XMNATIS

Les attaques

Comprendre les mécanismes vulnérables

XWIKI NATIS

Compétence demandée :

Comprendre les mécanismes vulnérables

XONATIS

XWIKI NATIS

Qu‘est-ce qu‘une vulnérabilité ?

XMNATIS

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

XMNATIS

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

XWIKI SAS

XEBIA NATIS

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

XWIKI SAS

XMCO NATIS

LES ATTAQUES MITM

XMNATIS

Que veut dire MITM ?

XWIKI SAS

XMNATIS

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

X◻NATIS

XONATIS

XMNATIS

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.

XMNATIS

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

XWIKI NATIS

A LA PLACE D‘UN HACKER …

XMCO NATIS

Starbucks Wifi 2
(fake)

XMNATIS

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

XMNATIS

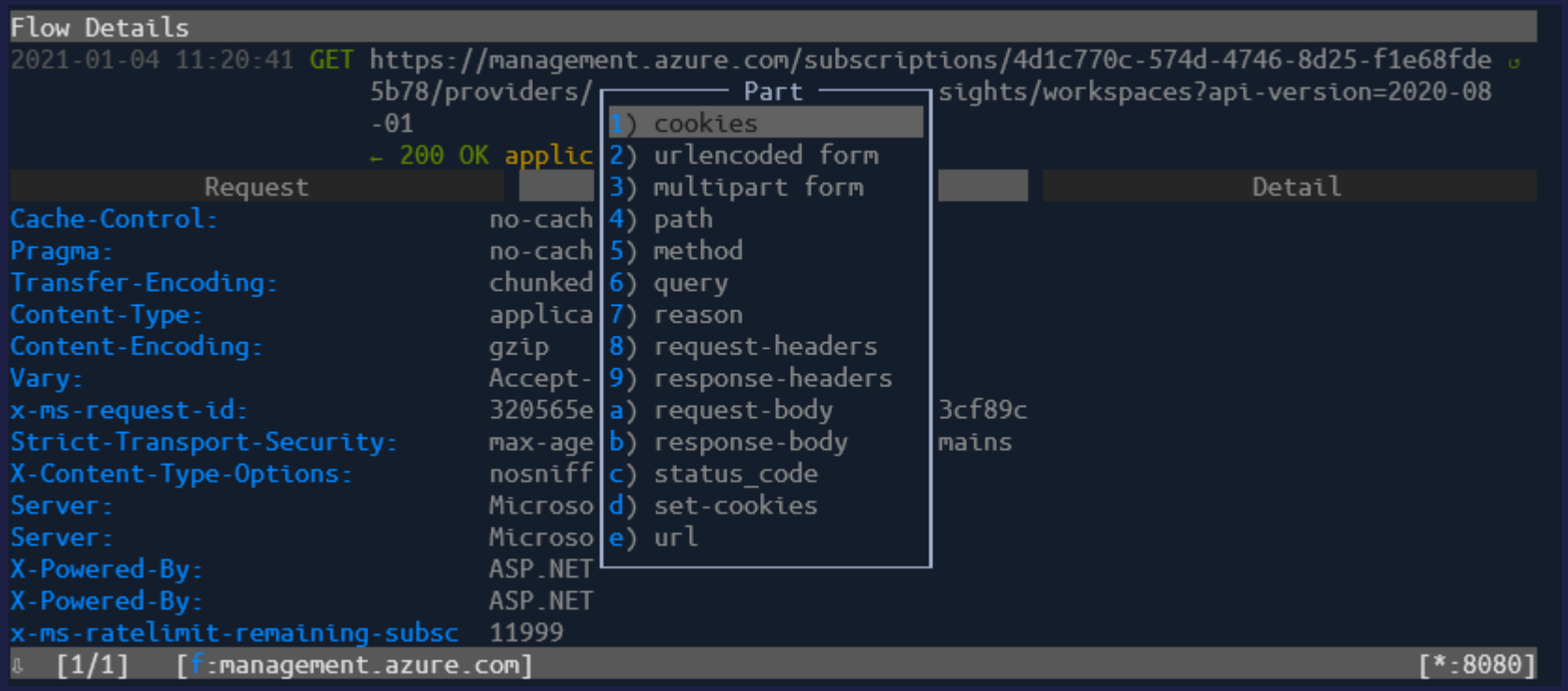
Mise en place :

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)

XEBIA NATIS



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

XONATIS

XMNATIS

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

XWIKI SAS

XWIKI NATIS

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.

XWIKI NATIS

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

XEBIA NATIS

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

XWIKI NATIS

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

XWIKI NATIS

QUESTION A 1 MILLION DE DOLLAR !

XWIKI NATIS

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

XWIKI NATIS

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

XWIKI NATIS

Rappel :

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

XWIKI NATIS

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

XONATIS

Bande annonce prévention :

XWIKI NATIS

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

Plus de détails plus tard !

To be continued …

XWIKI SAS