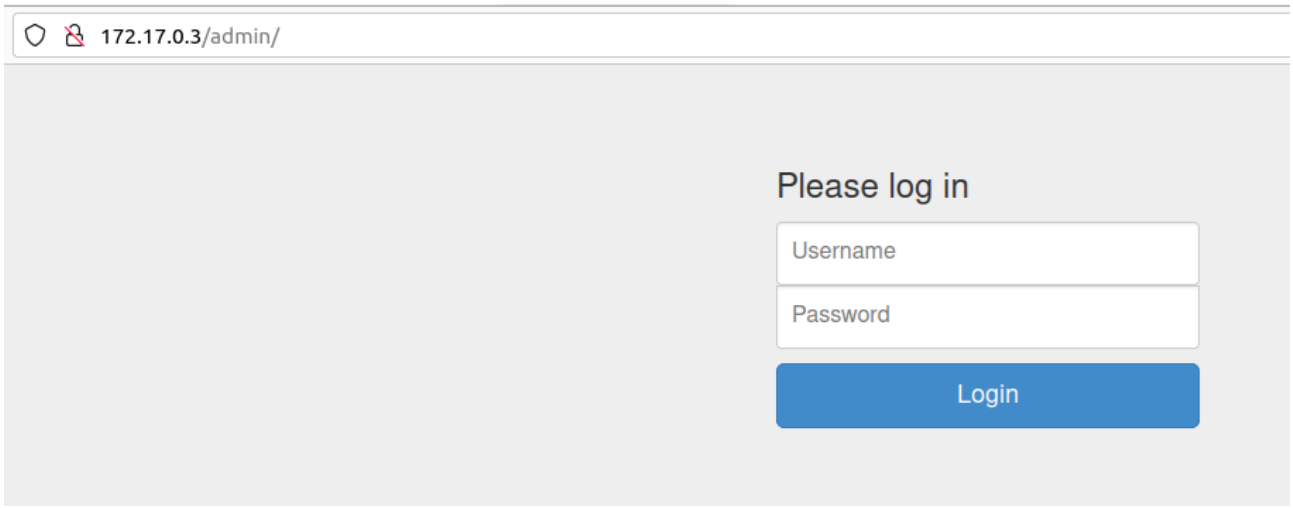
Frontend Flag

n0_0ne_th0ught_ab0ut_4dm1n3r

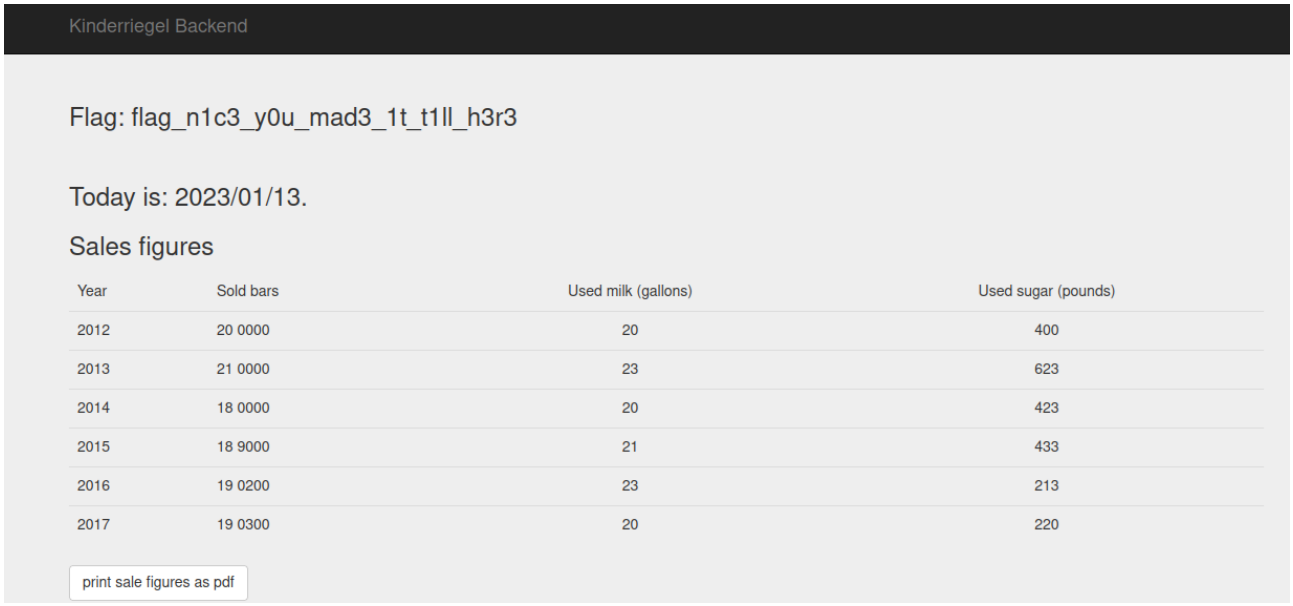
Looking around there was another table user with two users.



Now lets look into the other directory **/admin.** It's a simple admin login page which maybe could be exploited using sql injection



As suspected the users table from the database list the admin login credentials.
Enter the credentials
username: manager
password: make_money_money

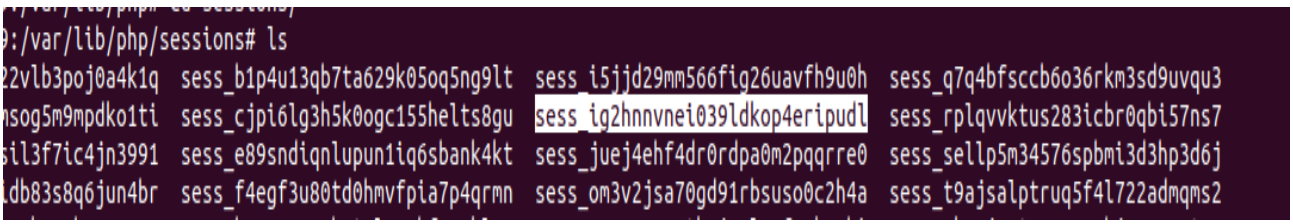


Backend Flag

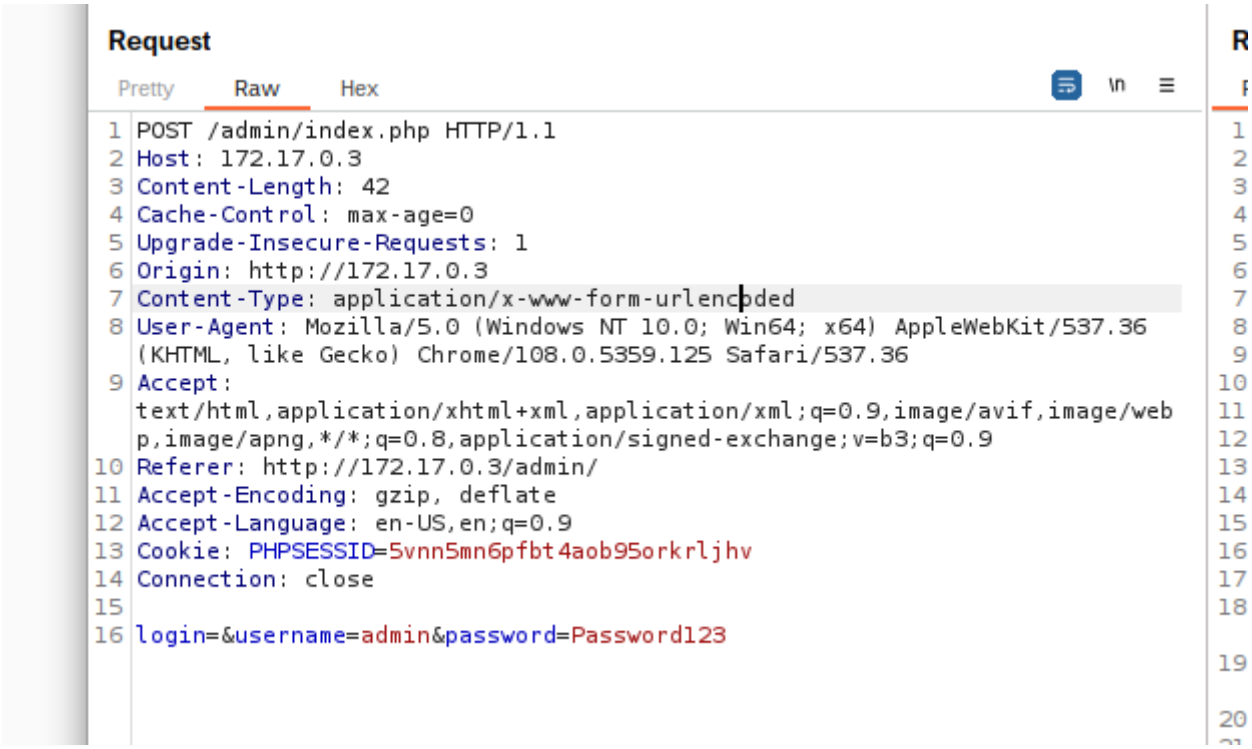
flag_n1c3_y0u_mad3_1t_t1ll_h3r3

3. **Can you discover a way to bypass the authentication and exploit the vulnerability even if the password has been changed?**

As I researched online a way to bypass authentication if the password has been changes is by using the session id. But provided that sessid is used in url??

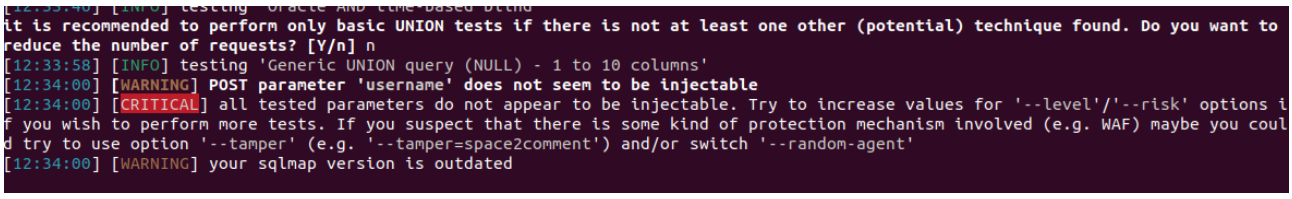


But just to see if sql injection exploitation can be used on the /admin login page. I will use sqlmap. Simply open Burpsuite and open browser. Enter the /admin page and enter any credentials. Check the burpsuite http history and copy the post request and save it as a txt file



We can provide the data being passed in the POST request body to scan by the SQLMap tool with the following command

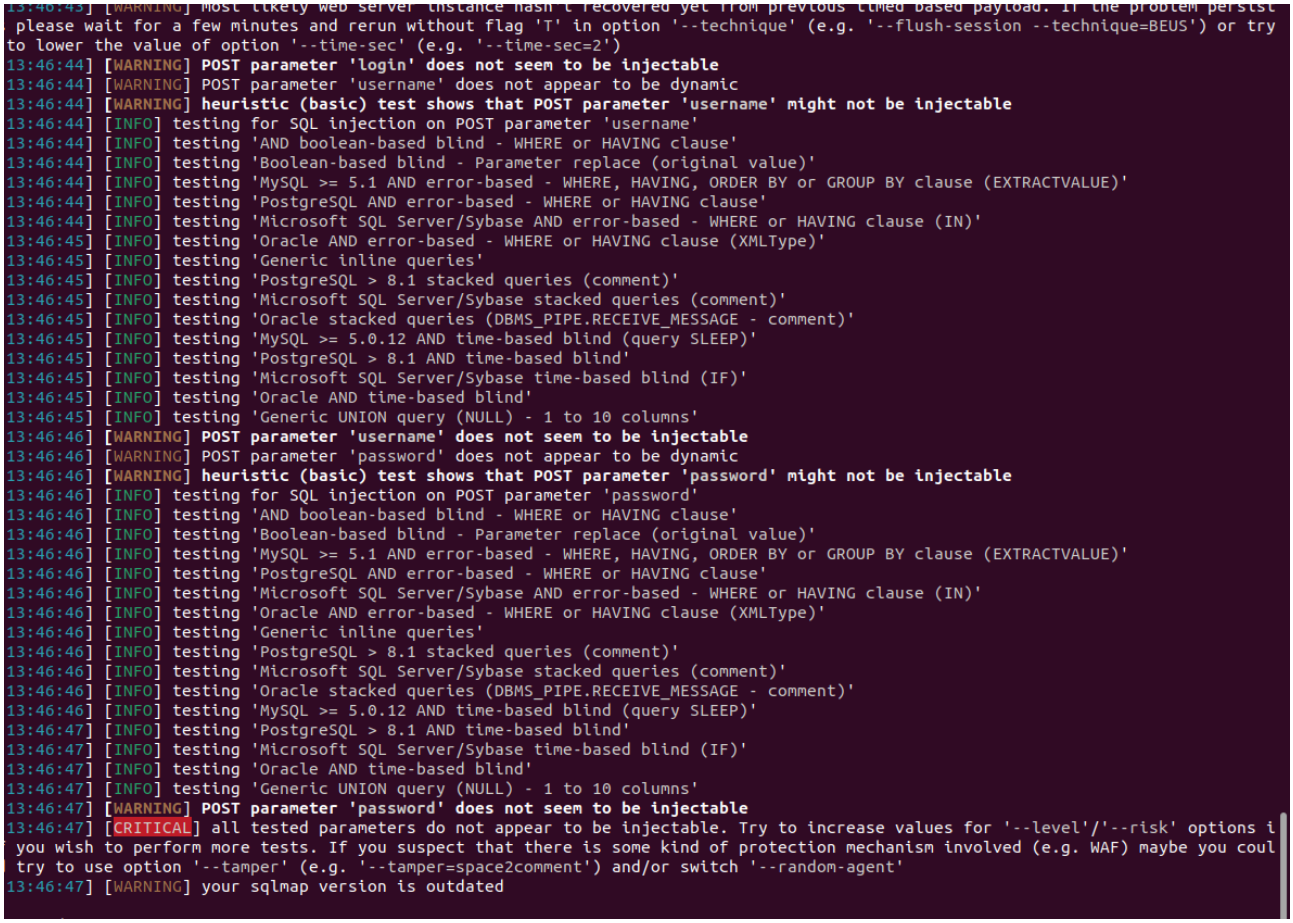
$ sqlmap -r <path to the request > -p username



It seems to be not injectable.

lets try to enumerate the database with the command

$sqlmap -r /*home*/areeb/kinderriegel.txt –dbs



Same result

Unfortunately I was not able to get root access