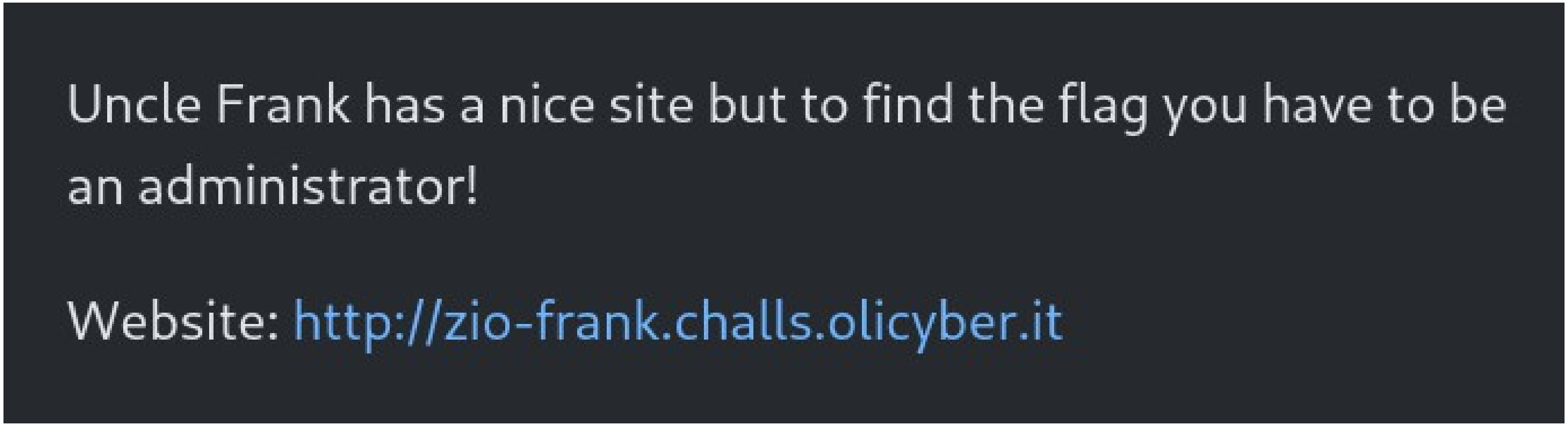
OLIcyber – Zio (Uncle) Frank

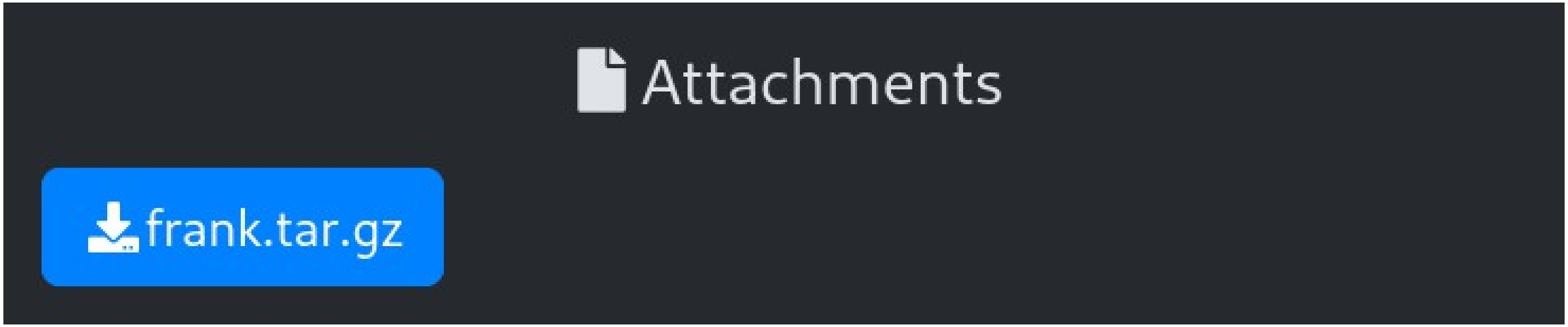


Uncle Frank has a nice site but to find the flag you have to be an administrator!

Website: http://zio-frank.challs.olicyber.it

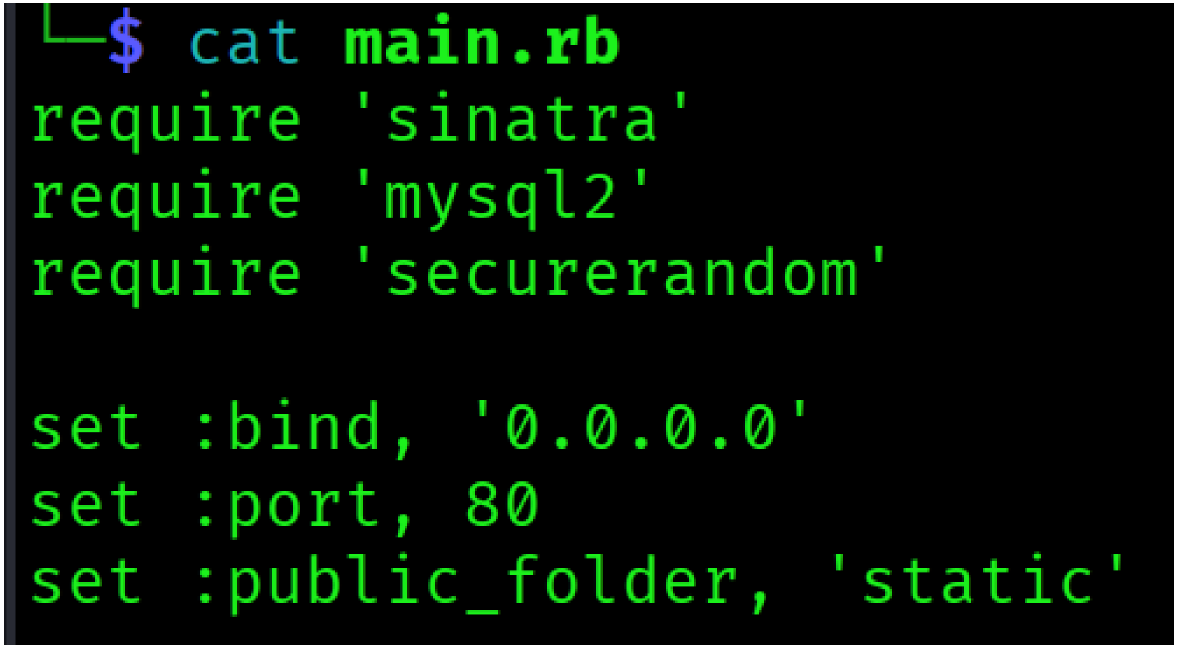
This challenge instructs us to become the administrator and get the flag

Zio (Uncle) Frank – Source Code Analysis



In certain CTF challenges there are source code files to download and analyze. We must always read challenge descriptions carefully

Zio (Uncle) Frank – Source Code Analysis

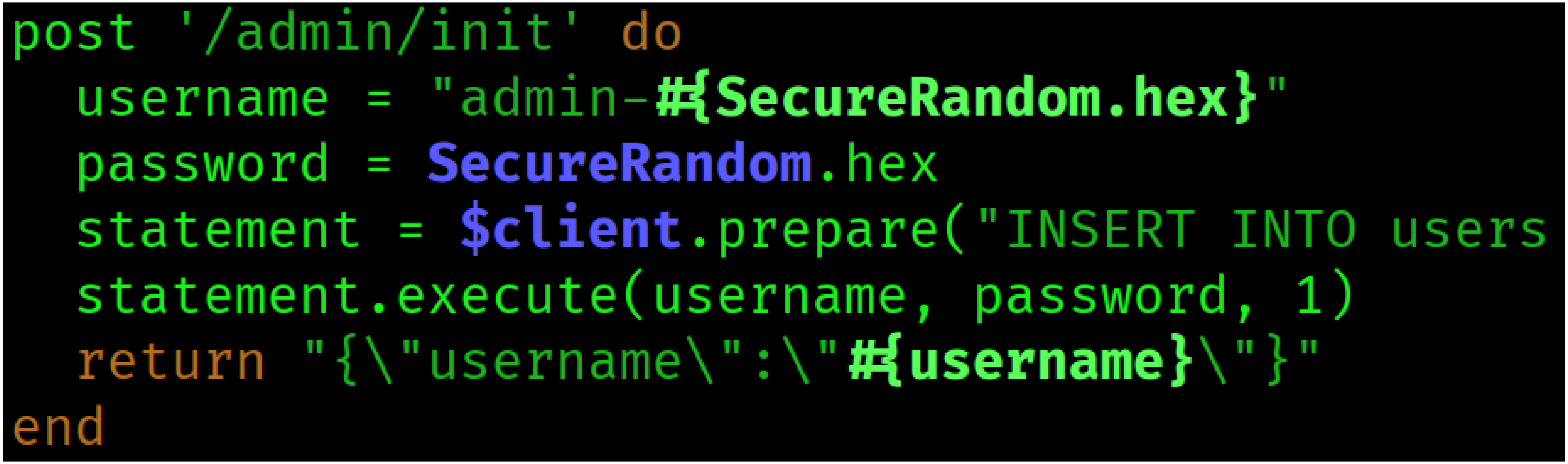


```
└─$ cat main.rb
require 'sinatra'
require 'mysql2'
require 'securerandom'

set :bind, '0.0.0.0'
set :port, 80
set :public_folder, 'static'
```

In the source code files, we find out that the web app is running on Ruby code

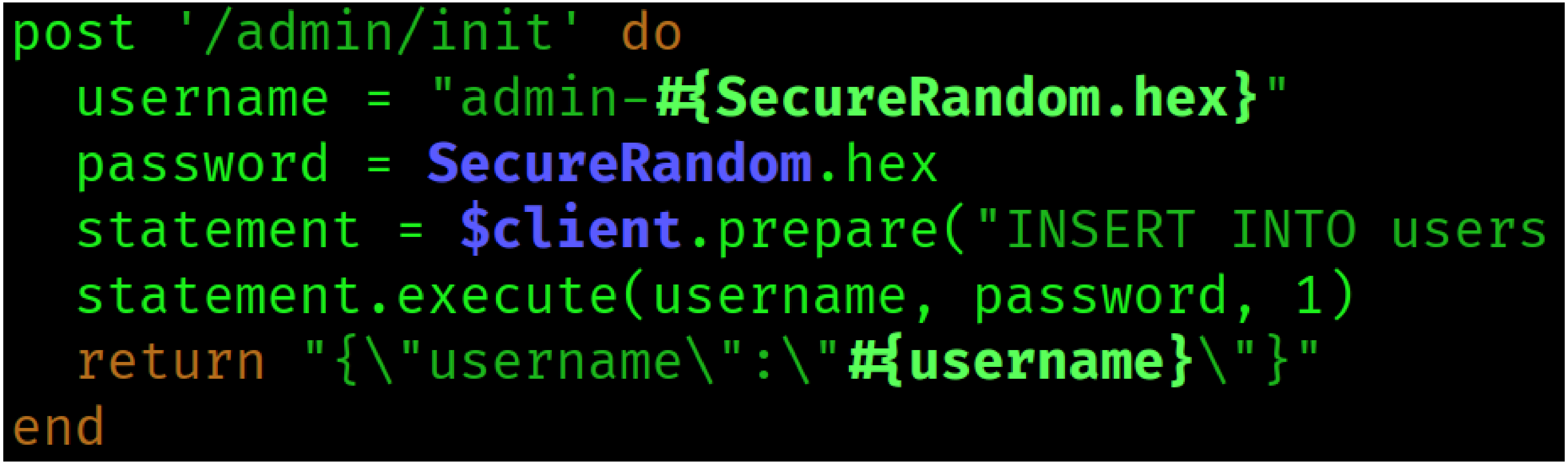
Zio (Uncle) Frank – Broken Access Control: Admin User Creation



```
post '/admin/init' do
  username = "admin-#{SecureRandom.hex}"
  password = SecureRandom.hex
  statement = $client.prepare("INSERT INTO users
  statement.execute(username, password, 1)
  return "{\"username\":\"#{username}\"}"
end
```

This app includes an unauthenticated function that creates an admin-level user

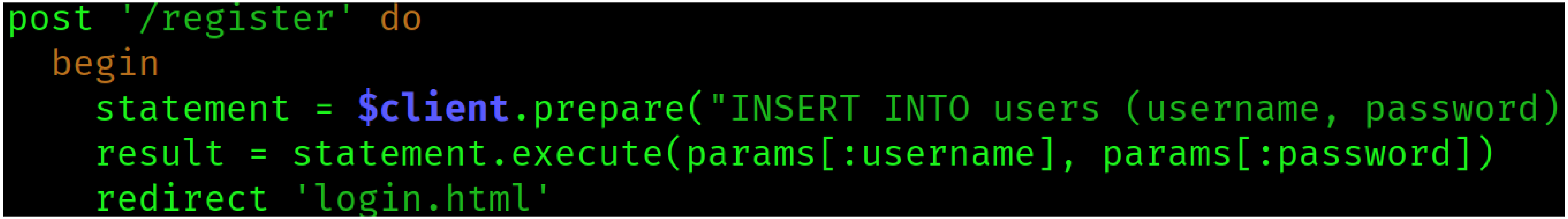
Zio (Uncle) Frank – Broken Access Control: Admin User Creation



```
post '/admin/init' do
  username = "admin-#{SecureRandom.hex}"
  password = SecureRandom.hex
  statement = $client.prepare("INSERT INTO users
  statement.execute(username, password, 1)
  return "{\"username\":\"#{username}\"}"
end
```

This by itself is not vulnerable, since the response doesn't include the password for the account

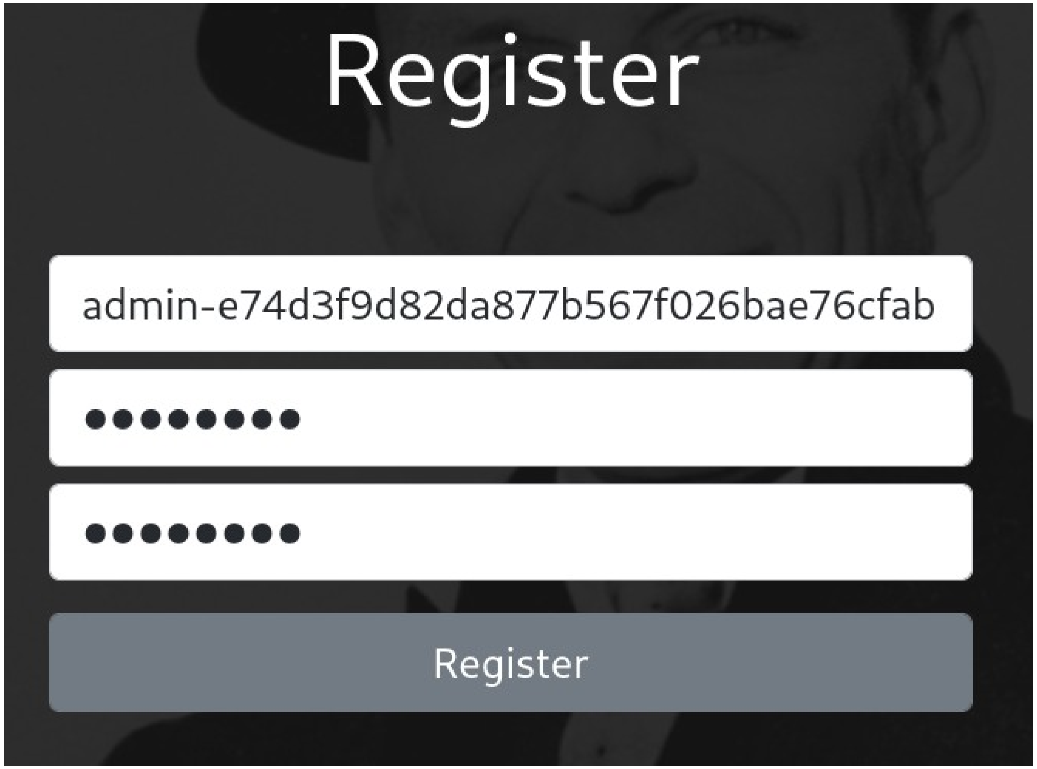
Zio (Uncle) Frank – Broken Access Control: Admin User Creation



```
post '/register' do
  begin
    statement = $client.prepare("INSERT INTO users (username, password)
    result = statement.execute(params[:username], params[:password])
    redirect 'login.html'
```

But the next function, which is used to register new users, doesn't check whether a username already exists in the system or not before creation

Zio (Uncle) Frank – Broken Access Control: Admin User Creation



Register

admin-e74d3f9d82da877b567f026bae76cfab

●●●●●●●●●

●●●●●●●●●

Which means we can overwrite the password for a created admin user account