UCAD - ESP - DGI - Crypto - DIC3 2022/2023

Rapport portant sur le choix d'un sujet

Présenté par :

- *Papa Abdou CALLOGA*
- *Yacine DIAGNE*
- *Yaye Khadidiatou DIOP*
- *Aby NDIAYE*
- *Alioune SALL*

Professeur : M. MENDY

Présentation

L'OWASP (Open Web Application Security Project) est une organisation à but non lucratif dont l'objectif premier est d'**assurer la sécurité des applications web**. Sa principale mission consiste à garantir la visibilité de la sécurité du logiciel. Elle vise également à fournir des informations et outils indispensables à l'amélioration de la sécurité des applications web dans leur ensemble.

L'un des projets les plus connus de cette organisation est **la création de l'OWASP Top 10**. Les listes OWASP Top 10 ont été créées pour différentes catégories. La liste OWASP Top 10 la plus utilisée est celle de 2017 et concerne notamment la sécurité des applications web. Elle prend en compte plusieurs risques de sécurité qu'on peut rencontrer sur un site internet.

Explication des facteurs de classement :

1. **CWEs associées :** le nombre de CWEs associées à une catégorie par l'équipe du Top 10.
2. **Taux d'incidence :** le taux d'incidence est le pourcentage d'applications vulnérables à cette CWE parmi la population testée par cette organisation pour cette année.
3. **Couverture (Test) :** Le pourcentage d'applications testées par toutes les organisations pour une CWE donnée.
4. **Exploitation pondérée :** le sous-score Exploitation des scores CVSSv2 et CVSSv3 attribués aux CVEs associées aux CWEs, normalisés et placés sur une échelle de 10 points.
5. **Impact pondéré :** le sous-score d'impact des scores CVSSv2 et CVSSv3 attribués aux CVEs associées aux CWEs, normalisés et placés sur une échelle de 10 points.
6. **Nombre total d'occurrences :** nombre total d'applications trouvées pour lesquelles les CWEs sont associées à une catégorie.
7. **Nombre total de CVEs :** nombre total de CVEs dans la base de données NVD qui ont été associées aux CWEs associées à une catégorie

Choix Catégorie

La catégorie que l'on a choisie sur la base de ces facteurs est : A02-2021 Défaillances cryptographiques, auparavant connu sous le nom A03-2017 Exposition de données sensibles.
En effet, celle-ci présente une corrélation directe avec le cours, et figure en deuxième position du classement de 2021. Elle était 3ième du classement de 2017, ce qui indique que cette catégorie constitue un risque constant, et grandissant. De plus, cette augmentation signale que la protection par mot de passe est de moins en moins suffisante, et que le cryptage doit être appliqué par défaut pour toutes les bases de données contenant des informations sensibles. (cf. tableau ci-après)

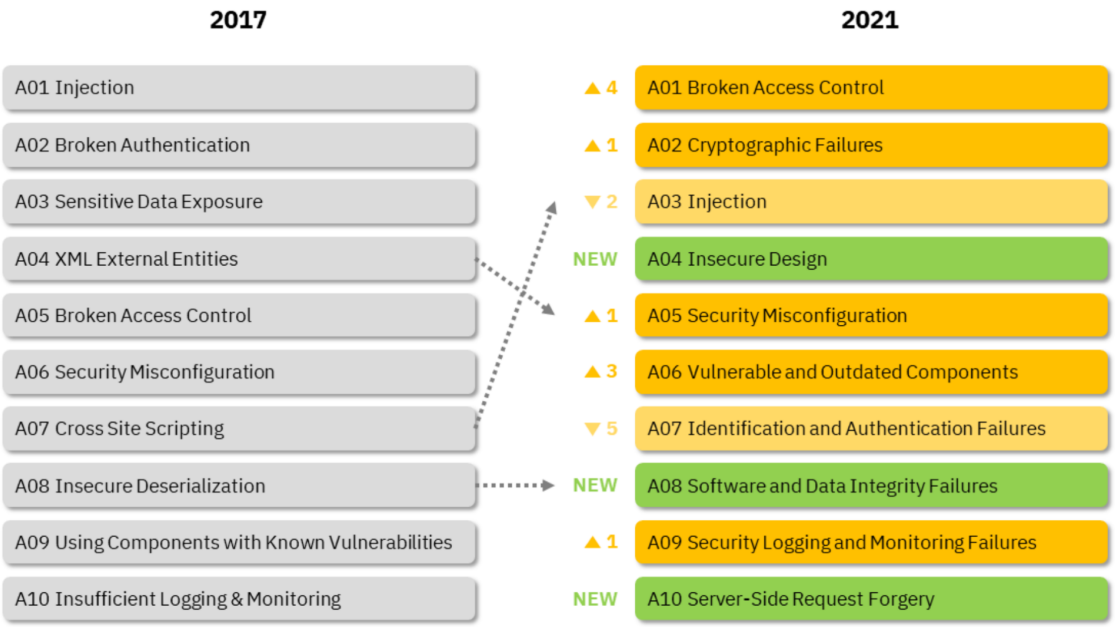

Figure 1 : Tableau de comparaison du rapport OWASP entre 2017 et 2021

Explication des chiffres

L'accent est mis sur les défaillances liées à la cryptographie (ou son absence). Cela entraîne souvent l'exposition de données sensibles. Les Common Weakness Enumerations (CWE) notables incluses sont CWE-259: Use of Hard-coded Password, CWE-327: Broken or Risky Crypto Algorithm, et CWE-331 Insufficient Entropy.

	CWE Asso	Taux Inc Max	Taux Inc Moy	Expl Pond Moy	Imp Pond Moy	Couv Max	Couv Moy	Nb Occ	Nb CVE	Rang
A01	34.0	55.97	3.81	6.92	5.93	94.55	47.72	318487.000	19013.0	1.0
A02	29.0	46.44	4.49	7.29	6.81	79.33	34.85	233788.000	3075.0	2.0
A03	33.0	19.09	3.37	7.25	7.15	94.04	47.90	274228.000	32078.0	3.0
A04	40.0	24.19	3.00	6.46	6.78	77.25	42.51	262407.000	2691.0	4.0
A05	20.0	19.84	4.51	8.12	6.56	89.58	44.84	208387.000	789.0	5.0
A06	3.0	27.96	8.77	51.78	22.47	5.00	5.00	30457.000	0.0	6.0
A07	22.0	14.84	2.55	7.40	6.50	79.51	45.72	132.195	3897.0	7.0
A08	10.0	16.67	2.05	6.94	7.94	75.04	45.35	47972.000	1152.0	8.0
A09	4.0	19.23	6.51	6.87	4.99	53.67	39.97	53615.000	242.0	9.0
A10	1.0	2.72	2.72	8.28	6.72	67.72	67.72	9503.000	385.0	10.0

A partir des différentes valeurs fournies dans le classement, on a pu établir le tableau suivant qui met en exergue la corrélation qui existe entre les différents facteurs et le rang.

On a pu remarquer que l'exploitation pondérée moyenne et l'impact pondéré moyen ont plus d'incidence sur le rang permet de voir la corrélation des différents facteurs de classement avec le rang.

	CWE Asso	Taux Inc Max	Taux Inc Moy	Expl Pond Moy	Imp Pond Moy	Couv Max	Couv Moy	Nb Occ	Nb CVE	Rang
CWE Asso	1.000000	0.526149	-0.398417	-0.422810	-0.381641	0.664477	0.124158	0.855452	0.562603	-0.841138
Taux Inc Max	0.526149	1.000000	0.228766	0.056919	0.040454	0.142789	-0.348206	0.654556	0.279834	-0.825255
Taux Inc Moy	-0.398417	0.228766	1.000000	0.780587	0.699929	-0.789331	-0.809840	-0.152894	-0.220747	0.005699
Expl Pond Moy	-0.422810	0.056919	0.780587	1.000000	0.988417	-0.882515	-0.824097	-0.328261	-0.215145	0.070659
Imp Pond Moy	-0.381641	0.040454	0.699929	0.988417	1.000000	-0.848718	-0.816274	-0.311615	-0.191988	0.048395
Couv Max	0.664477	0.142789	-0.789331	-0.882515	-0.848718	1.000000	0.729086	0.590160	0.488731	-0.412159
Couv Moy	0.124158	-0.348206	-0.809840	-0.824097	-0.816274	0.729086	1.000000	0.081311	0.198802	0.203526
Nb Occ	0.855452	0.654556	-0.152894	-0.328261	-0.311615	0.590160	0.081311	1.000000	0.612461	-0.894459
Nb CVE	0.562603	0.279834	-0.220747	-0.215145	-0.191988	0.488731	0.198802	0.612461	1.000000	-0.583779

Ce processus de classement est expliqué en détail sur le site de OWASP(cf references).

CWES Interessant:

Le CWE sur lequel l'on va se concentrer dans la suite de ce rapport est le CWE-327: Broken or Risky Crypto Algorithm. Ce dernier- nommé "Utilisation d'un algorithme cassé ou risqué" en français- est dangereux car un attaquant déterminé peut être en mesure de casser l'algorithme et de compromettre les données protégées.

Des techniques bien connues peuvent exister pour casser l'algorithme, et bon nombre d'algorithmes sont aujourd'hui considérés comme risqués car facilement cassables (Un des exemples les plus connus étant l'algorithme de César).
Cf. liens dans les références pour plus d'informations.

Références

- A02-2021 Défaillances cryptographiques
https://owasp.org/Top10/fr/A02_2021-Cryptographic_Failures/

- CWE-327: Utilisation d'un algorithme cassé ou risqué
https://cwe.mitre.org/data/definitions/327.html

- Les algorithmes de cryptage cassé
https://www.securiteinfo.com/cryptographie/cracked.shtml#:~:text=Cet%20algorithme%20est%20asym%C3%A9trique.,moins%20un%20multiple%20du%20nombre.

- Les techniques de cryptographie
http://deptinfo.cnam.fr/Enseignement/DESS/surete/securite/courcry.pdf

- Page d'accueil OWASP

https://owasp.org/Top10/fr/