Je tu problém?

```
@ApplicationPath("/")
public class HelloApp extends Application {

    @Path("/")
    public static class HelloResource {

        @Consumes("application/xml")
        @POST
        public String doPost(Document doc) {
            return "Hello, " + doc.getDocumentElement().getTextContent();
        }
    }
}
```

XML eXternal Entity (XXE) útok

Entita

- V XML referencuje text
- Interní vs. Externí
- Externí entita je definovaná přes systémový identifikátor 'SYSTEM':

```
<!ENTITY name SYSTEM "URI">
```

- URI je cesta k lokálnímu nebo vzdálenému obsahu
- Definována v DTD

Příklad:

```
<?xml version="1.0"?>
<!DOCTYPE copyright[
<!ENTITY c SYSTEM "http://www.w3.org/xmlspec/copyright.xml">
]>
<copyright>&c;</copyright>
```

XXE útok

- Na aplikace, které parsují XML vstup
- XML parsery mají obvykle defaultně povolené parsování externích entit
- Reference na externí entitu je nahrazena obsahem externího souboru
- Získání důvěrných informací jako hesla nebo uživatelská data

Příklad:

```
<?xml version="1.0"?>
<!DOCTYPE echo[
<!ENTITY xxe SYSTEM "/path/file">
]>
<echo>&xxe;</echo>
```

Demo aplikace

```
@ApplicationPath("/")
public class HelloApp extends Application {

    @Path("/")
    public static class HelloResource {

        @Consumes("application/xml")
        @POST
        public String doPost(Document doc) {
            return "Hello, " + doc.getDocumentElement().getTextContent();
        }
    }
}
```

Jak se bránit

- **Zakázat externí entity**
- Toto nastavení XML parserů není u všech stejné
- OWASP uvádí doporučené nastavení pro xml parsery
- Rešením je zakázat externí entity a deklaraci DTD v uživatelských xml datech a validovat xml vstup proti statickým DTD
- V Resteasy byla chyba opravena tak, že externí entity byly XML parseru zakázány defaultně

Reálné příklady

Příklad XXE útoku na Google - Toolbar Button galery - odměna $10,000
https://blog.detectify.com/2014/04/11/how-we-got-read-access-on-googles-production-servers

Příklad XXE útoku při uploadu GPX souboru na RunKeeper
http://blog.h3xstream.com/2014/06/identifying-xml-external-entity.html

Příklad XXE útoku na Facebook používající OpenID login - odměna $33,500
http://www.ubercomp.com/posts/2014-01-16_facebook_remote_code_execution

https://www.facebook.com/notes/facebook-bug-bounty/bug-bounty-highlights-and-updates/818902394790655/

Bug bounty programy

- Dohoda mezi webovými službami a jednotlivci
- Odhalený bug nebo zranitelnost je reportován nejdřív firmě. Odměnou jsou obvykle peníze.
- Počátek v Netscapu (1995), motivací bylo zapálení některých zaměstnanců pro odhalování chyb
- Programy mají Google, Twitter, Facebook ale i americká vláda - Hack the Pentagon
- Seznam bug bounty programů
- Hackerone - Služba pro propojení firem a těch kdo objeví bezpečnostní problém

End