J-ICON, Vol. 11 No. 1, Maret 2023, pp. 91~95
DOI: 10.35508/jicon.v11i1.9809

PENGUJIAN PENETRASI PADA WEBSITE ELEARNING2.BINADARMA.AC.ID DENGAN METODE PTES (*PENETRATION TESTING EXECUTION STANDARD*)

Rahmat Novrianda Dasmen[1], Rasmila[2], Tantri Langgeng Widodo[3], Kundari[4], dan Muhammad Tio Farizky[5]

[1,2,3,4,5] Program Studi Teknik Komputer Fakultas Vokasi Universitas Bina Darma Palembang, Indonesia
[1]Email: rahmat_novrianda@binadarma.ac.id
[2]Email: rasmila@binadarma.ac.id
[3]Email: tantrilanggengwidodo@gmail.com
[4]Email: kundarikun01@gmail.com
[5]Email: tiofarizky@gmail.com

ABSTRAK

Universitas Bina Darma merupakan salah satu kampus swasta terbaik yang menyediakan sistem pembelajaran dalam jaringan (daring) berbasis *website*. Dengan meningkatnya distribusi informasi secara daring di era pandemi Covid-19 dan tingginya antusiasme peserta didik dalam pembelajaran daring, maka sangat penting bagi Universitas Bina Darma untuk memperhatikan keamanan *website* sistem informasi yang digunakan untuk melindungi data pengguna. Adapun tujuan yang ingin dicapai pada penelitian ini adalah untuk mengimplementasikan pengujian penetrasi dengan metode *Black Box* dan metode *Penetration Testing Execution Standard* (PTES) pada *website* elearning2.binadarma.ac.id. Metode PTES dapat digunakan sebagai panduan standar untuk menilai keamanan aplikasi berbasis *web* yang terdiri dari 5 tahap, yang terdiri dari pengumpulan informasi, pemodelan ancaman, analisis kerentanan, eksploitasi, dan pelaporan. Pada akhir penelitian, dapat disimpulkan bahwa pengujian pada elearning2binadarma.ac.id teridentifkasi memiliki celah pada *Cross Site Scripting* (XSS) yang cukup berbahaya jika menyebar lebih jauh. Adapun cara penanganan celah ini dapat dilakukan dengan pengecekan kerentanan *website* secara rutin.
Kata kunci: Pengujian penetrasi, Website, E-Learning, PTES

ABSTRACT

Bina Darma University is one of the best private campuses that provides a website-based online learning system. With the increasing distribution of information online in the era of the Covid-19 pandemic and the high enthusiasm of students in online learning, it is very important for Bina Darma University to pay attention to the security of the information system website used to protect user data. The goal to be achieved in this research is to implement penetration testing with the Black Box method and the PTES method on the elearning2.binadarma.ac.id website. The PTES method can be used as a standard guide for assessing web-based application security which consists of 5 stages, which consist of information gathering, threat modeling, vulnerability analysis, exploitation, and reporting. At the end of the research, it can be concluded that testing on elearning2binadarma.ac.id was identified as having a loophole in Cross Site Scripting (XSS) which is quite dangerous if it spreads further. The way to handle this gap can be done by checking website vulnerabilities regularly.
Keywords: Penetration Testing, Website, E-Learning, PTES

1. PENDAHULUAN

Kemajuan dunia teknologi informasi yang semakin melesat maju, kebutuhan mekanisme dan konsep belajar mengajar berbasis IT tentunya tak terelakan bagi yang memerlukan sebuah keamanan pada sistem. Hal ini yg menciptakan konsep dengan *e-learning* membawa dampak positif yakni mengubah pola pendidikan konvensional menuju daring [1]. Pembelajaran pada mode *e-learning* tentu saja memiliki data yang disimpan, pada proses tersebut membuktikan bahwa adanya kegiatan *upload* dan *download* mahasiswa, pentingnya data tersebut tentu perlu diterapkan pengujian keamanan yakni dengan pengujian penetrasi untuk mengetahui tingkat kerentanan agar terhindar dari pihak yang bertanggung jawab.

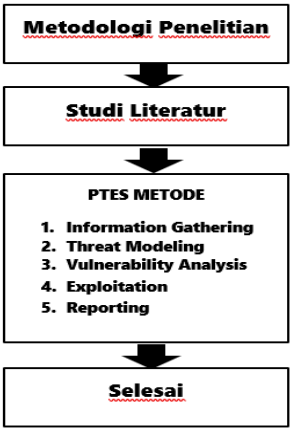
Keamanan informasi merupakan suatu praktik, atau tahapan yang dirancang dan diimplementasikan untuk melindungi suatu informasi atau data pribadi melalui akses, penggunaan, penyalahgunaan, gangguan, atau modifikasi yang tidak valid. *Website* merupakan halaman informasi yang didapatkan via internet sehingga bisa diakses oleh seluruh dunia selama masih terkoneksi dengan internet.

ISSN: 2337-7631 (Printed)
ISSN: 2654-4091 (Online)

Keamanan dalam suatu sistem tentunya sangat dibutuhkan untuk menjaga integritas data yang terkandung dalam sistem tersebut [2].

2. MATERI DAN METODE

Metode penelitian merupakan suatu cara atau teknik untuk memperoleh informasi dan sumber data yang akan digunakan pada penelitian. Selain itu, metodologi penelitian juga dapat diperoleh melalui media daring ataupun elektronik. Adapun tahapan-tahapan metode penelitian yang dilakukan peneliti dapat dilihat pada Gambar 1. PTES adalah cara melakukan *pentesting* dengan target serta tujuan untuk mengeksploitasi sistem [3]. Pengumpulan informasi (*information gathering*) merupakan cara untuk mengumpulkan data dan informasi sesuai target yg dicari. Semua data diambil melalui fase ini akan memeberikan kontribusi untuk dijadikan panduan dalam evaluasi kemungkinan kerentanan. Pemodelan ancaman (*threat modelling*) adalah tahapan dimana peneliti akan menggunakan model ancaman yang paling sesuai sebagai tahapan tes yang wajib dilakukan. Analisis kerentanan (*vulnerability analysis*) adalah tahap dimana peneliti melakukan sebuah analisis kerentanan pada *website* yang diuji. Eksploitasi (*exploitation*) adalah tahap dimana peneliti melakukan serangan pada target secara efektif untuk mengeksploitasi sistem elearning2.binadarma.ac.id. Dengan tahapan ini akan melakukan serangan berdasarkan tahapan sebelumnya. Laporan (*reporting*) merupakan cara *pentester* menggunakan laporan untuk menjelaskan hasil mengenai *pentesting* yang telah dilakukan.

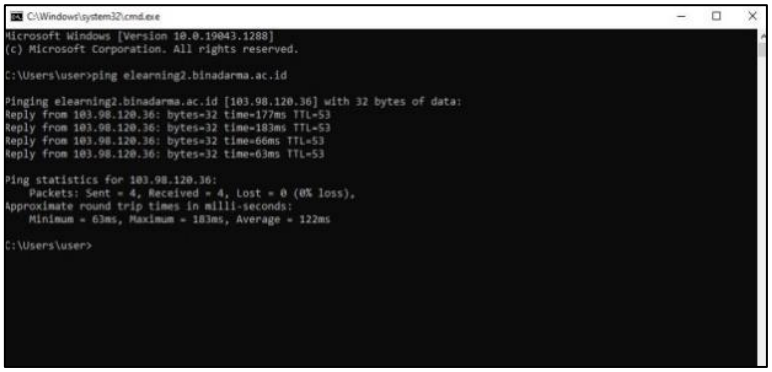


Gambar 1. Metode Penelitian

3. HASIL DAN PEMBAHASAN

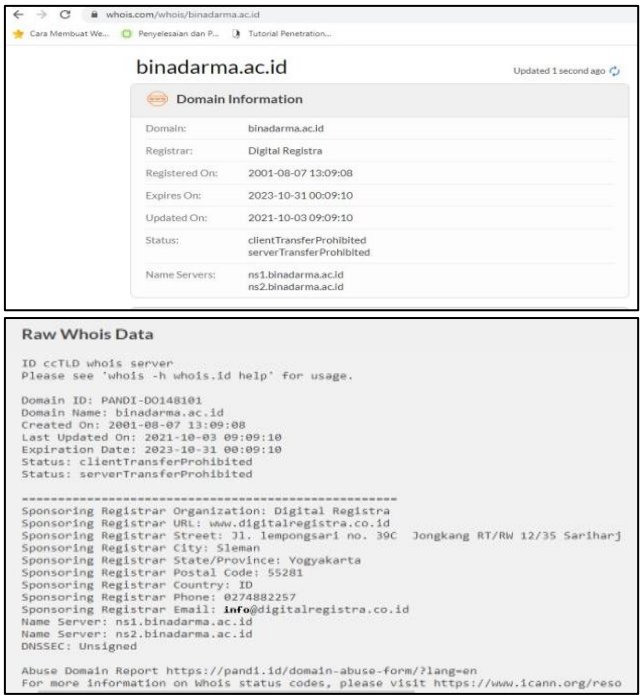
Information Gathering

Pada tahapan ini peneliti melakukan pengumpulan data berupa informasi *website*, *Internet Protocol* (IP) *address*, *server*, hostingan, jenis domain, *Domain Name System* (DNS) dan informasi lainnya yang berguna untuk pengujian penetrasi. Pada tahapan ini penguji melakukan pengecekan IP *address website* melalui *comand prompt windows*, seperti yang ditampilkan pada Gambar 2. IP tersebut dipakai untuk mencari info selanjutnya yaitu dengan Whois dan Reverse IP dari elearning2.binadarma.ac.id. Whois merupakan sebuah website yang digunakan untuk menemukan indentitas sebuah IP Address pada *domain name* sebuah *website* [4]. Hasil pengecekan pada Whois ditampilkan data seperti yang ditunjukan pada Gambar 3.



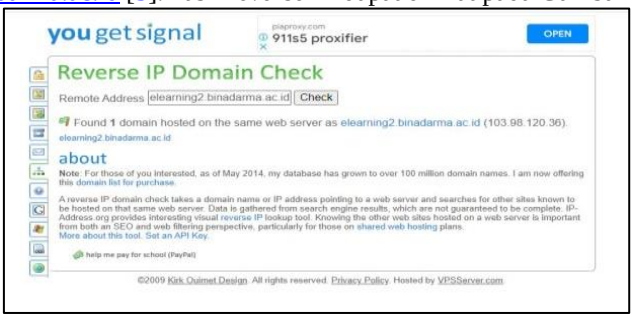
Gambar 2. Pengecekan IP pada *Command Prompt*

ISSN: 2337-7631 (Printed)
ISSN: 2654-4091 (Online)



Gambar 3. Pengecekan Whois pada *website* binadarma.ac.id

Jumping server merupakan aksi penyerang untuk melakukan lompatan/pemindahan dari satu direktori ke direktori yang lain yang berada pada satu *server*, yang selanjutnya diteruskan dengan tahapan *reverse* IP *lookup* yang digunakan untuk memutar balik IP *Address* dengan tujuan mengetahui sub-domain dari *website* elearning2binadarma.ac.id [5]. hasil *reverse* IP dapat dilihat pada Gambar 4.



Gambar 4. Pengecekan *reverse* IP

Thread Modeling

Pada tahapan ini, peneliti menentukan model ancaman yang harus diidentifikasi pada *website* target. Peneliti menggunakan OWASP *Testing Guide* 2017 [6]. Dari tahapan diatas kemungkinan penguji akan mencoba hanya 1 sample saja dari threat modeling OWASP yang digunakan sesuai dengan hasil *vulnerability analysis* nanti.

Vulnerability Analysis

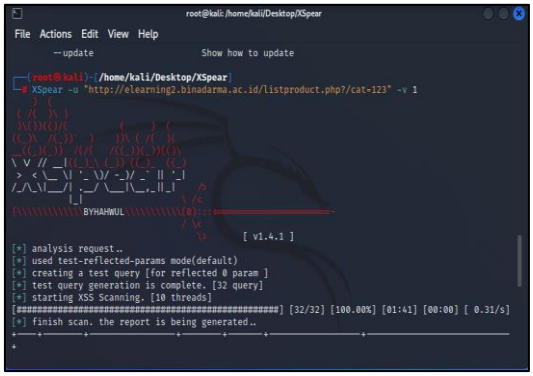
Pada tahapan ini adalah tahapan untuk mendapatkan informasi yang lebih baik. *Tools* yang digunakan yaitu Nikto karena merupakan bagian dari *vulnerability analysis* yang berfungsi menguji kerentanan pada suatu *website*. Pada Gambar 5, dapat dilihat perintah yang digunakan yakni nikto–h elearning2.binadarma.ac.id –ssl–Tuning 9 yang dimaksudkan agar Nikto melakukan *scanning host* secara keseluruhan pada elearning2.binadarma.ac.id menggunakan *Secure Socket Layer* (SSL) [7]. Setelah *scanning* selesai dilakukan, dan –Tuning 9 telah melakukan pengecekan fungsi pada *website*, maka dapat diketahui apakah pada *website* tersebut ada indikasi serangan Structured Query Language (SQL) *Injection* atau tidak. Pada hasil *scanning* Nikto, website *e-learning* tersebut terbukti bahwa terdapat celah XSS. XSS merupakan salah satu serangan injeksi *code* yang cara kerjanya yakni memasukan *HyperText Markup Language* (HTML) ke *website*[8].

ISSN: 2337-7631 (Printed)
ISSN: 2654-4091 (Online)

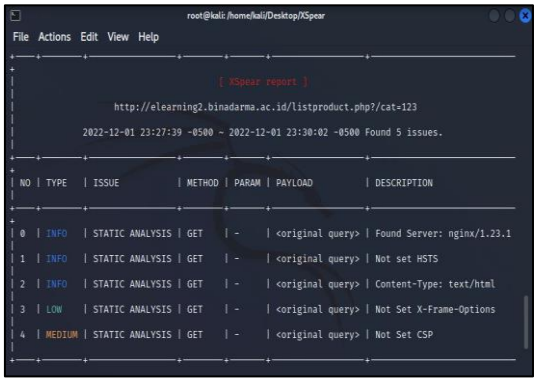
Gambar 5. Hasil *scanning* oleh Nikto

Exploitation

Pada tahap ini, peneliti melakukan serangan pada *website* berdasarkan hasil dari *vulnerability analysis*, yakni terdapat celah pada XSS. Adapun *tool* yang digunakan yakni X-Spear yang merupakan aplikasi *scanner* otomatis untuk *exploitation* pada *website* dengan aman dan mudah digunakan bagi pemula untuk mengeksplorasi kerentanan yang dapat digali pada *website* [9]. Tampilan utama dan hasil *exploitation* dengan X-Spear dapat dilihat pada Gambar 6 dan Gambar 7.



Gambar 6. *Exploitation* dengan X-Spear



Gambar 7. Hasil scanning Exploitation

Reporting

Berdasarkan hasil urutan penelitian diatas terbukti bahwa *website* elearning2.binadarma.ac.id terindikasi memiliki kerentanan XSS yang tentu saja dapat menggangu ekosistem pada *website*. Oleh karena itu pentingnya dilakukan perbaikan dan peningkatan keamanan *website* oleh pihak *back-end* kampus terkait, yang kemudian ditindaklanjutkan dengan pengujian oleh *Quality Assurance Engineer* untuk menvalidasi kemungkinan-kemungkinan yang membuat *website* menjadi *down* karena tentunya akan menggangu kegiatan pengguna sistem [10]. Tabel 1 menunjukan daftar hasil pengujian yang terindikasi XSS *Scripting*.

ISSN: 2337-7631 (Printed)
ISSN: 2654-4091 (Online)

Tabel 1. Hasil penetrasi tingkat kerentanan pada *website* elearning2.binadarma.ac.id

Tipe	Isu	Deskripsi	Level	Persentase
Info	Static Analysis	Not set HSTS	Medium	20%
Low	Static Analysis	Not set X-Frame-Option	Medium	35%
Medium	Static Analysis	Not set CSP	Medium	50%

4. KESIMPULAN DAN SARAN

Setelah peneliti melakukan penelitian singkat, terindikasi bahwa *website* elearning2.binadarma.ac.id memiliki kerentanan yang cukup sedang namun bukan berarti tidak memiliki kerentanan. Terbukti bahwa *website* masih memiliki celah yang dapat disusupi bahkan dimanipulasi oleh pihak yang tidak bertanggung jawab demi keuntungan pribadi. Walaupun *website* elearning2.binadarma.ac.id relatif cukup aman, *website* masih rentan terhadap ancaman karena bisa dieksploitasi oleh XSS.

Adapun saran yang peneliti berikan sebagai masukan pada pemeliharaan *website* agar untuk meningkatkan lagi keamanan tentang kerentanan terhadap serangan pada *website* dan diharapkan metode PTES ini dapat dikembangkan pada *website* elearning2.binadarma.ac.id agar dapat memonitoring atau mencegah serangan yang mungkin akan terjadi terhadap *website*.

DAFTAR PUSTAKA

[1] R. Alexandro, F. Hariatama, and M. Wulandari, "Dampak Positif E-learning pada Pendidikan," *J. Imiah Pendidik. dan Pembelajaran*, vol. 6, no. 1, p. 99, 2022, doi: https://doi.org/10.23887/jipp.v6i1.43695.

[2] R. Pramudita, S. Fuada, and N. W. A. Majid, "Keamanan Informasi dalam Suatu Website," *J. Media Inform. Budidarma*, vol. 4, no. 2, p. 309, 2020, doi: http://dx.doi.org/10.30865/mib.v4i2.1934.

[3] S. Utoro, B. A. Nugroho, M. Meinawati, and S. R. Widianto, "Analisis Keamanan Website E-Learning Menggunakan Metode Penetration Testing Execution Standard," *Multinetics*, vol. 6, no. 2, pp. 169–178, 2020, doi: https://doi.org/10.32722/multinetics.v6i2.3432.

[4] M. Kuliah, "Pengenalan Whois sebagai Protokol Informasi Domain pada Website," 2019.

[5] I. G. A. S. Sanjaya, G. M. A. Sasmita, and D. M. S. Arsa, "Evaluasi Tahap Reverse Ip address Pada Metode Penetration Testing Execution Standar," *J. Ilm. Merpati (Menara Penelit. Akad. Teknol. Informasi)*, vol. 8, no. 2, p. 113, 2020, doi: 10.24843/jim.2020.v08.i02.p05.

[6] S. Hidayatulloh and D. Saptadiaji, "Penetration Testing pada Website Menggunakan Open Web Application Security Project (OWASP)," *J. Algoritm.*, vol. 18, no. 1, pp. 77–86, 2021, doi: https://doi.org/10.33364/algoritma/v.18-1.827.

[7] A. M. Akmal, N. Heryana, and A. Solehudin, "Analisis Keamanan Website Menggunakan Nikto Sebagai Metode Vulnerability Analysis," *Al-Irsyad*, vol. 105, no. 2, p. 79, 2017, [Online]. Available: https://core.ac.uk/download/pdf/322599509.pdf.

[8] I. Riadi, R. Umar, and T. Lestari, "Analisis Kerentanan Serangan Cross Site Scripting (XSS) Menggunakan Framework OWASP," *JISKA (Jurnal Inform. Sunan Kalijaga)*, vol. 5, no. 3, pp. 146–152, 2020, doi: https://doi.org/10.14421/jiska.2020.53-02.

[9] Z. A. Anwari, I. G. P. Wedana, J. Deva, K. D. D. Widyaputra, G. A. J. Saskara, and I. M. E. Listartha, "Analisis Kerentanan Pada Suatu Website Menggunakan Tools Xspear," *J. Inform. Teknol. dan Sains*, vol. 4, no. 4, pp. 406–412, 2022, doi: https://doi.org/10.51401/jinteks.v4i4.2104.

[10] Y. A. Pohan, "Meningkatkan Keamanan Website Menggunakan Metode Penetration Testing Execution Standar," *J. Sistim Inf. dan Teknol.*, vol. 3, pp. 1–6, 2021, doi: https://doi.org/10.37034/jsisfotek.v3i1.36.

ISSN: 2337-7631 (Printed)
ISSN: 2654-4091 (Online)