

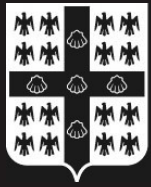
UNIVERSITÉ  
LAVAL

# CLUB DE HACKING

XXE - XML EXTERNAL ELEMENT

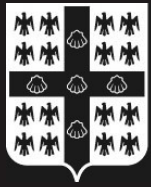
PAR

MAXIME LEBLANC



## XXE -PRINCIPE GÉNÉRAL

- FAIBLE 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 ÊTRE 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>
```

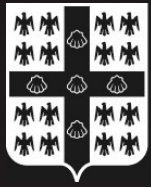


UNIVERSITÉ  
LAVAL

# CLUB DE HACKING

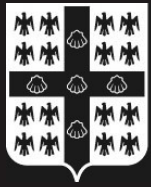
## XXE -DANGER

- 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 -FILTERS PHP

- IL EST POSSIBLE D'UTILISER LES FONCTIONNALITÉS DES FILTERS PHP "AFIN DE SANITIZER" LE RETOUR
- POUR NE PAS CORROMPRE LE XML GÉNÉRÉ PAR DES BALISES INVALIDES, PAR EXEMPLE



UNIVERSITÉ  
LAVAL

# CLUB DE HACKING

XXE -DÉMO

DÉMO TIME!

CIBLE1: 192.168.0.50

CIBLE2: 192.168.0.52