OWASP – ESAPI WAF

Arshan Dabirsiaghi
OWASP Project Lead
Aspect Security
arshan.dabirsiaghi@aspectsecurity.com
(301) 604-4882

AppSec DC
10/12/2009

The OWASP Foundation
http://www.owasp.org

OWASP ESAPI WAF

- Developed by Arshan Dabirsiaghi (w/ Jeff Williams)
- A sub-project under the ESAPI umbrella
- The *Star Trek: TNG* of WAFs

Free

Usable

Robust

Pragmatic

Performant

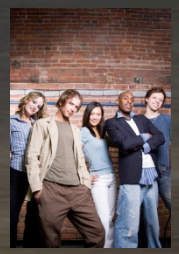
Open Source

"Yeah, well I hate WAFs"

- Perfect! Me too.

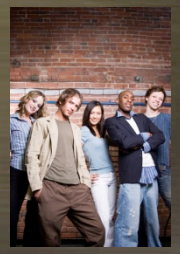
WAF criticism	Is criticism stupid?	Does ESAPI WAF have problem?
WAFs add attack surface	**Yes**	**Yes**
WAFs can create culture problems	**Maybe**	**(not sure, probably)**
WAFs can't fix business logic vulnerabilities	**No**	**No**
WAFs are way too expensive	**No**	**No**
WAFs complicate networks	**No**	**No**

WAFs *were* for Federalists (part 1)



Development Team A

App A



Development Team B

App B

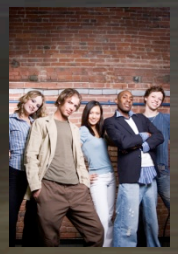
Development Team C

App C

WAF

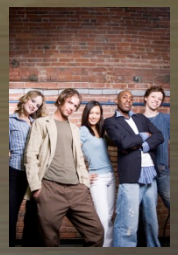
Security Team

WAFs *were* for Federalists (part 2)



Development Team A

App A w/ WAF

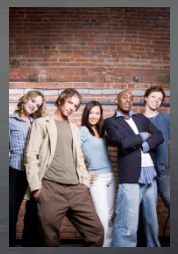


Development Team B

App B w/ WAF

DMZ

App C w/ WAF



Development Team C

Why fix in ESAPI WAF vs. fix in code?

Why fix in ESAPI WAF vs. fix in code?

Advantages of Application-Layer WAFs

- **Performance** – only your rules are checked, plus state is already managed by the app server
- **Capability** – being closer to the app lets us do more and I can't wait to tell you about it
- **Process** – rules are closer to application owner, shortening discovery-to-patch time, also fix-to-patch-removal time

Principle: Make common tasks easy, uncommon tasks possible

```
<virtual-patches>
  <virtual-patch
        id="bugtracker-id-1234"
        path="/vulnerable.do"

variable="request.parameters.bar"
        pattern="[0-9a-zA-Z]*"
        message="zmg attax" />
</virtual-patches>
```

EASY!

POSSIBLE...

STILL EASY!

```
<bean-shell-rules>
  <bean-shell-script
    id="user-lockout-rule"
    file="/
enforce_user_lockout.bsh"
    stage="before-request-
body"/>
</bean-shell-rules>
```

+

```
import org.acme.user.*;
User user =
session.getAttribute("u");
If ( user.isLocked() )
  action = new RedirectAction();
```

Fixing Injection Flaws

XSS

- Fix with input validation virtual patch (black/white list)
- Fix with sanitization (BeanShell script)
- Fix with output encoding (egress rule)

SQL injection

- Fix with input validation virtual patch (black/white list)
- Fix with sanitization (BeanShell script)

Command injection

- Fix with input validation virtual patch (black/white list)
- Fix with sanitization (BeanShell script)

Business Logic Flaws

/ws/ImptWebService.rest **/admin/shutdown** **/viewAccount?id=1826**

Missing Authentication	Missing Functional Access Control	Missing Data Layer Access Control
• YES WE CAN • Presence/value of session variable • Presence of appliance-supplied header • BeanShell script	• YES WE CAN • Check roles in session • Check roles provided by appliance-supplied header • BeanShell script	• YES WE CAN • BeanShell script

Adding “Outbound” Security

Headers

- Add anti-clickjacking header
- Set uniform content-type

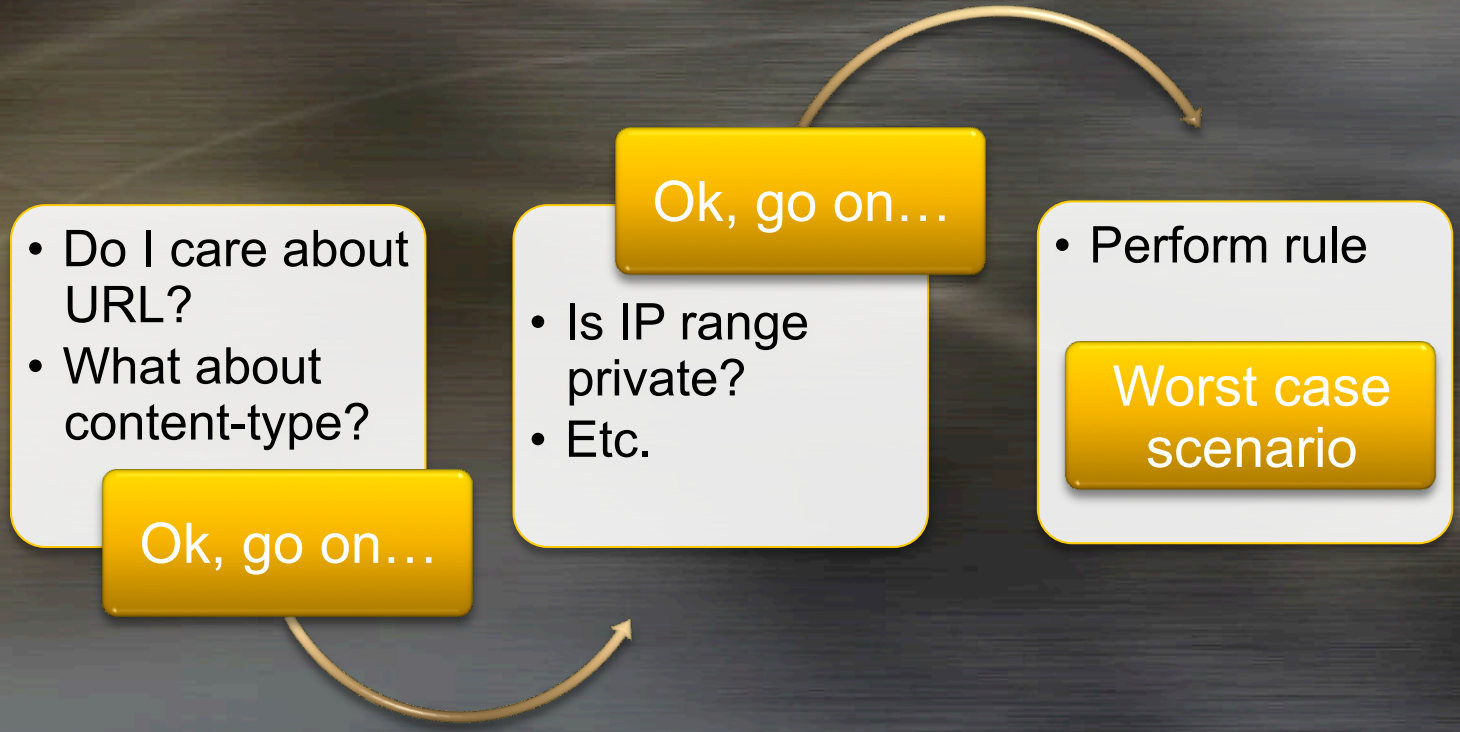
Cookies

- Add HttpOnly flag
- Add secure flag

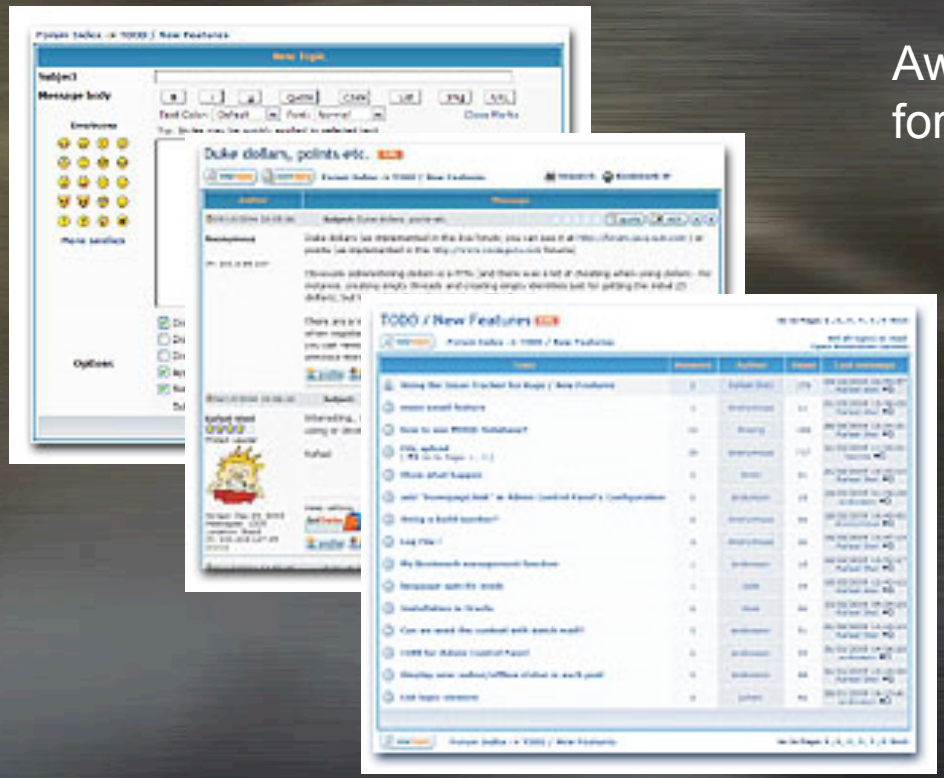
Body

- Detect outbound information
- Replace outbound information

Yes, we know all about early failing

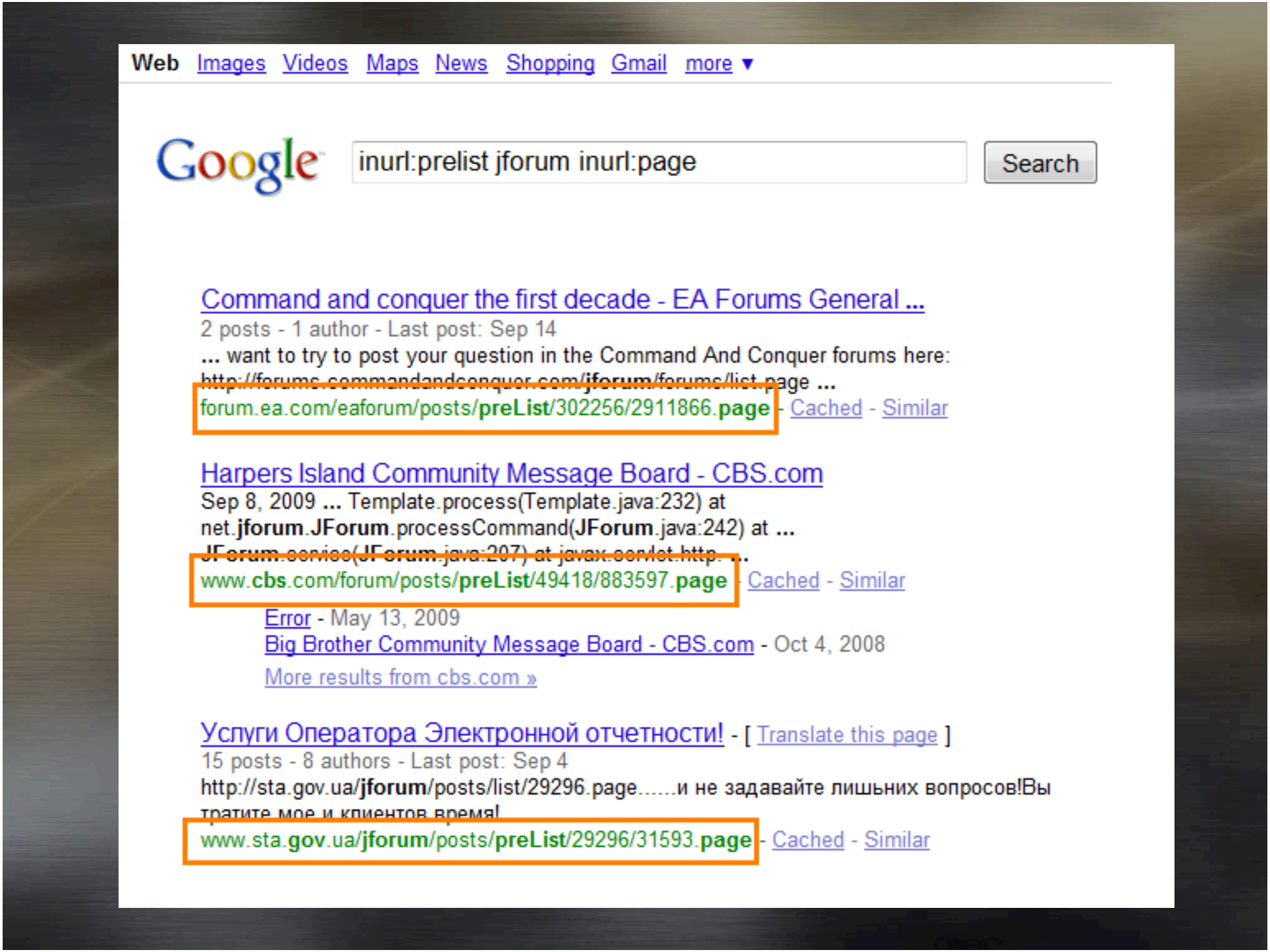


Meet JForum 2.1.8

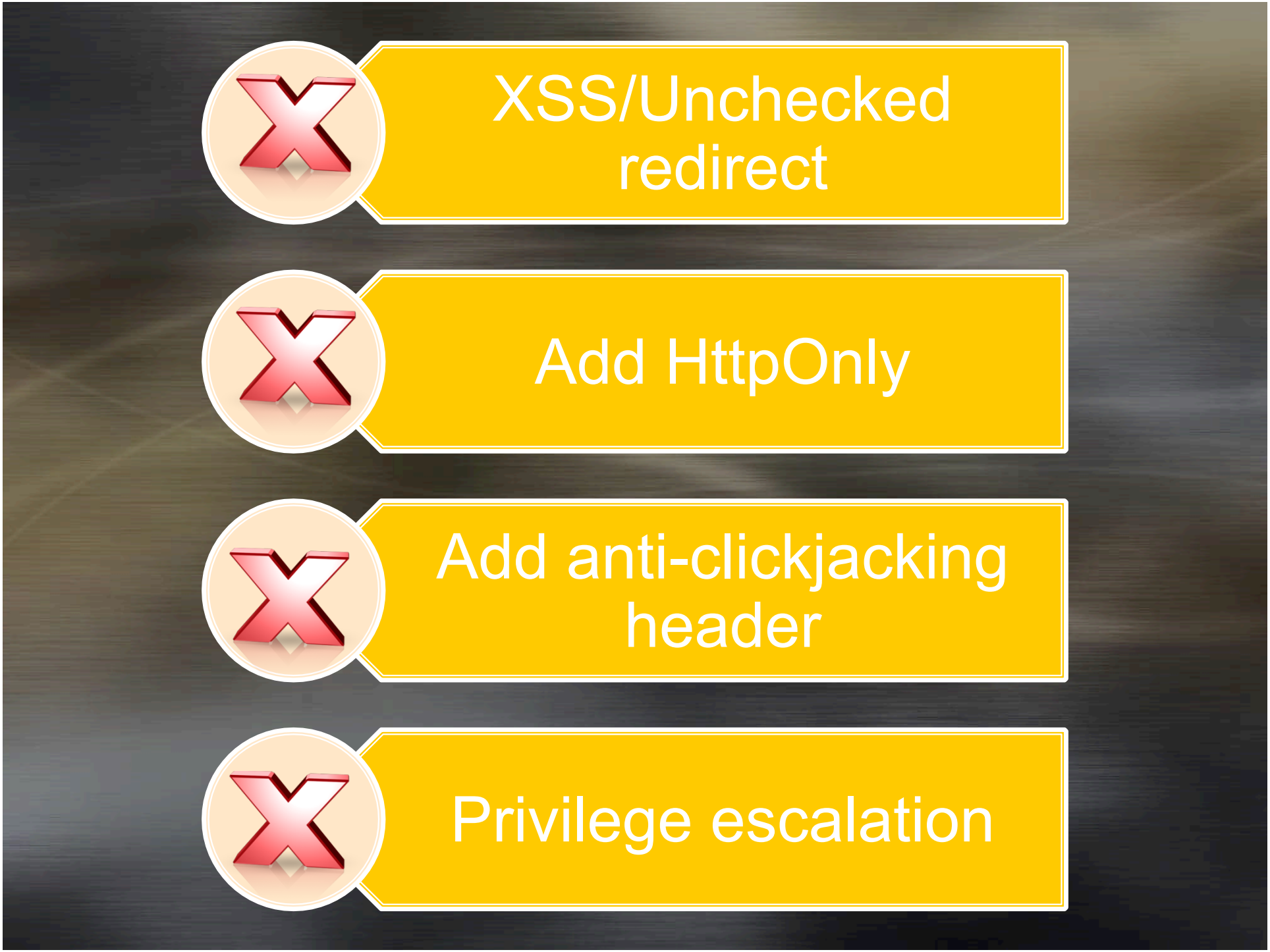


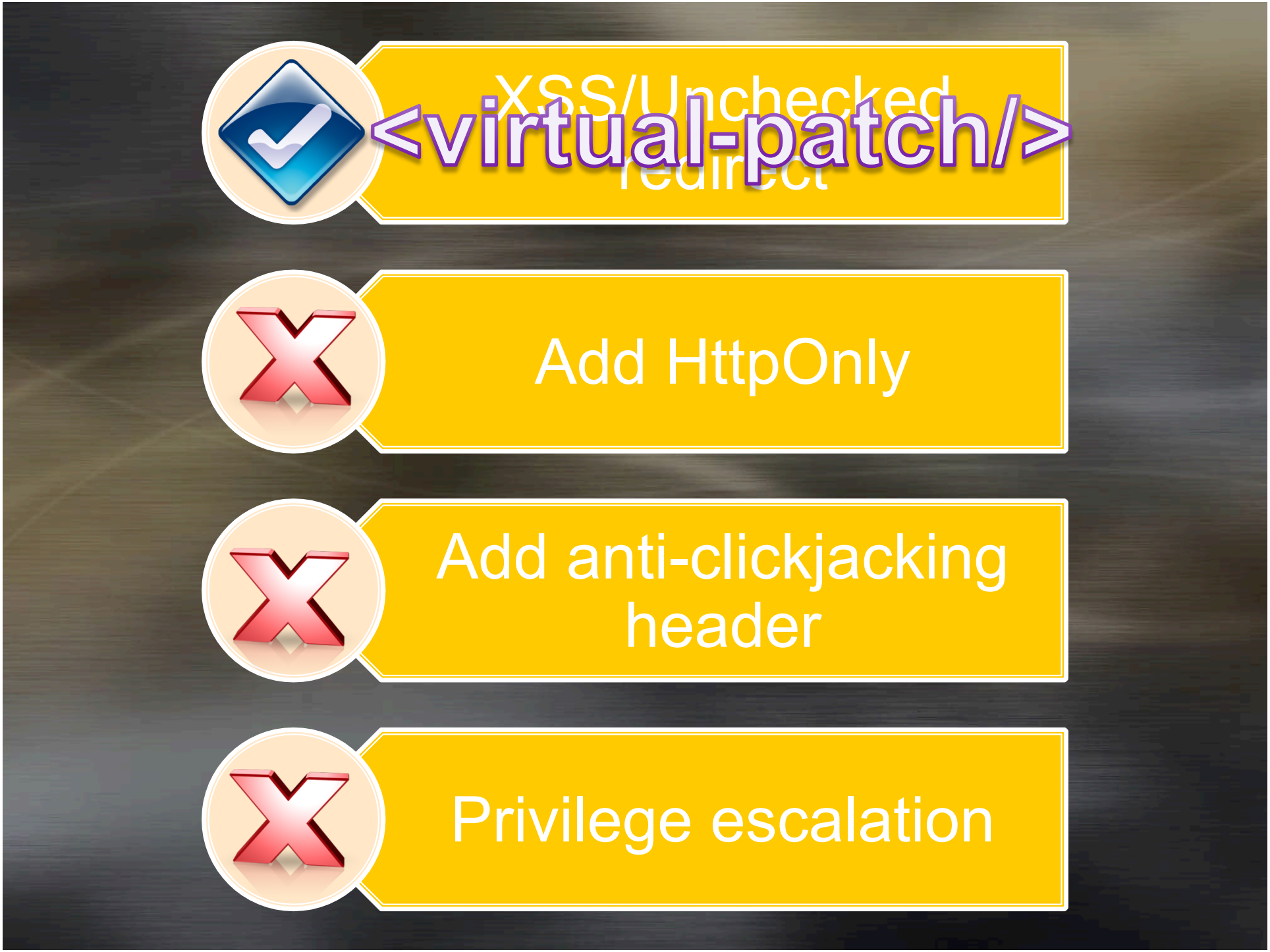
Awesome, free, fully featured forum software.

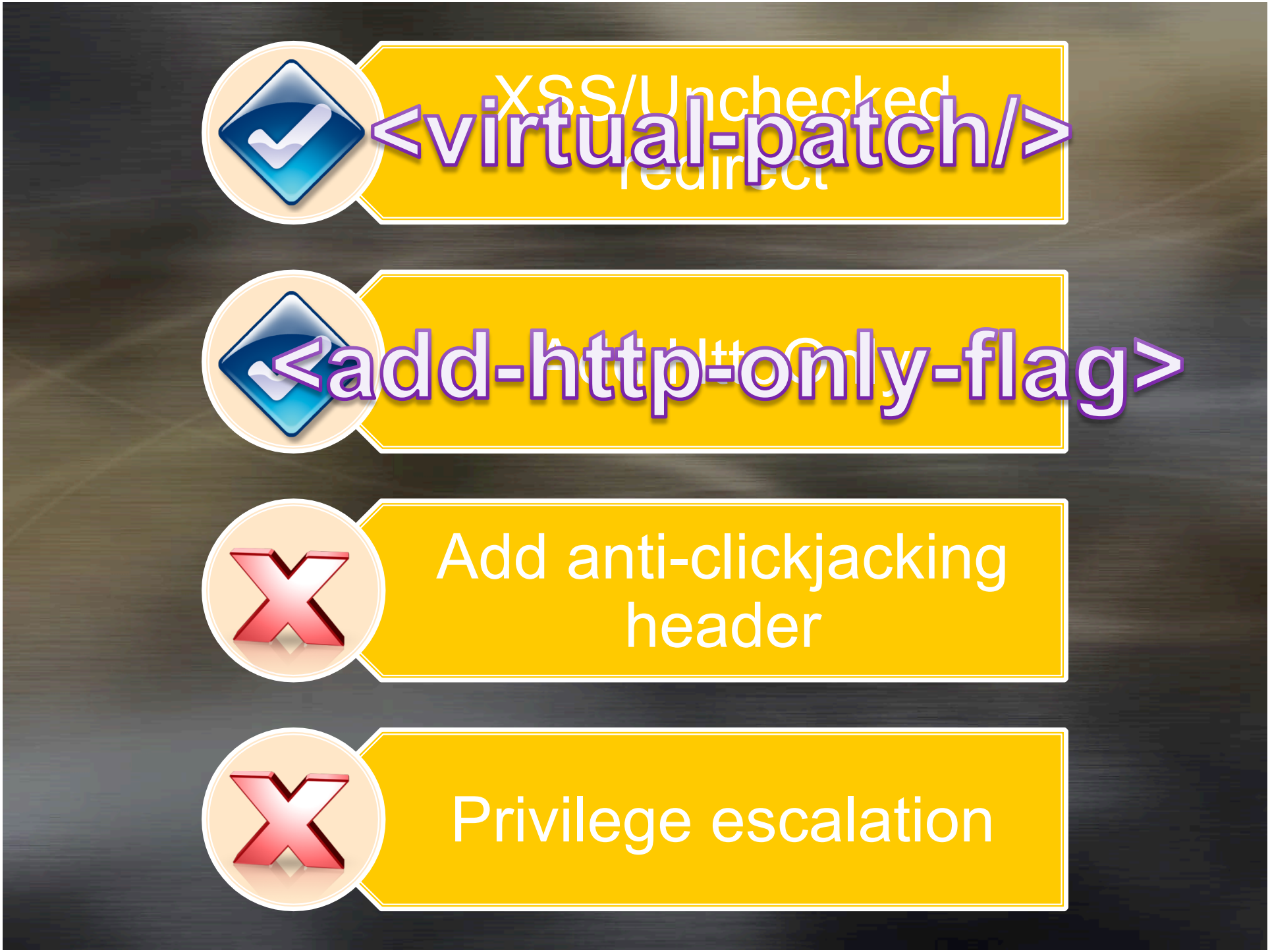
4 hours of code review/pen testing:
10 findings


Web Images Videos Maps News Shopping Gmail more ▼
Google
inurl:prelist jforum inurl:page
Search
Command and conquer the first decade - EA Forums General ...
2 posts - 1 author - Last post: Sep 14
... want to try to post your question in the Command And Conquer forums here:
http://forums.commandandconquer.com/jforum/forums/list.page ...
forum.ea.com/eaforum/posts/preList/302256/2911866.page - Cached - Similar
Harpers Island Community Message Board - CBS.com
Sep 8, 2009 ... Template.process(Template.java:232) at
net.jforum.JForum.processCommand(JForum.java:242) at ...
JForum.service(JForum.java:207) at javax.servlet.http. ...
www.cbs.com/forum/posts/preList/49418/883597.page - Cached - Similar
Error - May 13, 2009
Big Brother Community Message Board - CBS.com - Oct 4, 2008
More results from cbs.com »
Услуги Оператора Электронной отчетности! - [Translate this page]
15 posts - 8 authors - Last post: Sep 4
http://sta.gov.ua/jforum/posts/list/29296.page.....и не задавайте лишьних вопросов!Вы
тратите мое и клиентов время!
www.sta.gov.ua/jforum/posts/preList/29296/31593.page - Cached - Similar


Demo

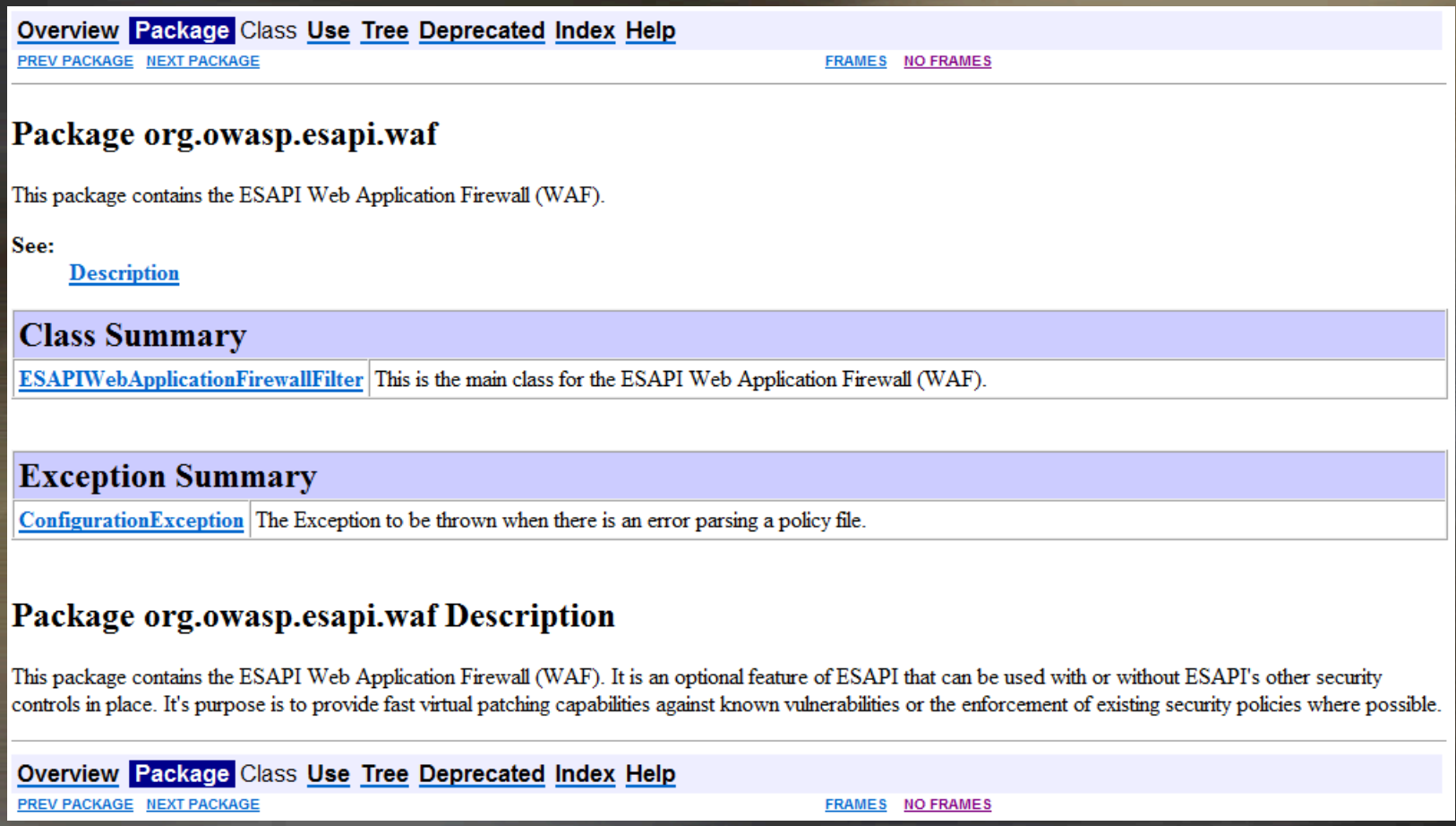

XSS/Unchecked redirect
Add HttpOnly
Add anti-clickjacking header
Privilege escalation


XSS/Unchecked redirect
<virtual-patch/>
Add HttpOnly
Add anti-clickjacking header
Privilege escalation


<virtual-patch/>
<add-http-only-flag>
Add anti-clickjacking header
Privilege escalation


XSS/Unchecked redirect
<virtual-patch/>
<add-http-only-flag>
Add anti-clickjacking header
<add-header/>
Privilege escalation


<virtual-patch/>
<add-http-only-flag>
<add-header/>
<bean-shell-rule/>



Overview Package Class Use Tree Deprecated Index Help

PREV PACKAGE NEXT PACKAGE FRAMES NO FRAMES

Package org.owasp.esapi.waf

This package contains the ESAPI Web Application Firewall (WAF).

See:

Description

Class Summary

ESAPIWebApplicationFirewallFilter	This is the main class for the ESAPI Web Application Firewall (WAF).

Exception Summary

ConfigurationException	The Exception to be thrown when there is an error parsing a policy file.

Package org.owasp.esapi.waf Description

This package contains the ESAPI Web Application Firewall (WAF). It is an optional feature of ESAPI that can be used with or without ESAPI's other security controls in place. It's purpose is to provide fast virtual patching capabilities against known vulnerabilities or the enforcement of existing security policies where possible.

Overview Package Class Use Tree Deprecated Index Help

PREV PACKAGE NEXT PACKAGE FRAMES NO FRAMES

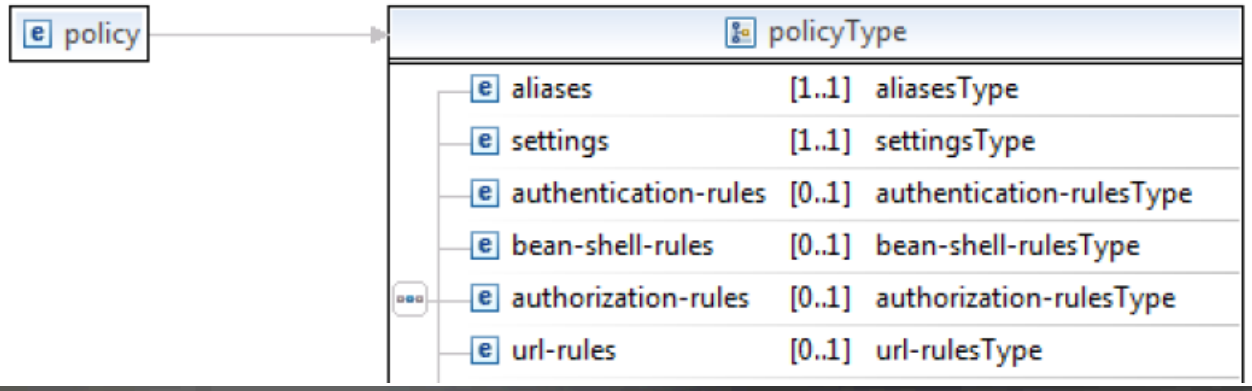
http://owasp-esapi-java.googlecode.com/svn/trunk_doc/2.0-rc3/index.html

JavaDocs

2. The policy file

The ESAPI Web Application Firewall (WAF) is driven by an XML policy file that tells it what rules to enforce in the application. These rules can do a number of things, from simple virtual patching to complex authorization enforcement with BeanShell scripts.

This document describes the structure of the policy file, the individual rules and how they work. There are also a number of examples in order to guide you during implementation. The following picture shows you a visual representation of the policy file XSD, a formal specification for the layout of a policy file:



http://owasp-esapi-java.googlecode.com/svn/trunk/documentation/OWASP%20ESAPI%20WAF%20Configuration%20Guide.pdf

Policy file specification

OWASP ESAPI WAF

AVAILABLE NOW!

$0

Arshan Dabirsiaghi
Director of Research, Aspect Secur
@nahsra, i8<messiah>.com
http://www.aspectsecurity.com/