STAGE 1ere année de Célia Baylet :

OKANTIS

2ème semaine du 3 au 7 juin 2024

03/06/2024

- J’ai commencé l'audit de l'application web.

- J'ai commencé les tests sur l'application. Je fais un rapport d'audit sur un document Word sur lequel je note au fur et à mesure les commentaires pour chaque point.

- Je note aussi sur le tableur Excel si les points sont bien respectés 'oui', ne le sont pas 'non', ou 'NA' (non applicable) lorsque je ne peux pas effectuer les tests. Par exemple, je mets ‘NA’ lorsque je ne peux pas avoir accès à l’authentification tant que l’application n’est pas mise en ligne.

- Sur la machine kali, pour me connecter à l'application je dois aussi modifier le fichier ‘hosts’. Donc j'utilise la même méthode que sur l'ordinateur Windows (action effectué jeudi 30). D’abord j’ai recherché le chemin pour modifier ce fichier sur une machine virtuelle kali.

Le chemin est '/etc/hosts' donc la commande pour modifier le fichier est 'sudo nano hosts' avant j'avais fait un 'cd /etc'.

- Pour tester la connectivité réseau j’ai fait un ‘ping 9.9.9.9’ (adresse qui est utilisée par le service DNS) et un ‘ping google.com’.

- J’ai installé l’application ‘zaproxy’, pour les flux TLS

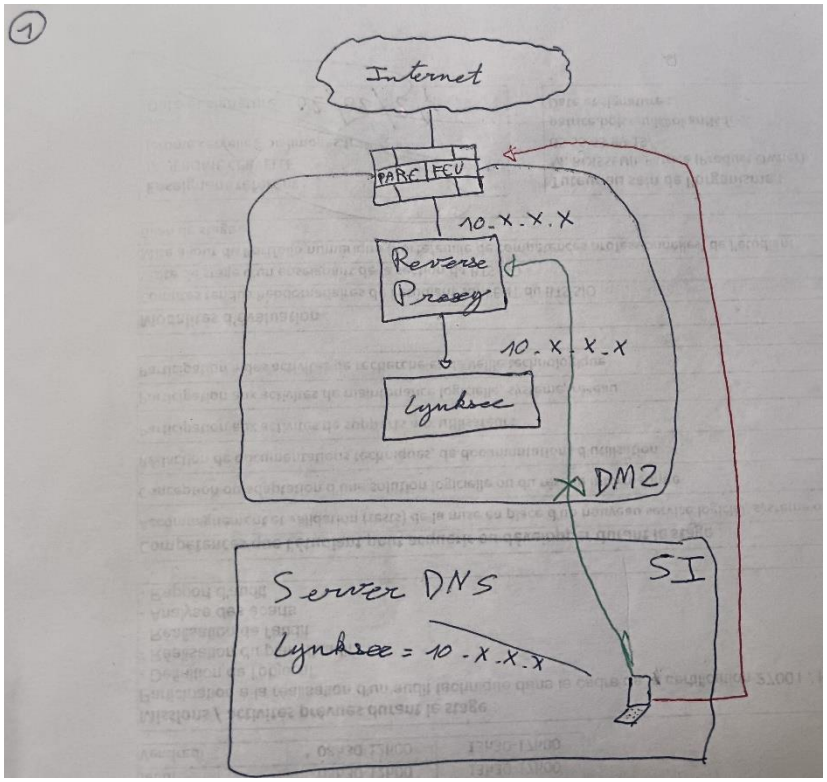
Zaproxy, lorsqu'il est utilisé comme serveur proxy, il permet à l'utilisateur de manipuler tout le trafic qui le traverse, y compris le trafic utilisant https. Ici, il joue le rôle du serveur TLS.

Zaproxy, enregistre toutes les requêtes effectuées.

-J’ai participé à une réunion de l’équipe sécurité, il y en a une chaque lundi.

(voir annexe 1 pour le vocabulaire et fiche technique)

Schéma :



04/06/2024

- Aujourd’hui j’ai avancé le rapport d'audit.

- Ange (alternant en master) m’a aidé un peu aujourd’hui pour l’audit. Il m'a fait découvrir 'Burpsuit' qui est déjà installé sur la kali. C'est un outil modulaire permettant de réaliser des tests (manuels et automatisés) qui vont aider à identifier efficacement des vulnérabilités sur les applications web.

- Ange m'a aidé à découvrir quelques vulnérabilités pour le rapport d'audit. J’en ai découvert certaines, presque par hasard, c’est intéressant.

-- Je dois rester discrète au sujet du rapport d’audit car ce document est confidentiel pour l’entreprise, je l’évoquerai assez superficiellement.

- Il m’a aussi fait installer 'wappalyzer' sur google qui est un utilitaire permettant ainsi de découvrir les technologies utilisées sur les sites Web

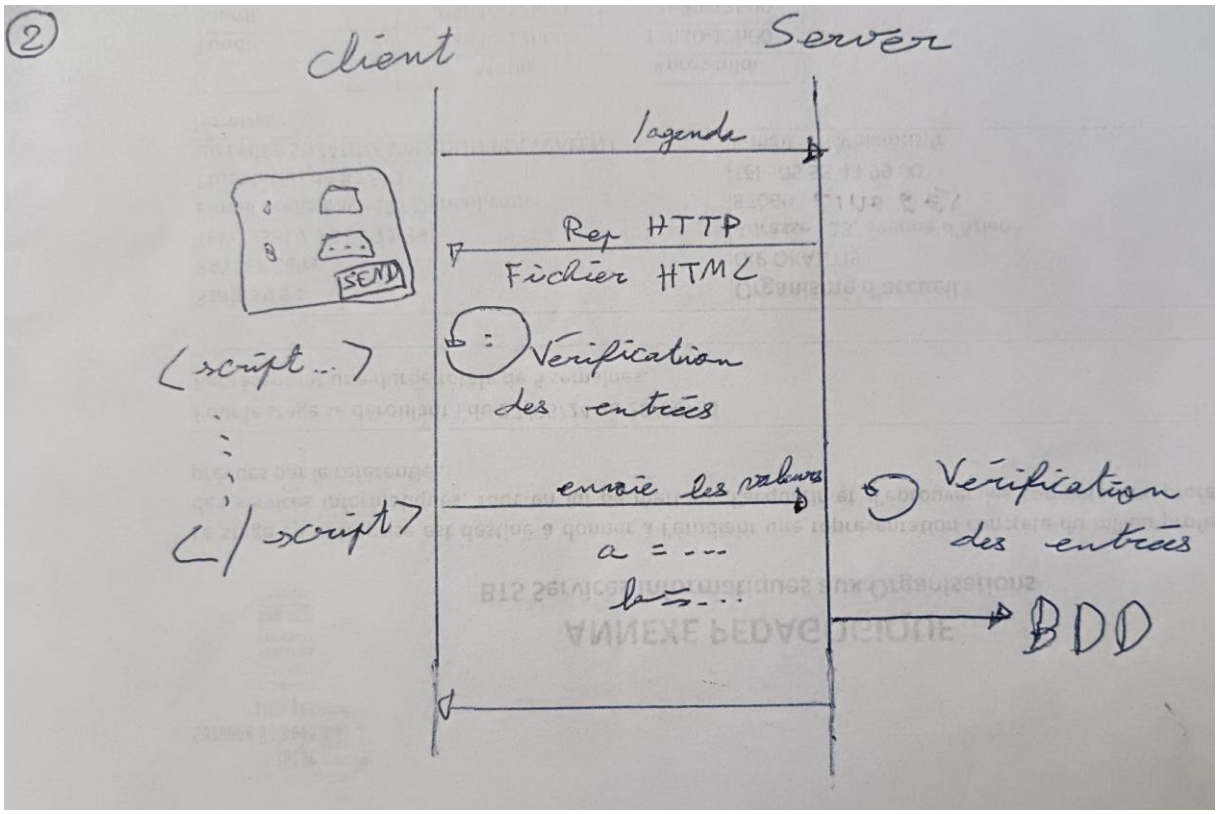
On peut tester sur le site : https://www.example.com/

(voir annexe 2)

05/06/2024

-Aujourd’hui j’ai avancé l’audit.

Schéma :



- Je devais chercher comment sont modifiés les caractères dangereux qui peuvent être injectés dans un champ, pour éviter une attaque.

L'encodage d’entités HTML est sûrement la mesure la plus essentielle car les scripts malveillants sont souvent injectés via des balises HTML. Ici, il s’agit donc d’encoder la plupart des entités HTML pouvant constituer un risque afin qu’elles soient interprétées comme des données fiables.

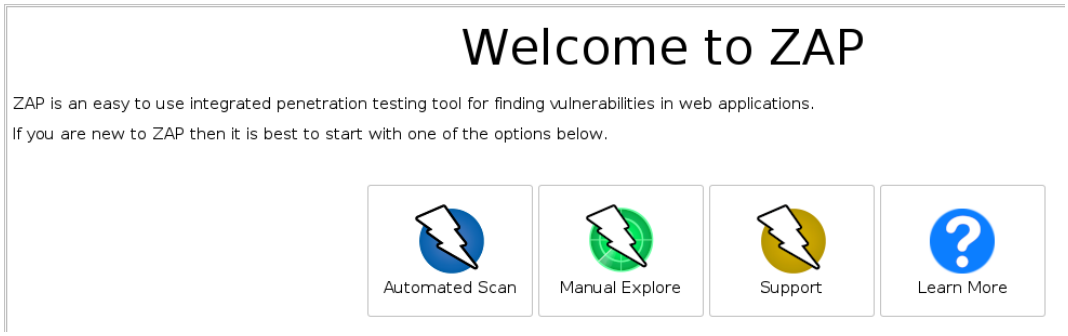
L'échappement des caractères dangereux est une pratique essentielle pour assurer la sécurité des applications web contre les attaques comme le XSS.

(voir annexe 3 pour la liste des caractères dangereux courants)

-J’ai utilisé ‘Zap’ pour explorer les CVE (c’est un dictionnaire des informations publiques relatives aux vulnérabilités de sécurité).

-J’ai utilisé cette commande sur ‘nmap’ : nmap --script vuln nom/du/site

-Avec zap on peut aussi faire des scan pour découvrir des éventuelles vulnérabilités (‘Automatic Scan’)



- Le site de décodage en base 64 a pu m’aider

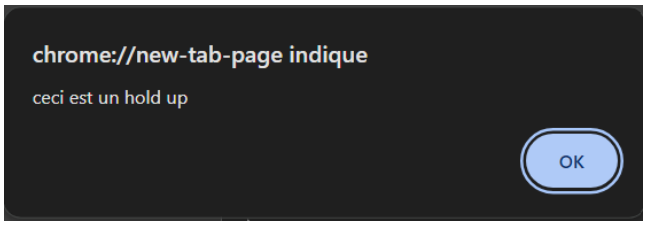
- Nous avons eu une réunion de l’escouade sécurité cet après-midi

- Depuis 3ans, ils font un quizz de sensibilisation à la sécurité pour les membres du personnel. Ils sont en réflexion pour changer de style de ‘jeux’ pour motiver les équipes.

<script>alert("ceci est un hold UP")</script>

Cette commande est utilisée dans les champs, en développement web pour afficher une boîte de dialogue (popup) avec un message à l'utilisateur. C’est une méthode courante pour tester les vulnérabilités XSS.

Pour tester j’ai fait inspecter la page, puis dans la console j’ai noté : alert("ceci est un hold UP"), un popup apparait.



-Pour finir la journée j’ai regardé un lien qui m’a été envoyé par Patrice Boisseuil, qui est un ‘jeu’ de cybersécurité. Des petites vidéos sont présentées, il faut choisir ce que l’on croit être la bonne réponse et le scénario se met en place petit à petit. C’est très intéressant.

https://targetedattacks.trendmicro.com/cyoa/fra/

(voir annexe 3)

06/06/2024

-J'ai avancé l'audit aujourd’hui.

-Ce matin, j’ai continué à rechercher des vulnérabilités avec l'outil : ‘testssl’ sur la kali linux.

J’ai tapé cette commande sur un terminal : testssl urlDuSite

-Une information à retenir d'un point de vue légal, c’est qu’on ne peut pas utiliser nmap sur n'importe quel site.

Nmap est un outil légal lorsqu'il est utilisé dans un cadre autorisé et éthique, tel que les tests de sécurité, la découverte de vulnérabilités, ou l'administration de réseaux. Il est important de respecter les lois et les politiques en vigueur, et d'obtenir les autorisations nécessaires avant de scanner des réseaux.

-J’ai utilisé cette commande : curl -v -X TRACE https...(url du site)

Le ‘-v’ permet d'ajouter beaucoup plus de précision à la commande

On cherche à savoir si «l’application accepte uniquement les méthodes http strictement requises et interdit la méthode trace».

- J'ai regardé aujourd'hui le guide de recommandations de sécurité relatives à TLS publié sur le site de l'ANSSI pour répondre à des points de cryptographie : 'anssi-guide-recommandations_de_securite_relatives_a_tls-v1.2.pdf'

- Nous avons parlé de la différence entre le hachage et le chiffrement, avec le hachage on ne peut pas revenir en arrière. Le chiffrement protège la confidentialité des données, les rendant lisibles uniquement par des parties autorisées, tandis que le hachage vérifie l'intégrité des données, garantissant qu'elles restent inchangées et non corrompues.

(voir annexe 4)

07/06/2024

- HTML et XML sont deux langages de balisage populaires dans le développement d'applications et le développement Web.

- Je fais un rapport d'audit, c'est à dire qu'il faut donner les erreurs qui apparaissent, comment on les a découvertes et proposer des solutions/recommandations.

- Les API (interface de programmation d'application) sont des mécanismes qui permettent à deux composants logiciels de communiquer entre eux, à l'aide d'un ensemble de définitions et de protocoles. Les attaques par injection se produisent lorsqu'un attaquant envoie des données malveillantes à une API, la trompant pour exécuter des commandes non prévues ou accéder à des données non autorisées.

J'ai utilisé les commandes :

tracert X.X.X.X(adresse ip) sur Windows

nslookup 'nom de domaine de l'appli'

pour voir si le serveur n'est pas directement accessible et si il y a des mécanismes de sécurité qui protège le serveur.

J'ai aussi utilisé 'nmap -sS' et 'nmap -T4' suivi du nom de domaine pour voir quels ports sont ouverts.

J'ai aussi rentré des fausses requêtes (modification du nom avec des chiffres par exemple, des lettres dans une date...) directement dans l'api pour voir les conséquences.

(voir annexe 5)

Annexe 1

Vocabulaire :

Escalade de répertoire : Procédure formelle qui consiste à demander l'intervention de ses supérieurs ou la collaboration de ressources spécialisées supplémentaires dans le traitement d'un dossier problématique.

CDN : Un réseau de diffusion de contenu (CDN) est un réseau de serveurs interconnectés qui accélère le chargement des pages Web pour les applications à forte densité de données.

TLS (Transport Layer Security) : est un protocole utilisé par les applications pour communiquer de manière sécurisée à travers un réseau, tout en prévenant la falsification et l'interception des courriels, navigations web, messageries et autres protocoles.

Gestionnaire de paquet : C'est un système ou un ensemble d'outils qui permet d'automatiser l'installation, la mise à niveau, la configuration et l'utilisation des logiciels.

Zaproxy : OWASP ZAP : est un outil de test de sécurité des applications web conçu pour aider les professionnels de la sécurité et les développeurs à identifier et à atténuer les vulnérabilités de sécurité des applications web pendant les phases de développement et de test.

AFNOR : L'Association française de normalisation est l'organisation française qui représente la France auprès de l'Organisation internationale de normalisation (ISO) et du Comité européen de normalisation (CEN).

Fiche technique :

-Pour faire un copier-coller sur machine virtuel :

contrôle + maj + C (ou V)

-Installation de ‘zaproxy’ sur la kali :

Sur un cmd j’ai tapé ces commandes :

apt update

apt upgrade

apt install zaproxy

Sous Linux, Debian est une distribution plus générale qui peut être utilisée pour de nombreux usages. Kali et Ubuntu sont des distributions basées sur Debian, donc en principe elles ont les mêmes commandes de base.

Kali est spécialement conçu pour la sécurité informatique.

Zaproxy fonctionnement :

-Passer en ‘Manual Explore’

-Clic droit sur le fichier que l’on souhaite analyer

-cliquer sur ‘Opend/Resend with Request Editor...’

- En haut à gauche on peut avoir accès aux requêtes et réponses. : Request Reponse

Avec zaproxy, il faut se reconnecter sur le navigateur (ayant une barre rouge et noir) au lien de l’application en développement. Il enregistre toutes les requetes effectuées, qu’on peut ensuite analysées.

Annexe 2

Vocabulaire :

LDAP (Lightweight Directory Access Protocol) : permet aux utilisateurs de trouver des données sur des entreprises, des personnes, etc. Ce protocole a deux objectifs principaux : stocker des données dans l'annuaire LDAP et authentifier les utilisateurs qui veulent y accéder.

API : En informatique, une interface de programmation d’application ou interface de programmation applicative, souvent désignée par le terme

API pour « application programming interface ». C'est une interface logicielle qui permet de « connecter » un logiciel ou un service à un autre logiciel ou service afin d'échanger des données et des fonctionnalités.

CVSS (Common Vulnerability Scoring System) :est un système permettant de calculer une note évaluant la criticité d'une vulnérabilité, et de construire une chaine de caractères (un vecteur) présentant les caractéristiques de cette vulnérabilité, et les critères utilisés pour ce calcul.

Fiche technique :

Sur la kali application : 'Burpsuit' pour l'utiliser il faut choisir -->Proxy --> Intercept -->'intercept is on' /'intercept is off' -->Forward (lorsque 'intercept' est sur 'on' pour faire passer les requêtes les unes après les autres.

J'ai entendu parler de 'Let's Encrypt' qui est une autorité de certification (Certificate Authority en anglais) gratuite, automatisée et ouverte, exploitée pour le bénéfice du public. C'est un service fourni par Internet Security Research Group (ISRG). --> Cette autorité n'est pas très conseillé.

Annexe 3

Vocabulaire :

Id de session : c'est avoir un identifiant de la connexion à la déconnexion. Si l'on va sur un autre navigateur, ou que l'on se reconnecte plus tard on doit avoir un autre identifiant (et de préférence non prédictible).

RSA : est une technique de chiffrement asymétrique qui utilise deux clés de chiffrement différentes mais liées (privées et publiques). Le chiffrement RSA utilise des clés opposées pour chiffrer et déchiffrer les données.

AES : L'Advanced Encryption Standard est un algorithme de chiffrement par blocs symétrique pour protéger les informations classifiées. Il est mis en œuvre dans les logiciels et le matériel dans le monde entier pour crypter les données sensibles.

Caractères dangereux courants :

< : échappé en &lt

> : échappé en &gt

& : échappé en &amp

" : échappé en &quot

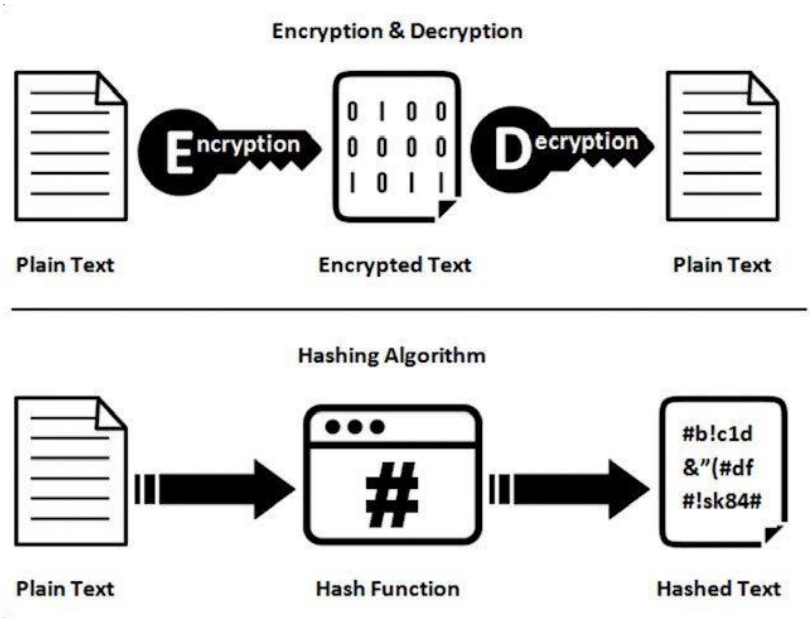
' : échappé en &#x27 (ou &apos dans certains cas)

/ : échappé en &#x2F (rare, mais utilisé dans certaines bibliothèques)

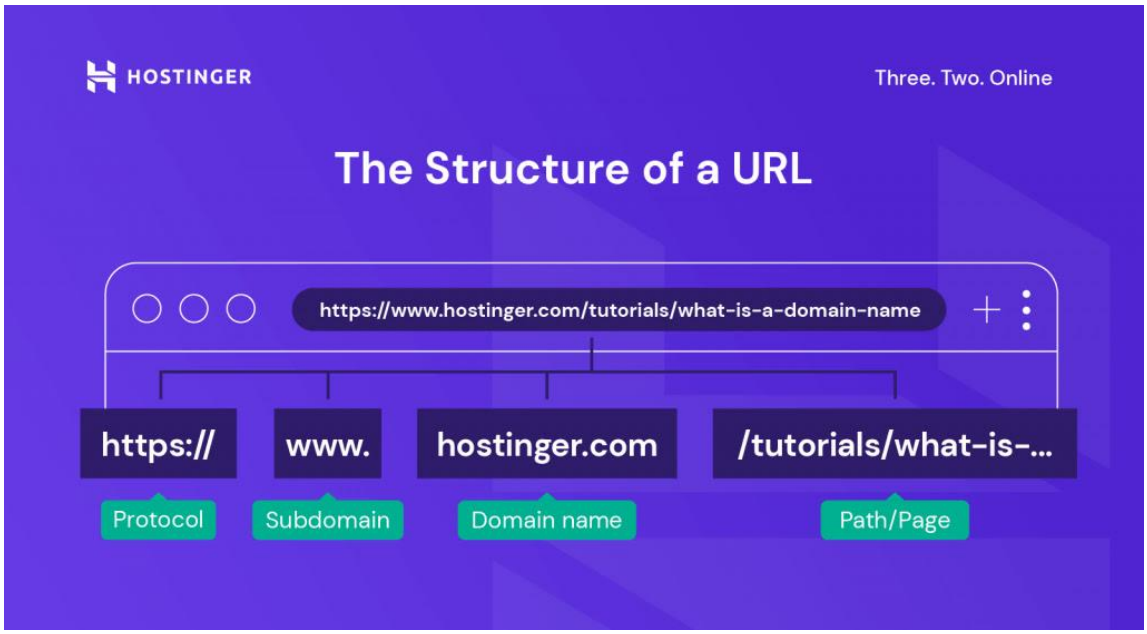
Source intéressante : https://www.vaadata.com/blog/fr/failles-xss-principes-types-dattaques-exploitations-et-bonnes-pratiques-securite/

Annexe 4

DTD : (Description de Type de Document) définit la structure d'un document, les éléments et attributs qui y sont autorisés, et le type de contenu ou d'attribut permis.



Annexe 5



Passer en root et définir le mdp :

```
┌──(utilisateur1㉿kali)-[~]
└─$ sudo passwd root
[sudo] password for utilisateur1:
New password:
Retype new password:
passwd: password updated successfully
```

Sites :

J’ai utilisé ce site pour apprendre à utiliser la commande ‘tracert’ :

https://www.pcastuces.com/pratique/windows/outils_reseau/page3.htm#:~:text=La%20commande%20tracert%20permet%20de,vous%20indiquez%20est%20alors%20affich%C3%A9.

Ce site est utile pour rechercher les cve :
https://nvd.nist.gov/vuln/detail/cve-XXXX-XXXX

(Il faut remplacer les ‘X’ par le nom de la CVE)

Vocabulaire :

-‘nslookup’ est un programme informatique de recherche d'information dans le Domain Name System (DNS), qui associe nom de domaine et adresses IP. ‘nslookup’ permet donc d'interroger les serveurs DNS pour obtenir les informations définies pour un domaine déterminé.

-Une vulnérabilité CSRF (pour Cross-Site Request Forgery, en français : falsification de requête inter-site) est une faille qui permet à un attaquant d'abuser à la fois d'un utilisateur, d'un navigateur web et d'un serveur.

-XXE (XML External Entity) : L'attaquant exploite la capacité d'un analyseur XML à traiter des entités externes pour accéder à des fichiers sensibles sur le serveur ou pour exécuter des requêtes malveillantes à des fins de divulgation d'informations ou de déni de service.

Ces attaques exploitent des failles dans la façon dont les applications gèrent les données XML, ce qui peut entraîner la divulgation d'informations sensibles, la modification non autorisée de données, ou des perturbations du service.