Performing a Web Application Security Assessment
Coordinate the Time of the Audit

- Set up a time window with the application owner
- Inform your security team
- Inform Web Operations (WebOps)
Scanning Environment

- An automated security scan could potentially affect your application
  - Overload the web and application servers
  - Cause denial of service
  - Insert junk data, e.g. post messages on a message board, send multiple e-mails, etc.

- It preferable to scan applications in pre-production

- Scan applications in production with caution
Get to Know the Site

- Site Model
  - What would be a good starting point?
  - Are there links to more than one host?
  - Are there parts of the site that should be excluded from the scan?
  - Is execution of JavaScript used for application flow?
  - Does your site contain FLASH?
  - Are there pages that require special user input?

- Authentication
  - What type of authentication does your web application use?
  - Does your system allow concurrent logins?
  - Does your authentication system disable your user account after x number of invalid login attempts?
Configuring and Running a Scan – Quick Scan UI

- Makes creating a scan simpler
- Scan is based on a predefined template
- User typically specifies
  - Starting URL
  - Login sequence
  - Pages to Scan (Manual Explore)
Creating a Scan Walkthrough
Creating a Scan – Specify Name and Template

- Specify Name
- Specify Template
- Click Create
Creating a Scan – Recording a Login Sequence

- Click **Record**
- Allows ASE to authenticate to the application

**Properties**

- **Type:** Developer

**Configuration**

**Login Sequence**

⚠️ Please make sure you are not already logged in to the site before recording a new login sequence. If you are already logged in, log out of the site and then re-record the login sequence.

![Record Button]

There are no items available.

[Save and Run, Save, Cancel]
Creating a Scan – Recording a Login Sequence (cont.)

- ASE Browser
- Login to your app/site
- Click the Stop button or close the browser
Creating a Scan – Specifying a Starting URL

- Starting point of the scan
Creating a Scan – Manual Explore

- Browse the application manually
  - Click on links
  - Input data
- The easiest way to define scan scope
- Use when scanning specific pages / functional path
Creating a Scan – Running the Scan

- Click **Save and Run**
### Viewing Scan Progress

- Status Icon
- Click on **Stats**

<table>
<thead>
<tr>
<th>Status</th>
<th>Type</th>
<th>Name</th>
<th>Contents</th>
<th>Description</th>
<th>Last Run</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>My Scan</td>
<td>Edit Stats</td>
<td>4 Reports</td>
<td></td>
</tr>
</tbody>
</table>
## Scan Statistics

### Key counters
- Elapsed time
- Pages found
- Pages scanned
- Security entities found
- Security entities tested
- Security issue variants
- Security tests sent

### Link to Log enabled if problems occurred

### Run Statistics for My Scan

![Run Statistics](image)

**Current State:** Running

**Pending Action:** None

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Last Run</th>
<th>Current Run</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run start</td>
<td>Mon 5/21/2007 2:22:56 PM</td>
<td></td>
</tr>
<tr>
<td>Run end</td>
<td>Estimated time left: 5:18:36</td>
<td></td>
</tr>
<tr>
<td>Elapsed time</td>
<td>0:02:57</td>
<td></td>
</tr>
<tr>
<td>Pages found</td>
<td>41 (0 pending)</td>
<td></td>
</tr>
<tr>
<td>Pages skipped</td>
<td>3 (0 duplicates, 3 not parsed)</td>
<td></td>
</tr>
<tr>
<td>Pages scanned</td>
<td>36</td>
<td></td>
</tr>
<tr>
<td>Page scan rate</td>
<td>12.88 / minute</td>
<td></td>
</tr>
<tr>
<td>Broken links</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Errors logged</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Security entities found</td>
<td>109</td>
<td></td>
</tr>
<tr>
<td>Security entities tested</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Security entity analysis rate</td>
<td>0.34 / minute</td>
<td></td>
</tr>
<tr>
<td>Security issue variants</td>
<td>82</td>
<td></td>
</tr>
<tr>
<td>Security tests sent</td>
<td>2746</td>
<td></td>
</tr>
</tbody>
</table>

**Done**
### Viewing Results

- **Status must be Ready**
- **Click on scan name**

<table>
<thead>
<tr>
<th>Status</th>
<th>Type</th>
<th>Name</th>
<th>Contents</th>
<th>Description</th>
<th>Last Run</th>
</tr>
</thead>
<tbody>
<tr>
<td>My Scan</td>
<td>Edit</td>
<td>Stats</td>
<td>4 Reports</td>
<td></td>
<td>Mon 5/21/2007 2:26:08 PM</td>
</tr>
</tbody>
</table>
Working with Reports

- **Report Pack Summary**
- **Report list**
- **Key reports**
  - Security Issues
  - Remediation Tasks
  - Pages
  - Broken Links
- **Click on report name to view**
Working with Reports – Setting Up Your View

- Group
- Show
- Search
- Layout
### Working with Reports – Viewing Issue Details

#### QuickScan > Altera Mutual > Users > John Smith > My Scan > Security Issues

**Security Issues**

**Last Updated:** 5/21/2007 2:26:11 PM

To view the details of an issue, click on the issue number.

#### Security Issues Table

<table>
<thead>
<tr>
<th>Status</th>
<th>Issue</th>
<th>Test URL</th>
<th>Element</th>
<th>Issue Type</th>
<th>Threat Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open</td>
<td>443</td>
<td><a href="http://www.altera.com">http://www.altera.com</a></td>
<td>uid</td>
<td>Cross-Site Scripting</td>
<td>Client-side Attacks</td>
</tr>
<tr>
<td>Open</td>
<td>497</td>
<td><a href="http://www.altera.com">http://www.altera.com</a></td>
<td>lang</td>
<td>Cross-Site Scripting</td>
<td>Client-side Attacks</td>
</tr>
</tbody>
</table>

---

**Legal Disclaimer**
Working with Reports – Advisory

- Explanation of the vulnerability
- WASC Threat Classification
- Security Risk
- Possible Cause
- Technical Description
- Products Affected
- References and Relevant Links
Working with Reports – Fix Recommendation

- How do you fix the problem?
- General Description
- ASP .NET Fix Recommendation
- J2EE Fix Recommendation
- PHP Recommendation
Working with Reports – Request / Response

- Issue variants
- Difference (hyperlink)
- Reasoning (hyperlink)
- Test HTTP Traffic
- Original HTTP Traffic
### Marking issue status

- In Progress
- Noise
- Fixed
- Passed
- Open

---

There are several issues whose remediation lies in sanitizing user input. By verifying that user input does not contain hazardous characters, it is possible to prevent malicious users from causing your application to execute unintended operations, such as launch arbitrary SQL queries, embed Javascript code to be executed on the client side, run various operating system commands etc.

It is advised to filter out all the following characters:

1. `|` (pipe sign)
2. `&` (ampersand sign)
3. `;` (semicolon sign)
Reviewing Test Results – Steps

Note:
- Test results MUST be reviewed for false positives
- Start with the high priority items

1. Click on the Issue Number link
2. Read the Advisory
3. Review the Request / Response Tab
   a) Look at the reasoning → highlighted text in the Test HTTP response
   b) If you are not convinced that this is a vulnerability
      1. Look at the difference
      2. Try to understand what the test is doing (go back to the advisory)
      3. Look at the test response
      4. Look at the original traffic – make sure it is valid (esp. was the page in session)
Reviewing Test Results

- False Positives
- False Negatives
Lab: Setting up and Running a Scan

1. Create a scan for http://demo.testfire.net
2. Use Manual Explore test policy
3. Run the scan
4. View your reports
5. Set up your report view
6. Examine a vulnerability of each of the following types:
   a) XSS
   b) SQL Injection
   c) SQL Injection on the login page
7. Classify the issues
Advanced Scan Options Explained

- Servers and Domains / URL Normalization
- Dynamic Components
- Custom Error Pages
- Automatic Form Fill
- Connection Settings
- Network Connection
- Scheduling
- Log Settings