UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

Seguretat d'aplicacions web: Principis i riscos OWASP

Pol Barco Martínez
Huiwen Cao
Max Vives Ribera
Adrian Préstamo Rubio

Índex

- SEGURETAT INFORMÀTICA
  - Objectius
  - Principis
- OWASP
  - Que és?
  - Per què serveix?
  - Què ofereix?
- OWASP Top 10
- PROBLEMES
- SOLUCIÓ
- CONCLUSIONS I VALORACIÓ PERSONAL
- REFERÈNCIES
- REPARTIMENT DEL TREBALL

Seguretat informàtica - Objectius

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

- Minimitzar els riscos
- Crear plataformes segures
- Protegir els llocs web, aplicacions web i serveis web
- Garantir els principis de la seguretat informàtica

Seguretat informàtica - Principis

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

- Integritat
- Privacitat
- Disponibilitat
- No rebuig o autenticitat

OWASP

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

Que és?

- OWASP (Open Web Application Security Project)
- Projecte sense ànim de lucre
- Busca millorar la seguretat del software
- Tots els materials disponibles de manera lliure
- Compta amb 32.000 voluntaris a tot el món

Per què serveix?

- Guies i metodologia a tenir en compte
- Referència en el procés de desenvolupament de noves aplicacions

OWASP - Què ofereix?

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

Materials d'educació:

- OWASP Top10
- Guia de desenvolupament OWASP
- Guia de Testing OWASP
- Guia OWASP per aplicacions web segures
- Moltes més

Software:

- WebGoat
- WebScarab
- ESAPI
- Moltes més

OWASP - Què ofereix?

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

Capítols locals:

- Comunitats interessades en Seguretat d'Aplicacions

Desenvolupament de nous projectes:

- Possibilitat d'utilitzar les eines i els col·laboradors disponibles per generar nous projectes

Beques de recerca:

- OWASP otorga beques a investigadors de la seguretat en aplicacions

OWASP - Top 10

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

- Projecte més conegut de OWASP
- Informe elaborat per experts en seguretat d'aplicacions
- Exposa les top 10 problemes més importants de les aplicacions web
- S'actualitza regularment
- Les organitzacions s'ho prenen com un document de conscienciació
- Gràcies a aquest ranking les organitzacions poden saber els riscs més importants

OWASP - Top 10

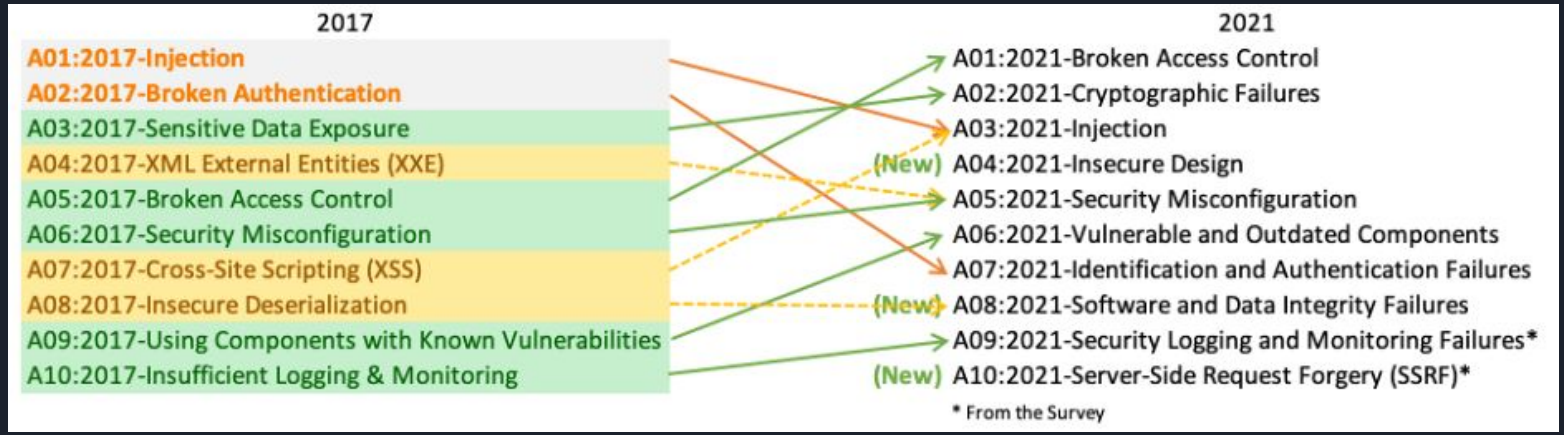
UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

A01:2021	Pèrdua de Control d'Accés
A02:2021	Fallades criptogràfiques
A03:2021	Injecció
A04:2021	Disseny insegur
A05:2021	Configuració incorrecta de la seguretat
A06:2021	Components vulnerables i obsolets
A07:2021	Falles d'identificació i autenticació
A08:2021	Falles en el Software i la integritat de les dades
A09:2021	Registre i supervisió insuficients
A10:2021	Falsificació de sol·licituds al costat del servidor

OWASP - Top 10

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

CANVIS AL TOP 10 DESDE 2017 FINS 2021



Com es relacionen amb els 4 principis de la seguretat?

	Confidencialidad	Integridad	Disponibilidad	No repudio	Autenticación
Pérdida de control de acceso		✓		✓	✓
Fallos criptográficos	✓	✓			
Inyección		✓			
Diseño inseguro		✓			
Mala configuración de la seguridad	✓	✓	✓	✓	✓
Uso de componentes con vulnerabilidades u obsoletos		✓	✓		
Autenticación rota	✓				✓
Fallos de integridad de software y datos		✓			
Fallos de registro y monitoreo de seguridad		✓			
Falsificación de solicitud por parte del servidor		✓	✓		

Problemes

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

- Per actualitzar l'informe es necessita temps
- Durant aquest temps les amenaces canvien

Solució

- Fer enquestes regulars a experts en seguretat y desenvolupament
- Exemple de una enquesta realitzada a experts:

Threat Agents / Attack Vectors		Security Weakness		Impacts	
Application Specific	Exploitability: 3	Prevalence: 3	Detectability: 3	Technical: 2	Business Specific
	3	3	3		
	Likelihood Rating: 3.0 (Average of Exploitability, Prevalence and Detectability)			* 2	
		Risk Ranking: 6.0 (Likelihood * Impact)			

Conclusions i valoració personal

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

- La seguretat informàtica és molt important actualment
- El OWASP top 10 ajuda a les empreses a saber quins riscs combatre

Referències

- https://owasp.org
- https://www.techtarget.com/searchsoftwarequality/definition/OWASP
- https://www.imperva.com/learn/application-security/owasp-top-10/
- https://owasp.org/www-project-webgoat/
- https://blog.pleets.org/article/conoce-owasp
- https://owasp.org/www-project-top-10-ci-cd-security-risks/
- https://owasp.org/www-pdf-archive/Introduccion_a_la_OWASP.pdf
- https://sucuri.net/guides/owasp_top_10_2021_edition/
- https://ostec.blog/es/seguridad-informacion/principios-basicos-de-la-seguridad-de-la-informacion/
- https://www.tecon.es/la-seguridad-de-la-informacion/

Repartiment de tasques

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

Cerca d'informació:

- Pol Barco
- Huiwen Cao
- Max Vives
- Adrian Préstamo

Presentació:

- Pol Barco
- Max Vives

Preparació del PowerPoint:

- Pol Barco
- Huiwen Cao
- Max Vives
- Adrian Préstamo

OWASP

Open Web Application Security Project

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH