S2-006

Summary

Multiple Cross-Site Scripting (XSS) in XWork generated error pages

Who should read this	All Struts 2 developers
Impact of vulnerability	Injection of malicious client side code
Maximum security rating	Important
Recommendation	Developers should either upgrade to Struts 2.2.3 or apply the configuration changes described below
Affected Software	Struts 2.0.0 - Struts 2.2.1.1
Original JIRA Tickets	WW-3579
Reporter	Dr. Marian Ventuneac, Genworth
CVE Identifier	CVE-2011-1772

Problem

By default, XWork doesn't escape action's names in automatically generated error page, allowing for a successful XSS attack. When Dynamic Method Invocation (DMI) is enabled, the action name is generated dynamically base on request parameters. This allows to call non-existing page and method to produce error page with injected code as below

http://localhost:8080/struts2-blank/home.action!login:cantLogin<script>alert(document.cookie)</script>=some_value

A more detailed description is found in the referenced JIRA ticket.

Solution

As of Struts 2.2.3 the action names are escaped when automatically generated error pages are rendered.

When staying with earlier releases, developers should either

- Disable DMI support in struts.xml

```
<constant name="struts.enable.DynamicMethodInvocation" value="false" />
```

or

- Define error page in struts.xml (as below)

```
<global-results>
  <result name="error">/error_page.jsp</result>
</global-results>

<global-exception-mappings>
  <exception-mapping exception="java.lang.Exception" result="error"/>
</global-exception-mappings>
```

You can obtain Struts 2.2.3 here.