High Bit Security, LLC
PO Box 533,
Port Sanilac MI, 48469
www.HighBitSecurity.com

LONGDATE
Author: AUTHOR

NOTE: This is a sample full, private report for visualization purposes – charts or data given in this sample may not correlate with any  data contained in this sample, nor is there any correlation with any actual client. This sample allows for visualization and test coverage for an external or internal penetration test, and includes sections pertinent to both. It also includes sections that may be omitted except in certain compliance driven engagements, and other sections that will be omitted when not in scope. Our report formats change from time to time and your final report may not match this format precisely.

# External Penetration Test Report

For

## org X, Inc.

CONFIDENTIAL

This document contains proprietary and confidential information and is subject to non-disclosure agreements. Reproduction or distribution without the express written permission of High Bit Security, LLC or the Client named above is strictly prohibited.

## Contents

## Executive Summary

The first objective of this external penetration test was to fully examine the internet facing Org X systems to identify vulnerabilities that could allow an  attacker to compromise the confidentiality, integrity or availability of those systems. Our second objective was to safeguard the stability of the Org X systems under test. Our third objective was to prove exploitability by pursuing vulnerabilities to the point of compromise. The priority of these objectives dictated that vulnerabilities were not necessarily pursued to the point of full exploitation and compromise.  Full exploitation was not pursued if the vulnerability appeared to be systemic, or if remediation was mandatory for PCI compliance, or if exploitation would have jeopardized either full test coverage or the stability of the systems under test.

The Remediation Guidance section, which follows this section, includes information to help with prioritizing and assignment of remediation efforts.

Full details of our findings are found in the Finding Details section of the report; the following is an executive level summary of issues found:

No faults were found with network devices or configuration, and host operating systems and services were found to be well patched and configured.

The application exposed several vulnerabilities. These application faults comprise the greatest risk to the security of the systems under test. There were no application vulnerabilities that we rated critical in severity, however there were two high severity and four medium severity findings.

Here is a visual summary of the categories we tested and findings contained in this report:

| Category | Untested | Info | Low | Med | High | Critical |
|---|---|---|---|---|---|---|
| Overall | | 1 | | 4 | 2 | |
| Network | | | | | | |
| Configuration | | | | | | |
| Application | | 1 | | 4 | 2 | |
| Wireless | X | | | | | |
| Social Engineering | X | | | | | |

## Remediation Guidance

This section contains guidance for managing remediation of the vulnerabilities identified in this report.

**Finding Reports:**

The finding details section of this report contains individual finding reports for all of the vulnerabilities identified. Finding reports are *also provided as separate pdf documents*. This allows you to selectively distribute specific finding reports to the personnel who need them.

**Remediation Checklist:**

This document is accompanied by a remediation checklist. If you will be requesting a remediation test from us, this document is required and will speed things up considerably by informing us about what you want us to re-test and what steps you took in remediation. If you do not intend to retest, it is still advisable to retain a record of the remediation steps taken. The provided checklist can be used for that purpose.

## Recommendations

High Bit recommends that all of the vulnerabilities be remediated, and a remediation test be conducted to verify remediation. If this is a test in support of PCI-DSS compliance, remediation verification is mandatory: (PCI-DSS 11.3.a: Verify that noted vulnerabilities were corrected and testing repeated.). Specific remediation guidance is given in the next section of the report.

## Scope of Testing

The following Org X hosts were in scope and included in this penetration test:

| Network Name | Type | Hosts (By IP Address) |
|---|---|---|
| CDE | Target | |
| Office | Source | |
| External | Source | |
| Dev | Source | |
| | | |

The following Org X applications were in scope  and included in this penetration test:

| Applications in Scope (By URL) |
|---|
| |

The following accounts and credentials were provided by Org X and used in application testing (if any):

| Testing Accounts and Credentials |
|---|
| |

The following engagement windows were defined for this test:

| Engagement Windows |
|---|
| |

The following testing activities were excluded from scope:

| Excluded Testing Activity |
|---|
| |

## PCI-DSS version 3 Scope and Methodology Summary

This section is intended for use by PCI-DSS auditors or consultants. It provides details of the specific scope and testing considerations relevant to PCI-DSS. Most of our testing methods exceed the requirements of PCI-DSS. This section is meant only to assist auditors in validating that the testing methodology and scope used in this test meet the minimum requirements defined under PCI-DSS version 3, by correlating this report and our methodology with the requirement.

| Ref | Specific Requirement | Compliance Statement |
|---|---|---|
| 11.3 | Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115) . | The methodology used in this test was based on NIST SP800-115 'Technical Guide to Information Security Testing and Assessment ' at 5.2 'Penetration Testing'.<br>Four phases are defined by this Guide: Planning, Discovery, Attack and Reporting.<br>Outcomes from the planning phase may be found in the general scope section of this document, and any PCI specific scope considerations are given in **PCI Specific Segmentation Testing Scope**, following this table.<br>Outcomes from the Discovery phase can be found in the **Discovery, Perimeter, Stateful Firewall and DNS Analysis** section of the report.<br>Outcomes from the Attack phase are given in the Executive Summary, Penetration Testing and the **Finding Details** sections of the report.<br>This document comprises the initial reporting. Subsequent remediation reports may be part of the reporting process, see 11.3.3. |
| 11.3 | Includes coverage for the entire CDE perimeter and critical systems. | **See PCI Specific Segmentation Testing Scope**, following this table. |
| 11.3 | Includes testing from both inside and outside the network . | See 11.3.1 and 11.3.2 |
| 11.3 | Includes testing to validate any segmentation and scope-reduction controls. | See 11.3.4 |
| 11.3 | Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5. | Any applications listed as 'in scope' for this engagement received application testing for all of the vulnerabilities descrbed in PCI-DSS section 6.5. |
| 11.3 | Defines network-layer penetration tests to include components that support network functions as well as operating systems. | For the purpuse of our testing, all hosts supporting networking functions for the CDE were considered to be part of the CDE and received testing for host level as well as network function.<br>**See PCI Specific Segmentation Testing Scope**, following this table. |

| | | |
|---|---|---|
| | | **See Discovery, Perimeter, Stateful Firewall and DNS Analysis** section. |
| 11.3 | Includes review and consideration of threats and vulnerabilities experienced in the last 12 months. | We obtained, reviewed and used the information contained in copies of the last four quarterly vulnerability scans from the client, in addtion to our own standard vulnerability scans.<br>We interviewed the client for any other information security relevant incidents occuring in the last 12 months and none were reported to us. |
| 11.3 | Specifies retention of penetration testing results and remediation activities results. | See 11.3.3. |
| 11.3.1 | Perform external penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). | This engagement is an annual External Penetration Test. |
| 11.3.2 | Perform internal penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). | N/A - This engagement is an annual External Penetration Test. |
| 11.3.3 | Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections. | **See Remediation Guidance** section.<br>**See Supplemental File: RemediationChecklist.doc.** |
| 11.3.4 | If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from in-scope systems. | **See PCI Specific Segmentation Testing Scope**, following this table.<br>**See Discovery, Perimeter, Stateful Firewall and DNS Analysis** section. |

**PCI Specific Segmentation Testing Scope:**

**Methodology: A preconfigured testing host was physically placed on the CDE network and testing of the CDE systems and network devices was conducted using this host. All other segmentation testing was achieved using VPN connections to the source network, and conducting port scans against the CDE Target network over VPN.**

| Network Name | Type | Hosts (By IP Address) |
|---|---|---|
| CDE (includes network function hosts) | Target | [CDE IP LIST] |
| CDE | Source | [Our source IP used during testing] |
| Office | Source | [Our source IP used during testing] |
| External | Source | [Our source IP used during testing] |
| Dev | Source | [Our source IP used during testing] |

# Testing Details

## Reconnaissance

A brief  reconnaissance encompassing both active and passive techniques was conducted using Whois queries, Search engines and other web resources to determine the breadth and depth of information available about the target network, with particular emphasis on harvesting of potential user names and information that could aid in dictionary attacks, phishing and social engineering attacks.

| Passive and Active Reconnaissance Information |
|---|
| |

# Discovery, Perimeter, Stateful Firewall and DNS Analysis

At a minimum, an analysis was conducted from an external host to the target network. If the engagement was an internal test and was conducted for PCI-DSS compliance, this table will show which networks were tested and from where, and can be used to validate network segmentation. Since these reports are lengthy, we give the result sommary here but the full reports are included as supplemental files, identified in the table below.

| Source Network | Target Network | Supplemental File |
|---|---|---|
| CDE | CDE | CDE_CDE_Analysis.pdf |
| Office | CDE | Office_CDE_Analysis.pdf |
| External | CDE | External_CDE_Analysis.pdf |
| Dev | CDE | Dev_CDE_Analysis.pdf |

## Result Summary

Based upon stateful firewall inspection tests, DNS queries, port scans and services identified, the network devices are well secured and segmentation rules are well configured.

## Vulnerability Scanning

### Scanners Used

OpenVAS with up to date signatures was used to scan the target hosts for known vulnerabilities.

### Summary of Scanning Results

Full details of the vulnerability scan are included in the attached report. Significant scanner reported issues were evaluated to eliminate false positives, and any remaining issues are addressed as findings in the Finding Details section of this report.

# Penetration Testing

## Objectives

The first objective was maximum test coverage; the second objective was safeguarding the stability of the systems under test, and the last objective was proof of exploitability. The priority of these objectives dictated that vulnerabilities were not necessarily pursued to the point of full exploitation and compromise. Full exploitation was not pursued if the vulnerability appeared to be systemic, or if remediation was mandatory by reason of compliance drivers, or if exploitation would have jeopardized either full test coverage or the stability of the systems under test.

### Network and Host Test Coverage: Common Network and Host Configuration Issues

| Network and Host Configuration Summary | |
|---|---|
| NetBios Enumeration | No faults found. |
| LDAP Enumeration | No faults found. |
| SNMP Enumeration | No faults found. |
| SMTP Account Enumeration | No faults found. |
| Open Administrative Interfaces | No faults found. |
| Authentication Attacks | No faults found. |

### Network and Host Test Coverage: Encryption

| Encryption Summary | |
|---|---|
| Transport Protocol | No faults found. |
| Transport Cipher Suites Support | No faults found. |
| Clear Text Transport of Sensitive Data | No faults found. |
| Other Encryption | No other encrypted data was noted |

### Application Test Coverage: Information Disclosure

| Information Disclosure Summary | |
|---|---|
| Robots.txt | No faults found. |

| | |
|---|---|
| Comments | No faults found. |
| Hidden Fields | No faults found. |
| Error Handling | No faults found. |

## Application Test Coverage: Authentication

| Authentication Summary | |
|---|---|
| User Account Enumeration | No faults found. |
| Guessable Accounts | No faults found |
| Brute Force and Account Lockout | No faults found. |
| Authentication Bypass | No faults found. |
| Password Recovery and Reset. | No faults found. |
| Password Complexity | No faults found. |
| Secure Logout | No faults found. |
| Browser Caching | No faults found. |
| CAPTCHA Devices | No faults found. |
| Multiple Factor Authentication | No faults found. |
| Race Conditions | No faults found. |

## Application Test Coverage: Authorization

| Authorization Summary | |
|---|---|
| Path Traversal | No faults found. |
| Authorization Bypass | No faults found. |
| Privilege Escalation | No faults found. |

## Application Test Coverage: Business Logic

| Business Logic Summary | |
|---|---|
| Business Logic | No faults found. |

## Application Test Coverage: Data Validation - Reflection Issues

| Data Validation – Reflection Issues Summary | |
|---|---|
| Reflected Cross Site Scripting | No faults found. |
| Persistent Cross Site Scripting | No faults found. |
| DOM Based Cross Site Scripting | No faults found. |
| Cross Site Flashing | No faults found. |

## Application Test Coverage: Data Validation – Injection and Miscellaneous

| Input Validation - Injection and Miscellaneous Summary | |
|---|---|
| SQL Injection | No faults found. |
| LDAP Injection | No faults found. |
| ORM Injection | No faults found. |
| XML Injection | No faults found. |
| SSI Injection | No faults found. |
| XPath Injection | No faults found. |
| IMAP/SMTP Injection | No faults found. |
| Code Injection | No faults found. |
| OS Commanding | No faults found. |
| Buffer overflow | No faults found. |
| Incubated Vulnerabilities | No faults found. |
| HTTP Splitting/Smuggling | No faults found. |

## Application Test Coverage: Denial of Service

| Denial of Service Summary | |
|---|---|
| SQL Wildcard Attacks | DOS was not in scope for the test due to PCI requiring testing of production environments, and PCI not requiring DOS testing. |
| Account Lockout | DOS was not in scope for the test due to PCI requiring testing of production environments, and PCI not requiring DOS testing. |
| Buffer Overflows | DOS was not in scope for the test due to PCI requiring testing of production environments, and PCI not requiring DOS testing. |
| User Specified | DOS was not in scope for the test due to PCI requiring testing of production |

| | |
|---|---|
| Object Allocation | environments, and PCI not requiring DOS testing. |
| User Input as a Loop Counter | DOS was not in scope for the test due to PCI requiring testing of production environments, and PCI not requiring DOS testing. |
| User Provided Data to Written to Disk | DOS was not in scope for the test due to PCI requiring testing of production environments, and PCI not requiring DOS testing. |
| Failure to Release Resources | DOS was not in scope for the test due to PCI requiring testing of production environments, and PCI not requiring DOS testing. |

### Application Test Coverage: Session Handling

| Session Handling Summary | |
|---|---|
| Session Predictability | No faults found. |
| Query Strings | No faults found. |
| Encrypted Transport | No faults found. |
| Cookie Attributes | No faults found. |
| Session Fixation | No faults found. |
| Session Re-Use | No faults found. |
| Cache Control | No faults found. |
| CSRF Vulnerabilities | No faults found. |

### Application Test Coverage: Web Services

| Web Services Summary | |
|---|---|
| Information Gathering | None discovered |
| WSDL | n/a |
| XML Structural Testing | n/a |
| XML content-level Testing | n/a |
| HTTP GET parameters/REST Testing | n/a |
| SOAP Attachments | n/a |
| Replay Testing | n/a |

## Application Test Coverage: AJAX

| AJAX Summary | |
|---|---|
| AJAX Vulnerabilities | No faults found. |

## Application Test Coverage: Application Server Configuration Issues

| Application Server Configuration Issues Summary | |
|---|---|
| File Extensions Handling | No faults found. |
| Old, Backup and Unreferenced Files | No faults found. |
| HTTP Methods and XST | No faults found. |

## Wireless Network Test Coverage

| Wireless Testing Summary | |
|---|---|
| Weak Protocols | No faults found. |
| Default or Guessable Administrative Credentials | No faults found. |
| Rogue Access Points | No faults found. |
| Hidden SSID discovery | No faults found. |
| MAC filter evasion | No faults found. |
| Mis-association | No faults found. |
| Dis-association | No faults found. |
| Wireless MITM | No faults found. |
| WPA Enterprise | No faults found. |

## Social Engineering Test Coverage

If in scope, electronic assisted social engineering attacks were attempted. The type of attacks used were dependent on vulnerabilities observed and available information.

| Social Engineering Summary | |
|---|---|
| | Not in scope, not tested. |

## Finding Details

NOTE: This section of the report will include details in the format below for each finding.

| **Finding: Sample Finding Title**<br>CATEGORY | |
|---|---|
| Severity: | SEVERITY |
| Target(s): | TARGET LIST |
| Description: | DESCRIPTION RISK |
| Remediation: | REMEDIATION |
| Test Notes: | NOTES |
| Screen Captures: | |
| | |

## Appendix 1: Severity Levels

There are a number of commonly used schemes for rating vulnerability severity; however many of them are rigid and do not consider context. While this has value, our own experience has shown that context matters very much in rating the true significance of any security fault. Our ratings are therefore subject to the context in which the fault is found and ultimately subject to the judgment of our security engineers.

5 severity levels are used in reporting security faults:

**CRITICAL**

In the opinion of our security engineer, the fault puts the application or system at imminent and substantial risk. These faults require immediate attention. These faults are severe and easily discovered by attackers. They are immediately exploitable without combination with any other fault, or may require combination with another fault that has already been observed in the application or system under test. This rating also includes information disclosure where the information itself is confidential or of very high value to an attacker. Examples of the latter include password files, credit card data, source code disclosure or world readable or writable file systems. These faults should receive top priority in remediation.

**HIGH**

Faults that, in the opinion of our security engineer could lead to compromise but are not easily discovered, or require significant time or unusual skill to exploit, or are serious but more limited in impact than a CRITICAL fault. These faults are immediately exploitable without combination with any other fault, or require combination with another fault that has already been observed in the application or system under test. These faults may include high value information disclosure if the information is useful for successful exploitation of another HIGH or CRITICAL fault, such as user account disclosure in combination with no account lockout, a condition that could lead to successful brute force or dictionary attack. These faults should be corrected immediately.

**MEDIUM**

Faults that, in the opinion of our security engineer could lead to compromise, but are difficult to detect, difficult to exploit, are limited in impact or require combination with at least one other fault to be successfully exploited and no such fault has been observed. Also includes high value information disclosure such as stack traces, configuration files, platform error messages, etc. Also, any fault that we know requires remediation for PCI compliance will receive this rating as a minimum. While more severe faults should be corrected first, these are still dangerous faults and should be corrected as soon as possible.

**LOW**

Faults that, in the opinion of our security engineer could aid in developing other attacks, or faults that if exploited would have limited impact. These faults also include information disclosure that may be helpful to an attacker but is of relatively low perceived value. While the relative value to an attacker is considered low, these are still security faults and should be corrected. They often lack only the existence of another fault, a newly discovered exploit, or an application, system or firewall change to take on greater significance.

**INFORMATIONAL**

This severity level is used when our security engineer obtains results that you should know about, but may or may not represent any specific security issue. This severity level is often used when our security engineer must rely on your judgment, for example: when unsecured content or functionality is found, but the security engineer does not know and cannot determine by its nature if it should be (or if you intended it to be) restricted by access controls. You should carefully review all such findings and take corrective action if appropriate.

## Appendix 2: Severity Levels, PCI Compliance and Public Reports

There is no mandated vulnerability rating system for PCI-DSS compliance penetration testing, however all faults that are known to require remediation under PCI-DSS are rated to at least a MEDIUM. Therefore, at a minimum you should plan to correct all MEDIUM and higher faults, and it is recommended that all faults be corrected.

Before formulating a remediation plan, you should consult with your QSA. Your auditor knows your network, systems and applications and thus has an inside perspective that our security engineers do not have when testing for and rating faults. For this reason, faults that we rate as LOW or INFORMATIONAL may be of higher significance to your auditor.

High Bit Security requires that all findings of low or higher severity be corrected before a public facing report is issued, unless the finding is specifically listed as an exception in the public facing report.