# **Compte Rendu du Projet de Sécurité Informatique**

Présenté par CONDE MAMADY LAMINE Etudiant en 3LFIAG (fsjegj)

## Thèmes

## Hackers ?

## L’API ?

## OWASP Mobile Security Project (Le projet OWASP de sécurité mobile) ?

## Quelle sont les organisations qui ont adoptées OWASP dans leurs référentiels ?

* **Hackers**

## Qu’est-ce qu’un hacker ?

Le terme **Hacker** est issu du verbe anglais**To Hack** qui signifie “découper quelque chose”. Il fait l’analogie avec la décomposition des étapes en plusieurs parties afin de **Qu’est-ce qu’un hacker ?**

Le terme **Hacker** est issu du verbe anglais**To Hack** qui signifie “découper quelque chose”. Il fait l’analogie avec la décomposition des étapes en plusieurs parties afin de les réassembler pour en faire éventuellement quelque chose de nouveau, de plus performant.

On emploi également les termes **bidouiller** ou **bricoler**. Le hacker est donc avant tout un bidouilleur si on fait l’abstraction de tout but qu’il peut chercher à atteindre.

Il cherche simplement à **améliorer son mode de vie** ou à atteindre divers buts en bidouillant quelque chose pour arriver à ses fins.

Le hacker au sens informatique est donc une personne qui cherche à connaître le fonctionnement détaillé d’un système partant à la recherche de petites combines qu’il juge pratiques et qui permettent de créer quelque chose de différent et/ou de **meilleur.** Il **détourne** donc un système ou réseau de son but initial.

Une autre définition :

[*« Un hacker est une personne qui cherche à comprendre le fonctionnement d'un système »*](https://twitter.com/intent/tweet?url=https://wp.me/p3kbYw-e&text=Un%20hacker%20est%20une%20personne%20qui%20cherche%20%C3%A0%20comprendre%20le%20fonctionnement%20d%27un%20syst%C3%A8me&via=LeBlogDuHacker&related=LeBlogDuHacker)

Ce détournement peut être tout à fait **légal** et utile, sachez par exemple que beaucoup d’inventions et de systèmes que vous utilisez aujourd’hui viennent du travail des hackers.

Vous pensez peut-être que les hackers ont contribué à certains sites ou à certaines technologies mais c’est encore mieux que cela, les hackers ont créé Internet, ils ont créé les **premiers** ordinateurs, ils ont inventé les interfaces **graphiques**, ils ont créé les systèmes d’exploitation Unix/[*Linux*](https://www.leblogduhacker.fr/produit/debuter-avec-linux/) et bien d’autres !

Mais comme vous vous en doutez, ce détournement peut aussi être **illégal** : typiquement il s’agit d’exploiter des bugs ou des faiblesses pour gagner l’accès à une machine. Et c’est probablement la définition la plus populaire de ce terme. Malheureusement, on a du mal à remettre de l’ordre dans ces définitions… Le terme en est devenu presque marketing, l’idée est surtout de bien comprendre qu’il y a deux significations derrières le terme hacker.

Hacker malveillant (black-hat), bienveillant (white-hat), script-kiddy (débutant)…etc. Autant de types de hackers qui sont décrits à la suite.

* **Les types de hacker :**

## Le gentil, le White Hat Hacker (le hacker au chapeau blanc) :

Il s’agit souvent d’une personne qui a atteint une maturité d’esprit ainsi que des qualifications **suffisantes** et **approuvées** par les autres.

Il **aide** les victimes, il aide à **sécuriser** les systèmes et combat contre la cybercriminalité.

Il travaille typiquement dans une grande entreprise pour sécuriser les systèmes et réseaux, mais il peut très bien être un jeune **passionné** ayant appris sur le tas.

Avec le slogan : [*« Apprendre l'attaque pour mieux se défendre »*](https://twitter.com/intent/tweet?url=https://wp.me/p3kbYw-h&text=Apprendre%20l%27attaque%20pour%20mieux%20se%20d%C3%A9fendre&via=LeBlogDuHacker&related=LeBlogDuHacker)

1. **Le méchant, le Black Hat Hacker (le hacker au chapeau noir) :**

Le hacker au chapeau noir peut être aussi expérimenté que celui au chapeau blanc, voire plus. Mais il agit par contre à des fins qui lui sont propres, **et qui sont illégales**.

Il **vole** des données, **s’introduit** illégalement dans les systèmes ou encore **pirate** des comptes.

C’est là qu’intervient le mot “pirate”. Le hacker au chapeau noir ne devrait pas être appelé “hacker”. Il s’agit malheureusement de la définition qu’on trouve souvent dans les médias : le terme hacker est utilisé à tort pour parler du pirate.

On a aussi longtemps essayé d’utiliser le mot “cracker” pour faire référence à ce pirate, mais entre “hacker au chapeau noir”, “pirate” et “cracker”, on s’y perd !

1. **Le troisième type : Le Grey Hat Hacker (le hacker au chapeau gris) :**

Comme si ce n’était pas encore assez compliqué, il nous a fallu un troisième type de hackers.

Vous l’avez compris, c’est un **mélange** de White Hat et de Black Hat.

Ce hacker agit des fois pour la bonne cause, comme un White Hat le fait mais peut commettre de temps à autre des délits.

Il s’introduit par exemple **illégalement** dans un système afin d’en **prévenir** ensuite les responsables des failles qu’il aura trouvées. Son action est louable, mais tout de même illégale.

1. **Les autres sous-types de hackers :**

***Les hacktivistes*** (contraction de hacker et activiste) qui agissent pour une cause souvent **politique**.

Ils attaquent généralement des entreprises et non pas des utilisateurs particuliers. ***Les script-kiddies*** (les gamins qui utilisent les scripts) sont tous ces jeunes hommes qui loin d’avoir compris les grands principes du hacking et l’éthique du hacker, se servent des programmes tout faits pour causer des **dommages** qui peuvent êtres très gênants.

Ils se vantent aussi la plupart du temps en se faisant passer pour les **créateurs** des programmes qu’ils utilisent et ne sont donc pas appréciés dans les communautés.

*Le*[***hacker éthique***](https://www.leblogduhacker.fr/lethique-du-hacker/) est celui qui cherche à comprendre le fonctionnement des attaques pour s’en protéger [*« Apprendre l'attaque pour mieux se défendre »*](https://twitter.com/intent/tweet?url=https://wp.me/p3kbYw-h&text=Apprendre%20l%27attaque%20pour%20mieux%20se%20d%C3%A9fendre&via=LeBlogDuHacker&related=LeBlogDuHacker).

## Conclusion :

On a vu que les définitions sont nombreuses et parfois redondantes. Le terme “hacker” tout court est souvent utilisé pour désigner toutes ces personnes individuellement.

Si vous devez donc retenir quelque chose de cet article, c’est la chose suivante :

* Il y a les hackers qui causent des **dommages** (piratage, attaques, vols, etc…) : ils agissent de façon **illégale** et sont sévèrement punis par la loi (pas seulement en France).
* Il y a les hackers qui apprennent les attaques pour se **défendre** ou aider les autres à se défendre : ils agissent de façon **légale** d’où [*les hackers éthiques*](https://www.leblogduhacker.fr/lethique-du-hacker/)*.*
* **L’AIP** (Application Programming Interface) :

 L'API peut être résumée à une solution informatique qui permet à des applications de communiquer entre elles et de s'échanger mutuellement des services ou des données. Il s'agit en réalité d'un ensemble de fonctions qui facilitent, via un [***langage de programmation***](https://www.journaldunet.com/developpeur/langage-programmation/)***,*** l'accès aux services d'une application.

La première chose que fait une API, c’est qu’elle ***expose***, autrement dit, elle rend disponibles des fonctionnalités ou des données. Pour les utiliser, **la plupart des API requièrent une clé (API key)**, voire parfois deux. Cette clé permet à l’API  de vous identifier comme étant un utilisateur ayant les droits nécessaires pour se servir de l’API.

Cette question d’**authentification est cruciale** quand on parle d’API. Prenons un exemple concret : à l’agence Debord, lorsqu’un formulaire de contact est envoyé, cela envoie les données de ce contact à notre espace client. Cet espace client, nous l’avons conçu avec une API afin de permettre à d’autres applications (notre site web, en l’occurence) d’y enregistrer des données. Que se passerait-il si cet enregistrement n’était pas soumis à des règles de sécurité ? Eh bien, n’importe qui pourrait enregistrer n’importe quoi dans notre espace client. Dans notre cas, chaque envoi de données via l’API de l’espace client réclame une authentification. Ainsi cela permet de valider que les informations à enregistrer proviennent bien de notre [*site**internet*](https://www.agencedebord.com/site-internet/) et pas d’ailleurs.

## *Domaines d'application de l'API*

Dans le domaine d'internet, l'API permet aux développeurs de pouvoir utiliser un programme sans avoir à se soucier du fonctionnement complexe d'une application. Les API peuvent par exemple être utilisées pour déclencher des campagnes publicitaires d'e-mailing de façon automatique sans avoir à passer par la compréhension d'une telle application (c'est le cas avec l'API AdWords de Google, par exemple). On les retrouve aujourd'hui dans de nombreux logiciels, en particulier dans les systèmes d'exploitation, les serveurs d'applications, dans le monde du graphisme (OpenGL), dans les applications SaaS ([Office 365](https://www.journaldunet.com/web-tech/guide-de-l-entreprise-collaborative/1172834-office-365-sous-toutes-les-coutures/), [G Suite](https://www.journaldunet.com/solutions/dsi/1175187-google-apps-for-work/), [Salesforce](https://www.journaldunet.com/solutions/dsi/1182014-salesforce/)...), les bases de données, l'open data, etc.

## OWASP Mobile Security Project (Le projet OWASP de sécurité mobile) ?

## Nous allons les répartirent dans un tableau :

|  |
| --- |
| **OWASP Mobile Top 10 Risks** |
| M1: Faibles contrôles côté serveur |
| M2: Stockage de données non sécurisé |
| M3: Protection de couche de transport insuffisante |
| M4: Fuite de données involontaire |
| M5: Mauvaise autorisation et authentification |
| M6: Cryptographie cassée |
| M7 : Injection côté client |
| M8: Décisions de sécurité via des entrées non fiables |
| M9: Gestion de session incorrecte |
| M10: Manque de protections binaires |

## Quelle sont les organisations qui ont adoptées OWASP dans leurs référentiels ?

## *****– 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…).

## *****– Webgoat :*****

## Il s’agit cette fois d’une application web volontairement non sécurisée. Elle est livrée avec un tutoriel et des exercices pratiques. Une fois de plus, 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.