Chad Ballay

**Vulnerability Assessment & Penetration for eClipse Bank**

**Issue 1**

*According to its banner, the version of PHP installed on the remote host is older than 4.4.5. Such versions may be affected by several issues, including buffer overflows, format string vulnerabilities, arbitrary code execution, 'safe\_mode' and 'open\_basedir' bypasses, and clobbering of super-globals.*

Resolution would be to upgrade the version of PHP. Extensive testing would be needed to proceed. A longer term goal would be to adopt a CI/CD pipeline that utilizes Infrastructure as Code and other modern best practices to help speed deployments.

**Issue 2**

*The remote version of Apache is vulnerable to an off-by-one buffer overflow attack.*

Resolution is to upgrade the version of Apache. Extensive testing would be needed to proceed. A longer-term goal would be to adopt a CI/CD pipeline that utilizes Infrastructure as Code and other modern best practices to help speed deployments.

**Issue 3**

*The remote DNS resolver does not use random ports when making queries to third party DNS servers.*

Resolution would be to enable port randomization. This would increase the complexity in the attack approach needed to feed bad results into the DNS cache. Research on capability required in DNS server application. (For example: <https://nlnetlabs.nl/documentation/unbound/patch-announce102/>)

**Issue 4**

*The remote server is incorrectly configured with a NULL password for the user 'Administrator' and has FTP enabled.*

Resolution is to change the password for this user in accordance with the organizations password policy. This may include a broader review of configuration management and credential storage. (Windows example: <https://www.wikihow.com/Set-Administrator-Password>) (Linux example: <http://man7.org/linux/man-pages/man1/passwd.1.html>)

**Issue 5**

*Cross-site scripting (reflected) – Multiple parameters for https://secure.eclipsebank.cxm/g enScript.php*

Resolution will require a review and redesign of the script as a possibility. The inputs will need to be sanitized to only contain HTML-encoded metacharacters. Additional input validation checks are recommended. (Additional background information: <https://owasp.org/www-community/attacks/xss/>)