Maryland State Board of Elections
Online Voter Services
Penetration Testing Report

September 28, 2012
Richard F. Forno, Ph.D., Project Director
University of Maryland, Baltimore County (UMBC)

Contents

Summary

UMBC conducted a security assessment of the Maryland State Board of Elections (SBE) *Online Voter Services* website between 6-27 August 2012. Although UMBC was able to conduct many types of attacks against the site, the website remained resilient against these attacks. Through this assessment, **UMBC was unable to identify any critical vulnerabilities that would compromise the website's integrity or availability**. However, testing did reveal opportunities for application and system improvement, and our corrective recommendations were reported to SBE. Those recommendations were implemented by SBE following this assessment. However, as with all information resources, we encourage the State Board of Elections to continually monitor and evaluate the operational and security capabilities of the site over time, and to employ defense in depth strategies such as with firewalls, intrusion detection systems, and proactive systems monitoring.

This document is intended to serve as a public description of the security testing performed on the Online Voter Services website during 6-27 August 2012. However, specific findings and recommendations are not discussed.

Overview

UMBC conducted a study to evaluate the security of Maryland State Board of Election's (SBE's) information system (*Online Voter Services*) by simulating probes and attacks from malicious outsiders, known as a penetration test or *pentest*. The study involved an active analysis of the system for any potential vulnerabilities that could result from poor or improper system configurations, both then-known and then-unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures. This analysis was carried out from the position of a potential attacker and involved attempted active exploitation of security vulnerabilities.

All assessment activities were developed in a formal Test Plan that was coordinated with and approved by authorized technical personnel from the Maryland State Board of Elections prior to work commencing.

Safeguards, Precautions, and Restoration

Although security testing of systems ideally will take place in an offline test environment, this test was conducted against the live, production *Online Voter Services* system. Thus, precautions to safeguard system operations may at times supersede a more comprehensive evaluation. For example, a more aggressive denial of service attack would be attempted against a non-production system where a disruptive incident would not adversely impact real-world operations. In addition to receiving SBE approval of the Test Plan prior to testing, the testing team kept logs and notes about the actions taken against the website and had control to terminate testing that may have degraded or denied the public use of the website. In cases where the test might cause a disruption that could not be recovered from remotely, the testing team was prepared to notify the Maryland State Board of Elections immediately and work with them to restore the system to the previous state. However, **no adverse situations occurred during testing to warrant emergency escalation**.

Technical Coordination

The UMBC Project Director was Dr. Richard Forno (richard.forno@umbc.edu), who supervised the activities of the testing team. The testing team maintained contact with the following persons at the Maryland State Board of Elections: Stacey Johnson (Stacey.Johnson@maryland.gov), Natasha Walker (Natasha.Walker@maryland.gov, Chere' Evans (cevans@elections.state.md.us), Ross Goldstein (Ross.Goldstein@maryland.gov).

Target to be Tested

Prior to the initiation of the test, SBE provided the UMBC testing team only the numeric Internet address of the website hosting the Online Voter Services system. Any other information obtained during the test was acquired by the testing team using standard information-gathering techniques.

To simulate an external attacker's perspective, the testing team did not have any *a priori* knowledge about implementation of the web application when the test began other than the web address, and had no physical access to the devices in the test environment. Regarding this assessment, SBE asked that each of the four features of the *Voter Services* web application be examined from both a security and operational perspective:

1. Polling Place Search
2. Individual Voter Information Search
3. Online Voter Registration
4. Online Ballot Wizard

Testing was conducted on remote machines that connected to UMBC's network, with network traffic originating from UMBC to the *Voter Services* site.

Artificial Changes from Production

Testing activities were conducted against a copy of the production *Voter Services* website. However, as described in the Test Plan and in subsequent conversations with SBE personnel, several artificial changes to the target environment were made that are not consistent with the production service. This was done *to protect the production service and ensure availability to legitimate users during the testing period*. First, the test service used the same IP address as the production server, but the tested service ran on port 8080 and the production service on port 443. Second, the tested service was protected by SSL using a self-signed certificate -- however, we confirmed that the SSL certificate used on the production site was legitimate. Third, unlike the public-access production service, the tested site was protected by HTTP Basic Authentication, and we were given a username and password to access the site. Finally, the Online Ballot Wizard was enabled on the tested site, even though it was not currently enabled on the public-access production service. None of these changes are believed to adversely impact the test results.

Tools and Techniques Used

A variety of tools were used based on the environment discovered during evaluation of the site.

Tools used in this test included:

- **Web Browsers** (Chrome 21.0, Firefox 14.0.1, Safari 6.0, and Internet Explorer 9.0)
- **Nmap**, a network scanner
- **Metasploit and Armitage**, a penetration testing framework
- **Burp Proxy**, an intercepting proxy server for web application security testing
- **w3af**, web application attack and audit framework
- **Nikto**, a web server scanner
- **Seige**, an HTTP load tester and benchmarking utility
- **Nessus**, a vulnerability scanner
- **Wireshark**, a network protocol analyzer

Security techniques used in this test included:

- Web browsing
- Stress testing
- Input validation
- Port Scanning
- Service Fingerprinting
- Packet Analysis
- HTML Analysis
- Public information gathering

Test Results

The specific results of this assessment and any related recommendations or observations were provided to SBE in two general reporting categories: web application analysis and server penetration tasks.

Web Application Analysis

Tests were conducted against the *Voter Services* web application. The goal was to first try to understand the application's logic by using the application and observing all web requests and responses at the network level. We then used more aggressive methods to understand, stress, and identify vulnerabilities in the *Voter Services* web application, including session management, authorization, and data validation. Within the scope of this assessment, **one potential item of medium concern was discovered during testing, addressed by SBE personnel, and later confirmed by the testing team to be addressed satisfactorily.** Among other application-level configurations, in reviewing the security of the Voter Services web application, the UMBC testing team was unable to:

1. Identify the type of database used
2. Conduct a SQL-Injection attack against the Voter Services application.
3. Identify a way to guess an individual user's password used for the online ballot delivery system.

Server Penetration

Tests were conducted against the operating system of the underlying servers hosting the *Voter Services* web application. These tests followed a traditional network-based vulnerability assessment process, including but not limited to public information gathering, the identification of insecure configurations, and/or the presence of insecure services. **No significant security or operational concerns were discovered.** We then used several automated in an attempt to locate vulnerabilities in the operating system but **were unable to compromise the underlying server**. Following the assessment activities, SBE personnel informed the testing team that the website became increasingly responsive during a simulated hostile stress test of the server (as one would expect in such situations), but that existing security mechanisms and configurations functioned as expected in detecting the incident. Additionally, the testing team was pleased that error messages generated by the server did not disclose any proprietary or sensitive information (technical or otherwise) to users.

As expected, testing did reveal opportunities for minor stylistic application and system improvements, and those observations and recommendations were presented to SBE for follow-up remediation as deemed appropriate. However, these **did not represent concerns that would impact the security, functionality or availability of the *Online Voter Services* site**. Many of those recommendations were implemented by SBE following this assessment.

# # # # #

Disclaimer: The systems analyzed in this report were examined during the period of 6-27 August 2012. While the results of this assessment provide a reasonably accurate view of the security level of the tested computer system(s) during that specific period of time in accordance with the approved Test Plan, UMBC and the testing team cannot be held responsible if this assessment fails to discover certain security or configuration issues on the tested computer system(s) either at the time of the assessment or that become known in the future.