ANALISIS KERENTANAN SISTEM INFORMASI BERBASIS WEBSITE MENGGUNAKAN METODE PENETRATION TESTING

I K.A.O. Ardita[1], I.B.G. Dwidasmara[2], dan I.M. Widiartha.[3]

ABSTRAK

Informasi merupakan aset penting bagi suatu organisasi, informasi harus memiliki perlindungan yang baik dan konsisten. Pentingnya mempertahankan keamanan teknologi informasi dalam suatu organisasi yang terkait dengan sejumlah alasan: 1) mempertahankan keunggulan kompetitif, 2) menjaga nama baik/reputasi, dan 3) memastikan organisasi tegak pada aturan dan hukum yang berlaku, Dalam melakukan pengamanan suatu sistem informasi dapat meberlakukan implementasi dari ISO 27001, ISO 27001 merupakan standar internasional yang dipergunakan sebagai pedoman untuk melakukan uji kemanan sistem informasi. Kegiatan PKL yang yang dilaksanankan pada tanggal 01 Oktober 2021 sampai dengan 30 November 2021, kegiatan ini hanya berfokus pada satu aspek yang di atur pada ISO 27001 yaitu aspek keamanan yang dimana aspek ini dapat diuji menggunakan metode uji kerentanan sistem atau penetration test, uji akan dilakukan pada tiga website yang sering mengalami masalah penyusupan yaitu https://banglikab.go.id/, https://bkdpsdm.banglikab.go.id/, dan https://banglikab.go.id/backoffice. Dapat ditarik kesimpulah bahwa terdapat celah keamnan yang perlu ditangani pada website https://bkdpsdm.banglikab.go.id/ dan https://banglikab.go.id/backoffice.

Kata kunci : Burp suite, Penetration test, Website, Kelemahan, Uji kerentanan

ABSTRACT

Information is an important asset for an organization, information must have good and consistent protection. The importance of maintaining information technology security in an organization is related to a number of reasons: 1) maintaining competitive advantage, 2) maintaining good name/reputation, and 3) ensuring that the organization adheres to applicable laws and regulations. from ISO 27001, ISO 27001 is an international standard that is used as a guide for conducting information system security tests. PKL activities which are carried out on October 1, 2021 until November 30, 2021, this activity only focuses on one aspect regulated in ISO 27001, namely the security aspect where this aspect can be tested using the system vulnerability test method or penetration test, the test will be carried out on three websites that often experience intrusion problems, namely https://banglikab.go.id/, https://bkdpsdm.banglikab.go.id/, and https://banglikab.go.id/backoffice. It can be concluded that there are security gaps that need to be addressed on the websites https://bkdpsdm.banglikab.go.id/ and https://banglikab.go.id/backoffice.

Keywords: Burp suite, Penetration test, Website, Weakness, Vulnerability test

[1] *Informatika, Matematika dan Ilmu Pengetahuan Alam, Universitas Udayana, Bali, Indonesia, aldy.ardita@gmail.com.*
[2] *Informatika, Matematika dan Ilmu Pengetahuan Alam, Universitas Udayana, Bali, Indonesia, dwidasmara@unud.ac.id.*
[3] *Informatika, Matematika dan Ilmu Pengetahuan Alam, Universitas Udayana, Bali, Indonesia, madewidiartha@unud.ac.id.*
Submitted: 7 November 2022 *Revised: 25 November 2022* *Accepted: 27 November 2022*

1. PENDAHULUAN

Informasi merupakan aset penting bagi suatu organisasi, informasi harus memiliki perlindungan yang baik dan konsisten. Pentingnya mempertahankan keamanan teknologi informasi dalam suatu organisasi yang terkait dengan sejumlah alasan: 1) mempertahankan keunggulan kompetitif, 2) menjaga nama baik/reputasi, dan 3) memastikan organisasi tegak pada aturan dan hukum yang berlaku (Hohan, Olaru and Pirnea, 2015).

Dalam menyediakan informasi di suatu website harus ada beberapa syarat yang dipenuhi diantaranya adalah 1) informasi yang disediakan benar, 2) tidak mengandung unsur politik yang bersifat memecah, 3) tidak menyebarkan paham teroris, 4) keamanan suatu website terjamin 5) kerahasiaan data pribadi harus dijaga (Sholikhatin, Setyanto and Luthfi, 2019).

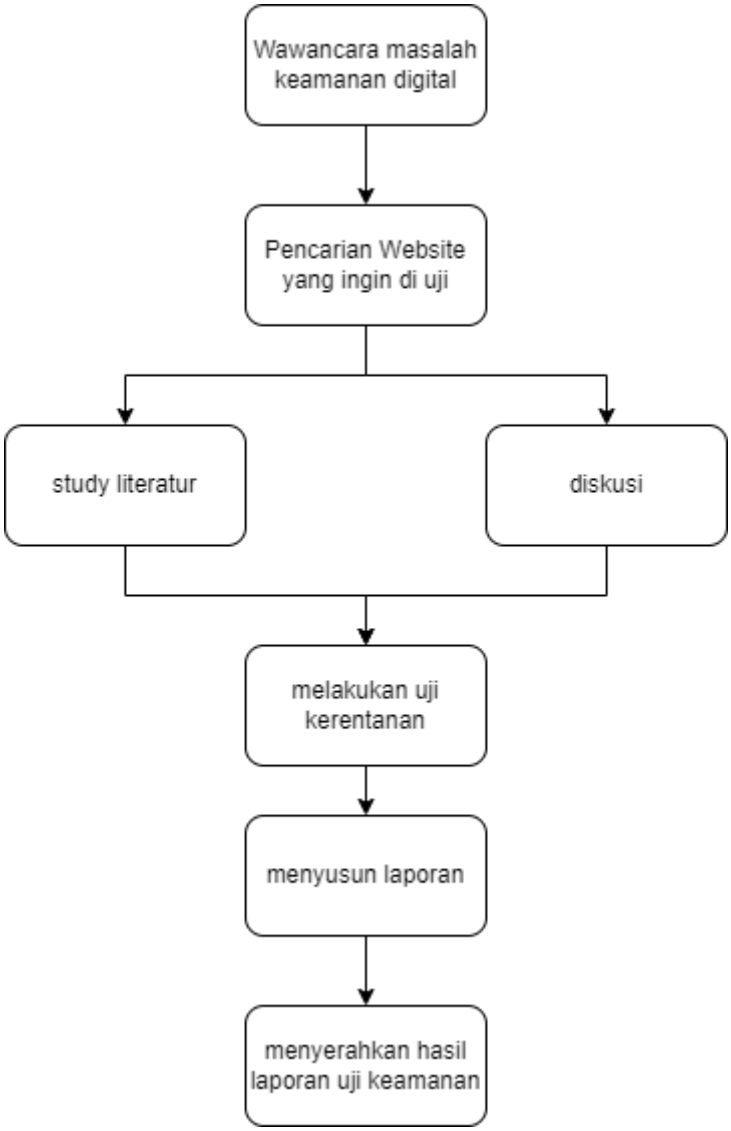
Di Indonesia lalu lintas informasi dan keamanan suatu informasi yang terkait dengan pemerintahan dan negara diatur oleh Kementerian Komunikasi dan Informatika (KOMINFO), seperti yang tertera pada Peraturan Menteri Komunikasi dan Informatika Nomor : 10/PER/M.KOMINFO/07/2010 ketersediaan informasi digital untuk publik disediakan melalui media *website* milik pemerintahan (Kementerian Komunikasi dan Informatika, 2010), Kominfo mengatur seluruh lalulintas informasi dari skala kabupaten oleh sebab itu terdapat masalah keamnan yang berbeda untuk tiap daerahnya.

Dalam melakukan pengamanan suatu sistem informasi dapat meberlakukan implementasi dari ISO 27001, ISO 27001 merupakan standar internasional yang dipergunakan sebagai pedoman untuk melakukan uji kemanan sistem informasi. Uji kemanan perlu dilakukan dikarenakan website milik pemerintahan sangatlah rentan untuk diserang oleh sebab itu harus dilakukan uji pada sistem informasi. Pengujian dapat dilakukan dengan menerapkan uji kerentanan/penetration test, uji ini adalah simulasi dari serangan yang mungkin dilakukan dengan tujuan mengetahui tingkat kelemahan atau celah suatu sistem (Khairina and Harahap, 2018), umumnya serangan yang dilakukan pada saat melakukan penetration test adalah sebagai berikut, brute force, sql injection, dan backdoor. Dalam analisis keamanan situs resmi milik kabupaten bangli digunakan tools burpsuite, tools ini adalah tools bawaan yang dimiliki oleh kali linux tools ini dapat digunakan untuk melakukan serangan secara manual.

2. MATERI DAN METODE

2.1. Metode

Dalam pelaksanaan kegiatan PKL di KOMINFOSAN kabupaten bangli, menggunakan pendekatan kualitatif yang diawali dengan melakukan wawancara pada karyawan mengenai masalah yang sering terjadi pada sistem informasi (*website*) yang dimiliki pemerintahan kabupaten bangli. Metode pada pengabdian ini dapat dilihat pada gambar 1.



Gambar 2.1. Pelaksanaan kegiatan PKL

Kegiatan awal yang di lakukan adalah melakukan wawancara dengan pegawai yang ditunjuk menjadi admin *website* resmi milik pemerintah kabupaten Bangli, tahapan awal ini ditujukan untuk mendapatkan daftar *website* yang penting dan sering menjadi target serangan bagi para oknum yang tidak bertanggung jawab. Kegiatan selanjutnya adalah melakukan studi literatur yang dapat dijadikan pedoman untuk melakukan uji kerentanan *website* resmi milik kabupaten Bangli, selain melakukan studi literatur kegiatan ini juga di barengi dengan melakukan diskusi dengan pihak *developer website* resmi milik kab Bangli, hal ini bertujuan memudahkan tahapan analisis yang akan dilakukan pada *website* dan diberikan hak untuk melihat *database* yang ada pada server. Tahap ketiga yaitu tahapan uji kerentanan sistem. Terakhir adalah penyusunan laporan yang berupa *risk management.* Kegiatan ini dilakukan dengan menggunakan sistem oprasi linux dan tools Burpsuite, Menurut Onno W. Purbo dalam (Purbo, 2020) dijelaskan bahwa Burpsuite merupakan tools grafis yang ditujukan untuk melakukan uji kerentanan pada suatu aplikasi web.

2.2. ISO 27001

ISO 27001 merupakan standar keamanan infomasi internasional yang dapat dijadikan pedoman untuk mengatur keamanan suatu informasi (Nqa, 2013), sistem keamanan yang di atur oleh ISO 27001 diantaranya meliputi beberapa aspek adalah:

1. Kerahasiaan – memastikan bahwa informasi tertentu hanya dapat diakses oleh mereka yang berhak atau memiliki wewenang untuk memperolehnya
2. Integritas – melindungi akurasi dan kelengkapan informasi melalui sejumlah metodologi pengolahan yang efektif
3. Ketersediaan – memastikan bahwa informasi terkait dapat diakses oleh mereka yang berwenang sesuai dengan kebutuhan

2.3. Bruteforce

Brute Force adalah serangan di mana kata sandi dibobol dengan mencoba setiap kata sandi sampai kata sandi yang benar ditemukan (Stiawan *et al.*, 2017).

2.4. Sql injection

Injeksi SQL adalah kerentanan keamanan dalam aplikasi berbasis database yang digunakan untuk menyerang kerentanan keamanan (Dalalana Bertoglio and Zorzo, 2017).

2.5. Backdoor

Backdoor adalah cara untuk mengakses suatu sistem, aplikasi, atau jaringan tanpa harus menangani proses otentikasi.

3. HASIL DAN PEMBAHASAN

Kegiatan PKL yang yang dilaksanankan pada tanggal 01 Oktober 2021 sampai dengan 30 November 2021, kegiatan pkl ini berfokus pada masalah seringnya terjadinya penyusupan oleh orang yang tidak bertanggung jawab ke *website* resmi milik kabupaten Bangli, hal ini mengakibatkan terjadinya keraguan terhadap keamnan sistem iformasi tersebut.

Pada pelaksanaanya kegiatan ini hanya berfokus pada satu aspek yang di atur pada ISO 27001 yaitu aspek keamanan yang dimana aspek ini dapat diuji menggunakan metode uji kerentanan sistem atau penetration test, uji akan dilakukan pada tiga website yang sering mengalami masalah penyusupan yaitu https://banglikab.go.id/, https://bkdpsdm.banglikab.go.id/, dan https://banglikab.go.id/backoffice.

3.1. Rincian Kegiatan

Dalam melakukan pelaksanaan kegiatan PKL di KOMINFOSAN Kab. Bangli terdapat beberapa kegiatan diantaranya:

1. Melakukan sesi wawancara dengan admin *website* dan mencatat *website* yang sering di incar oleh oknum yang kurang bertanggung jawab.
2. Mempelajari ISO 27001 dan menyiapkan tools yang akan digunakan dalam uji kerentanan sistem.
3. Diskusi dengan pihak *developer website* agar diberikan akses super admin website.
4. Analisis website yang sering mengalami masalah keamanan.
5. Menyusun laporan risk management dan menyerahkan laporan ke pihak KOMINFOSAN.

3.2. Analisis *website*

Pada laman ini tidak dapat dilakukan analisis karena laman ini hanya dilakukan menampilkan isi dari website tanpa adanya proses upload.

Tabel 3.1 Hasil analisis website

No	URL	Tingkat ketahanan terhadap simulasi serangan			keamanan
		Bruteforce	Sql injection	Backdor	
1	https://banglikab.go.id/	Baik	Baik	Baik	Keamanan web ini sangat baik
2	https://bkdpsdm.banglikab.go.id/	Tidak baik	Tidak baik	Tidak baik	Tingkat keamnan web ini kurang baik
3	https://banglikab.go.id/backoffice	Tidak baik	Baik	Tidak baik	Tingkat keamnan web ini kurang baik

Dari tabel diatas diketahui bahwa dua website memiliki tingkat keamnana yang perlu di tingkatkan dan menjadi perhatian, dalam ISO 27001 dikatakan bahwa aspek keamnan adalah aspek dimana suatu informasi harus dapat diakses oleh orang yang terautentifikasi atau orang yang memiliki akses (Nqa, 2013), pada website yang di uji pada PKL kali ini hal tersebut belum tercapai dikarenakan website diatas masih terdapat celah keamanan yang dapat ditembus dengan metode serangan pada tabel 3.1.

3.3. Respon mitra

Dalam menanggapi hasil analaisis *website* milik Kab. Bangli Dinas KOMINFOSAN mengambil tindakan dengan melakukan pengajuan untuk melakukan pnyempuraan website dan akan melakukan perubahan pada website kedepannya.

4. KESIMPULAN

Dari hasil pengabdian diatas dapat ditarik kesimpulan bahwa terdapat celah keamnan yang perlu ditangani pada website https://bkdpsdm.banglikab.go.id/ dan https://banglikab.go.id/backoffice, dengan adanya celah kerentanan pada website diatas oknum yang tidak bertanggung jawab dapat dengan mudah melakukan *hacking* atau peretasan terhadap data pribadi atau data penting yang ada pada website, selain itu website akan dengan mudah dibajak oleh oknum yang tidak bertanggung jawab.

UCAPAN TERIMA KASIH

Penulis mengucapkan terimakasih kepada prodi informatika, fakultas matematika dan ilmu pengetahuan alam, universitas udayana karena telah memberikan kesepatan untuk mengikuti kegiatan Praktek Kerja Lapangan (PKL) tahun 2021 dan kepada Dinas Komunikasi Informatika Dan Persandian Kabupaten Bangli yang telah menerima dan membimbing dalam proses PKL selama dua bulan.

DAFTAR PUSTAKA

Dalalana Bertoglio, D. and Zorzo, A. F. (2017) 'Overview and open issues on penetration test', *Journal of the Brazilian Computer Society*, 23(1), pp. 1–16. doi: 10.1186/s13173-017-0051-1.

Hohan, A. I., Olaru, M. and Pirnea, I. C. (2015) 'Assessment and Continuous Improvement of Information Security Based on TQM and Business Excellence Principles', *Procedia Economics and Finance*, 32(15), pp. 352–359. doi: 10.1016/s2212-5671(15)01404-5.

Kementerian Komunikasi dan Informatika (2010) 'Peraturan Menteri Komunikasi dan Informatika Nomor : 10/PER/M.KOMINFO/07/2010'. Available at: https://jdih.kominfo.go.id/produk_hukum/unduh/id/256/t/peraturan+menteri+komunikasi+dan+informatika+nomor+10permkominfo072010+tanggal+12+juli+2010.

Khairina, N. and Harahap, M. K. (2018) 'Menjaga Kerahasiaan Data dengan Steganografi Kombinasi LSB-2 dengan LSB-3 Dan Chess Board Pattern', *SinkrOn*, 3(1), p. 286. doi: 10.33395/sinkron.v3i1.217.

Nqa (2013) *ISO 27001:2013*.

Purbo, O. W. (2020) *Burp Suite*. Available at: https://id.wikipedia.org/wiki/Onno_W._Purbo.

Sholikhatin, S. A., Setyanto, A. and Luthfi, E. T. (2019) 'Analisis Keamanan Sistem Informasi Dengan ISO 27001 (Studi Kasus: Sistem Informasi Akademik Universitas Muhammadiyah Purwokerto)', *It Cida*, 4(1), pp. 1–9. Available at: http://journal.amikomsolo.ac.id/index.php/itcida/article/view/75.

Stiawan, D. *et al.* (2017) 'Cyber-attack penetration test and vulnerability analysis', *International Journal of Online Engineering*, 13(1), pp. 125–132. doi: 10.3991/ijoe.v13i01.6407.