Security Coursework

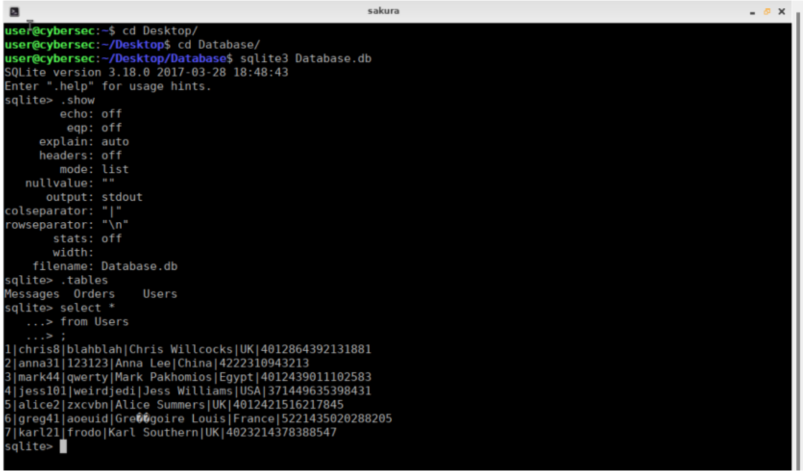
Vulnerability	Exploit / Problem	Mitigation
1) There is a user account called 'user' which has a weak password which is 'password'.	Someone could guess the password 'password' and gain access to the server.	The vulnerability can be secured by selecting an appropriately secured password, for example random mixed case letters, numbers, and symbols.
2) The database back-up contents can be opened through the terminal.	Private server customer information, including usernames and logins, full name, country and credit card numbers, can all be seen or changed by opening the database back-up through the command line. This can be seen in Fig 1.	Ensure the database is secured through requiring a username and password to access it. Also ensure that access is audited.
3) Excessive and incorrect permission/privileges are given to the users.	Through the 'user' account, we can view, read and write on several user files and the contents found within their respective folders, such as [redacted] secret diary. These actions can be easily performed through the command line. This is also an issue on other user accounts.	Increase the permissions for 'user' access to read, write and execute on files within [redacted] [redacted] folders. The current permissions can be seen in Fig 2. Ensure the permissions for all other users are also correct. A privilege model should be used, such as the Bell-Lapadula model.
4) Ports are left open, including port 8888 as seen in Fig 3, which can be easily accessed through the command line.	Root access can be gained through the open network connections, to read, write and execute on all files, due to the use of an old protocol (such as telnet). This can be done once accessing the open port 8888, allowing commands to be executed through a remote shell.	Update the device protocol to SSH, which uses public key authentication, ensuring more secure communication and sharing of data between ports. The website server is not connected to port 8888, so consider closing it if it serves no function.
5) The website server paths are unverified.	A path traversal attack can be run on the website resulting in leaked system information. This can allow access to user data, through the server, such as passwords. This example can be seen in Fig 4.	A modern configured server should be integrated, where access is denied past a certain boundary. For example, regular expressions can be whitelisted, hence only allowing valid inputs.
6) All the .c /Desktop files are openly accessible and unencrypted. The Bitcoins.c file is particularly insecure.	The .c files on the Desktop can be opened and viewed, causing potential vulnerabilities. For example, we can overflow the buffer for Bitcoins.c, causing the CEOs bitcoin key to be displayed, as seen in Fig 5.	The Bitcoins.c file can be complied with a stack protector, to stop stack smashing, preventing the flag from accepting a string if the buffer overflows. We could also check that our buffer bound is defined to ensure nothing goes over the 64 characters in length. All the .c files should also be encrypted.
7) The 'Login' page of the website accepts SQL statements.	An SQL injection attack can be run through inputting an SQL statement into one of the 'Login' fields, causing private details of all the users to be	A prepared statement can be created, to prevent the use of the statement seen in Fig 6, and similar varieties. This will prevent

	displayed in a table. This can be seen in Fig 6, along with the relevant SQL statement.	code and data from being mixed up.
8) The list of user countries on the 'Stats' page, includes repeated countries, as seen in Fig 10.	An inference attack can be performed with the user countries and 'list of users'. The number of users is equal to the number of user countries, resulting in the inference that the users and countries match-up with one another in the order displayed, which happens to be true. This is against the anonymity policy listed on the webpage.	Remove all country duplicates from the user countries table on the website by creating a 'countries' table in the database.
9) The server has a weak audit trail.	Currently, security breaches cannot be tracked. If someone were to internally access the database, then we cannot tell which data was breached. Additionally, if someone tried to login many times, without success, then this knowledge would be useful to help avoid a future breach.	Any changes or access to the system server or database should be monitored. Specifically, ensure all database changes through SQL commands, changes to permissions and login attempts are audited.
10) The SQLite version used to store the database back-up is out of date.	Patch 3.18.0 is used, as seen in Fig 7, which is a few years out of date. Recent patches will ensure the best level of security and that bugs are fixed. However, without updating there is a risk of a data breach with sensitive data being accessed.	Update to the latest version of SQLite, which is version 3.38.
11) Passwords and sensitive information are not securely saved in the database.	If the database contents are accessed, as seen in Fig 6, sensitive information is instantly known, such as passwords and card numbers. A simple dictionary attack can be run, to crack the passwords and gain access to sensitive information, as they are unencrypted.	All database contents should be encrypted. Upon choosing passwords, they should contain at least a certain number of characters, numbers and special characters. To ensure a secure database login system, passwords require hashing, and a salt should be added before.
12) User information is available on the website.	The usernames stored in the database all contain the first name of the user, followed by a number. This makes the usernames easy to guess. This would aid a dictionary attack, which aims to access sensitive information.	Usernames should be adjusted to be unique and not depend on user information. They should contain at least a certain number of random characters, numbers and special characters.
13) The kernel version is out of date.	The current kernel version used is 3.16.55, as seen in Fig 8, which is out of date, leaving open many more vulnerabilities which are resolved in subsequent patches.	The Linux version should be updated to the latest version of 5.17.

14) Link vulnerabilities exist between the password file and the zcip.script.	A link can be created to the /etc/passwd file. Through executing the zcip.script program, which can read/write root files, with this link, a new root user can be added to the system allowing complete control of the server.	Ensure that the right level of privilege/access is given to programs through a system such as AppArmor. Also, a flag should be added to all root level program files, ensuring their level of authority is not abused.
15) The ARP protocol is still in use (along with IPv4), as seen in Fig 11.	ARP translates between MAC addresses and IP addresses, however this is an out of date protocol. This allows denial of service, man in the middle attacks and session hijacking to be carried out more easily.	Upgrade the system to use IPv6 to make use of the NDP protocol, which is more secure in terms of defending against the three listed attacks.
16) There is no network traffic identifier in place.	Smurf and Fraggle denial of service attacks can be carried out and may succeed in shutting down the server, due to the lack of network traffic detection.	Use SNORT which prevents intrusion by tracking network traffic and data packets. It may also be useful to download anti-virus / anti-malware software.
17) The website server is not configured securely. The HTTP protocol is in use instead of HTTPS.	Malicious code can be injected into the webpage through a cross-side scripting (XSS) attack, causing sensitive information of users to be uncovered once the page is accessed by a victim. Cross-side scripting (XSS) attacks, including cookie theft, are the most common form of attacks.	An SSL certificate should be added to the website. Currently the HTTP protocol is used, which does not encrypt responses and requests. The HTTPS protocol should be used instead also. The server could be whitelisted, only allowing valid user inputs.
18) Hashed and salted passwords can be retrieved through the world-readable /etc/passwd file.	The /etc/passwd file can be printed to the terminal by any user, as seen in Fig 9. A hacker can easily run a rainbow table attack or a dictionary attack to find out what the passwords are, such as through Jack the Ripper.	The Linux version should be updated to the latest version of 5.17. This will move the passwords to /etc/shadow, which is only accessible by root users.
19) User encrypted files are poorly secured.	The encryption key of Jess and Mark's files are identical to their user passwords to access the system. If their passwords are known, their sensitive files can be viewed.	When encrypting files on the server, ensure that a different secure password is chosen, which contains at least a certain number of random characters, numbers and special characters.

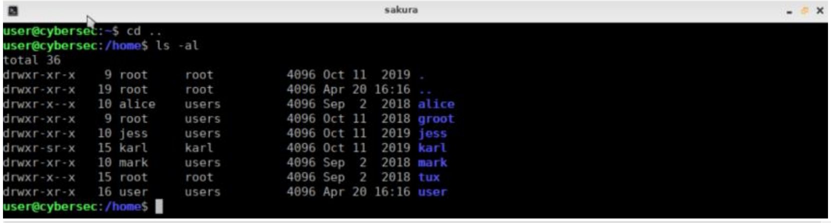
Solving the Mystery: [redacted] has a fake ID and her real name is [redacted] – [redacted] is the Bleeder. [redacted] loves [redacted], but [redacted] finds [redacted] annoying and really loves [redacted] [redacted] [redacted] penguin at night and is currently being stalked by [redacted], since she likes how strange he is. [redacted] also killed [redacted], since [redacted] head of security at Durhamazon and [redacted] was right in thinking that [redacted] became suspicious once he saw her leave a note at [redacted]. The Durham News was correct in reporting that the Bleeder kills all their victims with a biro to the throat, but also [redacted]

<u>Reference Images</u>

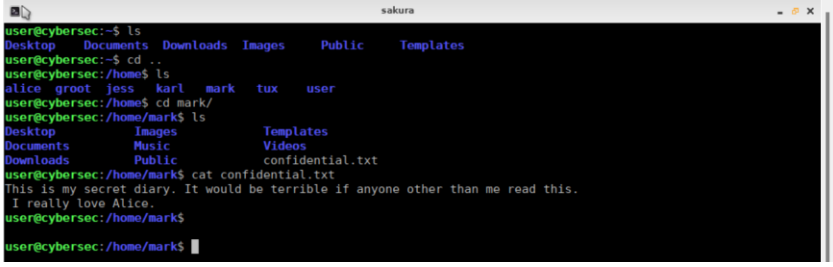


```
user@cybersec:~$ cd Desktop/
user@cybersec:~/Desktop$ cd Database/
user@cybersec:~/Desktop/Database$ sqlite3 Database.db
SQLite version 3.18.0 2017-03-28 18:48:43
Enter ".help" for usage hints.
sqlite> .show
        echo: off
         eqp: off
     explain: auto
     headers: off
        mode: list
   nullvalue: ""
      output: stdout
colseparator: "|"
rowseparator: "\n"
       stats: off
       width:
    filename: Database.db
sqlite> .tables
Messages  Orders    Users
sqlite> select *
   ...> from Users
   ...> ;
1|chris8|blahblah|Chris Willcocks|UK|4012864392131881
2|anna31|123123|Anna Lee|China|4222310943213
3|mark44|qwerty|Mark Pakhomios|Egypt|4012439011102583
4|jess101|weirdjedi|Jess Williams|USA|371449635398431
5|alice2|zxcvbn|Alice Summers|UK|4012421516217845
6|greg41|aoeuid|Gre��goire Louis|France|5221435020288205
7|karl21|frodo|Karl Southern|UK|4023214378388547
sqlite> █
```

Fig 1 – Private customer information



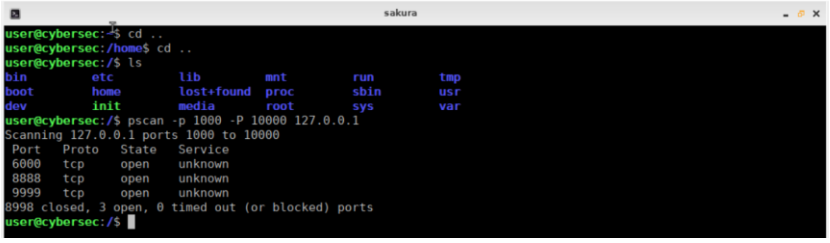
```
user@cybersec:~$ cd ..
user@cybersec:/home$ ls -al
total 36
drwxr-xr-x   9 root     root          4096 Oct 11  2019 .
drwxr-xr-x  19 root     root          4096 Apr 20 16:16 ..
drwxr-x--x  10 alice    users         4096 Sep  2  2018 alice
drwxr-xr-x   9 root     users         4096 Oct 11  2018 groot
drwxr-xr-x  10 jess     users         4096 Oct 11  2019 jess
drwxr-sr-x  15 karl     karl          4096 Oct 11  2019 karl
drwxr-xr-x  10 mark     users         4096 Sep  2  2018 mark
drwxr-x--x  15 root     root          4096 Sep  2  2018 tux
drwxr-xr-x  16 user     users         4096 Apr 20 16:16 user
user@cybersec:/home$ █
```



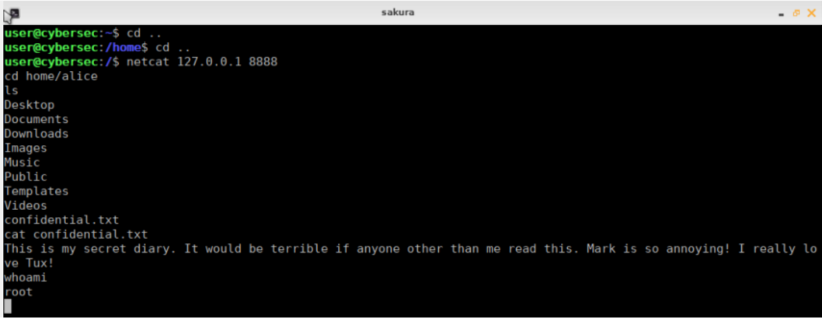
```
user@cybersec:~$ ls
Desktop    Documents  Downloads  Images     Public     Templates
user@cybersec:~$ cd ..
user@cybersec:/home$ ls
alice  groot  jess   karl   mark   tux    user
user@cybersec:/home$ cd mark/
user@cybersec:/home/mark$ ls
Desktop          Images           Templates
Documents        Music            Videos
Downloads        Public           confidential.txt
user@cybersec:/home/mark$ cat confidential.txt
This is my secret diary. It would be terrible if anyone other than me read this.
 I really love Alice.
user@cybersec:/home/mark$

user@cybersec:/home/mark$ █
```

Fig 2.1 and Fig 2.2 – Standard user permissions and [redacted] secret diary

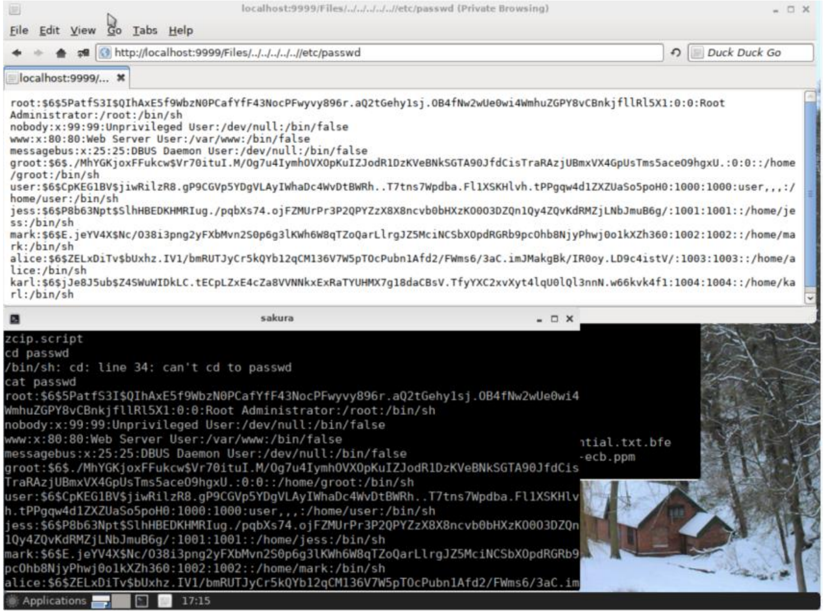


```
user@cybersec:~$ cd ..
user@cybersec:/home$ cd ..
user@cybersec:/$ ls
bin         etc         lib         mnt         run         tmp
boot        home        lost+found  proc        sbin        usr
dev         init        media       root        sys         var
user@cybersec:/$ pscan -p 1000 -P 10000 127.0.0.1
Scanning 127.0.0.1 ports 1000 to 10000
 Port   Proto   State   Service
 6000   tcp     open    unknown
 8888   tcp     open    unknown
 9999   tcp     open    unknown
8998 closed, 3 open, 0 timed out (or blocked) ports
user@cybersec:/$ █
```



```
user@cybersec:~$ cd ..
user@cybersec:/home$ cd ..
user@cybersec:/$ netcat 127.0.0.1 8888
cd home/alice
ls
Desktop
Documents
Downloads
Images
Music
Public
Templates
Videos
confidential.txt
cat confidential.txt
This is my secret diary. It would be terrible if anyone other than me read this. Mark is so annoying! I really lo
ve Tux!
whoami
root
█
```

Fig 3.1 and Fig 3.2 – Using pscan to see the open ports and gained root access


localhost:9999/Files/../../../../..//etc/passwd (Private Browsing)
File Edit View Go Tabs Help
Duck Duck Go
localhost:9999/...
sakura
Applications
17:15

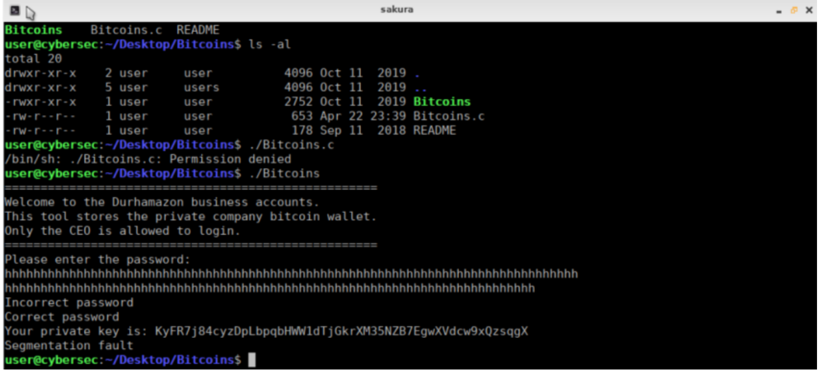
http://localhost:9999/Files/../../../../..//etc/passwd

```
root:$6$5PatfS3I$QIhAxE5f9WbzN0PCafYfF43NocPFwyvy896r.aQ2tGehy1sj.OB4fNw2wUe0wi4WmhuZGPY8vCBnkjfllRl5X1:0:0:Root
Administrator:/root:/bin/sh
nobody:x:99:99:Unprivileged User:/dev/null:/bin/false
www:x:80:80:Web Server User:/var/www:/bin/false
messagebus:x:25:25:DBUS Daemon User:/dev/null:/bin/false
groot:$6$./MhYGKjoxFFukcw$Vr70ituI.M/Og7u4IymhOVXOpKuIZJodR1DzKVeBNkSGTA90JfdCisTraRAzjUBmxVX4GpUsTms5aceO9hgxU.:0:0::/home
/groot:/bin/sh
user:$6$CpKEG1BV$jiwRilzR8.gP9CGVp5YDgVLAyIWhaDc4WvDtBWRh..T7tns7Wpdba.Fl1XSKHlvh.tPPgqw4d1ZXZUaSo5poH0:1000:1000:user,,,:/
home/user:/bin/sh
jess:$6$P8b63Npt$SlhHBEDKHMRIug./pqbXs74.ojFZMUrPr3P2QPYZzX8X8ncvb0bHXzKO0O3DZQn1Qy4ZQvKdRMZjLNbJmuB6g/:1001:1001::/home/je
ss:/bin/sh
mark:$6$E.jeYV4X$Nc/O38i3png2yFXbMvn2S0p6g3lKWh6W8qTZoQarLlrgJZ5MciNCSbXOpdRGRb9pcOhb8NjyPhwj0o1kXZh360:1002:1002::/home/ma
rk:/bin/sh
alice:$6$ZELxDiTv$bUxhz.IV1/bmRUTJyCr5kQYb12qCM136V7W5pTOcPubn1Afd2/FWms6/3aC.imJMakgBk/IR0oy.LD9c4istV/:1003:1003::/home/a
lice:/bin/sh
karl:$6$jJe8J5ub$Z4SWuWIDkLC.tECpLZxE4cZa8VVNNkxExRaTYUHMX7g18daCBsV.TfyYXC2xvXyt4lqU0lQl3nnN.w66kvk4f1:1004:1004::/home/ka
rl:/bin/sh
```

```
zcip.script
cd passwd
/bin/sh: cd: line 34: can't cd to passwd
cat passwd
root:$6$5PatfS3I$QIhAxE5f9WbzN0PCafYfF43NocPFwyvy896r.aQ2tGehy1sj.OB4fNw2wUe0wi4
WmhuZGPY8vCBnkjfllRl5X1:0:0:Root Administrator:/root:/bin/sh
nobody:x:99:99:Unprivileged User:/dev/null:/bin/false
www:x:80:80:Web Server User:/var/www:/bin/false
messagebus:x:25:25:DBUS Daemon User:/dev/null:/bin/false
groot:$6$./MhYGKjoxFFukcw$Vr70ituI.M/Og7u4IymhOVXOpKuIZJodR1DzKVeBNkSGTA90JfdCis
TraRAzjUBmxVX4GpUsTms5aceO9hgxU.:0:0::/home/groot:/bin/sh
user:$6$CpKEG1BV$jiwRilzR8.gP9CGVp5YDgVLAyIWhaDc4WvDtBWRh..T7tns7Wpdba.Fl1XSKHlv
h.tPPgqw4d1ZXZUaSo5poH0:1000:1000:user,,,:/home/user:/bin/sh
jess:$6$P8b63Npt$SlhHBEDKHMRIug./pqbXs74.ojFZMUrPr3P2QPYZzX8X8ncvb0bHXzKO0O3DZQn
1Qy4ZQvKdRMZjLNbJmuB6g/:1001:1001::/home/jess:/bin/sh
mark:$6$E.jeYV4X$Nc/O38i3png2yFXbMvn2S0p6g3lKWh6W8qTZoQarLlrgJZ5MciNCSbXOpdRGRb9
pcOhb8NjyPhwj0o1kXZh360:1002:1002::/home/mark:/bin/sh
alice:$6$ZELxDiTv$bUxhz.IV1/bmRUTJyCr5kQYb12qCM136V7W5pTOcPubn1Afd2/FWms6/3aC.im
```

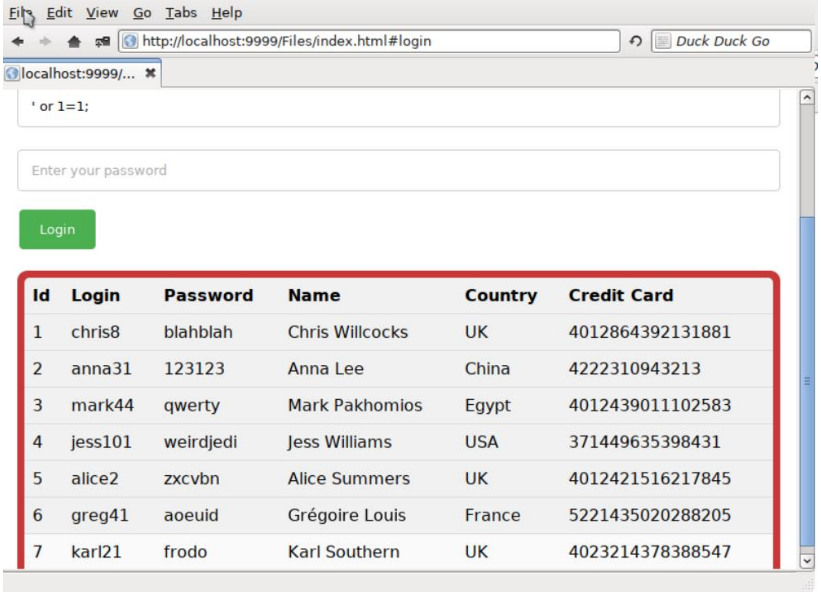
```
ntial.txt.bfe
-ecb.ppm
```

Fig 4 – The hashed passwords can be accessed through both the public server and with root access



```
Bitcoins    Bitcoins.c  README
user@cybersec:~/Desktop/Bitcoins$ ls -al
total 20
drwxr-xr-x    2 user     user          4096 Oct 11  2019 .
drwxr-xr-x    5 user     users         4096 Oct 11  2019 ..
-rwxr-xr-x    1 user     user          2752 Oct 11  2019 Bitcoins
-rw-r--r--    1 user     user           653 Apr 22 23:39 Bitcoins.c
-rw-r--r--    1 user     user           178 Sep 11  2018 README
user@cybersec:~/Desktop/Bitcoins$ ./Bitcoins.c
/bin/sh: ./Bitcoins.c: Permission denied
user@cybersec:~/Desktop/Bitcoins$ ./Bitcoins
====================================================
Welcome to the Durhamazon business accounts.
This tool stores the private company bitcoin wallet.
Only the CEO is allowed to login.
====================================================
Please enter the password:
hhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhh
hhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhh
Incorrect password
Correct password
Your private key is: KyFR7j84cyzDpLbpqbHWW1dTjGkrXM35NZB7EgwXVdcw9xQzsqgX
Segmentation fault
user@cybersec:~/Desktop/Bitcoins$
```

Fig 5 – Password bypass from buffer overflow



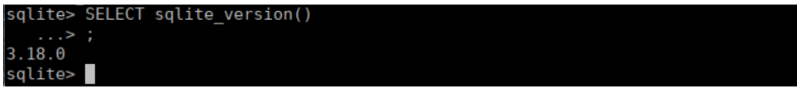
http://localhost:9999/Files/index.html#login

' or 1=1;

Enter your password

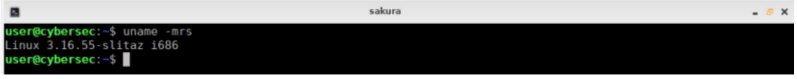
Id	Login	Password	Name	Country	Credit Card
1	chris8	blahblah	Chris Willcocks	UK	4012864392131881
2	anna31	123123	Anna Lee	China	4222310943213
3	mark44	qwerty	Mark Pakhomios	Egypt	4012439011102583
4	jess101	weirdjedi	Jess Williams	USA	371449635398431
5	alice2	zxcvbn	Alice Summers	UK	4012421516217845
6	greg41	aoeuid	Grégoire Louis	France	5221435020288205
7	karl21	frodo	Karl Southern	UK	4023214378388547

Fig 6 – SQL injection attack



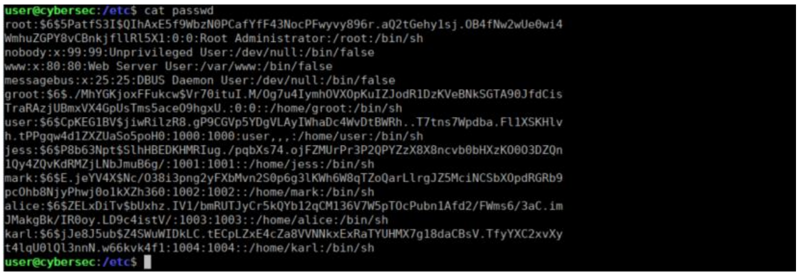
```
sqlite> SELECT sqlite_version()
   ...> ;
3.18.0
sqlite> 
```

Fig 7 – SQL version



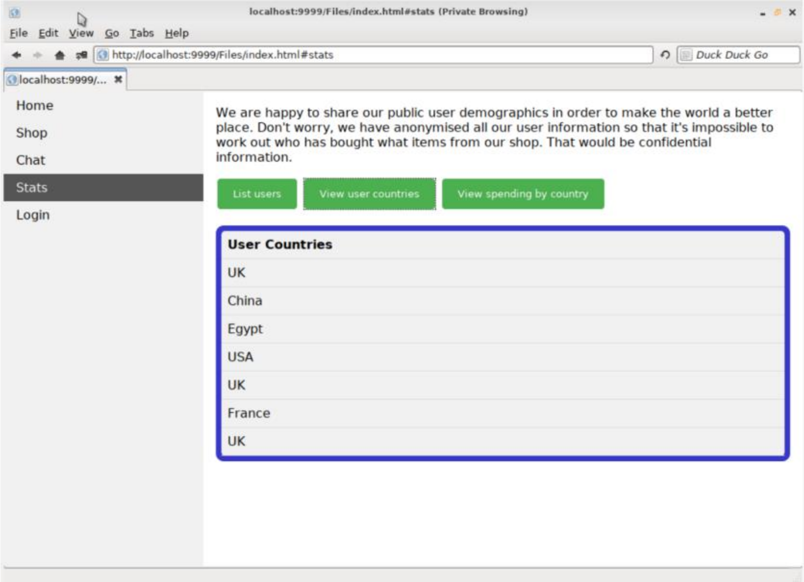
```
user@cybersec:~$ uname -mrs
Linux 3.16.55-slitaz i686
user@cybersec:~$ 
```

Fig 8 – Kernel version



```
user@cybersec:/etc$ cat passwd
root:$6$5PatfS3I$QIhAxE5f9WbzN0PCafYfF43NocPFwyvy896r.aQ2tGehy1sj.OB4fNw2wUe0wi4
WmhuZGPY8vCBnkjfllRl5X1:0:0:Root Administrator:/root:/bin/sh
nobody:x:99:99:Unprivileged User:/dev/null:/bin/false
www:x:80:80:Web Server User:/var/www:/bin/false
messagebus:x:25:25:DBUS Daemon User:/dev/null:/bin/false
groot:$6$./MhYGKjoxFFukcw$Vr70ituI.M/Og7u4IymhOVXOpKuIZJodR1DzKVeBNkSGTA90JfdCis
TraRAzjUBmxVX4GpUsTms5ace09hgxU.:0:0::/home/groot:/bin/sh
user:$6$CpKEG1BV$jiwRilzR8.gP9CGVp5YDgVLAyIWhaDc4WvDtBWRh..T7tns7Wpdba.Fl1XSKHlv
h.tPPgqw4d1ZXZUaSo5poH0:1000:1000:user,,,:/home/user:/bin/sh
jess:$6$P8b63Npt$SlhHBEDKHMRIug./pqbXs74.ojFZMUrPr3P2QPYZzX8X8ncvb0bHXzKO0O3DZQn
1Qy4ZQvKdRMZjLNbJmuB6g/:1001:1001::/home/jess:/bin/sh
mark:$6$E.jeYV4X$Nc/O38i3png2yFXbMvn2S0p6g3lKWh6W8qTZoQarLlrgJZ5MciNCSbXOpdRGRb9
pcOhb8NjyPhwj0o1kXZh360:1002:1002::/home/mark:/bin/sh
alice:$6$ZELxDiTv$bUxhz.IV1/bmRUTJyCr5kQYb12qCM136V7W5pTOcPubn1Afd2/FWms6/3aC.im
JMakgBk/IR0oy.LD9c4istV/:1003:1003::/home/alice:/bin/sh
karl:$6$jJe8J5ub$Z4SWuWIDkLC.tECpLZxE4cZa8VVNNkxExRaTYUHMX7g18daCBsV.TfyYXC2xvXy
t4lqU0lQl3nnN.w66kvk4f1:1004:1004::/home/karl:/bin/sh
user@cybersec:/etc$ 
```

Fig 9 – World-readable passwd file

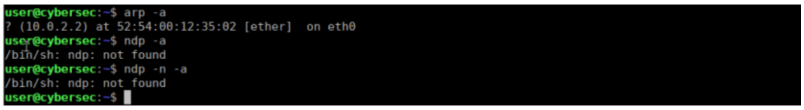


localhost:9999/Files/index.html#stats (Private Browsing)
File Edit View Go Tabs Help
http://localhost:9999/Files/index.html#stats
Duck Duck Go
localhost:9999/...
Home
Shop
Chat
Stats
Login
List users
View user countries
View spending by country

We are happy to share our public user demographics in order to make the world a better place. Don't worry, we have anonymised all our user information so that it's impossible to work out who has bought what items from our shop. That would be confidential information.

User Countries
UK
China
Egypt
USA
UK
France
UK

Fig 10 – Table containing repeated countries



```
user@cybersec:~$ arp -a
? (10.0.2.2) at 52:54:00:12:35:02 [ether]  on eth0
user@cybersec:~$ ndp -a
/bin/sh: ndp: not found
user@cybersec:~$ ndp -n -a
/bin/sh: ndp: not found
user@cybersec:~$ 
```

Fig 11 – ARP protocol still in use