

OWASP Top 10 Vulnerabilities

🔒 owasp.org/index.php/Category:OWASP_Top_Ten_2017_Project

marks 📁 Imported FF 📁 APIs 📁 Tools 9 📅 Calendar 🗄️ Drive

- Top 10

- A1:2017-Injection
- A2:2017-Broken Authentication
- A3:2017-Sensitive Data Exposure
- A4:2017-XML External Entities (XXE)
- A5:2017-Broken Access Control
- A6:2017-Security Misconfiguration
- A7:2017-Cross-Site Scripting (XSS)
- A8:2017-Insecure Deserialization
- A9:2017-Using Components with Known Vulnerabilities
- A10:2017-Insufficient Logging&Monitoring

Threat Model- XSRF

What is XSRF / CSRF

- X-site Request Forgery
- Demo1 <https://youtu.be/6TsjuC-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_laugh_attack
- YAML also has similar vulnerability
- How to prevent?
 - SAST tool might help
 - Awareness about parser/DTD

Zip Bomb Attack

```
bjha@bjha-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  
sys     0m1.837s  
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  
  -----  -----  -  
1073741824  Defl:N    1042051 100%  2019-10-30 21:44 5b64c2b0 1GB_file.img  
-----  -  
1073741824      1042051 100%                1 file  
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