## Gitlab

### Exploitation Proof of concept

By entering the address of our Gitlab machine we immediately redirected to the sign in page.

A screenshot of a computer

Description automatically generated

By known concepts we first check the robots.txt file of the web, and we see that it shows all allowed and disallowed directories. However, the more interesting part is that there is a list of words in the end of robots.txt, which reminds username or password list kind of.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

After some directory fuzzing, we find out that Administrator page is open under the root directory, however we cannot modify anything. So, by creating a wordlist of passwords from rorbots.txt we made a brute force attack to Administrator user and root, since we were not sure which one is the username.

A screenshot of a computer

Description automatically generated

By that we get that the username and password of Administrator is root:Shadow123123. As soon as we get to the admin page we see an error of Critical Security release of Gitlab Version, so our here Google comes in for help.

A screenshot of a computer

Description automatically generated

After making some search we find out that there is an exploit of this version.

<https://github.com/Occamsec/CVE-2023-2825>

A screenshot of a computer

Description automatically generated

By making some modifications in the script we can run it to our Gitlab user.

A screenshot of a computer

Description automatically generated

When we run the script we see that exploit creates 11 groups, and makes it as a public repo, after it automatically, makes path traversal and gets to /etc/passwd file.

A screenshot of a computer

Description automatically generated

Exploring the passwd file we see that there is user “plumber” whose hash is openly visible in passwd file.



We check the type of hash and get to yescrypt hash type. Most of the ‘find the hash’ programs did not find out, so I used chatgpt for assistance.

A screenshot of a computer

Description automatically generated

So, the stage is the hero’s one and only John the Ripper.

A screenshot of a computer

Description automatically generated

Hello Plumber user, I am in.

A screenshot of a computer

Description automatically generated

Flag also found. Interesting thing there is an alpine service zip there. Let’s explore how we can proceed.

When we write an ID command we see that our user is the member of the group named “lxd”.

A screenshot of a computer

Description automatically generated

After making some search I find out that there is a 2023 CVE related to lxd which is CVE-2023-5536.

<https://nvd.nist.gov/vuln/detail/CVE-2023-5536>

Further I searched for privilage escalation methods using LXD, and find out useful documentation: <https://medium.com/@mstrbgn/privilege-escalation-using-lxd-lxc-group-assignment-to-a-user-a-security-misconfiguration-a4892f611d6f>

A screenshot of a computer

Description automatically generated

ICSD{0e705c84c1a17ed632e91f9304676f07}