# UTS CSEC CTF FLAG WRITEUP

### Title: Jason Gets Confused

**Date made: 3/30/2020**

**Used in what CSEC CTF: Web?**

**Flag: CSEC{J50n\_@lw4yz\_g3Tz\_C0nFu53d\_0n\_t3h\_w3B}**

**Difficulty:Medium (probably hard, need a review)**

**Category: Web**

**Description: Jason always gets locked out of his house because he gets his keys confused**

**Hint(s): JWT**

**Writeup:**

**Look at robots.txt to find a key.pem file**

**Find username and password located in the source code of the login page**

**Login as that user**

**See JWT and that it’s signed with RS256, probably using key.pem as the public key**

**Decode JWT and see user role field**

**Use a JWT key confusion vulnerability to tamper with and sign your own token with HS256 instead of RS256, with the public key being used as the HMAC secret.**

**Apply the token and get flag**