BAB V

PENUTUP

5.1 kesimpulan

1. Setelah melakukan uji penetrasi menggunakan metode OWASP TOP 10 terhadap *website* SIM xxx terbukti memiliki 4 celah keamanan yang perlu untuk dilakukan perbaikan guna keamanan *website* SIM xxx kedepannya.

2. Pengujian celah keamanan website SIM(Sistem Informasi Manajemen) dengan Metode OWASP adalah dengan melakukan testing terhadap 10 *standard* keamanan yang ada pada OWASP TOP 10 yaitu *Injection* menggunakan SQL*Map*, *Broken Authentication* menggunakan *hydra*, *Sensitive Data Exposure* menggunakan *Dirb, Broken Access Control* menggunakan *Burpsuite*, XXE (XML *External Entities*) menggunakan *Burpsuite*, *Security Misconfiguration* menggunakan SSL*Scan* dan *Heartbleed Bug,* XXS (*Cross Site Scripting*) menggunakan *script manual* dan *burpsuite, Insecure Deserialization* menggunakan *Burpsuite, Using Components with known vulnerabillities* menggunakan *metasploit framework, insufficient logging and monitoring* menggunakan *Metasploit Framework.*

3. Adapun celah keamanan yang ditemukan adalah *Broken Authentication, Sensitive Data Exposure,* dan *Security Misconfiguration.* Adapun celah lain yang ditemukan namun tidak termasuk dalam TOP 10 keamanan OWASP yaitu *Clickjacking.*

4. Dari hasil yang didapatkan pada bab IV diatas, dapat disimpulkan bahwa metode OWASP TOP 10 efektif dijadikan sebagai standard keamanan untuk melakukan uji penetrasi terhadap suatu *website.* Hal itu disebabkannnya dengan *standard* keamanan yang dimiliki OWASP lengkap dan detail dilihat dari konfigurasi halaman *website* maupun konfigurasi *server*. banyak hasil temuan yang mengacu pada 10 *standard* keamanan OWASP tersebut. Maka dari itu metode OWASP TOP 10 menjadi rekomendasi untuk para *pentester* dalam melakukan uji penetrasi menggunakan Metode OWASP Top 10 2017.

5.2 saran

Berdasarkan hasil temuan dari penelitian ini, diperlukannya melakukan pengujian celah keamanan rutin yang lebih mendalam dan detail lagi terhadap *website* SIM xxx guna mencari kelemahan yang mungkin tidak disadari oleh pihak Tim IT SIM xxx. Adapun saran untuk penelitian selanjutnya lebih disarankan menggunakan *framework* OWASP karena lebih terstruktur dan lebih baik dalam menemukan celah-celah lainnya yang lebih *detail*. Adapan saran dari hasil penelitian berdasarkan hasil temuan penelitian ini untuk pihak Tim IT SIM xxx adalah :

1. *Broken Authentication*

   Untuk menghindari percobaan *BruteForce* dapat dilakukan hal-hal berikut

   1. Buat kombinasi *password* yang rumit
   2. Mengatur *limit login*
   3. Gunakan *captcha*
   4. Manfaatkan *two factor authentication*

2. *Sensitive Data Exposure*

   Perlu dilakukannya pengecekan ulang dan penyetingan yang lebih ketat terhadap direktori *website* SIM xxx guna mengurangi kemungkinan *attacker* dapat memperoleh informasi ataupun data *file sensitve* lainnya yang ada pada *website* SIM xxx.

3. *Security Misconfiguration*

   Pada *port* 443 atau SSL/HTTPS diharapkan untuk *disabled*

4. *Clickjacking*

   Untuk menghindari *Clickjacking attack* dapat dilakukan pencegahan dengan cara, pada sisi *client* dapat ditambahkan *addons no script* dan sementara pada sisi *server* bisa menggunakan *Frame Killer, X frame options***.**

Daftar pustaka

OWASP, ”The ten Most Critical Web Application Security Risk”, The Open Web Application Security Project, 2010. http://www.owasp.org).

OWASP Foundation Team. (2019). OWASP GUIDE. Retrieved from the free and open software security community: https://www.owasp.org/index.php

Kho, Y., & Hernawan, F. Y. (2019). Bug Hunting 101 - Web Application Security Testing. AlFursanID.

Jai Narayan Goel.,B.M.Mehtre, “Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology”. 3rd International Conference on Recent Trends in Computing 2015 (ICRTC2015), University of Hyderabad. India: Elsevier, PP710 – 715, 2015.

Waryanto. (2018, januari 22). Pengertian Website Lengkap dengan Jenis dan Manfaatnya. Retrieved from NIAGAHOSTER Blog:https://www.niagahoster.co.id/blog/pengertianwebsite/#Apa_Itu_Website

Markey. (2019). Web Aplikasi | Pengertian Web Applicationdan Cara Membuatnya. Retrieved from MARKEY:

https://markey.id/development/web-aplikasi-pengertian-webapplication-dan-cara-membuatnya#Pengertian_Web_Aplikasi

PT Cloud Hosting Indonesia. (2015). Pencarian WHOIS Lookup dan DNS Lookup. Retrieved from IDCloudHost: https://idcloudhost.com/whois/

Nmap.org. (2008). Panduan Refensi Nmap. Retrieved from NMAP.ORG: https://nmap.org/man/id/index.html

Sullo, C., & Lodge, D. (2019). Nikto2. Retrieved from CIRT.net: https://cirt.net/Nikto2

Kholiq, I. A. (2017, April 9). CELAH KEAMANAN JARINGAN (Vulnerability). Retrieved from CORETAN SEORANG AMATIR: http://imamfolkharmony.blogspot.com/2017/04/celah-keamananjaringan.html

Vielberth, M. and Pernul, G. (2018) ‘A Security Information and Event Management Pattern’, *Federal Ministry of Education and Research*, 1, pp. 1–12.

Horton Andrew. And Colese Brendan. (2018) . WhatWeb Package Description. Retrieved from WhatWeb | Penetration Testing Tools (kali.org)

Guimaraes Assumpcao, DameleBernardo &Miroslav Stampar. (2006). sqlmap Package Description. Retrieved from sqlmap | Penetration Testing Tools (kali.org)

Hauser, Van & Kessler, Roland. (2017). Hydra Package Description. Retrieved from https://tools.kali.org/password-attacks/hydra

PortSwigger. (2021). Burp Suite Package Description. Retrieved from https://tools.kali.org/web-applications/burpsuite

The Dark Raver. (2016). DIRB Package Description. Retrieved from https://tools.kali.org/web-applications/dirb

Rapid7. (2021). metasploit-framework Package Description. Retrieved from https://tools.kali.org/exploitation-tools/metasploit-framework

Peraturan Perundang-undangan

Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Lembaran Negara Republik Nomor 58 Tahun 2008, Tambahan Lembaran Negara Republik Indonesia Nomor 4843.