UNIVERSITÉ LAVAL

# CLUB DE HACKING

## XXE - XML eXTERNAL ELEMENT


Par

Maxime Leblanc

# XXE -Principe Général

- Faille de le "Parsing"des fichiers XML

- Certaines caractéristiques du standard XML son peu connues

- De ce fait, certaines implémentations ne tiennent pas compte de ces caractéristiques

# XXE -Principe Général

- Le standard XML contient ce qu'on appelle des #Entités"d'un certain type

- Un de ces types est une #Entité externe"

- Une entité externe peut etre définie par un contenu désigné via une certaine URI
  - Incluant des fichiers locaux et externes

# XXE -Entité Externe

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE root [
    <!ENTITY test_entity SYSTEM "/Users/username/test_entity.xml">
    <!ENTITY test_string "This is a test">
]>
<root>
    <tmp id="1">&test_entity;</tmp>
    <tmp id="2">&test_string;</tmp>
</root>
```

Sera interprété comme:

```
<root>
    <tmp id="1">Content of test_entity.xml</tmp>
    <tmp id="2">This is a test</tmp>
</root>
```

# XXE -Danger

- Il est ainsi possible de faire en sorte que l'application Web lise pour nous certains fichiers qui devraient etre privés

- On peut aussi faire lire au serveur des fichier distants (Ex: HTTP://... )

# XXE - Filtres PHP

- Il est possible d'utiliser les fonctionnalités des "filtres PHP" afin de "sanitizer" le retour
  - Pour ne pas corrompre le XML généré par des balises invalides, par exemple

# XXE -Démo

## Démo time!

Cible1: 192.168.0.50

Cible2: 192.168.0.52