Writeup: Kinderriegel Container

- 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.

First, I run “dirb http://172.17.0.2/” on the webserver. I found an admin page and a tools page which links to a database login page.

1) Login into database with standard credentials: root/root

2) Found Database credentials:

manager/make_money_money
support/turn_it_on_and_off

In the "kinderriegel" database the flag can be found:

Flag: n0_0n3_th0ught_ab0ut_4dm1n3r

In the admin panel the flag can be found:

Flag: flag_n1c3_y0u_mad3_1t_t1ll_h3r3

- Compromise the system. The flag can be found in the root directory of the server. Write down your actions.

In the “admin” page, a pdf file can be created. This is done by a call to the “admin.php”:

➔ /admin/admin.php?action=print&filename=sales-figures-2022-11-24.pdf

If we analyze the pdf we find that the pdf is created by a command line tool and the filename parameter gets inserted in the command line. The filename parameter can be injected to execute Linux commands on the webserver host system.

I run the following commands as filename parameter:

;ls%20/; → List all files in / directory -> found the flag file

;nl%20/the_flag_4_kinderriegel.txt; → Displays the content of the flag file

Flag: flag_k1nd3r13g3l_c4nt_r3pl4c3_a_gl4s_0f_m1lk

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

I use the vulnerability of task 2 and analyze the “admin.php” file. I found that if the HTTP Host header is set to "localhost" the php-session isn't get checked.

If we change the "Host" in the HTTP request in burpsuite to "localhost" we can exploit the vulnerability without being logged in.

- Show your l33t sk1llz: Can you extract the flag file on the root system without accessing the admin backend? Write down your actions.

The flag can be extracted using the database login. In SQL files can be loaded and displayed.