ANALISIS KEAMANAN *WEBSITE E-LEARNING* FAKULTAS KESEHATAN UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA MENGGUNAKAN METODE *VULNERABILITY ASSESSMENT*

Mafa Mageta[1], Alfirna Rizqi Lahitani[2], Adkhan Sholeh[3].

INTISARI

Latar Belakang: Kemajuan *website* di Indonesia dipercepat oleh peningkatan pengguna internet dan kebutuhan akan layanan online yang efisien. Hal ini mendukung berbagai sektor, termasuk pendidikan seperti FKES Universitas Jenderal Achmad Yani Yogyakarta (UNJAYA), yang memanfaatkan *website e-learning* untuk fleksibilitas akses. Namun, pertumbuhan ini juga membawa tantangan keamanan siber yang meningkat, seperti serangan *web defacement*. Sektor akademik menjadi sasaran, dengan kasus serangan yang signifikan tercatat setiap tahunnya. Perlindungan data dan evaluasi keamanan secara rutin menjadi kunci untuk melindungi *website*, termasuk implementasi HTTPS pada UNJAYA sebagai langkah awal peningkatan keamanan.

Tujuan: Penelitian ini bertujuan untuk dapat menemukan dan mengetahui potensi kerentanan yang ada pada *website e-learning* Fakultas Kesehatan (FKES) Universitas Jenderal Achmad Yani Yogyakarta (UNJAYA).

Metode Penelitian: Penelitian ini dilakukan dengan metode *Vulnerability Assessment* yang berpusat pada tahap *Footprinting* dan *Vulnerability Scanning* untuk melakukan evaluasi kerentanan. Target penelitian ini adalah *website e-learning* FKES UNJAYA, yang akan dites kerentanannya menggunakan alat dan aplikasi pemindaian kerentanan untuk mendapatkan informasi tentang kerentanan tersebut.

Hasil: Hasil pemindaian pada *website e-learning* menunjukkan hanya ada satu kategori tingkat kerentanan, yaitu *Info*. Kategori ini mengindikasikan risiko minimal dengan tidak ada kerentanan yang memiliki dampak signifikan pada *website* tersebut dan sekedar memberikan informasi dari pemindaian yang dilakukan. Meskipun kategori *Info* cukup aman dan tidak dianggap berbahaya secara langsung, namun tetap penting untuk diperhatikan.

Kesimpulan: Nessus memberikan rekomendasi solusi untuk 4 jenis *output*, seperti HSTS *Missing from* HTTPS Server, *Missing or Permissive Content-Security-Policy frame-ancestors* HTTP *Response Header*, *Missing or Permissive X-Frame-Options* HTTP *Response Header* dan Adanya port yang terbuka (Nessus SYN *scanner*).

Kata-kunci: *Website, E-learning, Vulnerability Assessment,* Nessus, dan Nmap

SECURITY ANALYSIS OF E-LEARNING WEBSITE OF FACULTY OF HEALTH, UNIVERSITY OF JENDERAL ACHMAD YANI YOGYAKARTA USING VULNERABILITY ASSESSMENT METHOD

Mafa Mageta[1], Alfirna Rizqi Lahitani[2], Adkhan Sholeh[3].

ABSTRACT

***Background**: The advancement of websites in Indonesia is accelerated by the increasing number of internet users and the demand for efficient online services. This supports various sectors, including education such as FKES Universitas Jenderal Achmad Yani Yogyakarta (UNJAYA), which utilizes e-learning websites for access flexibility. However, this growth also brings heightened cybersecurity challenges, such as web defacement attacks. The academic sector is a primary target, with significant attack cases recorded annually. Regular data protection and security evaluations are crucial to safeguard websites, including the implementation of HTTPS at UNJAYA as an initial step towards enhancing security.*

***Objective**: This research aims to identify and understand potential vulnerabilities in the e-learning website of the Faculty of Health Sciences (FKES) at Universitas Jenderal Achmad Yani Yogyakarta (UNJAYA).*

***Method**: This research employs the Vulnerability Assessment method focusing on Footprinting and Vulnerability Scanning stages to evaluate vulnerabilities. The target of this study is the e-learning website of FKES UNJAYA, which will undergo vulnerability testing using tools and vulnerability scanning applications to obtain information about these vulnerabilities.*

***Result**: The scanning results on the e-learning website indicate that there is only one category of vulnerability level, which is Info. This category signifies minimal risk with no vulnerabilities having a significant impact on the website, merely providing information from the conducted scan. Although the Info category is quite safe and not considered directly harmful, it is still important to be aware of.*

***Conclusion**: Nessus provided solution recommendations for four types of outputs, such as HSTS Missing from HTTPS Server, Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header, Missing or Permissive X-Frame-Options HTTP Response Header, and the presence of open ports (Nessus SYN scanner).*

***Keywords**: Website, E-learning, Vulnerability Assessment, Nessus, dan Nmap*