## Vulnerabilities

|  |  |  |  |
| --- | --- | --- | --- |
| Number | Vulnerability | Exploit \ Problem | Mitigation |
| 1 | All user personal information, including their credit card details, usernames and passwords, can be found via the website. | Someone could perform a simple SQL injection in the Login section of the website. | Use SQL injection parameters or a dictionary of banned words to prevent SQL injections. |
| 2 | The CEO's bitcoin wallet can be accessed via the command line using a buffer overflow. | Someone could gain access to the bitcoin wallet, and then go on to steal the bitcoins. | Use heap memory, and do proper bounds checking using fgets() not gets() in the C program. |
| 3 | JavaScript can be executed in the Chat section of the website (Cross site scripting). | Potential hackers can execute malicious JavaScript code and access potentially sensitive information. | Sanitise user input by removing potentially dangerous characters, text or code. |
| 4 | Find other files through the url of the website (can’t remember what it is called but in practical) |  |  |
| 5 | Access the root password using John the Ripper |  |  |
| 6 | Probably access user purchase history |  |  |
| 7 | Access DB records |  |  |
| 8 | Access other people’s desktops with their private info |  |  |
| 9 |  |  |  |
| 10 |  |  |  |
| 11 |  |  |  |
| 12 |  |  |  |
| 13 |  |  |  |
| 14 |  |  |  |
| 15 |  |  |  |