**Procedure Title:** Web Application Security Assessment  
**Procedure Number:** IS-P801  
**Responsible Office:** Information Security Office

---

**INTRODUCTION**

One of the most effective and thorough ways to identify and remediate potential vulnerabilities in web applications is to use a scanning tool. These tools are designed to perform specific security and compliance checks such as potential field manipulation and cookie poisoning, which allows a more focused assessment of web applications by exposing vulnerabilities of which other vulnerability scanning tools are unaware. Additionally, these tools can be used in test, development and production instances to find all linked pages and to check sites for vulnerabilities such as SQL injection, cross-site scripting and buffer overflows.

**WHAT MUST BE SCANNED AND REMEDIATED? (SCOPE)**

ALL applications accessed over a network such as the Internet or an intranet must be scanned, per the state auditors’ general recommendation.

Not all internet facing applications are expected to be scanned at once. To assist in prioritizing the list of applications to scan, please utilize the following checklist:

- **High Priority Applications**
  - **High priority applications** are those that require a URL to access them AND;
  - store or transmit Personal Information (i.e. Social Security Numbers, Credit Card Information, Financial information), as defined in the Data Classification Standard (IS-S302), AND/OR
  - would have a University-wide impact if unavailable AND/OR
  - would have a College or higher administrative unit-wide impact if unavailable

- **Medium Priority Applications**
  - **Medium priority applications** are those that require a URL to access them AND;
  - store or transmit any other Confidential University Data such as Personal Identifiable Information not already listed under high priority, Proprietary Information, Confidential Non-Personally Identifiable Information, as defined in the Data Classification Standard (IS-S302) AND/OR
  - would have a Department wide impact if unavailable

- **Low Priority Applications**
  - **Low priority applications** are those that require a URL to access them AND/OR
  - Any other applications that do not meet the high or medium priorities criterion (i.e. Static WebPages, Content Management Websites, etc)

Click [here](#) to see the flowchart of this prioritization process.

**WHEN SHOULD SCANS BE COMPLETED? (Timeline)**

The Web Application Security Review Procedure (IS-P802) requires annual scanning of all web applications.

- The University Application Security Standard (IS-S801) requires scanning of all new or significantly modified applications before they are released to a production environment.
- Web applications with any other regulatory requirements must be done in line with the regulation requirements.
**PRE-SCANNING PROCESS**

1. **Prerequisites (to be completed before access is granted):**
   The individual completing the scan must:
   a) Complete the Web Developer Information Security Essentials Training
   b) Complete UA’s IBM AppScan online training or attend a live Application Scanning Tool Training session (scheduled sessions will be available in the near future). For more information, contact the Information Security Office at 621-8476.
   c) Speak with your Server System Administrator to coordinate and identify the best time for running the scan against your application to ensure the resource will be available, and that there are no resource complications.

   ***Please note that the AppScan tool is checked out to you for a period of 5 business days***

2. **Request access to the Site-licensed Web Application Scanning Tool:**
   Be prepared to provide the following information:
   a) Requestor’s Name
   b) Server Administrator’s Name
   c) Server Administrator’s UA NetID
   d) College/Admin Unit Name
   e) Department(s) Name
   f) Web Server IP Address(es)
   g) URLs to be scanned (For assistance with list prioritization, refer back to “What must be scanned.”).

   ***To fill out the AppScan Access Request form, click [here]***

**SCANNING PROCESS**

Upon granting access to scanning tool, InfoSec will reply to the requestor with additional information and instructions regarding access and use of the tool. Please expect a turnaround of 2 business days.

Once the requester has received a response email and instructions from InfoSec, the requestor should begin the scan as soon as it is feasible.

The scanning process consists of three phases: *(detailed information will be sent when access is granted):*

1. **Scanning:** identifies web application vulnerabilities
2. **Remediating:** removes the high vulnerabilities identified in the scan
3. **Rescanning:** rescans web applications to ensure high vulnerabilities (at a minimum) have been remediated.

**IMPORTANT REMINDER:** AppScan **should not** run against production because it can be intrusive.

**POST SCANNING PROCESS**

All reports generated from scans should be retained for two years. After successfully scanning and remediating all required vulnerabilities, a copy of the executive summary report must be sent to the InfoSec office (iso@email.arizona.edu). InfoSec needs this summary for validation purposes. The executive summary must also include a remediation plan which addresses any unresolved vulnerabilities from the rescan (this includes addressing false positives found in the rescan).
Related UA Security Policy and Standards:
- Information Security Policy (IS-100)
- Information Security Terms Guideline (IS-G100)
- Exceptions Procedure (IS-P100)
- Data Classification Standard (IS-S302)
- Application Security Standard (IS-S801)
- Web Application Security Review Procedure (IS-P802)

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Draft:</td>
<td>11/13/08</td>
</tr>
<tr>
<td>UA-ISAC Review:</td>
<td>4/2/09</td>
</tr>
<tr>
<td>Effective Date</td>
<td>7/1/09</td>
</tr>
<tr>
<td>Revision Date:</td>
<td>7/20/11</td>
</tr>
</tbody>
</table>