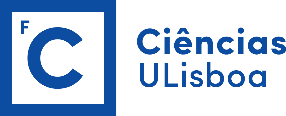
**“White Shuttle”**

**Vulnerabilities Definition**

Report:

Existem pelo menos 3 vulnerabilidades no código:

1. Ficheiro “Registered\_Users.csv” é criado em cada um dos clientes, onde contém a chave pública de cada user que entrou na app, juntamente com o ip e o seu nome de utilizador, no entanto é uma vulnerabilidade porque dá mais informação do que a necessária para qualquer user malicioso que possa entrar na app (confidencialidade dos dados)
2. Não garante integridade das mensagens, o algoritmo que usamos para assinar (SHA256withRSA), aplica a função de Hash e depois assina, onde o objetivo deste algoritmo é passar do domínio da mensagem para o domínio da função de assinatura:

<https://www.iacr.org/archive/crypto2000/18800229/18800229.pdf>

1. Uma vez que não há validação do user, qualquer user se pode fazer passar por outro e estar a falar com alguém pensando que é outra pessoa (spoofing)
2. Como o ficheiro onde são guardados os users registados é um CSV, se dermos um Username que contenha vírgulas, ele apenas regista como username o que vem antes da vírgula, e o restante fica guardado no ficheiro

