

Les attaques

Comprendre les mécanismes
vulnérables



Compétence demandée :
**Comprendre les mécanismes
vulnérables**

Qu'est-ce qu'une vulnérabilité ?





Dans le domaine de la sécurité informatique, une **vulnérabilité ou faille** est une faiblesse dans un système informatique permettant à **un attaquant de porter atteinte à l'intégrité de ce système**

Dans le domaine de la sécurité informatique, une vulnérabilité n'est pas nécessairement technique, **la faiblesse peut également venir des êtres humains (crédulité etc.)**



1. Les attaques MITM
2. Le phishing
3. Les attaques CSRF
4. Les modifications du DOM
5. Les injections
6. Le brute force

patote
brulante
tiède
chaude
brulante
brulante
tiède

LES ATTAQUES MITM

Que veut dire MITM ?



A votre avis, qu'est-ce qu'une
attaque Man In The Middle ?



Une **attaque MITM** (Man In The Middle) est une attaque qui a pour but d'intercepter les communications entre deux parties, sans que ni l'une ni l'autre ne puisse se douter que le canal de communication entre elles a été compromis.

Une **attaque MITM** est facilement réalisable sur une connexion HTTP, **mais plus difficilement avec connexion est chiffrée HTTPS (mais pas impossible !)**



A LA PLACE D'UN HACKER ...

Starbucks Wifi 2 (fake)



Objectifs :

1. Voler les informations envoyées par le client dans le payload (par POST)
2. Modifier la page HTML renvoyée par le site pour faire voir des illusions au client

Mise en place :

1. Créer un faux réseau Wifi avec un faux nom „Starbucks Wifi 2“ pour leurrer des clients et pour qu'ils viennent se connecter sur notre ordinateur
2. Regarder tout le trafic en HTTP non crypté (entrant et sortant)
3. Ecrire un programme pour modifier ce trafic (pour sauvegarder les payloads et injecter de l'HTML supplémentaire dans les réponses)

Flow Details

2021-01-04 11:20:41 GET https://management.azure.com/subscriptions/4d1c770c-574d-4746-8d25-f1e68fde-5b78/providers/-01/sights/workspaces?api-version=2020-08

- 200 OK applic

Request	Part	Detail
Cache-Control: no-cach	1) cookies	
Pragma: no-cach	2) urlencoded form	
Transfer-Encoding: chunked	3) multipart form	
Content-Type: applica	4) path	
Content-Encoding: gzip	5) method	
Vary: Accept-	6) query	
x-ms-request-id: 320565e	7) reason	
Strict-Transport-Security: max-age	8) request-headers	
X-Content-Type-Options: nosniff	9) response-headers	
Server: Microso	a) request-body	3cf89c
Server: Microso	b) response-body	mains
X-Powered-By: ASP.NET	c) status_code	
X-Powered-By: ASP.NET	d) set-cookies	
x-ms-ratelimit-remaining-subsc 11999	e) url	

[1/1] [f:management.azure.com] [*:8080]

On peut consulter les cookies, forcer un setcookie etc. nous pouvons tout faire

Nous subissons des attaques
MITM tous les jours en
entreprise, pourquoi ?



En entreprise, il est de l'ordre de la sécurité de **vérifier que les informations entrantes et sortantes des salariés** ne portent pas préjudice au business, donc le trafic est surveillé entre les salariés et internet.

Exemple : A la Société Générale, tout code source sortant est immédiatement et automatiquement signalé au responsable d'équipe

Question : un hopital doit-il laisser ses infirmiers envoyer les données des patients sur internet ?



Question : Microsoft doit-il laisser ses développeurs(ses) envoyer du code à l'extérieur ?



Question : Apple doit-il laisser ses commerciaux envoyer vos données à quelqu'un sans surveillance ?



**QUESTION A 1 MILLION
DE DOLLAR !**

Le Man In The Middle est-il **forcément une mauvaise chose** ?



**Non ! Cela peut être utilisé de manière
mal intentionné ou bien intentionné**

Rappel :

Une **attaque MITM** est facilement réalisable sur une connexion HTTP, **mais plus difficilement avec connexion chiffrée HTTPS** (mais pas impossible !)

En entreprise, même si vous êtes en HTTPS,
l'entreprise pourra quand même voir ce que
vous faites : votre ordinateur est paramétré
avec une exception, qui est l'employeur

Bande annonce prévention :

Hors entreprise, vous pouvez protéger vos visiteurs en **mettant votre site en HTTPS !**

Plus de détails plus tard !

To be continued ...

