Tampering 101

Automated Testing of Binary Web Protocols

Chilik Tamir
Information Security Architect, AppSec-Labs
Twitter: @_coreDump
Chilik <at> AppSec-Labs <dot> com

OWASP Israel
15 September 2011

BBC one
TODAY'S
SPECIAL OFFERS
Banana
Pepp
Strawb
YouTube

Agenda

1 slide - Standard web applications

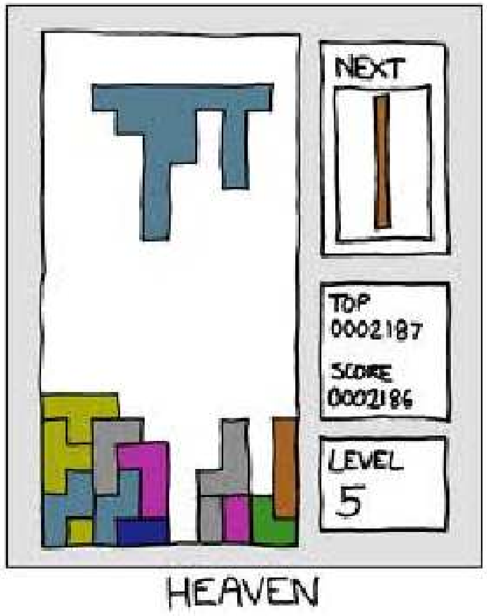
99% - Automating Binary protocols analysis

Standard web application

- Text-based Protocol
- Vast testing methodology

Tools

- Proxies / Sniffers
- Crawlers
- Scanners
- Manual Testing



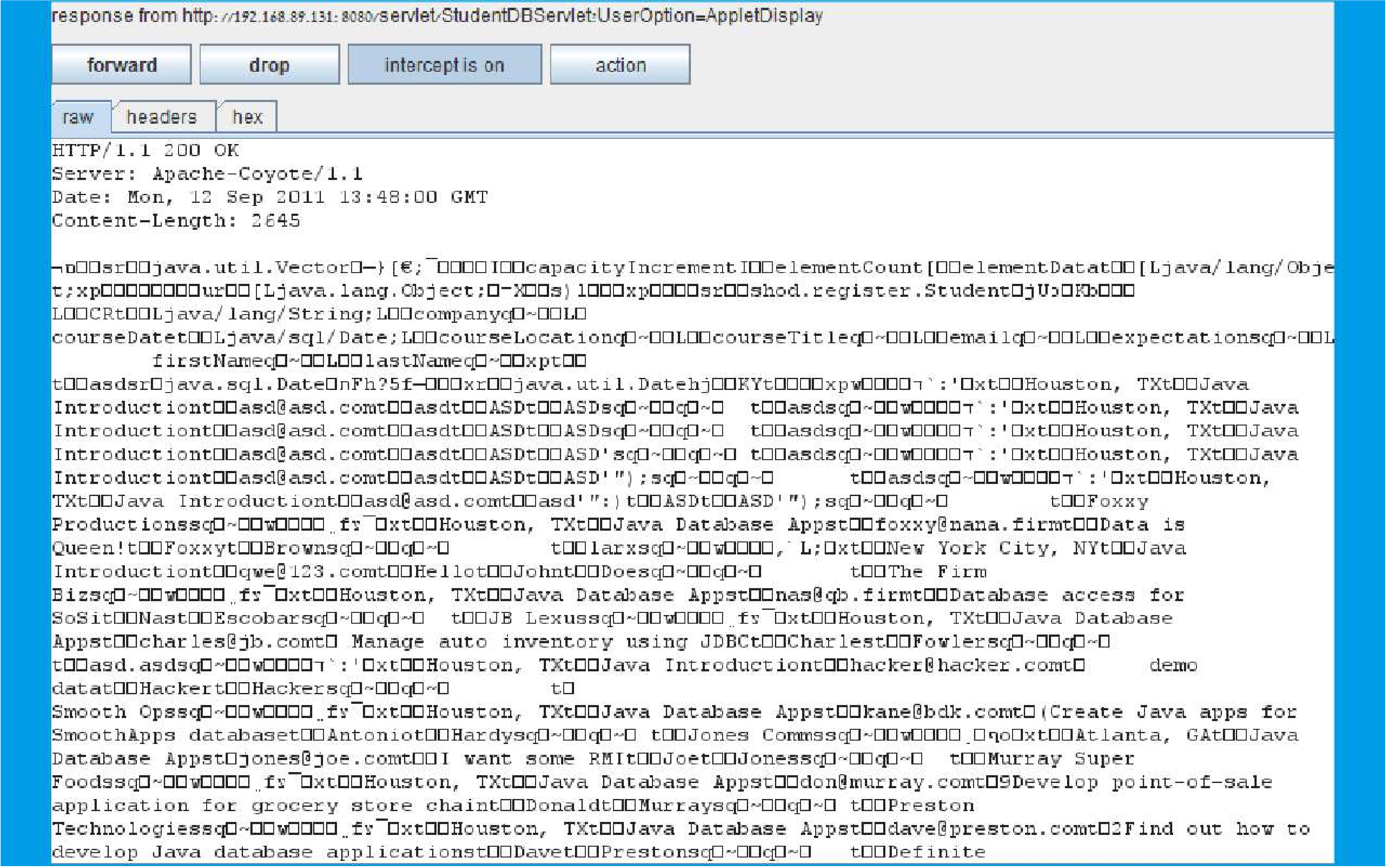
Binary Web apps

non-text protocols

Flash AMF
Java Serialization / RMI
Diameter / Radius
WCF
CORBA
etc...

Binary Comm. Demo (I)

http://192.168.89.131:8080/students/



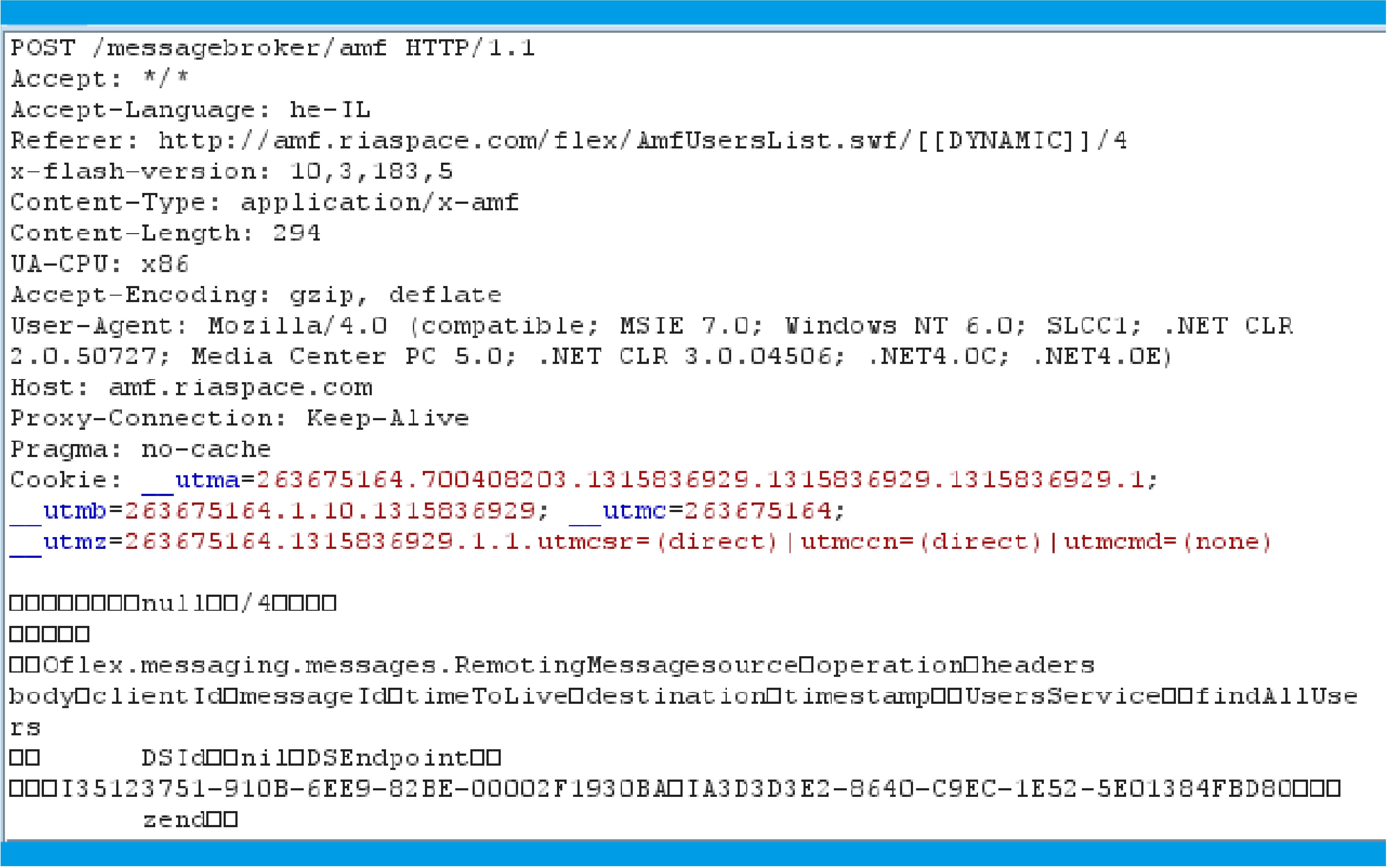
response from http://192.168.89.131:8080/servlet/StudentDBServlet?UserOption=AppletDisplay
forward
drop
intercept is on
action
raw
headers
hex

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Date: Mon, 12 Sep 2011 13:48:00 GMT
Content-Length: 2645

¬□□□sr□□java.util.Vector□—}[€;¯□□□□I□□capacityIncrementI□□elementCount[□□elementDatat□□[Ljava/lang/Obje
t;xp□□□□□□□□ur□□[Ljava.lang.Object;□¯X□□s)l□□□xp□□□□sr□□shod.register.Student□jU›□Kb□□□
L□□CRt□□Ljava/lang/String;L□□companyq□~□□L□
courseDatet□□Ljava/sql/Date;L□□courseLocationq□~□□L□□courseTitleq□~□□L□□emailq□~□□L□□expectationsq□~□□L
        firstNameq□~□□L□□lastNameq□~□□xpt□□
t□□asdsr□java.sql.Date□nFh?5f—□□□xr□□java.util.Datehj□□KYt□□□□xpw□□□□¬`:'□xt□□Houston, TXt□□Java
Introductiont□□asd@asd.comt□□asdt□□ASDt□□ASDsq□~□□q□~□  t□□asdsq□~□□w□□□□¬`:'□xt□□Houston, TXt□□Java
Introductiont□□asd@asd.comt□□asdt□□ASDt□□ASDsq□~□□q□~□  t□□asdsq□~□□w□□□□¬`:'□xt□□Houston, TXt□□Java
Introductiont□□asd@asd.comt□□asdt□□ASDt□□ASD'sq□~□□q□~□ t□□asdsq□~□□w□□□□¬`:'□xt□□Houston, TXt□□Java
Introductiont□□asd@asd.comt□□asdt□□ASDt□□ASD'");sq□~□□q□~□      t□□asdsq□~□□w□□□□¬`:'□xt□□Houston,
TXt□□Java Introductiont□□asd@asd.comt□□asd'":)t□□ASDt□□ASD'");sq□~□□q□~□        t□□Foxxy
Productionssq□~□□w□□□□„fr¯□xt□□Houston, TXt□□Java Database Appst□□foxxy@nana.firmt□□Data is
Queen!t□□Foxxyt□□Brownsq□~□□q□~□        t□□larxsq□~□□w□□□□,`L;□xt□□New York City, NYt□□Java
Introductiont□□qwe@123.comt□□Hellot□□Johnt□□Doesq□~□□q□~□       t□□The Firm
Bizsq□~□□w□□□□„fr¯□xt□□Houston, TXt□□Java Database Appst□□nas@qb.firmt□□Database access for
SoSit□□Nast□□Escobarsq□~□□q□~□  t□□JB Lexussq□~□□w□□□□„fr¯□xt□□Houston, TXt□□Java Database
Appst□□charles@jb.comt□ Manage auto inventory using JDBCt□□Charlest□□Fowlersq□~□□q□~□
t□□asd.asdsq□~□□w□□□□¬`:'□xt□□Houston, TXt□□Java Introductiont□□hacker@hacker.comt□     demo
datat□□Hackert□□Hackersq□~□□q□~□        t□
Smooth Opssq□~□□w□□□□„fr¯□xt□□Houston, TXt□□Java Database Appst□□kane@bdk.comt□(Create Java apps for
SmoothApps databaset□□Antoniot□□Hardysq□~□□q□~□ t□□Jones Commssq□~□□w□□□□¸□qo□xt□□Atlanta, GAt□□Java
Database Appst□jones@joe.comt□□I want some RMIt□□Joet□□Jonessq□~□□q□~□  t□□Murray Super
Foodssq□~□□w□□□□„fr¯□xt□□Houston, TXt□□Java Database Appst□□don@murray.comt□9Develop point-of-sale
application for grocery store chaint□□Donaldt□□Murraysq□~□□q□~□ t□□Preston
Technologiessq□~□□w□□□□„fr¯□xt□□Houston, TXt□□Java Database Appst□□dave@preston.comt□2Find out how to
develop Java database applicationst□□Davet□□Prestonsq□~□□q□~□   t□□Definite
```

Binary Comm. Demo (II)

http://amf.riaspace.com/

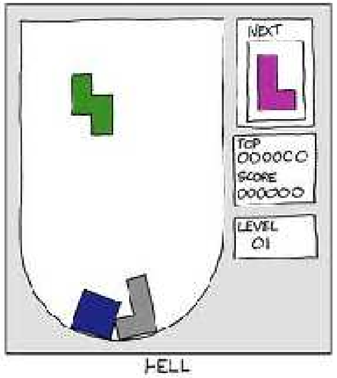


```
POST /messagebroker/amf HTTP/1.1
Accept: */*
Accept-Language: he-IL
Referer: http://amf.riaspace.com/flex/AmfUsersList.swf/[[DYNAMIC]]/4
x-flash-version: 10,3,183,5
Content-Type: application/x-amf
Content-Length: 294
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; SLCC1; .NET CLR
2.0.50727; Media Center PC 5.0; .NET CLR 3.0.04506; .NET4.0C; .NET4.0E)
Host: amf.riaspace.com
Proxy-Connection: Keep-Alive
Pragma: no-cache
Cookie: __utma=263675164.700408203.1315836929.1315836929.1315836929.1;
__utmb=263675164.1.10.1315836929; __utmc=263675164;
__utmz=263675164.1315836929.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none)

□□□□□□□□null□□/4□□□□
□□□□□
□□Oflex.messaging.messages.RemotingMessagesource□operation□headers
body□clientId□messageId□timeToLive□destination□timestamp□□UsersService□□findAllUse
rs
□□       DSId□□nil□DSEndpoint□□
□□□I35123751-910B-6EE9-82BE-00002F1930BA□IA3D3D3E2-8640-C9EC-1E52-5E01384FBD80□□□
        zend□□
```

Binary Comm. Setbacks

- Manual Tampering and Haxing
- Can't automate the process
- Can't use standard tools

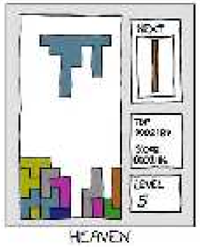


Standard web application

- Text-based Protocol
- Vast testing methodology

Tools

- Proxies / Sniffers
- Crawlers
- Scanners
- Manual Testing



Previous Work in Binary Communication Testing

- afx- Reconstructing serialized Java objects from sniffer logs (Forbidden Knowledge vol 14, 2001)
- Shai Chen - PT to Java Client Server Apps (OWASP Israel, 2008)
- Eric Monty et. al - Ruby for pentesers: JRuby (BlackHat, 2009)
- Marcin Wielgoszewski - Pentesting Adobe Flex Applications (OWASP NYNJMetro, 2010)

What's Missing

- On the fly analysis
- Co-op with availble tools
- Easy to adopt
- Zero-configuration
- Scriptable / Extendable
- Self Updateble

Enter BELCH

Burp ExternaL CHannel

One Tool to rule them all

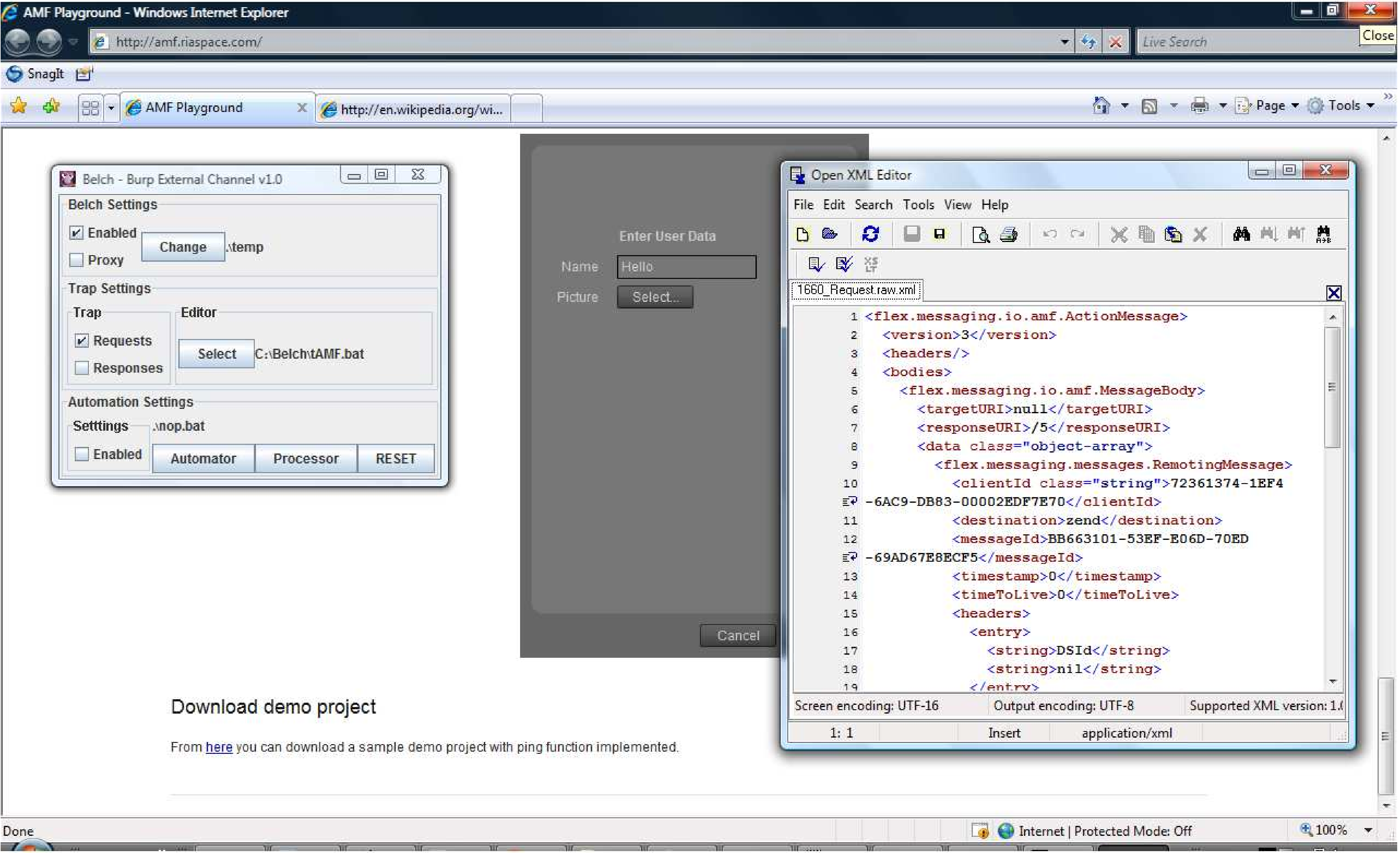
Belch - The missing link:

What's Missing

- On the fly analysis
- Co-op with availble tools
- Easy to adopt
- Zero-configuration
- Scriptable / Extendable
- Self Updateble

Additional:

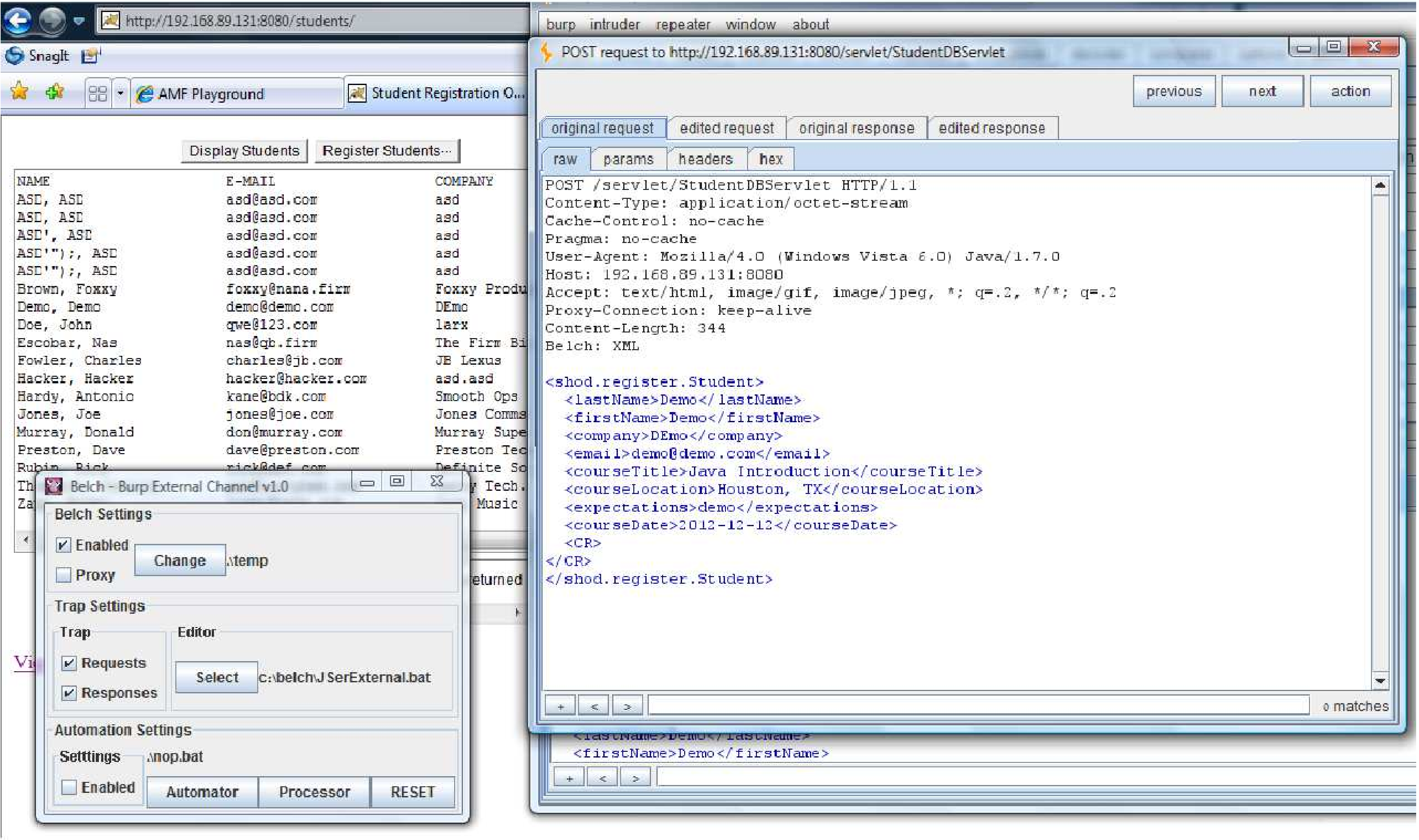
- Open source
- Free
- Simulate Binary requests
- Simulate Binary responses
- Load testing ?
- Insert BL into tampering
- Extendable +++



```
<flex.messaging.io.amf.ActionMessage>
  <version>3</version>
  <headers/>
  <bodies>
    <flex.messaging.io.amf.MessageBody>
      <targetURI>null</targetURI>
      <responseURI>/5</responseURI>
      <data class="object-array">
        <flex.messaging.messages.RemotingMessage>
          <clientId class="string">72361374-1EF4
-6AC9-DB83-00002EDF7E70</clientId>
          <destination>zend</destination>
          <messageId>BB663101-53EF-E06D-70ED
-69AD67E8ECF5</messageId>
          <timestamp>0</timestamp>
          <timeToLive>0</timeToLive>
          <headers>
            <entry>
              <string>DSId</string>
              <string>nil</string>
            </entry>
```

Download demo project

From here you can download a sample demo project with ping function implemented.


http://192.168.89.131:8080/students/
SnagIt
AMF Playground
Student Registration O...
burp intruder repeater window about
previous
next
action

Display Students | Register Students...

NAME	E-MAIL	COMPANY
ASD, ASD	asd@asd.com	asd
ASD, ASD	asd@asd.com	asd
ASD', ASD	asd@asd.com	asd
ASD'");, ASD	asd@asd.com	asd
ASD'");, ASD	asd@asd.com	asd
Brown, Foxxy	foxxy@nana.firm	Foxxy Produ
Demo, Demo	demo@demo.com	DEmo
Doe, John	qwe@123.com	larx
Escobar, Nas	nas@qb.firm	The Firm Bi
Fowler, Charles	charles@jb.com	JB Lexus
Hacker, Hacker	hacker@hacker.com	asd.asd
Hardy, Antonio	kane@bdk.com	Smooth Ops
Jones, Joe	jones@joe.com	Jones Comms
Murray, Donald	don@murray.com	Murray Supe
Preston, Dave	dave@preston.com	Preston Tec
Rubin, Rick	rick@def.com	Definite So
Th		y Tech.
Za		Music

Belch - Burp External Channel v1.0

Belch Settings

☑ Enabled Change \temp

☐ Proxy

Trap Settings

Trap
☑ Requests
☑ Responses

Editor
Select c:\belch\JSerExternal.bat

Automation Settings

Setttings \nop.bat
☐ Enabled

Automator | Processor | RESET

POST request to http://192.168.89.131:8080/servlet/StudentDBServlet

original request | edited request | original response | edited response

raw | params | headers | hex

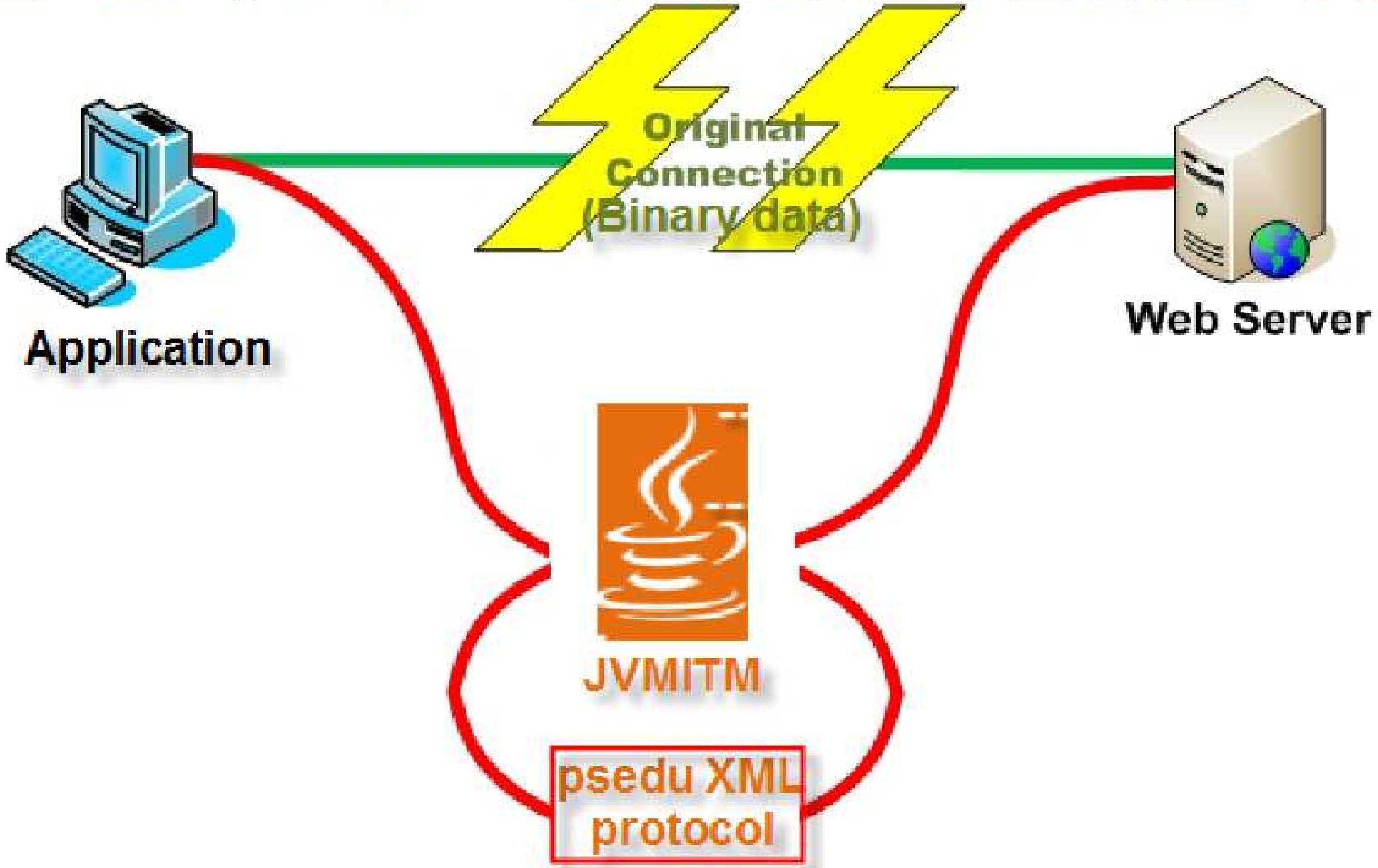
```
POST /servlet/StudentDBServlet HTTP/1.1
Content-Type: application/octet-stream
Cache-Control: no-cache
Pragma: no-cache
User-Agent: Mozilla/4.0 (Windows Vista 6.0) Java/1.7.0
Host: 192.168.89.131:8080
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Proxy-Connection: keep-alive
Content-Length: 344
Belch: XML

<shod.register.Student>
  <lastName>Demo</lastName>
  <firstName>Demo</firstName>
  <company>DEmo</company>
  <email>demo@demo.com</email>
  <courseTitle>Java Introduction</courseTitle>
  <courseLocation>Houston, TX</courseLocation>
  <expectations>demo</expectations>
  <courseDate>2012-12-12</courseDate>
  <CR>
</CR>
</shod.register.Student>
```

0 matches

  <lastName>Demo</lastName>
  <firstName>Demo</firstName>

FTW? - JVMITM !!



Original Connection (Binary data)

Application

Web Server

JVMITM

psedu XML protocol

Belch engine: JVMITM

Binary Object → Java Object → XML (psuedo-protocol)

i. Channel binary communication to JVM

ii. Use JVM to reconstruct object in Context

iii. Use JVM Serialization support to represent Object and Contexnt as XML

iv. wrap with a pseudo-protocol

v. Tamper with data (manual and scanners)

vi. Reverse the flow

XML (psuedo-protocol) → Java Object → Binary Object

Binary Comm. Setbacks

- Manual Tampering and Testing
- Can't automate the process
- Can't use standard tools

Questions?

Tampering 101

Automated Testing of Binary Web Protocols

Chilik Tamir
Information Security Architect, AppSec-Labs
Twitter: @_coreDump
Chilik <at> AppSec-Labs <dot> com

OWASP Israel
15 September 2011

AppSec Application security Labs