



VULNERABILITY SCANNING AUTHORIZATION

Overview

The Office of Information Security Controls and Compliance (OISC²) conducts regular, planned PC, Server, and Web Application Vulnerability Scanning to all agencies within West Virginia State Government. Agencies not under the technical authority of WVOT may request and participate in the Vulnerability Scanning Service (VSS). The Vulnerability Scanning Service provides:

- Consultation regarding the benefits of the Vulnerability Management Services;
- In-depth network-based assessment of workstations, servers, devices and the overall security of the network infrastructure;
- Coordination, collaboration and general technical consulting before, during and after the assessment; and
- Follow-up documentation/reports and additional consulting as needed after the assessment.

The intent of vulnerability scanning being performed by OISC² is to independently identify technical weaknesses in scanned systems and to assist in the prioritization of remediation based on the importance of affected systems and by the severity of the vulnerability. Such assessments will inform agencies which systems need to be properly updated and patched. The scans also allow systems containing sensitive information to be properly configured to leverage access, and control against security intrusions.

Required Elements

The required elements for Vulnerability Scanning Services include, but are not limited to, the following:

- A documented request by and an agreement with the Agency for a network-based or web application Vulnerability Assessment. See attached form.
- Timely and bi-directional coordination, collaboration and communication between OISC² and the Agency receiving the assessment.
- Identification of and authorization to assess the range of IP addresses assigned to or “owned” by the Agency.
- Appropriate network and/or physical access to the Agency networks and resources, as agreed to by both parties.
- A service account with appropriate access will be required if a credentialed scan is necessary.
- Sufficient notification by OISC² of when the assessment will take place, what tests will be performed and what source IP address range will be used in the execution of assessment activities.
- Appropriate documentation of findings, results and recommendations to facilitate the remediation of vulnerabilities by the Agency themselves or in conjunction with other resources (e.g. WVOT), if required.



Vulnerability Scanning Request Form

The purpose of this document is to request and grant authorization to members of Office of Information Security Controls and Compliance to conduct vulnerability assessments and penetration tests against the Agency's assets. Scan results will be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with State of West Virginia policy relating to Confidential information and is not to be released to the public or other personnel who do not have a valid "need-to-know", and without requesting agency approval. No portion of this document and subsequent reports may be furnished to the media, either in written or verbal form. **To enable this scanning, the undersigned provides the following information and attests to the validity of the answers:**

SYSTEM BEING SCANNED:	
IP RANGES:	
TYPE OF SCAN REQUIRED:	<input type="checkbox"/> Credentialed (<i>Requires account creation</i>) <input type="checkbox"/> Non-Credentialed
PURPOSE OF SCAN:	
WILLING TO OPEN FIREWALLS TO SPECIFIC TRAFFIC, IF NEEDED?	<input type="checkbox"/> Yes <input type="checkbox"/> No
POINT OF CONTACT AND INFORMATION:	
DATE AND TIME FOR SCAN:	
SPECIAL/OTHER INFORMATION:	
WEB APPLICATION SCANNING OPTIONS	
DOES THE SYSTEM HAVE A CURRENT BACKUP?*	<input type="checkbox"/> Yes <input type="checkbox"/> No
TYPE OF APPLICATION:	<input type="checkbox"/> Development <input type="checkbox"/> Test <input type="checkbox"/> Production
APPLICATION MAINTENANCE PERFORMED BY:	<input type="checkbox"/> WVOT <input type="checkbox"/> Agency <input type="checkbox"/> Vendor±
TYPE OF SERVER:	<input type="checkbox"/> Shared Server <input type="checkbox"/> Load Balanced <input type="checkbox"/> Stand Alone
IS THERE A TEST OR REPLICA ENVIRONMENT AVAILABLE?	<input type="checkbox"/> Yes <input type="checkbox"/> No

* All live systems must have a current backup before scanning.

± When applications are hosted, managed or supported by a third-party vendor, the Agency holds the responsibility of determining if third party/vendor approval is required based on contract terms and conditions.

By signing this authorization, the Agency declares that the Agency owns the systems to be tested and the undersigned has the proper authority to allow OISC to perform application security verification activities.

Agency: _____

Agency Authority: _____

Agency Authority Signature: _____