Vol. 1, No. 2 - December 2021, Hal. 80-86
DOI: https://doi.org/10.25008/jitp.v1i2.15

Penerapan Keamanan Owasp Terhadap Aplikasi GTFW Pada Website Universitas Battuta

Baginda Harahap
Program Studi Informatika, Fakultas Teknologi, Universitas Battuta
E-mail: profesionalbaginda@gmail.com

Received:	Revised:	Accepted:	Available online:
15.12.2021	21.12.2021	29.12.2021	31.12.2021

Abstract: *In this study, we will test the penetration of GTFW-based applications that have been carried out, then obtain the results as a session management category vulnerability test, namely 3 that did not pass, namely cookie attributes, CSRF, and session timeout, then the vulnerability of the input validation category there was 1 that did not pass, namely stored XSS. The xplorin application has a cookie attribute vulnerability with a Medium vulnerability risk level. The xplorin application has a CSRF vulnerability with a Medium vulnerability risk level. The xplorin application has a session timeout vulnerability with a Low vulnerability risk level. The xplorin application has a stored XSS vulnerability with a Low risk level of vulnerability.*
Keywords*: Owasp Security, GTFW App, Website*

Abstrak: Pada penelitian ini akan menguji penetrasi pada aplikasi berbasis GTFW yang telah dilakukan, kemudian memperoleh hasil sebagai pengujian kerentanan kategori session management yaitu 3 yang tidak lolos adalah cookie attributes, CSRF, dan session timeout, kemudian kerentanan kategori input validation ada 1 yang tidak lolos yaitu stored XSS. Aplikasi xplorin memiliki kerentanan cookie attributes dengan tingkat resiko kerentanan Medium. Aplikasi xplorin memiliki kerentanan CSRF dengan tingkat resiko kerentanan Medium. Aplikasi xplorin memiliki kerentanan session timeout dengan tingkat resiko kerentanan Low. Aplikasi xplorin memiliki kerentanan stored XSS dengan resiko tingkat kerentanan Low.
Kata kunci: Keamanan Owasp, Aplikasi GTFW, Website

1. PENDAHULUAN

Keamanan jaringan tergantung pada kecepatan pengaturan jaringan dalam menindak lanjuti system saat terjadi ganguan. Untuk memperkuat keamanan jaringan komputer dapat diterapkan sistem pendeteksi serangan dalam jaringan komputer. Server sebagai sarana vital untuk menyimpan database, aplikasi dan layanan penting sangat diperlukan sisi keamanannya. Baik dari segi infrastruktur sendiri maupun aplikasi pendukungnya. Diharapkan server terhindar dari hal-hal yang menggangu kinerjanya sehingga pelayanan terhadap *client* berfungsi secara maksimal. Keamanan jaringan komputer sebagai bagian dari sebuah sistem menjadi sangat penting untuk menjaga validitas dan integritas data serta menjamin ketersediaan layanan bagi penggunanya. Suatu serangan ke dalam server jaringan komputer dapat terjadi kapan saja. Baik pada saat administrator yang sedang bekerja ataupun tidak. Dengan demikian dibutuhkan sistem keamanan di dalam server itu sendiri yang mampu mendeteksi langsung.

Namun tanpa meninggalkan aspek keamanan bagi server untuk sebuah web, sistem keamanan yang digunakan adalah salah satu IDS *engine open source* yang dirilis oleh OISF Amerika Serikat. Suricata merupakan perangkat lunak pendeteksi dan sekaligus pencegah gangguan atau Intrusion *Detection and Prevention System* (IDPS) *open source* yang merupakan generasi lanjutan dari IDS/IPS. *(Open Information System Foudation)* organisasi non-profit yang didanai oleh pemerintah

Keamanan web merupakan proses mengamankan aplikasi web dari kerentanan yang memungkinkan pihak yang tidak berwenang dapat mengakses dan memodifikasi data-data dari *website* yang tersimpan secara online. Adanya kerentanan dalam *website* dapat meningkatkan ancaman tersendiri, hal ini memungkinkan penyerang dapat melakukan ekploitasi terhadap sistem. Tujuan keamanan aplikasi adalah kerahasiaan *(confidentiality)*, integritas *(integrity)*, ketersediaan informasi *(availability).* Ketiga konsep ini membentuk apa yang sering disebut sebagai Triad CIA. Ketiga konsep tersebut mewujudkan tujuan keamanan mendasar baik untuk data maupun informasi dan layanan komputasi (William Stallings, 2011). Berdasarkan data laporan kerentanan aplikasi web dari Acunetix tahun 2016, dari 55% aplikasi web setidaknya memiliki 1 kerentanan tingkat tinggi, 84% memiliki 1 kerentanan tingkat sedang dan dalam 12 bulan kerentanan tingkat tinggi naik 9% dari 46% di tahun 2015. *Gamatechno Web Application Framework* merupakan *framework* PHP yang dikembangkan oleh PT Gamatechno Indonesia. Sudah banyak klien yang menggunakan aplikasi GTFW dari bidang akademik, pemerintahan maupun korporasi.

Solusi yang baik untuk menghindari eksploitasi website berbasis GTFW yaitu melakukan analisa celah keamanan dan melakukan pengujian dengan OWASP Testing, yang bertujuan untuk

Vol. 1, No. 2 - December 2021, Hal. 80-86
DOI: https://doi.org/10.25008/jitp.v1i2.15

menemukan kerentanan aplikasi web berbasis GTFW dan mencari solusi yang tepat untuk menutup kerentanan tersebut.

2. METODE

Tujuan penelitian adalah memasang sistem keamanan pada server, karena serangan ke dalam server pada jaringan komputer dapat terjadi kapan saja. Tahapan penelitian ini dimulai dengan menganalisa masalah, mempelajari literatur, menganalisa system, merancang system, mengimplementasikan system dan menguji sistem.

Gambar 1. Metode Pengujian Sistem

2.1. Menganalisa Masalah

Langkah analisis masalah merupakan langkah untuk dapat memahami serta mencari masalah yang telah ditentukan ruang lingkup atau batasannya. Dengan menganalisis masalah yang telah ditentukan tersebut, maka diharapkan masalah dapat dipahami dengan baik.

2.2. Mempelajari Literatur

Studi literatur dilakukan dengan mempelajari buku-buku beberapa sumber jurnal, diktat ilmiah, *website* resmi, majalah dan informasi lain yang ada kaitannya dengan implementasi keamanan *web serve*r dan *database server* menggunakan GTFW pada Linux Mint.

2.3. Menganalisa Sistem

Tahap ini akan dilakukan proses perancangan dan metode analisis terhadap keamanan jaringan komputer serta metode yang digunakan dalam mengatasinya. Pada tahap ini melakukan konfigurasi pada GTFW yang merupakan gambaran dari solusi yang akan dihasilkan, dengan konfigurasi dan rule nya dapat menghasilkan output yang diinginkan yaitu *host* (komputer) aman dari serangan atau penyusup lainnya.

2.4. Mengimplementasikan GTFW

Gamatechno Web Application Framework atau yang lebih familiar disebut GTFW, merupakan framework PHP yang dikembangkan oleh PT Gamatechno Indonesia. Sejak Gamatechno berdiri pada tahun 2005, telah banyak aplikasi berbasis GTFW yang diimplementasikan di ratusan klien pada segmen akademik, pemerintahan maupun korporasi. Gamatechno saat ini menyediakan informasi tentang *framework* ini secara terbuka di laman web dan berusaha terus mengembangkan GTFW dari sisi teknologi dan keamanannya. Dalam proses pengembangan aplikasi, GTFW menggunakan model pendekatan *Model-ViewController* (MVC) kemudian pada GTFW versi 4.0 arsitektur diganti dengan model pendekatan shell aplikasi *(app shell)*. *App shell* adalah metode arsitektur yang memisahkan antara layout dan konten.

GTFW mempunyai 3 komponen yaitu *webapps*, *php-app/api* dan *phpbase*. *webapps* adalah aplikasi *frontend* yang menjadi antar muka pengguna. *phpapp/api* merupakan aplikasi berbasis PHP yang masih mempertahankan model lama dan support *framework* baru. Dan php-base merupakan *framework* berbasis PHP yang didalamnya ada salah satu model *microprocess*, saat ini *php-base* sudah

Vol. 1, No. 2 - December 2021, Hal. 80-86
DOI: https://doi.org/10.25008/jitp.v1i2.15

sampai ke versi 4.0.

2.5. Menguji Sistem

Tahap berikutnya setelah perancangan dan pembangunan sistem adalah pengujian sistem. Hal ini dilakukan untuk melihat sejauh mana Suricata ini mampu memecahkan permasalahan. Pengujian dilakukan dengan metode *port scaning* menggunakan aplikasi NMAP dan *brute force* menggunakan Brutus. Pengujian dilakukan sebelum suricata diaktifkan dan setelah suricata diaktifkan, Hasilnya kemudian dievaluasi apakah sudah sesuai dengan hasil yang dicapai dalam keamanan jaringan komputer.

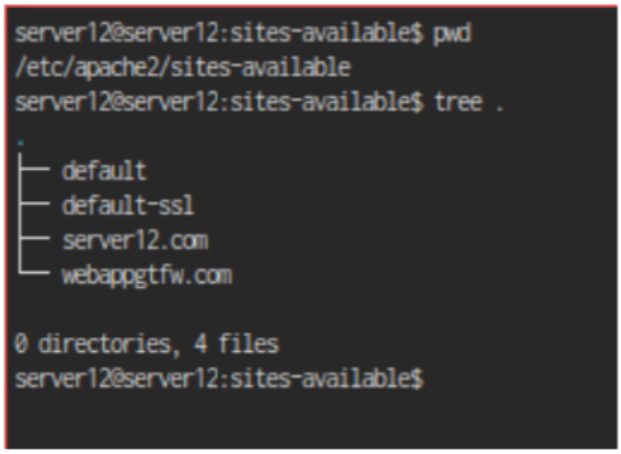
2.5.1. Alat dan Komponen yang digunakan

1. Perangkat keras, perangkat ini terdiri dari :
   - Satu unit computer server, dengan spesifikasi sebagai berikut :
   - Processor Xeon
   - Motherboard DELL
   - Hardisk SATA 500 Giga Byte
   - Memory RAM 4 Giga Byte
   - Ethernet Card RTL 8111/8168B PCI Express Gigabit
   - Switch, menggunakan Dlink DES-1016D
   - Router, menggunakan Mikrotik Router Board 750
   - Wireless, menggunakan TP-LINK 3G/3.75 Wireless Lite N Router
2. *Unit computer* sebagai *client*, dengan spesifikasi sebagai berikut :
   - Minimal processor Pentium Dual core
   - Hardisk ATA 320 Giga Byte
   - Memory RAM 2 Giga Byte
3. *Software*, perangkat ini terdiri dari:
   - Linux Mint
   - PuTTY Versi 0.62
   - Google Chom Client
   - GTFW (*Gamatechno Web Application Framework)*
   - Nmap 5.62
   - Brutus AET2

3. HASIL DAN PEMBAHASAN

Pada hasil dan pembahasan ini akan diperlihatkan seperti apa kinerja dari GTFW terhadap keamana Oasp pada website Universitas Battuta.

1. Membuat alamat domain webappgtfw.com, dengan membuat file baru dengan nama webappgtfw.com di /etc/apache2/sites-available/.



Gambar 2. Direktori Web

Vol. 1, No. 2 - December 2021, Hal. 80-86
DOI: https://doi.org/10.25008/jitp.v1i2.15

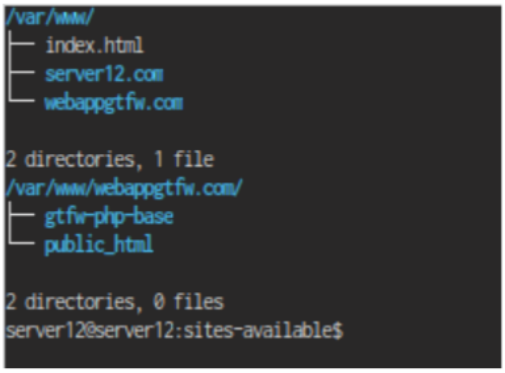
2. Menambahkan konfig file webappgtfw.com, seperti berikut :

```
<VirtualHost *:80>
        ServerAdmin webappgtfw@localhost
        ServerName webappgtfw.com
        ServerAlias www.webappgtfw.com
        DocumentRoot /var/www/webappgtfw.com/public_html
        <Directory />
                Options FollowSymLinks
                AllowOverride None
        </Directory>
        <Directory /var/www/>
                Options Indexes FollowSymLinks MultiViews
                AllowOverride None
                Order allow,deny
                allow from all
        </Directory>

        ScriptAlias /cgi-bin/ /usr/lib/cgi-bin/
        <Directory "/usr/lib/cgi-bin">
                AllowOverride None
                                Options  +ExecCGI  -MultiViews
+SymLinksIfOwnerMatch
                Order allow,deny
                Allow from all
        </Directory>
```

```
        ErrorLog ${APACHE_LOG_DIR}/error.log

          # Possible values include: debug, info, notice, warn,
error, crit,
        # alert, emerg.
        LogLevel warn

        CustomLog ${APACHE_LOG_DIR}/access.log combined

    Alias /doc/ "/usr/share/doc/"
    <Directory "/usr/share/doc/">
        Options Indexes MultiViews FollowSymLinks
        AllowOverride None
        Order deny,allow
        Deny from all
        Allow from 127.0.0.0/255.0.0.0 ::1/128
    </Directory>

</VirtualHost>
```

Gambar 3. Konfig File Webappgtfw.com

3. Buat direktori web di web root website di (/var/www), nama folder webappgtfw.com dan folder public_html di dalam direktori webappgtfw.com. Perintah yang digunakan adalah "mkdir nama_folder" atau "mkdir -p nama_folder/sub_folder", sehingga perintah menjadi "mkdir -p webappgtfw.com/public_html"

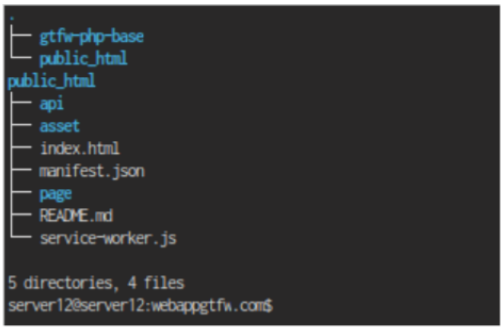


Gambar 4. Direktori we root

4. Jalankan perintah "a2ensite" diikuti dengan nama situs, perintah ini digunakan agar apache dapat mengenali domain yang baru dibuat. Perintah yang dijalankan adalah "sudo a2ensite webappgtfw.com".
5. Restart web service apache dengan perintah "sudo service apache2 restart".

Vol. 1, No. 2 - December 2021, Hal. 80-86
DOI: https://doi.org/10.25008/jitp.v1i2.15

6. Mengkonfigurasi komponen aplikasi xplorin, letakkan komponen gtfwphp-base didalam root folder, kemudian api didalam public_html dan pindahkan semua data file webapps ke dalam folder public_html, sehingga akan menjadi struktur seperti berikut.



Gambar 5. Direktori Aplikasi xplorin

7. Membuat database xplorin, perintah yang digunakan adalah "create database xplorin". Sebelumnya jalankan mysql dan lakukan otentikasi login ke mysql.
8. Konfigurasi database aplikasi, file untuk mengkonfigurasi database ada di /public_html/api/database.php. Ubah data pada "connection 0" dengan database yang sudah dibuat. Seperti pada Gambar 6 berikut.

```
// connection number 0, digunakan base utk mengakses user
$database['db_conn'][0]['db_driv'] = 'default';
$database['db_conn'][0]['db_type'] = 'mysqli';
$database['db_conn'][0]['db_host'] = 'localhost';
$database['db_conn'][0]['db_user'] = 'root';
$database['db_conn'][0]['db_pass'] = 'admin';
$database['db_conn'][0]['db_name'] = 'xplorin';
$database['db_conn'][0]['db_debug_enabled'] = 'true';
```

Gambar 6. Configurasi database

Konfiguarasi selain "connection 0" adalah optional, boleh diisi atau tidak.

9. Mengkonfigurasi file gtfw_base_dir.php, isikan pasth gtfw base pada file tersebut. Sehingga menjadi seperti berikut.
   /var/www/webappgtfw.com/gtfw-php-base
10. Ubahlah nama file di dalam folder "/public_html/api/config" menjadi file .php seperti pada gambar berikut.

Gambar 7. Direktori config

11. Konfigurasi file "gtfw.env.js" yang berada di direktori "/public_html/asset/custom/js ". Ganti menjadi seperti berikut.

```
var gtfwEnvirontment = {
   "server": '/api/', /*Set service/API server base url*/
   "DEVELOPMENT": true };
```

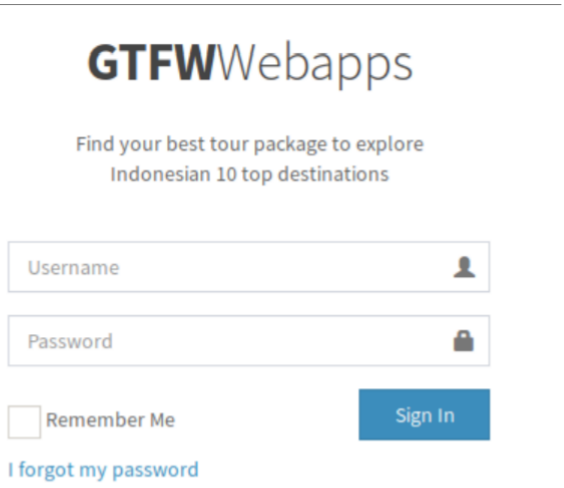
Gambar 8. Config gtfw.env.js

Vol. 1, No. 2 - December 2021, Hal. 80-86
DOI: https://doi.org/10.25008/jitp.v1i2.15

12. Ubah file di dalam direktori "public_html/asset/custom/js" menjadi file Javascript (.js), seperti berikut.

Gambar 9. File config webapps

13. Buka alamat domain webappgtfw.com dari browser, maka akan ditampilkan halaman login dari aplikasi xplorin.



Gambar 10. Halaman login xplorin

4. KESIMPULAN

Berdasarkan pengujian penetrasi pada aplikasi berbasis GTFW terhadap website Universitas battuta yang telah dilakukan dapat disimpulkan bahwa :

1. Pengujian kerentanan kategori session management ada 3 yang tidak lolos yaitu cookie attributes, CSRF, dan session timeout.
2. Pengujian kerentanan kategori input validation ada 1 yang tidak lolos yaitu stored XSS.
3. Aplikasi xplorin memiliki kerentanan cookie attributes dengan tingkat resiko kerentanan Medium.
4. Aplikasi xplorin memiliki kerentanan CSRF dengan tingkat resiko kerentanan Medium.
5. Aplikasi xplorin memiliki kerentanan session timeout dengan tingkat resiko kerentanan Low.
6. Aplikasi xplorin memiliki kerentanan stored XSS dengan resiko tingkat kerentanan Low.
7. Aplikasi xplorin lolos uji dari kerentanan bypassing session management schema, logout functionality, HTTP verb tampering, dan OS command Injection.
8. Aplikasi berbasis GTFW memiliki 4 kerentanan dengan 2 kerentanan memiliki tingkat resiko kerentanan medium dan 2 kerentanan memiliki tingkat resiko kerentanan low.
9. Hasil pengujian dan analisis dengan metode OWASP menunjukkan bahwa manajemen sesi dan validasi input belum diimplementasikan dengan baik.

DAFTAR PUSTAKA

Faris, 'Afif, Muhammad. 2017. Implementasi keamanan Owasp Terhadap Aplikasi Berbasis GTFW. Skripsi. Program Studi Informatika Sekolah Tinggi Manajemen Informatika dan Komputer Akakom. Yogyakarta.

Vol. 1, No. 2 - December 2021, Hal. 80-86
DOI: https://doi.org/10.25008/jitp.v1i2.15

Nazwita. Ramadhani, Siti. 2017. Analisis Sistem Keamanan Web Server dan Database Server Menggunakan Suricata. Jurnal Teknologi Informasi, Komunkasi dan Industri SNTIKI. UIN Sultan Syarif Kasim. Riau.

Bella, Sri Setia. 2012. Membangun Aplikasi Pembelajaran Secure Web Programming Berbasis Owasp Top 10. Skripsi. STMIK AKAKOM. Yogyakarta.

Dr. Raden Teduh Dirgahayu, S.T., M.Sc., Yudi Prayudi, S.Si., M.Kom., dan Adi Fajaryanto. 2015. Penerapan Metode ISSAF dan OWASP versi 4 Untuk Uji Kerentanan Web Server. Universitas Islam Indonesia. Yogyakarta.

Elias Athanasopoulos, Vasileios P. Kemerlis, Michalis Polychronakis, dan Evangelos P. Markatos. 2012. ARC: Protecting against HTTP Parameter Pollution Attacks Using Application Request Caches. Department of Computer Science Columbia University. USA.

Fajri Rahmat, Ary Mazharuddin S., dan Hudan Studiawan. 2013. Sistem Pendeteksi dan Pencegah Peretasan Terhadap Aplikasi Berbasis Web dengan Teknik Web Application Firewall (WAF). Institut Teknologi Sepuluh Nopember (ITS). Surabaya.

OWASP. 2013. OWASP Testing Guide 4. https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_ Contents, 4 Oktober 2016, 08:01 PM WIB.

Symantec. 2016. A New Zero-Day Vulnerability Discovered Every Week in 2015. https://www.symantec.com/content/dam/symantec/docs/infographics/istrzero-day-en.pdf, 4 Oktober 2016, 07:02 PM WIB.

OWASP. 2016. OWASP Risk Rating Methodology. https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology, 9 Agustus 2017, 7:27 AM WIB.

S. Dave, B. Trivedi, and J. Mahadevia, "Application Profiling based on Attack Alert Aggregation,"

Glob. J. Comput. Sci. Technol. Network, Web Secur., vol. 13, no. 16, pp. 20–30, 2013.

W. I. E. Nvironment, "Efficacy Of Attack Detection Capability Of IDPS Based On ITSD Eployment In Wired and Wireless Environtment," Int. J. Netw. Secur. Its Appl., vol. 5, no. 2, pp. 103–115, 2013.

T. Oisf et al., "Known issues & missing features About Suricata," pp. 1–2.

J.M. Kizza (springer-Verlag London), Computer Communications and Networks. 2013.

A. M. R. Wajong, "Kerentanan yang dapat terjadi dijaringan komputer umumnya," ComTech, vol. 3, no. 9, pp. 474–481, 2012.

M. Anif, S. Hws, and M. D. Huri, "Penerapan Intrusion Detection System (IDS) dengan metode Deteksi Port Scanning pada Jaringan Komputer di Politeknik Negeri Semarang," J. Tele, vol. 13, no. Maret, pp. 25–30, 2015.

B. S. Candra, "Analisis Penerapan Keamanan Menggunakan IDN dan Honeypot," Fak. Ilmu Komput., vol. 1, no. Mei, pp. 1–23, 2015.

A. Dan, I. Honeypot, and M. Honeyd, "Analisis dan Implementasi Honeypot menggunakan Honeyd sebagai Alat Bantu Pengumpulan Informasi Aktivitas Serangan pada Jaringan," J. Jarkom, vol. 1,