ANALISIS KEAMANAN TERHADAP KOMBINASI *XSS* DAN *SOCIAL ENGINEERING* PADA *WEBSITE*

Rian Firgiawan Gusti Ananda[1], Endang Sulistiyani[2]

[1,2] Jurusan Sistem Informasi, Universitas Nahdlatul Ulama Surabaya, Indonesia
[1]rifirwan26@gmail.com, [2] sulistiyani.endang@unusa.ac.id

.

Abstrak

Meningkatnya intensitas kejahatan siber dari tahun ke tahun menjadikan keamanan siber sebagai aspek penting dalam menjaga kerahasiaan, integritas, dan ketersediaan data serta informasi di era digital. Perkembangan sistem informasi berbasis web tidak hanya meningkatkan efisiensi, tetapi juga memperluas potensi celah keamanan yang dapat dimanfaatkan oleh pelaku kejahatan siber. Berdasarkan laporan Badan Siber dan Sandi Negara (BSSN), serangan *Cross-Site Scripting (XSS)* dan *Social Engineering* merupakan dua jenis serangan yang mendominasi insiden keamanan siber di Indonesia pada periode 2020–2021. Hal ini menunjukkan bahwa ancaman terhadap sistem informasi berasal dari kombinasi kelemahan teknis sistem dan faktor non-teknis yang berkaitan dengan perilaku pengguna. Sebagian besar penelitian sebelumnya membahas mengenai serangan *XSS* dan *Social Engineering* secara terpisah, sementara kajian mengenai dampak kombinasi kedua teknik tersebut masih terbatas. Oleh karena itu, penelitian ini bertujuan untuk menganalisis tingkat risiko serangan kombinasi *XSS* dan *Social Engineering* pada sistem informasi berbasis web. Metode penelitian yang digunakan adalah penetration testing untuk mensimulasikan skenario serangan, yang selanjutnya dianalisis menggunakan tabel risiko keamanan informasi. Hasil penelitian menunjukkan bahwa kombinasi *Reflected XSS* dengan teknik *Pretexting* menghasilkan tingkat keparahan sebesar 6,8 dengan kategori *Medium* dan probabilitas 3 (*Possible*). Sementara itu, kombinasi *Stored XSS* dengan *Pretexting* menunjukkan tingkat keparahan yang lebih tinggi sebesar 7,6 dengan kategori *High* dan probabilitas 5 (*Frequent*). Kedua kombinasi serangan menunjukkan tingkat keparahan yang lebih tinggi dibandingkan dengan tingkat keparahan dari *Reflexted XSS* (5,4) dan *Stored XSS* (7,1). Temuan ini menunjukkan bahwa serangan kombinasi memiliki tingkat risiko yang lebih signifikan dibandingkan penggunaan teknik serangan secara terpisah.

Kata kunci: *XSS*, *Social engineering*, *penetration testing*, keamanan siber, serangan hibrida.

1. Pendahuluan

Keamanan siber merupakan aspek krusial dalam melindungi data dan informasi di era digital. Urgensi dari keamanan siber semakin meningkat seiring dengan tingginya angka kejahatan siber yang terus bertambah setiap tahunnya (Susanto et al., 2023). Kegagalan dalam melindungi data dan informasi dari ancaman siber dapat menyebabkan berbagai dampak, seperti kerugian finansial, hilangnya kepercayaan pengguna, hingga gangguan operasional perusahaan (Restika & Sonita, 2023). Sebagai lapisan perlindungan, keamanan siber bertindak untuk mengamankan informasi yang disimpan, diproses dan dikirim melalui sistem dan jaringan komputer. Oleh karena itu, keamanan siber diperlukan untuk melindungi aset teknologi informasi baik pada individu, organisasi maupun perusahaan di era digital saat ini.

Meskipun keamanan siber sudah diterapkan tetapi masih saja dihadapkan dengan berbagai tantangan. Salah satu tantangan yang ada dalam keamanan siber yaitu serangan siber. Dalam serangan siber terdapat dua jenis serangan yang terdiri dari serangan teknis dan serangan non-teknis (Fitria & Mutijarsa, 2023). Serangan teknis dalam keamanan siber memanfaatkan kerentanan dalam perangkat lunak, sistem, atau jaringan seperti *Malware*, *SQL Injection*, *Cross-Site Scripting* (*XSS*), *Denial of Service* (*DoS*), *Ransomware*. Sedangkan serangan non-teknis melibatkan manipulasi psikologis dan sosial untuk mendapatkan informasi atau akses seperti *Social engineering* (Butarbutar, 2023). Menurut laporan Badan Siber dan Sandi Negara (BSSN) pada ID-SIRTII/CC di tahun 2021 terdapat 2.354 kasus serangan *XSS* dan 4.491 kasus serangan non-teknis yaitu *Social engineering*. Sedangkan di tahun 2020 serangan *XSS* hanya 1.642 laporan dan untuk kasus *Social engineering* hampir tidak ada perbedaan yaitu 4.366 laporan (ID-SIRTII/CC, 2020 & 2021). Terjadinya peningkatan kasus serangan *XSS* dan juga *Social engineering* pada tahun 2020 sampai 2021 di Indonesia menunjukkan bahwa permasalahan pada keamanan siber masih menjadi ancaman bagi data dan informasi digital.

Saat ini, berbagai penelitian telah dilakukan untuk membahas serangan siber di Indonesia, dengan fokus utama pada evaluasi keamanan dan mitigasi ancaman.

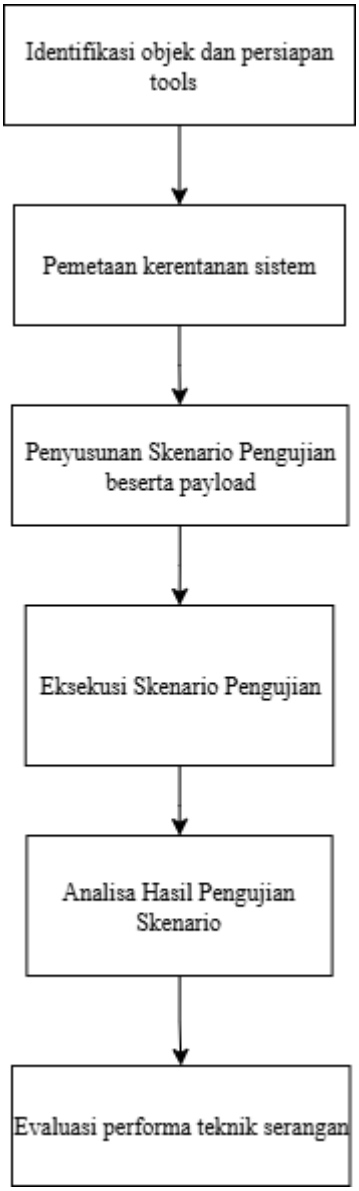
Studi terkait serangan *Cross-Site Scripting*, seperti yang dilakukan oleh (Gustiyono et al., 2024) dan (Mulyanto et al., 2022) menunjukkan bahwa kerentanan *XSS* dan *CSRF* masih sering ditemukan pada berbagai aplikasi web. Pendekatan berbasis *tools*, seperti *OWASP*, menjadi salah satu pilihan dalam mendeteksi celah keamanan dengan lebih efisien. Selain itu, penerapan *penetration testing* pada target sering digunakan untuk mengevaluasi efektivitas sistem keamanan terhadap serangan. Sementara itu, penelitian terkait pengujian serangan non-teknis, seperti yang dilakukan oleh (Gumay et al., 2024) dan (Ansyafa et al., 2024) menunjukkan penggunaan teknik *Social engineering*, termasuk *Phishing* dan *email spoofing* dalam *penetration testing*. Penelitian mitigasi keamanan siber terhadap serangan *Social engineering* juga dilakukan oleh (Safitri et al., 2020), (Junaedi, 2017) dan (Ramadhan & Purwandari, 2023). Hasil penelitian ini menyoroti pentingnya analisis tingkat kesadaran pengguna dan staf terhadap keamanan informasi melalui survei. Selain itu, peneliti mengidentifikasi teknik serangan yang sering digunakan oleh peretas, penyebab kerentanan sistem, dan dampak yang ditimbulkan, seperti kebocoran informasi atau akses tidak sah. Penelitian ini juga memberikan rekomendasi langkah-langkah mitigasi untuk mengurangi risiko serangan di masa depan.

Meskipun berbagai penelitian tentang serangan siber telah dilakukan, sebagian besar masih terbatas pada pengujian masing-masing teknik dengan kategori serangan teknis secara terpisah. Padahal, Perkembangan global yang semakin pesat telah menciptakan bentuk ancaman baru yang lebih kompleks, salah satunya adalah *Hybrid Attack*. Kombinasi serangan atau *Hybrid Attack* menggabungkan serangan teknis dan non-teknis, sehingga meningkatkan efektivitas dan dampak serangan (Vimy et al., 2022). Kombinasi serangan *XSS* dan *Social engineering* dipilih karena memiliki potensi yang signifikan untuk meningkatkan efektivitas serangan melalui eksploitasi kelemahan teknis dan manusia. Hal ini menimbulkan kekhawatiran bahwa kombinasi serangan tersebut dapat menghasilkan konsekuensi yang jauh lebih serius terhadap keamanan sistem informasi.

Berangkat dari hal itu, penulis berencana melakukan evaluasi keamanan dan mitigasi kombinasi *Cross-Site Scripting* (*XSS*) dan *Social engineering* pada keamanan sistem informasi berbasis web. Guna mengevaluasi keamanan terhadap kombinasi kedua serangan ini, penulis akan menggunakan metode *Penetration testing*, yakni pengujian keamanan dengan melakukan simulasi serangan terhadap sistem berbasis web. Dalam penelitian ini, ada tiga skenario pengujian yang akan dilakukan untuk mengevaluasi dampak dan efektivitas serangan, yaitu dengan melakukan pengujian serangan *XSS* dan serangan *Social engineering* masing-masing secara terpisah kemudian pengujian kombinasi kedua serangan tersebut. Melalui pengujian ini, diharapkan dapat diketahui sejauh mana kombinasi serangan tersebut memengaruhi keamanan sistem informasi dan penulis dapat memberikan rekomendasi mitigasi untuk meningkatkan perlindungan terhadap ancaman sejenis. Adapun Objek yang digunakan pada penelitian ini yaitu Sistem Informasi Manajemen (SIM). Sistem ini dipilih sebagai sistem berbasis web dengan interaksi penggunanya yang tinggi menyediakan lingkungan ideal untuk mengevaluasi keamanan kedua serangan ini, karena memiliki elemen teknis dan aktivitas pengguna yang rentan terhadap eksploitasi.

2. Metode Penelitian

Pada Gambar 1. menunjukkan bagaimana tahapan-tahapan yang dilakukan pada penelitian ini.



Gambar 1. Tahapan Penelitian

2.1 Identifikasi Objek dan Persiapan *Tools*

Objek kombinasi serangan terdiri menjadi 2 jenis yaitu komponen (*Cross Site Scripting*) dan pemangku kepentingan (*Social engineering*) pada Sistem Informasi Manajemen (SIM). *Tools* yang akan digunakan sebagai alat pengujian yaitu *Burpsuite*. Persiapan *tools* mencakup beberapa langkah, pertama adalah menyiapkan kebutuhan alat pengujian dengan mengidentifikasi spesifikasi *tools*, kedua adalah menggali informasi prosedur *tools* guna memastikan proses pengujian dilakukan secara efektif dan efisien sesuai fungsi dan karakteristik masing-masing alat. Spesfikasi *tools* didapati melalui dokumentasi resmi pada website https://portswigger.net/burp/documentation.

2.2 Pemetaan Kerentanan Sistem

Proses pemetaan kerentanan sistem ditujukan pada serangan *Cross Site Scripting* dengan fokus utama mencari celah keamanan pada komponen sisrem. Komponen sistem dipetakan berdasarkan metode pengiriman *HTTP*, Validasi inputan, dan jenis kerentanan yang sesuai dengan teknik dalam konteks *Cross Site Scripting* seperti *Reflected XSS, Stored XSS,* dan *dom XSS*.

2.3 Penyusunan Skenario Pengujian Beserta *Payload*

Pada tahap penyusunan skenario pengujian serta *payload*, dipetakan berdasarkan kombinasi teknik serangan. Di mana skenario setiap kombinasi akan disesuaikan dengan teknik *Social engineering* yang digunakan. Pemilihan teknik kombinasi juga dipilih dengan komunikasi yang sesuai kondisi lingkungan pengujian dengan memanfaatkan urgensi korban. Sementara itu, *payload Cross-Site Scripting* menggunakan *script* pada umumnya yang biasa digunakan untuk eksploitasi serangan *XSS*.

2.4 *Penetration testing*

Penetration testing, dilakukan dengan memperhatikan langkah-langkah skenario yang memadukan teknik serangan. Pada pengujian ini dilibatkan sebanyak 20 partisipan yang dibagi menjadi dua kelompok, masing-masing beranggotakan 10 orang untuk setiap teknik kombinasi serangan. Pelaksanaan pengujian dilakukan pada hari yang berbeda. Pembagian kelompok ini bertujuan untuk menganalisa tingkat kesadaran terhadap serangan siber. Kelompok pertama akan di *briefing*, sementara kelompok kedua tidak diberi tahu mengenai serangan.

2.5 Analisa Hasil Pengujian Skenario

Hasil pengujian akan dianalisa berdasarkan pengukuran tingkat keparahan dan tingkat probabilitas. Pada teknik serangan *XSS* pengukuran didasarkan pada tingkat keparahan atau dampak dengan mengadaptasi standar terbuka yaitu *Common Vulnerability Scoring System* (*CVSS*), yang memberikan penilaian terhadap dampak kerentanan pada sistem. Sedangkan serangan *Social engineering* diukur berdasarkan tingkat probabilitas dengan adaptasi dari pendekatan standar ISO/IEC 27005:2018 yang digunakan dalam manajemen risiko keamanan informasi.

Tabel 1. Daftar Metrik *CVSS*

Metrik	Pilihan	Deskripsi
***Attack Vector* (AV)**	*Network* (N)	Serangan dapat dilakukan dari jarak jauh melalui jaringan internet atau LAN.
	Adjacent (A)	Serangan hanya dapat dilakukan dalam satu jaringan lokal.
	Local (L)	Membutuhkan akses langsung ke sistem, seperti login terlebih dahulu.
	Physical (P)	Memerlukan akses fisik ke perangkat target.
***Attack Complexity* (AC)**	*Low* (L)	Serangan dapat dilakukan tanpa syarat atau konfigurasi khusus.
	High (H)	Membutuhkan kondisi tertentu atau pengaturan sistem yang kompleks.
***Privileges Required* (PR)**	*None* (N)	Tidak memerlukan kredensial atau otorisasi.
	Low (L)	Membutuhkan login pengguna biasa.
	High (H)	Membutuhkan hak akses tingkat administrator.
***User Interaction* (UI)**	*None* (N)	Serangan terjadi secara otomatis tanpa interaksi pengguna.
	Required (R)	Membutuhkan tindakan dari pengguna, seperti mengeklik tautan atau membuka file.
***Scope* (S)**	*UnChanged* (U)	Dampak kerentanan hanya terbatas pada sistem atau komponen yang sama.
	Changed (C)	Kerentanan memengaruhi komponen lain, termasuk perubahan izin atau kontrol sistem.
***Confidentiality* (C)**	*None* (N)	Tidak ada kebocoran data.
	Low (L)	Terjadi kebocoran data terbatas atau tidak sensitif.
	High (H)	Mengakibatkan kebocoran data penting, sensitif, atau informasi login.
***Integrity* (I)**	*None* (N)	Tidak terjadi perubahan data.
	Low (L)	Perubahan data bersifat terbatas dan tidak signifikan.
	High (H)	Terjadi perubahan data kritis yang dapat dimanipulasi.
***Availability* (A)**	*None* (N)	Tidak memengaruhi ketersediaan layanan.
	Low (L)	Menyebabkan gangguan ringan terhadap layanan.
	High (H)	Layanan menjadi tidak tersedia atau tidak dapat diakses sepenuhnya.

Nilai yang dihasilkan oleh metrik *CVSS* umumnya berkisar antara 0,0 hingga 10,0, yang digunakan untuk menggambarkan tingkat keparahan suatu kerentanan. Dalam *CVSS*, terdapat tiga jenis metrik, yaitu: (1) *Base Metrics*, (2) *Temporal Metrics*, dan (3) *Environmental Metrics*. Pada penelitian ini, digunakan Base Metrics sebagai dasar pengukuran tingkat keparahan kerentanan. *Base Metrics* sendiri merupakan metode penilaian yang menjelaskan karakteristik mendasar dari suatu kerentanan tanpa mempertimbangkan kondisi khusus atau faktor eksternal. Tabel 1 menyajikan penjelasan parameter dan opsi yang digunakan untuk menghasilkan *base score*.

Tabel 2. Kategori Tingkat Probabilitas

Kategori	Nilai	Deskripsi
Very UnLikely	1	Kemungkinan sangat kecil. Serangan hanya berhasil pada <10% target; umumnya terjadi secara insidental.
UnLikely	2	Kemungkinan rendah. Serangan hanya berhasil pada 10–25% target; terjadi dalam kondisi atau konteks terbatas.
Possible	3	Kemungkinan sedang. Serangan berhasil pada 26–50% target; masih memerlukan kondisi atau respon tertentu.
Likely	4	Kemungkinan tinggi. Serangan berhasil pada 51–75% target; umumnya berhasil tanpa hambatan teknis atau sosial.
Frequent	5	Kemungkinan sangat tinggi. Serangan berhasil pada >75% target; dapat dilakukan berulang dengan hasil konsisten.

Pada Tabel 2 ditampilkan kategori dan nilai tingkat probabilitas beserta penjelasannya. Nilai probabilitas ini menggambarkan sejauh mana kemungkinan suatu serangan *Social engineering* berhasil serta seberapa besar target yang dapat tereksploitasi. Penilaian probabilitas tersebut digunakan sebagai salah satu parameter dalam pengukuran risiko, yang selanjutnya menjadi dasar dalam penetapan matriks risiko pada tahap evaluasi performa teknik serangan.

2.6 Evaluasi Performa Teknik

Evaluasi hasil serangan pada masing-masing kombinasi teknik sangat penting untuk menggambarkan keseluruhan efektivitas dan potensi ancaman dari setiap teknik serangan terhadap objek. Selain itu evaluasi performa teknik juga memberikan gambaran sejauh mana kombinasi serangan mampu meningkatkan risiko keamanan baik dari sisi teknis maupun sosial. Hasil ini diharapkan dapat menjadi acuan dalam strategi penyusunan mitigasi pada pihak institusi terkait maupun umum terhadap sistem yang dibangun.

3. Hasil dan Pembahasan

3.1 Identifikasi Objek dan Persiapan *Tools*

Dalam konteks Sistem Informasi Manajemen (SIM) berbasis website, objek yang diidentifikasi dikelompokkan menjadi dua kategori utama, yaitu komponen sistem dan pemangku kepentingan.

a. *Cross Site Scripting* (*XSS*)

Objek komponen yang teridentifikasi dalam sistem, diklasifikasikan berdasarkan tiga elemen utama sebagai vektor serangan, yaitu *Uniform Resource Locator* (*URL*), *HTTP Method*, dan komponen input. Ketiga elemen ini menjadi jalur utama yang memungkinkan skrip berbahaya dieksekusi apabila sistem tidak memiliki mekanisme validasi dan sanitasi yang memadai.

b. *Social engineering*

Objek pemangku kepentingan yang di identifikasi dalam sistem merujuk pada individu-individu yang memiliki peran tertentu dalam pengelolaan sistem secara terorganisasi dan sistematis. Dalam Sistem Informasi Manajemen (SIM), ada tiga peran utama yang melakukan aktivitas pada sistem, yaitu Dosen, Mahasiswa, dan Admin Program Studi. Setiap peran memiliki status dan aktivitas spesifik di dalam sistem.

Selanjutnya, diperlukan persiapan kebutuhan alat uji terlebih dahulu, khususnya dengan mengidentifikasi spesifikasi *tools* yang akan digunakan. Pada tahap ini, fokus utama adalah penentuan kebutuhan dan konfigurasi Burp Suite sebagai perangkat uji utama. Semua informasi mengenai spesifikasi alat pengujian tersebut di dapati melalui situs resmi dari *Burpsuite* sendiri yaitu *portswigger.net*. Spesifikasi minimum perangkat diketahui sebagai berikut.

a. Minimum : CPU 2x *Cores* / 4 GB RAM
b. Rekomendasi : CPU 2*x Cores* / 16 GB RAM
c. *Advanced:* 4*x cores* / 32 GB RAM
d. *Support Platform: Windows, Linux , Mac OS*

3.2 Pemetaan Kerentanan Sistem

Setelah proses identifikasi obyek, dilakukan pemetaan terhadap kerentanan sistem pada serangan *Cross-Site Scripting* (*XSS*) guna mengetahui komponen mana saja yang relevan untuk uji skenario. Hasil pemetaan pada Tabel 3. menunjukkan adanya kerentanan *Stored XSS* pada form pesan, reply, bimbingan akademik, dan pengajuan KHP, yang berpotensi dimanfaatkan untuk pencurian sesi, manipulasi data, serta kebocoran informasi pribadi. Sementara itu, *Reflected XSS* pada input pencarian memungkinkan penyerang menyisipkan tautan berbahaya yang dapat digunakan untuk *Phishing* maupun pencurian data sensitif.

Tabel 3. Kerentanan komponen sistem

	Komponen	*HTTP Method*	Jenis Kerentanan	Alasan
a.	*Form* Tulis	*POST*	*Stored XSS*	Data

Komponen	*HTTP Method*	Jenis Kerentanan	Alasan
b. Pesan Form Reply c. Input Bimbingan Akademik d. Form Pengajuan Kartu Hasil Prestasi (KHP)			disimpan ke *server* lalu saat eksekusi pesan ditampilkan
Input Pencarian	*POST*	*Reflected XSS*	Data tidak di simpan ke *server* melainkan hasil langsung ditampilkan saat setelah dieksesuksi

3.3 Penyusunan Skenario Beserta *Payload*

Pada tahap ini disusun dua skenario serangan kombinasi, yaitu *Stored XSS* + *Pretexting* dan *Reflected XSS* + *Pretexting*. *Pretexting* dipilih karena selaras dengan mekanisme *XSS* yang memanfaatkan input pengguna. Pada kedua skenario, penyerang memanfaatkan rekayasa sosial untuk meyakinkan korban agar membuka halaman berisi *payload*, yang kemudian dieksekusi dan memungkinkan pencurian *cookie*. Hal ini menunjukkan bahwa kombinasi serangan teknis dan psikologis lebih berbahaya dibandingkan penggunaan *XSS* secara tunggal.

Tabel 4. Skenario Serangan

Teknik	Skenario
Stored XSS + Pretexting	Penyerang menyisipkan skrip atau *payload* pada *form* tulis pesan ke dalam sistem. Lalu korban diarahkan untuk membuka halaman tersebut melalui komunikasi *end-to-end* dengan dalih penyerang mendapati *bug* sistem yang sangat aneh lalu diarahkan untuk mengganti *id URL* dengan muatan *payload* tadi setelah korban mengakses penyerang secara otomatis mendapatkan *cookie* korban.
Reflected XSS + Pretexting	Korban diarahkan untuk membuka halaman tersebut melalui komunikasi *end-to-end* dengan dalih penyerang mendapati *bug* sistem yang sangat aneh lalu diarahkan untuk mengganti *id URL* dengan muatan *payload* tadi setelah korban mengakses penyerang secara otomatis mendapatkan *cookie* korban.

Daftar *payload* pada Tabel 5. menunjukkan variasi serangan *XSS* berdasarkan metode *HTTP* yang sering digunakan, yakni GET dan POST. *Payload Reflected XSS* dikirim melalui *URL* dan langsung dipantulkan dalam respon, *Stored XSS* dikirim lewat *body form* dengan metode POST lalu disimpan di server, sedangkan *DOM-based XSS* dieksekusi melalui fragmen *URL* yang diproses oleh *JavaScript* di sisi klien. Perbedaan ini menggambarkan beragam vektor serangan *XSS* yang dapat dimanfaatkan sesuai celah pada sistem.

Tabel 5. Daftar *Payload XSS*

Teknik *XSS*	*HTTP Method*	Bentuk *Payload*	Keterangan
Reflected XSS	*GET*	*?q=<script> alert(1)</scri pt>*	*Payload* dikirim via *URL*, dipantulkan langsung ke respon
Stored XSS	*POST*	*<img src=x onerror="ale rt(1) ">*	Dikirim lewat *body form POST* dan disimpan dalam *server* lalu tampil dalam respon
DOM-based XSS	*GET*	*#<img src=x onerror=alert (1)>*	*Payload* aktif dari *URL fragment*, diproses oleh *JavaScript* klien

3.4 *Penetration testing*

Setelah skenario disusun, tahap selanjutnya adalah pengujian melalui *penetration testing*. Fokus pengujian mencakup dua kombinasi, yaitu *Reflected XSS* dan *Stored XSS* dengan *Pretexting*, untuk menilai kewaspadaan pengguna terhadap serangan teknis sekaligus sosial serta mengamati respon partisipan, baik yang telah diberi informasi maupun yang belum, terhadap manipulasi berbasis rasa ingin tahu. Sementara itu, pada pengujian *DOM XSS* tidak menunjukkan adanya celah, sehingga penelitian terbatas hanya pada dua skenario tersebut.

Tabel 6. Hasil Uji Skenario *Reflected XSS dan Pretexting*

Uji	Hasil
4	Target mengikuti skenario dan menginput *JavaScipt* yang telah ditentukan sehingga *cookie* berhasil didapat.
2	Target tidak mengikuti skenario, karena merasa tahu apa kode *JavaScript*.
2	Target tidak tertarik
2	Target tidak mengikuti skenario, karena merasa curiga.

Pengujian selama satu hari pada tanggal 24 Juni 2025 terhadap 10 mahasiswa menunjukkan hasil yang tercantum pada Tabel 6, yaitu 6 partisipan bersikap waspada dan mengabaikan skenario serangan, sementara 4 lainnya mengikuti instruksi yang diberikan. Pada kelompok yang terpengaruh, penyerang berhasil membujuk korban untuk memasukkan input berisi skrip berbahaya sehingga memicu eksekusi *Reflected XSS* dan memungkinkan

pencurian *cookie* sesi melalui browser. Temuan ini memperlihatkan bahwa kombinasi teknik manipulasi sosial (*Pretexting*) dan celah teknis (*Reflected XSS*) secara sinergis meningkatkan efektivitas serangan, khususnya terhadap target yang sudah merasa percaya karena komunikasi tampak personal dan tidak mencurigakan.

Tabel 7. Hasil Uji Skenario *Stored XSS dan Pretexting*

Uji	Hasil
1-10	Target mengikuti skenario dan mengganti id menjadi 58406 sehingga mengakses pesan berisi *payload*, lalu *cookie* tercatat.

Pada pengujian yang dilakukan pada 25 Juni 2025 selama satu hari, kombinasi teknik manipulasi sosial (*Pretexting*) dan eksploitasi teknis (*Stored XSS*) berhasil membujuk seluruh partisipan (10 mahasiswa) untuk mengakses tautan berisi *payload*. Skrip *Stored XSS* pun berhasil dijalankan secara otomatis saat halaman dimuat, sehingga penguji memperoleh *cookie* sesi tanpa disadari target. Pada Tabel 6. ditunjukkan bahwa seluruh partisipan mengikuti skenario pengujian dengan hasil serangan berhasil 100%. Hasil ini menegaskan tingginya efektivitas serangan kombinasi tersebut serta pentingnya peningkatan kesadaran keamanan dan validasi pada sisi pengguna maupun sistem.

3.5 Analisa Hasil Pengujian Skenario

Pada bagian ini, dilakukan analisis hasil pengujian pada 2 parameter yaitu, tingkat keparahan (*severity*) dan tingkat probabilitas. Serangan *XSS* diukur berdasarkan tingkat keparahan atau dampak dengan mengadaptasi standar terbuka *Common Vulnerability Scoring System* (*CVSS*), yang memberikan penilaian terhadap dampak kerentanan pada sistem. Sedangkan serangan *Social engineering* diukur berdasarkan tingkat probabilitas dengan adaptasi dari pendekatan standar ISO/IEC 27005:2018 yang digunakan dalam manajemen risiko keamanan informasi (Meitarice et al., 2024).

Berdasarkan hasil pengujian, skenario *Stored XSS + Pretexting* yang ditunjukkan pada Tabel 8. memiliki tingkat keberhasilan tertinggi (100%), dengan seluruh partisipan berhasil dimanipulasi dan *cookie* terekam otomatis. Skor *CVSS* mencapai 7.6 sehingga dikategorikan keparahan tinggi dan probabilitas sangat sering terjadi (*Frequent*).

Tabel 8. Hasil Kombinasi *XSS* dan *Social engineering*

Teknik Kombinasi	Keberhasilan	Tingkat Keparahan (*Severity*)	Tingkat Probabilitas
Stored XSS + Pretexting	10/10 (100%)	*High* (Skor *CVSS*: 7.6)	*Frequent* (5)
Reflected XSS + Pretexting	5/10 (50%)	*Medium* (Skor *CVSS*: 6,8)	*Possible* (3)

Sebaliknya, pada skenario *Reflected XSS + Pretexting*, tingkat keberhasilan hanya 50%, dengan skor *CVSS* 6.8 yang menunjukkan keparahan sedang mendekati tinggi dan probabilitas sedang (*Medium*) karena bergantung pada interaksi pengguna. Temuan ini sejalan dengan studi mengenai rekayasa sosial oleh (Naz et al., 2024) yang menegaskan bahwa manipulasi psikologis, seperti *Pretexting* dan phishing, secara signifikan meningkatkan tingkat keberhasilan serangan terhadap pengguna.

3.6 Evaluasi Performa Teknik

Berikut adalah hasil evaluasi masing-masing metode serangan berdasarkan matriks risiko keamanan. Evaluasi ini menggambarkan efektivitas dan potensi ancaman dari setiap teknik, serta menunjukkan bagaimana kombinasi serangan dapat meningkatkan risiko baik secara teknis maupun sosial. Temuan ini diharapkan menjadi acuan dalam merumuskan strategi mitigasi yang lebih komprehensif.

Tabel 9. Tingkat Risiko Keamanan Informasi

Probability	**Severity**	Tingkat Risiko
Frequent (5)	Low	Medium
Frequent (5)	Medium	High
Frequent (5)	High	High
Likely (4)	Low	Medium
Likely (4)	Medium	High
Likely (4)	High	High
Possible (3)	Low	Low
Possible (3)	Medium	Medium
Possible (3)	High	High
Unlikely (2)	Low	Low
Unlikely (2)	Medium	Medium
Unlikely (2)	High	Medium
Very Unlikely (1)	Low	Low
Very Unlikely (1)	Medium	Low
Very Unlikely (1)	High	Medium

Tingkat Risiko Keamanan Informasi digunakan untuk menggabungkan penilaian dampak (*severity*) dan kemungkinan (*probability*). Penilaian matriks yang ditunjukkan Tabel 9. sebagaimana ditentukan oleh gabungan skala probabilitas dan keparahan, jika level *severity* rendah (*Low*) meskipun probabilitasnya meningkat nilai risiko tetap relatif rendah. Nilai risiko hanya meningkat ke level *Medium* jika kejadian dengan dampak rendah tersebut terjadi berulang kali pada frekuensi yang tinggi. Hal ini menunjukkan bahwa risiko tidak hanya ditentukan oleh besarnya dampak, tetapi juga dipengaruhi oleh tingkat keterulangan kejadian. Selain itu, level *severity Medium*, nilai risiko dapat bervariasi mulai dari *Low* hingga *High* tergantung dari tingkat probabilitas. Pada *severity* tinggi (*High*), risiko tidak pernah berada pada level rendah karena tingkat keparahan sudah cukup kritis.

Evaluasi kombinasi serangan berdasarkan matriks risiko yang diadaptasi melalui standar pendekatan ISO/IEC 27005:2018 pada Tabel 9. menunjukkan bahwa kedua teknik *Reflected XSS + Pretexting* dan

Stored XSS + Pretexting memiliki tingkat risiko yang tinggi. Kombinasi *Reflected XSS + Pretexting* memiliki skor *CVSS* sebesar 6.8 dengan kategori keparahan *Medium* dan probabilitas *Possible* (skala 3), yang menghasilkan klasifikasi risiko *Medium* menurut matriks keamanan informasi.

Tabel 10. Evaluasi Tingkat Risiko

Kombinasi Serangan	*CVSS*	*Severity*	*Probability* (Skala 1–5)	Tingkat Probabilitas	Tingkat Risiko (Matriks)
Reflected XSS + Pretexting	6.8	*Medium*	3	*(Possible)*	***Medium***
Stored XSS + Pretexting	7.6	*High*	5	*Frequent*	***High***

Sementara itu, *Stored XSS + Pretexting* menunjukkan tingkat risiko serupa namun dengan nilai yang lebih tinggi, yakni *CVSS* 7.6 (*High*) dan probabilitas *Frequent* (skala 5), sehingga juga diklasifikasikan tingkat risiko sebagai *High*. Hasil ini menunjukkan peningkatan tingkat risiko dibandingkan beberapa penelitian sebelumnya yang menguji serangan secara terpisah. Misalnya, penelitian oleh (Gustiyono et al., 2024) menilai tingkat risiko pada website perusahaan terhadap kerentanan *XSS* murni hanya berada pada kategori *medium*, sedangkan studi oleh (Dio Firizqi & Putra Setiawan, 2025) mengenai serangan *social engineering* berbasis *Pretexting* pada pemain gim daring menunjukkan tingkat keberhasilan sebesar 34,4% dari 124 responden, yang jika dikonversikan ke dalam skala probabilitas serangan termasuk kategori *Possible* (skala 3). Dengan demikian, hasil penelitian ini memperlihatkan bahwa kombinasi serangan teknis dan manipulasi sosial menghasilkan risiko yang lebih tinggi dibandingkan apabila kedua teknik diterapkan secara terpisah.

4. Kesimpulan

Hasil analisis menunjukkan bahwa kombinasi serangan *Cross-Site Scripting* (*XSS*) dan *Social engineering* memiliki tingkat risiko yang signifikan. Pada *Reflected XSS* dengan *Pretexting* diperoleh skor *CVSS* sebesar 6.8 (*Medium*) dengan probabilitas 3 (*Possible*), sedangkan pada *Stored XSS* dengan *Pretexting* mencapai 7.6 (*High*) dengan probabilitas 5 (*Frequent*). Temuan ini menunjukkan bahwa serangan kombinasi menghasilkan risiko yang lebih tinggi dibandingkan penggunaan teknik tunggal.

Penelitian ini memiliki keterbatasan pada ruang lingkup pengujian, yaitu hanya dilakukan di lingkungan kampus dengan partisipan mahasiswa program studi Sistem Informasi. Oleh karena itu, hasil penelitian ini belum sepenuhnya dapat digeneralisasi ke konteks yang lebih luas. Untuk penelitian selanjutnya, disarankan memperluas cakupan uji coba ke berbagai lingkungan dengan karakteristik pengguna yang lebih beragam serta menggunakan sampel yang lebih terkontrol. Selain itu, penelitian lanjutan juga dapat mengeksplorasi kombinasi teknik serangan lainnya, seperti *Phishing* dengan *Malware Injection*, *Clickjacking* dengan *Credential Stuffing*, atau *Man-in-the-Middle* (*MitM*) dengan *Social engineering*, guna memperoleh pemahaman yang lebih komprehensif mengenai potensi ancaman serta strategi mitigasi yang lebih adaptif.

Daftar Pustaka:

Ansyafa, K. Z., Fajarudin, M., Fadhil, M., & Neyman, S. N. (2024). Analisis Keamanan Media Sosial terhadap Serangan Phising Online menggunakan Metode Zphisher dan *Social engineering* Toolkit. *Journal of Internet and Software Engineering*, *1*(4), 10. https://doi.org/10.47134/pjise.v1i4.2641

Butarbutar, R. (2023). Kejahatan Siber Terhadap Individu: Jenis, Analisis, Dan Perkembangannya. *Jurnal Hukum & Pembangunan*, *2*(2). https://doi.org/10.21143/telj.vol2.no2.1043

Dio Firizqi, J., & Putra Setiawan, V. (2025). Analisis Serangan *Social engineering* melalui *Pretexting*, Impersonating, dan Phishing pada Pemain Game Mobile Online. *Jurnal Pendidikan Dan Teknologi Indonesia*, *5*(7), 1981–1992. https://doi.org/10.52436/1.jpti.873

Fitria, E. Y., & Mutijarsa, K. (2023). SURVEI PENELITIAN METODE KECERDASAN BUATAN UNTUK MENDETEKSI ANCAMAN TEKNOLOGI SERANGAN SIBER. *Jurnal Teknologi Informasi Dan Ilmu Komputer*, *10*. https://doi.org/10.25126/jtiik.2023107341

Gumay, B., Hendrawan, A. H., & Kusumah, F. S. F. (2024). ANALISIS DAMPAK ANCAMAN CYBERCRIME TERHADAP DATA MAHASISWA PADA SERANGAN WEB PHISING SIAK UIKA. *INFOTECH Journal*, *10*(2), 297–305. https://doi.org/10.31949/infotech.v10i2.11463

Gustiyono, A., Alwi, E. I., & Abdullah, S. M. (2024). Analisa Kerentanan Website Terhadap Serangan Cross-Site Scripting (*XSS*) Metode Penetration Testing. *Cyber Security Dan Forensik Digital*, *7*(1), 25–33. https://doi.org/10.14421/csecurity.2024.7.1.4432

Junaedi, D. I. (2017). Antisipasi Dampak *Social engineering* Pada Bisnis Perbankan. *Infoman's*, *11*(1), 1–10. https://doi.org/10.33481/infomans.v11i1.13

Meitarice, S., Febyana, L., Fitriansyah, A., Kurniawan, R., & Nugroho, R. A. (2024). Risk Management Analysis of Information Security

in an Academic Information System at a Public University in Indonesia: Implementation of ISO/IEC 27005:2018 and ISO/IEC 27001:2013 Security Controls. *Journal of Information Technology and Cyber Security*, *2*(2), 58–75. https://doi.org/10.30996/jitcs.12099

Mulyanto, Y., Zaen, M. T. A., Yuliadi, Y., & Sihab, S. (2022). Analisis Keamanan Website SMA Negeri 2 Sumbawa Besar Menggunakan Metode Penetration Testing (Pentest). *Journal of Information System Research (JOSH)*, *4*(1), 202–209. https://doi.org/10.47065/josh.v4i1.2335

Naz, A., Sarwar, M., Kaleem, M., Mushtaq, M. A., & Rashid, S. (2024). A comprehensive survey on *social engineering*-based attacks on social networks. *International Journal of Advanced and Applied Sciences*, *11*(4), 139–154. https://doi.org/10.21833/ijaas.2024.04.016

Ramadhan, T., & Purwandari, B. (2023). ANALISIS TINGKAT KESADARAN KEAMANAN INFORMASI: STUDI KASUS PENGGUNA APLIKASI PERBANKAN DIGITAL DI INDONESIA GUNA MENCEGAH *SOCIAL ENGINEERING*. *SYNTAX IDEA*, *5*(6), 1. https://doi.org/10.36418/syntax-idea.v3i6.1227

Restika, R., & Sonita, E. (2023). TANTANGAN KEAMANAN SIBER DALAM MANAJEMEN LIKUIDITAS BANK SYARIAH : MENJAGA STABILITAS KEUANGAN DI ERA DIGITAL. *Krigan: Journal of Management and Sharia Business*, *1*(2), 25. https://doi.org/10.30983/krigan.v1i2.7929

Safitri, E. M., Ameilindra, Z., & Yulianti, R. (2020). Analisis Teknik *Social engineering* Sebagai Ancaman Dalam Keamanan Sistem Informasi: Studi Literatur. *JIFTI-Jurnal Ilmiah Teknologi Informasi Dan Robotika*, *2*. https://doi.org/10.33005/jifti.v2i2.26

Susanto, E., Antira, Lady, Kevin, K., Stanzah, E., & Majid, A. A. (2023). Manajemen Keamanan Cyber di Era Digital. *Journal of Business and Entrepreneurship*, *11*(1), 23–33. https://doi.org/10.46273/job&e.v11i1.365

Vimy, T., Wiranto, S., Widodo, P., Suwarno, P., Studi Keamanan Maritim, P., Keamanan Nasional, F., & Pertahanan Republik Indonesia, U. (2022). ANCAMAN SERANGAN SIBER PADA KEAMANAN NASIONAL INDONESIA. *Jurnal Kewarganegaraan*, *6*(1). https://doi.org/10.31316/jk.v6i1.2989