OWASP

1. Qu’est-ce que OWASP ?

OWASP (Open Web Application Security Project) est une communauté en ligne ouverte et libre travaillant sur la sécurité des applications Web. OWASP se propose de permettre aux organisations de concevoir, développer, acquérir, exploiter et maintenir des applications logicielles fiables.  
OWASP est aujourd'hui reconnue dans le monde de la sécurité des systèmes d'information pour ses travaux et recommandations liées aux applications Web. Ces recommandations vont dans le sens de bonnes/mauvaises pratiques de développement, d’une base sérieuse en termes de statistiques, et d’un ensemble de ressources amenant à une base de réflexion sur la sécurité. Des outils sont aussi proposés pour effectuer des audits de sécurité.  
La Fondation OWASP, un organisme de bienfaisance à but non lucratif soutient les efforts de l'OWASP à travers le monde. Tous les outils, documents, forums et chapitres d'OWASP sont gratuits et ouverts à toute personne intéressée par l'amélioration de la sécurité des applications.  
OWASP est libre de toute pression commerciale et n'est affilié à aucune entreprise de technologie. Cela lui permet de fournir des informations objectives, pratiques et effectives sur la sécurité des applications.   
Les professionnels de la sécurité peuvent intégrer les recommandations d'OWASP dans leurs travaux. Les fournisseurs de service sécurité peuvent baser leurs produits et services sur les standards OWASP. Les consommateurs peuvent utiliser les normes comme documents de référence pour tester les applications ou les services qu'ils utilisent.

1. Dans quel contexte arrive OWASP ?

De nos jours, le développement de produits informatiques est fermement axé sur la vitesse. La course du Time-To-Market est extrêmement compétitive. Pour innover, les entreprises développent à un rythme effréné, en établissant des méthodologies qui permettent de perfectionner leur logiciel tout en réduisant le temps de développement. La sécurité, cependant, est souvent une réflexion secondaire pour les développeurs et les clients poussent toujours à livrer plus rapidement. Cela ouvre la porte à des failles de sécurité, de plus en plus présentes dans les logiciels. Et le Web n’échappe pas à cet état de fait.

De même, il est souvent difficile de trouver des conseils impartiaux, objectifs et des informations pratiques aidant à la prise en compte de la sécurité dans le développement. Le marché concurrentiel de la technologie et des services a beaucoup à dire sur ce point, mais une grande partie les conseils et recommandations sont donnés pour vous orienter vers un outil ou un fournisseur de services particulier.  
L'OWASP a été créé pour lutter contre ce problème, en offrant des conseils impartiaux et objectifs sur les meilleures pratiques et en encourageant la création de normes ouvertes.

1. Origines

OWASP a été créé par un certain Mark Curphey le 9 septembre 2001. Son but initial étatit de lancer un projet pour définir une méthodologie de test standard pour la sécurité des applications Web. Il continue de définir des recommandations de sécurité, des spécifications et des explications dans des domaines clés de la sécurité des applications Web.

Sa philosophie est d'être à la fois libre et ouverte à tous. Elle a pour vocation de publier des recommandations de sécurisation Web et de proposer aux internautes, administrateurs et entreprises des méthodes et outils de référence permettant de contrôler le niveau de sécurisation de ses applications Web.

1. Principes

Sur le site web officiel de l’OWASP, il est dit : “Nous préconisons une approche de la sécurité des applications en tant que problème de personnes, de processus et de technologie, car les approches les plus efficaces en matière de sécurité des applications incluent des améliorations dans tous ces domaines.  
Les Principes de l’OWASP sont:

* Gratuit et ouvert
* Régi par un consensus et un code de fonctionnement
* Respect d’un code d'éthique
* Sans but lucratif
* Non motivé par des intérêts commerciaux
* Approche fondée sur le risque

1. Projets

Tous les projets OWASP d'outils, de documents et de bibliothèques de codes sont organisés dans les catégories suivantes:

* Projets phares:

La désignation OWASP Flagship est attribuée aux projets qui ont démontré leur valeur stratégique pour l’OWASP et la sécurité des applications dans son ensemble.

* Projets de laboratoire:

Les projets OWASP Labs représentent des projets qui ont produit un livrable de valeur révisé par l’OWASP.

* Projets d'incubation:

Les projets OWASP Incubators représentent les projets qui sont encore en cours d'élaboration, avec des idées et dont le développement sont toujours en cours.

Les projets d'OWASP couvrent de nombreux aspects de la sécurité des applications. Elles concernent des documents, des outils, des environnements d'enseignement, des lignes directrices, des listes de vérification et d'autres documents pour aider les organisations à améliorer leur capacité à produire du code sécurisé. Les projets sont l'une des principales méthodes par lesquelles OWASP s'efforce de réaliser sa mission, qui est de rendre la sécurité plus « visible ».

Comme avec les groupes OWASP, les projets OWASP sont animés par des bénévoles et sont ouverts à tous. Cela signifie que n'importe qui peut diriger un projet, que n'importe qui peut contribuer à un projet et que n'importe qui peut utiliser un projet.

Voici une liste (non exhaustive) de projets populaires, ainsi qu’une description succincte :

* Webscarab :

Un outil d’audit de sécurité. Il s’agit d’un proxy disposant d’une interface graphique qui, une fois relié à un navigateur, intercepte les requêtes/réponses HTTP entre le client et le serveur, ce qui permet de les analyser, de forger des requêtes soi-même, de tenter différentes injections, etc… Le proxy est intercalé entre le client et le serveur à la façon d’une attaque « Man in the middle ». Webscarab dispose de nombreux plugins permettant d’augmenter le nombre de fonctionnalités offert par l’outil (WebServices, Spider, XSS/CRLF, SessionID Analysis, etc…). L’intérêt de cette solution : avoir un outil qui facilite un audit applicatif. Ce logiciel ne permettra pas d’avoir une application ayant une sécurité élevée s’il est utilisé seul. D’autres tests seront à faire pour accroitre la sécurité de votre application.

* Webgoat :

Il s’agit cette fois d’une application web volontairement non sécurisée. Elle est livrée avec un tutoriel et des exercices pratiques. L’OWASP met en avant l’aspect pédagogique de ces solutions, ayant pour but d’instruire l’intéressé sur les différentes techniques d’exploitation de vulnérabilités. L’intérêt est de former le développeur à produire un code sûr.

* Owasp Testing Guide :

Il s'agit d'un document de plusieurs centaines de pages destiné à aider une personne à évaluer le niveau de sécurité d'une application Web.

* Owasp code Review Guide :

Il s'agit d'un document de plusieurs centaines de pages présentant une méthode de revue de code sécurité.

* Owasp Application Security Verification Standard :

Le projet ASVS vise à créer un ensemble de normes commerciales permettant d'effectuer une vérification de sécurité rigoureuse d’une application au niveau applicatif.

* Top 10 :

Il s’agit d’un document de sensibilisation à la sécurité des applications Web. La liste résulte d’un consensus entre les experts en sécurité leaders dans le domaine, concernant les dix failles de sécurité les plus critiques pour les applications Web. Le classement de ces failles de sécurité est basé sur leur fréquence, la gravité des vulnérabilités et l'ampleur de leur impact commercial potentiel. Le Top 10 de l’OWASP a pour but d’informer sur l’existence de ces risques et de fournir des guides simplifiés sur les bonnes pratiques pour s’en prémunir. L’OWASP maintient le Top 10 depuis 2003. Il a été créé à l'origine pour aider les organisations à établir une base, un point de départ leur permettant de déterminer si leur infrastructure de sécurité est prête à résister aux principales menaces. La liste continue de servir de liste de contrôle et de standard de développement d'applications Web pour plusieurs des plus grandes organisations du monde.

La liste est mise à jour tous les trois ou quatre ans pour suivre le rythme des changements qui se produisent sur le marché de la sécurité des applications Web. La version la plus récente a été publiée en 2017. Celle-ci, contrairement à celles précédentes, n’est plus uniquement basé sur la « vision » de l’OWASP sur le sujet. Le processus méthodologique a été entièrement revu. Il repose ainsi sur les remontées de 500 utilisateurs et de 40 sociétés spécialisées dans le domaine de la sécurité des applications. La liste des contributeurs et les données techniques issues de leurs remontées sont disponibles en Open Source sur Github. En outre, les statistiques concernent un panel de plus de 100 000 applications et services Web.

Cet ensemble de vulnérabilités d'application Web largement accepté est complété par un ensemble de directives de codage et de test sécurisés. Ces guides sont disponibles sur le site de l'OWASP et s'adressent aux développeurs, architectes, chefs de projets, managers ...

Evaluer la sécurité d’une application Web en se basant sur le Top 10 de l’OWASP est une pratiquement largement acceptée. De nombreuses organisations, notamment le Conseil des normes de sécurité PCI, l'Institut national des normes et technologies (NIST) et la Commission Fédérale du Commerce (FTC), citent régulièrement le Top 10 d'OWASP comme un guide de référence intégral pour atténuer les vulnérabilités des applications Web et respecter les principales normes de sécurité.

1. Qu’est ce que le Top 10 règle-t-il ?

Les auditeurs considèrent souvent l'échec d'une organisation à prendre en compte le Top 10 d'OWASP comme une indication que l’organisation n’accorde pas une grande importance à la sécurité. L'intégration du Top 10 dans le cycle de développement logiciel témoigne d'un engagement pour de meilleures pratiques du en matière de développement sécurisé.  
En effet, la plupart des attaques d'applications Web ne sont pas considérées comme difficiles. Les pirates profitent de vulnérabilités dont les experts sont conscients depuis des années. Des failles telles que le Cross Site Scripting (XSS) et l'injection SQL apparaissent dans le Top 10. Une seule de ces vulnérabilités peut être utilisée à maintes reprises par les pirates en tant que vecteur d'attaque.  
Il est également important de noter que le Top 10 d'OWASP n'est pas orientée conformité. Au contraire, c'est une liste de choses qui pourraient mal tourner. Les organisations qui cherchent à utiliser cette liste pourraient l'intégrer dans les programmes de formation des développeurs. Cela garantit que les développeurs comprennent comment corriger ces 10 vulnérabilités spécifiques. Après tout, les équipes de sécurité utilisent souvent le Top 10 comme liste de contrôle lors de l'évaluation des vulnérabilités. De plus, de nombreux scanners de vulnérabilités automatisés permettent le scan et la génération de rapports en se basant sur cette liste.

1. Est-ce que top 10 seulement ?

Le Top 10 d'OWASP identifie les 10 failles de sécurité les plus fréquentes qui menacent la sécurité des applications Web. Ce n'est pas une liste complète de tous les problèmes de sécurité des applications Web. Dans l'ensemble, le Top 10 offre un aperçu des problèmes qui affectent la sécurité des applications Web. Mais, même si l’on parvient à éradiquer ces dix failles, si l’on se limite qu’à ce Top 10, il y a de fortes chances que l’application en question soit encore très vulnérable. Sur ce point de vue, l’OWASP a la même position.  
C'est une bonne pratique de conduire un modèle des menaces ou une analyse des risques de l'application avant qu'elle ne soit implémentée.   
Une autre bonne pratique consiste à évaluer l'application à mesure qu'elle est implémentée en utilisant des techniques d'analyse de code sécurisé.  
Une fois l'application en place, un test approfondi de pénétration est une autre façon de détecter les failles autres que celles présentes dans le Top 10. Les tests de pénétration permettent une investigation plus approfondie de l'application Web pour trouver les vulnérabilités qui ne figurent pas dans la liste.

1. Démarches concurrentes

Owasp Top 10 n’est pas la seule liste de vulnérabilités existante en matière de sécurité, comme dit plus haut, il y a aussi, parmi les plus populaires :

* La liste CWE :

Le Common Weakness Enumeration (CWE) est une liste de vulnérabilités que l’on retrouve lors du développement d’applications. C'est un projet géré par MITRE. Pour chaque entrée, le CWE fournit une description de la vulnérabilité ainsi que les étapes pour y remédier.  
Cependant, contrairement aux Top 10 d’OWASP qui recense les 10 vulnérabilités les plus critiques, le CWE se veut être une démarche plus globale. Au moment ou nous écrivons ces lignes, 714 vulnérabilités sont recensées sur la liste CWE. Elle peut constituer une suite à la gestion de la sécurité pour une organisation après que celle-ci ait pris en compte le Top 10. Cette liste est disponible sur le lien suivant : cwe.mitre.org.

* Le CWE/Sans Top 25

MITRE s'est associé à Sans Institute pour développer le CWE/Sans Top 25, une liste des 25 vulnérabilités logicielles les plus critiques. Bien que le Top 10 Owasp et le CWE / 25 e OWASP soient différents, ils partagent la plupart des mêmes vulnérabilités. En effet, là où le Top 10 adresse les failles en faisant une approche groupée, le CWE/Sans Top 25 utilise une approche plus granulaire. Par exemple, la correspondance Owasp Top 10 – CWE/Sans Top 25 peut être faite sur le point A1 : Injection

|  |  |
| --- | --- |
| Owasp Top 10 | CWE/Sans Top 25 |
| A1: Injection | * CWE-78: Improper Neutralization of Special Elements Used in an OS Command (‘OS Command Injection’) * CWE-89: SQL Injection * CWE-94: Code Injection * CWE-434: Unrestricted Upload of File with Dangerous Type * CWE-494: Download of Code Without Integrity Check * CWE-829: Inclusion of Functionality from Untrusted Control Sphere |

Cette correspondance peut être faite pour toutes les entrées du Top 10 d’Owasp.

* La WASC Threat Classification

1. Training sur owasp

OWASP fournit de nombreuses ressources permettant d’améliorer les connaissances et compétences dans le domaine de la sécurité des applications Web. Ces ressources sont gratuites et disponibles en ligne. Nous avons notamment :

* l’OWASP Online Academy :

L’OWASP Online Academy OWASP offre une formation en ligne gratuite sur la sécurité des applications Web, des tests de sécurité Web et Mobile, le codage sécurisé conçue et fournie par des experts en sécuirté du monde entier. Actuellement, le site web du projet OWASP online academy est en phase de test Alpha. L’OWASP Online Academy est basé sur l’Hackademic Project. Cette plateforme est créée pour être interactive. choose and finish your own course, pass a self-assessment exam and receive a Certification of Course Completion from OWASP Online Academy.

L'Académie en ligne et l'apprentissage de la sécurité des applications Web, des tests mobiles et du codage sécurisé conçus et fournis par des experts du monde entier.. OWASP Online Academy est basé sur le projet Hackademic. Nous créons cette plate-forme pour la rendre plus interactive, choisissez et terminez votre propre cours, passez un examen d'auto-évaluation et recevez une certification de fin de cours de la OWASP Online Academy

* l’OWASP Hacking Lab

Hacking-Lab is an online ethical hacking, computer network and security challenge platform, dedicated to finding and educating cyber security talents. Furthermore, Hacking-Lab is providing the CTF and mission style challenges for the OWASP University Challenges and for the European Cyber Security Challenge. The Hacking-Lab also provides free OWASP TOP 10 online security labs. Hacking-Labs’ goal is to raise awareness towards increased education and ethics in information security through a series of cyber competitions that encompass forensics, cryptography, reverse-engineering, ethical hacking and defense.

OWASP Hacking Lab is providing free remote security (web) challenges and riddles (OWASP TOP 10, OWASP WebGoat, OWASP Hackademics). It differs from other damn vulnerable applications and sites with it's unique teacher application. Every challenge is asking for the vulnerability, exploit and mitigation. Send in your solution and other OWASP volunteers will grade your submission. A system where you can interact with human beings.

OWASP Hacking Lab is free to use. It is licensed under the http://creativecommons.org/licenses/by-sa/3.0/ Creative Commons Attribution-ShareAlike 3.0 license], so you can copy, distribute and transmit the work, and you can adapt it, and use it commercially, but all provided that you attribute the work and if you alter, transform, or build upon this work, you may distribute the resulting work only under the same or similar license to this one.

* Cours gratuits

Des cours sont offerts gratuitement sur le site Web de l’OWASP à quiconque s'intéresse à la sécurité des applications Web. Ces cours sont accompagnés des liens et logiciels qu’ils requièrent. De plus, ces cours sont disponibles en format éditable et sous une licence open source et l’OWASP encourage à les utiliser pour ses propres formations et ainsi apporter sa pierre à l’édifice.

1. outils permettant d evaluer la conformite owasp en prendre quelques uns et expliquer (on en reparlera a l evaluation du framework a developper)
2. owasp quels frameworks qui implementent owasp : sur jee, sur .Net par exemple, sur php
3. Conclusion

Le guide OWASP regorge d’informations utiles pour tout niveau de compétence. Le développeur non initié au domaine de la sécurité verra cet univers démystifié, l’expert y verra une base de connaissances sur laquelle il pourra se reposer. Les outils proposés sont efficaces même si certains ne sont pas assez maintenus ou accumulent un retard par rapport à d’autres solutions Open-source. L’OWASP reste toutefois un référentiel soutenu par le milieu professionnel et amène à une réflexion intellectuelle sur le domaine de la sécurité, auquel chaque développeur devrait être sensibilisé.

Sécurité de l’information

1. Pourquoi sécuriser ?
2. Que faut il securiser ?
3. De qui ?
4. Menaces et Vulnerabilites
5. qu est ce qui a amene les gens a prendre en compte les problemes de securite et quand ont commence a etre pris en compte et comment ca se faisaitwx et Quelles organisations etaient en place