# Analyse Des Attaques Courantes Des Applications Web Et Quelques Bonnes Pratiques De Programmation

**BOKUNGU BOBOY Jacques**
**Assistant**
**ISP/Gemena**
**Domaine : Anglais et Informatique des Affaires**

**Résumé :***Conscients du fait que les applications web sont plus confrontées à des menaces(1) variées en raison de leur hébergement sur des serveurs distants et leur accessibilité via le réseau Internet, dans cet article, nous avons fait le choix de réfléchir sur les menaces courantes dont elles sont victimes et ce, en proposant quelques bonnes pratiques afin d'en garantir la sécurité. Parlant de ces attaques web courantes, force est de constater que le XSS, le DDoS, le DoS, l'ingénierie sociale et bien d'autres font partie des menaces existentielles des applications web. Loin de se contenter uniquement de citer ces attaques, nous avons pris soin de proposer quelques bonnes pratiques en programmation(2) web pouvant offrir une garantie de sécurité à nos applications et sites web.*
**Mots-clés : Cyberattaque, programmation**

**Abstract :** *Knowing the fact that web applications are confronted to various cyber-attacks because of their hosting in the furthest servers and their access which is made possible via Internet, in this article, we have chosen deepening our thoughts on the most frequent threats (attacks) that web applications are usually victims and we have also suggested some good practices in order to assure their security. Talking about these most frequent threats (attacks), let's notice that the above cyber-attacks are the top list: SQL injection, DoS, DDoS, social engineering etc. Beyond the fact that we have cited and fully presented these cyber-attacks, we have also recommended some best practices that web developers are supposed to use to secure their applications.*
**Keywords : cyber attack, programming**

## Introduction :

Les applications web avec leurs usages et fonctionnalités multivariés sont devenues des éléments majeurs de l'Internet ces dernières années au point que nombreux utilisateurs non avertis confondent les deux (le web de l'Internet). Ce fait est accentué par la complexification(3)des applications web et la généralisation de leurs services qui créent des difficultés lorsqu'il s'agit d'assurer leurs protections contre les cyberattaques à différents mobiles partant du préjudice financier à l'atteinte de la réputation, en passant par le vol des informations critiques et personnelles malgré une législation abondante en la matière.

Notant le fait que les applications web fonctionnent avec des bases de données qui contiennent des informations utiles au bon fonctionnement des organisations qui les ont créés, les cybercriminels choisissent d'attaquer prioritairement ces bases de données(4)hébergées sur

(1) Menaces : en informatique, ce concept désigne tout acte de l'homme susceptible de créer un dysfonctionnement ou un arrêt de service d'un système informatique. Il peut s'agir d'un virus, d'une attaque et bien d'autres.
(2)Programmation : en informatique, ce concept désigne le fait d'écrire un programme.
(3)ENISA, , 2020, p ??
(4)Base de données : ensemble de données structurées et enregistrés sur des supports électroniques en vue d'une consultation ultérieure.

des serveurs distants et rattachées en back-end des applications web aux fins de créer soit le dysfonctionnement ou carrément voler les informations des utilisateurs qui y sont stockées.

Au nombre des attaques les plus courantes, nous pouvons citer : les injections SQL, le XSS (Cross-Site Scripting), le XSRF (Cross-Site-Request Forgery), le DoS (Denied of Services), le DDoS (Distributed Denial of Service), le Trojan Horse…

Prenant en considération à leur juste valeur la recrudescence de ces attaques, nous avons choisi au cours de cette étude de les décrire et en fin proposer quelques astuces de programmation nécessaires qui permettront aux développeurs juniors de les contourner en dotant leurs applications web de la capacité d'auto-défense.

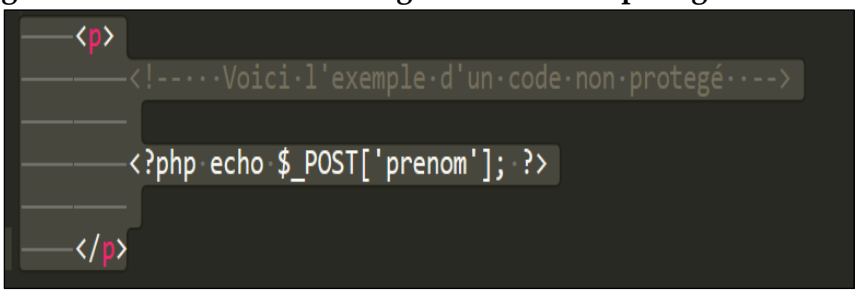
## I. Les Attaques Courantes des Applications et Sites Web :

Par menaces, nous faisons allusion aux attaques informatiques les courantes que rencontrent les applications et sites web lorsqu'ils sont déployés sur des serveurs distants. Ainsi, les lignes qui suivent nous présenteront certaines de ces menaces jugées plus récurrentes dans la vie des applications web.

### 1.1.Le XSS (Cross-Site-Scripting) :

Communément appelée faille XSS de son acronyme anglais (Cross-Scripting-Site)[5] est une faille de sécurité informatique spécialement pour les applications web dont le mode de nuisance consiste à injecter du code HTML ou JavaScript afin d'exécuter les codes d'un autre langage informatique (JavaScript le plus souvent) et la plupart de temps via un formulaire en ligne.
Sachant que les informations renseignées via un formulaire étant stockées dans les variables super globales $_POST en PHP et quand il (PHP) reçoit une variable au travers d'un formulaire, il place cette valeur à l'endroit où $_POST est appelé dans le code HTML.
L'image ci-dessous illustre l'échantillon des codes non-protégés qui peuvent facilement faire l'objet d'une faille de sécurité dite XSS.

**Figure n° 1. Illustration d'une ligne de code non protégé en PHP :**




### 1.2. L'Injection SQL :

L'injection SQL est une faille de sécurité qui consiste à injecter une requête SQL non prévue par le système et pouvant compromettre sa sécurité. Pour les sites web conçus avec le langage PHP, il est de notoriété publique que le PHP se charge de communiquer avec le SGBD

[5]Jacques BOKUNGU B. , *Mise en place d'une application web pour l'enregistrement des prisonniers,* Mémoire de fin de cycle, UNIKIN, 2021.

via une interface. En PHP5, c'est le plus souvent l'interface PDO (Personal Data Object) qui permet d'accéder à une base de données.

Pour éviter ce genre de menace, il est conseillé de ne pas écrire les codes tel que présenté dans l'image suivante en concaténant les variables.

**Figure n° 2. Illustration d'une requête SQL pour faire une intrusion à la BD.**

```
<?php

$reponse=$bdd->querry('SELECT nom FROM

jeux_video WHERE possesseur=\.$_GET['possesseur'].'\');


?>
```

### 1.3. Les Attaques XSRF :

Les attaques XSRF (Cross-Site Request Forgery) utilisent le navigateur d'un utilisateur pour envoyer des requêtes au serveur web. Ces requêtes paraitront donc tout à fait aux yeux du serveur et l'utilisateur réalisera donc des actions à son insu.

#### *1.3.1. Attaque par déni de service distribué :*

Une attaque par déni de service distribué (ou Dos pour Denial of Service) est un type d'attaque Dos qui a pour but de saturer un serveur web des requêtes pour le rendre indisponible.

De nos jours, on parle d'attaque DDoS (Distributed denial of Service) car ce type d'attaque est provoquée par plusieurs machines contre une seule cible. Les pirates construisent une armée des ordinateurs contrôlés à l'insu de son utilisateur par un pirate souvent grâce à un ver ou un cheval de Troie (trojan horse) pour attaquer leurs cibles.

Le principe est d'utiliser plusieurs esclaves pour l'attaque et des maitres qui les contrôlent. Le pirate communique directement avec les maitres via TCP, ensuite le maitre envoie des commandes aux esclaves via UDP ou encore l'attaque par réflexion (Smurf attack) qui est un flood via le protocole ICMP ou encore le Ping flood l'attaque la plus simple.

#### *1.3.2. L'Ingénierie sociale :*

L'ingénierie[6] sociale est une manipulation consistant à obtenir un bien ou une information, en exploitant la confiance, l'ignorance ou la crédulité des tierces personnes. Il n'est pas nécessaire d'avoir des connaissances approfondies en réseau et en informatique pour utiliser ce genre d'attaque. Il s'agit d'exploiter le facteur humain, qui peut être considéré dans certains cas comme un maillon faible de la sécurité du système d'information.

Les techniques employées rentrent toujours dans le domaine psychologique et social, le moyen de s'en protéger est de sensibiliser les utilisateurs sur ce genre d'attaque. Les entreprises établissent des consignes et une liste des règles à suivre pour éviter les fuites d'information sur leur parc informatique.

---

[6]Comprendre comment se protéger contre l'ingénierie sociale et autres cyber menaces les plus rependues sur la toile. *www.websecurity.com/Accueil/web-securiy-and-social-engineering*

## II. Les Attaques Web relevant de l'Ingénierie Sociale :

### 2.1. Le Phishing :

Le Phishing ou hameçonnage en français consiste à soutirer des renseignements personnels comme les mots de passe ou les numéros de carte de crédit en se faisant passer pour un tiers de confiance (banque, site connu, service de messagerie, etc.).

Au concret dans ce genre d'attaque, l'attaquant va présenter une interface utilisateur ressemblant à celle d'une organisation, site e-commerce ou application et vous demander de saisir vos informations personnelles qu'il va utiliser pour des fins nuisibles.

### 2.2. La Rogue :

Est un faux logiciel de protection qui prétend que votre ordinateur est infecté avec des fausses preuves à l'appui. Le plus souvent, la rogue se télécharge via une publicité en sur internet ou lors d'un téléchargement Peer to Peer. Généralement, il affiche une fenêtre disant que votre PC est infecté et qu'il vous faudra d'acheter un antivirus.

### 2.3. Le cheval de Troie (Trojan horse) :

Ça fait partie de l'ingénierie sociale. Dans ce type d'attaque[7], l'attaque planifie un acte de générosité tel qu'un logiciel gratuit à télécharger sur Internet alors qu'en réalité il s'agit d'un malware qui peut causer préjudice à l'utilisateur en volant des informations utiles.

### 2.4. Le Spyware :

C'est un logiciel espion que l'on rencontre généralement sur Internet. Ce petit logiciel dissimilé derrière le téléchargement effectué en ligne, peut causer des grands dommages à l'utilisateur en volant des informations sensibles et en les transmettant aux pirates informatiques auteurs de ce logiciel.

## III. Quelques Bonnes Pratiques en Programmation Web :

Analysant les causes de la vulnérabilité des applications web, notre étude nous révèle que les mauvaises pratiques liées à la programmation[8] sont en grande partie, la cause principale de la vulnérabilité constatée après audit de la plupart des applications web développées en RDC. Ayant identifié ce mode de développement, nous recommandons aux développeurs les bonnes pratiques suivantes :

### 3.1. Règle de développement :

Il est possible de se protéger de plusieurs attaques expliquées précédemment en suivant ces quelques règles de développement.

#### *3.1.1. Toutes les données doivent être vérifiées :*

---

[7] BRUCE SCHNEIER, « *Applied Cryptography* », traduit par « *Cryptographie appliquée* »

[8] Initiation à la programmation web pour débutants. Cours en ligne offert par Open class room, anciennement site du zéro. *www.open-classroom.fr/cours-de-programmation-web-pour-les-débutants*

Les valeurs saisies dans un formulaire doivent être validées au niveau du navigateur avec du code JavaScript[9], car le client n'est pas une source fiable. Les valeurs doivent également être contrôlées au niveau du serveur au moment de la récupération des paramètres, tout comme les paramètres de requête. Il n'est pas certain que ce soit l'utilisateur de l'application[10] qui envoie la requête http. Ainsi, pour chaque valeur :

- Vérifier que le type correspond à celui attendu ;
- Pour plus de sécurité, Caster les données avant de les mettre dans des variables ;
- Vérifier la présence de tous les arguments attendus ;
- Pour les nombres, contraindre la valeur entre deux bornes ;
- Pour les listes, vérifier que la valeur appartient à la liste des valeurs autorisées (select, radio, checkbox…);
- Coder les caractères spéciaux avec le code HTML correspondant ;
- Contraindre la valeur saisie avec une taille minimale ou une taille maximale ;
- Vérifier la valeur avec une expression régulière ;
- N'accepter que les lettres de l'alphabet et/ou les chiffres par défaut, pour les autres caractères devant être refusés. Dans le cas où d'autres caractères doivent être autorisés, ils doivent être limités à une liste prédéfinie ou être remplacés par les codes HTML ;
- Vérifier si la valeur nulle doit être acceptée ;
- Même les données envoyées vers l'utilisateur doivent être vérifiées, avec au minimum les actions suivantes :
- Coder les caractères spéciaux avec le HTML correspondant ;
- Définir le jeu de caractère de la page ;

### *3.1.2. Privilégier l'utilisation des requêtes POST :*

Cela permet de ne pas prendre en compte les paramètres frauduleux de dans les adresses. :

- Utilisation des fonctions de hachage lors de la programmation (Ex : **sha1()**);
- Le cryptage de informations sensibles tels que les mots de passe et les identifiants des utilisateurs (Ex : **htmlentities(), strip_tags())** ;
- Utilisation des requêtes préparées (comportant la fonction : Ex : **prepare**()) ;
- Sur le serveur Apache, mettre en place le firewall modsecurity ;
- Utiliser un navigateur mis à jour constamment ;
- Eviter de lire les mails provenant des sources inconnues ;
- Eviter de cliquer sur n'importe quel lien ;

## IV. Analyse des Résultats :

Comme nous l'avons relevé tantôt, l'utilisation accrue du web, par ricochet de l'internet a malheureusement permis la croissance non seulement des cyberattaques, mais aussi a asphalté le boulevard de la diversification des types d'attaques.

De ce point vue, les résultats d'une étude que nous avons conduite pour tester la sécurité des applications web développées en République Démocratique du Congo et pour la

---

[9]KUTANGILA MAYOYA D., *Notes de cours de programmation web*, UNIKIN, G2 Anglais et Informatique, 2017.

[10]MICHAEL HOWARD et DAVID LEBLANC, "*Writing Secure Code*", œuvre écrite sous le label OWAPS (Open Web Application Security Project).

plupart par des programmeurs autodidactes (sites d'informations en ligne, sites des institutions, pages web vitrine…) nous montrent que la plupart de ces application web sont vulnérables à plus de 67 %.

Cependant, grâce à la même étude, nous sommes parvenus à identifier la cause principale de la vulnérabilité collective des applications web développées en RDC, qui est due au manque des connaissances avancées en programmation informatique. Les développeurs des applications web, très souvent amateurs ou passionnés autodidactes de l'informatique, intéressés par l'unique intérêt de servir le client et recevoir de celui-ci en contrepartie de l'argent, se préoccupent moins aux questions liées à la sécurité de leurs applications oubliant que l'univers informatique dans lequel devront évoluer leurs applications web est plein de risques d'attaques tel que le tableau ci-dessous nous le démontre.

**Tableau n°1. Récapitulatif des attaques informatiques de grande ampleur selon la presse congolaise de 2019 à Octobre 2024.**

| N° | Sites ciblés | Victimes | Mobiles de l'attaque | Dommages subis | Année |
|---|---|---|---|---|---|
| 1 | *www.minesu.cd* | Ministère de l'enseignement supérieur | Créer le dysfonctionnement | Arrêt des activités | 2024 |
| 2 | *www.snl.cd* | La SNL | Créer le dysfonctionnement | Arrêt du Traffic sur le site | 2021 |
| 3 | *www.cenirdc.cd* | La CENI | Vol des données | Aucune | 2023 |
| 4 | *www.politioco.cd* | Média en ligne | Prendre le contrôle | Publication des fake news | 2023 |
| 5 | *www.7sur7.cd* | Media en ligne | Prendre le contrôle | Dysfonctionnement | 2022 |
| 6 | *www.actualites.cd* | Media en ligne | Salir les personnalités | Dysfonctionnement et arrêt des services | 2023 |

**Source : Données recueillies au ministère du numérique de la République Démocratique du Congo, Direction de la cyberdéfense.**

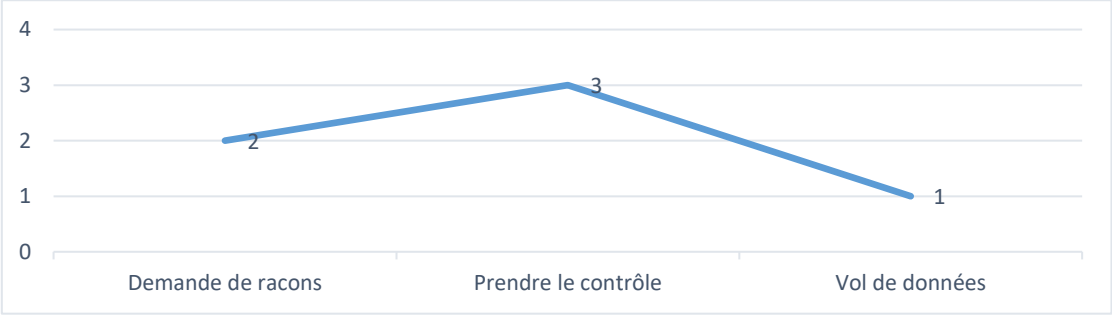
Explorant ce tableau n° 1, nous remarquons que les principaux sites web (applications) ciblés par les pirates informatiques sont les sites appartenant aux institutions publiques et à ce titre, le mobile des attaques demeure de générer le dysfonctionnement ou organiser le vol de données sensibles. Ainsi, les statistiques assorties de notre étude nous donnent les résultats présentés de la manière suivante :

**Figure n° 3: Représentation graphique des attaques informatiques d'ampleur de 2019 à Octobre 2024.**


**Source : Interprétation graphique du tableau N°1**

Plongeant dans la compréhension de ces graphiques, nous remarquons qu'au moins chaque année, il y a eu une attaque informatique de grande ampleur ciblant en grande partie, les sites web ou applications web appartenant aux entreprises publiques ou institutions de l'Etat. Cependant les objectifs de ces attaques diffèrent d'une application web à une autre comme les illustrent les graphiques ci-dessous.

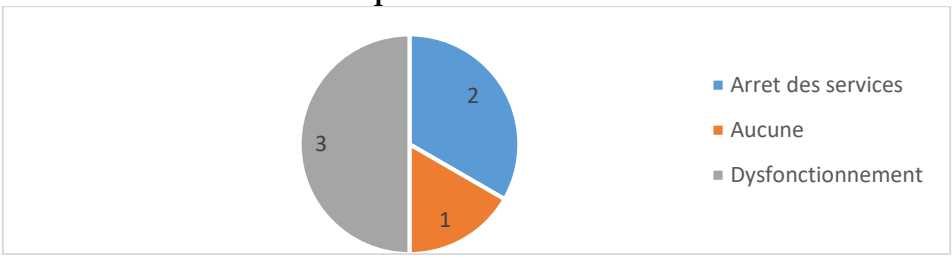
**Figure n° 4. Représentation graphique des mobiles des attaques informatiques de 2019-2024**




**Source : Interprétation graphique du tableau N°1**

Comme nous pouvons le réaliser, les attaques informatiques ont des différents mobiles. Certaines d'entre elles ont pour objectif de créer le dysfonctionnement, d'autres le vol de données, intenter à la réputation, prendre le contrôle de l'administration de l'application web et bien d'autres. Dans ce contexte, les graphiques ci-dessous nous montrent que 50% des attaques informatiques recensées de 2019 à Octobre 2024 en RDC avaient pour objectif de prendre le contrôle et plus de 30% avaient pour objectif la demande de rançon et 20 % pour le vol de données sensibles.

**Figure n° 5 Représentation graphique des dommages subis par les applications web attaquées de 2019 à 2024**




**Source : Interprétation graphique du tableau N°1**

La figure n°6 ci-dessus nous montrent que 50% des attaques informatiques emblématiques vécues en RDC de 2019 à Octobre 2024 ont causé comme dommages le dysfonctionnement des applications web ou sites concernés. Tandis que 30% de ces attaques ont causé comme dommage l'arrêt des services des applications et sites web concernés.

Nous basant sur les résultats de l'étude menée, nous sommes en droit d'affirmer que la plupart des sites web et applications qui sont victimes des attaques informatiques de 2019 à Octobre 2024 en République Démocratique du Congo appartiennent aux entreprises ou institutions publiques rattachées à l'Etat. Une autre lecture nous amène à comprendre que les médias en ligne sont la seconde victime des attaques informatiques en République Démocratique du Congo, et que les sites web appartenant aux particuliers ou petites organisations ne sont pas dans le collimateur des pirates informatiques en République Démocratique du Congo.

Toujours grâce à la même étude, notre attention a été portée sur le mobile des attaques et surtout les dommages subis par les sites (applications web) qui ont fait l'objet des attaques informatiques durant cette période partant de 2019 à Octobre 2024. A ce point, nous avons constaté que le mobile de ces attaquants était pour la plupart encouragé par l'envie de prendre

le contrôle de ces sites (applications) web, suivi d'une tendance de vol de données et en fin la demande des rançons.

Quant aux dommages subis par les sites qui ont fait l'objet des attaques informatiques, nos investigations nous attestent que le dommage le plus percutant subi est l'arrêt des services des sites web attaqués, suivi du dysfonctionnement et que d'autres sites ont été invulnérable aux nombreuses attaques subies, c'est le cas du site de la CENI RDC.[11]

## V. Conclusion et perspectives :

En résumé, dans le présent article, il a été question de sensibiliser sur les attaques web les plus récurrentes (injection SQL, l'ingénierie sociale, le DoS, le XSS) et par la suite, proposer quelques bonnes pratiques qui puissent permettre de s'en protéger. Dans le développement de la présente étude, nous avons identifié les principales attaques auxquelles les applications web en sont fréquemment victimes et avons énuméré quelques attaques d'ampleur subies par les applications et sites web appartenant à des institutions publiques en RDC de 2019 à 2023. En outre, nous avons proposé quelques bonnes pratiques de programmation partant du développement des applications web mieux, dès leur programmation, jusqu'à leur déploiement sur des serveurs distants et durant leur utilisation.

De surcroit, nous basant sur les résultats de notre étude, il en est ressorti qu'à eux seuls, les sites web institutionnels et les médias en ligne détiennent le plus grand record des applications web les plus susceptibles des attaques informatiques et partant de ce constat, nous avons insisté sur le fait que leur développement, mieux leur conception et réalisation devrait être l'apanage des programmeurs professionnels et expérimentés en programmation web en vue de prévenir les attaques informatiques éventuelles qui généralement mettent en péril le fonctionnement harmonieux des applications web.

### 5.1. Perspectives :

Conscients de la limite de nos recherches et surtout prenant en compte le fait que l'informatique est une science en évolution continue, nous nous rabattons sur l'apport d'autres chercheurs qui ont mené des investigations similaires aux nôtres afin que leurs contributions puissent apporter des éléments additionnels au présent article.

## Bibliographie :

### I. Ouvrages :


1) GUILLAUME HARRY, *Failles de sécurité des applications Web,* OWASP, 2012.
2) BRUCE SCHNEIER, « *Applied Cryptography* », traduit par « *Cryptographie appliquée* »
3) MICHAEL HOWARD et DAVID LEBLANC, "*Writing Secure Code*", œuvre écrite sous le *label OWAPS (Open Web Application Security Project)*


### II. Travaux :


4) Jacques BOKUNGU B., *Mise en place d'une application web pour l'enregistrement des prisonniers*, Mémoire de fin de cycle, UNIKIN, 2021.


(11) *www.ceni-rdc.cd*

5) KUTANGILA MAYOYA D., *Notes de cours de programmation web,* UNIKIN, G2 Anglais et Informatique, 2017.

**III. Webographie :**

6) Comprendre comment se protéger contre l'ingénierie sociale et autres cyber menaces les plus rependues sur la toile. *www.websecurity.com/Accueil/web-securiy-and-social-engineering* le 20/01/ 2025 .
7) Initiation à la programmation web pour débutants. Cours en ligne offert par Open class room, anciennement site du zéro. *www.open-classroom.fr/cours-de-programmation-web-pour-les-débutants*