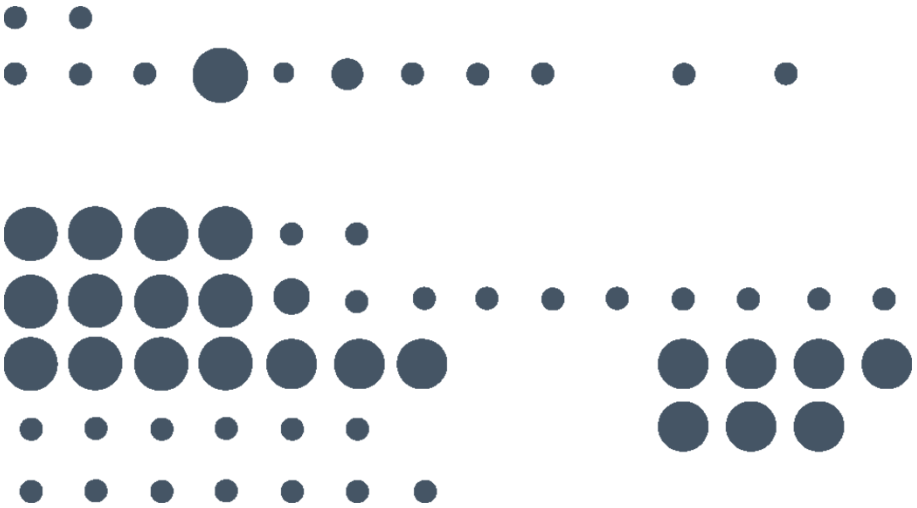
dimension data



VA Report – Platinum Credit Kenya

Internet Banking Penetration Testing and Vulnerability Assessment

31 October 2022 | Document Version 0.02

Dimension Data contact details

We welcome any enquiries regarding this document, its content, structure, or scope. Please contact:

Ayub Mwangi - Senior Information Security Engineer, Mobile Phone: 0727517942

Dimension Data Solutions Ltd

Purshottam Place

Westlands Road

Nairobi

0727517942

ayub.mwangi@dimensiondata.com

Please quote reference in any correspondence or order.

Confidentiality

This document contains confidential and proprietary information of Dimension Data Solutions Ltd ('Dimension Data'). Platinum Credit Kenya may not disclose the confidential information contained herein to any third party without the written consent of Dimension Data, save that Platinum Credit Kenya may disclose the contents of this document to those of its agents, principals, representatives, consultants or employees who need to know its contents for the purpose of Platinum Credit Kenya's evaluation of the document. Platinum Credit Kenya agrees to inform such persons of the confidential nature of this document and to obtain their agreement to preserve its confidentiality to the same extent as Platinum Credit Kenya. As a condition of receiving this document, Platinum Credit Kenya agrees to treat the confidential information contained herein with at least the same level of care as it takes with respect to its own confidential information, but in no event with less than reasonable care. This confidentiality statement shall be binding on the parties for a period of five (5) years from the issue date stated on the front cover unless superseded by confidentiality provisions detailed in a subsequent agreement.

Terms and conditions

This document is valid until 30 November 2022 and, in the absence of any other written agreement between the parties, Dimension Data and Platinum Credit Kenyaacknowledge and agree is subject to Dimension Data's standard terms and conditions which are available on request or at dimensiondata.com/en-gb/legal . Dimension Data reserves the right to vary the terms of this document in response to changes to the specifications or information made available by Faulu. Submission of this document by Dimension Data in no way conveys any right, title, interest, or license in any intellectual property rights (including but not limited to patents, copyrights, trade secrets or trademarks) contained herein. All rights are reserved.

Dimension Data does not assume liability for any errors or omissions in the content of this document or any referenced or associated third party document, including, but not limited to, typographical errors, inaccuracies, or out-dated information. This document and all information within it are provided on an 'as is' basis without any warranties of any kind, express or implied. Any communication required or permitted in terms of this document shall be valid and effective only if submitted in writing.

All contracts with Dimension Data will be governed by Kenyan Law and be subject to the exclusive jurisdiction of the Kenyan courts.

Document configuration management

Document identification

Title	Internet Banking Penetration Testing and Vulnerability Assessment
Document Type	VAPT Report
File Name	output.docx
Version	Version 0.01
Sensitivity Classification	Company Confidential - Client / Vendor Information
Document Owner	Ayub Mwangi

Preparation

Action	Name	Role / Function	Date
Prepared by:	Rashpal Mediratta	Information Security Engineer	2022-11-28
Reviewed/Approved by:	Ayub Mwangi	Senior Information Security Engineer	2022-11-28

Release

	Date Released	Change Notice	Remarks
0.01	2022-06-17	Release	1st Draft

Contribution (C) and distribution (D) list

Name	C/D	Organisation	Title
Rashpal Mediratta	C	Dimension Data	Information Security Engineer
Ayub Mwangi	C & D	Dimension Data	Senior Information Security Engineer

Table of Contents

List of Figures

List of Tables

1. About This Design Document

1.1. Document Purpose

A vulnerability assessment (VA) report summarizes the findings of a vulnerability assessment, which is a process of identifying, analyzing, and prioritizing vulnerabilities in an organization's assets

The purpose of this document is to provide in detail the recommended findings and remediations for the IP/Sytems in scope. This document provides details on the findings and remediations that can be implemented to have a better overall security posture.

1.2. Intended Audience

The intended audience of this document are Platinum Credit Kenya / Dimension Data technical staff who will be implementing and operating the new network.

1.3. Document Usage Guidelines

The document should be used as a guideline for deriving the necessary information to ultimately remediate the findings that were discovered during the external assessment.

- This document comprises the following components: -
- In Scope URL’s
- Findings
- Remediations
- Vulnerability References
- Evidence

2. Executive Summary

2.1. Introduction

We have the pleasure of presenting the main findings on our VA scan of as enumerated and documented in the shared IPs. We also want to express our appreciation to for the support given by the respective staff during this review.

2.2. Scope

The following IP addresses were in scope for the vulnerability Assessment:

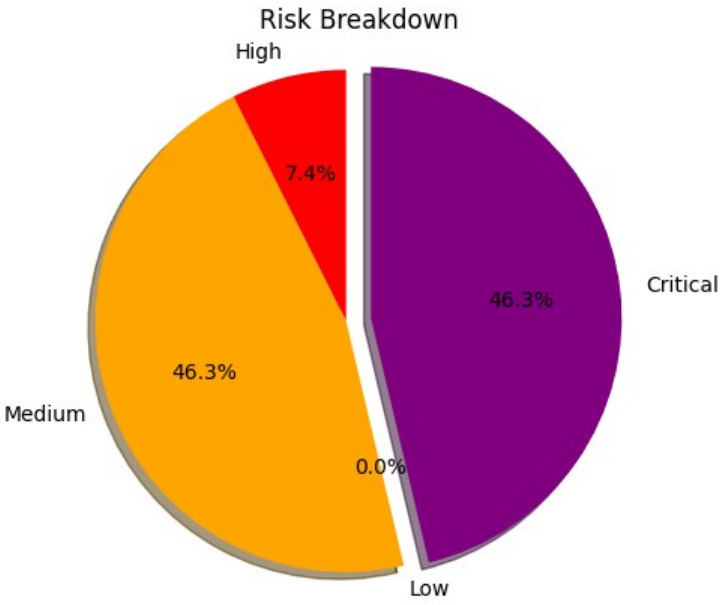
IPs	IPs platinumcredit.co.ke,helpdesk.platinumcredit.co.ke,legal.platinumcredit.co.ke,payroll.platinumcredit.co.ke,lbfapp.platinumcredit.co.ke,chqtracker.platinumcredit.co.ke,hr.platinumcredit.co.ke,lbfupdates.platinumcredit.co.ke,recordings.platinumcredit.co.ke,cms.platinumcredit.co.ke,dms.platinumcredit.co.ke,lms.platinumcredit.co.ke,ess.platinumcredit.co.ke,academy.platinumcredit.co.ke

2.3. Risk Break down

This Is a severity based approach which involves ranking vulnerabilities based on the potential impact they could have on an organization's assets, such as the potential for data loss, disruption of service, or unauthorized access to sensitive information.

Vulnerabilities with a higher potential impact are typically considered more severe and are given a higher priority for remediation.

The breakdown of the vulnerabilities is as follows: Critical Vulnerabilities account for 46.3% of the total vulnerabilities, High severity vulnerabilities account for 7.41% of the total vulnerabilities, Medium severity vulnerabilities account for 46.3% of the total vulnerabilities, Low severity vulnerabilities account for 0% of the total vulnerabilities. Highest risk is Critical


Risk Breakdown
High
7.4%
Critical
46.3%
Medium
46.3%
0.0%
Low

2.4. Host Breakdown

In the context of vulnerabilities, a host refers to a computer, device, or network that is connected to the internet or another network and is potentially vulnerable to attack.

The host with the highest risk is academy.platinumcredit.co.ke with 27 vulnerabilities,which accounts for 50.0% of the total vulnerabilities.The Top 5 hosts with the most vulnerabilities are: ['academy.platinumcredit.co.ke', 'chqtracker.platinumcredit.co.ke', 'cms.platinumcredit.co.ke', 'ess.platinumcredit.co.ke', 'hr.platinumcredit.co.ke'] with [27, 2, 6, 3, 4] vulnerabilities which accounts for 77.78% of the total vulnerabilities respectively.

2.5. Common Vulnerabilities

The frequency of vulnerabilities refers to how often new vulnerabilities are discovered in systems, applications, or networks.

The most common vulnerability is Apache 2.4.x 2.4.54 Multiple Vulnerabilities with 8 occurences and a risk of Critical. Its solution is to Upgrade to Apache version 2.4.54 or later.The second most common vulnerability is Apache 2.4.x 2.4.47 Multiple Vulnerabilities with 7 occurences and a risk of Critical. Its solution is to Upgrade to Apache version 2.4.47 or later.The third most common vulnerability is HSTS Missing From HTTPS Server (RFC 6797) with 6 occurences

2.6. Critical Vulnerabilities

Critical vulnerabilities are vulnerabilities that have the potential to cause significant damage to an organization's assets or compromise the confidentiality, integrity, or availability of sensitive information.

These types of vulnerabilities are typically considered the most serious and should be prioritized for remediation as soon as possible.

The most common vulnerability is Apache 2.4.x 2.4.54 Multiple Vulnerabilities with 8 occurencesand a risk of Critical. Its solution is to Upgrade to Apache version 2.4.54 or later.The Second most common vulnerability is Apache 2.4.x 2.4.47 Multiple Vulnerabilities with 7 occurencesand a risk of Critical. Its solution is to Upgrade to Apache version 2.4.47 or later.The Third most common vulnerability is Apache 2.4.x 2.4.53 Multiple Vulnerabilities with 4 occurences and a risk of Critical. Its solution is to Upgrade to Apache version 2.4.53 or later.

2.7. Risk Rating Matrix

Risks are classified as Critical, High, Moderate or Low as per the matrix defined below.

Rating	Description
Critical	Loss of [confidentiality | integrity | availability] is proven and is currently being exploited in the wild. Countermeasures recommended to mitigate these risks should be implemented as soon as possible and the environment should be reviewed for any signs of compromise.
High	Loss of [confidentiality | integrity | availability] is likely to have a serious adverse effect on the organization or individuals associated with the organization (e.g., employees, customers). Countermeasures recommended to mitigate these risks should be implemented as soon as possible
Medium	Loss of [confidentiality | integrity | availability] is likely to have a moderately adverse effect on the organization or individuals associated with the organization (e.g., employees, customers). Countermeasure implementation should be planned for the near future
Low	Loss of [confidentiality | integrity | availability] is likely to have only a limited to little adverse effect on the organization or individuals associated with the organization (e.g., employees, customers). Countermeasure implementation will enhance security and is of less urgency than the above risks.

Table 1: Risk Rating Matrix

2.8. Vulnerability Assessment Summary Findings

This section details the summary findings of the vulnerability Assessment conducted on the IPs in scope.

NB: The detailed findings have been shared as an addendum to this report. It serves as the remediation tracker

2.8.1 Vulnerability Count

IP Address	Critical	High	Medium	Low
academy.platinumcredit.co.ke	7	2	0	0
chqtracker.platinumcredit.co.ke	0	0	2	0
cms.platinumcredit.co.ke	0	1	4	0
dms.platinumcredit.co.ke	0	0	0	0
ess.platinumcredit.co.ke	0	0	3	0
helpdesk.platinumcredit.co.ke	0	0	0	0
hr.platinumcredit.co.ke	0	0	4	0
lbfapp.platinumcredit.co.ke	0	1	7	0
lbfupdates.platinumcredit.co.ke	0	0	0	0
legal.platinumcredit.co.ke	0	0	0	0
lms.platinumcredit.co.ke	0	0	4	0
payroll.platinumcredit.co.ke	0	0	0	0

IP Address	Critical	High	Medium	Low
platinumcredit.co.ke	0	0	0	0
recordings.platinumcredit.co.ke	0	0	0	0
Total	0	0	0	0

Table 2: Vulnerability Count Per Host

2.8.2 Summary of Vulnerabilities

This section defines the Vulnerabilities found, their count as well as their risks.

Vulnerability	Count	Severity
web.config File Information Disclosure	1	Medium
Web Application Potentially Vulnerable to Clickjacking	1	Medium
SSL Certificate Expiry	1	Medium
JQuery 1.2 3.5.0 Multiple XSS	1	Medium
Browsable Web Directories	1	Medium
nginx 1.17.7 Information Disclosure	2	Medium
TLS Version 1.1 Protocol Deprecated	3	Medium
TLS Version 1.0 Protocol Detection	3	Medium
SSL Certificate Cannot Be Trusted	5	Medium
HSTS Missing From HTTPS Server (RFC 6797)	6	Medium
Apache >= 2.4.30 2.4.49 mod_proxy_uwsgi	1	High
Apache >= 2.4.17 2.4.49 mod_http2	1	High
SSL Medium Strength Cipher Suites Supported (SWEET32)	2	High
Apache 2.4.49 Multiple Vulnerabilities	1	Critical
Apache 2.4.49 Multiple Vulnerabilities	1	Critical
Apache 2.4.x >= 2.4.7 / 2.4.52 Forward Proxy DoS / SSRF	1	Critical
Apache 2.4.x 2.4.54 Multiple Vulnerabilities	1	Critical
Apache 2.4.x 2.4.53 Multiple Vulnerabilities	1	Critical
Apache 2.4.x 2.4.52 mod_lua Buffer Overflow	1	Critical
Apache 2.4.x 2.4.47 Multiple Vulnerabilities	1	Critical

Table 3: Summary of Key Findings

2.8.3 Prioritizations

This section indicates which vulnerabilities on which asset poses the greatest risk to Platinum Credit Kenya We recommend that they are addressed first to address the highest risks.

The following factors have been taken into consideration when prioritizing vulnerabilities:

1. The severity of the vulnerability
2. The severity of the vulnerability
3. The complexity of the vulnerability
4. The availability of a fix or workaround
5. The potential for damage

Vulnerability Title	**Apache 2.4.x >= 2.4.7 / 2.4.52 Forward Proxy DoS / SSRF**	
Risk Profile	CVSS3 Score	7.5
	Risk Factor	High
Exploitability	Ease	No known exploits are available
	Exploit Available	false Exploited by malware:
IP	academy.platinumcredit.co.ke	
Synopsis	The remote web server is affected by a denial of service or server-side request forgery vulnerability.	
Solution	Upgrade to Apache version 2.4.52 or later.	
Reference	CVE	CVE-2021-44790
	Links	
Vulnerability Title	**Apache 2.4.x 2.4.53 Multiple Vulnerabilities**	
Risk Profile	CVSS3 Score	7.5
	Risk Factor	High
Exploitability	Ease	No known exploits are available

	Exploit Available	false Exploited by malware:
IP	academy.platinumcredit.co.ke	
Synopsis	The remote web server is affected by multiple vulnerabilities.	
Solution	Upgrade to Apache version 2.4.53 or later.	
Reference	CVE	CVE-2022-23943
	Links	http://www.apache.org/dist/httpd/Announcement2.4.html https://httpd.apache.org/security/vulnerabilities_24.html
Vulnerability Title	**Apache 2.4.x 2.4.52 mod_lua Buffer Overflow**	
Risk Profile	CVSS3 Score	7.5
	Risk Factor	High
Exploitability	Ease	No known exploits are available
	Exploit Available	false Exploited by malware:
IP	academy.platinumcredit.co.ke	
Synopsis	The remote web server is affected by a buffer overflow vulnerability.	
Solution	Upgrade to Apache version 2.4.52 or later.	
Reference	CVE	CVE-2021-44790
	Links	
Vulnerability Title	**Apache 2.4.49 Multiple Vulnerabilities**	
Risk Profile	CVSS3 Score	6.8
	Risk Factor	Medium

Exploitability	Ease	Exploits are available
	Exploit Available	true Exploited by malware:
IP	academy.platinumcredit.co.ke	
Synopsis	The remote web server is affected by a vulnerability.	
Solution	Upgrade to Apache version 2.4.49 or later.	
Reference	CVE	CVE-2021-40438
	Links	https://downloads.apache.org/httpd/CHANGES_2.4 https://httpd.apache.org/security/vulnerabilities_24.html
Vulnerability Title	**Apache 2.4.x 2.4.47 Multiple Vulnerabilities**	
Risk Profile	CVSS3 Score	7.5
	Risk Factor	High
Exploitability	Ease	No known exploits are available
	Exploit Available	Exploited by malware:
IP	academy.platinumcredit.co.ke	
Synopsis	The remote web server is affected by multiple vulnerabilities.	
Solution	Upgrade to Apache version 2.4.47 or later.	
Reference	CVE	CVE-2021-26691
	Links	https://downloads.apache.org/httpd/CHANGES_2.4
Vulnerability Title	**Apache 2.4.49 Multiple Vulnerabilities**	
Risk Profile	CVSS3 Score	7.5
	Risk Factor	High

Exploitability	Ease	No known exploits are available
	Exploit Available	Exploited by malware:
IP	academy.platinumcredit.co.ke	
Synopsis	The remote web server is affected by a vulnerability.	
Solution	Upgrade to Apache version 2.4.49 or later.	
Reference	CVE	CVE-2021-39275
	Links	https://downloads.apache.org/httpd/CHANGES_2.4 https://httpd.apache.org/security/vulnerabilities_24.html
Vulnerability Title	**Apache 2.4.x 2.4.54 Multiple Vulnerabilities**	
Risk Profile	CVSS3 Score	7.5
	Risk Factor	High
Exploitability	Ease	No known exploits are available
	Exploit Available	false Exploited by malware:
IP	academy.platinumcredit.co.ke	
Synopsis	The remote web server is affected by multiple vulnerabilities.	
Solution	Upgrade to Apache version 2.4.54 or later.	
Reference	CVE	CVE-2022-31813
	Links	https://httpd.apache.org/security/vulnerabilities_24.html
Vulnerability Title	**JQuery 1.2 3.5.0 Multiple XSS**	
	CVSS3 Score	4.3

Risk Profile	Risk Factor	Medium
Exploitability	Ease	Exploits are available
	Exploit Available	true Exploited by malware:
IP	cms.platinumcredit.co.ke	
Synopsis	The remote web server is affected by multiple cross site scripting vulnerability.	
Solution	Upgrade to JQuery version 3.5.0 or later.	
Reference	CVE	CVE-2020-11022
	Links	https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/ https://security.paloaltonetworks.com/PAN-SA-2020-0007
Vulnerability Title	**SSL Medium Strength Cipher Suites Supported (SWEET32)**	
Risk Profile	CVSS3 Score	5.0
	Risk Factor	Medium
Exploitability	Ease	
	Exploit Available	Exploited by malware:
IP	lbfapp.platinumcredit.co.ke cms.platinumcredit.co.ke	
Synopsis	The remote service supports the use of medium strength SSL ciphers.	
Solution	Reconfigure the affected application if possible to avoid use of medium strength ciphers.	
Reference	CVE	CVE-2016-2183
	Links	https://www.openssl.org/blog/blog/2016/08/24/sweet32/ https://sweet32.info

Vulnerability Title	Apache >= 2.4.17 2.4.49 mod_http2	
Risk Profile	CVSS3 Score	5.0
	Risk Factor	Medium
Exploitability	Ease	No known exploits are available
	Exploit Available	Exploited by malware:
IP	academy.platinumcredit.co.ke	
Synopsis	The remote web server is affected by a vulnerability.	
Solution	Upgrade to Apache version 2.4.49 or later.	
Reference	CVE	CVE-2021-33193
	Links	https://downloads.apache.org/httpd/CHANGES_2.4 https://httpd.apache.org/security/vulnerabilities_24.html

Table 4: Prioritizations

2.8.4 Strategic Recommendations

To continuously map out and manage the attack surface, have a patch management process in place to:

1. Remove unused dependencies, unnecessary features, components, files, and documentation.
2. Continuously inventory the versions of both client-side and server-side components (e.g., frameworks, libraries) and their dependencies
3. Monitor for libraries and components that are unmaintained or do not create security patches for older versions. If patching is not possible, consider deploying a virtual patch to monitor, detect, or protect against the discovered issue.
4. A penetration test should be done when considerable change has been introduced to the system.

Appendix A VAPT Report acceptance

I hereby confirm acceptance and agreement of VAPT Report document for the Internet Banking Penetration Testing and Vulnerability Assessment for and the contents contained within, excluding the exceptions described in the notes below.

Notes:

Dimension Data	
Signature	Signature
Print Name and Title	Print Name and Title
Date	Date

should send this signed VAPT Report Acceptance Sheet to ayub.mwangi@dimensiondata.com