BadStore Web Application Remediation Vulnerability Report

Gage Berghoff

Wright State University

11/30/2019

Table of Contents

[Remediation Plan 3](#_Toc26015342)

[Security Controls Plan 3](#_Toc26015343)

[Remediation Vulnerability Report 3](#_Toc26015344)

[Remediation Analysis 3](#_Toc26015345)

# Remediation Plan

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

# Security Controls Plan

## Updates

* 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 //SQL and general

* Scanbot - Restricted Directories
* Scanbot - Internal IP Address
* Search - SQL Error

## Insufficient Input Validation

* Registration - Expiration Date
* Registration - Email Address, Password

## Weak Configuration

* Registration – No password required

## Publicly exposed Admin Interface

## Unencrypted Storage

## Utilization of weak encryption protocol – MD5

# Remediation Vulnerability Report

// Ties back into phase 2, retest individual vulns

# Remediation Analysis

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