Journal of Digital Business and Technology Innovation (DBESTI)

https://journal.nurulfikri.ac.id/index.php/DBESTI
P-ISSN: 3047-1028 E-ISSN: 3032-775X

ANALISIS KEAMANAN *WEBSITE* KABUPATEN SEMARANG MELALUI METODE *ZERO ENTRY HACKING* DENGAN ACUNETIX

Vidya Febriyana[1], Efrizal Zaida[2], April Rustianto[3]

[1,2,3]Teknik Informatika, Sekolah Tinggi Teknologi Terpadu Nurul Fikri
Depok, Jawa Barat, Indonesia 16451
vidy21285ti@student.nurulfikri.ac.id, efrizalzd67@gmail.com, april.rustianto@dosen.nurulfikri.ac.id

Abstract

In today's digital era, the increasing use of information technology makes it easier for people to access public services, but it also increases the potential for cyber threats that target weaknesses in information systems. Semarang Regency, as one of the regions that is actively developing digital infrastructure and web-based services, also faces challenges in maintaining data and information security. This study aims to evaluate the level of public security accessed through the website, using the ZEH method, which consists of four main stages, namely reconnaissance, scanning, exploitation, and post-exploitation. The tools used in this research are Acunetix to conduct penetration testing of the target system. The results showed that there were two types of vulnerabilities found, including Cross Site Scripting (XSS) with a high risk level. Risk assessment was performed using the CVSS score system with values ranging from 3,1 to 5,3. The results of this study show that the ZEH method is effective in detecting and evaluating the vulnerability of the Semarang Regency website. This research helps provide an overview of the website's security condition and the improvements that need to be made.

Keywords: *Acunetix, Semarang Regency, Vulnerability, Website Security, Zero Entry Hacking (ZEH)*

Abstrak

Di era digital saat ini, peningkatan penggunaan teknologi informasi memudahkan masyarakat dalam mengakses layanan publik, namun di sisi lain juga meningkatkan potensi ancaman siber yang menargetkan kelemahan sistem informasi. Kabupaten Semarang sebagai salah satu wilayah yang tengah aktif mengembangkan infrastruktur digital dan layanan berbasis *website*, juga menghadapi tantangan dalam menjaga keamanan data dan informasi. Penelitian ini bertujuan untuk mengevaluasi tingkat keamanan publik yang diakses melalui *website*, dengan menggunakan metode ZEH, yang terdiri dari empat tahapan utama, yaitu *reconnaissance*, *scanning*, *exploitation*, dan *post-exploitation*. *Tools* yang digunakan dalam penelitian ini yaitu Acunetix untuk melakukan pengujian penetrasi terhadap sistem target. Hasil penelitian menunjukkan bahwa terdapat dua jenis kerentanan yang ditemukan, termasuk *Cross Site Scripting* (XSS) dengan tingkat risiko tinggi. Penilaian risiko dilakukan menggunakan sistem skor CVSS dengan nilai berkisar antara 3,1 hingga 5,3. Hasil dari penelitian ini menunjukkan bahwa metode ZEH efektif dalam mendeteksi dan mengevaluasi kerentanan *website* Kabupaten Semarang. Penelitian ini membantu memberikan gambaran tentang kondisi keamanan *website* serta perbaikan yang perlu dilakukan.

Kata kunci: Acunetix, Kabupaten Semarang, Keamanan *Website*, Kerentanan, *Zero Entry Hacking* (ZEH)

1. PENDAHULUAN

Di era digital, keamanan sistem informasi *website* menjadi hal yang sangat penting, termasuk bagi Kabupaten Semarang yang tengah mengembangkan infrastruktur digital. *Website* pemerintah menjadi akses utama masyarakat dalam menyimpan berbagai informasi penting, seperti data kependudukan dan informasi pelayanan publik lainnya. Namun, masih banyak yang rentan terhadap serangan siber seperti *Cross Site Scripting* (XSS), *Cookie Session*, dan lain sebagainya. Rendahnya kesadaran akan pentingnya keamanan siber juga menjadi tantangan besar, dapat menimbulkan risiko kebocoran data, bahkan gangguan terhadap pelayanan masyarakat. Oleh karena itu, dibutuhkan metode yang efektif untuk mendeteksi kerentanan sebelum dimanfaatkan oleh pihak yang tidak bertanggung jawab [1].

Masalah utama yang dikaji dalam penelitian ini adalah bagaimana metode ZEH dapat digunakan untuk mendeteksi kerentanan serta seberapa efektif pendekatan tersebut dalam

Diterima 14 Juli 2025, Direvisi 24 November 2026, Diterima untuk publikasi 24 November 2026

meningkatkan keamanan *website* pemerintah daerah [2]. Melalui analisis ini, diharapkan dapat diperoleh gambaran menyeluruh mengenai potensi celah keamanan yang ada serta langkah-langkah mitigasi yang dapat dilakukan [3].

Penelitian ini bertujuan untuk menganalisis dan mendeteksi kerentanan pada *website* Kabupaten Semarang menggunakan metode *Zero Entry Hacking* (ZEH). Metode ini terdiri dari empat tahapan, yaitu *reconnaissance*, *scanning*, *exploitation*, dan *post-exploitation*, yang dilakukan dengan bantuan *tools* seperti Acunetix [4]. Penelitian difokuskan pada satu *website* yang memiliki IP dan *port* terbuka.

Manfaat dari penelitian ini tidak hanya dirasakan oleh penulis sebagai bentuk penerapan ilmu akademis, tetapi juga diharapkan bermanfaat bagi instansi terkait sebagai bahan evaluasi keamanan sistem, serta bagi masyarakat dalam meningkatkan pemahaman tentang pentingnya keamanan digital. Secara akademik, hasil penelitian ini dapat menjadi referensi lanjutan dalam pengembangan studi di bidang keamanan siber, khususnya dalam konteks *website* instansi pemerintahan.

Untuk menjaga agar penelitian ini tetap fokus dan tidak melebar dari tujuan utama, maka ruang lingkup penelitian dibatasi hanya pada satu *website* resmi milik Pemerintah Kabupaten Semarang yang dapat diakses oleh publik [5]. Penelitian ini untuk meningkatkan keamanan *website* Kabupaten Semarang dan tidak untuk tujuan lain yang dapat membahayakan keamanan sistem *website*.

2. METODE PENELITIAN

2.1 Rancangan Penelitian

Perancangan penelitian ini disusun sebagai tahap awal untuk menjelaskan secara rinci kegiatan yang akan dilakukan dalam penelitian, yang meliputi jenis penelitian, metode analisis data, metode pengumpulan data, dan lingkungan pengembangan.

2.1.1 Jenis Penelitian

Pada penelitian ini menggunakan metode jenis penelitian eksperimen dalam melakukan pengujian secara langsung terhadap *website* Daerah Kabupaten Semarang. Penelitian eksperimen ini bertujuan untuk menguji efektivitas metode *Zero Entry Hacking* (ZEH) dalam mendeteksi kerentanan pada suatu *website* [6]. Dengan menemukan jenis-jenis kerentanan tertentu yang ada pada *website* yang telah diuji.

2.1.2 Metode Analisis Data

Dalam penelitian ini, menggunakan analisis data kuantitatif untuk memberikan penjelasan yang lebih sistematis dan mudah dipahami penjelasan mendalam tentang *Zero Entry Hacking* (ZEH) dalam mendeteksi kerentanan keamanan *website*, yang di mana data didapatkan dari hasil pengujian langsung dengan menggunakan metode *Zero Entry Hacking* (ZEH), melalui *tools* yang dipaparkan.

2.1.3 Metode Pengumpulan Data

Dalam penelitian ini, selain itu pengujian dalam penelitian ini akan berfokus kepada pendekatan *blackbox testing* dalam pengujian keamanan untuk mengidentifikasi dan mengeksploitasi kerentanan sistem, dan dengan metode pengumpulan data akan dikumpulkan melalui beberapa metode, termasuk analisis kerentanan keamanan pada sebuah *website*. Penjelasan di bawah ini menunjukkan metode yang digunakan dalam pengumpulan data, sebagai berikut:

1. Studi Literatur

Dalam penelitian ini mengumpulkan berbagai macam informasi yang digunakan sebagai studi literatur dari berbagai sumber tertulis untuk mendukung penelitian ini, termasuk dari berbagai artikel, buku, jurnal, skripsi, serta sumber dari internet, semua yang mencakup tentang penelitian ini.

2. Observasi

Dalam penelitian observasi ini, penulis melakukan observasi dengan cara mengumpulkan berbagai macam informasi dan data terkait sebagai dasar acuan melakukan penelitian ini yaitu berfokus pada *website* Kabupaten Semarang wi****.ba****.semarangkab.go.id. Observasi ini dilakukan dengan cara mencari informasi-informasi terkait permasalahan kerentanan keamanan apa saja yang terjadi pada situs *website* tersebut.

3. Wawancara

Dalam memperkuat observasi, penulis juga melakukan tahap wawancara dengan salah satu pihak instansi dari Dinas Kesbangpol Kabupaten Semarang yaitu oleh pihak instansi terkait. Proses wawancara dilakukan melalui percakapan via WhatsApp dari hasil pertanyaan tersebut terkait pada topik penelitian.

2.1.4 Lingkungan Pengembangan

a) *Hardware* (Tabel 1)

Tabel 1. *Hardware*

No	Nama Perangkat Lunak	Spesifikasi
1	*Processor*	Intel(R) Core (TM) i3-1005G1 CPU @ 1.20GHz 1.20 GHz
2	RAM	12 GB
3	*Storage Memory*	1 TB

b) *Software* (Tabel 2)

Tabel 2. *Software*

No	Nama Perangkat Lunak	Spesifikasi
1	*Operating System* (OS)	Windows 11 dan Kali Linux
2	*Application Software*	Oracle VM VirtualBox-amd 64

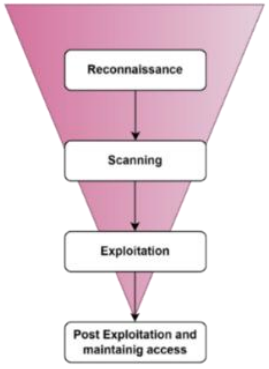
c) Spesifikasi Komponen Acunetix (Tabel 3)

Tabel 3. Spesifikasi Komponen Acunetix

Komponen	Minimum Spesifikasi
Processor	Intel(R) Core (TM) i3-1005G1 CPU @ 1.20GHz 1.20 GHz
Memory	12 GB
Storage	1 TB
Operating System	Windows 11 dan Kali Linux
Software	Acunetix

2.2 Tahapan Penelitian

Gambar 1 menunjukkan alur pengerjaan sebagai alat bantu dalam proses tujuan tertentu.



Gambar 1. Tahapan Penelitian

1. Pengintaian Sistem (*Reconnaissance*):

Reconnaissance yaitu langkah pertama dari pengumpulan informasi mengenai target yang akan diserang, dengan mencari informasi sebanyak-banyaknya.

2. Pemindaian (*Scanning*):

Scanning yaitu dilakukan pemindaian terhadap target dengan menggunakan *tools* Acunetix untuk mencoba berusaha mencari sebuah kerentanan yang didapat [7]. Serta untuk melihat suatu target dalam mengidentifikasi *port* yang terbuka [8].

3. Eksploitasi Celah Keamanan (*Exploitation*):

Exploitation yaitu digunakan untuk memperoleh akses ke sistem target, di mana menguji kerentanan yang telah didapat dari hasil *scanning*, biasanya dapat diuji menggunakan *tools* dan lain sebagainya [9].

4. Pascaeksploitasi (*Post Exploitation*):

Post Exploitation yaitu tahap terakhir, merupakan tahap untuk melaporkan hasil pengujian yang telah dilakukan dan serta memberikan informasi terkait rekomendasi untuk mengatasi kerentanan yang sebelumnya ditemukan [10].

3. HASIL DAN PEMBAHASAN

Pada bagian ini menjelaskan hasil dari sebuah pembahasan terkait dalam metode penelitian di atas dengan menggunakan metode *Zero Entry Hacking* (ZEH).

3.1 Implementasi Sistem

3.1.1 Instalasi dan Penggunaan Acunetix

Proses instalasi Acunetix dimulai dengan mengunduh *installer* melalui tautan GitHub, kemudian menjalankan perintah instalasi melalui terminal Linux seperti pada Gambar 2. Setelah instalasi selesai, pengguna membuat akun untuk mengakses aplikasi melalui alamat https://kali:3443/. Maka akan dilakukan *login* ke antarmuka Acunetix, dilanjutkan dengan memulai proses pemindaian dengan memasukkan URL target. Setelah proses selesai, sistem akan menampilkan hasil pemindaian secara lengkap, termasuk jumlah dan jenis kerentanan yang terdeteksi pada *website* target.



Gambar 2. Instalasi dan Penggunaan Acunetix

Setelah instalasi Acunetix, tahap selanjutnya yaitu membahas hasil pengujian secara lengkap, dengan tahapan awal dalam proses pengujian penetrasi pada *tools* Acunetix menggunakan metode *Zero Entry Hacking* yang meliputi 4 tahapan, sebagai berikut:

3.1.2 *Reconnaissance*

Gambar 3 menunjukkan tahap *reconnaissance* yang bertujuan untuk mengetahui teknologi yang digunakan pada *website* target sebagai langkah awal untuk melakukan *penetration testing*, mendapati informasi seperti HTTP *Server*, *access* kontrol, serta IP *website* domain tersebut. Dengan mengetikkan perintah *whatweb* pada terminal Linux dan mengetikkan sebuah *website* target yang dituju.



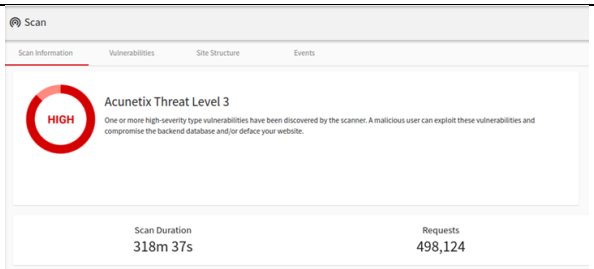
Gambar 3. *Reconnaissance*

3.1.3 *Scanning*

Hasil *scanning* yang dilakukan dengan menggunakan Acunetix selama 318 menit 21 detik mengungkap bahwa *server* yang menggunakan sistem operasi Unix dan *web server* Apache versi 2.4.41 (Ubuntu) berada pada level ancaman "High" yang ditunjukkan oleh Gambar 4. Dalam proses tersebut, terdeteksi sebanyak 327 peringatan yang terdiri dari 23 peringatan dengan tingkat keparahan tinggi, 210 sedang, 20 rendah, dan 74 bersifat informatif, yang menandakan adanya potensi risiko signifikan terhadap sistem atau aplikasi yang dianalisis. Berikut adalah hasil dari *scanning* Acunetix pada Tabel 4:

Tabel 4. Jenis Kerentanan Acunetix

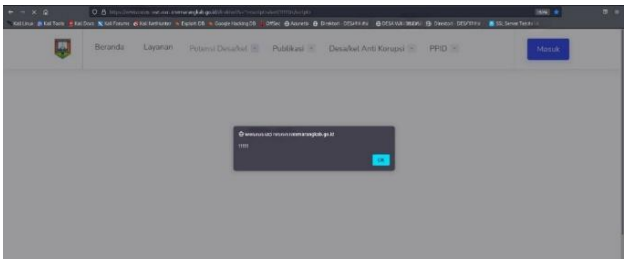
No	Nama Perangkat Lunak	Spesifikasi
1	*Cross-Site Scripting* (XSS)	*High*
2	*SQL Injection*	*High*
3	*Application Error Message*	*Medium*
4	*HTML form without CSRF Protection*	*Medium*
5	*Vulnerable JavaScript Library*	*Medium*
6	*Clickjacking: X-Frame-Options header missing*	*Low*
7	*Cookie without HttpOnly flag set*	*Low*
8	*Documentation File*	*Low*



Gambar 4. Hasil *Scanning* Acunetix

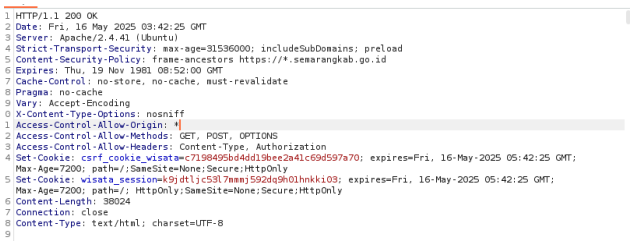
3.1.4 *Exploitation*

Pada tahap *exploitation* berhasil mengidentifikasi celah *Cross Site Scripting* (XSS), dengan tingkat keparahan tinggi pada domain wi****.ba****.semarangkab.go.id yang ditunjukkan oleh Gambar 5. Kerentanan ini dapat dimanfaatkan dengan menyuntikkan skrip melalui parameter pada URL. Melalui uji coba menggunakan *payload* "><script>alert(11111)</script>//, penyerang berhasil memperoleh *cookie session*, yang membuktikan bahwa situs tersebut sangat rentan terhadap serangan XSS dan memungkinkan skrip berbahaya dijalankan di *browser* pengguna.



Gambar 5. *Cross Site Scripting*

Konfigurasi *Cookie without HttpOnly* membuka kemungkinan terjadinya celah serangan lintas situs (*cross-site*) hanya lewat HTTPS seperti yang ditunjukkan oleh Gambar 6. Harus diperkuat dengan kontrol tambahan (misalnya validasi *origin*, penggunaan CSRF token, atau pembatasan metode HTTP).



Gambar 6. *Cookie Without HttpOnly*

3.1.5 *Post Exploitation*

Post Exploitation adalah tahap di mana untuk melakukan *backdoor* akan tetapi tidak dapat diupayakan, pascaeksploitasi hanya dapat melaporkan hasil pengujian yang telah dilakukan dan serta memberikan informasi terkait rekomendasi untuk mengatasi kerentanan yang telah ditemukan. Tabel 5 menunjukkan hasil *Post Exploitation*.

Tabel 5. Tabel *Post Exploitation*

Kegiatan	Hasil
Pelaksanaan dan persiapan	Mendapatkan sebuah informasi dari *website* target, dan mendapatkan kerentanan *high*, *medium*, dan *low*. Sehingga menghasilkan kerentanan pada *cross site scripting* (XSS).
Eksploitasi Terkontrol	Peneliti mengeksploitasi sistem target hanya untuk menguji kelemahan, bukan untuk merusak ataupun mencuri data pada sistem target.

Berdasarkan hasil dari keseluruhan penelitian di atas, menunjukkan bahwa deteksi kerentanan dari hasil *scanning*

menggunakan *tools* Acunetix mendapatkan hasil jenis kerentanan seperti pada Tabel 6:

Tabel 6. Hasil Celah Kerentanan

Kerentanan	Celah Kerentanan	Hasil	*Base Score* CVSS
Cross-Site Scripting	Terdeteksi	*Pop-up* Muncul	5,3
Cookie Without HttpOnly	Terdeteksi	Membuka Peluang JavaScript	3,1

Berdasarkan analisis kerentanan yang ditampilkan dalam Tabel 6, ditemukan beberapa jenis celah keamanan pada *website* yang telah diuji. Setiap celah diklasifikasikan berdasarkan tingkat keparahan, jenis kerentanan, hasil eksploitasi, serta skor CVSS menampilkan *base score* 3,1–5,3. Temuan ini mengindikasikan bahwa sistem masih memiliki sejumlah kelemahan yang berpotensi dimanfaatkan, khususnya pada kerentanan dengan tingkat risiko tinggi. Informasi ini menjadi acuan penting dalam menentukan langkah prioritas untuk perbaikan dan penguatan sistem keamanan, guna mencegah potensi penyalahgunaan oleh pihak yang tidak bertanggung jawab.

4. KESIMPULAN

Penelitian ini bertujuan menguji keamanan *website* Pemerintah Kabupaten Semarang menggunakan metode *Zero Entry Hacking* (ZEH), yang terdiri dari empat tahap: *reconnaissance*, *scanning*, *exploitation*, dan *post-exploitation*. *Tools* Acunetix digunakan untuk memindai dan mengidentifikasi celah keamanan pada sistem target.

Hasil pengujian menemukan dua jenis kerentanan, termasuk *Cross Site Scripting* (XSS) yang tergolong berisiko tinggi. Tingkat risiko dianalisis menggunakan skor CVSS, dengan rentang skor antara 3,1–5,3, yang menunjukkan risiko dari kategori rendah hingga menengah. Temuan ini menunjukkan bahwa metode ZEH efektif dalam mendeteksi dan membantu mengelola kerentanan keamanan, serta memberikan dasar bagi pengelola *website* untuk memperkuat sistem dan mencegah potensi penyalahgunaan oleh pihak yang tidak bertanggung jawab.

Sejumlah saran yang dapat diterapkan baik oleh Pemerintah Kabupaten Semarang maupun oleh peneliti selanjutnya. Untuk Pemerintah Kabupaten Semarang, disarankan agar sistem operasi dan *website* diperbarui secara rutin, administrator dan tim pengembang melakukan pemeriksaan berkala, serta memantau seluruh aktivitas pada sistem dan jaringan guna mencegah potensi ancaman. Sementara itu, untuk penelitian selanjutnya, disarankan agar analisis diperluas dengan menggunakan *tools* tambahan seperti Metasploit dan Nikto untuk mendapatkan perbandingan hasil yang lebih menyeluruh. Selain itu, uji keamanan juga dapat ditingkatkan dengan menerapkan metode *white box* atau *grey box testing*, serta menguji integrasi *Web Application Firewall* (WAF) dengan konfigurasi khusus guna memperkuat sistem keamanan aplikasi web.

DAFTAR PUSTAKA

[1] A. Hermawan, T. Hartati, and Y. A. Wijaya, "Analisa Keamanan Data Melalui Website Zahra Software Menggunakan Metode Keamanan Informasi CIA Triad," *Jurnal Informatika: Jurnal Pengembangan IT*, vol. 7, no. 3, pp. 125–130, 2022.

[2] H. Herdianti and F. Umar, "Analisis keamanan website menggunakan teknik footprinting dan vulnerability scanning," *INFORMAL: Informatics Journal*, vol. 5, no. 2, pp. 43–48, 2020.

[3] F. Fachri, A. Fadlil, I. Riadi, and A. Dahlan, "Analisis Keamanan Webserver menggunakan Penetration Test," *J. Inform*, vol. 8, no. 2, pp. 183–190, 2021.

[4] A. Zirwan, "Pengujian dan Analisis Keamanan Website Menggunakan Acunetix Vulnerability Scanner," *Jurnal Informasi dan Teknologi*, pp. 70–75, 2022.

[5] Dimas Ramadhani, "Analisa Keamanan Aplikasi Berbasis Web Menggunakan Tools Arachni (Studi Kasus: Dinas Komunikasi dan Informatika Daerah Istimewa Yogyakarta)," *Sekolah Tinggi Teknologi Terpadu Nurul Fikri*, 2024.

[6] M. Yaqi, Vulnerability Assessment dan Penetration Testing (Vapt) Menggunakan Metode Zero Entry Hacking (Zeh) Terhadap Website Studi Kasus: Dinas Penanaman Modal …. 2023. [Online]. Available: https://repository.uinjkt.ac.id/dspace/handle/123456789/73422%0Ahttps://repository.uinjkt.ac.id/dspace/bitstream/123456789/73422/1/MUHAMMAD 56 YAQI-FST.pdf.

[7] F. Al Fajar, "Analisis Keamanan Aplikasi Web Prodi Teknik Informatika Uika Menggunakan Acunetix Web Vulnerability," *Jurnal Inovatif: Inovasi Teknologi Informasi dan Informatika*, vol. 3, no. 2, pp. 110–120, 2020.

[8] E. Rosmiyati, D. K. Sari, and E. Pratiwi, "Penerapan Teknik Scanning Dalam Meningkatkan Kemampuan Pemahaman Membaca Siswa," *Journal Of Human And Education (JAHE)*, vol. 4, no. 3, pp. 460–464, 2024.

[9] F. Fachri, "Optimasi Keamanan Web Server Terhadap Serangan Brute-Force Menggunakan Penetration Testing," *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)*, vol. 10, no. 1, pp. 51–58, 2023.

[10] Y. A. Pohan, Y. Yuhandri, and S. Sumijan, "Meningkatkan Keamanan Webserver Aplikasi Pelaporan Pajak Daerah Menggunakan Metode Penetration Testing Execution Standar," *Jurnal Sistim Informasi dan Teknologi*, pp. 1–6, 2021.