de

# 

# Document Control

|  |  |  |
| --- | --- | --- |
| **Document Version** | **Owner & Role** | **Status & comments** |
| v1.0 | Andrew Pham – Security Analyst | Internal Draft {Restricted Scope) |

# 

# Legal Disclaimer

The content of this report is highly confidential and may include critical information on Example Corp systems, network, and applications. The report should be shared only with intended parties.

Although maximum effort has been applied to make this report accurate, Example Corp, Security Audit Team cannot be held responsible for inaccuracies or system changes after the report has been issued since new vulnerabilities may be found once the tests are completed.

Guidance should be taken from a Legal Counsel, CISO and Blue Team on how best to implement the recommendations.

All other information and the formats, methods, and reporting approaches is the intellectual property of Example Corp and is considered proprietary information and is provided for the purpose of internal use only.

Any copying, distribution, or use of any of the information set forth herein or in any attachments hereto form outside of Example Corp authorized representatives is strictly prohibited.

# Table of Contents

[Document Control 2](#_heading=h.30j0zll)

[Legal Disclaimer 3](#_heading=h.3znysh7)

[Table of Contents 4](#_heading=h.2et92p0)

[1.](#_heading=h.tyjcwt) Executive Summary 5

[2.](#_heading=h.1t3h5sf) A Glance Through Target Security Posture 6

[3.](#_heading=h.2s8eyo1) Testing Methodology 7

[4.](#_heading=h.17dp8vu) Tools & Websites Used 7

[Detailed Technical Reports (Scope Limited) 8](#_heading=h.26in1rg)

[[sagarbansal.com] 9](#_heading=h.35nkun2)

[Finding X: TITLE HERE – RATING 10](#_heading=h.2jxsxqh)

[Steps to Reproduce 11](#_heading=h.z337ya)

[Appendixes 12](#_heading=h.4i7ojhp)

[Appendix A: Vulnerability Score Analysis – CVSS 3.0 13](#_heading=h.2xcytpi)

[Appendix B: Modified Exploit Code For CVE-XXXX-XXXXX 14](#_heading=h.1ci93xb)

[Appendix C: Screenshots For Nessus & Faraday 15](#_heading=h.3whwml4)

[Appendix D: Screenshots Of Exploited Web App 16](#_heading=h.2bn6wsx)

[Appendix E: OSINT / Phishing Results Data Used 17](#_heading=h.qsh70q)

# Executive Summary

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec tortor lectus, blandit eget rhoncus vel, volutpat non eros. Donec tincidunt tristique diam eget pharetra. Donec blandit risus vitae porttitor suscipit. In

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec tortor lectus, blandit eget rhoncus vel, volutpat non eros. Donec tincidunt tristique diam eget pharetra. Donec blandit risus vitae porttitor suscipit. In eget orci sed leo efficitur molestie eu et lacus. Duis at venenatis

e sapien cursus accumsan tempor. Morbi ut massa diam. Donec pretium congue metus vel feugiat. Pellentesque ultrices urna et neque condimentum, eget lobortis massa pellentesque. Morbi maximus metus at dui finibus, non euismod purus consequat. Suspendisse hendrerit enim a pulvinar gravida. Phasellus odio nisi, euismod at nunc non, finibus varius felis. Maecenas quis pretium libero.

Phasellus ut maximus ligula. Suspendisse interdum metus quis velit elementum laoreet. Praesent non nunc pellentesque nulla accumsan egestas eget non arcu. Curabitur sagittis ac purus at rhoncus. Praesent rutrum gravida dui a finibus. Vestibulum vehicula id arcu vel dignissim. Nulla sed augue mi. Nullam non erat sapien. Pellentesque hendrerit elementum nulla id rutrum. Quisque vel felis ac lacus tincidunt hendrerit at ac mi. Aenean rhoncus trist.

# A Glance Through Target Security Posture



Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec tortor lectus, blandit eget rhoncus vel, volutpat non eros. Donec tincidunt

tristique diam eget pharetra. Donec blandit risus vitae porttitor suscipit. In eget orci sed leo efficitur molestie eu et lacus. Duis at venenatis turpis. Nunc lobortis malesuada v ere are 2 Vulnerabilities out of which 1 is.

****

Overall Security Rating – Some Action Attention Required/Should Be Considered/Needed

# Testing Methodology

# Tools & Websites Used



# Detailed Technical Reports (Scope Limited)

# example.com

This host contains 1 high and 3 medium vulnerabilities.

|  |  |  |  |
| --- | --- | --- | --- |
| **Total Findings** | **Critical** | **High** | **Medium** |
| **3** | **0** | **1** | **3** |

## 

## Finding X: Apache CouchDB Unauthenticated Administrative Access on port 5984 TCP– High

**Vulnerability Description:**

Nessus was able to perform administrative actions on the remote CouchDB server without providing authentication. A remote attacker could exploit this to take control of the CouchDB server.

**Exposure/Analysis:**

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec tortor lectus, blandit eget rhoncus vel, volutpat non eros. Donec tincidunt tristique diam eget pharetra. Donec blandit risus vitae porttitor suscipit. In eget orci sed leo efficitur molestie eu et lacus. Duis at venenatis turpis. Nunc lobortis malesuada viverra

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec tortor lectus, blandit eget rhoncus vel, volutpat leo efficitur molestie eu et lacus. Duis at venenatis turpis. Nunc lobortis malesuada viverra

**Recommendations:**

Secure the CouchDB installation with an administrative account.

## Steps to Reproduce

1. Lorem ipsum dolor sit amet, consectetur adipiscing elit.  
   **Lorem ipsum dolor sit amet, consectetur adipiscing elit.** 

## Finding X: HTTP TRACE / TRACK Methods Allowed on port 80 and 443 TCP– Medium

**Vulnerability Description:**

The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.

**Exposure/Analysis:**

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec tortor lectus, blandit eget rhoncus vel, volutpat non eros. Donec tincidunt tristique diam eget pharetra. Donec blandit risus vitae porttitor suscipit. In eget orci sed leo efficitur molestie eu et lacus. Duis at venenatis turpis. Nunc lobortis malesuada viverra

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec tortor lectus, blandit eget rhoncus vel, volutpat leo efficitur molestie eu et lacus. Duis at venenatis turpis. Nunc lobortis malesuada viverra

**Recommendations:**

Disable these HTTP methods.

## Steps to Reproduce

1. Lorem ipsum dolor sit amet, consectetur adipiscing elit.  
   **Lorem ipsum dolor sit amet, consectetur adipiscing elit.** A computer and a cup of coffee

   Description automatically generated with low confidence

## Finding X: Apache mod\_status /server-status Information Disclosure on port 443 TCP– Medium

**Vulnerability Description:**

A remote unauthenticated attacker can obtain an overview of the remote Apache web server's activity and performance by requesting the URL '/server-status'. This overview includes information such as current hosts and requests being processed, the number of workers idle and service requests, and CPU utilization.

**Exposure/Analysis:**

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec tortor lectus, blandit eget rhoncus vel, volutpat non eros. Donec tincidunt tristique diam eget pharetra. Donec blandit risus vitae porttitor suscipit. In eget orci sed leo efficitur molestie eu et lacus. Duis at venenatis turpis. Nunc lobortis malesuada viverra

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec tortor lectus, blandit eget rhoncus vel, volutpat leo efficitur molestie eu et lacus. Duis at venenatis turpis. Nunc lobortis malesuada viverra

**Recommendations:**

Update Apache's configuration file(s) to either disable mod\_status or restrict access to specific hosts.

## Steps to Reproduce

1. Lorem ipsum dolor sit amet, consectetur adipiscing elit.  
   **Lorem ipsum dolor sit amet, consectetur adipiscing elit.** A computer and a cup of coffee

   Description automatically generated with low confidence

# Appendixes

# Appendix A: Vulnerability Score Analysis – CVSS 3.0

**1. CVE-XXXX-XXXXX  
https://example.cco**

**Final Vector:**

**AV:SOMETHING AND SOMETHING**

**Adjusted Scores:**

**CVSS Base Score: X.X**

**Impact Subscore: X.X**

**Exploitability Subscore: X.X**

**CVSS Temporal Score: X.X**

**CVSS Environmental Score: X.X**

**Modified Impact Subscore: X.X**

**Overall CVSS Score: X.X**

**Risk Rating – Low/Medium/High/Critical**

# Appendix B: Modified Exploit Code For CVE-XXXX-XXXXX

***Example:***

#!/usr/bin/env python3

import requests

echo Some Random Code By Sagar Bansal;

<meta name="viewport" content="width=device-width, initial-scale=1">

<style>

body {background-color:#ffffff;background-repeat:no-repeat;background-position:top left;background-attachment:fixed;}

h1{font-family:Arial, sans-serif;color:#000000;background-color:#ffffff;}

p {font-family:Georgia, serif;font-size:14px;font-style:normal;font-weight:normal;color:#bc1a1a;background-color:#cba4a4;}

</style>

</head>

<body>

<h1>It Can Be Python, Ruby, PHP</h1>

<p>Here, it is HTML as it's just an example</p>

</body>

End();

# Appendix C: Screenshots For Nessus & Faraday

Graphical user interface

Description automatically generated

A screenshot of a computer

Description automatically generated

# Appendix D: Screenshots Of Exploited Web App



# Appendix E: OSINT / Phishing Results Data Used

