Web Secure Programming

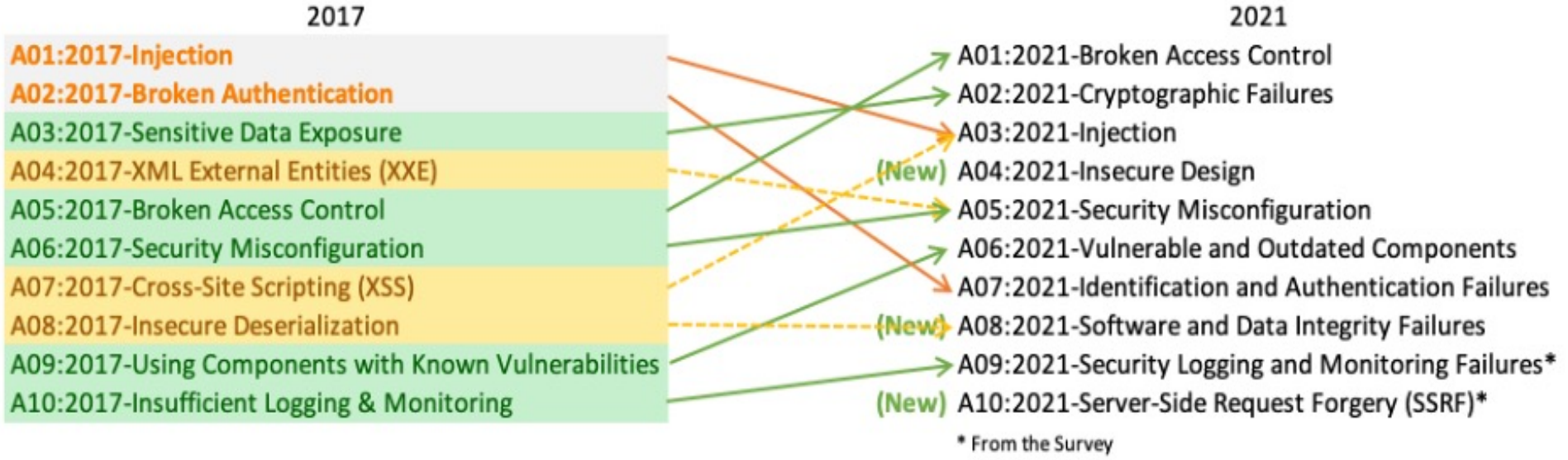
Lecture 5

Tamara Rezk

Project

- Topic deadline: 24/1 (it must be validated)
- Document deadline: 28/1 (max: 5 pages)
  - introduction, with an indication of sources
  - description of attacks, with examples
  - description of defenses, with examples
  - conclusion
- Presentation: 30/1 9-13h (compulsory presence)
  - Location: **Inria, Salle Euler Violet**
  - 30 minutes presentation + questions
  - possibility of obtaining 1..3 points if exceptional project + answer to questions (individual)

OWASP top-10


2017
A01:2017-Injection
A02:2017-Broken Authentication
A03:2017-Sensitive Data Exposure
A04:2017-XML External Entities (XXE)
A05:2017-Broken Access Control
A06:2017-Security Misconfiguration
A07:2017-Cross-Site Scripting (XSS)
A08:2017-Insecure Deserialization
A09:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging & Monitoring
2021
A01:2021-Broken Access Control
A02:2021-Cryptographic Failures
A03:2021-Injection
(New) A04:2021-Insecure Design
A05:2021-Security Misconfiguration
A06:2021-Vulnerable and Outdated Components
A07:2021-Identification and Authentication Failures
(New) A08:2021-Software and Data Integrity Failures
A09:2021-Security Logging and Monitoring Failures*
(New) A10:2021-Server-Side Request Forgery (SSRF)*
* From the Survey

OWASP A1 (2021)

https://owasp.org/Top10/A01_2021-Broken_Access_Control/

CSRF: bypassing access control

Transmits unauthorized commands from a user who has rightfully logged in to a website

CSRF example: Attack to GMail : January 2007

Google didn't check what page requested your contact list.

Hypothesis: you are logged in Gmail and have opened attacker.com site.

Attack: The page from attacker.com requests you contact list from google server. Since you are logged in google, your cookie is sent along the request and the request goes through.

Consequence: Attacker gets your contact list.

Prevention

- Server side:
  - add a secret (token) that the attacker cannot guess
  - re-authenticate for critical operations
  - set cookies to SameSite=Lax recommended reading: https://simonwillison.net/2021/Aug/3/samesite/
- User side:
  - logging off one site before using others
  - set your browser default

Question: could it have worked setting a cookie with the random number?

TP

- Write JavaScript code to perform a CSRF attack
- First, use a token to defend
- Second, use SameSite cookies to defend