Sicherheitsmaßnahmen

Welche Sicherheitsprobleme konnten wir erkennen?

Man konnte Javascript über die Config hinzufügen und somit Stored XSS ausführen. Ein Angreifer konnte die Config ändern, sobald er im selben Netz war wie die Anwendung.

Wie können wir die Anwender vor Angriffen im Internet schützen?

Indem man einen Login hinzufügt und indem der Input escapet wird und die möglichen benutzbare Zeichen auf ein Minimum reduziert werden (Whitelist).

An welchen Stellen in unserer Implementierung haben wir welche Schutzmaßnahmen eingebaut?

Beim Hochladen der Config wird der Name gegen Javascript escapet, damit kein schädlicher Code gespeichert wird. Aus zeitlichen Gründen konnte der Rest nicht implementiert werden.