JURNAL PENELITIAN MULTIDISIPLIN BANGSA
e-ISSN : 3048-4251
Volume 2, No. 2, Tahun 2025
https://ejournal.amirulbangunbangsapublishing.com/index.php/jpnmb/index

Pengujian Keamanan Website Dinas Kearsipan Provinsi Sumsel Dengan Metode *OWASP* Menggunakan *Penetration Testing*

Delfin Christofa[1], Syahril Rizal[2]
[1,2] *Universitas Bina Darma, Indonesia*

Received : 23 Juni 2025, Revised : 26 Juni 2025, Published : 4 Juli 2025

Corresponding Author
Nama Penulis: Delfin Christofa
E-mail: delfinchristofa1@gmail.com

Abstrak

Keamanan informasi dalam layanan berbasis website menjadi krusial di era digital, terutama pada instansi pemerintah yang mengelola data strategis. Penelitian ini bertujuan untuk menguji keamanan website Dinas Kearsipan Provinsi Sumatera Selatan dengan menggunakan metode OWASP melalui pendekatan penetration testing. Pengujian dilakukan menggunakan tool OWASP ZAP dengan menyimulasikan berbagai serangan terhadap situs arsip.sumselprov.go.id. Hasil pengujian mengungkapkan 15 temuan kerentanan dengan tingkat risiko berbeda-beda. Di antara kerentanan tersebut terdapat pustaka JavaScript yang rentan, absennya token anti-CSRF, hingga konfigurasi header HTTP yang tidak aman. Berdasarkan temuan tersebut, disusun solusi dan rekomendasi perbaikan keamanan. Hasil ini menunjukkan pentingnya evaluasi berkala terhadap sistem web instansi pemerintah untuk mendukung tata kelola informasi yang aman dan andal

Kata kunci *– keamanan website, penetration testing, OWASP, ZAP, arsip digital*

Abstract

Information security in web-based services is critical in the digital era, especially in government institutions managing strategic data. This study aims to assess the security of the website of the South Sumatra Provincial Archives Service using the OWASP methodology through a penetration testing approach. Testing was conducted using the OWASP ZAP tool by simulating various attacks on the website arsip.sumselprov.go.id. The results revealed 15 vulnerabilities with varying risk levels, including a vulnerable JavaScript library, absence of anti-CSRF tokens, and misconfigured HTTP headers. Based on these findings, solutions and recommendations were proposed. These results highlight the importance of regular evaluations of government websites to ensure secure and reliable information governance.

Keywords *- website security, penetration testing, OWASP, ZAP, digital archive*

How To Cite : *Christofa, D., & Rizal, S. Pengujian Keamanan Website Dinas Kearsipan Provinsi Sumsel Dengan Metode OWASP Menggunakan Penetration Testing. Jurnal Penelitian Multidisiplin Bangsa, 2(2), 231–237. https://doi.org/10.59837/jpnmb.v2i2.475*

PENDAHULUAN

Transformasi digital telah membawa perubahan signifikan dalam cara instansi pemerintah memberikan pelayanan publik. Saat ini, banyak lembaga pemerintah memanfaatkan aplikasi berbasis web untuk menyediakan layanan yang cepat, efisien, dan mudah diakses oleh Masyarakat (Kuzmin & Matveev, 2023). Salah satunya adalah Dinas Kearsipan Provinsi Sumatera Selatan yang mengembangkan situs web resmi sebagai media penyedia informasi, layanan arsip digital, serta sarana komunikasi antara pemerintah dan masyarakat.

Namun, seiring dengan peningkatan ketergantungan terhadap layanan berbasis web, risiko terhadap keamanan siber juga meningkat secara drastis. Website milik instansi pemerintah sering kali menjadi target serangan karena menyimpan data strategis dan sensitif yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab. Serangan seperti *defacement*, *injection*, dan pencurian data merupakan ancaman nyata yang dapat berdampak pada kerugian materiil, kerusakan reputasi, bahkan gangguan layanan publik (Elanda & Lintang Buana, 2021)

Untuk mengatasi tantangan ini, pengujian keamanan atau penetration testing menjadi salah satu metode utama yang digunakan untuk mengevaluasi ketahanan sistem terhadap ancaman. Pengujian ini dilakukan dengan cara mensimulasikan serangan terhadap sistem untuk menemukan potensi kerentanan sebelum dapat dimanfaatkan oleh pihak eksternal. Metode ini telah terbukti efektif dalam mengidentifikasi celah keamanan dan menjadi bagian penting dari pengelolaan keamanan sistem informasi (Haris et al., 2024; Nagendran et al., 2019)

Dalam konteks pengujian keamanan aplikasi web, *OWASP* (*Open Web Application Security Project*) menjadi standar global yang banyak digunakan oleh profesional keamanan dan pengembang. *OWASP* menyediakan berbagai panduan seperti *OWASP* Top 10, *OWASP Testing Guide*, dan *tools* seperti *OWASP ZAP* (*Zed Attack Proxy*) yang dapat digunakan untuk mendeteksi kerentanan pada aplikasi web. Pendekatan *OWASP* mengedepankan prinsip keterbukaan dan kemudahan akses, sehingga sangat ideal untuk diaplikasikan di sektor publik (Riandhanu, 2022)

Website Dinas Kearsipan Provinsi Sumatera Selatan yang beralamat di arsip.sumselprov.go.id memegang peranan penting dalam pengelolaan arsip digital. Website ini tidak hanya berfungsi sebagai pusat informasi publik, tetapi juga sebagai gerbang layanan kearsipan. Oleh karena itu, jika terdapat celah keamanan pada sistem tersebut, maka potensi kerusakan dan penyalahgunaan data arsip menjadi sangat besar. Hal ini mendorong pentingnya pengujian keamanan secara menyeluruh sebagai upaya preventif (Haris et al., 2024)

Penelitian ini bertujuan untuk menerapkan metode *OWASP* dalam melakukan pengujian keamanan terhadap website Dinas Kearsipan Provinsi Sumatera Selatan. Melalui proses pemindaian menggunakan *OWASP ZAP*, dilakukan identifikasi kerentanan, analisis risiko, serta penyusunan rekomendasi mitigasi. Di samping itu, penelitian ini juga merupakan bagian dari praktik magang yang bertujuan untuk menerapkan pengetahuan mahasiswa dalam konteks dunia kerja nyata, khususnya dalam bidang keamanan informasi (Ahmadi & Nursari, 2022)

TINJAUAN PUSTAKA

Keamanan Sistem Informasi

Keamanan sistem informasi adalah elemen fundamental dalam pengembangan teknologi informasi, khususnya pada aplikasi berbasis web yang terhubung langsung ke jaringan publik. Sistem informasi yang tidak aman dapat mengakibatkan berbagai ancaman seperti pencurian data, kerusakan sistem, hingga gangguan terhadap layanan publik. Keamanan informasi umumnya mencakup tiga aspek utama, yaitu kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) data, atau dikenal dengan istilah *CIA* (Ahmadi & Nursari, 2022). Ketiga aspek ini harus dijaga secara bersamaan untuk menjamin keandalan suatu sistem.

Penetration Testing

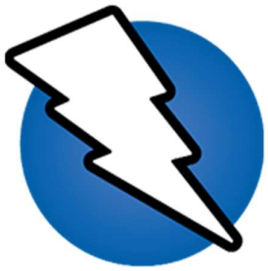
Penetration Testing merupakan metode yang digunakan untuk mengevaluasi keamanan sistem informasi dengan cara mensimulasikan serangan terhadap sistem tersebut. Tujuan utama dari metode ini adalah untuk mengidentifikasi celah atau kerentanan sebelum benar-benar dimanfaatkan oleh pihak yang tidak berwenang. *Penetration testing* biasanya dilakukan oleh tim profesional yang memiliki pengetahuan teknis tinggi tentang sistem dan potensi serangan (Riadi et al., 2020). Proses ini bersifat legal dan dilakukan dalam lingkup yang telah disepakati oleh pemilik sistem.

***OWASP* (*Open Web Application Security Project*)**

OWASP adalah organisasi nirlaba yang berfokus pada peningkatan keamanan perangkat lunak, khususnya aplikasi web. Salah satu kontribusi *OWASP* yang paling populer adalah publikasi *OWASP Top 10*, yaitu daftar sepuluh besar jenis kerentanan aplikasi web yang paling umum ditemukan. Selain itu, *OWASP* juga mengembangkan berbagai tools untuk pengujian keamanan, salah satunya adalah *OWASP ZAP* (*Zed Attack Proxy*), yang dapat digunakan untuk mendeteksi kerentanan seperti *cross-site scripting (XSS), insecure cookie, dan header HTTP* yang tidak aman (Riandhanu, 2022)

***OWASP ZAP* sebagai Alat Uji Keamanan**

OWASP ZAP adalah tools sumber terbuka (*open source*) yang digunakan secara luas untuk melakukan pengujian keamanan terhadap aplikasi web. Tool ini mampu melakukan pemindaian pasif dan aktif terhadap aplikasi untuk mendeteksi berbagai macam celah keamanan yang tersembunyi.



Gambar 1.
Logo *OWASP ZAP*

Berdasarkan penelitian yang dilakukan oleh Haris et al. (2024), *OWASP ZAP* terbukti mampu mengidentifikasi kerentanan pada situs pemerintahan yang sebelumnya tidak terdeteksi oleh pengembang internal. *Tool* ini juga menyediakan klasifikasi hasil temuan berdasarkan tingkat risiko dan *confidence level*, sehingga memudahkan dalam proses mitigasi.

Keamanan Website Instansi Pemerintah

Website milik instansi pemerintah menjadi sasaran empuk bagi penyerang siber karena umumnya menyimpan data penting dan memiliki banyak titik akses terbuka (Yang et al., 2020). Sayangnya, banyak instansi pemerintah yang belum menerapkan praktik keamanan secara optimal. Penelitian oleh Elanda dan Lintang Buana (2021) menunjukkan bahwa sebagian besar situs pemerintahan di Indonesia tidak mengimplementasikan *header* keamanan dasar *seperti X-Frame-Options, Content-Security-Policy,* dan *Strict-Transport-Security*. Hal ini menunjukkan masih rendahnya kesadaran terhadap pentingnya hardening konfigurasi keamanan pada sistem publik.

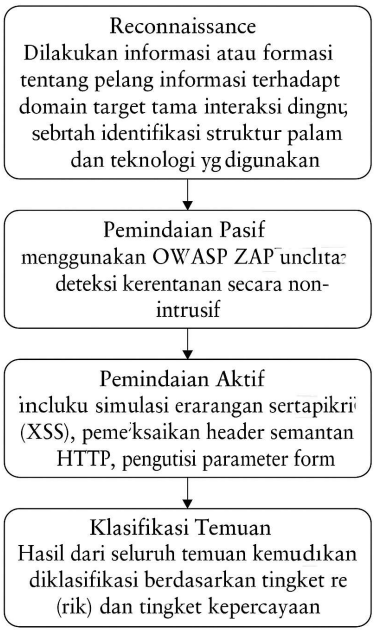
METODE

Penelitian ini menggunakan pendekatan studi kasus dengan objek penelitian berupa website resmi Dinas Kearsipan Provinsi Sumatera Selatan yang beralamat di https://arsip.sumselprov.go.id. Pendekatan studi kasus digunakan untuk mengevaluasi keamanan aplikasi web secara mendalam melalui proses penetration testing berbasis metode *OWASP* (*Open Web Application Security Project*).

Tujuan utama dari pengujian ini adalah untuk mengidentifikasi, mengevaluasi, dan memberikan rekomendasi perbaikan terhadap kerentanan sistem yang ditemukan (Al-Ahmad et al., 2023).

Metodologi yang digunakan dalam pengujian ini mengacu pada standar *OWASP Testing Guide*, yang menyediakan kerangka kerja lengkap dalam melakukan pengujian keamanan terhadap aplikasi web. Tool utama yang digunakan adalah *OWASP ZAP* (*Zed Attack Proxy*) versi 2.16.1, yaitu alat *open-source* yang dikembangkan oleh komunitas *OWASP*. *OWASP ZAP* digunakan untuk melakukan pemindaian pasif maupun aktif terhadap situs target guna mengidentifikasi potensi kerentanan seperti injection, konfigurasi *cookie* yang lemah, informasi server yang terbuka, dan lain sebagainya (Riandhanu, 2022)

Langkah-langkah dalam pengujian dilakukan secara sistematis. Pertama, dilakukan proses reconnaissance atau pengumpulan informasi terhadap domain target tanpa interaksi langsung, seperti identifikasi struktur halaman dan teknologi yang digunakan. Kedua, dilakukan pemindaian pasif menggunakan *OWASP ZAP* untuk mendeteksi kerentanan secara non-intrusif. Ketiga, dilakukan pemindaian aktif yang mencakup simulasi serangan seperti penyisipan skrip (XSS), pemeriksaan header keamanan HTTP, dan pengujian parameter form login. Keempat, hasil dari seluruh temuan kemudian diklasifikasikan berdasarkan tingkat risiko (*risk*) dan tingkat kepercayaan (*confidence*) untuk memudahkan proses analisis (Anggraeni et al., 2022).



Gambar 2.
Langkah-langkah pengujian

Setiap temuan dalam hasil pemindaian *OWASP ZAP* dievaluasi dengan pendekatan analitis berdasarkan dua aspek: tingkat keparahan (*severity*) dan potensi eksploitasinya. Penilaian ini penting untuk menentukan prioritas mitigasi yang harus dilakukan oleh pengelola sistem. Selain itu, dilakukan juga pencocokan dengan daftar *OWASP Top 10* untuk mengetahui apakah kerentanan yang ditemukan termasuk dalam 10 besar kerentanan aplikasi web yang paling umum. Dengan metode ini, hasil pengujian diharapkan dapat memberikan gambaran nyata mengenai tingkat keamanan situs web serta rekomendasi teknis yang dapat diimplementasikan secara praktis oleh Dinas Kearsipan (Haris et al., 2024; Nagendran et al., 2019)

PEMBAHASAN

Hasil dari pengujian keamanan yang dilakukan terhadap website Dinas Kearsipan Provinsi Sumatera Selatan menunjukkan adanya sejumlah kerentanan yang perlu segera ditindaklanjuti. Proses pengujian dilakukan dengan menggunakan *tool OWASP ZAP* yang mampu melakukan pemindaian pasif dan aktif untuk mendeteksi celah keamanan pada aplikasi web. Total ditemukan 15 temuan kerentanan yang terbagi ke dalam empat kategori tingkat risiko, yaitu *High, Medium, Low*, dan *Informational*.

Setiap temuan dikelompokkan berdasarkan kombinasi antara tingkat risiko (*risk level*) dan tingkat keyakinan terhadap validitas temuan (*confidence level*). *Risk level* menunjukkan potensi dampak apabila kerentanan dimanfaatkan, sementara *confidence level* menunjukkan seberapa yakin sistem terhadap keberadaan kerentanan tersebut berdasarkan data yang dikumpulkan selama proses scanning

Tabel 1.
Ringkasan Hasil Pemindaian Berdasarkan *Risk* dan *Confidence* 1

Risk Level	User Confirmed	High	Medium	Low	Total
High	0	0	1	0	1
Medium	0	1	2	1	4
Low	0	2	3	1	6
Informational	0	0	2	2	4
Total	**0**	**3**	**8**	**4**	**15**

Temuan tingkat risiko tinggi (*High*) melibatkan penggunaan pustaka *JavaScript* yang rentan, yaitu *bootstrap-select.min.js* versi 1.12.2 yang diketahui memiliki kelemahan keamanan yang telah terdokumentasi dalam *CVE*. Hal ini berisiko tinggi jika tidak segera diperbarui, karena pustaka eksternal yang tidak aman dapat dimanfaatkan untuk menyisipkan kode jahat/*JavaScript injection* (Staicu et al., 2020).

Pada kategori risiko menengah (*Medium*), ditemukan empat jenis kerentanan, di antaranya tidak adanya token *anti-CSRF* pada form login, tidak diterapkannya *Content Security Policy* (CSP), serta ketiadaan *header anti-clickjacking*. Ketiadaan fitur keamanan ini membuat aplikasi lebih rentan terhadap serangan pemalsuan permintaan lintas situs dan *clickjacking*, yang dapat digunakan untuk mengecoh pengguna dalam melakukan tindakan yang tidak dikehendaki (Riandhanu, 2022)

Tabel 2.
Ringkasan Hasil Pemindaian Berdasarkan *Risk* dan *Confidence*

No	Jenis Kerentanan	Risk	Confidence	Jumlah Temuan
1	Vulnerable JS Library	High	Medium	1
2	Absence of Anti-CSRF Tokens	Medium	High	1
3	Content Security Policy Header Not Set	Medium	Medium	2
4	Missing Anti-clickjacking Header	Medium	Medium	1
5	Cookie Without Secure Flag	Low	High	2
6	Server Leaks Version Information via HTTP Header	Low	Medium	3
7	X-Content-Type-Options Header Missing	Low	Medium	1
8	Suspicious Comments	Informational	Medium	2
9	Session Management Response Identified	Informational	Medium	2

Temuan risiko rendah (*Low*) termasuk konfigurasi *cookie* yang tidak menggunakan atribut *Secure*, server yang mengungkapkan versi software melalui *header HTTP*, serta tidak diterapkannya *header X-Content-Type-Options* yang dapat mencegah *MIME-sniffing* oleh browser. Meskipun tidak bersifat kritikal, kerentanan-kerentanan ini tetap harus ditangani untuk memperkecil permukaan serangan secara keseluruhan (Elanda & Lintang Buana, 2021)

Adapun temuan kategori *Informational* seperti komentar mencurigakan dalam kode HTML dan pola respons manajemen sesi yang mudah ditebak, tetap perlu diperhatikan karena berpotensi menjadi titik awal serangan apabila dikombinasikan dengan kerentanan lain yang lebih serius. Hal ini menekankan pentingnya hardening pada setiap lapisan aplikasi, tidak hanya pada komponen-komponen utama saja (Ahmadi & Nursari, 2022)

Secara keseluruhan, hasil pengujian menunjukkan bahwa masih terdapat celah-celah keamanan yang signifikan pada website Dinas Kearsipan. Rekomendasi utama yang dapat diberikan adalah melakukan update pustaka eksternal, mengimplementasikan token *anti-CSRF*, mengatur *header* keamanan dengan benar, serta menonaktifkan pengungkapan informasi sensitif pada konfigurasi server. Dengan mitigasi yang tepat, maka sistem informasi kearsipan dapat menjadi lebih tangguh terhadap ancaman siber di masa mendatang.

KESIMPULAN

Berdasarkan hasil pengujian keamanan terhadap website Dinas Kearsipan Provinsi Sumatera Selatan menggunakan pendekatan metode *OWASP* dan tools *OWASP ZAP*, dapat disimpulkan bahwa sistem masih memiliki sejumlah kerentanan yang berpotensi membahayakan integritas dan keamanan data. Total 15 temuan berhasil diidentifikasi, mencakup berbagai kategori risiko mulai dari *High, Medium, Low*, hingga *Informational*. Temuan-temuan ini menunjukkan bahwa meskipun sistem secara fungsional berjalan baik, namun masih terdapat celah teknis yang dapat dieksploitasi jika tidak segera ditangani.

Salah satu temuan paling kritis adalah penggunaan pustaka *JavaScript* versi lama yang mengandung kerentanan keamanan. Selain itu, tidak diterapkannya header keamanan dasar seperti *Content-Security-Policy* dan *X-Content-Type-Options* memperbesar peluang bagi serangan seperti *cross-site scripting* dan *MIME-sniffing*. Kondisi ini diperparah oleh absennya *token anti-CSRF*, yang merupakan lapisan perlindungan penting terhadap manipulasi permintaan dari pihak ketiga. Hal ini menunjukkan kurangnya penerapan prinsip keamanan berlapis (*defense in depth*) dalam pengelolaan situs tersebut.

Dari hasil analisis, dapat disimpulkan bahwa penting bagi instansi pemerintah untuk tidak hanya fokus pada penyediaan layanan informasi yang fungsional, tetapi juga menjadikan aspek keamanan sebagai prioritas utama. Pengujian secara berkala dengan pendekatan penetration testing dan pemanfaatan panduan *OWASP* dapat membantu mengidentifikasi dan meminimalkan risiko sejak dini sebelum dieksploitasi oleh pihak tidak bertanggung jawab.

Dengan demikian, pengujian keamanan ini tidak hanya berperan dalam meningkatkan ketahanan sistem, tetapi juga mendukung kepercayaan publik terhadap layanan digital pemerintah. Diharapkan hasil dari penelitian ini dapat menjadi bahan evaluasi bagi Dinas Kearsipan dalam memperkuat sistemnya, serta menjadi acuan bagi instansi pemerintah lain untuk mengadopsi pendekatan serupa dalam menjaga keamanan aset digital mereka.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Dinas Kearsipan Provinsi Sumatera Selatan atas kesempatan yang telah diberikan untuk melaksanakan kegiatan magang sekaligus melakukan pengujian keamanan pada sistem informasinya. Ucapan terima kasih juga disampaikan kepada

Universitas Bina Darma, khususnya Program Studi Teknik Informatika, atas dukungan akademik dan fasilitas yang telah diberikan selama proses penelitian ini berlangsung.

Tidak lupa penulis menyampaikan apresiasi yang setinggi-tingginya kepada dosen pembimbing, Bapak Syahril Rizal R I, S.T., M.M., M.Kom, dan pembimbig mitra, Ibu Hj. Nyimas Masyito, S.Sos, M.Si, yang telah memberikan bimbingan, arahan, dan masukan berharga selama proses penyusunan artikel ini. Semoga hasil dari penelitian ini dapat memberikan kontribusi yang bermanfaat bagi pengembangan keamanan sistem informasi, khususnya pada sektor pemerintahan

DAFTAR PUSTAKA

Ahmadi, M. F., & Nursari, S. R. C. (2022). Pengujian Kondisi Struktur Kontrol pada Website (Studi Kasus: Erigo Official). *Journal of Informatics and Advanced Computing*.

Al-Ahmad, A. S., Kahtan, H., & Alzoubi, Y. I. (2023). Overview on Case Study Penetration Testing Models Evaluation. *Emerging Science Journal*, *7*(3), 1019–1036. https://doi.org/10.28991/ESJ-2023-07-03-025

Anggraeni, D. P., Zen, B. P., & Pranata, M. (2022). Security Analysis On Websites Using The Information System Assessment Framework (Issaf) And Open Web Application Security Version 4 (OWASPv4) Using The Penetration Testing Method. *Jurnal Pertahanan: Media Informasi Tentang Kajian Dan Strategi Pertahanan Yang Mengedepankan Identity, Nasionalism Dan Integrity*, *8*(3), 497–506.

Elanda, A., & Lintang Buana, R. (2021). *Analisis Kualitas Keamanan Sistem Informasi E-Office Berbasis Website Pada Stmik Rosma Dengan Menggunakan Owasp Top 10* (Vol. 6, Issue 2).

Haris, R., Muhammad, A. H., & Nasiri, A. (2024). Prioritas Investasi Keamanan Informasi Menggunakan Analytic Network Process (ANP) Bagi Pemerintah Daerah Provinsi Kalimantan Tengah. *Jurnal Teknologi Informasi Dan Ilmu Komputer*, *11*(6), 1361–1370. https://doi.org/10.25126/JTIIK.1169245

Kuzmin, A. E., & Matveev, A. A. (2023). The Impact of Digital Transformation on the Process of Interaction of Public Authorities with Citizens. *Proceedings of the 2023 Communication Strategies in Digital Society Seminar 2023, ComSDS 2023*, 151–154. https://doi.org/10.1109/COMSDS58064.2023.10130430

Nagendran, K., Adithyan, A., Chethana, R., Camillus, P., & Bala Sri Varshini, K. B. (2019). Web Application Penetration Testing. *VOLUME-8 ISSUE-10, AUGUST 2019, REGULAR ISSUE*, *8*(10), 1029–1035. https://doi.org/10.35940/IJITEE.J9173.0881019

Riadi, I., Yudhana, A., & Korspondensi, P. (2020). *Analisis Keamanan Website Open Journal System Menggunakan Metode Vulnerability Assessment*. *7*(4). https://doi.org/10.25126/jtiik.202071928

Riandhanu, I. O. (2022). Analisis Metode *Open Web Application Security Project* (OWASP) Menggunakan Penetration Testing pada Keamanan Website Absensi. *Jurnal Informasi Dan Teknologi*. https://doi.org/10.37034/jidt.v4i3.236

Staicu, C. A., Torp, M. T., Schafer, M., Moller, A., & Pradel, M. (2020). Extracting taint specifications for javascript libraries. *Proceedings - International Conference on Software Engineering*, 198–209. https://doi.org/10.1145/3377811.3380390;PAGE:STRING:ARTICLE/CHAPTER

Yang, H., Huang, L., Luo, C., & Yu, Q. (2020). Research on Intelligent Security Protection of Privacy Data in Government Cyberspace. *2020 IEEE 5th International Conference on Cloud Computing and Big Data Analytics, ICCCBDA 2020*, 284–288. https://doi.org/10.1109/ICCCBDA49378.2020.9095637