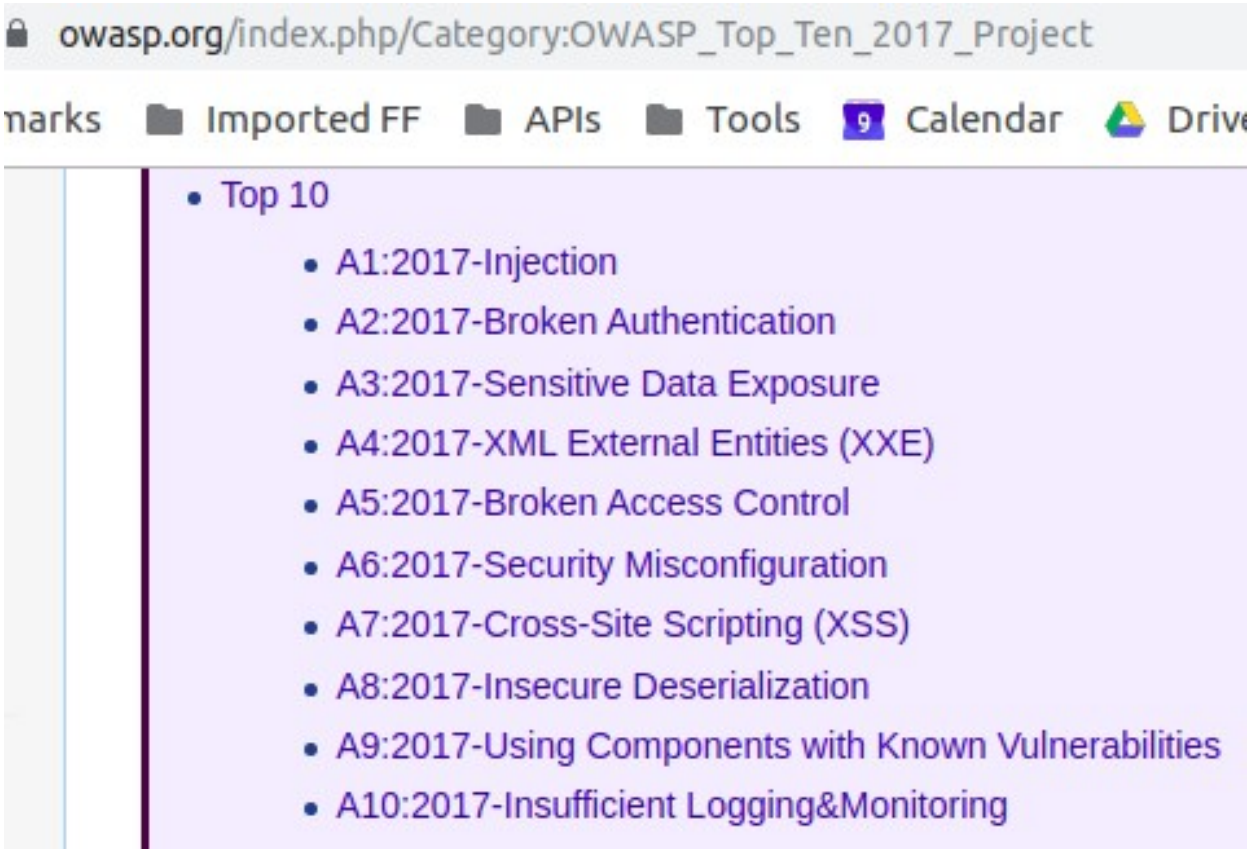
OWASP Top 10 Vulnerabilities



Threat Model- XSRF

What is XSRF / CSRF

- X-site Request Forgery
- Demo1 https://youtu.be/6TsjwC-AYc0
- Demo2 https://youtu.be/5joX1skQtVE
- How to prevent ?
  - XSRF Token
  - Server side transaction handling

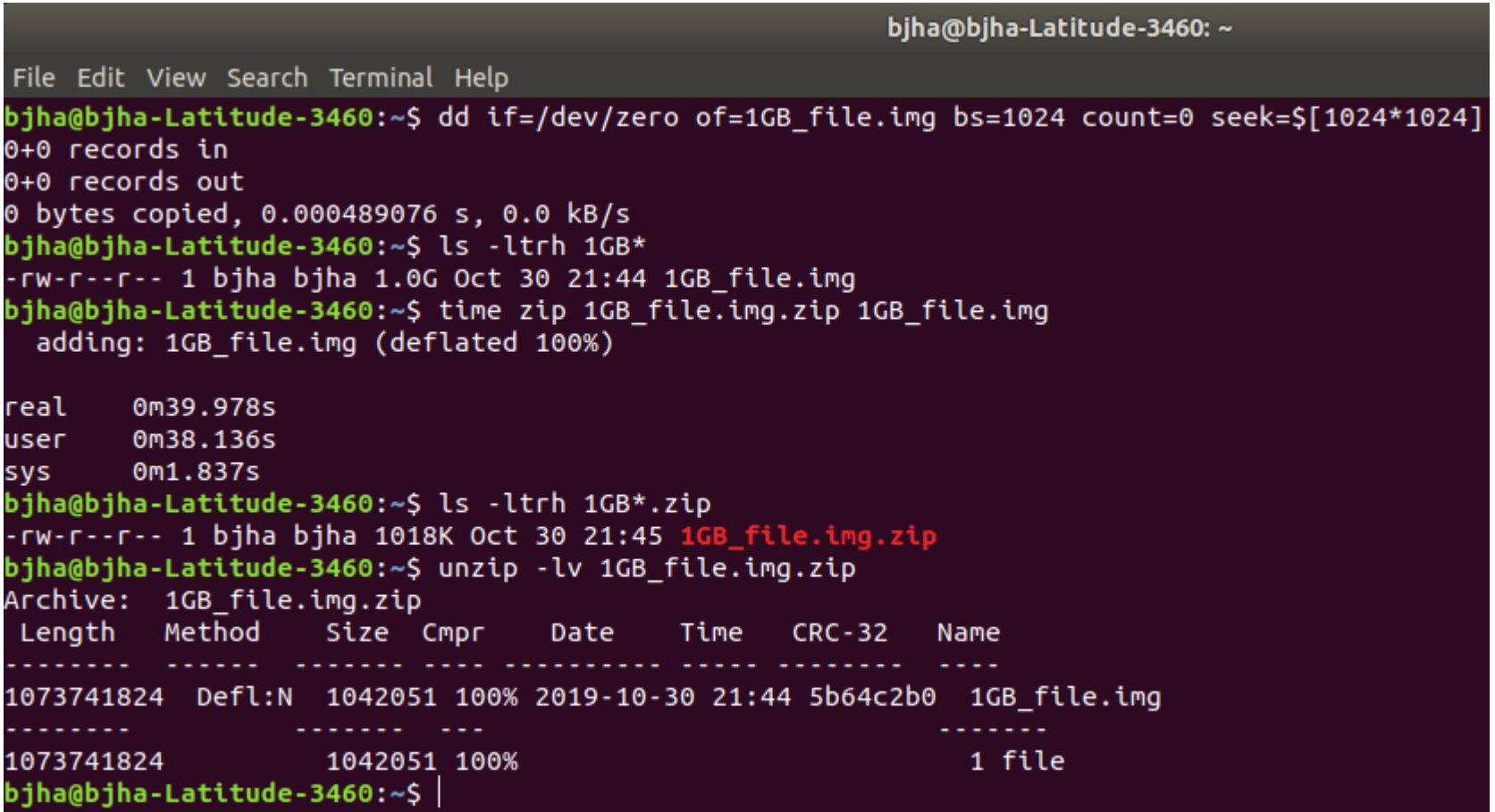
Insecure Direct Object Reference (IDOR) Attack

- Information Disclosure
- Insufficient Authorization Checks
- Demo https://youtu.be/TRDyvgkBcUs

XXE attack

- Demo https://youtu.be/1l9erhtZt00
- Also called Billion Laugh (Lol;) Attack https://en.wikipedia.org/wiki/Billion_laughs_attack
- YAML also has similar vulnerability
- How to prevent?
  - SAST tool might help
  - Awareness about parser/DTD

Zip Bomb Attack



Security Misconfiguration

- Path traversal attack https://youtu.be/L95M0F55Fp0
- AWS demo: https://youtu.be/5joX1skQtVE
- Lessons?
  - Information disclosure
  - DoS
  - Reputation loss etc