After a brief security analysis on the US Squash / Club Locker system, there are a number of vulnerabilities that should cause serious concern to the security of player's personally identifiable data.

While the descriptions below are technical, the underlying message is that player's data is exposed to theft, the platform itself is open to attack that could lead to further personal theft of data and there are very limited security controls in place to stop intruders from causing serious damage to the system.

Specific examples have been omitted from this report so as not to encourage any malicious behavior.

Cross-site scripting

Once logged in to the US Squash / Club Locker platform, there appear to be no checks done for XSS-style attacks (https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)). This means that an attacker can easily insert JavaScript or other malicious code into standard text input fields (such as player profile information) that would then be run on other user's browsers. Such types of attacks could include stealing cookie information, displaying inappropriate material to other users, redirects that could lead to sites designed to trick people into giving personal details, and many other similar styles of attacks.

Updating user data

There appear to be no security methods in place, such as cross-site forgery protection, to update data in the Club Locker system. Using a basic web address format, it's possible to update the personal information of anyone in the database. All that is needed is a simple ID, which appears to be auto-incrementing, along with an updated list of fields. There isn't even a requirement to be logged in to the system in order to update profile records. This poses a major security risk, as someone with malicious intent could update all player's information within a matter of minutes.

Based on these two tests alone, there should be serious questions raised about the integrity of data on the Club Locker platform and the quality and expertise of those building the system.