OWASP

Open Web Application
Security Project

OWASP – bay area workshop

#	Vulnerability	Found
1	Insecure deserialization - pickle	
2	Insecure deserialization - yaml	
3	Server side template injection	
4	External entity attack	
5	Stored cross site scripting	
6	Reflected cross site scripting	
7	Cross site request forgery	
8	CORS misconfiguration	
9	Path/directory traversal	
10	Insecure file upload	
11	Hardcoded credentials	
12	JWT token is forgeable	
13	Username enumeration	
14	SQL injection	
15	Username enumeration	
16	Obscure backdoor	
17	Client side constraints	

The Open Web Application Security Project (OWASP) is a 501(c)(3) worldwide not-for-profit charitable organization focused on improving the security of software. Our mission is to make software security visible, so that individuals and organizations are able to make informed decisions. OWASP is in a unique position to provide impartial, practical information about AppSec to individuals, corporations, universities, government agencies and other organizations worldwide. Operating as a community of like-minded professionals, OWASP issues software tools and knowledge-based documentation on application security.