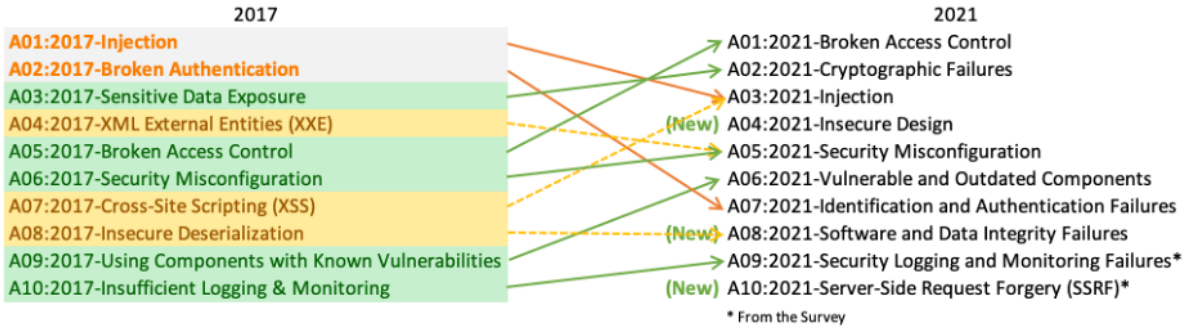
Auditoria Ciberseguretat

Llista de coses a mirar en una auditoria de ciberseguretat d'una pàgina web.

Metodologia OWASP

```
* Control d'accés remot.
* Errors criptogràfics.
* Injeccions.
* Disseny insegur.
* Mala configuració de seguretat.
* Components vulnerables i desactualitzats.
* Errors d'autenticació i identificació.
* Errors d'integritat de dades.
* Errors de monitoratge i sistema de logs.
* Vulnerabilitats: SSRF (Server-Side Request Forgery), XSS (Cross-site
    scripting), etc.
```



https://owasp.org/www-project-top-ten/

Domini

```
* Certificats
```

Sistema

```
* OS o serveis com OpenSSH desactualitzat.
* Xifrats insegurs.
* Defensa de ports per possible escaneig de ports.
* Permisos de directoris i fitxers.
* Rotació de logs.
```

Base de dades

```
* Revisar definicions de rols.
* Backups
```

Web

```
* Codi
* Assegurar tokens amb caducitat.
* Pérdua d'autenticació.
* Possible exposició de dades sensibles.
* Revisar si les contrasenyes i altres dades passen per canal encriptat.
* Revisar defenses contra atacs de força bruta. Poden fer falta bloquejos relacionats amb autenticacions incorrectes o altres coses.
* Que no s'enviïn contrasenyes per correu quan un usuari demana la recuperació de contrasenya.
* Permisos. Per exemple que no es puguin descarregar fitxers sense permís i autorització, com pot ser descarregar fitxers d'un altre usuari.
* Revisar que els errors que es retornen no incloguin dades del sistema o codi. (Stack Trace Disclosure)
* Desbordament potencial del buffer. Això pot passar quan la grandària de les dades que ha de rebre el servidor no es limita.
* Revisar si existeix possibilitat de pujar fitxers maliciosos.
* Anàlisi de métodes HTTP (GET, POST, PUT, DELETE, etc).
```

Altres

```
* Complexitat de contrasenyes: OS, bdd, web.
* Alertes per detectar possibles atacs, falta de RAM, espai i CPU.
* Tests d'intrusió. Pentesting.
* Tests en general per a tot.
```