Ekobis: Jurnal Ekonomi dan Bisnis
Universitas Moch. Sroedji Jember
Vol. 1 No. 2 Desember , 2024, Hal. 66 - 71

Ekobis: Jurnal Ekonomi dan Bisnis

https://ejournal.umsj.ac.id/index.php/ekobis

Vol. 1 No. 2 Desember , 2024, Hal. 66 - 71

EVOLUSI PERANGKAT LUNAK DALAM MENINGKATKAN ASPEK KEANDALAN & KEAMANAN PADA SISTEM INFORMASI AKUNTANSI DAN MANAJEMEN BISNIS WEBERP BERDASARKAN ISO/IEC 25010

Nur Haryadi
Institut Teknologi Sepuluh Nopember, Surabaya

Abstrak Sistem Informasi webERP adalah perangkat lunak berbasis web yang bersifat open source / sumber terbuka yang dikembangkan oleh sebuah komunitas untuk bisnis skala kecil dan menengah sehingga pelaku bisnis skala kecil dan menengah bisa mendapatkan sebuah sistem dengan budget terjangkau bahkan gratis. Karena bersifat open source / sumber terbuka webERP memiliki beberapa vulnerability / kerentanan terutama dari aspek keamanan. Oleh sebab itu tujuan dari penulisan ini adalah menambahkan kode program agar SQL injection pada CVE-2018-19436 terkait vulnerability / kerentanan tertutup dan sesuai dengan standar ISO / IEC 25010 untuk mencegah kebocoran data pada sebuah unit usaha yang menggunakan sistem informasi webERP.

Kata Kunci: webERP, Peningkatan Aspek Keamanan, ISO/IEC 25010, Burp Suite Community Edition.

Abstract *webERP Information System is a web-based open-source software developed by a community for small and medium-scale businesses, enabling small and medium business owners to obtain a system with affordable budget or even for free. Being open source, webERP has several vulnerabilities, especially in terms of security aspects. Therefore, the purpose of this writing is to add program code to prevent SQL injection related to CVE-2018-19436 vulnerability and align it with ISO/IEC 25010 standards to prevent data leak at business unit that use webERP information system .*

Keywords: *webERP, Security Aspect Improvement, ISO/IEC 25010, Burp Suite Community Edition.*

Alamat Korespondensi
Fakultas Teknik Elektro dan Informatika Cerdas, Institut Teknologi Sepuluh Nopember, Surabaya
E-mail: (Nur Haryadi - *6025241003@student.its.ac.id*)

Pendahuluan

Sistem Informasi Akuntansi dan Manajemen Bisnis webERP adalah perangkat lunak berbasis web yang bersifat *open source* / sumber terbuka yang dikembangkan oleh sebuah komunitas untuk pelaku bisnis skala kecil dan menengah sehingga pelaku bisnis skala kecil dan menengah dapat menggunakan Sistem Informasi Akuntansi dan Manajemen Bisnis dengan budget terjangkau bahkan gratis (Githa Hidayat, Nuryasin, & Suharso, 2020). Karena bersifat open source / sumber terbuka webERP memiliki beberapa *vulnerability* / kerentanan terutama dari aspek keamanan, banyak issue dari beberapa perangkat lunak

open source yang ter-*expose* pada *Forum Common Vulnerabilities and Exposures (CVE)* yang tujuannya agar pemilik / komunitas suatu perangkat lunak mempunyai *awareness* terhadap *vulnerability* / kerentanan perangkat lunak tersebut (Aghaei, Shadid, & Al-Shaer, 2020; Das, Serra, Halappanavar, Pothen, & Al-Shaer, 2021; Martono, 2012).

Pembahasan ini berguna untuk peningkatan aspek keamanan berdasarkan ISO/IEC 25010, tidak menutup kemungkinan perangkat lunak *open source* yang terpasang memiliki *vulnerability* / kerentanan dan dapat menurunkan kredibilitas perangkat lunak / sistem informasi Akuntansi dan Manajemen Bisnis itu sendiri (Sohal, Gupta, & Singh, 2018).

Untuk mengetahui *vulnerability* / kerentanan pada sebuah sistem informasi salah satunya dapat menggunakan beberapa forum CVE yang ada di internet seperti https://cve.mitre.org/. webERP memiliki beberapa daftar CVE di https://cve.mitre.org/ salah satunya terkait SQL *injection vulnerability* (Ally, 2014).

Pada beberapa penelitian sebelumnya hanya membahas *vulnerability* / kerentanan dari beberapa perangkat lunak *open source* salah satunya webERP namun tidak membahas lebih detil terkait *vulnerability* / kerentanan yang terjadi pada perangkat lunak tersebut (Ally, 2014).

Penelitian ini akan membahas bagaimana cara menutup *vulnerability* / kerentanan yang ditemukan pada https://cve.mitre.org/ dengan kode CVE-2018-19435 sub-bagian webERP SQLI-2 - WebERP SQL *injection vulnerability*. Kode program yang ada pada webERP akan dimodifikasi sehingga SQL *injection* yang diuji dengan *tools* Burp Suite Community Edition tidak berhasil dilakukan dengan kata lain *vulnerability* / kerentanan pada webERP sudah ditutup, sehingga pengguna melakukan transaksi dalam sistem dengan aman(Nuryanti & Satria, 2023). Kemudian metode yang diajukan dan hasil akan di bahas pada bab Metode dan bab Hasil & Pembahasan. Pada bagian / bab akhir penelitian ini akan dibahas Kesimpulan dan rencana penelitian selanjutnya.

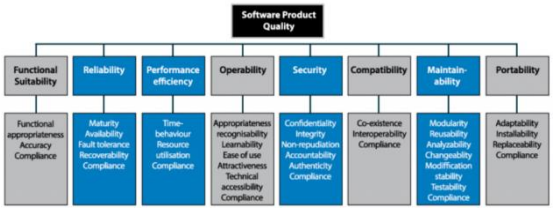
Tinjauan Pustaka

Pada Pembangunan sebuah perangkat lunak maupun perangkat lunak yang sudah dikembangkan komunitas harus melengkapi standar ISO / IEC 25010 (Barletta, Caivano, Colizzi, Dimauro, & Piattini, 2023). *Software quality product* / kualitas produk perangkat lunak yang mana aspek yang tercatum diantaranya,

a. *Functional suitability*
b. *Performance efficiency*
c. *Compatibility*
d. *Usability*
e. *Reliability*
f. *Security*
g. *Maintainability*
h. *Portability*

Terkait detil poin masing-masing dari *software quality product* / kualitas produk perangkat lunak di jelaskan pada table berikut (Chen, Pan, Ma, & Chiang, 2022; Oriol, Marco, & Franch, 2014).

Gambar 1. ISO / IEC 25010 *software quality product* / kualitas produk perangkat lunak



Penelitian terkait aspek keamanan pada sistem informasi menyatakan bahwa sebuah celah yang terjadi akibat SQL *injection* dikarenakan tidak mengikuti standar ISO/IEC 25010 pada aspek *security* / keamanan (Trenggono, 2014). Penelitian lainnya juga menyatakan bahwa sebuah system yang sudah *comply* dengan ISO / IEC 25010 memiliki *measurement* yang baik termasuk pada aspek keamanan (Echefunna et al., 2024; Fadilah & Rochimah, 2023).

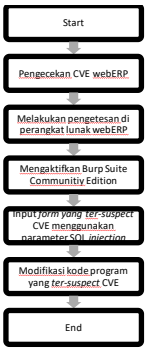
Dalam rancang bangun sebuah perangkat lunak juga membutuhkan suatu pengetesan terkait *vulnerability* / kerentanan yang banyak ditemukan di *Forum Common Vulnerabilities and Exposures (CVE)*, webERP pada versi 4.15 memiliki kode CVE-2018-19435 sub-bagian webERP SQLI-2 - WebERP SQL *injection vulnerability*. CVE yang ditemukan bisa dilakukan menggunakan berbagai

macam *tools* baik berbayar maupun gratis seperti Burp Suite Communitiy Edition (Echefunna et al., 2024).

Metode

Berikut adalah bagan alir bagaimana penelitian ini dilakukan dalam meningkatkan aspek keamanan webERP berdasarkan ISO / IEC 25010,

Gambar 2. Bagan alir metode penelitian



A. webERP

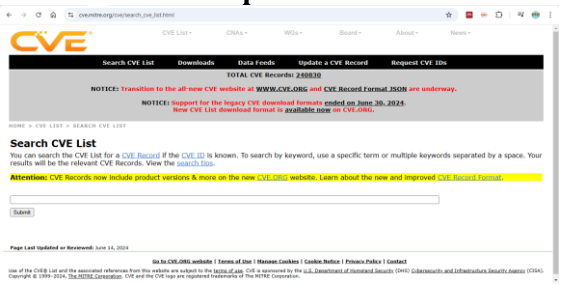
webERP adalah sistem akuntansi dan manajemen bisnis yang berbasis web yang memiliki berbagai fitur yang cocok untuk banyak bisnis terutama bisnis untuk pendistribusian, grosir, dan manufaktur. webERP memiliki berberapa fitur modul diantaranya *sales and orders, taxes, accounts receivable, inventory, purchasing, accounts payable, bank, general ledger, manufacturing, contract costing, dan fixed assets*. webERP memiliki pertumbuhan yang cukup signifikan dikarenakan aplikasi ini berbasis *open source* maka tiap orang dapat gratis mendownload dan menggunakannya. webERP sepenuhnya berbasis web PHP (PHP Hypertext PreProcessor) dan menggunakan database MySQL (Fauzan, 2015).

B. CVE, SQL *injection*, Burp Suite Communitiy Edition, modifikasi kode program

Common Vulnerabilities and Exposures (CVE) merupakan sebuah wadah untuk menemukan berbagai macam *vulnerability* / kerentanan dari perangkat lunak yang beredar atau yang ada di internet. Pada perangkat lunak webERP terutama versi 4.15 ditemukan CVE-2018-19435 pada laman https://cve.mitre.org/ berikut langkah menemukan vulnerability / kerentanan pada CVE-2018-19435, untuk melakukan pemeriksaan dari CVE tersebut maka digunakan Burp Suite Community Edition (Sinha, 2018),

a. Buka laman https://cve.mitre.org/

Gambar 3. Laman pencarian CVE



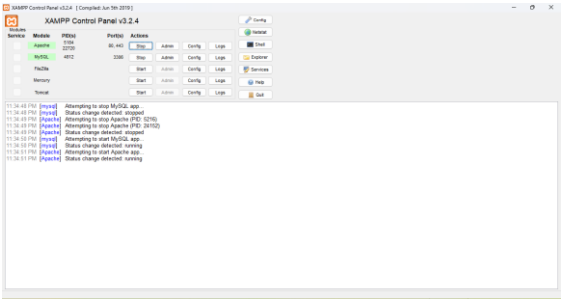
b. Ketik webERP pada kolom pencarian

Gambar 4. Hasil pencarian CVE webERP

C. Pengecekan SQL *injection* menggunakan Burp Suite Communitiy Edition pada webERP 4.15 *local environment*

Step 1 : aktifkan XAMPP *environment*

Gambar 5. XAMPP

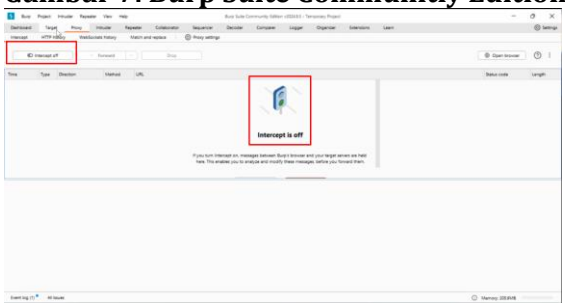


Step 2 : akses pada browser perangkat lunak webERP

Gambar 6. webERP local environment

Step 3 : aktifkan Burp Suite Communitiy Edition

Gambar 7. Burp Suite Communitiy Edition



Step 4 : pada menu *home* webERP pilih menu *Manufacturing - Multiple Work Orders Total Cost Inquiry*

Gambar 8. webERP *Manufacturing - Multiple Work Orders Total Cost Inquiry*

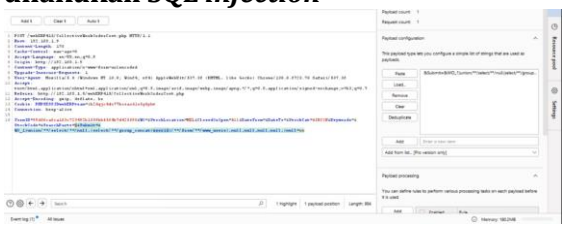
Step 5: laman *Multiple Work Orders Total Cost Inquiry*

Gambar 9. laman *Multiple Work Orders Total Cost Inquiry*

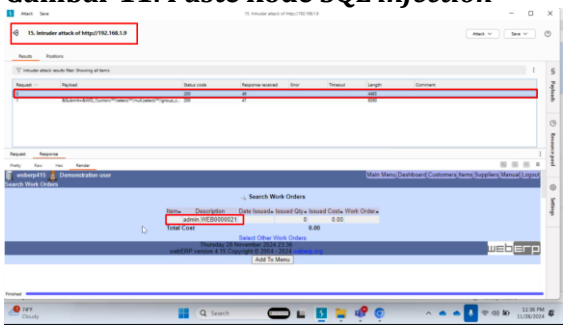
Step 6 : masukan kode SQL *injection* pada laman *Multiple Work Orders Total Cost Inquiry* pada *payload*

```
&Submit=&WO_1)union/**/select/**/null,(select/**/group_co
ncat(userid)/**/from/**/www_users),null,null,null,null,(null=on
```

Gambar 10. *Send to Intruder* untuk memunculkan halaman yang siap dilakukan SQL *injection*

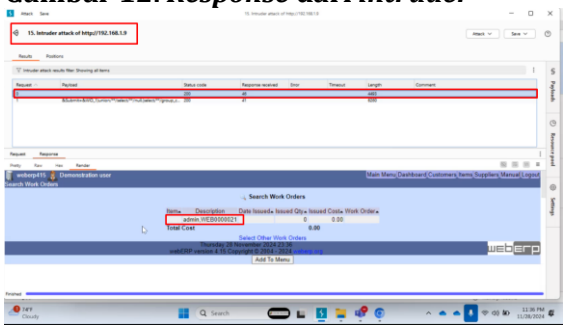


Gambar 11. Paste kode SQL *injection*



Step 7 : melihat hasil *intruder* pada Burp, memperlihatkan hasil SQL *injection* yang menampilkan kolom *userid* pada table *www_users*

Gambar 12. *Response* dari *intruder*



Hasil dan Pembahasan

Untuk mencegah dari *script SQL injection* pada webERP 4.15 yang tertera pada CVE-2018-19435 dengan deskripsi ***An issue was discovered in the Manufacturing component in webERP 4.15. CollectiveWorkOrderCost.php has Blind SQL Injection via the SearchParts parameter*** perlu di lakukan modifikasi program pada *script* CollectiveWorkOrderCost.php seperti berikut :

Step 1 : menambahkan kode program sebagai berikut :

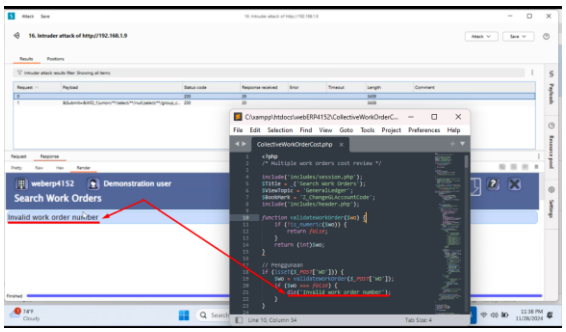
Gambar 13. Kode program untuk mencegah *script* SQL *injection*

```php
<?php
/* Multiple work orders cost review */

include('includes/session.php');
$Title = _('Search Work Orders');
$ViewTopic = 'GeneralLedger';
$BookMark = 'Z_ChangeGLAccountCode';
include('includes/header.php');

function validateWorkOrder($wo) {
    if (!is_numeric($wo)) {
        return false;
    }
    return (int)$wo;
}

// Penggunaan
if (isset($_POST['WO'])) {
    $wo = validateWorkOrder($_POST['WO']);
    if ($wo === false) {
        die('Invalid work order number');
    }
}
```

Step 2 : Jalankan Burp Suite Communitiy Edition dengan memasukan kembali *script* SQL *injection*.

Step 3 : Hasil Burp Suite Communitiy Edition setelah dilakukan modifikasi kode program.

Gambar 14. *Response* dari *intruder* setelah modifikasi kode program



Perbandingan pada hasl dan pembahasan terkait modifikasi kode program untuk menutup *vulnerability* / kerentanan pada Sistem Informasi Akuntansi dan Manajemen Bisnis webERP.

Tabel 1. Hasil & Pembahasan modifikasi program

Kode Program	Sebelum penambahan kode program	Sesudah penambahan kode program
CollectiveWorkOrderCost.php	Menampilkan informasi pada table tertentu melalui &Submit=&WO_1)union/**/select/**/null,(select/**/group_concat(userid)/**/from/**/www_users),null,null,null,null,(null=on	1*Exception* : *Invalid work order number* tampil karena karakter yang tidak diizinkan pada kode program

Setelah dilakukan modifikasi program pada Gambar 12 maka *vulnerability* / kerentanan pada kode program CollectiveWorkOrderCost.php sudah tidak ditemukan dan kode sudah dapat digunakan di *environment production*.

Kesimpulan

Untuk mencegah dari *script* SQL injection pada webERP 4.15 yang tertera pada CVE-2018-19435 dengan deskripsi ***An issue was discovered in the Manufacturing component in webERP 4.15. CollectiveWorkOrderCost.php has Blind SQL Injection via the SearchParts parameter*** perlu di lakukan modifikasi program pada *script* CollectiveWorkOrderCost.php sehingga script SQL *injection* tidak bisa diterapkan lagi pada kode program CollectiveWorkOrderCost.php.

Selain kode program CollectiveWorkOrderCost.php yang ditemukan *vulnerability* / kerentanan penelitian selanjutnya perlu dilakukan pengetesan terhadap kode program lain yang ada pada webERP untuk lebih meningkatkan aspek keamanan disertakan perhitungan *Measurement* pada *Access Controllability* sesuai rumusan yang ada pada ISO/IEC 25010.

Daftar Referensi

Aghaei, E., Shadid, W., & Al-Shaer, E. (2020). ThreatZoom: Hierarchical neural network for CVEs to CWEs classification. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, *335*. https://doi.org/10.1007/978-3-030-63086-7_2

Ally, S. (2014). Security Vulnerabilities of the Web Based Open Source Information Systems: Adoption Process and Source Codes Screening. *Huria: Journal of the Open University of Tanzania*, *17*(1), 1–13.

Barletta, V. S., Caivano, D., Colizzi, L., Dimauro, G., & Piattini, M. (2023). Clinical-chatbot AHP evaluation based on "quality in use" of ISO/IEC 25010. *International Journal of Medical Informatics*, *170*. https://doi.org/10.1016/j.ijmedinf.2022.104951

Chen, S. J., Pan, Y. C., Ma, Y. W., & Chiang, C. M. (2022). The Impact of the Practical Security Test during the Software Development Lifecycle. *International Conference on Advanced Communication Technology, ICACT*, *2022-February*. https://doi.org/10.23919/ICACT53585.2022.9728868

Das, S. S., Serra, E., Halappanavar, M., Pothen, A., & Al-Shaer, E. (2021). V2W-BERT: A Framework for Effective Hierarchical Multiclass Classification of Software Vulnerabilities. *2021 IEEE 8th International Conference on Data Science and Advanced Analytics, DSAA 2021*. Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/DSAA53316.2021.9564227

Echefunna, C. C., Osamor, J., Iwendi, C., Owoh, P., Ashawa, M., & Philip, A. (2024). Evaluation of Information Security in Web Application Through Penetration Testing Techniques Using OWASP Risk Methodology. *2024 International Conference on Advances in Computing Research on Science Engineering and Technology (ACROSET)*, 1–21. IEEE. https://doi.org/10.1109/ACROSET62108.2024.10743903

Fadilah, M. D., & Rochimah, S. (2023). Security Evaluation of Insurance Portal Agency Information System Based on ISO/IEC 25010 Quality Standard Utilizing OWASP ZAP. *2023 3rd International Conference on Intelligent Cybernetics Technology and Applications, ICICyTA 2023*, 352–357. Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ICICyTA60173.2023.10428701

Fauzan, R. (2015). Pemanfaatan Web-Erp Untuk Sistem Informasi Akutansi Di Perusahaan. *Jurnal Teknologi Dan Informasi (JATI)*.

Githa Hidayat, R., Nuryasin, I., & Suharso, W. (2020). Implementasi Sistem Informasi Penjualan dan Persediaan Menggunakan webERP Pada Cribo Inc Malang. *REPOSITOR*, *2*(8), 1067–1074. Retrieved from www.weberp.org.

Martono, A. (2012). *E-Business ERP (Enterprise Resources Planning) untuk Kompetisi Bisnis* (Vol. 3). Retrieved from www.catcha.com,

Nuryanti, A., & Satria, F. (2023). Analisis Faktor Pendorong Nasabah Perbankan Melakukan Transaksi Digital Menggunakan Mobile Banking. *Journal of Comprehensive Science (JCS)*, *2*(12). https://doi.org/10.59188/jcs.v2i12.557

Oriol, M., Marco, J., & Franch, X. (2014). Quality models for web services: A systematic mapping. *Information and Software Technology*, Vol. 56. https://doi.org/10.1016/j.infsof.2014.03.012

Sinha, S. (2018). Beginning ethical hacking with Kali Linux: Computational techniques for resolving security issues. In *Beginning Ethical Hacking with Kali Linux: Computational Techniques for Resolving Security Issues*. https://doi.org/10.1007/978-1-4842-3891-2

Sohal, A. S., Gupta, S. K., & Singh, H. (2018). Trust in open source software development communities: A comprehensive analysis. *International Journal of Open Source Software and Processes*, *9*(4). https://doi.org/10.4018/IJOSSP.2018100101

Trenggono, D. H. (2014). Perancangan Sistem Peminjaman Berbasis Web Sebagai Media Layanan di Studio Multimedia SMK 2 Sewon. *Skripsi*, 10–17.