# ABSTRAK

Penggunaan internet di pemerintahan untuk mendorong realisasi e-government dapat memberikan manfaat peningkatan kekuatan masyarakat dengan meningkatkan akses informasi, meningkatkan pelayanan pemerintah kepada masyarakat, memperkuat interaksi antara pemerintah dan swasta di industri terkait, serta meningkatkan kemudahan dan keterbukaan pengelolaan pemerintahan. Salah satu alat yang digunakan untuk mengidentifikasi kerentanan dalam aplikasi web adalah Acunetix Web Vulnerability. Alat ini adalah sebuah scanner keamanan yang dapat secara otomatis mendeteksi kerentanan umum dalam aplikasi web, termasuk serangan SQL injection, Cross-Site Scripting (XSS), dan lainnya. Tujuan dilakukannya penelitian ini adalah melakukan audit web e-government, langkah-langkah analisis keamanan e-government dan memberikan rekomendasi perbaikan dari hasil analaisis keamanan menggunakan acunetix web vulnerability pada website DPMPTSP Kota Padang. Data diperoleh dengan menggunakan tools acunetix web vulnerability memperoleh laporan dari proses uji penetrasi yang berisi informasi tentang kerentanan keamanan yang ditemukan pada website SINOPEN https://nonperizinan.web.dpmptsp.padang.go.id/sinopen. Temuan kerentanan sebanyak 148 data berada pada level high, 107 data berada pada level medium, 16 data berada pada level low. Beberapa diantaranya serangan yang ditemukan sebanyak 11 serangan yaitu Blind sql injection, Cross site scripting (xss), Sql injection,Application error message, HTML form without CSRF protection, Clickjacking:X-Frame-Option Header Missing, Cookie Without Secure Flag Set, File Upload, Login Page Password-Guessing Attack, Broken Links, Password Type Input With Auto-Complete Enabled. Tools acunetix web vulnerability digunakan sebagai dasar menganalisis perbaikan yang dilakukan setelah melakukan scanning pada website tersebut. Hasil setelah dilakukan audit keamanan e-government guna melakukan analisis dan perbaikan level kerentanan yang ditemukan pada website SINOPEN berada pada level low, sehingga meningkatkan level keamanan dari serangan dan status website dapat dikatakan aman dari kerentanan serangan.

**Kata kunci**: Audit, e-government, Acunetix Web Vulnerability, Vulnerability Assessment, SINOPEN

# ABSTRACT

The use of the internet in government to encourage the realization of e-Government can provide benefits in increasing the power of society by increasing access to information, improving government services to the community, strengthening interaction between government and the private sector in related industries, and increasing the ease and openness of government management. One tool used to identify vulnerabilities in web applications is Acunetix Web Vulnerability. This tool is a security scanner that can automatically detect common vulnerabilities in web applications, including SQL injection attacks, Cross-Site Scripting (XSS), and others. The purpose of this research is to conduct an e-Government web audit, steps for e-Government security analysis and provide recommendations for improvements from the results of security analysis using Acunetix web vulnerabilities on the Padang City DPMPTSP website. Data was obtained using the Acunetix Web Vulnerability tool to obtain a report from the penetration test process which contains information about security vulnerabilities found on website https://nonperizinan.web.dpmptsp.padang.go.id/sinopen. The vulnerability findings of 148 data were at a high level, 107 data were at a medium level, 16 data were at a low level. Some of the attacks found were 11 attacks, namely Blind SQL injection, Cross site scripting (XSS), SQL injection, Application error message, HTML form without CSRF protection, Clickjacking: X-Frame-Option Header Missing, Cookie Without Secure Flag Set, File Upload, Login Page Password Guessing Attack, Broken Link, Password Type Input With AutoComplete Enabled. The Acunetix web vulnerability tool is used as a basis for analyzing improvements made after scanning the website. The results after an e-gov security audit was carried out to analyze and improve the level of vulnerabilities found on the SINOPEN website were at a low level, thereby increasing the level of security from attacks and the status of the website can be said to be safe from attack vulnerabilities.

**Keywords**: Audit, e-Government, Acunetix Web Vulnerability, Vulnerability Assessment, SINOPEN