Advanced Web Security

Philipp Oesch
01.03.2012

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

Tel +41 55-214 41 60
Fax +41 55-214 41 61
team@csnc.ch
www.csnc.ch

About Philipp Oesch

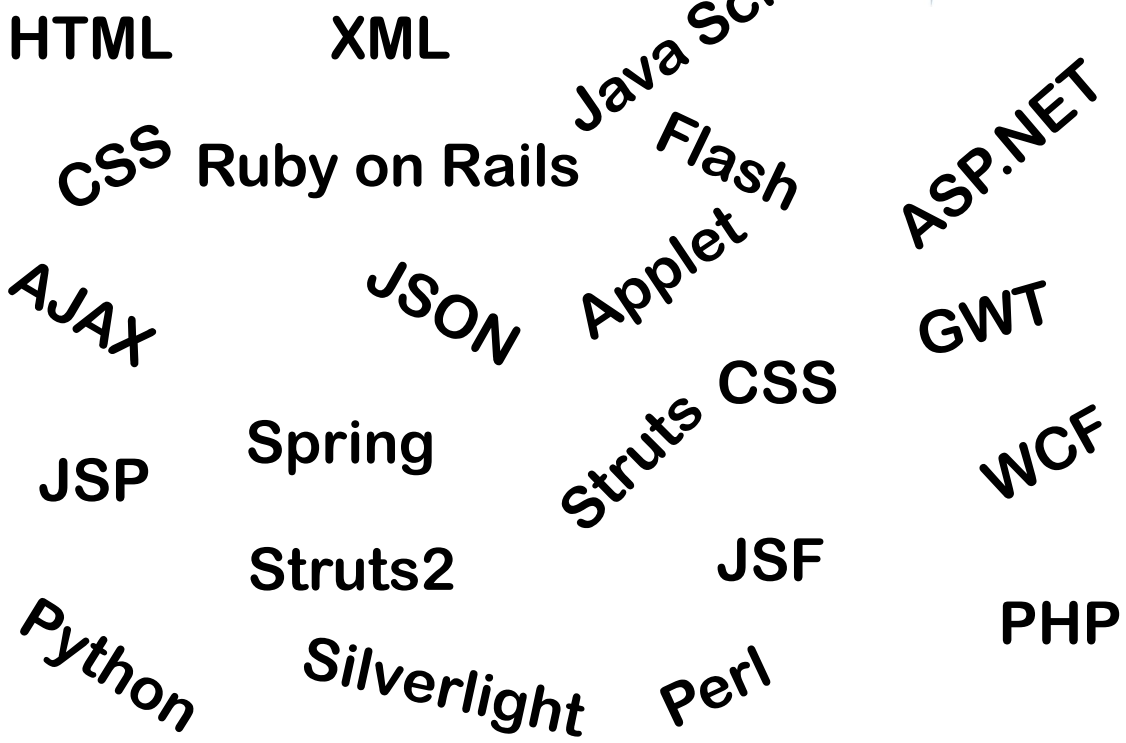
Security
&
Software
Development

Security Analyst - Head of Devleopment - Compass Security AG
before 2008 ...: Software Engineer - Projectleader - ELCA Informatik AG

Agenda

- New Challenges Today
- Risks with Open Source & Standard Frameworks
- Live Hacking Demo – Struts 2
- Recommendations
- Live Hacking Demo – (XXE & MySQL UDF)
- New HTTP Headers

Evolution Of Web Technologies



Challenges In The Past

Situation

- Selfmade applications

Challenges

- Understanding of basic web technologies
- Knowledge about web security & secure coding

Challenges Today

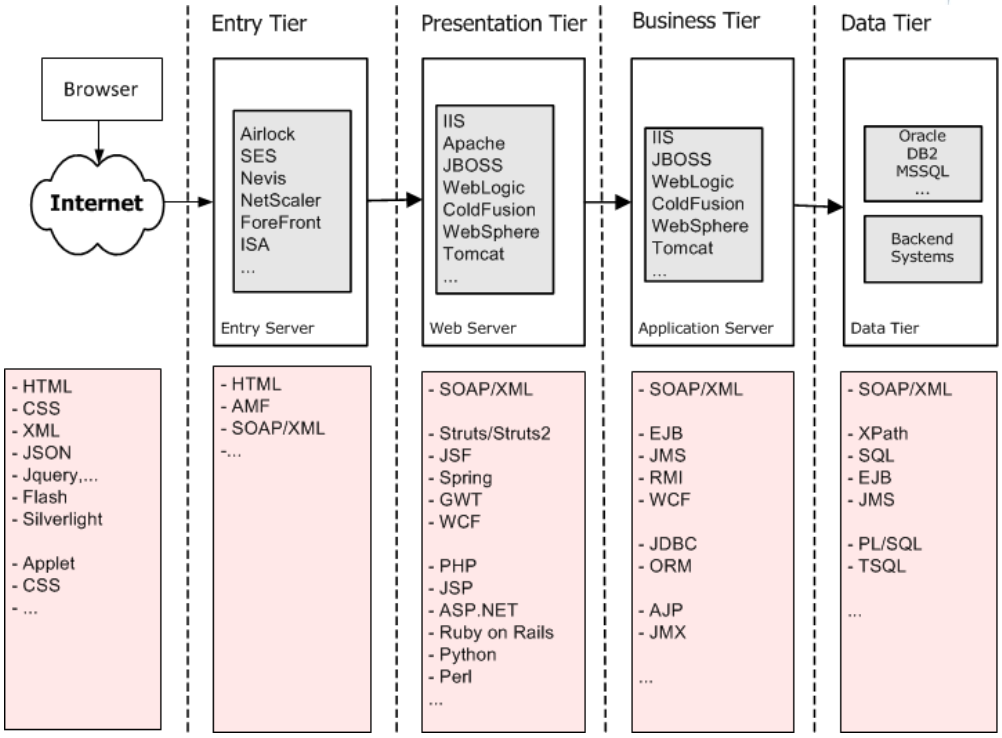
Situation

- Different technologies & libraries
- Complex frameworks

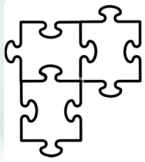
Challenges

- Knowledge of technologies
- Knowledge of frameworks
- Understanding of underlying technologies
- Knowledge about web security & secure coding

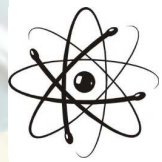
Technology Stack Today



Risks Today



Growing application landscape
- Different frameworks
- Different technologies



Growing framework complexity
- Function overview
- Understanding of underlying technology

Quick and dirty application migrations
- Integration of new features & technologies
- Integration of backend & external systems

Competence / Responsibilities

Development

- Programming of applications
- Bugfixing of applications

Operations

- Deployment in the productive environment
- Backup & Logging
- System updates
  - Operation system
  - Installed software
- System hardening

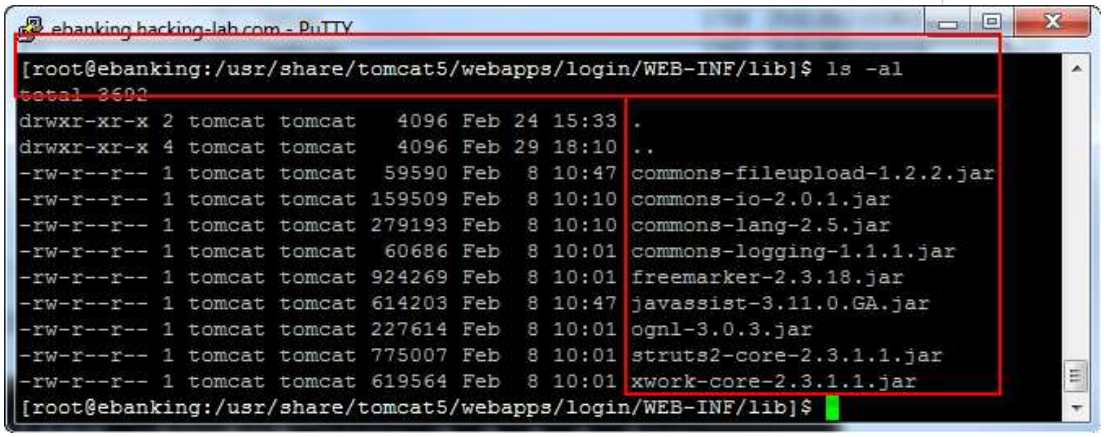
But Who is responsible for?

- Secure configuration of used frameworks
- Updating/Patching from used framework & libraries
- Overall security

Security Measure

Software Stack	Security Measure
Application	Manual Hacking Vulnerability Scan Source Code Review
Standard Frameworks (Struts, JSF, Hibernate, ..)	?
Web Server Application Server	Server Hardening Vulnerability Scan
Operation System	OS Hardening Vulnerability Scan

Don't forget to patch the framework



Framework libraries are often forgotten in the update Process!

Struts 2 Framework Vulnerability

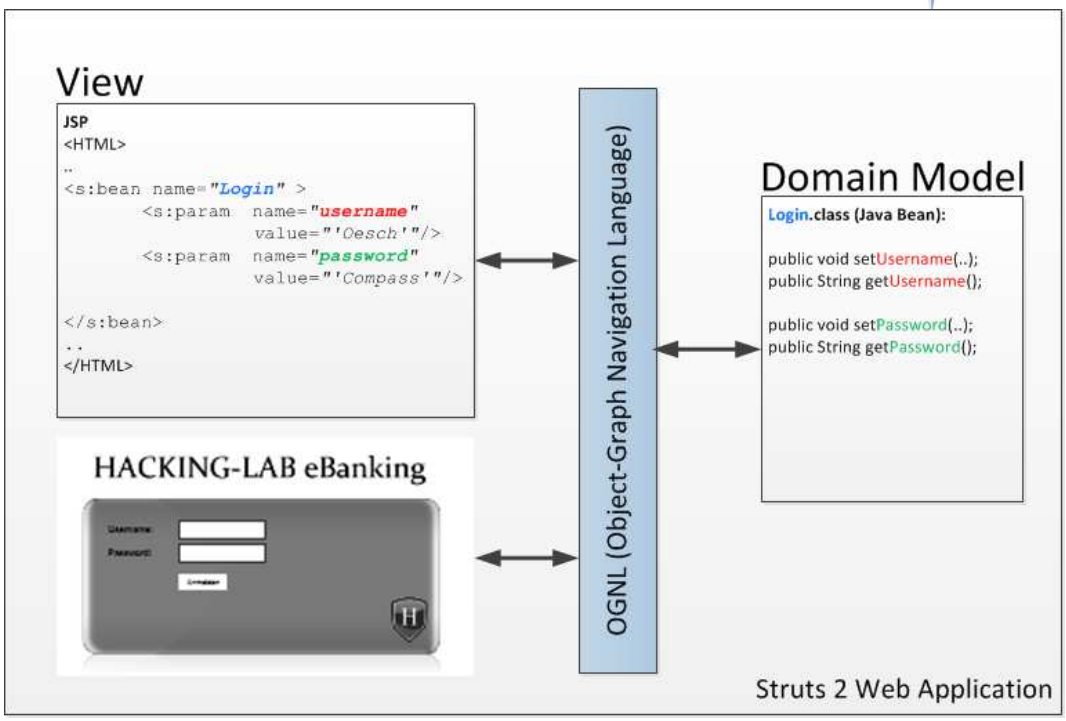
Struts 2

OGNL - Vulnerability

Object-Graph Navigation Language

The Apache Software Foundation
http://www.apache.org/

Struts 2 Framework - OGNL INTRO



Struts 2 Framework - OGNL INTRO

OGNL is used to access java objects and session values:

Set java object value:

```
<s:bean name="Login" var="loginbean">
    <s:param name="username" value="'Oesch'"/>
    <s:param name="password" value="'Compass'"/>
</s:bean>
```

Read java object values:

```
Username= <s:property value="#loginbean.username" />
Password= <s:property value="#loginbean.password" />
```

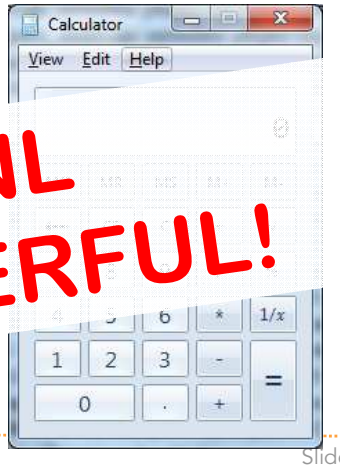
Read session values:

```
User= <s:property value="#session.user" />
```

Struts 2 Framework - OGNL INTRO

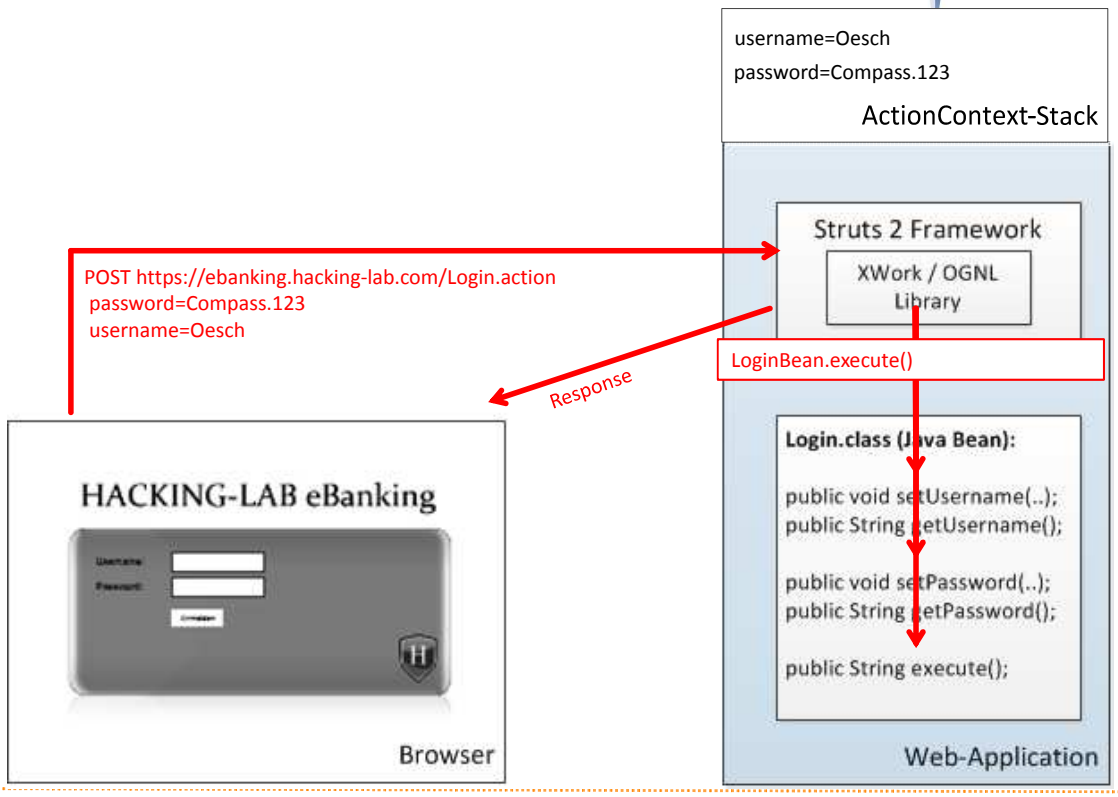
But it is also possible to execute Java Code!

```
<s:property value="(
  #context[\"xwork.MethodAccessor.denyMethodExecution\"]= new
            java.lang.Boolean(false),
  #_memberAccess[\"allowStaticMethodAccess\"]= new java.lang.Boolean(true),
  @java.lang.Runtime@getRuntime().exec('calc.exe')
)"/>
```

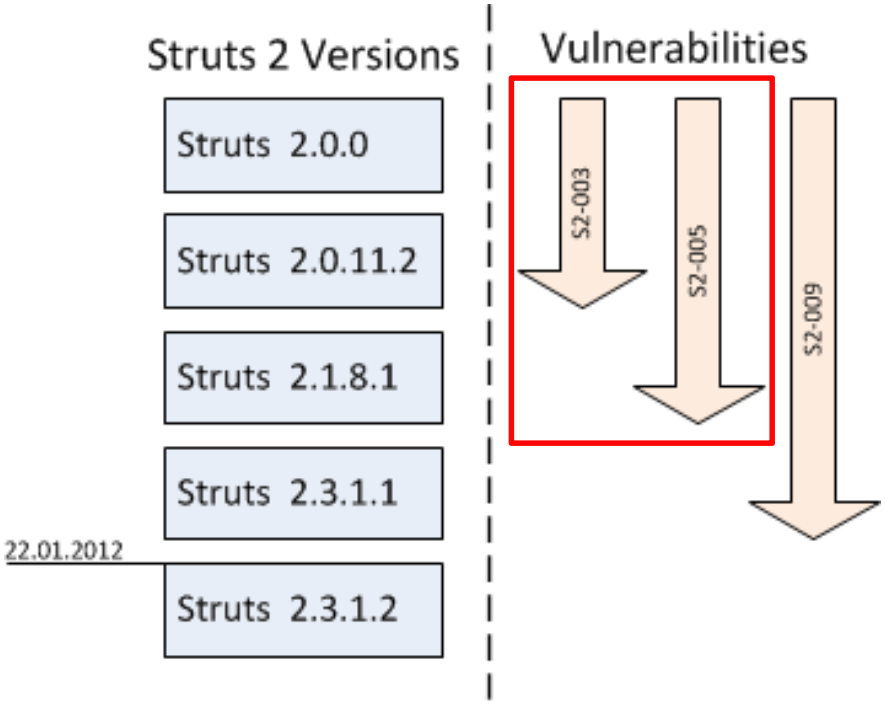


Struts 2 - Live Hacking Demo

Normal Request

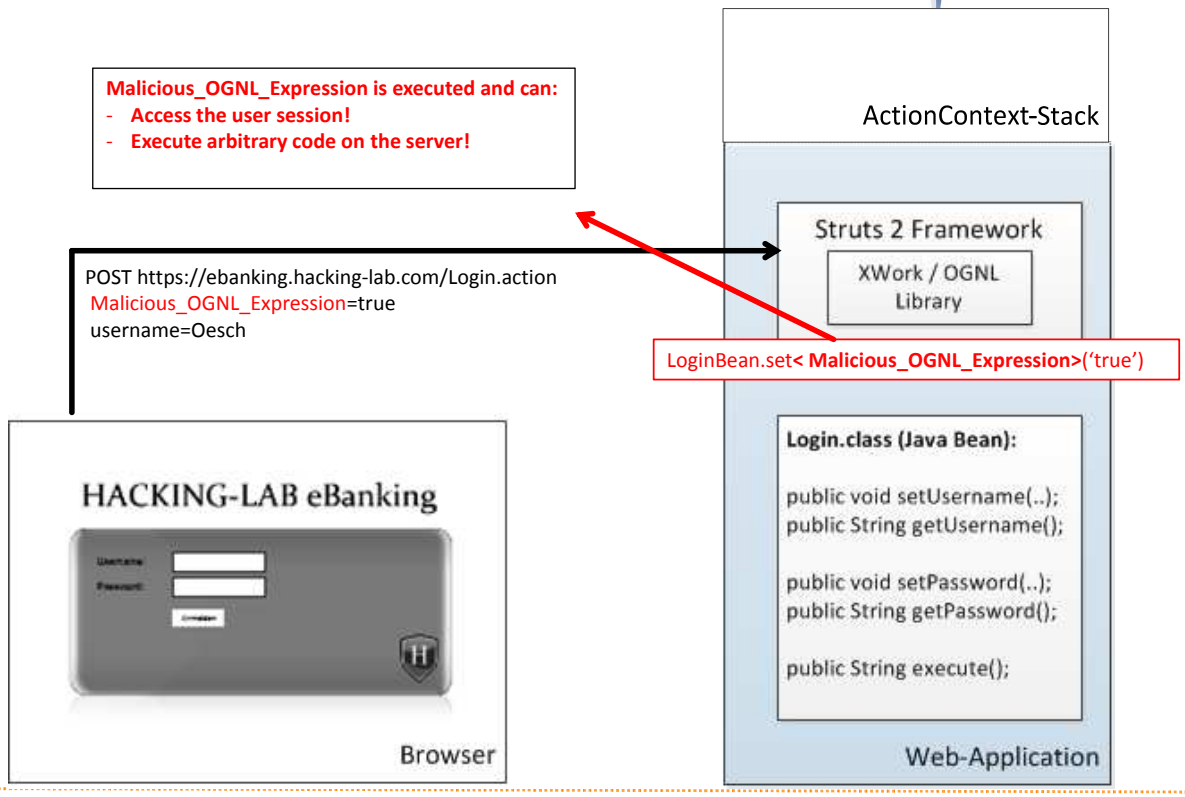


Struts 2 - Vulnerabilities



Struts 2 - Live Hacking Demo

Remote Code Execution Vulnerability S2-003/S2-005



Struts 2 - Live Hacking Demo

Vulnerability S2-003 (Struts 2.0.0 - Struts 2.0.11.2)

- Problem: malicious OGNL expression in parameter name
- Patch: Regexp for allowed parameter names (Whitelist)

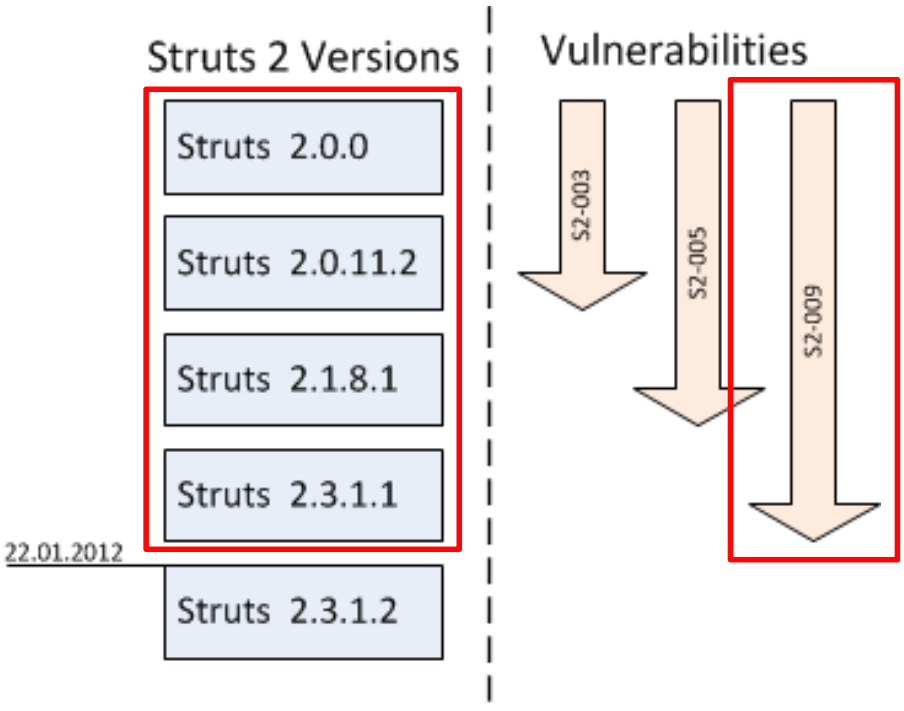
Whitelist was not restrictive enough -> S2-005!

Vulnerability S2-005 (Struts 2.0.0 - Struts 2.1.8.1)

- Problem: malicious OGNL expression in parameter name
- Patch: Improved regexp for allowed parameter names (Whitelist)

Malicious OGNL expression in parameter name was not possible anymore but remote code execution was still possible! -> S2-009!

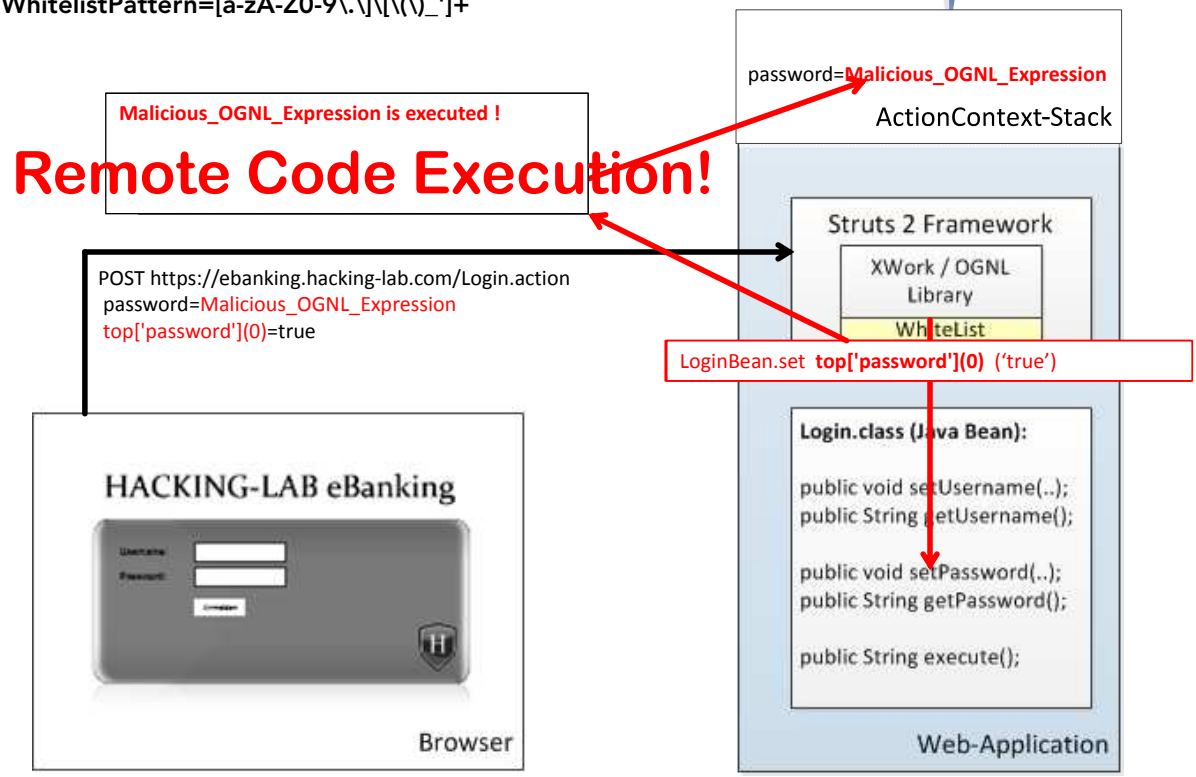
Struts 2 - Vulnerabilities



Struts 2 - Live Hacking Demo

Remote Code Execution Vulnerability S2-009

WhitelistPattern=[a-zA-Z0-9\.\]\[\(\)_']+



Struts 2 - Live Hacking Demo

Struts 2 – Source Code Check

Comparing the Source Code:

- Vulnerable version (S2-009): Struts 2.3.1.1/ognl 3.0.3 /xwork-core.2.3.1.1
  - Following pattern was used to filter attack string in attribute names
    - Pattern=[a-zA-Z0-9\.\]\[\(\)_']+
- Attack String in parameter name: top['password'](0)
- Current Version: Struts 2.3.1.2 / ognl 3.0.4 / xwork-core.2.3.1.2
  - Pattern for attribute name changed
    - New Pattern=\w+((\.\w+)|(\[\d+\])|(\(\d+\))|(\['\w+'\])|(\('\w+'\)))*

Upgrade to Struts 2.3.1.2.

Struts 2

Upgrade to Struts 2.3.1.2!

The Apache Software Foundation
http://www.apache.org/

Struts2 Metasploit Module

metasploit®

Apache Struts < 2.2.0 Remote Command Execution

This module exploits a remote command execution vulnerability in Apache Struts versions < 2.2.0. This issue is caused by a failure to properly handle unicode characters in OGNL extensive expressions passed to the web server. By sending a specially crafted request to the Struts application it is possible to bypass the "#" restriction on ParameterInterceptors by using OGNL context variables. Bypassing this restriction allows for the execution of arbitrary Java code.

Rank

Excellent

Authors

bannedit < bannedit [at] metasploit.com >
Meder Kydyraliev < >

References

CVE-2010-1870
OSVDB-66280
http://www.exploit-db.com/exploits/14360/

http://www.metasploit.com/modules/exploit/multi/http/struts_code_exec

Dependence

RAILS

springsource community

Joomla!™

jQuery write less, do more.

OpenCms

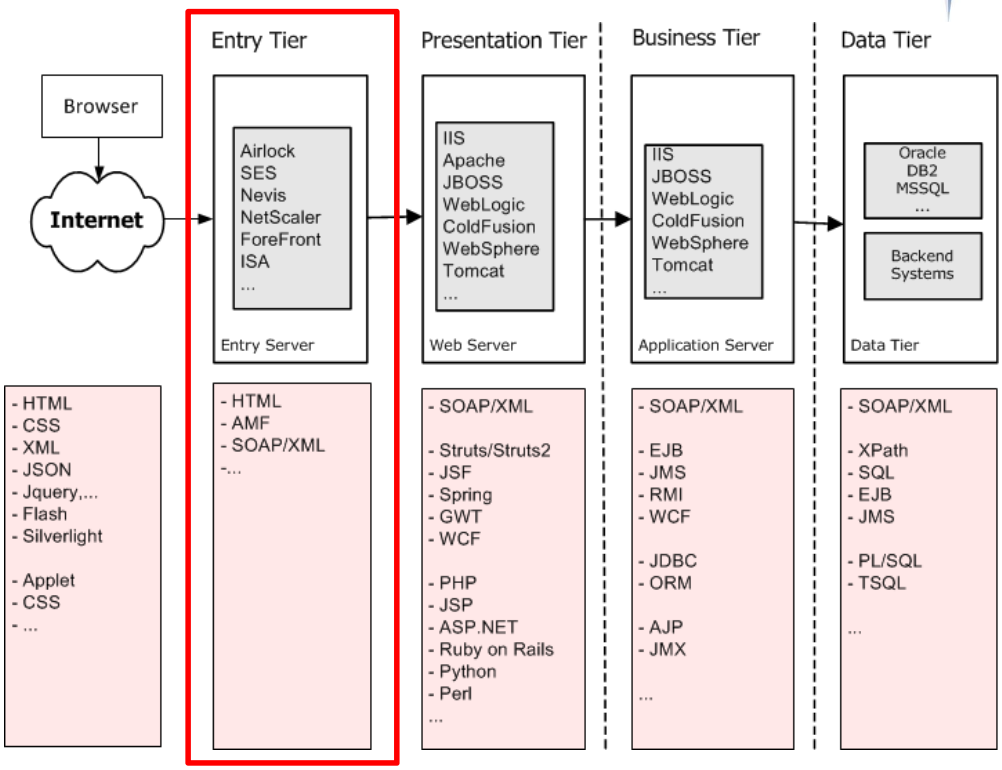
Foreign products & frameworks are not controllable!

php

MySQL

The Apache Software Foundation http://www.apache.org/

How to protect?

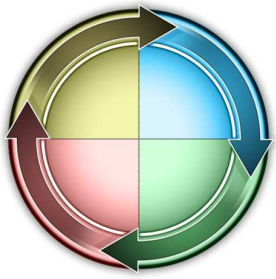


Recommendations

Entry Server (WAF) – InputFilter on parameters & requests

- Whitelisting of expected parameters/requests
- Blacklisting of known attack vectors

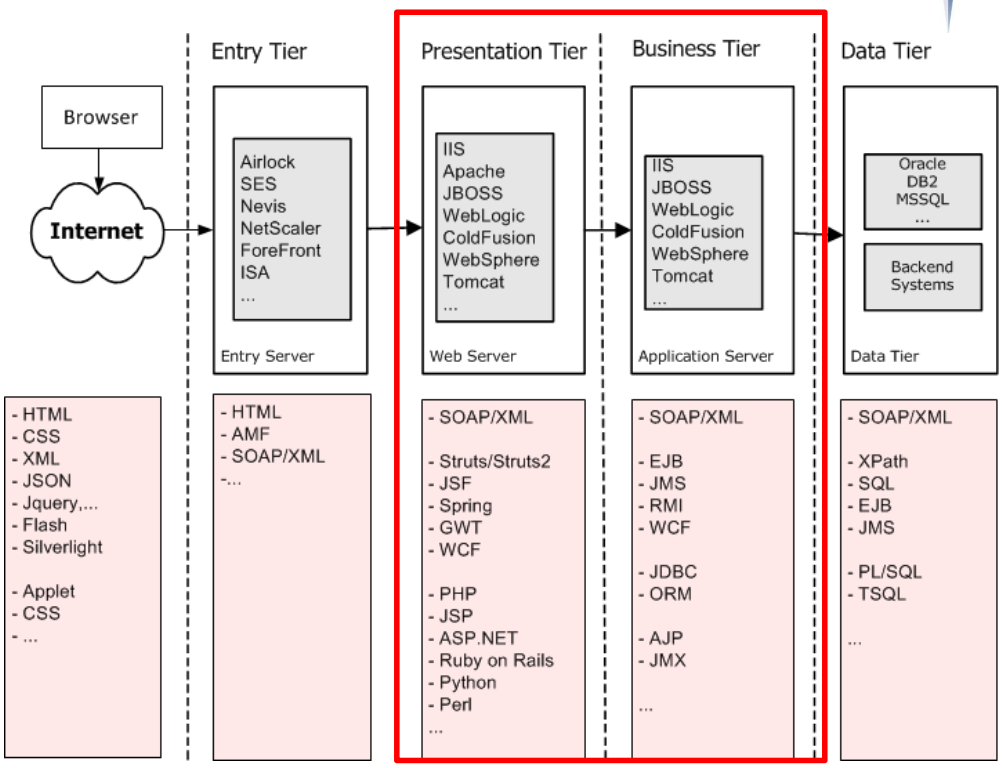
Improve collaboration between development & operation:



Define:

- Interfaces between different systems
- Transferred data
- Technologies and frameworks
- WAF – Input Filter Configuration

How to protect?



Recommendations

Company guidelines

- Technologies & framework guidelines
- Clear competence & responsibility

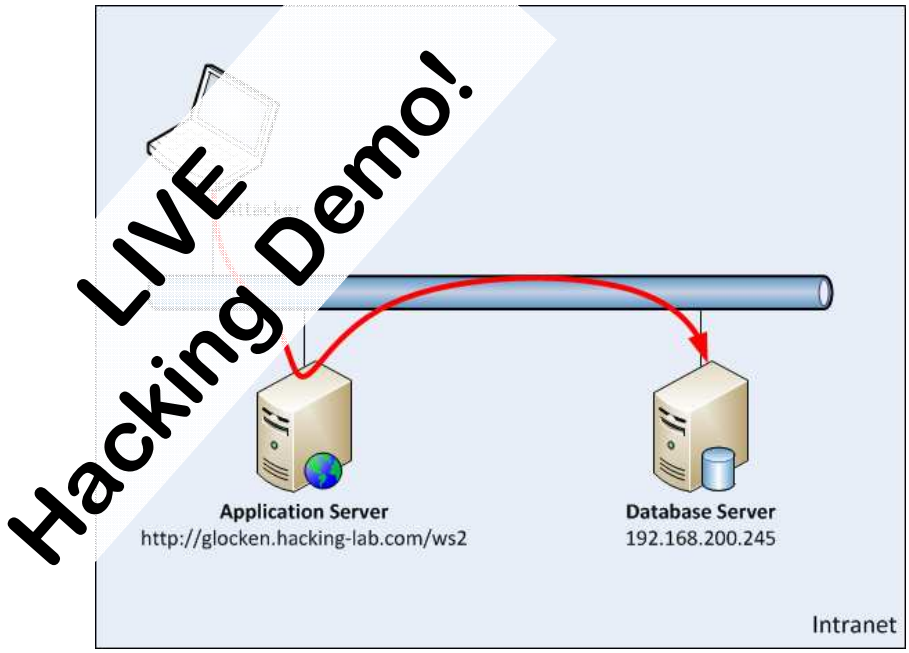
Web application

- Limit technologies & frameworks (keep it simple)
- Deploy only the required set of functions and libraries
- Track versions and update regularly
- Secure coding & configuration

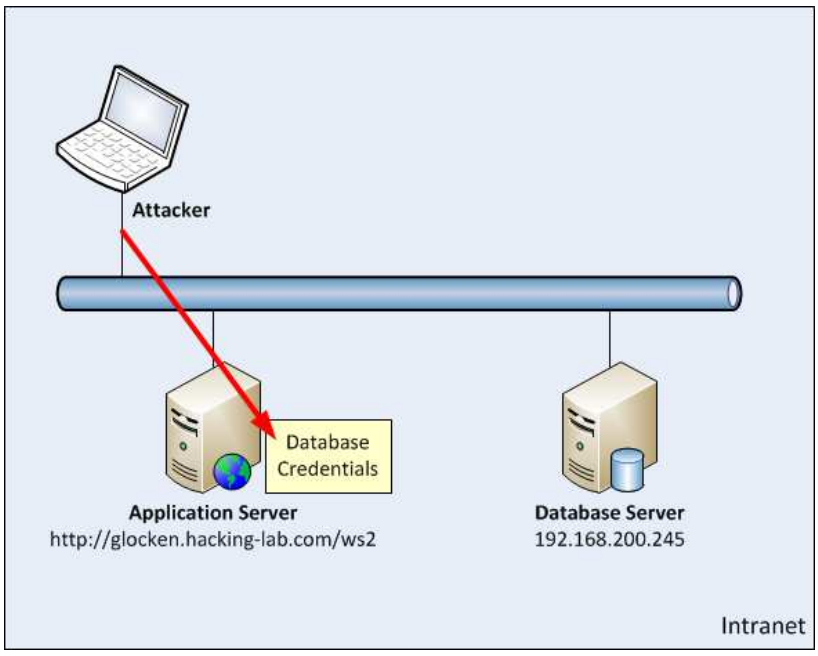
Update process

- Track the used versions and monitor new vulnerabilities
- Update all components
  - OS, Web Server, DB , ..
  - Also application libraries & frameworks!

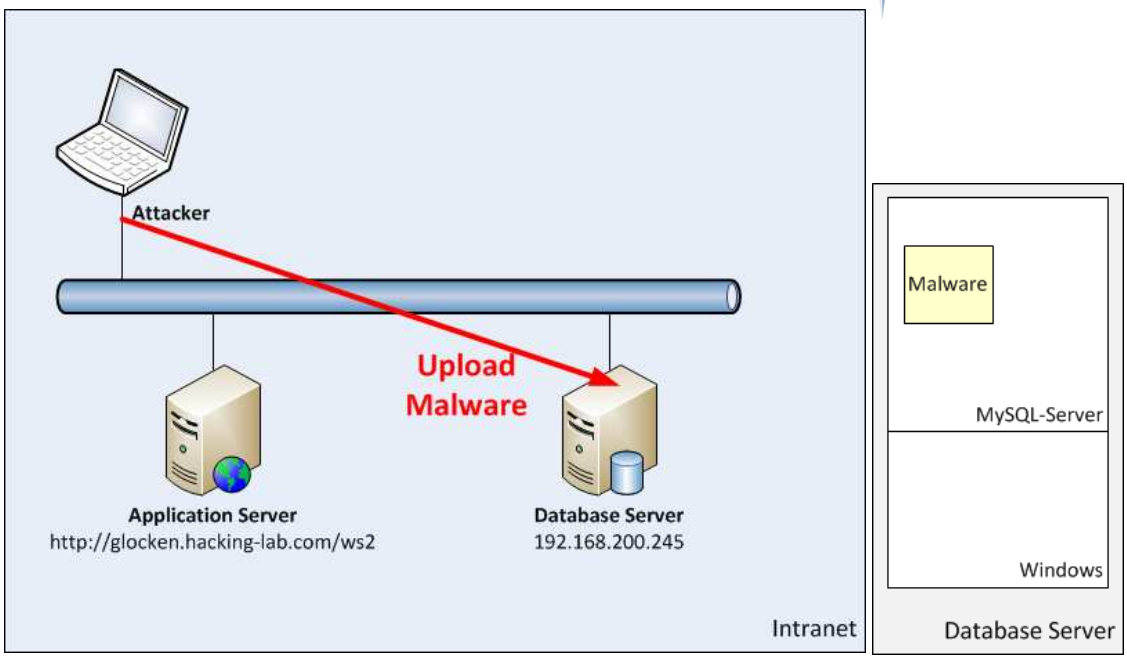
XXE UDF - Live Hacking Demo



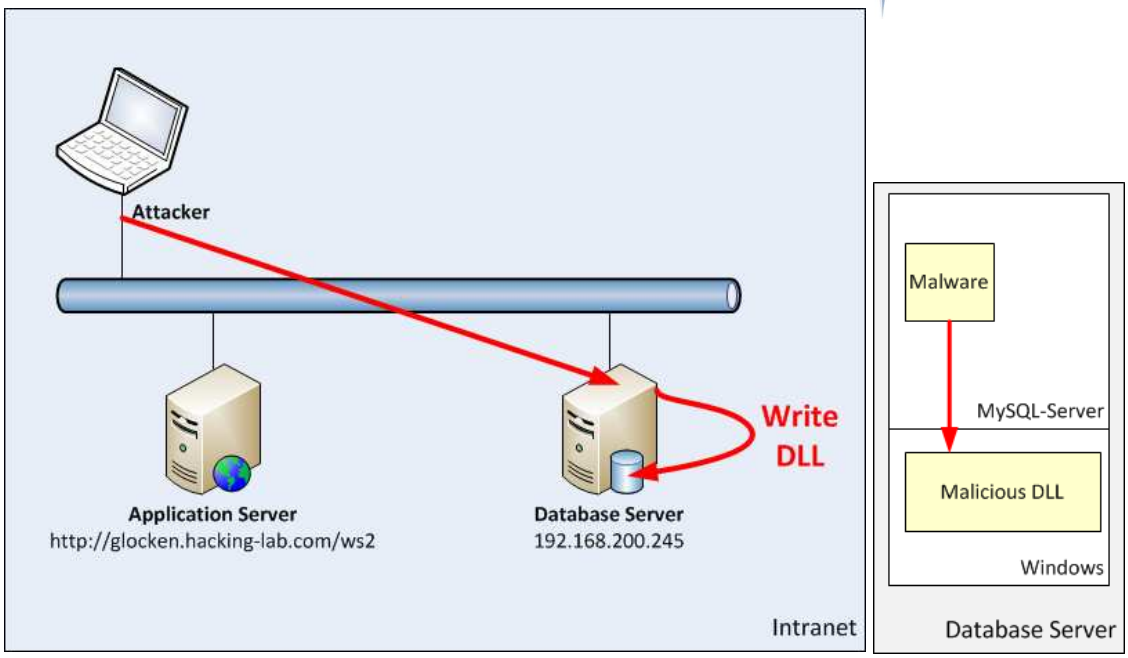
XXE UDF - Live Hacking Demo



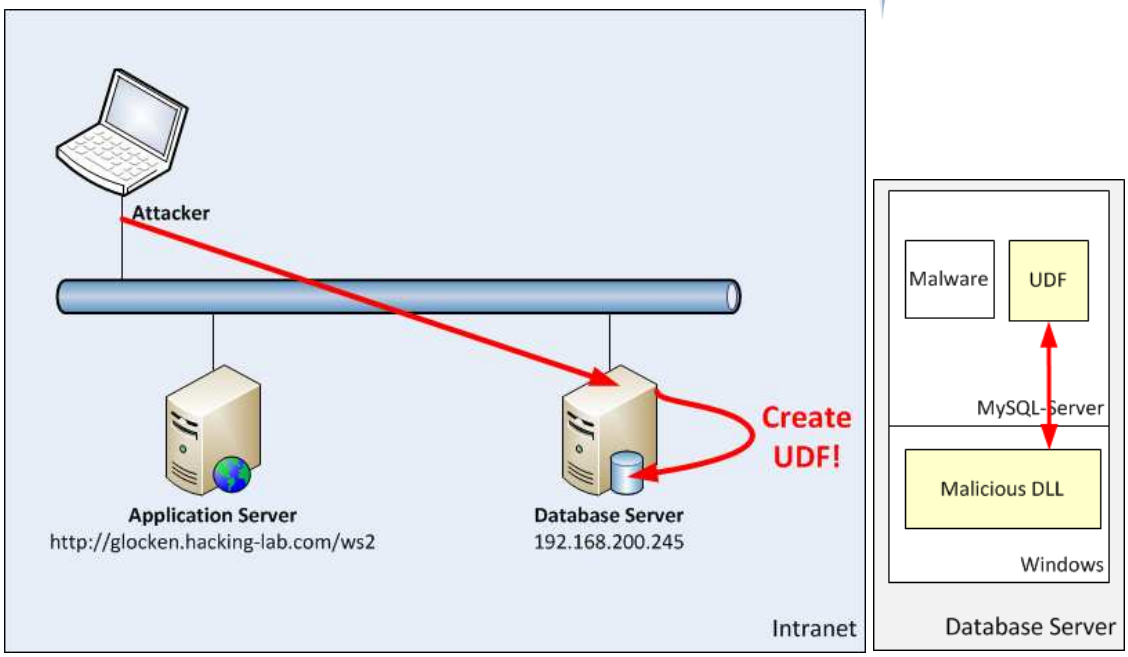
XXE UDF - Live Hacking Demo



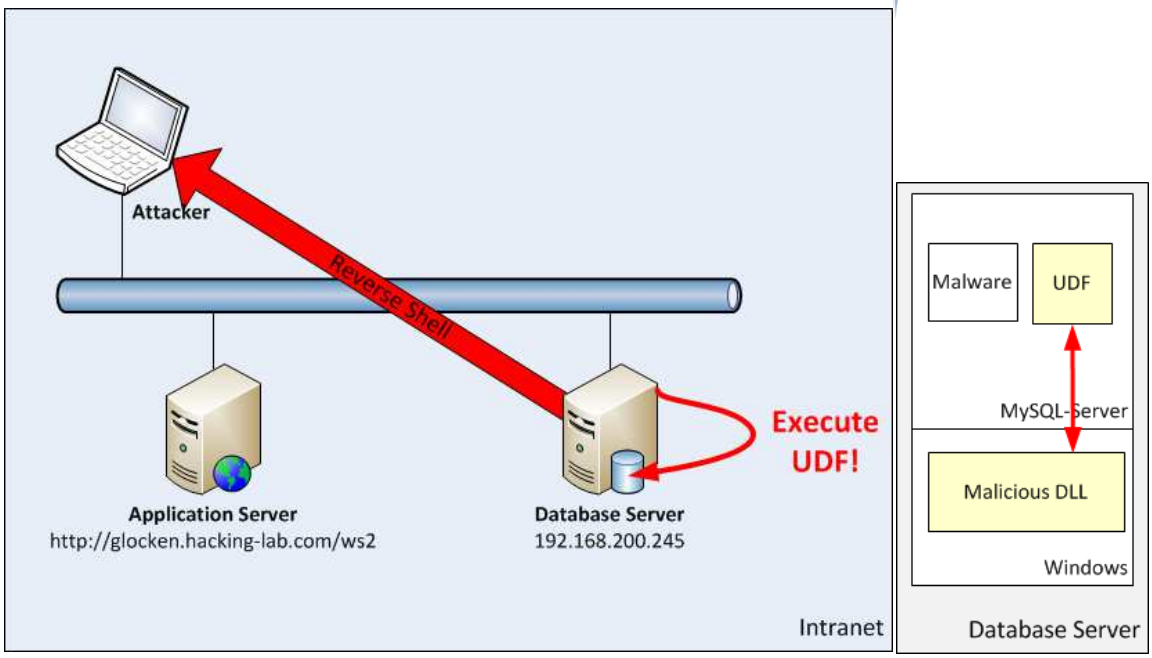
XXE UDF - Live Hacking Demo



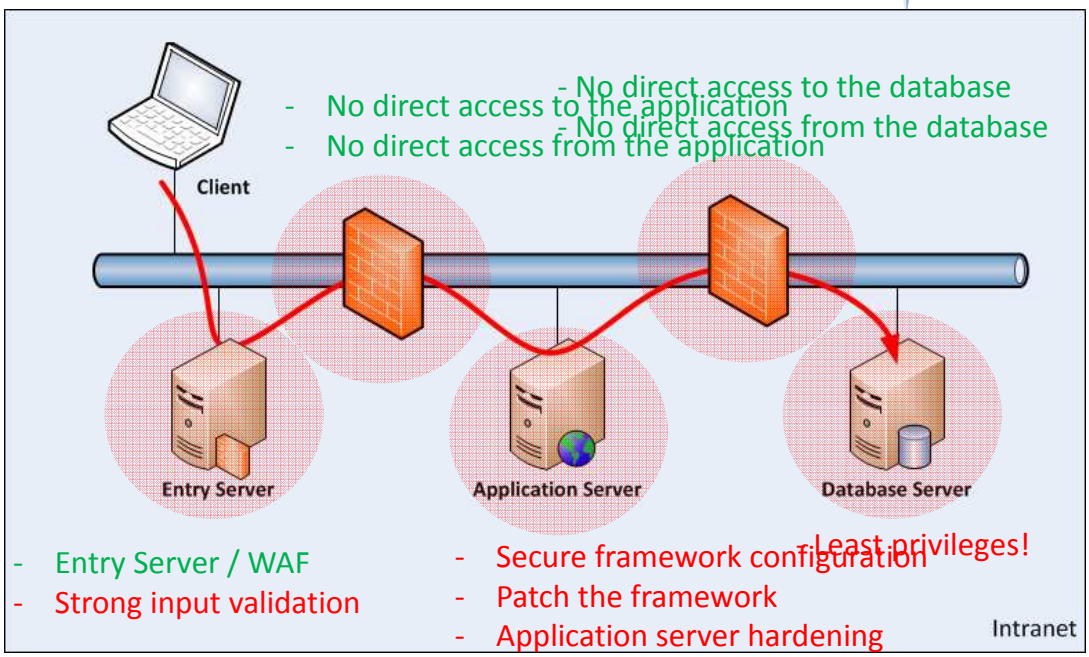
XXE UDF - Live Hacking Demo



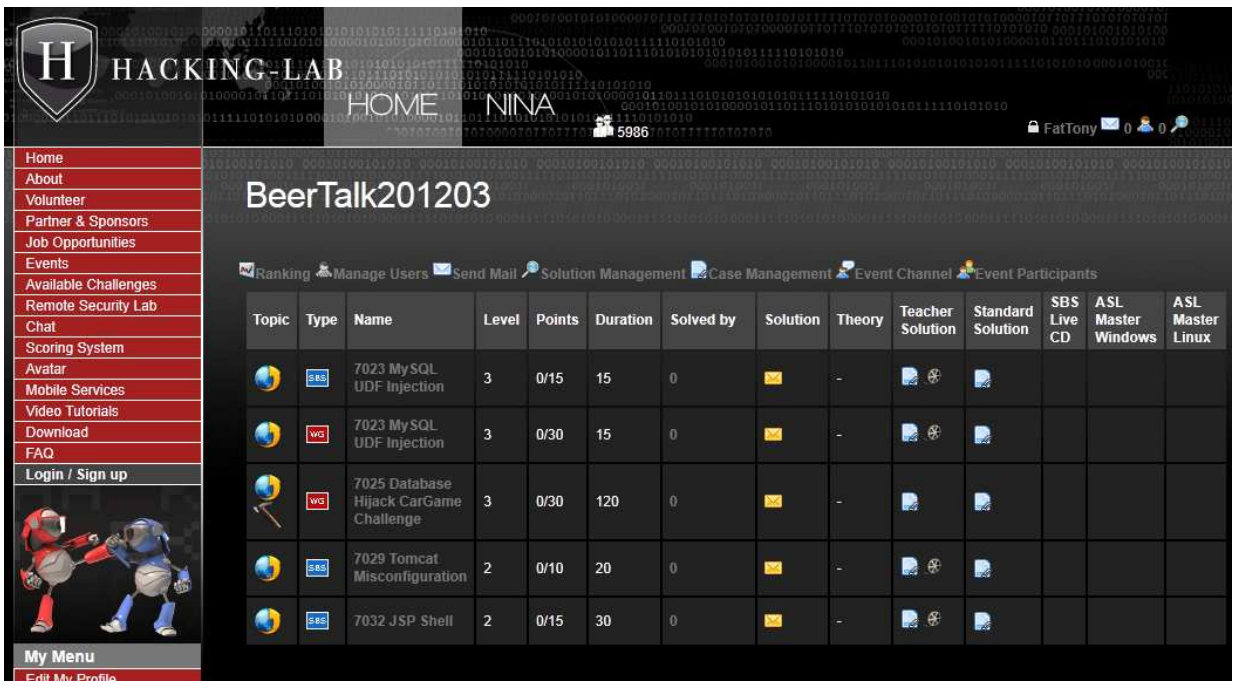
XXE UDF - Live Hacking Demo



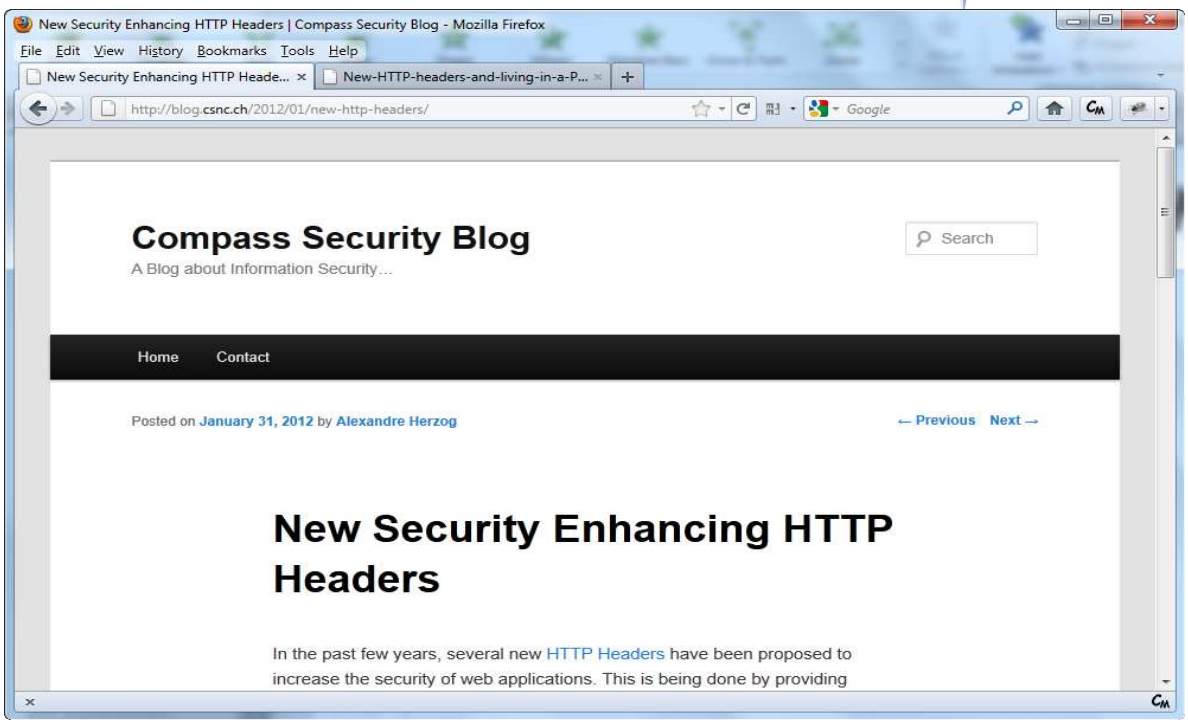
Where can we improve?



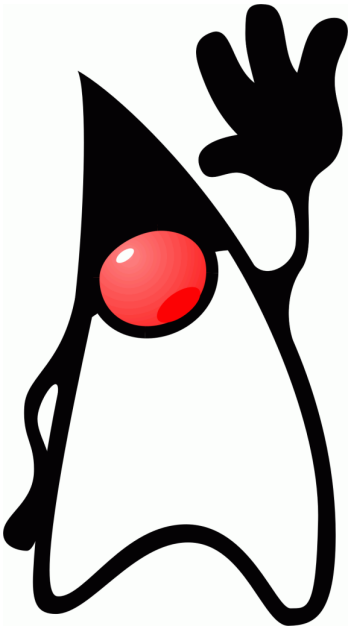
Try it yourself!



Visit: http://blog.csnc.ch



Thank You



References

http://struts.apache.org/2.2.1/docs/s2-003.html

http://struts.apache.org/2.2.1/docs/s2-005.html

http://struts.apache.org/2.x/docs/s2-009.html

http://blog.csnc.ch/2012/01/new-http-headers/