

Audit Report

WebApp Throwdown

Audited on January 11 2010

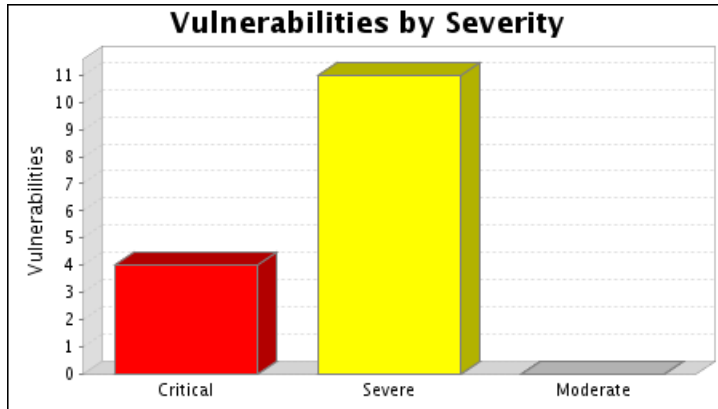
Reported on January 12 2010

1. Executive Summary

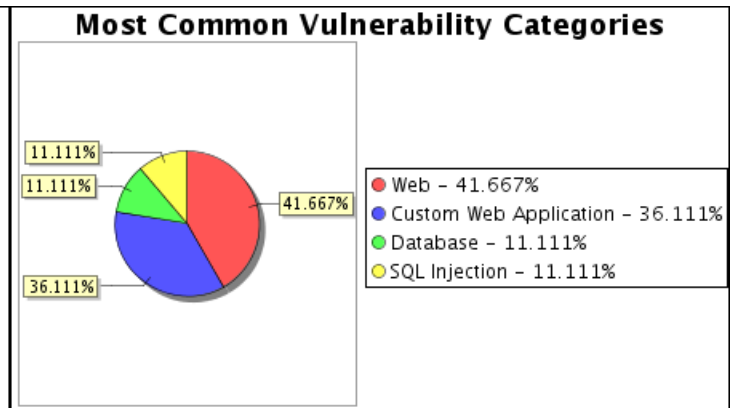
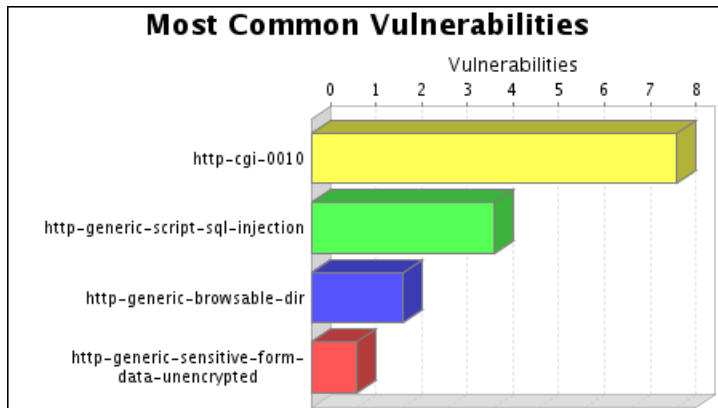
This report represents a security audit performed by NeXpose from Rapid7 LLC. It contains confidential information about the state of your network. Access to this information by unauthorized personnel may allow them to compromise your network.

| Site Name | Start Time | End Time | Total Time | Status |
|------------------|-----------------------------|-----------------------------|------------|---------|
| WebApp Throwdown | January 11, 2010 17:33, EST | January 11, 2010 17:41, EST | 7 minutes | Success |

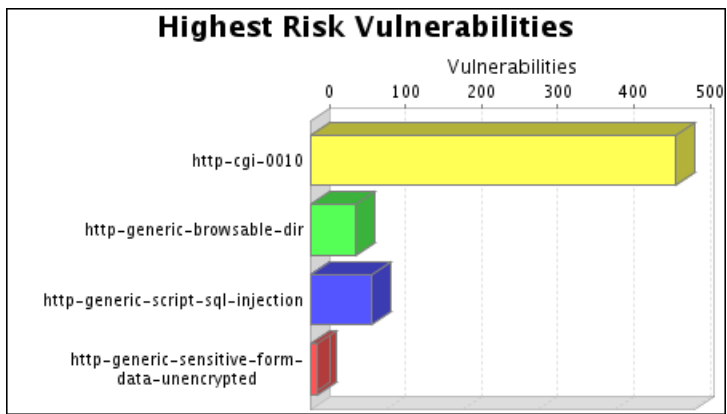
The audit was performed on one system which was found to be active and was scanned.



There were 15 vulnerabilities found during this scan. Of these, 4 were critical vulnerabilities. Critical vulnerabilities require immediate attention. They are relatively easy for attackers to exploit and may provide them with full control of the affected systems. 11 vulnerabilities were severe. Severe vulnerabilities are often harder to exploit and may not provide the same access to affected systems. There were no moderate vulnerabilities discovered. These often provide information to attackers that may assist them in mounting subsequent attacks on your network. These should also be fixed in a timely manner, but are not as urgent as the other vulnerabilities.



There were 8 occurrences of the http-cgi-0010 vulnerability, making it the most common vulnerability. There were 15 vulnerabilities in the Web category, making it the most common vulnerability category.



The http-cgi-0010 vulnerability poses the highest risk to the organization with a risk score of 480. Vulnerability risk scores are calculated by looking at the likelihood of attack and impact, based upon CVSS metrics. The impact and likelihood are then multiplied by the number of instances of the vulnerability to come up with the final risk score.

One operating system was identified during this scan.

One service was found to be running during this scan.

2. Discovered Systems

| Node | Operating System | Risk | Aliases |
|---------------|-------------------------------|------|--------------------|
| 65.61.137.117 | Microsoft Windows Server 2003 | 1.51 | •demo.testfire.net |

3. Discovered and Potential Vulnerabilities

3.1. Critical Vulnerabilities

3.1.1. SQL Injection Vulnerability (http-generic-script-sql-injection)

Description:

Web applications that do not properly sanitize user input before passing it to a database system are vulnerable to SQL injection. This type of attack potentially allows a malicious user to recover and/or modify any data that the application has access to.

Affected Nodes:

| Affected Nodes: | Additional Information: |
|------------------|--|
| 65.61.137.117:80 | Injected into the "uid" form parameter on http://demo.testfire.net/bank/login.aspx : 34: <h1>An Error Has Occurred</h1> 35: 36: <h2>Summary:</h2> 37: 38: ...t_lblSummary">Syntax error in string in query expression 'username ... |
| 65.61.137.117:80 | Injected into the "uid" form parameter on http://demo.testfire.net/bank/login.aspx : 34: <h1>An Error Has Occurred</h1> 35: 36: <h2>Summary:</h2> 37: 38: ...t_lblSummary">Syntax error in string in query expression 'username ... |
| 65.61.137.117:80 | Injected into the "passw" form parameter on http://demo.testfire.net/bank/login.aspx : 34: <h1>An Error Has Occurred</h1> 35: 36: <h2>Summary:</h2> 37: 38: ...t_lblSummary">Syntax error in string in query expression 'username ... |
| 65.61.137.117:80 | Injected into the "passw" form parameter on http://demo.testfire.net/bank/login.aspx : 34: <h1>An Error Has Occurred</h1> 35: 36: <h2>Summary:</h2> 37: |

Audit Report

| Affected Nodes: | Additional Information: |
|-----------------|---|
| | 38: ...t_lblSummary">Syntax error in string in query expression 'username |

References:

| Source | Reference |
|--------|---|
| URL | http://en.wikipedia.org/wiki/Sql_injection |
| URL | http://msdn2.microsoft.com/en-us/library/ms161953.aspx |
| URL | http://www.owasp.org/index.php/SQL_injection |

Vulnerability Solution:

Ensure that the script properly validates user input before passing it to the underlying database system.

3.2. Severe Vulnerabilities

3.2.1. Cross Site Scripting Vulnerability (http-cgi-0010)

Description:

The web application is vulnerable to cross-site scripting (XSS). Cross-site scripting vulnerabilities allow malicious attackers to take advantage of web server scripts to inject JavaScript or HTML code that is executed on the client-side browser. This is often caused by server-side scripts written in languages such as PHP, ASP, .NET, Perl or Java that do not adequately filter data sent along with page requests. This malicious code will appear to come from your web application when it runs in the browser of an unsuspecting user.

An exploit script can be made to:

- access other sites inside another client's private intranet.
- steal another client's cookie(s).
- modify another client's cookie(s).
- steal another client's submitted form data.
- modify another client's submitted form data (before it reaches the server).
- submit a form to your application on the user's behalf which modifies passwords or other application data

The two most common methods of attack are:

- Clicking on a URL link sent in an e-mail
- Clicking on a URL link while visiting a website

In both scenarios, the URL will generally link to the trusted site, but will contain additional data that is used to trigger the XSS attack.

Audit Report

Note that SSL connectivity does not protect against this issue.

Affected Nodes:

| Affected Nodes: | Additional Information: |
|------------------|---|
| 65.61.137.117:80 | Detected successful persistent XSS injection in http://demo.testfire.net/comments.txt 1: , test@example.com, test, </XSS/*-*/STYLE=xss:e/**/xpression(nxpsstes... |
| 65.61.137.117:80 | Injected into the "aspxerrorpath" URL parameter in http://demo.testfire.net/notfound.aspx?aspxerrorpath=/Citrix/MetaFrame/auth/login.aspx by changing the URL to <a href="http://demo.testfire.net/notfound.aspx?aspxerrorpath=<script>nxpsstest">http://demo.testfire.net/notfound.aspx?aspxerrorpath=<script>nxpsstest 75: <div class="fl" style="width: 99%; "> 76: 77: <h1>An Error Has Occurred</h1> 78: 79: <p>Could not find the page y... |
| 65.61.137.117:80 | Injected into the "txtSearch" form parameter on http://demo.testfire.net/search.aspx : 76: 77: <h1>Search Results</h1> 78: 79: <p>No results were found for the query: 80: <script>nxpsstest</span... |
| 65.61.137.117:80 | Injected into the "txtSearch" form parameter on http://demo.testfire.net/search.aspx : 76: 77: <h1>Search Results</h1> 78: 79: <p>No results were found for the query: 80: <script>nxpsstest</span... |
| 65.61.137.117:80 | Injected into the "uid" form parameter on http://demo.testfire.net/bank/login.aspx : 85: <td> 86: Username: 87: </td> 88: <td> 89: <input type="text" id="uid" name="uid" value="<script>nxpsste... |
| 65.61.137.117:80 | Injected into the "uid" form parameter on http://demo.testfire.net/bank/login.aspx : 85: <td> 86: Username: 87: </td> 88: <td> 89: <input type="text" id="uid" name="uid" value="<script>nxpsste... |
| 65.61.137.117:80 | Injected into the "name" form parameter on http://demo.testfire.net/comment.aspx : 75: <div class="fl" style="width: 99%; "> |

Audit Report

| Affected Nodes: | Additional Information: |
|------------------|--|
| | 76: 77: <h1>Thank You</h1> 78: 79: <p>Thank you for your comments, <script>npxsstest. They will be rev... |
| 65.61.137.117:80 | Injected into the "name" form parameter on http://demo.testfire.net/comment.aspx : 75: <div class="fl" style="width: 99%;"> 76: 77: <h1>Thank You</h1> 78: 79: <p>Thank you for your comments, <script>npxsstest. They will be rev... |

References:

| Source | Reference |
|--------|---|
| CERT | CA-2000-02 |
| URL | http://en.wikipedia.org/wiki/Cross_site_scripting |

Vulnerability Solution:

Audit the affected url and other similar dynamic pages or scripts that could be relaying untrusted malicious data from the user input. In general, the following practices should be followed while developing dynamic web content:

- Explicitly set the character set encoding for each page generated by the web server
- Identify special characters
- Encode dynamic output elements
- Filter specific characters in dynamic elements
- Examine cookies

For more information on the above practices, read the following CERT advisory: [CERT Advisory CA-2000-02](#)

- For ASP.NET applications, the validateRequest attribute can be added to the page or the web.config. For example:

```
<%@ Page ... validateRequest="true" %>
```

OR

```
<system.web>  
  <pages validateRequest="true" />  
</system.web>
```

In addition, all dynamic content should be HTML encoded using `HTTPUtility.HtmlEncode`.

- For PHP applications, input data should be validated using functions such as `strip_tags` and `utf8_decode`. Dynamic content should be HTML encoded using `htmlspecialchars`.

- For Perl applications, input data should be validated whenever possible using regular expressions. Dynamic content should be HTML encoded using `HTML::Entities::encode` or `Apache::Util::html_encode` (when using `mod_perl`).

3.2.2. Browsable web directory (`http-generic-browsable-dir`)

Description:

A web directory was found to be browsable, which means that anyone can see the contents of the directory. These directories can be found:

- via page spidering (following hyperlinks), or
- as part of a parent path (checking each directory along the path and searching for "Directory Listing" or similar strings), or
- by brute forcing a list of common directories.

Browsable directories could allow an attacker to view "hidden" files in the web root, including CGI scripts, data files, or backup pages.

Affected Nodes:

| Affected Nodes: | Additional Information: |
|------------------|---|
| 65.61.137.117:80 | http://demo.testfire.net/bank/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 1: <html><head><META http-equiv="Content-Type" content="text/html; cha... 2: 3: <pre> [To Parent Directory] 1/22/2007 4:17 PM ... |
| 65.61.137.117:80 | http://demo.testfire.net/bank/ 1: <html><head><META http-equiv="Content-Type" content="text/html; cha... 2: 3: <pre> [To Parent Directory] 1/22/2007 4:17 PM ... |

References:

None

Vulnerability Solution:

- Apache

Disable web directory browsing for all directories and subdirectories

In your `httpd.conf` file, disable the "Indexes" option for the appropriate `<Directory>` tag by removing it from the Options line.

In addition, you should always make sure that proper permissions are set on all files and directories within the web root (including CGI scripts and backup files). Do not copy files in the web root unless you want these files to be available over the web. Periodically go

through your web directories and clean out any unused, obsolete, or unknown files and directories.

- IIS, PWS, Microsoft-IIS, Internet Information Server, Internet Information Services, Microsoft-PWS

Disable web directory browsing for all directories and subdirectories

In the Internet Information Services control panel or MMC, choose the appropriate virtual directory entry and select Properties.

Uncheck the 'Allow Directory Browsing' option.

In addition, you should always make sure that proper permissions are set on all files and directories within the web root (including CGI scripts and backup files). Do not copy files in the web root unless you want these files to be available over the web. Periodically go through your web directories and clean out any unused, obsolete, or unknown files and directories.

- Java System Web Server, iPlanet

Disable web directory indexing for all directories and subdirectories

The iPlanet web server indexes directories by searching the directory for an index file (by default index.html or home.html). If an index file is not found, the Document Preferences settings are checked to see what the Directory Indexing setting contains. This should be set to None to disable directory indexing.

For older versions of iPlanet that do not support the Directory Indexing setting, create a file called index.html or home.html in each directory. This page will then be served instead of a directory listing.

- Apache Tomcat, Tomcat, Tomcat Web Server, Apache Coyote, Apache-Coyote

Disable web directory browsing for all directories and subdirectories

Edit Tomcat's web.xml file. In the "default" servlet, change the "listings" parameter from "true" to "false". Restart the server.

In addition, you should always make sure that proper permissions are set on all files and directories within the web root (including CGI scripts and backup files). Do not copy files in the web root unless you want these files to be available over the web. Periodically go through your web directories and clean out any unused, obsolete, or unknown files and directories.

3.2.3. Form action submits sensitive data in the clear ([http-generic-sensitive-form-data-unencrypted](#))

Description:

A web form contains fields with data that is probably sensitive in nature. This form data is submitted over an unencrypted connection, which could allow hackers to sniff the network and view the data in plaintext.

Affected Nodes:

| Affected Nodes: | Additional Information: |
|------------------|--|
| 65.61.137.117:80 | Form with action http://demo.testfire.net/bank/login.aspx submits the following sensitive fields unencrypted: passw |

References:

None

Vulnerability Solution:

Enable the HTTPS protocol on the server. Change the "action" URL of the form tag to use the HTTPS protocol ("https://...") instead of just the HTTP protocol ("http://..."). All sensitive data should be sent over HTTPS instead of over HTTP.

3.3. Moderate Vulnerabilities

No moderate vulnerabilities were reported.

4. Discovered Services

4.1. HTTP

HTTP, the HyperText Transfer Protocol, is used to exchange multimedia content on the World Wide Web. The multimedia files commonly used with HTTP include text, sound, images and video.

4.1.1. General Security Issues

Simple authentication scheme

Many HTTP servers use BASIC as their primary mechanism for user authentication. This is a very simple scheme that uses base 64 to encode the cleartext user id and password. If a malicious user is in a position to monitor HTTP traffic, user ids and passwords can be stolen by decoding the base 64 authentication data. To secure the authentication process, use HTTPS (HTTP over TLS/SSL) connections to transmit the authentication data.

4.1.2. Discovered Instances of this Service

| Device | Protocol | Port | Vulnerabilities | Additional Information |
|---------------|----------|------|-----------------|--|
| 65.61.137.117 | tcp | 80 | 2 | <ul style="list-style-type: none">•Microsoft IIS 6.0•ASP.NET:•http.banner: Microsoft-IIS/6.0•http.banner.server: Microsoft-IIS/6.0•http.banner.x-powered-by: ASP.NET•verbs-1: GET•verbs-2: HEAD•verbs-3: OPTIONS•verbs-4: POST•verbs-5: TRACE•verbs-count: 5 |

5. Discovered Users and Groups

No user or group information was discovered during the scan.

6. Discovered Databases

No database information was discovered during the scan.

7. Discovered Files and Directories

No file or directory information was discovered during the scan.

8. Policy Evaluations

No policy evaluations were performed.

9. Spidered Web Sites

9.1. <http://65.61.137.117:80>

9.1.1. Common Default URLs

The following URLs were guessed. They are often included with default web server or web server add-on installations.

Access Error (403)

- [admin](#)
- [aspnet_client](#)
 - [system_web](#)
- [images](#)
- [transfer](#)

Redirect (302)

- Citrix
- MetaFrame
 - [auth](#)
 - [login.aspx](#)
- [ScriptResource.axd?d=test](#)
- [WebResource.axd?d=test](#)

Successful (200)

- [static](#)
- [test.aspx](#)

9.1.2. Guessed URLs

The following URLs were guessed using various tricks based on the discovered web site content.

Access Error (403)

- [admin](#)
- [?P=+ADw-script+AD4-alert\(42\)+ADw-](#)
 - [script+AD4-](#)
 - [script+AD4-](#)
 - [script+AD4-](#)
 - [script+AD4-](#)
- [aspnet_client](#)
- [bank](#)
- [20060308_bak](#)
- [Trace.axd](#)

- [Web.sitemap](#)

- [web.config](#)

- images

- [Trace.axd](#)

- [Web.sitemap](#)

- [web.config](#)

- transfer

Error (400)

- "[<script>TestScriptValueHere<](#)

- [script>"](#)

- [script>"](#)

- Citrix

- MetaFrame

- auth

- login.aspx

- [<script>xss<](#)

- [script>](#)

- [script>](#)

- [script>](#)

- [script>](#)

- [script>](#)

- [script>](#)

- [script>](#)

- [script>](#)

- [script>](#)

- [script>](#)

- [script>](#)

- [script>](#)

- [script>](#)

- [script>](#)

- [script>](#)

- [script>](#)

- [script>](#)

- [script>](#)

- [script>](#)

- [script>](#)

- [script>](#)

- [script>](#)

- [script>](#)

- [script>](#)

- bank
 - account.aspx
 - apply.aspx
 - customize.aspx
 - default.aspx
 - index.aspx
 - logout.aspx
 - main.aspx
 - members
 - [%3f.jsp%00](#)
 - queryxpath.aspx
 - servererror.aspx
 - transaction.aspx
 - transfer.aspx
- bug.aspx
- comment.aspx
- feedback.aspx
- search.aspx
- static
 - survey_questions.aspx
- test.aspx

Redirect (302)

- [Trace.axd](#)

- [Trace.axd](#)

- admin
 - [Trace.axd](#)

- bank
 - [Trace.axd](#)
 - [default.aspx](#)
 - [index.aspx](#)

- [index.aspx](#)

- [index.aspx](#)

- [index.aspx](#)

- static
 - [Trace.axd](#)
 - [index.aspx](#)

- [Trace.axd](#)

- [index.aspx](#)

- transfer
 - [Trace.axd](#)

- [Trace.axd](#)

- [comments.txt](#)
- static
- [default.htm](#)

9.1.3. Linked URLs

The following URLs were found as links in the content of other web pages.

Access Error (403)

- bank
- [20060308_bak](#)

Error (500)

- bank
- [customize.aspx](#)
- [queryxpath.aspx](#)
- [comment.aspx](#)

Redirect (302)

- bank
- [account.aspx](#)
- [account.aspx.cs](#)
- [apply.aspx](#)
- [apply.aspx.cs](#)
- [bank.master](#)
- [bank.master.cs](#)
- [customize.aspx.cs](#)
- [login.aspx.cs](#)
- [logout.aspx](#)
- [logout.aspx.cs](#)
- [main.aspx](#)
- [main.aspx.cs](#)
- [queryxpath.aspx.cs](#)
- [transaction.aspx](#)
- [transaction.aspx.cs](#)
- [transfer.aspx](#)
- [transfer.aspx.cs](#)
- static
- [default.aspx?content=personal_savings.htm](#)
- [survey_questions.aspx](#)

Requires Authentication (401)

- bank
- [members](#)

Successful (200)

- bank
- [login.aspx](#)
- [mozxpath.js](#)
- [servererror.aspx](#)
- [ws.asmx](#)
- [bug.aspx](#)
- [default.aspx](#)
- [feedback.aspx](#)
- [search.aspx](#)
- servererror.aspx?aspxerrorpath=
 - [Trace.axd](#)
- [style.css](#)
- [survey_questions.aspx](#)