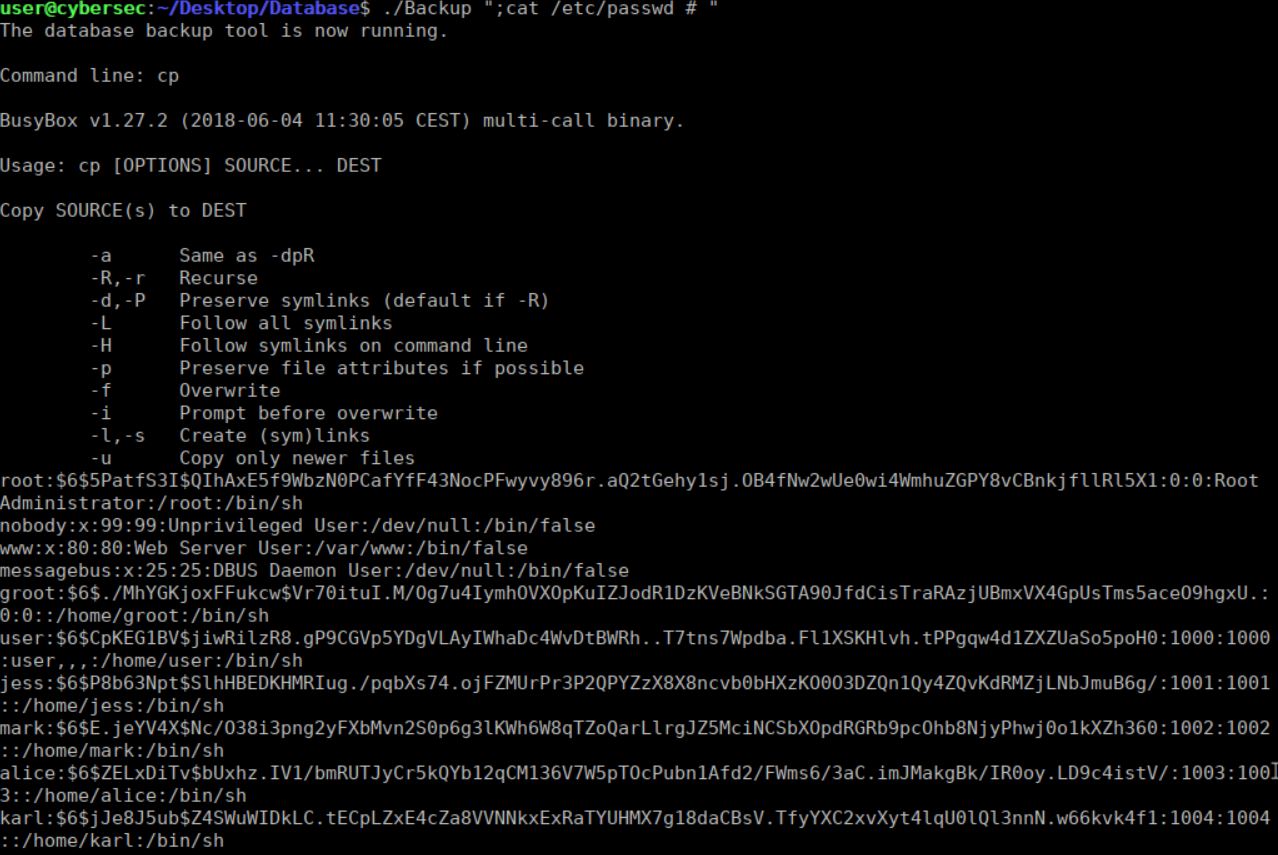
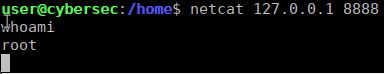
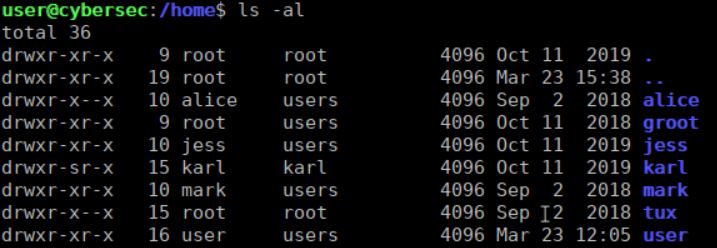
|  |  |  |
| --- | --- | --- |
| **Vulnerability** | **Exploit/Problem** | **Mitigation** |
| All users’ passwords are stored as plain text. | Open the database with  **Sqlite3 Database.db**  Run SQL Command   * SELECT \* * FROM users   To view entire table of plaintext passwords.**1** | Add a random salt to the plaintext password and then hash the result. |
| Multiple ports have been left open. Port 8888 has access to a root shell. | Open a shell using  **Netcat 127.0.0.1 8888**  Identify the level of the shell  **Whoami 2** | Remove or alter the program which keeps port 8888 open.  Use a firewall to block traffic on unspecified ports. |
| Multiple system user’s “other” permissions have read and execute permissions. | Anyone can access users  **Groot, Jess, Karl, Mark**  And any of their files.**3** | Change permissions to remove read and execute permissions in “other” eg  **Chmod o-rx groot** |
| The database backup has root permission and uses system(). | Any user input is run as root.  Run the program as  **“./Backup “; cat /etc/passwd #”**  To make system() run a multiline command with the original destination commented out. | Disable user input, saving only to a pre-specified location.  Reset setuid bit when not attempting to backup. |
| Website is vulnerable to cross-site scripting (xss). | Inject malicious code into the chat username or message box.  **“/><script>alert(/Hello there!/);</script> 5** | Introduce HTML escaping and sanitisation so that all input doesn’t cause unexpected and malicious behaviour. |
| The website is vulnerable to path traversal attacks. | Files can be traversed adding the path, for example  [**http://localhost:9999/%2e%2e%2f**](http://localhost:9999/%2e%2e%2f) **6** | Add a whitelist so that only set expressions are accepted. |
| The bootloader (Grub) can be edited. | Add the option  **Init = /bin/sh**  To the bootloader options to boot directly to a root shell. **7** | Add a password to the bootloader. |
| List of users and countries match. | As spending per country is listed the items brought by each user can be inferred. | Randomise the country list so as to not match users list. Or remove sensitive data. |
| Bitcoins.c has a buffer variable limited to 64 characters. | Input 65 characters with the last having value >= 1 to overflow the buffer, this will print out the key. **8** | Compile with  **-fstack-protector**  Use fgets() to only read specified amount of characters.  Use heap memory so memory can grow. |
| Multiple users have weak passwords. | Access the /etc/passwd file using the root shell exploit (2).  Run john on the file to get multiple user passwords. **9** | Set minimum length, character type and case requirements to increase password strength. |
| SQL injection works on login page. | Enter this as a password:  **‘ OR 1 = 1 --**  And all user details are displayed. **10** | Parameterise the SQL statement so the code and data don’t mix. |
| ECB encrypts identical plaintext blocks into the same cipher text. | The encrypted image on Jess’ account is still recognisable due to patterns still being present. | Encrypt the image with a different such as CBC to remove patterns. |
| Jess and Karl use the same password multiple times. | Using the same password as obtained from (9) you can decrypt their files, eg run  **bcrypt [filename]**  Enter the key: **starwars**  For Jess’ | Advise staff not to use passwords in multiple places. |
| The bitcoin wallet password is stored in plaintext and can be viewed. | Run  **cat Bitcoins**  And the plaintext password is present in the text. **11** | Hash the password in the code and then compare the hashed user input to it. |
| The website’s login page is vulnerable to brute force attack. | Consecutive login requests can be made using wordlists to attempt to gain access. | Set a maximum amount of login attempts allowed within a certain time period. |
| Database backup is only in one location and on one media type. | If anything happens on site or to the system the database and its backups are lost. | Create automatic backups on at least 2 types of media and have an off-site copy. |
| Device files can be accessed by root. | Anyone with access to root can access terminals and memory of all users allowing | Make sure root is secure to deny access. |
| Database will not record changes or access. | Any unauthorised changes to the database or exploits will be missed meaning more damage could be done before being stopped. | Add auditing software to the database to record changes, access history and DOS monitoring. |
| The backup file is vulnerable to stack smashing. | The input buffer only holds 1024 characters. Inputting can alter the jump instruction for execution of shell code. | Use heap memory so that the input string has enough memory allocated. |
| Any logged in users can see sensitive information about others. | Anyone logged in can steal credit card, login or location information of all other users and exploit it. | Change the SQL query in Server.c to only SELECT non- sensitive information rather than \*. |
| The server does not filter or authenticate incoming traffic. | This can leave the server open to DDOS, IP-spoofing and smurf and fraggle attacks. | Add an authentication protocol.  Filter all traffic to only allow valid users.  Add access control lists. |
|  |  |  |
|  |  |  |
|  |  |  |



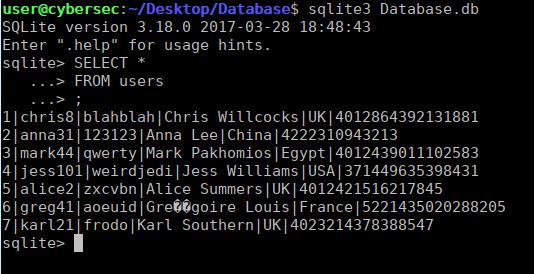
4



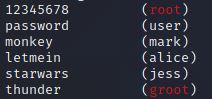
2



3



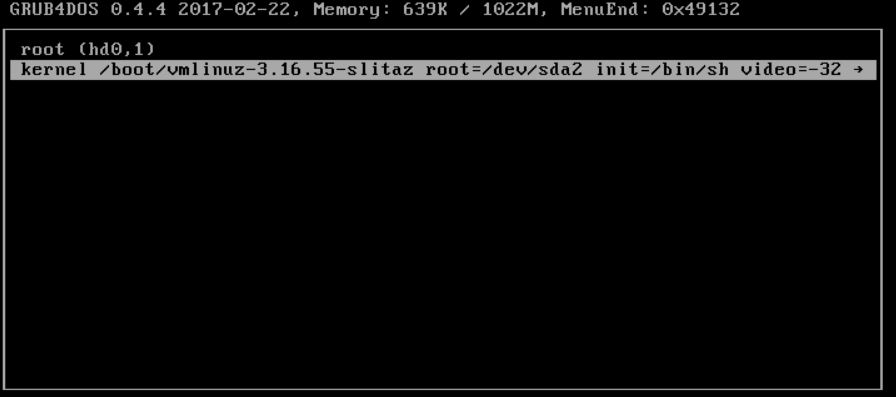
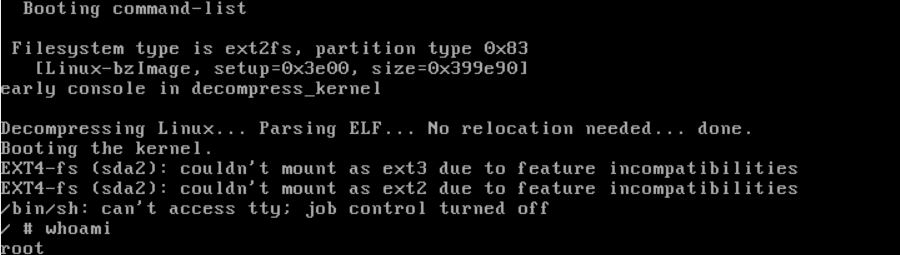
1



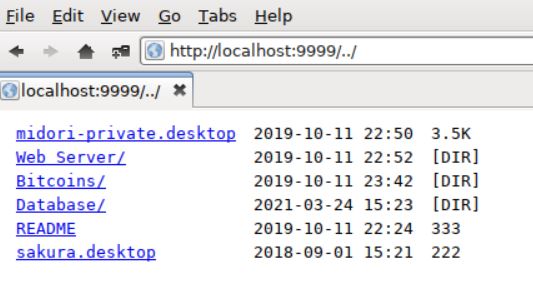
9



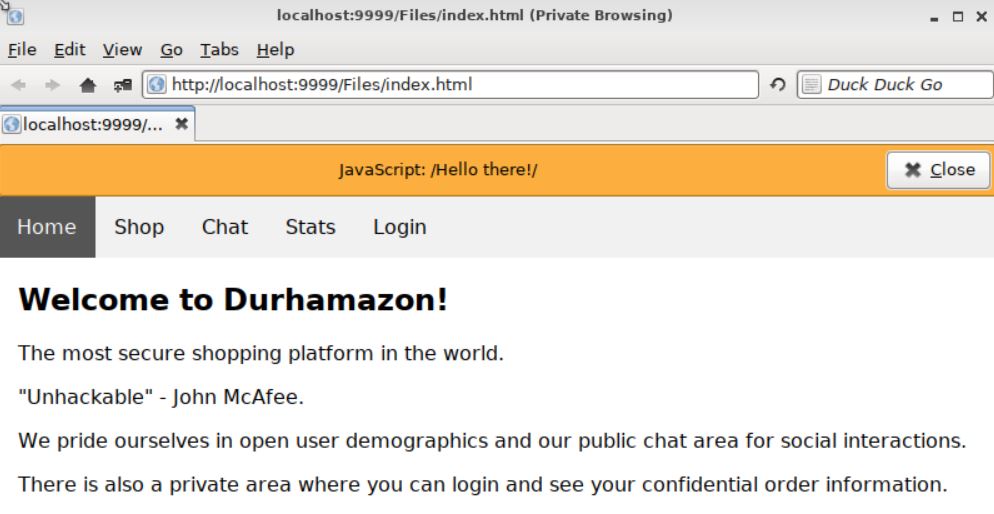
8



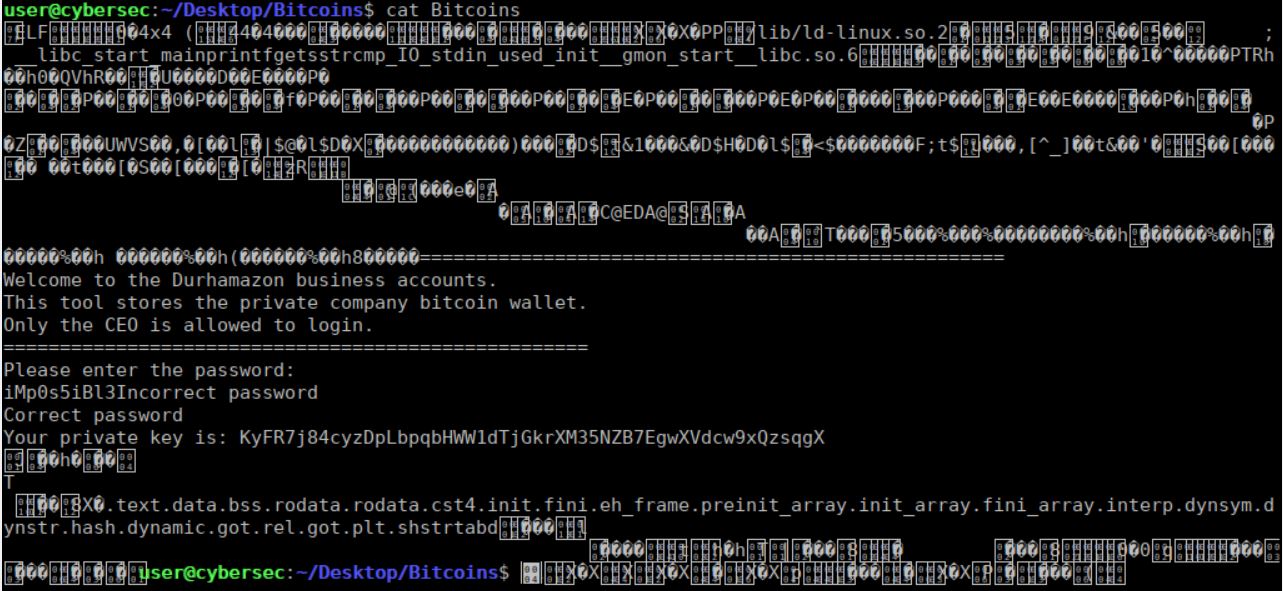
7



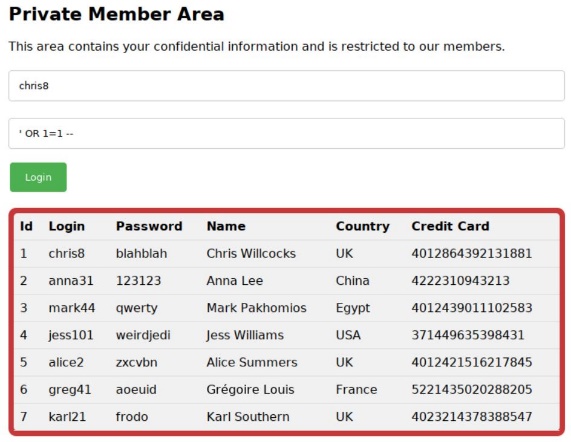
6



5



11



10