[redacted]

Safety Assessment Results Report

Business Confidential

Date: August 1, 2023
Project: DC-001
Version 1.0

ADF SECURITY

Table of Contents

Privacy Statement

This document is the exclusive property of [redacted] and ALV Security (ALVS). This document contains confidential and proprietary information. Duplication, redistribution or use, in whole or in part, in any way, requires the consent of both [redacted] and ALVS.

[redacted] may share this document with auditors under confidentiality agreements to demonstrate compliance with penetration testing requirements.

Resignation

A penetration test is considered a snapshot in time. The conclusions and recommendations reflect the information gathered during the evaluation but not the changes or modifications made outside that period.

Time-limited commitments do not allow for a full assessment of all security controls. ALVS prioritized assessment to identify the weakest security controls that an attacker would exploit. ALVS recommends conducting similar evaluations annually by internal or external evaluators to ensure the continued success of the controls.

Contact Information

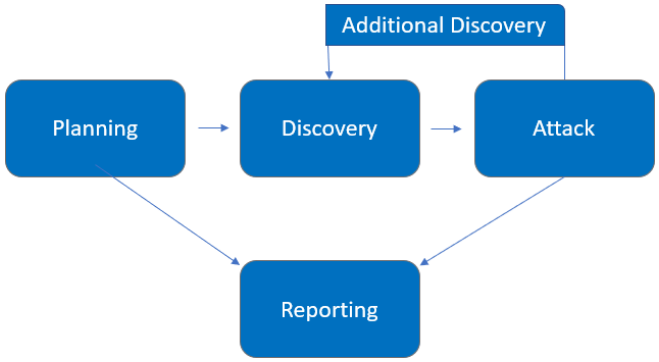
Name	Title	Contact Information
[redacted]		
[redacted]	[redacted]	Email: [redacted]
ALV Security		
[redacted]	[redacted]	Email: [redacted]

Assessment Overview

From August 1, 2023 to August 4, 2023, [redacted] engaged ALVS to assess the security posture of its infrastructure against current industry best practices that included an internal network penetration test. All tests performed are based on NIST SP *800-115 Technical Guide for Information Security Testing and Assessment, OWASP Test Guide (v4), and custom test frameworks*.

The phases of penetration testing activities include the following:

- Planning: The client's objectives are collected and the rules of engagement are obtained.
- Detection: Perform analysis and enumeration to identify potential vulnerabilities, weak areas, and vulnerabilities.
- Attack: Confirm potential vulnerabilities through exploitation and make additional discoveries upon new access.
- Reporting: Document all vulnerabilities and vulnerabilities found, failed attempts, and company strengths and weaknesses.



Evaluation Components

External Penetration Test

An external penetration test emulates the role of an attacker trying to gain access to an internal network without internal resources or internal knowledge. An ALVS engineer attempts to collect sensitive information through open-source intelligence (OSINT), including employee information, breached historical passwords, and more that can be leveraged against external systems to gain access to the internal network. The engineer also performs scanning and enumeration to identify potential vulnerabilities in hopes of exploiting them.

Find severity ratings

The following table defines the severity levels and the corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

Severity	CVSS V3 Scoring Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is recommended to form an action plan and patch immediately.
High	7.0-8.9	Exploitation is more difficult, but it could cause elevated privileges and potentially data loss or downtime. It is recommended to form an action plan and patch as soon as possible.
Moderate	4.0-6.9	The vulnerabilities exist but are not exploitable or require additional steps such as social engineering. It is recommended to form an action plan and patch after high-priority issues have been resolved.
Low	0.1-3.9	The vulnerabilities are not exploitable, but they would reduce an organization's attack surface. It is recommended that you form an action and patch plan during the next maintenance window.
Informative	N/A	There is no vulnerability. Additional information is provided on the items observed during testing, robust controls, and additional documentation.

Risk factors

Risk is measured by two factors: Probability and impact:

Probability

Probability measures the potential for a vulnerability to be exploited. Ratings are awarded based on the difficulty of the attack, the tools available, the attacker's skill level, and the customer's environment.

Impact

Impact measures the effect of potential vulnerability on operations, including the confidentiality, integrity, and availability of customer systems and/or data, reputational damage, and financial loss.

Scope

Evaluation	Details
Internal Penetration Test	[redacted]

Scope exclusions

At the customer's request, ALVS did not perform any of the following attacks during testing:

- Denial of Service (DoS)
- Phishing/Social Engineering

All other attacks not specified above were allowed by [redacted].

Customer Assignments

[redacted] has not provided any allowances to assist with testing.

Executive Summary

ALVS assessed [redacted]'s internal security posture through penetration testing from August 1, 2023 to August 4, 2023. The following sections provide a high-level overview of the vulnerabilities discovered, successful and failed attempts, and strengths and weaknesses.

Scope and time constraints

Outreach during engagement did not allow for denial of service or social engineering on all test components.

Time constraints were set for testing. Internal network penetration testing was allowed for four (4) business days.

Tester Notes and Recommendations

The results of the tests of the [redacted] network are indicative that an organization undergoes its first penetration test, which is the case that concerns us. Many of the findings discovered are vulnerabilities within the Cross-Site Scripting framework.

During testing, two constants stood out: a medium password policy and weak patches. We recommend that [redacted] reevaluate its current password policy and consider a policy of 15 characters or more for its normal user accounts and 30 characters or more for its domain administrator accounts. We also recommend that [redacted] scan the password blacklist and provide a list of cracked user passwords for the team to evaluate. Finally, a privilege access management solution should be considered.

We recommend that the [redacted] team review the patch recommendations made in the Technical Findings section of the report along with the review of the provided Nessus scans for a complete description of the items to be patched. We also recommend that [redacted] improve its patch management policies and procedures to help prevent potential attacks within your network.

On a positive note, our testing team triggered several alerts during the engagement. [redacted]'s security operations team discovered our vulnerability scan and was alerted when we tried to use noisy attacks on a compromised machine. While not all attacks were discovered during testing, these alerts are a positive start. Additional guidance on alerting and detection for findings, where necessary, has been provided in the Technical Findings section.

Overall, [redacted]'s network performed as expected for a first-time penetration test. We recommend that the [redacted] team thoroughly review the recommendations made in this report, review the findings, and retest annually to improve their overall internal security posture.

Key strengths and weaknesses

Key strengths identified during the assessment are identified below:

1. Some scanning of common enumeration tools (Nessus) was observed
2. The password policy is average, it does not allow you to create an account without a minimum of 8 special characters.
3. TLS Protocol Version 1.0 Detected
4. Deprecated TLS Version 1.1 protocol detected
5. HTTP TRACE/TRACK methods allowed on the remote web server

Vulnerability summary and report card

The following tables illustrate the vulnerabilities detected by the impact and recommended fixes:

Internal Penetration Test Results

0	0	3	0	27
Critical	High	Moderate	Low	Informative

Find	Severity	Recommendation
Internal Penetration Test		

Find	Severity	Recommendation
TLS Version 1.0 Protocol Detection	Moderate	Enable support for TLS 1.2 and 1.3 and disable support for TLS 1.0.
TLS Version 1.1 Protocol Deprecated	Moderate	Enable TLS 1.2 and/or 1.3 support and disable TLS 1.1 support.
HTTP TRACE / TRACK Methods Allowed	Moderate	Disable these HTTP methods. See the add-on output for more information.
Additional DNS Hostnames	Informative	Use special vhost syntax, such as: www.example.com[192.0.32.10]
Apache HTTP Server Version	Informative	It is possible to obtain the version number of the remote Apache HTTP server.
Common Platform Enumeration (CPE)	Informative	It is possible to list the CPE names that matched on the remote system.
Device Type	Informative	It is possible to guess the type of remote device.
HSTS Missing From HTTPS Server	Informative	Configure the remote web server to use HSTS.
HTTP Server Type and Version	Informative	This plugin attempts to determine the type and version of the remote web server.
HyperText Transfer Protocol (HTTP) Information	Informative	Some information about the remote HTTP configuration can be extracted.
Nessus SYN scanner	Informative	Protect your lens with an IP filter.
Nessus Scan Information	Informative	This plugin displays information about Nessus scanning.
OS Identification	Informative	It is possible to guess the remote

		operating system.
OpenSSL Detection	Informative	The remote service appears to use OpenSSL to encrypt traffic.
SSL / TLS Versions Supported	Informative	Remote service encrypts communications.
SSL Certificate Chain Contains Unnecessary Certificates	Informative	Remove unnecessary certificates from the certificate chain.
SSL Certificate Chain Not Sorted	Informative	Reorder the certificates in the certificate chain.
SSL Certificate Information	Informative	This plugin displays the SSL certificate.
SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)	Informative	Contact the certificate authority to have the certificate reissued.
SSL Cipher Block Chaining Cipher Suites Supported	Informative	The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine earlier blocks with later ones.
SSL Cipher Suites Supported	Informative	SSL Cipher Suites Supported
SSL Perfect Forward Secrecy Cipher Suites Supported	Informative	The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even in the event of key theft.
SSL Root Certification Authority Certificate Information	Informative	Ensure that the use of this CA root certificate complies with your organization's acceptable security and use policies.
SSL/TLS Recommended Cipher Suites	Informative	Only enable support for recommended cipher suites.
Service Detection	Informative	Remote service could be identified.
TLS Version 1.1 Protocol Detection	Informative	Enable TLS 1.2 and/or 1.3 support and disable TLS 1.1 support.
TLS Version 1.2 Protocol Detection	Informative	The remote service accepts encrypted connections using TLS 1.2.
Traceroute Information	Informative	It was possible to obtain traceroute information to the remote host.
Web Server No 404 Error Code Check	Informative	The remote web server does not return 404 error codes.

Web Application Cookies Are Expired	Informative	Each cookie should be carefully reviewed to determine whether contains sensitive data or if relied upon for a security decision. Set an expiration date in the future for the cookie to persist or remove the Expires cookie attribute altogether to convert the cookie to a session cookie.

Technical findings

Penetration Test Results

XXS Sensitive Stored (Moderate)

Description:	On its website [redacted] is sensitive to XXS through the Surname field, you can save the following code: <script>prompt(1)</script> and a prompt appears with which you can inject sequences of malicious code or scripts.
Risk:	It is risky since the attack occurs in the website code that runs in the browser, and not on the site's server. It can steal cookies, personal data, credentials, access to computer control.
System:	[redacted]
References:	mitre.org: Attacks of XXS https://portswigger.net/web-security/cross-site-scripting

Evidence

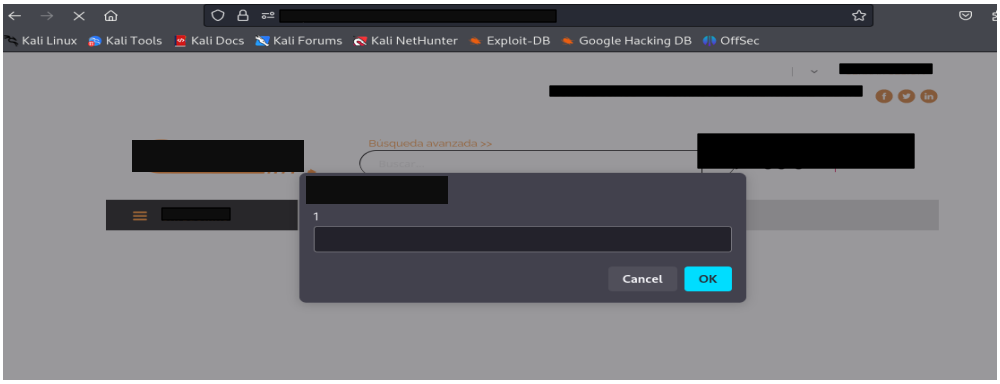


Figure 1: Prompt

Mitigation

It filters user data input as specifically as possible and scrambles the output data for users (HTML, URLs, JavaScript, and CSS). Check out the OWASP guide here.

Implements a WAF (Web Application Firewall) As with SQL injections, a web application firewall helps prevent the execution of XSS attacks, filtering and monitoring HTTP traffic between an application and the Internet.

Missing Content-Type Header (Moderate)

Description:	A missing header was detected, which means that this website could be at risk of MIME detection attacks.
Risk:	MIME type tracing is a standard functionality in browsers to find a proper way to render data where the HTTP headers sent by the server are inconclusive or missing. This allows older versions of Internet Explorer and Chrome to perform a MIME trace on the response body, which could cause the response body to be interpreted and displayed as a different content type than the intended content type. The problem arises once a website allows users to upload content that is then published to the web server. If an attacker can carry out an XSS (Cross-site Scripting) attack by manipulating the content in a way that it is accepted by the web application and rendered as HTML by the browser, it is possible to inject code, for example, into an image file and have the victim execute it by viewing the image.
System:	[redacted]
References:	https://www.invicti.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/

Mitigation

When serving resources, be sure to submit the content type header so that it appropriately matches the type of resource being given. Add the X-Content-Type-Options header with a value of "nosniff" to inform the browser that it trusts that what the site has sent is the appropriate content type.

TLS Version 1.1 Protocol Deprecated (Moderated)

Description:	The remote service encrypts traffic using an earlier version of TLS.
Risk:	The remote service accepts encrypted connections using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC compute and authenticated encryption modes such as GCM cannot be used with TLS 1.1 As of March 31, 2020, endpoints that are not enabled for TLS 1.2 and later versions will no longer work properly with major web browsers and major vendors.
System:	[redacted]
References:	http://www.nessus.org/u?c8ae820d https://datatracker.ietf.org/doc/html/rfc8996

Mitigation

Enable TLS 1.2 and/or 1.3 support and disable TLS 1.1 support. Follow Microsoft's guidance here.

HTTP TRACE / TRACK Methods Allowed (Moderate)

Description:	The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods used to debug web server connections
Risk:	A Cross-Site Tracing (XST) attack involves the use of Cross-Site Scripting (XSS) and the TRACE or TRACK HTTP methods. According to RFC 2616, "TRACE allows the client to see what is being received at the other end of the request chain and use that data to test or diagnose information." The TRACK method works the same way but is specific to Microsoft IIS. Web server. XST could be used as a method to steal the user's cookies through Cross-site Scripting (XSS), even if the cookie has the "HttpOnly" flag set or exposes the user's authorization header.
System:	[redacted]
References:	http://www.apacheweek.com/issues/03-01-24 https://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf

Mitigation

Disable these HTTP methods. See the add-on output for more information. Follow the OWASP guide here. On Apache versions 1.3.34, 2.0.55, and later, set the TraceEnable policy to "off" in the main configuration file, and then restart Apache. See TraceEnable for more information.

Last page