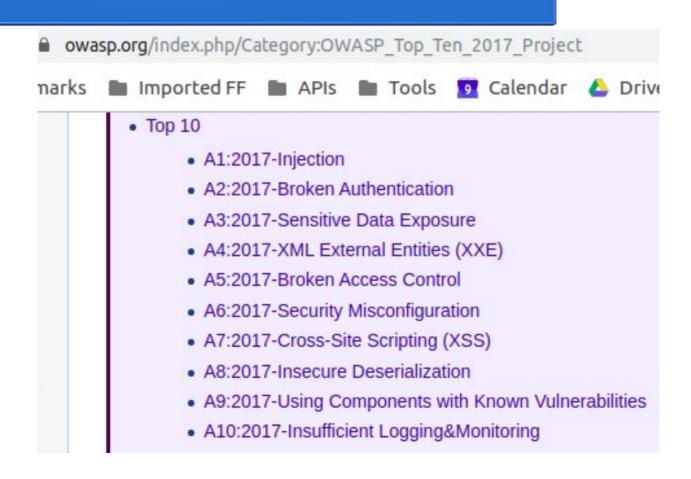
OWASP Top 10 Vulnerabilities



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

```
biha@biha-Latitude-3460: ~
File Edit View Search Terminal Help
bjha@bjha-Latitude-3460:~$ dd if=/dev/zero of=1GB file.img bs=1024 count=0 seek=$[1024*1024]
0+0 records in
0+0 records out
0 bytes copied, 0.000489076 s, 0.0 kB/s
bjha@bjha-Latitude-3460:~$ ls -ltrh 1GB*
-rw-r--r-- 1 bjha bjha 1.0G Oct 30 21:44 1GB file.img
bjha@bjha-Latitude-3460:~$ time zip 1GB file.img.zip 1GB file.img
 adding: 1GB file.img (deflated 100%)
real
       0m39.978s
user
       0m38.136s
       0m1.837s
svs
bjha@bjha-Latitude-3460:~$ ls -ltrh 1GB*.zip
-rw-r--r-- 1 bjha bjha 1018K Oct 30 21:45 1GB file.img.zip
bjha@bjha-Latitude-3460:~$ unzip -lv 1GB file.img.zip
Archive: 1GB file.img.zip
Length Method Size Cmpr Date Time CRC-32
                                                    Name
1 file
1073741824
                  1042051 100%
bjha@bjha-Latitude-3460:~$
```

Security Misconfiguration

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