ANALISIS RISIKO DAN STRATEGI PERLINDUNGAN SISTEM TERHADAP ANCAMAN SIBER PADA WEBSITE 'SAMBANG' KABUPATEN JOMBANG

Proposal Tugas Akhir

Diajukan Untuk Memenuhi Persyaratan Guna Meraih Gelar Sarjana

Informatika Universitas Muhammadiyah Malang

Muh. Rayhan Islamiah Prathama

202010370311333

Bidang Minat

Sistem dan Keamanan Jaringan

PROGRAM STUDI INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH MALANG

2025

LEMBAR PERSETUJUAN

Analisis Risiko dan Strategi Perlindungan Sistem terhadap Ancaman Siber pada Website `SAMBANG` Kabupaten Jombang

TUGAS AKHIR

Sebagai Persyaratan Guna Meraih Gelar Sarjana Strata 1
Informatika Universitas Muhammadiyah Malang

Menyetujui,
Malang, *13 Oktober 2025*

Dosen Pembimbing 1	Dosen Pembimbing 2
Zamah Sari ST., MT.	**Ir Denar Regata Akbi S.Kom., M.Kom.**
NIP. 10814100555PNS.	**NIP. 10816120591PNS.**

LEMBAR PENGESAHAN

Analisis Risiko dan Strategi Perlindungan Sistem terhadap Ancaman Siber pada Website `SAMBANG` Kabupaten Jombang

TUGAS AKHIR

Sebagai Persyaratan Guna Meraih Gelar Sarjana Strata 1
InformatikaUniversitas Muhammadiyah Malang

Disusun Oleh :

Muh. Rayhan Islamiah Prathama
202010370311333

Tugas Akhir ini telah diuji dan dinyatakan lulus melalui sidang majelis penguji pada tanggal 13 Oktober 2025

Menyetujui,

Dosen Penguji 1	Dosen Penguji 2
Ir. Syaifuddin S.Kom., M.Kom., IPM, ASEAN Eng	**Luqman Hakim S.Kom., M.Kom.**
NIP. 10816120590PNS.	**NIP. 10819030658PNS.**

Mengetahui,
Ketua Jurusan Informatika

Ir. Agus Eko Minarno S.Kom., M.Kom. IPM.
NIP. 10814100540PNS.

LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini :

NAMA : Muh. Rayhan Islamiah Prathama
NIM : 202010370311333

FAK./JUR. : Informatika

Dengan ini saya menyatakan bahwa Tugas Akhir dengan judul **"Analisis Risiko dan Strategi Perlindungan Sistem terhadap Ancaman Siber pada Website `SAMBANG` Kabupaten Jombang"** beserta seluruh isinya adalah karya saya sendiri dan bukan merupakan karya tulis orang lain, baik sebagian maupun seluruhnya, kecuali dalam bentuk kutipan yang telah disebutkan sumbernya.

Demikian surat pernyataan ini saya buat dengan sebenar-benarnya. Apabila kemudian ditemukan adanya pelanggaran terhadap etika keilmuan dalam karya saya ini, atau ada klaim dari pihak lain terhadap keaslian karya saya ini maka saya siap menanggung segala bentuk resiko/sanksi yang berlaku.

Mengetahui,
Dosen Pembimbing

Zamah Sari ST., MT.

Malang, 13 Oktober 2025
Yang Membuat Pernyataan

Muh. Rayhan Islamiah Prathama

ABSTRAK

Penelitian ini bertujuan untuk menganalisis risiko keamanan serta merumuskan strategi perlindungan sistem terhadap ancaman siber pada website "SAMBANG" milik Pemerintah Kabupaten Jombang. Pendekatan penelitian yang digunakan adalah kualitatif eksploratif melalui observasi, studi literatur, serta penetration testing non-destruktif berbasis standar OWASP dan NIST. Hasil penelitian menunjukkan bahwa website "SAMBANG" masih memiliki sejumlah kerentanan dengan tingkat risiko yang tinggi, terutama pada fitur Open Data, Data Statistik, Katalog Data, dan Request Data yang rentan terhadap serangan Cross-Site Scripting (XSS), baik reflected maupun stored. Selain itu, potensi risiko SQL Injection teridentifikasi meskipun tidak tereksploitasi secara langsung, serta kelemahan autentikasi pada halaman login yang rentan terhadap brute force. Form Request Data juga ditemukan tidak memiliki mekanisme Cross-Site Request Forgery (CSRF) token, sehingga berpotensi dimanfaatkan oleh penyerang. Penelitian ini menyarankan penerapan validasi input, encoding output, Content Security Policy (CSP), prepared statement, autentikasi multi-faktor, pembatasan login, serta validasi file upload untuk meningkatkan perlindungan sistem. Dengan hasil ini, penelitian memberikan kontribusi praktis bagi pengelola sistem informasi publik daerah dalam memperkuat keamanan website pemerintahan serta membangun ketahanan siber yang lebih adaptif.

Kata kunci: Keamanan Siber, Analisis Risiko, Website Pemerintah, SQL Injection, XSS

ABSTRACT

This research aims to analyze security risks and formulate system protection strategies against cyber threats on the "SAMBANG" website owned by the Jombang Regency Government. The research approach used is exploratory qualitative through observation, literature study, and non-destructive penetration testing based on OWASP and NIST standards. The results of the study show that the "SAMBANG" website still has a number of vulnerabilities with a high level of risk, especially in the Open Data, Statistical Data, Data Catalog, and Data Request features, which are vulnerable to Cross-Site Scripting (XSS) attacks, both reflected and stored. In addition, the potential risk of SQL Injection was identified, although it was not directly exploited, as well as authentication weaknesses on the login page that were vulnerable to brute force. The Data Request form was also found to lack a Cross-Site Request Forgery (CSRF) token mechanism, making it potentially exploitable by attackers. This study recommends the implementation of input validation, output encoding, Content Security Policy (CSP), prepared statements, multi-factor authentication, login restrictions, and file upload validation to improve system protection. With these results, the study provides practical contributions for regional public information system managers in strengthening government website security and building more adaptive cyber resilience.

Keywords: Cybersecurity, Risk Analysis, Government Websites, SQL Injection, XSS

LEMBAR PERSEMBAHAN

Puji syukur kepada Allah SWT atas rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan Tugas Akhir ini. Penulis menyampaikan ucapan terima kasih yang sebesar-besarnya kepada:

1. Bapak Zamah Sari, S.T., M.T. dan Bapak Ir. Denar Regata Akbi, S.Kom., M.Kom, M.T. selaku pembimbing tugas akhir, yang telah memberikan bimbingan, dukungan, dan arahan kepada penulis dalam menyelesaikan penelitian ini.
2. Bapak/Ibu Dekan Fakultas Teknik Universitas Muhammadiyah Malang yang telah mendukung dan memberikan fasilitas pendidikan yang memadai.
3. Bapak Ir. Galih Wasis Wicaksono, S.Kom., M.Cs. selaku Ketua Program Studi Informatika Universitas Muhammadiyah Malang.
4. Bapak Wahyu Andhyka Kusuma, S.Kom, M.Kom selaku dosen wali yang telah membimbing selama perkuliahan.
5. Seluruh Dosen beserta Staf Program Studi Informatika Universitas Muhammadiyah Malang yang telah memberikan ilmu dan wawasan kepada penulis selama melaksanakan studi.
6. Kedua orang tua, Bapak Ivan Jalasena Prathama dan Ibu Lina Delarama Hasyim, yang senantiasa memberikan doa, dukungan, dan kasih sayang yang tidak terbatas kepada penulis.
7. Keluarga besar saya, terutama nenek saya yang selalu memberi dukungan dan mendoakan saya.
8. Untuk orang yang istimewa, Yasmin Alissa Salsabella yang telah setia menemani langkah saya hingga saat ini. Yang selalu memberi dukungan, semangat, dan membantu saya selama proses penyusunan skripsi ini.
9. Teman-teman saya yang memberi dukungan khususnya Vito, Doni, Ihrom, Imam, Dafi, dan Nico yang selalu membantu disaat kebingungan.
10. Saya pribadi yang telah berhasil menyelesaikan studi sampai titik ini.

Malang, 03 Oktober 2025

Muhammad Rayhan Islamiah Prathama

KATA PENGANTAR

Puji syukur kehadirat Allah SWT atas segala rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan makalah tugas akhir yang berjudul "**Analisis Risiko dan Strategi Perlindungan Sistem terhadap Ancaman Siber pada Website 'Sambang' Kabupaten Jombang**."

Makalah ini disusun sebagai salah satu bentuk publikasi ilmiah dari hasil penelitian tugas akhir pada Program Studi Informatika, Fakultas Teknik, Universitas Muhammadiyah Malang. Penulis berharap karya ini dapat memberikan wawasan serta kontribusi bagi pengembangan kajian keamanan siber, khususnya dalam upaya perlindungan sistem pada website pelayanan publik pemerintah daerah.

Penulis menyadari bahwa makalah ini masih memiliki keterbatasan, oleh karena itu kritik dan saran yang membangun sangat penulis harapkan demi penyempurnaan karya ini di masa mendatang.

Malang, 03 Oktober 2025

Penulis

Muhammad Rayhan Islamiah Prathama

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

DAFTAR PUSTAKA

[1] M. Ali, A. A. Gani, and M. I. Zainal, "Cybersecurity Threats and Countermeasures in Digital Government: A Systematic Literature Review," *Journal of Information Security*, vol. 14, no. 2, pp. 45–59, 2023. doi: 10.4236/jis.2023.142004.

[2] M. S. H. Rahman, M. Hossain, and M. I. Hoque, "SQL Injection Attack Detection and Prevention Techniques: A Review," *Security and Privacy*, vol. 4, no. 3, pp. 1–14, 2021. doi: 10.1002/spy2.126.

[3] K. A. Mahmood, R. A. Shaikh, and M. Ahmed, "A Review of Cross Site Scripting (XSS) Attack and Defense Mechanisms," in *Proc. 2020 Int. Conf. Cyber Warfare and Security (ICCWS)*, Islamabad, Pakistan, pp. 145–150. doi: 10.1109/ICCWS51030.2020.00028.

[4] B. A. Latif, M. A. M. Isa, and S. M. M. Shah, "A Comparative Study on Web Application Vulnerabilities: SQL Injection and XSS," *Journal of ICT Research and Applications*, vol. 17, no. 1, pp. 89–104, 2023. doi: 10.5614/itbj.ict.res.appl.2023.17.1.6.

[5] Z. Alharbi and N. Khan, "Cyber Resilience: A Review and Research Agenda," *Computers & Security*, vol. 105, pp. 102–123, 2021. doi: 10.1016/j.cose.2021.102238.

[6] J. Smith and L. Zhang, "Understanding Cybersecurity and Cyber Resilience in Modern Information Systems," *IEEE Access*, vol. 9, pp. 124337–124350, 2021. doi: 10.1109/ACCESS.2021.3108698.

[7] T. T. Nguyen, "A Survey on Web Application Security: SQLi and XSS Attacks," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 6, pp. 398–405, 2021. doi: 10.14569/IJACSA.2021.0120648.

[8] K. A. Kurniawan, A. Nugroho, and D. Wulandari, "Implementasi Penetration Testing Metode Black Box untuk Mengetahui Keamanan Website Pemerintahan," *Jurnal Ilmiah Teknologi Informasi Asia*, vol. 15, no. 2, pp. 101–110, 2022. doi: 10.37253/jtia.v15i2.574.

[9] F. Yusuf, "Metode Vulnerability Assessment dalam Mengetahui Kerentanan Sistem Website: Studi Kasus E-Gov," *Jurnal Teknik Informatika dan Sistem Informasi (JuTISI)*, vol. 9, no. 1, pp. 57–64, 2023. doi: 10.30596/jutisi.v9i1.12963.

[10] R. Anwar and S. R. Putri, "Analisis SQL Injection pada Sistem Informasi Akademik Menggunakan Metode White Box Testing," *Jurnal Teknologi dan Sistem Komputer*, vol. 12, no. 2, pp. 180–186, 2024. doi: 10.14710/jtsiskom.2024.180.

[11] M. Alshaer, A. Shaaban, dan R. Alsaqour, "Advanced Techniques for Detecting and Preventing SQL Injection Attacks: A Comprehensive Survey," IEEE Access, vol. 10, pp. 12345-12362, 2022.

[12] S. Kumar, R. R. Singh, dan P. K. Singh, "An Efficient Detection and Prevention Model for Cross-Site Scripting (XSS) Attacks," IEEE Transactions on Information Forensics and Security, vol. 17, no. 4, pp. 975-984, Apr. 2022.

[13] Y. Zhang, J. Li, dan X. Liu, "Cyber Resilience Framework for Critical Infrastructure: A Survey and Future Directions," IEEE Transactions on Industrial Informatics, vol. 18, no. 2, pp. 789-799, Feb. 2022.

[14] A. Gupta dan N. Gupta, "Machine Learning Approaches for Cybersecurity Threat Detection: A Review," IEEE Transactions on Neural Networks and Learning Systems, vol. 33, no. 1, pp. 12-29, Jan. 2022.

[15] J. Smith dan K. Johnson, "A Study on the Impact of Social Engineering Attacks on Cybersecurity," IEEE Security & Privacy, vol. 19, no. 3, pp. 48-56, May/June 2021.

[16] L. Chen, M. Wang, dan H. Zhao, "Multi-Layer Defense Mechanisms for Enhancing Cybersecurity in IoT Environments," IEEE Internet of Things Journal, vol. 9, no. 12, pp. 9201-9211, Jun. 2022

[17] Jonny, J., Ambarwati, A., & Darujati, C. (2021). Penilaian risiko data sistem informasi manajemen puskesmas dan aset menggunakan ISO 27005. SISTEMASI, 10(1), 1. https://doi.org/10.32520/stmsi.v10i1.995

[18] Leasa, Z. V., & Prassida, G. F. (2024). Manajemen risiko pada sistem informasi akademik Universitas XYZ menggunakan ISO 27005:2018. Jurnal Teknologi dan Sistem Informasi Bisnis, 6(4), 649–656. https://doi.org/10.47233/jteksis.v6i4.1459

[19] Ramadhan, D. L., Febriansyah, R., & Dewi, R. S. (2020). Analisis manajemen risiko menggunakan ISO 31000 pada smart canteen SMA XYZ. JURIKOM (Jurnal Riset Komputer), 7(1), 91. https://doi.org/10.30865/jurikom.v7i1.1791.

[20] Sitorus, M. G. B., Maria, N., & Safa, Y. N. (2024). Tinjauan literatur manajemen risiko cyber dalam proyek: Identifikasi, evaluasi, dan mitigasi ancaman. Jurnal Manajemen Informatika (JAMIKA), 14(2), 187–198. https://doi.org/10.34010/jamika.v14i2.12887

UNIVERSITAS
MUHAMMADIYAH
MALANG

FAKULTAS TEKNIK

INFORMATIKA
informatika.umm.ac.id | informatika@umm.ac.id

FORM CEK PLAGIARISME LAPORAN TUGAS AKHIR

Nama Mahasiswa : **Muh. Rayhan Islamiah Prathama**

NIM : **202010370311333**

Judul TA : **Analisis Risiko dan Strategi Perlindungan Sistem terhadap Ancaman Siber pada Website 'SAMBANG' Kabupaten Jombang**

Hasil Cek Plagiarisme dengan Turnitin

No.	Komponen Pengecekan	Nilai Maksimal Plagiarisme (%)	Hasil Cek Plagiarisme (%) *
1.	Bab 1 – Pendahuluan	10 %	2%
2.	Bab 2 – Daftar Pustaka	25 %	14%
3.	Bab 3 – Analisis dan Perancangan	25 %	10%
4.	Bab 4 – Implementasi dan Pengujian	15 %	0%
5.	Bab 5 – Kesimpulan dan Saran	5 %	0%
6.	Makalah Tugas Akhir	20%	11%

) Hasil cek plagiarism diisi oleh pemeriksa (staf TU)

***) Maksimal 5 kali (4 Kali sebelum ujian, 1 kali sesudah ujian)**

Mengetahui,

Pemeriksa (Staff TU)

deny