Travail pratique #04

Objectifs

1. Rechercher de l'information sur un type de faille répandue dans les applications web
2. À partir des informations trouvées sur une faille, être en mesure de la reproduire dans un contexte réaliste d'exploitation
3. Comprendre comment se protéger des failles les plus communes dans les applications web
4. Présenter les résultats d'une recherche devant un groupe

Instructions

Ce travail est à réaliser en équipe de 2 ou 3 étudiants. Ceux qui n'auront pas d'équipe seront placés ensemble de façon aléatoire pour former des équipes.

Chaque équipe doit choisir une des failles web les plus répandues selon OWASP (voir la liste complète ci-dessous) et en faire un sujet de recherche qui sera ensuite présenté devant la classe.

Consignes :

1. Vous devez faire un document power point (ou autre logiciel de présentation équivalent ou meilleur) d'au minimum 10 slides comme support de présentation en classe
2. La première page de vos slides doit contenir le nom de votre faille ainsi que le nom de chacuns des cooéquipiers. La dernière doit contenir vos références.
3. Votre présentation doit durer 15 minutes par équipe (minimum 15, maximum 20) et chaque membre doit participer de façon équivalente.
4. Vous devez faire une démonstration "live" de votre faille devant la classe.

5. Pour la démonstration de votre faille, vous pouvez construire vous-même un environnement qui vous permet de reproduire votre faille si vous le désirez, mais assurez-vous que ce soit réaliste. Si vous choisissez de prendre un site web existant, il est de votre devoir de vous assurer de le faire en toute légalité et d'avoir obtenu les autorisations nécessaires.
6. Vous devez expliquer comment il est possible de se protéger de votre faille et donner un exemple
7. Un même sujet ne peut être choisi par plus d'une équipe, premier arrivé premier servi. Pour réserver votre sujet, vous devez annoncer publiquement sur le channel tp04 du serveur discord du cours 2 choses : votre nom et celui de vos cooéquipier, et le sujet choisi.

Liste des failles :

1. Broken Access Control
2. Cryptographic Failures
3. Injection
4. Insecure Design
5. Security Misconfiguration
6. Vulnerable and Outdated Components
7. Identification and Authentication Failures
8. Software and Data Integrity Failures
9. Security Logging and Monitoring Failures
10. Server Side Request Forgery (SSRF)

De plus, les sujets suivants provenant de la version précédente (2017) du classement OWASP sont pertinents et acceptés :

1. XML External Entities (XXE)
2. Cross-Site Scripting (XSS)
3. Insecure Deserialization

Vous pouvez aussi choisir le sujet suivant de l'édition 2013 du classement OWASP :

1. Cross-Site Request Forgery (CSRF)

Vous pouvez vous servir du site de OWASP comme point de départ pour vos recherches, mais n'hésitez pas à consulter d'autres ressources en ligne pour être certain de bien maîtriser votre sujet.

Vous serez évalués sur la qualité de votre recherche et des informations présentées, la véracité des faits présentés, la qualité de la présentation en classe ainsi que la pertinence de la démonstration de votre faille.

Vous serez évalués par vos pairs lors de votre présentation devant la classe.

Soyez attentif aux présentations de vos collègues, vous êtes invités à prendre des notes car les informations présentées pourront être évaluées ultérieurement.

Références

1. Site de OWASP, documentation du top 10 des failles : https://owasp.org/Top10/

Remise

Avant la fin du cours d'aujourd'hui : votre équipe et votre sujet.

Votre document de présentation doit être remis avant le début du cours dans lequel les présentation auront lieu.

Veuillez vous référer à Vortex pour la date exacte.