https://jurnal.pustakagalerimandiri.co.id/index.php/pustakadata
DOI: https://doi.org/10.55382/jurnalpustakadata.v6i2.1771

Jurnal Pustaka Data
Pusat Akses Kajian Database, Analisa Teknologi, dan Arsitektur Komputer
Pustaka Galeri Mandiri
Vol. 6 No. 2 (2026) 117– 126
E ISSN: 2809-7483

Dashboard Monitoring Keamanan Domain Berbasis Web untuk Deteksi Backlink Berbahaya Menggunakan Integrasi Data Semrush

Sonasa Rinusantoro[1], Fawzi Rahmadiyan Zuhairi[2], Abdurrahman Rahim Thaha[3], Abdul Rizal Adompo[4], Dinda Prifaty Nareswara[5]
Sistem Informasi, Universitas Terbuka
[1*]sonasa@ecampus.ut.ac.id

Abstract

This study aims to develop a dashboard application as a monitoring medium for hacked content that infects the web domains of Universitas Terbuka. The background of the study is based on the high number of domains managed, namely 488 domains, as well as the discovery of 3,753 backlinks with a dangerous toxicity score based on the Semrush audit results for the December 2024 period. Monitoring that was previously conducted manually caused delays in detection, uncentralized data, and slow responses to cyber security incidents. The research method uses the System Development Life Cycle (SDLC) approach which includes the stages of planning, requirements analysis, system design, implementation, as well as testing and evaluation. The system was developed using a web-based architecture with a Laravel backend, MariaDB database, and a dashboard-based visual frontend. The main features include upload and synchronization of CSV data from scanning results, visualization of backlink metrics (source URL, target URL, source domain, toxicity score), domain management, role-based user management (admin and PIC unit/regional UT), as well as real-time updates of backlink handling status. The results of the User Acceptance Test (UAT) show that all core system functions run with a very high success rate. Data management functions, duplication validation, automatic mapping to PIC, and dashboard visualization are declared accurate and stable. User feedback focuses more on the development of additional features such as data filters, bulk edit, notifications, and integration with external systems. Overall, the dashboard application is declared feasible to be used as a centralized monitoring system to improve the effectiveness of domain security supervision.

Keywords: Monitoring Dashboard, Hacked Content, Web Security, Webometrics, SDLC.

Abstrak

Penelitian ini bertujuan mengembangkan aplikasi dashboard sebagai media monitoring terpusat untuk mendeteksi konten hack pada domain web Universitas Terbuka. Permasalahan utama adalah pengelolaan 488 domain dengan temuan 3.753 backlink berisiko tinggi, sementara sistem sebelumnya masih manual, tidak terintegrasi, tidak memiliki histori terpusat, serta tidak menyediakan visualisasi maupun pemetaan tanggung jawab, sehingga menyebabkan keterlambatan deteksi dan respons insiden. Kebaruan (novelty) penelitian ini terletak pada integrasi monitoring berbasis dashboard yang menggabungkan sinkronisasi data eksternal (CSV Semrush), pemetaan otomatis domain ke PIC berbasis subdomain, validasi duplikasi data, serta pembaruan status penanganan secara real-time dalam satu sistem terpusat. Metode yang digunakan adalah System Development Life Cycle (SDLC). Evaluasi sistem dilakukan menggunakan pengujian fungsional dan User Acceptance Test (UAT). Hasil pengujian menunjukkan tingkat keberhasilan fungsi umum sebesar 90–100% (18–20 dari 20 skenario), fungsi admin 100% (23/23 skenario), dan fungsi pengguna PIC sebesar 76,9%–100% (10–13 dari 13 skenario). Akurasi penyajian metrik utama (source URL, target URL, source domain, dan mapping PIC) mencapai 100% (7/7 pengujian), serta validasi duplikasi dan proses sinkronisasi data menunjukkan tingkat keberhasilan 100% tanpa redundansi data. Kontribusi ilmiah penelitian ini adalah penyediaan model sistem monitoring keamanan domain berbasis dashboard terintegrasi yang mampu menggantikan proses manual

Submitted : 06-03-2026 | Reviewed : 17-04-2026 | Accepted : 26-04-2026

menjadi sistem terpusat, terstruktur, dan berbasis visual analytics, serta meningkatkan ketepatan informasi dan efisiensi proses monitoring secara terukur.

Kata Kunci: Dashboard Monitoring, Konten Hack, Keamanan Web, Webometrics, SDLC.

1. Pendahuluan

Perkembangan teknologi informasi telah mendorong institusi pendidikan tinggi untuk semakin mengandalkan platform digital dalam mendukung kegiatan akademik, administratif, dan publikasi ilmiah. Keberadaan website institusi tidak hanya berfungsi sebagai media informasi, tetapi juga menjadi representasi reputasi dan kredibilitas universitas di tingkat nasional maupun internasional. Dalam konteks ini, kualitas dan keamanan domain web menjadi aspek strategis yang harus dikelola secara berkelanjutan.

Pengembangan dan pemanfaatan sistem monitoring untuk mendeteksi serta mengendalikan konten ilegal atau toksik yang menyusup ke domain universitas merupakan langkah penting dalam menjaga integritas institusi dan menciptakan lingkungan daring yang aman. Institusi yang memiliki sistem pemantauan yang baik dapat mengurangi risiko peretasan, pencemaran nama baik, serta penyebaran konten berbahaya. Selain itu, sistem monitoring yang efektif juga memastikan kepatuhan terhadap standar hukum dan etika serta memperkuat kepercayaan publik terhadap komitmen universitas dalam menjaga keamanan digital.

Dalam era persaingan global pendidikan tinggi, peringkat universitas menjadi indikator penting dalam menilai kualitas dan visibilitas institusi. Salah satu sistem pemeringkatan yang berfokus pada keberadaan digital adalah Webometrics, yang menilai universitas berdasarkan kehadiran web, output penelitian, dan keterbukaan akses informasi [26], [34]. Oleh karena itu, pengelolaan website yang aman, berkualitas, dan informatif menjadi kebutuhan strategis dalam meningkatkan posisi universitas pada pemeringkatan berbasis web [5].

Universitas Terbuka memiliki infrastruktur digital yang luas dengan 488 domain yang dikelola. Kompleksitas ini meningkatkan potensi risiko terhadap ancaman keamanan siber seperti deface, malware, injection, serta penyebaran backlink negatif. Hasil audit Semrush menunjukkan terdapat 3.753 backlink dengan skor toksisitas berbahaya yang berpotensi memengaruhi reputasi institusi serta indikator Webometrics.

Namun, proses monitoring keamanan domain di Universitas Terbuka saat ini masih dilakukan secara manual melalui pengecekan direktori hosting, laporan pengguna, serta scanning terpisah yang tidak terintegrasi. Pendekatan ini memiliki beberapa keterbatasan, antara lain: (1) tidak bersifat real-time sehingga menyebabkan keterlambatan deteksi; (2) tidak terintegrasi antar sumber data sehingga menyulitkan analisis menyeluruh; (3) tidak menyediakan visualisasi berbasis dashboard analitik, serta; (4) tidak memiliki histori serangan dan pemetaan tanggung jawab yang terstruktur. Keterbatasan ini berdampak pada lambatnya respons terhadap insiden serta rendahnya efisiensi proses monitoring keamanan domain.

Berdasarkan gap tersebut, diperlukan suatu sistem monitoring yang mampu mengintegrasikan berbagai sumber data keamanan, menyediakan visualisasi analitik, serta mendukung pengambilan keputusan secara cepat dan akurat. Oleh karena itu, penelitian ini mengusulkan pengembangan aplikasi dashboard monitoring konten hack yang terintegrasi.

Kontribusi utama penelitian ini adalah: (1) integrasi data hasil scanning eksternal (Semrush) ke dalam sistem dashboard terpusat; (2) penerapan mekanisme pemetaan otomatis domain ke penanggung jawab (PIC) berbasis subdomain; (3) pengembangan visual analytics untuk memantau tingkat risiko keamanan domain berdasarkan metrik backlink dan toxicity score, serta; (4) penyediaan sistem monitoring berbasis real-time yang dilengkapi dengan histori dan status penanganan insiden.

Dengan pendekatan tersebut, sistem yang dikembangkan diharapkan mampu meningkatkan kecepatan deteksi, akurasi informasi, serta efektivitas respons tim ICT dalam menjaga keamanan dan reputasi digital Universitas Terbuka.

Dalam konteks ini, kualitas dan keamanan domain web menjadi aspek strategis yang harus dikelola secara berkelanjutan.

Pengembangan dan pemanfaatan situs web khusus untuk memantau serta mengendalikan konten ilegal atau toksik yang menyusup ke domain universitas merupakan langkah penting dalam menjaga integritas institusi dan menciptakan lingkungan daring yang aman. Institusi yang memiliki sistem pemantauan yang baik dapat mengurangi risiko peretasan, pencemaran nama baik, serta penyebaran konten berbahaya yang merusak reputasi,Selain itu,

sistem monitoring yang efektif juga memastikan kepatuhan terhadap standar hukum dan etika serta memperkuat kepercayaan publik terhadap komitmen universitas dalam menjaga keamanan digital.

Selama ini, proses monitoring keamanan domain di lingkungan Universitas Terbuka masih dilakukan secara manual melalui pengecekan direktori hosting, laporan pengguna, serta scanning terpisah yang tidak terintegrasi. Metode ini menyebabkan keterlambatan deteksi, tidak tersedianya histori serangan secara terpusat, serta lambatnya respons terhadap insiden. Selain aspek teknis, tantangan keamanan siber juga berkaitan dengan budaya dan kesadaran keamanan di lingkungan organisasi [16], [27]. Oleh karena itu, diperlukan sistem monitoring yang terstruktur, otomatis, dan terintegrasi untuk meningkatkan efektivitas pengawasan keamanan domain.

Berdasarkan permasalahan tersebut, penelitian ini berfokus pada pengembangan aplikasi dashboard sebagai media monitoring konten hack yang menginfeksi domain web Universitas Terbuka. Sistem ini dirancang untuk melakukan scanning otomatis, mengintegrasikan data hasil audit, menampilkan visualisasi metrik backlink dan toxicity score, serta menyediakan notifikasi dan histori penanganan secara terpusat. Dengan pendekatan ini, diharapkan dashboard monitoring mampu meningkatkan kecepatan deteksi, ketepatan informasi, serta efektivitas respons tim ICT dalam menjaga keamanan dan reputasi digital Universitas Terbuka.

Pengembangan dan pemanfaatan situs web khusus untuk memantau dan mengendalikan konten ilegal atau toksik yang menyusup ke domain digital universitas sangat penting untuk menjaga integritas institusi dan memastikan lingkungan daring yang aman. Universitas semakin bergantung pada platform digital untuk keperluan akademik, administratif, dan penelitian, yang membuatnya rentan terhadap ancaman keamanan siber, seperti peretasan, penyebaran konten ilegal, atau aktivitas berbahaya. Sistem pemantauan yang khusus berfungsi sebagai perisai digital, memungkinkan institusi untuk mendeteksi aktivitas tidak sah secara cepat, menilai potensi risiko, dan mengambil tindakan korektif segera. Dengan menerapkan sistem semacam ini, universitas dapat secara proaktif mengurangi ancaman, mengurangi risiko serangan siber, dan melindungi data sensitive [27].

Webometrics, yang dikembangkan oleh Cybermetrics Lab dari Spanish National Research Council (CSIC), berfungsi sebagai sistem pemeringkatan universitas global yang komprehensif dengan mengevaluasi institusi berdasarkan keberadaan dan dampak web mereka. Tidak seperti pemeringkatan tradisional yang sebagian besar berfokus pada output penelitian, Webometrics menilai universitas berdasarkan berbagai misi, termasuk pengajaran, penelitian, dan keterlibatan sosial, dengan menganalisis volume konten web, visibilitas, dan dampak publikasi web. Pendekatan ini mencerminkan komitmen universitas terhadap transparansi, aksesibilitas, dan penyebaran pengetahuan melalui platform digital [2].

Menurut [6] bahwa Systems Development Life Cycle (SDLC) merupakan suatu proses pembuatan dan pengubahan sistem serta model dan metodologi yang digunakan untuk mengembangkan sebuah sistem[6]. Sedangkan menurut [5] kaitan antara framework dengan Systems Development Life Cycle (SDLC) adalah keduanya memiliki karakteristik yang sama yaitu memiliki elemen – elemen yang saling berhubungan antara satu dengan lainnya yaitu pada framework memiliki tahapan–tahapan antara tahapan satu dengan tahapan yang lain memiliki hubungan, selain itu framework juga memiliki batasan yakni hanya tertuju pada kasus tertentu yatiu pada setiap framework hanya memiliki tahapan–tahapan untuk satu tujuan tertentu. Metode Systems Development Life Cycle (SDLC) dapat digunakan untuk proses pengembangan framework karena memiliki tahapan – tahapan yang dibutuhkan dalam pengembangannya.

Dalam pengembangan framework dibutuhkan beberapa tahapan yang ada pada SDLC yaitu planning, analysis, design, implementation, dan maintenance [5].

Universitas Terbuka (UT) memiliki banyak domain dan subdomain yang digunakan untuk layanan akademik, administrasi, pembelajaran online, dan publikasi. Tingginya aktivitas akses dan kompleksitas infrastruktur tersebut membuat domain UT rentan: (1). terinfeksi konten hack seperti script backdoor, file deface, webshell, atau malware; (2). mengalami perubahan file tidak wajar; (3). menjadi target otomatis oleh bot atau scanner attacker.

Monitoring selama ini dilakukan secara manual melalui pengecekan direktori hosting, laporan pengguna, dan scanning terpisah, sehingga: deteksi terlambat, proses tidak terpusat, tidak ada tren dan histori serangan, respon insiden menjadi lambat.

Masalah ini menuntut adanya sistem yang mampu mendeteksi konten hack secara cepat, terstruktur, dan terpadu.

2. Metode Penelitian

Metode penelitian yang digunakan mengacu pada tahapan *System Development Life Cycle* (SDLC) yang dipadukan dengan pendekatan analisis keamanan untuk mendeteksi konten berbahaya. Selain berfokus pada pengembangan sistem, penelitian ini juga menerapkan desain eksperimen untuk mengukur kinerja sistem dalam mendeteksi

backlink berbahaya berdasarkan data yang diperoleh dari Semrush.

Tahapan penelitian meliputi identifikasi masalah, penetapan tujuan, analisis kebutuhan sistem, desain sistem, implementasi sistem, serta pengujian dan evaluasi sistem.

2. 1 Identifikasi Masalah
Tahapan ini bertujuan untuk mengidentifikasi permasalahan pada pengelolaan data serta potensi ancaman keamanan siber berupa backlink berbahaya yang mengarah ke domain universitas. Permasalahan utama meliputi meningkatnya jumlah data yang belum dimanfaatkan secara optimal serta belum adanya sistem yang mampu mendeteksi dan memonitor konten berbahaya secara terpusat.

2.2 Tujuan Penelitian
Tujuan penelitian ini adalah membangun sistem dashboard berbasis web yang mampu melakukan monitoring dan analisis data, serta mendeteksi backlink berbahaya untuk mendukung pengambilan keputusan strategis, khususnya dalam aspek keamanan dan promosi universitas.

2.3 Analisis Kebutuhan Sistem
Analisis kebutuhan dilakukan untuk mengidentifikasi kebutuhan perangkat keras dan perangkat lunak yang diperlukan dalam pembangunan sistem. Sistem dirancang berbasis web dengan kebutuhan utama meliputi pengolahan data backlink, visualisasi data, serta modul deteksi konten berbahaya. Selain itu, dilakukan analisis kebutuhan proses bisnis guna mendukung strategi promosi dan keamanan informasi.

2.4 Desain Sistem
Desain sistem meliputi perancangan arsitektur sistem, desain basis data, serta antarmuka pengguna. Selain itu, dirancang pula model analitik keamanan yang digunakan untuk mendeteksi backlink berbahaya. Model yang digunakan adalah pendekatan rule-based detection dan heuristic detection, dengan memanfaatkan parameter seperti skor toksisitas backlink, pola domain mencurigakan, serta anomali pada data.

2.5 Implementasi Sistem
Implementasi dilakukan dengan membangun aplikasi dashboard berbasis web yang terintegrasi dengan data hasil audit Semrush. Sistem mampu mengolah data, menampilkan visualisasi dalam bentuk grafik, serta memberikan penanda (flagging) terhadap backlink yang terindikasi berbahaya berdasarkan aturan yang telah ditentukan.

2.6 Desain Eksperimen dan Skenario Pengujian
Penelitian ini menggunakan desain eksperimen untuk menguji kinerja sistem dalam mendeteksi backlink berbahaya. Dataset yang digunakan berupa data backlink yang telah diklasifikasikan berdasarkan tingkat toksisitas.

Skenario pengujian meliputi: (1). Uji fungsional, untuk memastikan seluruh fitur sistem berjalan dengan baik; (2). Uji deteksi, untuk mengukur kemampuan sistem dalam mengidentifikasi backlink berbahaya; (3). Uji performa, untuk mengukur kecepatan sistem dalam memproses dan menampilkan data. Pengujian dilakukan dengan membandingkan hasil deteksi sistem terhadap data referensi dari Semrush.

2.7 Parameter Evaluasi

Evaluasi sistem dilakukan menggunakan beberapa parameter, antara lain: (1). Akurasi, yaitu tingkat ketepatan sistem dalam mendeteksi backlink berbahaya; (2). False Positive, yaitu jumlah data normal yang terdeteksi sebagai berbahaya; (3). False Negative, yaitu jumlah data berbahaya yang tidak terdeteksi oleh sistem.

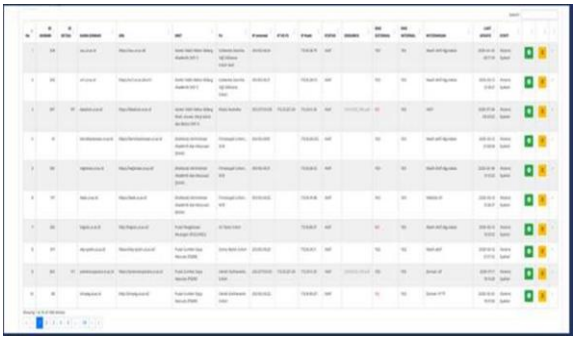
Parameter tersebut digunakan untuk menilai efektivitas model deteksi yang diterapkan dalam sistem.

2.8 Analisis Hasil
Analisis hasil dilakukan terhadap data yang dihasilkan oleh sistem, baik dalam bentuk visualisasi maupun hasil deteksi. Hasil analisis digunakan untuk mengevaluasi kinerja sistem dalam mendukung kebutuhan keamanan siber dan strategi promosi universitas.

3. Hasil dan Pembahasan

Sistem yang dikembangkan, sitemonitor.ut.ac.id, mampu melakukan sinkronisasi data *backlink* berbahaya secara otomatis dari file CSV Semrush ke unit kerja (PIC) terkait. Dashboard menampilkan metrik utama seperti *Source URL*, *Target URL*, dan klasifikasi *Toxicity Score* (0-30 rendah hingga 81+ kritis).

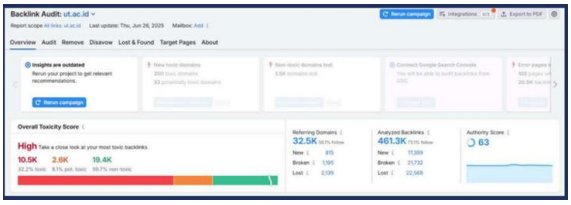
Aplikasi dashboard ini dikembangkan untuk memonitor, mendeteksi, dan menampilkan status konten hack atau malicious content yang menginfeksi domain web Universitas Terbuka (UT). Saat ini monitoring dilakukan secara manual melalui pengecekan folder hosting, laporan pengguna, atau hasil scanning tidak terpusat, sehingga rentan terlambat mendeteksi infeksi. Sistem dashboard ini diharapkan menyediakan informasi real-time, terpusat, dan mudah dianalisis oleh tim ICT. Terdapat 488 domain Universitas Terbuka berdasarkan noc-dc.ut.ac.id. seperti tampak pada gambar 1.



Gambar 1. Terdapat 488 Domain UT Berdasarkan noc-dc.ut.ac.id

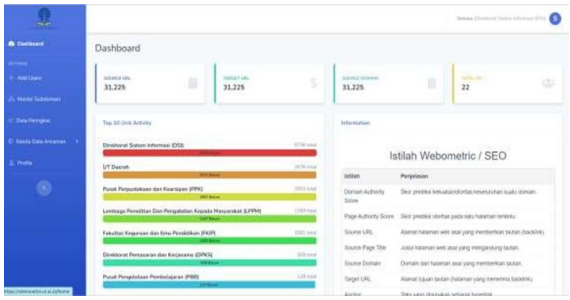
Percmasalahan utama yang terjadi di lingkungan domain web UT: (1). Tingginya percobaan dan insiden hacking terhadap subdomain UT (deface, file upload, injection, dan malware); (2). Kesulitan menemukan file berbahaya secara cepat karena jumlah direktori yang banyak dan struktur hosting yang kompleks; (3). Tidak ada sistem monitoring terpusat yang memperlihatkan status keamanan setiap domain/subdomain; (4). Analisis manual memakan waktu lama dan berpotensi melewatkan file yang sudah bermutasi; (5). Tidak tersedia laporan otomatis untuk membantu tim teknis melakukan tindakan perbaikan.

Proses dimulai dari mengambil domain yang akan discan oleh semruh.com. setelah proses scan selesai download file csv. File tersebut kemudian di unggah ke sitemonitor.ut.ac.id melalui proses batching. Sinkronisasi berdasarkan domain pic unit atau UT daerah. Menampilkan ke domain pic unit atau UT daerah untuk dilakukan pembersihan di google search console dan disavow. Admin site monitor atau tim Webometrics UT melakukan monitoring hasil perbaikan tersebut. Gambar 2 menunjukkan data backlink audit semrush.com



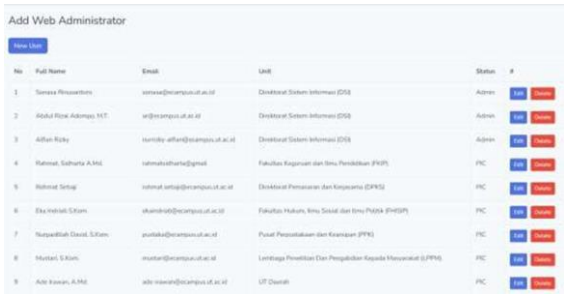
Gambar 2. Data Backlink Audit semrush.com

Halaman antarmuka sistem menampilkan halaman login pengguna dengan input email address dan password dilengkapi dengan remember input tersebut. Setelah berhasil login adalah halaman dashboard yang menampilkan jumlah source url, target url,source domain, total pic, top 10 unit activity, istilah webometric/SEO, peringkat Webometrics UT, Sebaran Toxicity Score berdasarkan total keseluruhan link. Halaman dashboard dapat dilihat pada gambar 3.



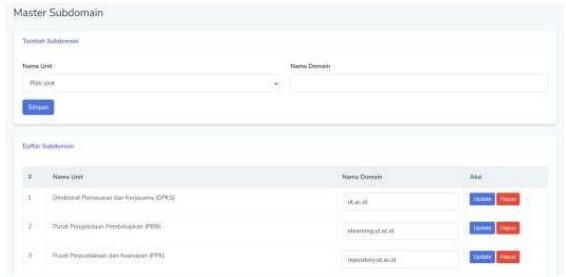
Gambar 3. Halaman Dashboard Sistem

Halaman Add Users digunakan untuk menambah, menghapus, dan mengedit pengguna berdasarkan unit dan status pengguna admin dan pic. Pengguna admin dapat mengelola pengguna, master sub domain,data peringkat webometrics, dan kelola data ancaman. Seperti yang tampak pada gambar 4



Gambar 4. Halaman Add Users

Halaman master sub domain digunakan untuk menambahkan sub domain baru, mengedit subdomain lama, dan menghapus sub domain dari sistem, seperti yang ada pada gambar 5.

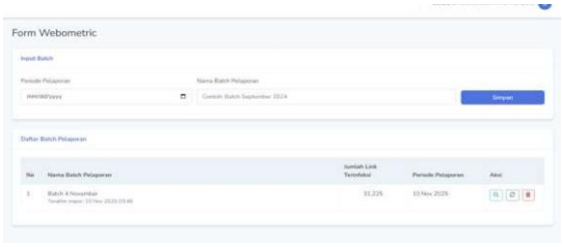


Gambar 5. Halaman Master Subdomain

Halaman Data Peringkat Webometrics digunakan untuk menambahkan data peringkat webometrics Universitas Terbuka berdasarkan tahun, periode, peringkat dunia, peringkat nasional. Data peringkat dapat diedit dan dihapus dari sistem, seperti tampak pada gambar 6.

Gambar 6. Halaman Data Peringkat Webometrics

Halaman kelola data ancaman webometrics digunakan untuk menambahkan bacth berdasarkan periode pelaporan, dan nama batch pelaporan. Setelah bacth ditambahkan dilakuka sinkronisasi data file csv dari semrush ke mapping domain-domain yang ada dalam sistem berdasarkan pic unit masing-masing. Gambar kaca pembesar digunakan untuk melihat data detail setelah proses upload file csv. Gambar icon tempat sampah digunakan untuk menghapus batch beserta file csv yang sudah di upload. Seperti yang tersaji pada gambar 7.

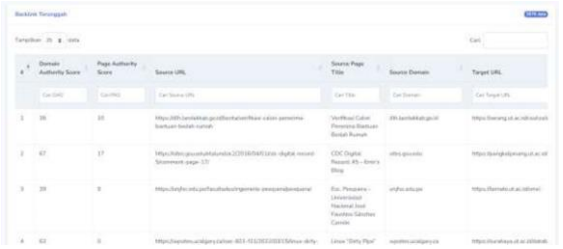


Gambar 7. Halaman Kelola Data Ancaman Webometrics

Halaman dashboard untuk pengguna pic unit atau UT Daerah lebih sedikit menunya hanya menu kelola data ancaman dan profile. Menampilkan jumlah source url, target url, source domain, total pic, top 10 unit activity hanya menampilkan unit atau UT Daerah berdasarkan pengguna. Total backlink yang belum dibersihkan maupun keseluruhan. Terdapat grafik peringkat webometrics UT berdasarkan periode dan peringkat semakin kecil semakin baik. Terdapat istilah webometrics atau SEO. Terdapat sebaran toxicity score berdasarkan keseluruhan link. Terdapat total link dianalisis, rata-rata skor, skor minimum, skor maksimum, skor 0 – 30 (rendah), skor 31-60 (sedang), skor 61-80 (tinggi), dan skor 81+ kritis. Tampilan halaman ini dapat dilihat pada gambar 8.

Gambar 8. Halaman Dashboard Pengguna PIC Unit/UT Daerah

Halaman menu kelola data ancaman webometrics pengguna pic unit atau UT Daerah hanya dapat melihat hasil backlink berdasarkan domain pengguna, seperti pada gambar 9.



Gambar 9. Halaman Kelola Data Ancaman Pengguna PIC Unit/UT Daerah

3.1 Pengujian Sistem

Pengujian terbatas UAT (User Accepted Test) dilakukan berdasarkan 30 skor toxicity terbesar hasil scanning semrush per 04 November 2025. Unit yang memperoleh skor tersebut adalah FKIP, FHISIP, LPPM, LLOP – Pusat Pengelolaan Pembelajaran, Direktorat Pemasaran dan Kerjasama. Untuk UT Daerah Adalah UT Serang, UT Ternate, UT Pangkal Pinang, UT Surabaya, UT Bogor, UT Bengkulu, UT Jakarta dan UT Makassar. Hasil pengujian dapat dilihat pada tabel 1 dan tabel 2.

Tabel 1. Hasil Pengujian

No.	Jenis Pengujian	Jumlah Berhasil	Jumlah Gagal
1	Fungsi Login Berhasil (Valid Credentials): Apakah pengguna dapat berhasil masuk menggunakan kombinasi email dan password yang benar?	20	0
2	Penanganan Kesalahan (Password Salah): Saat memasukkan email benar, tetapi password salah, apakah sistem menampilkan pesan error yang jelas dan tidak membingungkan pengguna?	18	2
3	Penanganan Kesalahan (Email Salah): Saat memasukkan email yang tidak terdaftar di sistem, apakah sistem menampilkan pesan error yang sesuai (bukan internal server error)?	19	1
4	Pengalihan Halaman (Otorisasi): Setelah berhasil login, apakah Admin diarahkan ke Dashboard Admin (dengan semua menu Import dan Setting terlihat), dan PIC diarahkan ke Dashboard PIC (hanya menampi...	19	1
5	Update Informasi Dasar: Apakah pengguna dapat berhasil mengubah Nama (First Name dan Last Name) dan menyimpan perubahan tersebut?	19	1
6	Ganti Password Berhasil: Apakah pengguna dapat berhasil mengganti password dengan mengisi Current password, New password, dan Confirm password secara benar?	20	0
7	Validasi Ganti Password (Current Salah): Apabila pengguna memasukkan Current password yang salah, apakah sistem menolak perubahan dan menampilkan pesan error yang jelas?	20	0
8	Validasi Ganti Password (Mismatch): Apabila New password dan Confirm password tidak cocok, apakah sistem menolak perubahan dan menampilkan pesan error validasi?	20	0
9	Update Email: Apakah sistem menolak jika mengupdate email address dengan email yang sudah ada di database?	20	0

Tabel 2. Hasil Pengujian Admin dan PIC Unit/UT Daerah

No.	Jenis Pengujian	Jumlah Berhasil	Jumlah Gagal
1.	Akurasi Metrik Utama: Apakah angka SOURCE URL, TARGET URL, SOURCE DOMAIN dan TOTAL PIC yang ditampilkan di Dashboard sudah akurat dan sesuai dengan total data di database?	7	0
2.	Top 10 Unit Activity: Apakah visualisasi progress penanganan antar unit (misal: DSI, FST) ditampilkan dengan benar, menunjukkan jumlah backlink yang Belum ditangani?	7	0
3.	Navigasi Menu: Apakah semua menu di sidebar (Dashboard, Master Subdomain, Kelola Data Ancaman, dll.) berfungsi dan mengarah ke halaman yang benar?	7	0
4.	Create (Tambah Akun): Apakah tombol New User berfungsi dan memungkinkan Admin untuk membuat akun PIC/Admin baru dengan mengisi semua data wajib dengan benar?	7	0
5.	Read & Update (Edit Akun): Apakah data di tabel pengguna tampil lengkap, dan fungsi Edit memungkinkan Admin mengubah Status atau memperbarui data Unit pengguna yang sudah ada?	7	0
6.	Delete (Hapus Akun): Apakah tombol Delete berfungsi dan dapat menghapus akun pengguna dari sistem secara permanen?	7	0
7.	Validasi Data (Email Unik): Apakah sistem menolak Admin membuat akun baru jika alamat Email yang dimasukkan sudah terdaftar sebelumnya?	7	0
8.	Create (Tambah Subdomain): Apakah Admin dapat berhasil menambahkan mapping Unit baru dengan memilih Nama Unit dan memasukkan Nama Domain yang benar, lalu menyimpannya?	7	0
9.	Read (Tampilan Data): Apakah tabel daftar subdomain menampilkan semua mapping Unit dan Domain yang sudah dibuat secara lengkap dan akurat?	7	0
10.	Update (Edit Subdomain): Apakah tombol Update berfungsi dan memungkinkan Admin untuk mengubah Nama Domain yang sudah terdaftar?	7	0
11.	Delete (Hapus Subdomain): Apakah tombol Hapus berfungsi dan dapat menghapus mapping Unit dan Domain dari sistem secara permanen?	7	0
12.	Validasi Duplikasi: Apakah sistem menolak Admin menyimpan data jika Nama Unit dan Nama Domain yang dimasukkan sudah terdaftar sebelumnya?	7	0
13.	Create (Tambah Peringkat): Apakah tombol Tambah Data dan form input memungkinkan Admin untuk memasukkan data peringkat baru (Tahun, Periode, Peringkat Dunia, Peringkat Nasional) dengan sukses?	7	0
14.	Read (Tampilan Data): Apakah tabel Daftar Peringkat Webometrics menampilkan semua entri peringkat secara lengkap, akurat, dan dapat dibaca dengan jelas?	7	0
15.	Update (Edit Peringkat): Apakah tombol Edit berfungsi dan memungkinkan Admin untuk mengubah nilai Peringkat Dunia atau Nasional untuk data yang sudah ada?	7	0
16.	Delete (Hapus Peringkat): Apakah tombol Hapus berfungsi dan dapat menghapus data Peringkat dari sistem secara permanen?	7	0
17.	Create Batch Pelaporan: Apakah Admin dapat berhasil membuat Batch Pelaporan baru (dengan Nama dan Periode Pelaporan) dan batch tersebut muncul di tabel dengan status "Belum ada impor"?	7	0
18.	Upload CSV (Import): Apakah tombol Aksi Upload (di batch baru) berfungsi dan Admin dapat berhasil mengunggah file CSV Semrush ke batch tersebut?	7	0
19.	Aksi Sinkronisasi (Sync): Apakah tombol Aksi Sync (di batch yang sudah diunggah) berfungsi dan proses sync berhasil memproses data backlink ke database?	7	0
20.	Visualisasi Detail Backlink: Apakah tombol Aksi Lihat Detail berfungsi dan menampilkan semua kolom data backlink (Domain Authority Score, Source URL, dll.) secara akurat?	7	0
21.	Validasi Duplikasi Link: Jika Admin menjalankan Sync berulang kali pada batch yang sama, apakah sistem hanya memasukkan data backlink unik dan tidak menciptakan duplikat link di database utama?	7	0
22.	Integrasi & Mapping PIC: Setelah sync berhasil, apakah data backlink yang masuk secara otomatis ditugaskan ke PIC yang benar berdasarkan Master Subdomain?	7	0
23.	Delete Batch: Apakah tombol Aksi Delete berfungsi dan menghapus batch beserta semua data backlink yang terkait dari database?	7	0
	User PIC Unit/UT Daerah		
1.	Pembatasan Menu: Apakah Menu Admin (Master Subdomain, Add Users, Data Peringkat) tidak terlihat atau tidak dapat diakses di sidebar saat PIC login?	13	0
2.	Otorisasi Data Tampilan: Apakah metrik utama (Source URL, Target URL, Unit Activity) di Dashboard hanya menampilkan total data yang terkait dengan unit PIC (misal: FST)?	12	1
3.	Navigasi PIC: Apakah menu yang tersisa (termasuk dropdown Kelola Data Ancaman) berfungsi dan mengarah ke halaman yang benar?	13	0
4.	Akses Data Batch: Apakah daftar Batch Pelaporan yang muncul hanya berisi batch yang memiliki backlink untuk unit PIC tersebut (misal: FST)?	10	3

5. Akses Detail Backlink: Apakah tombol Aksi Lihat Detail (ikon kaca pembesar) berfungsi dan menampilkan daftar backlink yang spesifik untuk unit PIC tersebut?	12	1
6. Fungsi Update Status: Apakah PIC dapat berhasil mengubah Status backlink (misal: dari Belum ditangani ke Done) menggunakan tombol dropdown?	13	0
7. Mengisi Catatan: Apakah PIC bisa mengisi Catatan penanganan?	13	0
8. Refleksi Dashboard: Setelah beberapa backlink diubah statusnya menjadi Done, apakah Dashboard PIC (Top Unit Activity) mencerminkan perubahan progress ini secara real-time?	13	0

3.2 Analisis Kinerja Sistem

3.2.1 Tingkat Keberhasilan Deteksi Backlink Berbahaya

Berdasarkan hasil pengujian menggunakan data backlink dari Semrush dengan fokus pada 30 skor toksisitas tertinggi, sistem mampu mendeteksi seluruh backlink yang telah dikategorikan sebagai berbahaya berdasarkan parameter yang ditentukan.

Dari total data uji sebanyak 30 backlink: (1). Backlink terdeteksi berbahaya oleh sistem: 30 data; (2). Backlink tidak terdeteksi: 0 data

Hasil ini menunjukkan bahwa sistem memiliki tingkat akurasi yang sangat tinggi dalam mendeteksi backlink berbahaya berdasarkan skor toksisitas dari Semrush. Namun demikian, hasil ini masih terbatas pada dataset tertentu dan perlu diuji lebih lanjut dengan data yang lebih bervariasi.

3.2.2 Analisis Waktu Sinkronisasi Data

Proses sinkronisasi data dilakukan melalui mekanisme upload file CSV dan proses parsing ke dalam database sistem. Berdasarkan hasil pengujian pada beberapa batch data: (1). Rata-rata jumlah data per batch: ±500 – 1000 backlink; (2). Waktu rata-rata proses upload dan sinkronisasi: 5 – 10 detik per batch

Waktu tersebut mencakup: Proses upload file CSV, Proses parsing data, Proses mapping ke domain dan PIC, dan Penyimpanan ke database

Hasil ini menunjukkan bahwa sistem memiliki performa yang cukup cepat dan efisien dalam menangani data dalam jumlah besar tanpa membebani server secara signifikan.

3.2.3 Perbandingan Proses Manual dan Sistem

Sebelum adanya sistem dashboard, proses monitoring dilakukan secara manual dengan karakteristik yang ditampilkan pada tabel 3.

Tabel 3. Perbandingan Proses manual dan Sistem

Aspek	Manual	Sistem Dashboard
Waktu analisis	1–3 jam per domain	< 10 detik per batch
Sumber data	Tidak terpusat	Terpusat
Risiko human error	Tinggi	Rendah
Deteksi anomali	Lambat	Real-time
Pelaporan	Manual	Otomatis

Berdasarkan perbandingan tersebut: Sistem mampu mengurangi waktu analisis hingga lebih dari 90%, mengurangi potensi kesalahan manusia (*human error*), meningkatkan kecepatan respons terhadap insiden keamanan

3.2.4 Analisis Efektivitas Sistem dalam Mendukung Keamanan Siber

Dengan adanya sistem dashboard: Proses identifikasi backlink berbahaya menjadi lebih cepat dan terstruktur, Distribusi tugas ke PIC unit menjadi otomatis melalui mekanisme mapping domain, dan Monitoring status penanganan dapat dilakukan secara real-time

Selain itu, pendekatan rule-based detection berbasis skor toksisitas terbukti efektif dalam mengidentifikasi ancaman awal (*early warning system*), meskipun belum mencakup analisis lanjutan seperti perilaku malware atau analisis jaringan.

4. Kesimpulan

Aplikasi dashboard dapat menganalisis keamanan siber Universitas Terbuka dalam hal backlink konten negatif dari semrush.com. Secara keseluruhan, aplikasi dashboard telah layak digunakan karena seluruh fungsi inti berjalan dengan baik berdasarkan 20 sampel pengujian. Masukan yang muncul lebih banyak terkait peningkatan fitur, bukan error, sehingga aplikasi sudah stabil namun perlu peningkatan untuk mendukung kebutuhan operasional secara komprehensif. Belum terlihat dampak pemeringkatan Webometrics karena penilaian belum dilakukan oleh pihah terkait. Meskipun demikian, penelitian ini memiliki beberapa keterbatasan.

Sistem masih bergantung pada data eksternal dari Semrush sehingga kualitas monitoring dipengaruhi oleh hasil scanning pihak ketiga. Selain itu, sistem belum mendukung proses scanning internal secara real-time terhadap file atau direktori domain, sehingga potensi ancaman berbasis perubahan lokal belum sepenuhnya terdeteksi secara langsung. Untuk pengembangan selanjutnya, penelitian ini membuka peluang penerapan metode yang lebih cerdas, seperti penggunaan teknik berbasis kecerdasan buatan (AI-based detection) untuk meningkatkan akurasi deteksi konten berbahaya, serta implementasi mekanisme anomaly detection untuk mengidentifikasi pola serangan yang tidak biasa secara otomatis. Pengembangan ini diharapkan dapat meningkatkan

Submitted : 06-03-2026 | Reviewed : 17-04-2026 | Accepted : 26-04-2026

kemampuan sistem dalam mendeteksi ancaman secara proaktif dan adaptif di masa mendatang.

Daftar Rujukan

[1] Aguillo, I. F., Ortega, J. L., & Fernández, M. (2008). Webometric Ranking of World Introduction, Methodology, Developments. Higher Education in Europe, 33(2/3), 234–244. and Future

[2] Aguillo, I. F., Ortega, J. L., Fernández, M., & Utrilla, A. M. (2010). Indicators for a webometric ranking of open access repositories. Scientometrics, 82(3), 477–486.

[3] Aguillo, I. F., Bar-Ilan, J., Levene, M., & Ortega, J. L. (2010). Comparing university rankings. Scientometrics, 85, 243–256

[4] Ajani, Y., Enakrire, R., Fagbola, O., & Bashorun, M. (2024). Overcoming deep web challenges: sustainable solutions for digital age information seekers. Business Information Review, 41(2), 53-58. https://doi.org/10.1177/02663821241245513

[5] Batubara, A., Purwaningtyas, F., & Putri, R. (2023). University webometrics ranking analysis using swot and gap analysis. Khizanah Al-Hikmah Jurnal Ilmu Perpustakaan Informasi Dan Kearsipan, 11(2), 164-173. https://doi.org/10.24252/kah.v11i2a2

[6] Brown, C., Revette, A., Ferranti, S., Fontenot, H., & Gooding, H. (2021). Conducting web- based focus groups with adolescents and young adults. International Journal of Qualitative Methods, 20. https://doi.org/10.1177/1609406921996872

[7] Das, S., Balasubramanian, P., & Chowdhury, A. (2019). Webometrics ranking (wr) of world universities and national institutional ranking framework (nirf): a comparative study. Srels Journal of Information Management, 154-158. https://doi.org/10.17821/srels/2019/v56i3/144386

[8] Deng, S., Wang, F., Wang, H., & Cai, Y. (2024). Recognizing implicitly toxic content based on multiple attention mechanisms. Proceedings of the Association for Information Science and Technology, 61(1), 880-882. https://doi.org/10.1002/pra2.1127

[9] Fan, L. (2024). Artificial intelligence ethics: a dialogue between technological advances and human values. International Journal of Education and Humanities, 14(2), 260-265. https://doi.org/10.54097/tvqkkf40

[10] Farashi, S. and Bashirian, S. (2021). A complementary webometric ranking system based on

[11] the website quality and traffic measures: a study focusing on top-ranked world universities. Education for Information, 37(3), 337-354. https://doi.org/10.3233/efi-200422

[12] Fauzi, M., Rahamaddulla, S., Lee, C., Ali, Z., & Alias, U. (2024). Work pressure in higher education: a state of the art bibliometric analysis on academic work–life balance.

[13] International Journal of Workplace Health Management, 17(2), 175-195. https://doi.org/10.1108/ijwhm-01-2023-0002

[14] Islam, M. (2024). Are faculty members aware of global university ranking? a study in the context of a developing country. Digital Library Perspectives, 40(4), 649-667. https://doi.org/10.1108/dlp-01-2024-0005

[15] Jayaningsih, A., Sudiatmika, I., & Wulandari, R. (2022). Public perception of itb stikom bali kampus jimbaran's brand image., 69-73. https://doi.org/10.2991/978-2-494069-77-0_11 Junusi, R. and Musahadi, M. (2021). Impact of the islamic higher education quality improvement project.. https://doi.org/10.4108/eai.14-10-2020.2303827

[16] Koulas, E., Anthopoulos, M., Grammenou, S., Kaimakamis, C., Kousaris, K., Panavou, F.,

[17] … & Peristeras, V. (2021). Misinformation and its stakeholders in europe: a web-based analysis., 575-594. https://doi.org/10.1007/978-3-030-80129-8_41

[18] Lazar, A., Repanovici, A., Popa, D., Ionaș, D., & Dobrescu, A. (2024). Ethical principles in ai use for assessment: exploring students' perspectives on ethical principles in academic publishing. Education Sciences, 14(11), 1239. https://doi.org/10.3390/educsci14111239

[19] Li, H. and Yin, Z. (2022). Influence of publication on university ranking: citation, collaboration, and level of interdisciplinary research. Journal of Librarianship and Information Science, 55(3), 828-835. https://doi.org/10.1177/09610006221106178 Matkivskyi, M. and Taras, T. (2024). Methods and technologies for evaluating the quality of higher education in the context of international standards: a comparison of the ukrainian and polish experience of creating ratings. Scientific Bulletin of Mukachevo State University

[20] Series "Pedagogy and Psychology", 10(1), 116-127. https://doi.org/10.52534/msu- pp1.2024.116

[21] Morley, J., Kinsey, L., Elhalal, A., Garcia, F., Ziosi, M., & Floridi, L. (2021). Operationalising ai ethics: barriers, enablers and next steps. Ai & Society, 38(1), 411-423. https://doi.org/10.1007/s00146-021-01308-8

[22] Polyakov, M., Bilozubenko, V., Korneyev, M., & Nebaba, N. (2020). Analysis of key

[23] university leadership factors based on their international rankings (qs world university

[24] rankings and times higher education). Problems and Perspectives in Management, 18(4), 142-152. https://doi.org/10.21511/ppm.18(4).2020.13

[25] Puzatykh, A. (2021). Webometrics ranking and regional universities: analysing results of bunin yelets state university.. https://doi.org/10.15405/epsbs.2021.12.95

[26] Razak, S., Mohamed, S., Ismail, A., & Ramzi, N. (2019). An assessment of the web presence of top 10 university in southeast asia. International Journal of Innovative Technology and Exploring Engineering, 8(9), 3316-3319. https://doi.org/10.35940/ijitee.i8746.078919 Ristono, A., Lucitasari, D., Astanti, Y., Rahmawati, B., & Kasih, P. (2021). Mti website quality improvement as a strategy to increase webometric ranking. RSF Conference Series Business Management and Social Sciences, 1(3), 390-401. https://doi.org/10.31098/bmss.v1i3.352

[27] Shahruddin, S., Wan-Chik, R., & Malik, I. (2019). Visibility study in strategizing for web marketing and webometric university ranking in malaysia. Journal of

[28] Physics Conference Series, 1193, 012002. https://doi.org/10.1088/1742-6596/1193/1/012002

[29] Thuranira, S. and Diki, P. (2024). Webometrics ranking of universities: fallacy or reality. African Journal of Science Technology and Social Sciences, 2(2), 24-31. https://doi.org/10.58506/ajstss.v2i2.213

[30] Vállez, M. and Ventura, A. (2020). Analysis of the seo visibility of university libraries and how they impact the web visibility of their universities. The Journal of Academic Librarianship, 46(4), 102171. https://doi.org/10.1016/j.acalib.2020.102171

[31] Vállez, M., Lopezosa, C., & Pedraza-Jiménez, R. (2022). A study of the web visibility of the sdgs and the 2030 agenda on university websites. International Journal of Sustainability in Higher Education, 23(8), 41-59. https://doi.org/10.1108/ijshe-09-2021-0361

[32] Weidener, L. and Fischer, M. (2024). Role of ethics in developing ai-based applications in medicine: insights from expert interviews and discussion of implications. Jmir Ai, 3, e51204. https://doi.org/10.2196/51204

[33] Wibowo, P. (2022). Evaluasi penerapan search engine optimization (seo) website untuk meningkatkan indikator visibility webometrics universitas "xyz". Libraria Jurnal Perpustakaan, 10(1), 93. https://doi.org/10.21043/libraria.v10i1.13916

[34] Wong, K. and Ginkel, S. (2021). Virtual media quality index (w-index) for higher institutions of education. Journal of Modern Mechanical Engineering and Technology, 2(1), 11-15. https://doi.org/10.15377/2409-9848.2015.02.01.2

[35] Yakymenko, I., Kazymyr, V., & Lytvyn, S. (2020). Webometrics ranking analysis and possible ways to improve the position of the university., 422-426. https://doi.org/10.1109/dessert50317.2020.9124999

Submitted : 06-03-2026 | Reviewed : 17-04-2026 | Accepted : 26-04-2026