Implementasi Penetration Test Pada Telkom Iot Platform Di Indonesia Telecommunication & Digital Research Institute (Itdri)

1st Akhmad Ikhtarom Mudin
Fakultas Ilmu Terapan
Universitas Telkom
Bandung, Indonesia
ikhtarommudin@student.telkomuniversity.ac.id

2nd Mochammad Fahru Rizal
Fakultas Ilmu Terapan
Universitas Telkom
Bandung, Indonesia
mfrizal@telkomuniversity.ac.id

***Abstrak* — Keamanan sistem informasi merupakan aspek penting dalam lingkungan teknologi informasi yang berkembang pesat. Ancaman keamanan yang dapat merusak integritas, kerahasiaan, dan ketersediaan data semakin meningkat. Penetration test atau uji penetrasi merupakan salah satu metode yang digunakan untuk menguji keamanan sistem dengan mensimulasikan serangan yang mungkin dilakukan oleh pihak yang tidak berwenang. Penelitian ini bertujuan untuk mengimplementasikan penetration test pada Telkom IoT Platform di Indonesia Telecommunication & Digital Research Institute (ITDRI). Telkom IoT Platform merupakan infrastruktur yang digunakan untuk menghubungkan dan mengelola perangkat Internet of Things (IoT) secara efisien. Metode yang digunakan dalam penelitian ini mencakup analisis sistem, uji penetrasi, dan identifikasi temuan keamanan. Analisis sistem dilakukan untuk memahami infrastruktur dan aplikasi yang terlibat dalam Telkom IoT Platform. Selanjutnya, uji penetrasi dilakukan untuk mencari potensi kerentanan seperti *SQL injection, cross-site scripting (XSS), dan clickjacking*. Dalam konteks yang semakin kompleks dan meningkatnya ancaman keamanan terhadap sistem IoT, penting untuk melakukan pengujian penetrasi guna mengidentifikasi dan mengevaluasi kerentanan keamanan yang mungkin ada dalam platform ini.**

***Kata kunci* — Implementasi, Uji Penetrasi, Telkom IoT Platform, Keamanan Aplikasi Web.**

I. PENDAHULUAN

Internet of Things (IoT) merupakan sebuah invoasi teknologi yang sudah banyak digunakan untuk mengembangkan perangkat menjadi lebih efisien dengan memanfaatkan konektivitas internet. Dalam konteks ini, Telkom IoT Platform hadir sebagai platform yang diproduksi oleh ITDRI (Indonesia Telecommunication Digital Research Institute) yang juga merupakan bagian PT Telkom Indonesia untuk mengelola dan mengintegrasikan perangkat IoT yang terhubung. Namun, semakin banyaknya perangkat yang terhubung meningkatkan risiko keamanan yang harus diatasi.

Pada saat ini, serangan terhadap sistem IoT semakin kompleks dan sering terjadi. Keberhasilan serangan dapat mengakibatkan kerugian finansial yang signifikan, kebocoran data sensitif, atau bahkan mengancam nyawa manusia. Oleh karena itu, sangat penting untuk secara teratur melakukan uji kerentanan atau penetration test pada sistem IoT.

Penelitian ini bertujuan untuk melakukan penetration test pada Telkom IoT Platform untuk mengidentifikasi dan menguji kerentanan yang mungkin ada dalam sistem. Dengan melakukan serangan simulasi dan menganalisis respons sistem, dapat diidentifikasi kerentanan yang perlu diperbaiki. Penelitian ini akan memberikan rekomendasi perbaikan keamanan yang efektif untuk meningkatkan keamanan Telkom IoT Platform.

II. KAJIAN TEORI

A. VMWare Workstation Player 16

VMware Workstation Player adalah aplikasi virtualisasi desktop yang efisien menjalankan sistem operasi lain di komputer yang sama tanpa perlu *reboot*. VMware Workstation Player menyediakan antarmuka pengguna yang sederhana, dukungan sistem operasi yang tak tertandingi, dan portabilitas di seluruh ekosistem VMware [1].

B. Kali Linux

Kali Linux adalah distribusi Linux berbasis Debian yang bersifat *open-source* yang ditujukan untuk penetration testing dan security auditing tingkat lanjut. Kali Linux berisi modifikasi khusus untuk industri serta ratusan *tools* yang ditargetkan untuk berbagai tugas Keamanan Informasi, seperti *Penetration Testing*, *Security Research*, *Computer Forensics*, *Reverse Engineering*, *Vulnerability Management*, dan *Red Team Testing* [2].

C. Nmap

Nmap adalah sebuah *tool open-source* yang biasa digunakan untuk eksplorasi dan audit keamanan jaringan. Alat ini dirancang untuk memeriksa jaringan besar secara cepat, meskipun juga dapat bekerja terhadap *host* tunggal. Dengan menggunakan paket IP raw dan pendekatan yang canggih, Nmap dapat dengan tepat mendeteksi *host-host* yang aktif di dalam jaringan, menyediakan informasi rinci tentang layanan yang berjalan (termasuk aplikasi dan versinya), mengidentifikasi sistem operasi yang digunakan

dan versinya, mengenali jenis firewall atau filter paket yang berlaku, serta menyajikan beragam karakteristik lainnya [3].

D. DIRB

DIRB merupakan *Web Content Scanner*. DIRB berperan sebagai pemindai konten web yang melakukan pencarian terhadap elemen-elemen web yang terbuka atau tersembunyi. Proses kerjanya melibatkan serangan berbasis kamus terhadap server web dan penganalisisan responsnya. Selain itu, DIRB memiliki kumpulan *wordlist* serangan yang telah disiapkan sebelumnya untuk memudahkan penggunaan, namun juga memungkinkan pengguna untuk menggunakan daftar kata kunci yang disesuaikan. Tujuan utama DIRB adalah untuk membantu dalam melakukan audit aplikasi web profesional, terutama pada pengujian yang berkaitan dengan keamanan [4].

E. Sqlmap

Sqlmap digolongkan sebagai perangkat uji penetrasi yang bersifat *open-source*, yang mampu mengotomatisasi proses mendeteksi dan mengeksploitasi kerentanan *SQL injection*, serta mengambil alih *server database*. Perangkat ini dilengkapi dengan mesin deteksi yang terpercaya, fitur-fitur khusus untuk pengujian penetrasi secara maksimal, dan berbagai opsi yang mencakup *fingerprinting database*, pengambilan data dari *database*, akses ke sistem *file* yang mendasari, dan pelaksanaan perintah-perintah pada sistem operasi melalui koneksi *out-of-band* [5].

F. Burpsuite

Burp Suite merupakan *tools* yang komprehensif untuk pengujian keamanan aplikasi web [6]. *Tools* ini dirancang khusus untuk membantu para profesional keamanan dan pengujian dalam mengidentifikasi, memanipulasi, dan memeriksa kerentanan dalam aplikasi web.

G. XSStrike

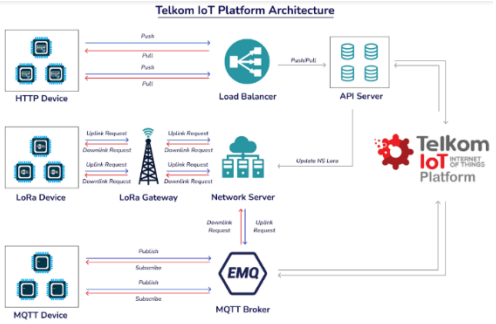
XSStrike adalah sebuah rangkaian alat deteksi *Cross-Site Scripting (XSS)* yang dilengkapi dengan empat *parser* yang ditulis secara manual, *payload generator* yang cerdas, *fuzzing engine* yang kuat, dan *crawler* yang beroperasi sangat cepat. XSStrike melakukan analisis respons menggunakan beberapa *parser* dan kemudian membuat *payload* yang dijamin berfungsi melalui analisis konteks yang terintegrasi dengan *fuzzing engine*. Selain itu, XSStrike memiliki kemampuan *crawling*, *fuzzing*, penemuan parameter, dan deteksi *WAF*. Alat ini juga melakukan pemindaian untuk kerentanan DOM XSS [7].

III. METODE

Pengujian yang dilakukan adalah melakukan *port scanning, direktori scanning, SQL Injection, Cross Site Scripting*, dan *Clickjacking*.

A. Analisis Sistem

Berikut merupakan arsitektur yang digunakan dalam sistem Telkom IoT Platform.



GAMBAR 3. 1
Arsitektur Telkom IoT Platform

Telkom IoT Platform memiliki arsitektur yang terintegrasi untuk menerima data dari berbagai jenis perangkat yang terhubung. Berikut adalah gambaran arsitektur sistem ini.

HTTP device, LoRa device, dan MQTT device adalah tiga jenis perangkat yang terhubung ke Telkom IoT Platform. Setiap jenis perangkat menggunakan jalur komunikasi yang berbeda untuk mengirimkan data ke platform.

B. Analisis Sistem

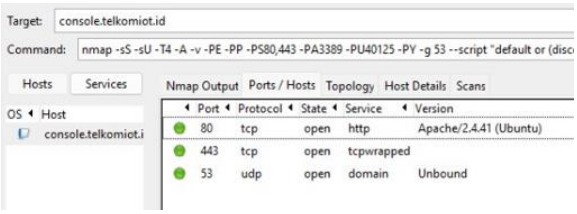
GAMBAR 3. 2
Alur Pengerjaan Penetration Test

IV. HASIL DAN PEMBAHASAN

A. *Scanning Port*

Nmap digunakan untuk melakukan *scanning port* pada Telkom IoT Platform. *Command* yang digunakan untuk *scanning port* adalah “nmap -sS -sU -T4 -A -v -PE -PP -PS80,443 -PA3389 -PU40125 -PY -g 53 --script "default or (discovery and safe)" console.telkomiot.id”. Terdapat tiga port yang terbuka yaitu:

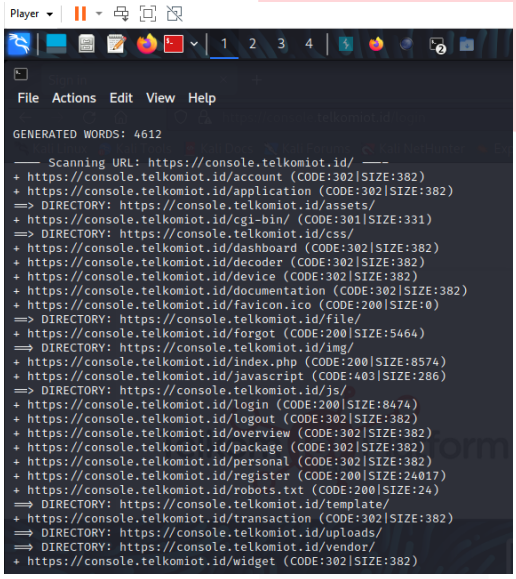
- port 80,
- port 443,
- dan port 53.



GAMBAR 4. 1
Hasil Pengujian Nmap

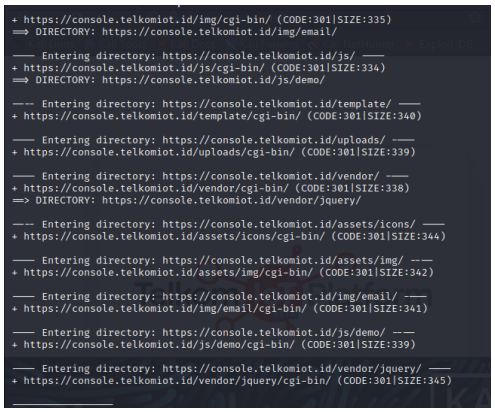
B. *Scanning* Direktori

Scanning direktori dilakukan menggunakan *tools* bernama DIRB dengan tujuan untuk mengetahui dan mengidentifikasi sumber daya (*resource*) yang ada dalam Telkom IoT Platform seperti direktori-direktori maupun juga *file-file* yang terbuka secara publik. Berikut adalah hasil dari *scan* direktori Telkom IoT Platform.



GAMBAR 4. 2
Direktori Scanning

GAMBAR 4. 3
Direktori Scanning



GAMBAR 4. 4
Direktori Scanning

Dari hasil *scan* terdapat beberapa direktori yang teridentifikasi memiliki HTTP status code 200 yang berarti dapat diakses pengguna umum. Beberapa diantaranya adalah:

1. console.telkomiot.id/index.php
2. console.telkomiot.id/login
3. console.telkomiot.id/register
4. console.telkomiot.id/forgot
5. console.telkomiot.id/favicon.ico
6. console.telkomiot.id/robots.txt
7. console.telkomiot.id/template/sampellora.csv
8. console.telkomiot.id/template/sampel-upload-multiple-non-lora.csv
9. console.telkomiot.id/file/lora_upload.csv

Dari beberapa direktori tersebut terdapat beberapa yang mungkin seharusnya tidak dapat diakses pengguna secara umum yaitu pada direktori:

1. console.telkomiot.id/robots.txt
2. console.telkomiot.id/template/sampellora.csv
3. console.telkomiot.id/template/sampel-upload-multiple-non-lora.csv
4. console.telkomiot.id/file/lora_upload.csv

Direktori-direktori tersebut mungkin berisi informasi penting yang mungkin dapat digunakan oleh orang untuk melakukan penyerangan ke sistem.

C. SQL *Injection*

Untuk mencari kerentanan serangan SQL injection dilakukan dengan menggunakan tools sqlmap. *Command* yang digunakan yaitu:

1. sqlmap -u https://console.telkomiot.id/ --level=3 –risk=3,
2. sqlmap -u https://console.telkomiot.id/ --level=5 –risk=3

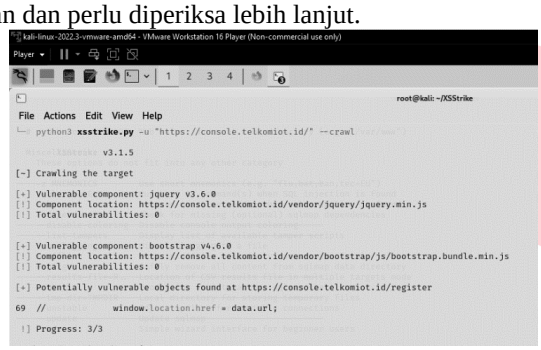
Hasil pengujian menggunakan sqlmap menunjukkan bahwa tidak ditemukan celah atau kerentanan SQL injection pada parameter-parameter yang telah diuji. Kedua *command* yang digunakan menunjukkan hasil yang sama. Seperti yang tertera pada gambar hasil pengujian yang menunjukkan keterangan "*all tested parameters do not appear to be injectable*". Hal ini menunjukkan bahwa Telkom IoT Platform mungkin sudah memiliki mekanisme keamanan yang memadai dan efektif dalam mencegah serangan SQL injection.

D. *Cross Site Scripting*

XSStrike digunakan untuk mencari kerentanan *Cross Site Scripting* pada aplikasi web Telkom IoT Platform. Command

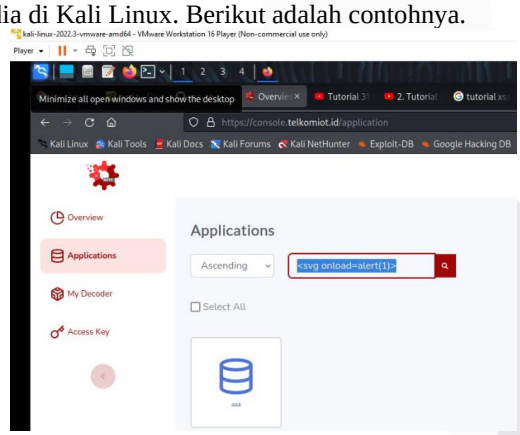
yang kali ini digunakan untuk mencari kerentanan xss adalah -u “https://console.telkomiot.id/ “ --crawl.

Hasilnya ditemukan potensi kerentanan seperti yang ditunjukkan pada gambar di atas. Di akhir terdapat kalimat “*Potentially vulnerable objects found at* https://console.telkomiot.id/register” yang berati ditemukan kerentanan pada URL tersebut dan dibawahnya terdapat sebuah potongan kode JavaScript “*69 // window.location.href = data.url;”* yang juga mengarah pada kerentanan. Potongan kode “*window.location.href*” memiliki fungsi untuk mengarahkan pengguna ke URL yang diberikan oleh “*data.url*”. Tidak adanya perlindungan yang memadai dapat membuka celah untuk serangan XSS. XSStrike mendeteksi potongan kode ini sebagai objek yang berpotensi rentan dan perlu diperiksa lebih lanjut.



GAMBAR 4. 5
Hasil Pengujian XSS menggunakan XSStrike

Mencari kerentanan XSS secara manual juga dilakukan pada Telkom IoT Platform dengan cara memasukkan sejumlah *payloads* ke dalam area yang dapat menerima input dari pengguna. Pada hal ini dilakukan pada kolom pencarian. *Payloads* yang digunakan diambil dari *payloads* yang sudah tersedia di Kali Linux. Berikut adalah contohnya.

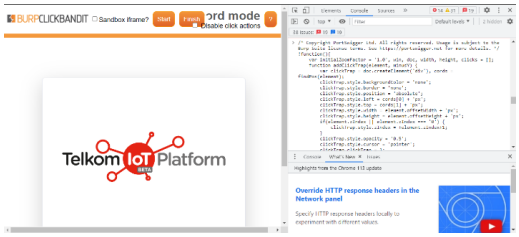


GAMBAR 4. 6
Pengujian XSS Manual

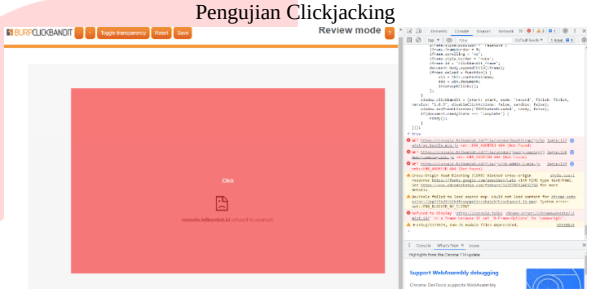
Dari sejumlah *payloads* yang digunakan tidak ada efek apapun yang terlihat pada halaman web. Hal ini berarti aplikasi web Telkom IoT Platform telah menerapkan tindakan perlindungan yang efektif terhadap untuk mencegah serangan XSS. Ini bisa termasuk penggunaan teknik sanitasi yang kuat, validasi *input* yang ketat, atau penggunaan metode *output encoding* yang tepat.

E. Clickjacking

Untuk menguji kerentanan clickjacking digunakan fitur Burp Clickbandit pada Burp Suite yang dapat digunakan untuk menguji kerentanan clickjacking dengan cara menyalin skrip yang disediakan oleh Burp Clickbandit dan menginputkannya ke JavaScript *console* di *web browser*.



GAMBAR 4. 7
Pengujian Clickjacking



GAMBAR 4. 8
Pengujian Clickjacking

Berdasarkan hasil pengujian menunjukkan bahwa Telkom IoT Platform sudah tergolong aman dari serangan clickjacking karena pada saat pengujian halaman web tidak dapat ditampilkan dan pada console *web browser* terdapat tulisan "*Refused to display 'https://console.telkomiot.id/' in a frame because it set 'X-Frame-Options' to 'sameorigin'*".

Tulisan tersebut berarti halaman web hanya diizinkan untuk dimuat dalam frame jika asal (*origin*) halaman yang memuatnya sama dengan asal halaman yang dimuat di dalam *frame*. Dalam hal ini, halaman web melarang pemuatan halaman dalam *frame* dari situs web lain untuk mencegah potensi serangan clickjacking di mana penyerang mencoba menyusupkan konten berbahaya ke dalam frame tersebut.

V. KESIMPULAN

Setelah melakukan scanning port, tiga port teridentifikasi terbuka, yaitu port 80, 443, dan 53. Hal ini menunjukkan bahwa saat pengujian dilakukan layanan web, HTTPS, dan DNS sedang aktif. Pada saat scanning direktori ditemukan 9 direktori yang berstatus HTTP 200 yang menandakan bahwa direktori-direktori tersebut dapat diakses secara publik. Pengujian kerentanan SQL injection menggunakan sqlmap tidak ditemukan celah atau kerentanan pada sistem yang diuji. Hal ini menunjukkan bahwa sistem telah menggunakan keamanan yang memadai dan efektif dalam mencegah serangan SQL injection. Pengujian *Cross Site Scripting* menggunakan XSStrike ditemukan potensi kerentanan pada “https://console.telkomiot.id/register” dan juga pada “window.location.href = data.url;”. Pada pengujian secara manual menggunakan sejumlah payloads tidak ditemukan

celah keamanan pada Telkom IoT Platform. Hal ini menunjukkan bahwa Telkom IoT Platform sudah menerapkan sistem keamanan yang efektif untuk mencegah serangan XSS. Telkom IoT Platform sudah tergolong aman dari serangan clickjacking karena sudah menggunakan sameorigin pada X-Frame-Options. Hal tersebut menunjukkan bahwa halaman web melarang pemuatan halaman dalam frame dari situs web lain untuk mencegah potensi serangan clickjacking di mana penyerang mencoba menyusupkan konten berbahaya ke dalam frame tersebut.

REFERENSI

[1] VMware, Inc. "VMware Workstation 16.1.2 Player Release Notes." [Online]. Available: https://docs.vmware.com/en/VMware-Workstation-Player/16.1.2/rn/VMware-Workstation-1612-Player-Release-Notes.html. [Accessed: May 20, 2023].

[2] OffSec Services Limited. "What is Kali Linux? | Kali Linux Documentation." [Online]. Available: https://www.kali.org/docs/introduction/what-is-kali-linux/. [Accessed: May 20, 2023].

[3] "Panduan Refensi Nmap (Man Page, bahasa Indonesia)." [Online]. Available: https://nmap.org/man/id/. [Accessed: May 20, 2023].

[4] OffSec Services Limited. "Dirb." [Online]. Available: https://www.kali.org/tools/dirb/#tool-documentation. [Accessed: May 20, 2023].

[5] "sqlmap: automatic SQL injection and database takeover tool." [Online]. Available: https://sqlmap.org/. [Accessed: May 20, 2023].

[6] PortSwigger Ltd. "Getting started with Burp Suite." [Online]. Available: https://portswigger.net/burp/documentation/desktop/getting-started. [Accessed: May 20, 2023].

[7] S. Sangwan. "GitHub - s0md3v/XSStrike: Most advanced XSS scanner." [Online]. Available: https://github.com/s0md3v/XSStrike. [Accessed: May 20, 2023].