TUGAS AKHIR

ANALISIS KEAMANAN WEBSITE EJOURNAL.UIN-SUKA.AC.ID TERHADAP SERANGAN PASSWORD RESET POISONING MELALUI TEKNIK HOST HEADER INJECTION

Untuk Memenuhi Sebagian Persyaratan Mencapai Derajat Sarjana S-1 Program Studi Informatika

Disusun Oleh :

OCTOVIAN AURORA PARIKESIT

NIM. 21106050076

PROGRAM STUDI INFORMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA

YOGYAKARTA

2024

HALAMAN PENGESAHAN

KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA
FAKULTAS SAINS DAN TEKNOLOGI
Jl. Marsda Adisucipto Telp. (0274) 540971 Fax. (0274) 519739 Yogyakarta 55281

PENGESAHAN TUGAS AKHIR

Nomor : B-759/Un.02/DST/PP.00.9/05/2025

Tugas Akhir dengan judul : ANALISIS KEAMANAN WEBSITE EJOURNAL.UIN-SUKA.AC.ID TERHADAP SERANGAN PASSWORD RESET POISONING MELALUI TEKNIK HOST HEADER INJECTION

yang dipersiapkan dan disusun oleh:

Nama : OCTOVIAN AURORA PARIKESIT
Nomor Induk Mahasiswa : 21106050076
Telah diujikan pada : Jumat, 02 Mei 2025
Nilai ujian Tugas Akhir : A-

dinyatakan telah diterima oleh Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta

TIM UJIAN TUGAS AKHIR

Ketua Sidang

Dr. Ir. Bambang Sugiantoro, M.T., IPU., ASEAN Eng.
SIGNED

Valid ID: 682449da9fedf

Penguji I

Ir. Muhammad Didik Rohmad Wahyudi, S.T., M.T.
SIGNED

Valid ID: 68243552776c1

Penguji II

Eko Hadi Gunawan, M.Eng.
SIGNED

Valid ID: 68242e1721b52

Yogyakarta, 02 Mei 2025
UIN Sunan Kalijaga
Dekan Fakultas Sains dan Teknologi

Prof. Dr. Dra. Hj. Khurul Wardati, M.Si.
SIGNED

Valid ID: 6826ef7c5bc0a

PERNYATAAN KEASLIAN SKRIPSI

SURAT PERNYATAAN KEASLIAN SKRIPSI

Yang bertanda tangan di bawah ini:

Nama	: Octovian Aurora Parikesit
NIM	: 21106050076
Program Studi	: Informatika
Fakultas	: Sains dan Teknologi

Dengan ini menyatakan bahwa isi skripsi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar sarjana di suatu Perguruan Tinggi dan sesungguhnya skripsi ini merupakan hasil pekerjaan penulis sendiri sepanjang pengetahuan penulis, bukan duplikasi atau saduran dari karya orang lain kecuali bagian tertentu yang penulis ambil sebagai bahan acuan. Apabila terbukti pernyataan ini tidak benar, sepenuhnya menjadi tanggung jawab penulis.

Yogyakarta, 16 April 2025

Octovian Aurora Parikesit
NIM 21106050076

SURAT PERSETUJUAN SKRIPSI / TUGAS AKHIR

KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA
FAKULTAS SAINS DAN TEKNOLOGI
Jl. Marsda Adisucipto Telp. (0274) 515856 Yogyakarta 55281

SURAT PERSETUJUAN SKRIPSI

Hal : Persetujuan Skripsi / Tugas Akhir
Lamp :

Kepada:
Yth. Dekan Fakultas Sains dan Teknologi
UIN Sunan Kalijaga Yogyakarta
Di Yogyakarta

Assalamu'alaikum wr.wb.

Setelah membaca, meneliti, memberikan petunjuk dan mengoreksi serta mengadakan perbaikan seperlunya, maka saya selaku pembimbing berpendapat bahwa skripsi Saudara:

Nama : Octovian Aurora Parikesit
NIM : 21106050076
Judul Skripsi : ANALISIS KEAMANAN WEBSITE EJOURNAL.UIN-SUKA.AC.ID TERHADAP SERANGAN PASSWORD RESET POISONING MELALUI TEKNIK HOST HEADER INJECTION

Sudah dapat diajukan kepada Program Studi Informatika Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta sebagai salah satu syarat untuk memperoleh gelar Sarjana Strata Satu dalam Program Studi Informatika.

Dengan ini saya mengharap agar skripsi tersebut di atas dapat segera dimunaqosyahkan. Atas perhatiannya saya ucapkan terimakasih.

Wassalamu'alaikum wr.wb.

Yogyakarta, 16 April 2025
Pembimbing,

Dr. Ir. Bambang Sugiantoro, M.T., IPU., ASEAN Eng.
NIP 19751024 200912 1 002

MOTTO

“Demi masa. Sesungguhnya manusia itu benar-benar dalam kerugian, kecuali orang-orang yang beriman dan mengerjakan amal saleh dan nasehat menasehati supaya mentaati kebenaran dan nasehat menasehati supaya menetapi kesabaran.”

QS. Al-‘Ashr: 1-3

“Sesungguhnya **bersama** kesulitan ada kemudahan. Maka apabila engkau telah selesai (dari suatu urusan), tetaplah bekerja keras (untuk urusan yang lain), dan hanya kepada Tuhanmu lah engkau berharap”

Q.S. Al-Insyirah : 6-8

"Allah mengabulkan doa-doa ketika kita sudah siap, bukan ketika kita menginginkannya"

KH. Ahmad Bahauddin Nursalim

HALAMAN PERSEMBAHAN

Bismillahirrahmaanirrahiim, dengan rahmat Allah Yang Maha Pengasih lagi Maha Penyayang, penulis mempersembahkan skripsi ini sebagai ungkapan rasa syukur dan terima kasih kepada:

1. Orang tua yang senantiasa menjadi sumber ilmu, kasih sayang, serta tempat berbagi dalam setiap perjalanan kehidupan. Terima kasih atas segala nasihat, doa, serta dukungan tanpa henti yang selalu menguatkan dan mengajarkan arti ketulusan serta keyakinan dalam setiap usaha. Semoga Allah SWT senantiasa memberikan kesehatan dan kebahagiaan untuk menemani anak-anakmu dalam meraih kesuksesan di masa depan.
2. Kakek dan nenek tercinta yang selalu menjadi penyemangat dalam penyelesaian skripsi ini.
3. Kakak tercinta Dhita Elsha Pangestika yang selalu memberikan kasih sayang, dukungan, serta keyakinan bahwa setiap tantangan dapat dihadapi dengan penuh semangat dan keteguhan hati.
4. Nazura Atikafani yang selalu memberikan semangat dan dukungannya, serta selalu menemani penulis dalam penyusunan skripsi ini.

LEMBAR PEDOMAN PENGGUNAAN TUGAS AKHIR

Tugas Akhir ini tidak dipublikasikan, tetapi tersedia di perpustakaan dalam lingkungan UIN Sunan Kalijaga, yang diperkenankan dipakai sebagai referensi kepustakaan, tetapi pengutipan harus seizin penyusun, dan harus menyebutkan sumbernya sesuai dengan kebiasaan ilmiah. Dokumen Tugas Akhir ini merupakan hak milik UIN Sunan Kalijaga Yogyakarta

INTISARI

Keamanan sistem informasi penting untuk menjaga integritas dan kepercayaan pengguna, terutama pada platform publikasi ilmiah seperti ejournal.uin-suka.ac.id. Salah satu ancaman yang perlu diwaspadai adalah serangan terhadap mekanisme reset password yang dapat dimanfaatkan untuk pengambilalihan akun.

Penelitian ini menggunakan metode penetration testing berdasarkan NIST SP 800-115, dengan fokus pada serangan Password Reset Poisoning melalui teknik Host Header Injection. Selain itu, pengujian sekunder dilakukan menggunakan Nessus untuk mendeteksi kelemahan tambahan.

Hasil pengujian menunjukkan bahwa sistem tidak memvalidasi header X-Forwarded-Host, memungkinkan manipulasi tautan reset password. Sistem juga tidak menerapkan rate limiting, sehingga rawan diserang secara massal. Mitigasi yang disarankan meliputi validasi header, allowlist domain, dan pembatasan permintaan reset.

Kata Kunci: Password Reset Poisoning, Host Header Injection, Rate Limiting, Penetration Test, NIST SP 800-115

ABSTRACT

Information system security is crucial to maintaining the integrity and trust of users, especially on scientific publication platforms like ejournal.uin-suka.ac.id. One potential threat is attacks on the password reset mechanism, which can lead to account takeover.

This research applies penetration testing based on the NIST SP 800-115 framework, focusing on Password Reset Poisoning via Host Header Injection. Additional vulnerability scanning was conducted using Nessus to identify other weaknesses.

The results show that the system does not validate the X-Forwarded-Host header, allowing attackers to manipulate password reset links. Furthermore, the absence of rate limiting exposes the system to mass reset requests. Recommended mitigations include strict header validation, domain allowlisting, and implementing rate-limiting mechanisms.

Keywords: Password Reset Poisoning, Host Header Injection, Rate Limiting, Penetration Test, NIST SP 800-115

KATA PENGANTAR

Alhamdulillahirabbil'alamin, penulis panjatkan puja dan puji syukur ke hadirat Allah SWT yang telah memberikan rahmat dan hidayah-Nya, sehingga penulis dapat menyelesaikan skripsi yang berjudul *"Analisis Keamanan Website ejournal.uin-suka.ac.id terhadap Serangan Password Reset Poisoning melalui Teknik Host Header Injection"*. Shalawat serta salam tak lupa penulis curahkan kepada junjungan kita, Nabi Muhammad SAW, yang telah menjadi teladan terbaik bagi umat manusia. Skripsi ini dibuat untuk memenuhi tugas akhir perkuliahan sebagai salah satu syarat memperoleh gelar Sarjana Strata 1 di Program Studi Informatika UIN Sunan Kalijaga Yogyakarta.

Pada kesempatan ini, penulis ingin menyampaikan banyak terima kasih kepada berbagai pihak yang telah memberikan bantuan, bimbingan, dukungan, serta motivasi sehingga penulis dapat menyelesaikan tugas akhir ini, di antaranya:

1. Prof. Noorhaidi, M.A, M.Phil., Ph.D**.,** selaku Rektor UIN Sunan Kalijaga Yogyakarta.
2. Prof. Dr. Dra. Hj. Khurul Wardati, M.Si., selaku Dekan Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta.
3. Dr. Muhammad Mustakim, S.T. M.T., selaku Ketua Program Studi Informatika UIN Sunan Kalijaga Yogyakarta.
4. Dr. Ir. Bambang Sugiantoro, M.T., IPU., ASEAN Eng., selaku Dosen Pembimbing yang telah memberikan bimbingan dan motivasi dalam penyusunan skripsi ini.
5. Bapak Eko Hadi Gunawan, M.Eng., selaku Dosen Pembimbing Akademik yang telah memberikan bimbingan , semangat, dan motivasi dalam penyusunan skripsi ini.
6. Kedua orang tua penulis atas doa, kasih sayang, serta dukungan moral dan materi yang tiada henti kepada penulis.

7. Kakak penulis Dhita Elsha Pangestika, atas dukungan dan motivasi yang selalu diberikan kepada penulis.
8. Nazura Atikafani, atas dukungan, semangat, dan motivasi yang selalu diberikan kepada penulis.
9. Sahabat penulis ”merkurius”, atas dukungan dan semangat yang selalu diberikan kepada penulis.
10. Seluruh pihak yang bersangkutan yang telah memberikan bimbingan, arahan, semangat dan motivasi kepada penulis.

Akhir kata, penulis berharap bahwa skripsi ini dapat bermanfaat bagi penulis sendiri maupun bagi pembaca pada umumnya. Penulis juga menyadari bahwa skripsi ini masih memiliki kekurangan, oleh karena itu, kritik dan saran yang membangun sangat diharapkan demi penyempurnaan di masa mendatang.

Yogyakarta, April 2025

Penulis

Octovian Aurora Parikesit

DAFTAR ISI

DAFTAR TABEL

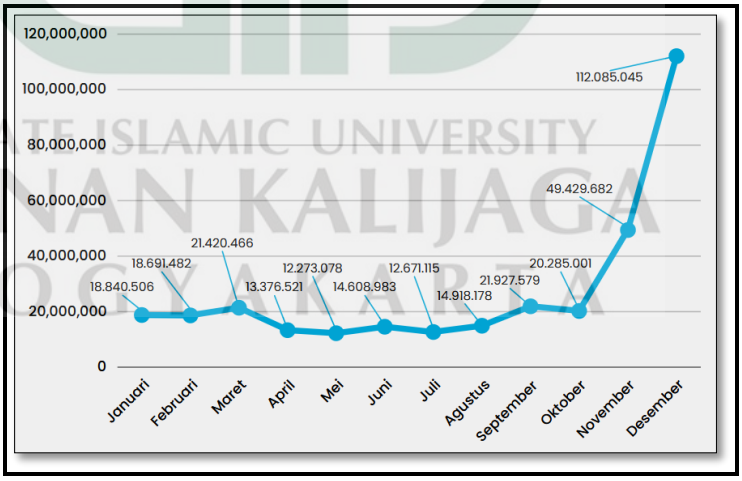
DAFTAR GAMBAR

BAB I

PENDAHULUAN

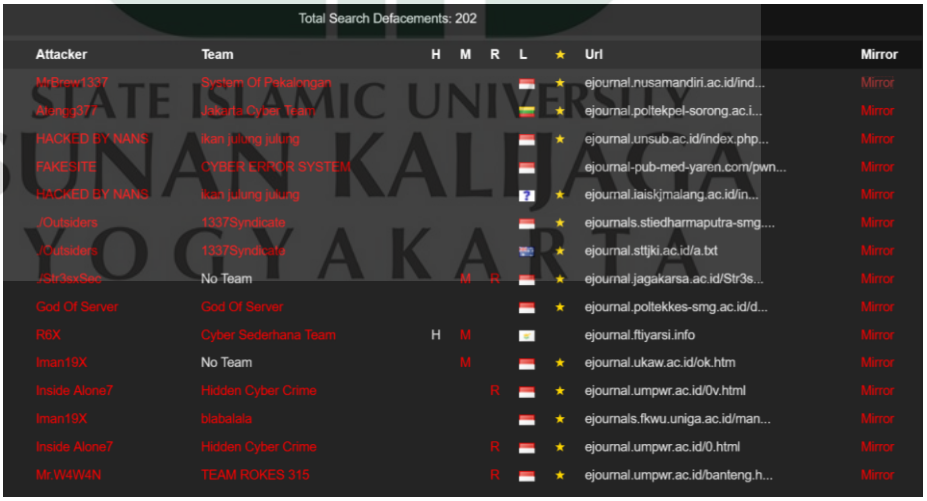
1.1 Latar Belakang

Website telah menjadi media utama bagi institusi pendidikan, termasuk dalam menyampaikan informasi kepada berbagai pemangku kepentingan. Pembelajaran berbasis web memiliki peran penting dalam pendidikan karena dapat meningkatkan interaktivitas, fleksibilitas, serta efektivitas dalam proses belajar mengajar. Dengan perkembangan teknologi, pembelajaran jarak jauh menjadi lebih mudah diakses, memungkinkan mahasiswa untuk belajar di mana saja dan kapan saja. Website mendukung berbagai aktivitas akademik dan administratif dengan menyediakan data serta fitur layanan yang memudahkan interaksi antara mahasiswa, dosen, dan pengelola kampus. Salah satu aplikasi yang penting adalah sistem e-journal, yang memungkinkan mahasiswa dan dosen untuk mengakses serta mengelola publikasi akademik. Website ejournal.uin-suka.ac.id di Universitas Islam Negeri Sunan Kalijaga Yogyakarta menjadi salah satu portal penting dalam mendukung kegiatan pendidikan dan penelitian. Namun, dengan meningkatnya ketergantungan pada website, muncul juga potensi ancaman terhadap keamanan siber, yang dapat merusak integritas data serta sistem yang digunakan[1].



Gambar 1. 1Total Trafik Anomali (Sumber: Id-SIRTII/CC)

Dalam beberapa tahun terakhir, peningkatan insiden serangan siber di Indonesia menunjukkan tren yang mengkhawatirkan. Sepanjang tahun 2024, total trafik anomali yang terdeteksi oleh Badan Siber dan Sandi Negara (BSSN) mencapai 330.527.636 anomali. Anomali tertinggi terjadi pada bulan Desember dengan jumlah 112.085.045 anomali, sedangkan anomali terendah terjadi pada bulan Mei dengan jumlah 12.273.078 anomali. Aktivitas anomali ini dapat berdampak pada penurunan performa perangkat dan jaringan, pencurian data sensitif, hingga perusakan reputasi dan penurunan kepercayaan terhadap suatu organisasi. Berbagai sektor, baik pemerintah maupun swasta, turut menjadi sasaran serangan siber yang signifikan sepanjang tahun[2]. Beberapa kasus besar yang terjadi meliputi pencurian data pelanggan PT Kereta Api Indonesia (KAI), serangan *insider threat* terhadap Biznet, serta *ransomware* yang melumpuhkan Pusat Data Nasional (PDN). Selain itu, data pegawai negeri sipil dari Badan Kepegawaian Negara (BKN) bocor di forum peretas, sementara Indodax mengalami kerugian besar akibat peretasan, dan data Nomor Pokok Wajib Pajak (NPWP) Direktorat Jenderal Pajak turut beredar di pasar gelap[3]. Beberapa insiden serangan siber ini menunjukkan bahwa keamanan sistem digital masih menjadi tantangan besar, termasuk bagi platform akademik seperti ejournal.uin-suka.ac.id yang menjadi fokus penelitian ini.



Gambar 1. 2 Zone-Xsec

Meskipun data dari BSSN belum secara spesifik mengklasifikasikan sektor pendidikan, indikasi bahwa platform akademik turut menjadi sasaran serangan dapat dilihat melalui situs pelaporan insiden Zone-Xsec. Hingga awal tahun 2025, tercatat sebanyak 202 kasus defacement yang menargetkan berbagai subdomain *e-journal* milik sejumlah perguruan tinggi di Indonesia[4].

Date	Notifier	H	M	R	L	Domain
2023/04/11	Moroccan Revolution			R		ejournal.uin-suka.ac.id/
2021/08/10	MiSh			R		ejournal.uin-suka.ac.id/
2020/06/23	KingSkrupellos			R		ejournal.uin-suka.ac.id/
2017/05/26	Mr E[R]					ejournal.uin-suka.ac.id/

Gambar 1. 3 Insiden Serangan ejournal.uin-suka.ac.id pada Zone-H

Lebih lanjut, situs pelaporan insiden keamanan siber seperti Zone-H mencatat bahwa subdomain pada *ejournal.uin-suka.ac.id* telah menjadi target defacement secara berulang dalam berberapa tahun terakhir[5]. Sebagian besar insiden yang tercatat diklasifikasikan sebagai *reliable*, yang menunjukkan bahwa bukti serangan telah tervalidasi oleh pihak Zone-H. Pola serangan yang berulang terhadap sistem ini mengindikasikan adanya celah keamanan yang belum sepenuhnya ditangani, termasuk potensi kerentanan pada komponen penting seperti mekanisme pemulihan akun melalui reset password. Jenis serangan ini umumnya terjadi ketika penyerang berhasil mendapatkan akses tidak sah ke akun administrator, yang salah satunya dapat dilakukan melalui teknik pengambilalihan akun seperti Password Reset Poisoning. Temuan ini memperkuat bahwa sistem publikasi akademik pun menghadapi ancaman nyata dalam konteks keamanan siber.

Sejalan dengan itu, serangan terhadap mekanisme reset password mengalami peningkatan signifikan dalam beberapa tahun terakhir, yang sebagian besar dipicu oleh penggunaan bot atau automation[6]. Meningkatnya volume serangan berbasis reset password ini, termasuk serangan Password Reset Poisoning, memperlihatkan betapa rentannya sistem yang masih bergantung pada otentikasi berbasis password tradisional[7]. Serangan Password Reset Poisoning terjadi ketika penyerang mengeksploitasi celah dalam validasi header HTTP, seperti header Host, pada tautan reset kata sandi. Jika sistem tidak melakukan validasi dengan benar, penyerang dapat

mengalihkan tautan tersebut ke domain milik mereka dan mengganti kata sandi korban tanpa izin. Risiko terhadap serangan semacam ini terus meningkat karena mekanisme reset password masih menjadi metode utama dalam pemulihan akun, sementara teknologi keamanan alternatif seperti biometrik belum sepenuhnya diadopsi. Tanpa mekanisme validasi yang memadai, celah ini dapat digunakan oleh penyerang untuk mengambil alih akun dan mengakses data sensitif, yang berdampak serius terhadap integritas dan privasi pengguna.

Berdasarkan latar belakang tersebut, penelitian ini disusun dengan judul "Analisis Keamanan Website ejournal.uin-suka.ac.id terhadap Serangan Password Reset Poisoning melalui Teknik Host Header Injection". Tujuan dari penelitian ini adalah untuk mengidentifikasi serta menganalisis kerentanan terkait dengan serangan password reset poisoning melalui Host Header Injection. Hasil dari penelitian ini diharapkan dapat membantu kewaspadaan kepada pengelola website mengenai potensi kelemahan dalam mekanisme reset kata sandi dan untuk memberikan rekomendasi terkait implementasi praktik keamanan terbaik guna mengurangi risiko serangan siber terhadap website kampus. Dengan demikian, studi ini dapat berkontribusi dalam menjaga integritas dan keamanan data pengguna serta mendukung lingkungan digital yang lebih aman bagi komunitas akademik.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, permasalahan yang akan dijadikan objek dalam penelitian ini adalah sebagai berikut:

1. Berapa nilai CVSS dari kerentanan Password Reset Poisoning melalui teknik Host Header Injection pada website ejournal.uin-suka.ac.id, apa saja faktor eksploitasi yang berkontribusi terhadap kerentanan tersebut, dan bagaimana dampaknya terhadap sistem?

1.3 Batasan Masalah

Batasan masalah dalam penelitian ini dibatasi dengan ruang lingkup sebagai berikut:

1. Penelitian ini akan menganalisis kerentanan Password Reset Poisoning pada website ejournal.uin-suka.ac.id, khususnya terkait dengan eksploitasi melalui Host Header Injection yang dapat memanipulasi mekanisme reset kata sandi, dengan fokus pada dampak serangan yang dapat membahayakan integritas akun pengguna.
2. Penelitian ini akan difokuskan pada subdomain atau bagian spesifik dari website ejournal.uin-suka.ac.id, yaitu ejournal.uin-suka.ac.id/saintek, dan tidak mencakup analisis terhadap sistem lain yang berada dalam domain utama ejournal.uin-suka.ac.id.
3. Penelitian ini hanya akan memberikan rekomendasi penanganan untuk mengatasi kerentanan Password Reset Poisoning pada website ejournal.uin-suka.ac.id, dengan merujuk pada literatur terkait yang membahas perbaikan mekanisme validasi Host Header.
4. Analisis tidak mencakup dampak sosial atau hukum dari insiden peretasan atau kebocoran data akibat serangan ini, tetapi hanya fokus pada solusi teknis untuk meningkatkan keamanan aplikasi web yang rentan terhadap Host Header Injection.
5. Penelitian ini hanya akan menganalisis tingkat kerentanan Password Reset Poisoning pada website ejournal.uin-suka.ac.id menggunakan metode perhitungan skor kerentanan berdasarkan Base Score Common Vulnerability Scoring System (CVSS) versi 3, untuk menilai tingkat keparahan celah keamanan yang ditemukan.

1.4 Tujuan Penulisan

Tujuan dari proyek Analisis Keamanan Website ejournal.uin-suka.ac.id terhadap Serangan Password Reset Poisoning Menggunakan Host Header Injection adalah sebagai berikut:

1. Menilai kerentanan website ejournal.uin-suka.ac.id terhadap Password Reset Poisoning melalui Host Header Injection menggunakan CVSS, serta mengidentifikasi faktor eksploitasi dan mengevaluasi dampaknya terhadap sistem.

1.5 Manfaat Penulisan

Adanya beberapa manfaat yang dapat diambil dari proyek yang dibuat sebagai berikut:

1. Bagi institusi pendidikan, penelitian ini dapat membantu mengidentifikasi kerentanan Password Reset Poisoning pada website ejournal.uin-suka.ac.id, khususnya terkait dengan eksploitasi melalui Host Header Injection. Dengan memahami celah keamanan ini, institusi dapat menerapkan solusi mitigasi yang efektif untuk mencegah penyalahgunaan mekanisme reset kata sandi, sehingga mengurangi risiko serangan serupa di masa depan.
2. Bagi pengembang dan administrator sistem, penelitian ini memberikan wawasan tentang teknik-teknik identifikasi dan perbaikan kerentanan Password Reset Poisoning, serta cara-cara untuk meningkatkan mekanisme validasi Host Header dan langkah-langkah keamanan aplikasi web lainnya.
3. Rekomendasi penanganan yang diberikan dapat membantu pengembang dalam memperkuat sistem keamanan dan mencegah potensi eksploitasi serupa di aplikasi web lainnya.
4. Bagi komunitas keamanan siber, penelitian ini menyediakan referensi studi kasus yang berharga mengenai eksploitasi Password Reset Poisoning melalui Host Header Injection, serta langkah mitigasi yang dapat diterapkan dalam meningkatkan keamanan aplikasi web secara lebih efektif. Pengetahuan yang diperoleh dapat memperkaya pemahaman komunitas tentang langkah-langkah praktis untuk mencegah dan menangani celah keamanan yang terkait dengan mekanisme reset kata sandi.

BAB V
PENUTUP

5.1 Kesimpulan

Penelitian ini bertujuan untuk menilai kerentanan *website* ejournal.uin-suka.ac.id terhadap serangan Password Reset Poisoning melalui teknik Host Header Injection, serta mengevaluasi dampak dan faktor eksploitasi yang berkontribusi terhadap kerentanan tersebut. Berdasarkan hasil pengujian, ditemukan bahwa sistem tidak melakukan validasi terhadap nilai X-Forwarded-Host yang dikirim oleh klien. Nilai tersebut digunakan secara langsung untuk membentuk tautan reset password yang dikirim ke email pengguna tanpa proses sanitasi atau perlindungan tambahan seperti domain allowlist. Hal ini memungkinkan penyerang untuk menyisipkan tautan ke domain berbahaya yang mereka kontrol.

Analisis menggunakan CVSS v3 menunjukkan bahwa kerentanan Password Reset Poisoning ini memiliki skor keparahan 7.5 (High) karena berdampak serius terhadap integritas sistem. Selain itu, ditemukan pula kelemahan *No Rate Limiting* pada *endpoint* reset *password* yang memungkinkan pengiriman permintaan secara massal tanpa batasan, yang meningkatkan risiko penyalahgunaan dan gangguan terhadap server.

Adapun faktor-faktor eksploitasi yang berkontribusi terhadap kerentanan ini adalah:

- Tidak adanya validasi terhadap header X-Forwarded-Host,
- Penggunaan langsung header tersebut dalam tautan reset password tanpa sanitasi,
- Ketiadaan domain allowlist atau token verifikasi berbasis domain,
- Tidak diterapkannya batasan jumlah permintaan reset dalam periode tertentu, serta
- Ketiadaan mekanisme CAPTCHA, delay, atau throttling.

Dampak dari Password Reset Poisoning mencakup pengalihan proses reset ke domain eksternal, potensi penyalahgunaan layanan, dan gangguan terhadap integritas sistem. Sedangkan dampak dari No Rate Limiting meliputi lonjakan trafik reset, beban berlebih pada server, serta gangguan ketersediaan layanan (DoS).

5.2 Saran

Berdasarkan hasil penelitian, terdapat beberapa langkah yang dapat dilakukan untuk meningkatkan keamanan sistem, antara lain:

1. Mengimplementasikan validasi ketat pada Host Header untuk memastikan hanya domain yang sah yang digunakan dalam proses reset password.
2. Menambahkan allowlist domain guna membatasi tautan reset hanya dikirim ke domain yang telah ditentukan oleh administrator sistem.
3. Menerapkan rate limiting pada fitur reset password untuk mencegah penyalahgunaan akibat serangan otomatisasi.
4. Menggunakan CAPTCHA atau OTP sebagai metode verifikasi tambahan agar hanya pengguna sah yang dapat melakukan reset password.
5. Melakukan pengujian keamanan secara berkala, termasuk uji penetrasi dan analisis kerentanan, untuk mendeteksi serta mengatasi kelemahan baru sebelum dapat dieksploitasi oleh penyerang.

Dengan penerapan langkah-langkah di atas, diharapkan website ejournal.uin-suka.ac.id dapat lebih terlindungi dari serangan Password Reset Poisoning serta meningkatkan keamanan dan keandalan sistem dalam melindungi data penggunanya.

DAFTAR PUSTAKA

[1] I. Suharjo and P. W. Setyaningsih, "Identifikasi Dan Analisis Terjadinya Peretasan Pada Domain Website dari Data Google Cache," 2024.

[2] Id-SIRTII/CC, "LANSKAP KEAMANAN SIBER INDONESIA 2024", [Online]. Available: https://www.bssn.go.id/wp-content/uploads/2025/02/LANSKAP-KEAMANAN-SIBER-2024-1.pdf

[3] Dani Aswara, "6 Serangan Siber Besar di Indonesia," Kaleidoskop 2024: 6 Serangan Siber Besar di Indonesia. Accessed: Feb. 12, 2025. [Online]. Available: https://www.tempo.co/hukum/kaleidoskop-2024-6-serangan-siber-besar-di-indonesia-1188275

[4] Zone-Xsec, Accessed: Feb. 05, 2025. [Online]. Available: https://zone-xsec.com/search/q=ejournal

[5] zone-h.org, [Online]. Available: https://www.zone-h.org/archive/filter=1/fulltext=1/domain=ejournal.uin-suka.ac.id

[6] Stephen Pritchard, "Rapid Growth of Password Reset Attacks Boosts Fraud and Account Takeovers." Accessed: Feb. 05, 2024. [Online]. Available: https://www.infosecurity-magazine.com/news/password-reset-attacks-fraud/

[7] Carl Petoskey, "The Growing Threat of Password Reset Poisoning." [Online]. Available: https://www.techgyd.com/growing-threat-of-password-reset-poisoning/49574/

[8] R. Merlang, "SIMULASI PENETRATION TESTING CENTER OF E-LEARNING AND EDUCATION FOR STUDENTS (CERDAS) UNIVERSITAS ISLAM RIAU DENGAN METODE BRUTE FORCE MENGGUNAKAN HATCH".

[9] Irfan Murti Raazi, "ANALISIS PENILAIAN KEAMANAN SERVER TERHADAP SISTEM INFORMASI MANAJEMEN KEPEGAWAIAN DENGAN METODE NIST SP 800-115 PADA UNIVERSITAS ISLAM NEGERI AR-RANIRY".

[10] Y. Liang *et al.*, "Internet's Invisible Enemy: Detecting and Measuring Web Cache Poisoning in the Wild," in *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security*, Salt Lake City UT USA: ACM, Dec. 2024, pp. 452–466. doi: 10.1145/3658644.3690361.

[11] Victor Benny Alexsius Pardosi, Bernadete Deta, Fifto Nugroho, dan Arnes Yuli Vandika, *SISTEM KEAMANAN INFORMASI*. Kota Solok, Sumatera Barat, Kode Pos 27312: PT MAFY MEDIA LITERASI INDONESIA. Accessed: Feb. 18, 2025. [Online]. Available: https://repository.um.ac.id/5536/1/fullteks.pdf

[12] Dr. Budi Raharjo, S.Kom., M.Kom., MM., *KEAMANAN SISTEM INFORMASI*. Yayasan Prima Agus Teknik, 2021. Accessed: Feb. 24, 2025. [Online]. Available: https://digilib.stekom.ac.id/assets/dokumen/ebook/feb_preveb984_1641362578.pdf

[13] M. Kuusisto, "HTTP HEADER FIELDS AND THEIR VERSATILE USE," 2024, [Online]. Available:

https://trepo.tuni.fi/bitstream/handle/10024/160612/KuusistoMiika.pdf
[14] A. Deshpande, “Leveraging Signature Patterns and Machine Learning for Detecting HTTP Header Manipulation Attacks,” *Journal of Information Systems Engineering and Management*, vol. 10, pp. 636–650, Feb. 2025, doi: 10.52783/jisem.v10i9s.1290.
[15] T. Innocenti, S. A. Mirheidari, A. Kharraz, B. Crispo, and E. Kirda, “You’ve Got (a Reset) Mail: A Security Analysis of Email-Based Password Reset Procedures,” in *Detection of Intrusions and Malware, and Vulnerability Assessment*, vol. 12756, L. Bilge, L. Cavallaro, G. Pellegrino, and N. Neves, Eds., in Lecture Notes in Computer Science, vol. 12756. , Cham: Springer International Publishing, 2021, pp. 1–20. doi: 10.1007/978-3-030-80825-9_1.
[16] Safiera Anindya S, “Identifikasi Kerentanan,” Identifikasi Kerentanan Sistem melalui Vulnerability Assessment. Accessed: Jun. 12, 2024. [Online]. Available: https://widyasecurity.com/2024/02/01/identifikasi-kerentanan-sistem-melalui-vulnerability-assessment/
[17] “What is Common Vulnerability Scoring System (CVSS)?” Accessed: Mar. 14, 2025. [Online]. Available: https://www.armis.com/faq/vulnerability-score-cvss-vs-risk-score-what-is-the-difference/
[18] P. Mell *et al.*, “Measuring the Common Vulnerability Scoring System base score equation,” National Institute of Standards and Technology (U.S.), Gaithersburg, MD, NIST IR 8409, Nov. 2022. doi: 10.6028/NIST.IR.8409.
[19] K. A. Scarfone, M. P. Souppaya, A. Cody, and A. D. Orebaugh, “Technical guide to information security testing and assessment.,” National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-115, 2008. doi: 10.6028/NIST.SP.800-115.