BadStore Web Application Remediation Vulnerability Report

Gage Berghoff

Wright State University

11/30/2019

Table of Contents

[Remediation Plan 3](#_Toc26099003)

[Security Controls Plan 3](#_Toc26099004)

[Updates 3](#_Toc26099005)

[Sitewide - Depreciated Apache Version 3](#_Toc26099006)

[Information Disclosures 3](#_Toc26099007)

[Information Disclosure - Restricted Directories // 2 scan bot things wtf do 3](#_Toc26099008)

[Information Disclosure - Internal IP Address 3](#_Toc26099009)

[Information Disclosure - HTML Source Code 3](#_Toc26099010)

[Information Disclosure - Sensitive Information 3](#_Toc26099011)

[Administrative Interface Externally Accessible 3](#_Toc26099012)

[Weak Configurations 3](#_Toc26099013)

[Weak Password Reset – Unlimited Tries 3](#_Toc26099014)

[Weak Configuration - Unlimited Tries – Login 4](#_Toc26099015)

[Weak Configuration - No Log Out Functionality – Site Wide 4](#_Toc26099016)

[Weak Configuration - No Password Required for Registration 4](#_Toc26099017)

[Utilization of a Default Password – MySQL service, and Password Reset Functionality 4](#_Toc26099018)

[Unencrypted Storage of Sensitive Information - Credit Card # 4](#_Toc26099019)

[Unencrypted Storage of Sensitive Information – Username 4](#_Toc26099020)

[Utilization of a Weak Encryption Protocol - MD5 4](#_Toc26099021)

[Insufficient Password Complexity Policy 4](#_Toc26099022)

[Remediation Vulnerability Report 4](#_Toc26099023)

[Remediation Analysis 4](#_Toc26099024)

# Remediation Plan

// Gnatt chart goes here with explanation of the time frame and wtf we are solving in each section

# Security Controls Plan

## Updates

Due to BadStore’s age many services required for BadStore to operate have become outdated over time. Assuring these services are updated regularly can help patch vulnerabilities found in older versions of the services.

### Sitewide - Depreciated Apache Version

* BadStore is currently running Apache version 2 for security reasons this should be upgraded to Apache version 2.4. Information on this procedure can be found here <https://httpd.apache.org/docs/2.4/upgrading.html>.

## Information Disclosures

BadStore has many instances where information that should not be publicly available is exposed to the public. The causes of these information disclosures range from poor configuration to bad code design.

### Information Disclosure - Restricted Directories // 2 scan bot things wtf do

* Holder

### Information Disclosure - Internal IP Address

* Holder

### Information Disclosure - HTML Source Code

* Holder

### Information Disclosure - Sensitive Information

* Holder

### Administrative Interface Externally Accessible

* Holder

## Weak Configurations

During the initial setup process of some BadStore services steps to properly configure said services were not taken. Such as usage of default service passwords, weak encryption methods used etc. These configuration mistakes increase the security risk of the site overall.

### Weak Password Reset – Unlimited Tries

* Holder

### Weak Configuration - Unlimited Tries – Login

* Holder

### Weak Configuration - No Log Out Functionality – Site Wide

* Holder

### Weak Configuration - No Password Required for Registration

* Holder

### Utilization of a Default Password – MySQL service, and Password Reset Functionality

The use of a default password can be found in multiple areas in BadStore. This can allow for an attacker to easily access services or users accounts.

* MySQL –
* Password Reset - Welcome

### Unencrypted Storage of Sensitive Information - Credit Card #

* Holder

### Unencrypted Storage of Sensitive Information – Username

* Holder

### Utilization of a Weak Encryption Protocol - MD5

* Holder

### Insufficient Password Complexity Policy

* Holder

## SQL Injection

* Holder

## Cross Site Scripting

* Holder

# Remediation Vulnerability Report

//copy paste your entire phase 2 report in here, add a subsection for each vuln and explain how we fixed it, then retest it

# Remediation Analysis

// bullshit calculations on how safe the system is now.