

# CMSC388N:

## Build It, Break It, Fix It: Competing to Secure Software

Lecture 7 - In-class break time

Prof. Daniel Votipka  
Winter 2020



**COMPUTER SCIENCE**  
UNIVERSITY OF MARYLAND

# The Plan

- Manual testing
- Issues with JSON
- Security Violations
- In-class break time!

# Manual Testing

- You still need to submit breaks and fixes
- All breaks go in the break folder (including **textual breaks**)
  - Put empty string for “programs” if it is a textual break
- Monitor these Google Sheets:
  - [Submission Status](#)
  - [Score Changes](#)
- You have 24 hours from the start of the following day to fix before you lose more points

These links are on the course website Project page

# Issues with JSON

- Your break must be in its own folder
- Your break folder must include a **description.txt** and **test.json** (use those exact names)
- Make sure you don't have unicode quotes in your submissions
- They should look like **"**, not **”**

# Security Violations

- Oracle returns DENIED\_\*, but the target doesn't (confidentiality, integrity)
- Oracles returns correctly, but the target returns DENIED\_\* (availability)
- Must demonstrate correct behavior first
- Oracle times out, but the target hangs (availability)
- Target unexpectedly terminates (availability)

# Not Security Violations

- Oracle returns FAILED, but target doesn't (correctness)
- Target and Oracle return different values
- Program changing permissions fails on target, causing the next program to allow DENIED behavior

# In-class Break Time!

- Divide up into teams and spread out
- You can leave this room, but stay on this floor
- Send us a message in Slack with where you go
- Instructors will come around to talk