FORVIS

PENETRATION TESTING REPORT / UNEMPLOYMENT COMPENSATION MODERNIZATION AND IMPROVEMENT COUNCIL, STATE OF KANSAS

AS OF APRIL 20, 2022

FORVIS

Two Leadership Square South Tower, 211 N. Robinson Avenue, Suite 600 / Oklahoma City, OK 73102
P 405.606.2580 / **F** 405.600.9799
forvis.com

April 20, 2022

Unemployment Compensation Modernization and Improvement Council, State of Kansas
300 SW 10th Ave., Ste. 551
Topeka, KS 66612

We have performed the procedures enumerated in this report, which were agreed to by the Unemployment Compensation Modernization and Improvement Council (the Council) pursuant to our contract dated January 4, 2022, and addendum signed May 17, 2022, solely to assist you with respect to evaluating the Kansas Department of Labor's external and internal network security, including website security. Neither our services nor our reports shall in any way guarantee that the Council will not have a data breach, identity theft, network hacking, ransomware, etc. While our services and reports may contain findings, recommendations, and identify potential cybersecurity threats, the management of KDOL is responsible for the overall security of the Kansas Department of Labor's network. Had we performed additional procedures, other findings of significance may have been reported to you. The sufficiency of the procedures is solely the responsibility of the parties specified in this report. Management is also responsible for identifying and ensuring compliance with all laws and regulations applicable to its activities.

We were not engaged to, and did not, conduct an examination, the objective of which would be the expression of an opinion on the internal control systems management has in place. Accordingly, we do not express such an opinion.

Our report is intended for use only by the Council solely for reporting findings with respect to the procedures performed by us. This report is not intended to be, and should not be, used by anyone other than these specified parties unless express written consent is obtained from FORVIS.

We wish to take this opportunity to thank Kansas Department of Labor's management and staff members who contributed positively to our efforts. We would be pleased to further discuss any of the items in this report at your convenience.

FORVIS, LLP

FORVIS, LLP

Table of Contents

Executive Summary

Forward Vision Drives Our Unmatched Client Experiences™

We are pleased to provide our report on the penetration testing procedures performed by **FORVIS, LLP** ("FORVIS") for the Kansas Department of Labor as of April 20, 2022. The overall objective of this engagement is to assist the Council with assessing the confidentiality, integrity, and availability of their information and systems.

The penetration testing procedures included:

- External Penetration Testing
- Internal Penetration Testing including Web Application Security Testing
- Social Engineering

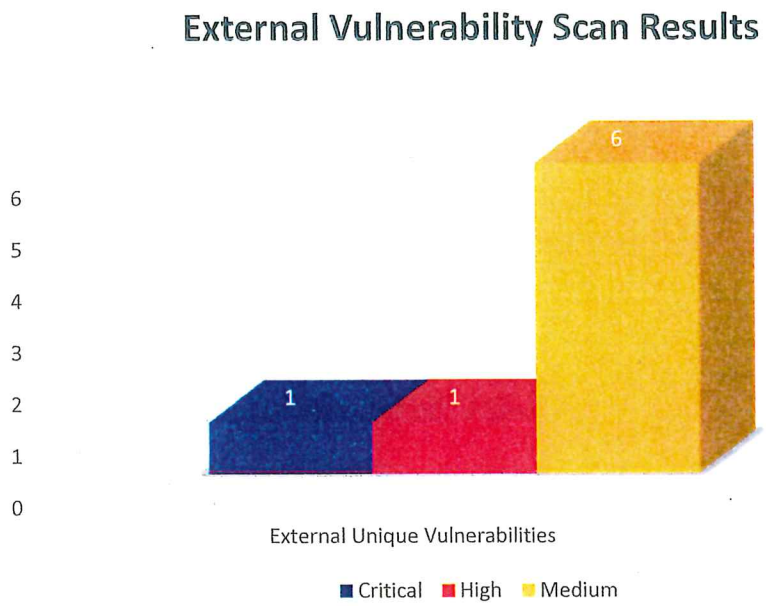
The procedures we developed, the Council approved per the contract dated January 4, 2022, and we performed are included in Section VI. The results of our procedures were discussed with Kansas Department of Labor's management at the conclusion of our engagement and are included in Section V.

Prior to the start of testing, a penetration testing device was shipped to Kansas Department of Labor and connected to the internal network for the purpose of executing the engagement from the agreed-upon simulation. The provided device was connected to the network by the State's IT staff. Remote access to the device was granted to the tester. Testing credentials for the development website were provided.

The scope of work included social engineering, internal penetration testing of the external and internal IP addresses associated with the State, and the development and production website for the unemployment benefits. The addresses and URLs included and were verified by Rob Sipes, Information Security Officer.

External Vulnerability Scan Results

The Kansas Department of Labor had eight unique results based on the Common Vulnerability Scoring System (CVSS), ranked Medium to Critical, which is defined in Section III. The graph below shows the number of findings by rating. Due to the confidential nature and security risks with IP addresses, that information is available to the State of Kansas upon request.

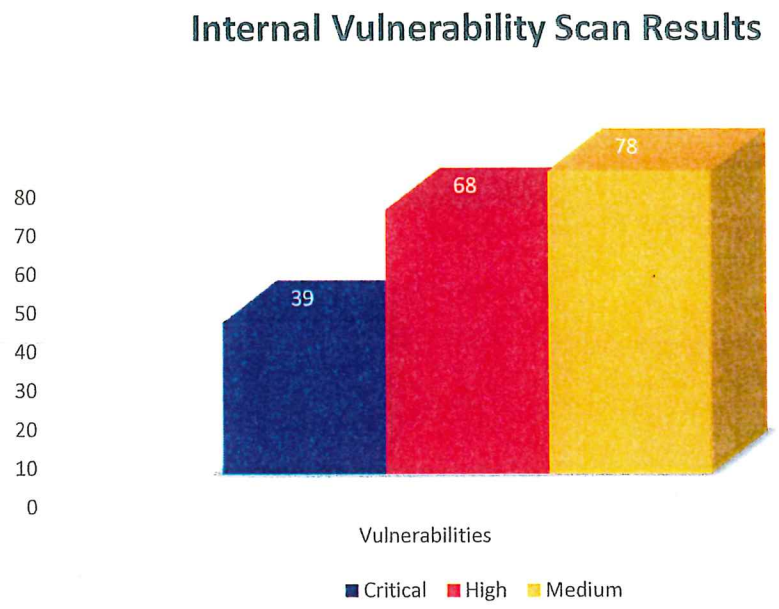


External Penetration Test Findings

The State had no findings based on probability and impact, which are defined in Section III.

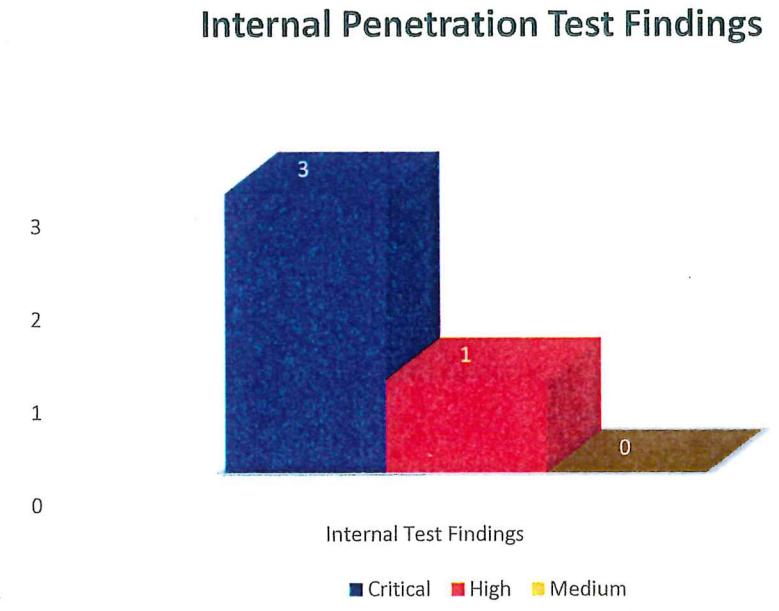
Internal Vulnerability Scan Results

The State had 185 unique results ranked Medium to Critical based on the Common Vulnerability Scoring System (CVSS), which is defined in Section III. The graph below shows the number of findings by rating.



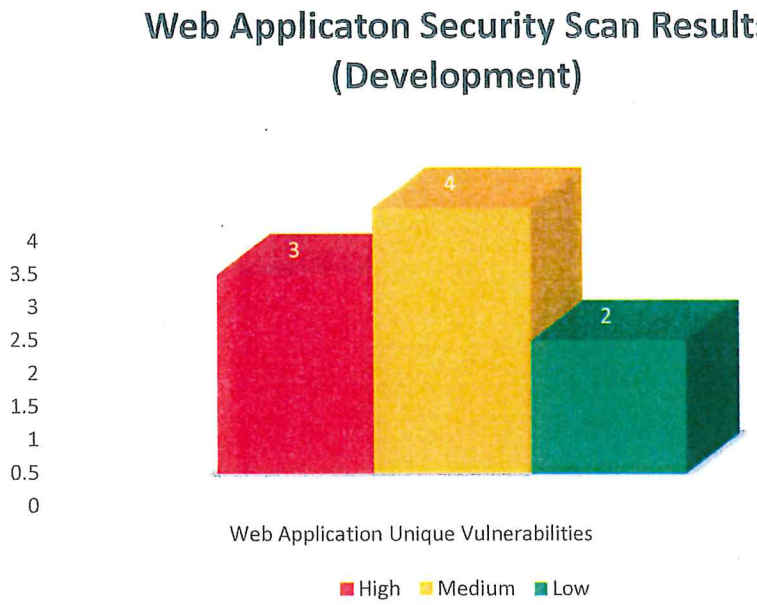
Internal Penetration Test Findings

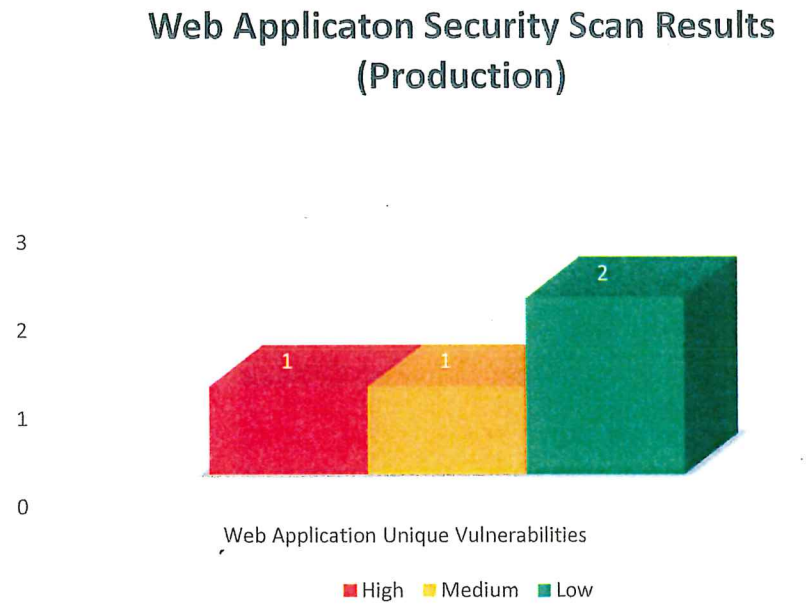
The State had four findings based on probability and impact, which are defined in Section III. The graph below shows the number of findings by rating. Detailed information can be found in Section V and is intended to assist management with prioritizing corrective action.



Web Application Security Scan Results

The State had 12 unique results for the development environment and four unique results for the production environment. The graphs below show the number of findings by rating, which are defined in Section III.





Web Application Security Testing Findings

The State had one finding based on probability and impact.

[redacted] This issue could not be reproduced in production. Using the supplied credentials, it was not possible to elevate privileges or steal the session of another user.

We believe any findings, regardless of the risk ratings assigned, if not addressed, could lead to significant issues. Findings based on probability and impact are viewed as an immediate risk because they often lead to a breach of the State's network and systems.

We recommend management track and report resolution status to the designated committee.

Social Engineering Testing Results

The State had no findings based on probability and impact.

Social Engineering phishing tests were attempted. During setup of the test, the control environment of the State stopped the attempts. Only one phishing email out of the test set made it to a user's email, and that was moved automatically to a spam folder.

No further attempts were made.

Definitions of Ratings

Ratings of External & Internal Vulnerability Scan Results

The tools we use for vulnerability scanning utilize the industry standard Common Vulnerability Scoring System (CVSS) to ascertain the criticality of identified vulnerabilities. The CVSS is based on either Version 2 (v2) or Version 3 (v3) and utilizes the scoring system indicated in the table below. Not all vulnerabilities have a v3 score and will default to the v2 score, which applies to older systems and vulnerabilities, and may not be available in v3. Scores have been provided for both v2 and v3 when available. FORVIS may also include an informational finding that does not have a CVSS score but is still deemed relevant in regard to security best practices.

Common Vulnerability Scoring System		
Vulnerability Score	**v3 Definition**	**v2 Definition**
Critical	Base Score of 9.0 to 10.0	N/A
High	Base Score of 7.0 to 8.9	Base Score of 7.0 to 10.0
Medium	Base Score of 4.0 to 6.9	Base Score of 4.0 to 6.9
Low	Base Score of 0.1 to 3.9	Base Score of 0.0 to 3.9
Informational	No CVSS score but security best practice	No CVSS score but security best practice

More information can be found in regard to CVSS scoring and calculations by accessing the National Vulnerabilities Database hosted by the National Institute of Standards and Technology (NIST) at https://nvd.nist.gov.

Web Application Security Scan Results

These scanning results are rated based upon industry standards and impact. Results are classified according to severity as documented in the following table. This reflects the likely impact of each issue for a typical organization. Issues are also classified according to confidence of the vulnerability scanner results as Certain, Firm or Tentative. This reflects the inherent reliability of the technique that was used to identify the issue.

Risk Rating	Definition
Critical	Indicates a matter requiring immediate remediation.
High	Indicates a matter requiring higher priority remediation.
Medium	Indicates a matter to be given priority for remediation.
Low	Indicates a matter to be remediated in the normal course of business.

Definitions of Ratings

Ratings of Network Security

The following ratings of network security are based solely on the procedures performed and relate only to the items tested. Had we performed additional procedures, other matters might have come to our attention that could have changed the rating of the network security posture.

- **Satisfactory –** Identified findings did not lead to compromise of systems or data, but control improvements and other recommendations may have been identified that should be implemented as resources permit. If applicable, remediation efforts should be tracked by management.
- **Needs Improvement –** Compromise of systems or data may have been achieved, or control improvements and other recommendations have been identified and warrant prompt corrective action to allow the internal control systems to function effectively. Remediation efforts should be tracked and reported to the Board until all actions are completed and the Board approves the corrective measures.
- **Unsatisfactory –** Identified findings are being actively exploited by threat actors to breach systems and networks, or vulnerabilities exploited during testing resulted in root or system level privileges on the network. These require management's immediate corrective action to mitigate the risk. Remediation efforts should be tracked and reported to the Board until actions are completed and the Board approves the corrective measures.

Penetration Attack Summary

Summary of Attacks & Testing

Prior to the start of the testing, a penetration testing device was shipped to the State and connected to the internal network for the purpose of executing the engagement from the agreed-upon simulation. The provided device was connected to the network by the State's IT staff. Remote access to the device was granted to the tester.

Broadcast name resolution poisoning began in parallel to initial port scanning of the network during the first day of testing. Interception of the default Internet proxy server was also attempted. [redacted]. Subsequent searches for sensitive information were not successful.

Domain administrative access was not obtained during this test.

No sensitive information or PII were obtained during this test.

Often, when Domain Name Systems (DNS) resolution fails, Microsoft systems will resort to using other methods to resolve hosts on a Windows network [Link Local Multicast Name Resolution (LLMNR), Net Bios Name Service (NBTNS), etc.]. This is considered to be a feature; however, this feature can be abused by an attacker.

[redacted]

External testing of the environment was conducted against the provided IP addresses. Two of the systems were found to be running a vendor unsupported web server, according to the version numbers.

[redacted]

Testing of the unemployment website was conducted against the development site using both uncredentialed and credentialed testing. Testing against the production site was conducted using uncredentialed testing. [redacted] This issue could not be reproduced in production. Using the supplied credentials, it was not possible to elevate privileges or steal the session of another user.

Social Engineering Phishing attacks were attempted. These emails were blocked by the controls in place and were unsuccessful.

Findings & Recommendations

Finding #1

Risk Rating: **Critical**

Probability: High

Impact: High

At.

IP Addresses:

[redacted]

Recommendation:

[redacted] An attacker can intercept traffic on a network and impersonate the identity of legitimate systems.

[redacted]

It should be noted that discovery of this problem is limited to the local broadcast network only. It should be assumed that similar systems on other subnets may also share this issue even though they could not be detected during testing.

Management Response:

[redacted]

See also:

[redacted]

Finding #2

Risk Rating: **Critical**

Probability: High

Impact: High

[redacted]

It should be noted that discovery of this problem is limited to the local broadcast network only. It should be assumed that similar systems on other subnets might also share this issue even though they could not be detected during testing.

Recommendation:

[redacted]

See also:

[redacted]

Finding #3

Risk Rating: **Critical**

Probability: High

Impact: High

[redacted]

Recommendation:

[redacted]

See also:

[redacted]

Finding #4

Risk Rating: High

Probability: Medium

Impact: High

[redacted]

[redacted]

Recommendation:

[redacted]

See also:

[redacted]

Finding #5

Risk Rating: **High**

Probability: Medium

Impact: High

[redacted]

This was found on the Development site and was not reproducible on the Production site.

Recommendation:

[redacted]

Scope of Services

The scope of procedures performed by FORVIS for the State as of April 20, 2022, from our proposal in accordance with the agreement.

External Penetration Testing

This review is an assessment of the security posture of the Kansas Department of Labor from an external perspective and begins with social engineering and surveillance of the systems and the network of the Kansas Department of Labor. Then, using a combination of tools and techniques, the security engineer determines if there are any vulnerabilities which may be exploited to further gain access to the Kansas Department of Labor's systems. If there are vulnerabilities, they are exploited using knowledge about the specific operating system or device drilling further into the Kansas Department of Labor's network and system.

Internal Penetration Testing

This review is an assessment of the security posture of the Kansas Department of Labor from an internal perspective and helps identify risks if someone were able to obtain access from inside the organization. By using a combination of tools and techniques, the security engineer determines if there are any vulnerabilities which may be exploited to further gain access to the Kansas Department of Labor's systems. If there are vulnerabilities, they are exploited using knowledge about the specific operating system or device drilling further into the Kansas Department of Labor's network and system.

Social Engineering

This assessment is designed to help the organization train personnel and reinforce awareness of attempts to gain information from employees.

Appendix

Appendix A: Details of Internal Vulnerability Scan Results

Due to the sensitive and confidential nature of the detail of KDOL network and systems information contained in the scans, the information is not included here and is available upon request by KDOL or the Council.