PEMANFAATAN METODE WAVS (WEB APPLICATION SECURITY SCANNERS) MENGGUNAKAN BURP SUITE TOOLS DALAM AUDIT TEKNIS KEAMANAN SISTEM INFORMASI SURAT TUGAS SEKOLAH VOKASI UNDIP

Arkhan Subari[1)], Saiful Manan[1)], Eko Ariyanto[1)], Adnan Fauzi[2)]
[1)]Program Studi Str. Teknik Listrik Industri, Sekolah Vokasi, Universitas Diponegoro
Jl. Prof. Soedarto, SH, Kampus Undip Tembalang, Semarang, Indonesia 50275
[2)]Program Studi Teknik Komputer, Fakultas Teknik, Universitas Diponegoro
Jl. Prof. Soedarto, SH, Kampus Undip Tembalang, Semarang, Indonesia 50275

ABSTRACT

An official travel assignment letter is a type of assignment letter needed by an employee in carrying out work assignments. In many ways, the assignment letter information system is built based on web-programming. In web-programming there are two methods to send data from client to server. The two methods are the POST method and the GET method. Information security is an important aspect that needs to be considered in design a information system. There are many attacker spying data on information system daily. Usually the attacker uses the loopholes in the data transmission method to attack the system. There are many techniques used to attack information systems likes WAVs (Web Application Security Scanners). WAVs is a program that is used to find security holes in web-based information systems using several methods, such as XSS, SQL Injection, Intercept and Bruteforce. One program that can be used is Burp Suite. Burp Suite is often used by security auditors, researchers, and testers for analysis of different systems. Burp's core functionality is to intercept and display HTTP requests in a structured manner. The Vocational School of Diponegoro University has developed an information system that is used to manage this assignment letter. The information system is design using a web-based application. However, the system has never been technically audited on its security level. Therefore, it is necessary to audit the information system security techniques so that the level of information system security can be ascertained and corrective steps can be taken if there are security holes found. This study is intended to conduct a technical audit of the security of the UNDIP Vocational School assignment letter information system. The audit was conducted using the WAVs (Web Application Security Scanners) method with the Burp Suite application. The results of the brutefoce test using Burpsuite showed that there was no suitable password. However, the fact that an attacker can attack 30,0006 times is a weakness that needs to be fixed.

Keywords: *technical audit; information security; WAVs (Web Application Security Scanners); bruteforce; Burpsuite;*

PENDAHULUAN

Seiring dengan perkembangan teknologi, muncullah konsep E-Goverment sebagai bentuk transformasi proses bisnis konvensional ke proses otomatisasi dalam bidang pelayanan publik[1]. E-government didefinisikan sebagai cara bagi pemerintah untuk menggunakan teknologi informasi dan komunikasi yang paling inovatif, khususnya aplikasi internet berbasis web, untuk memberi akses informasi dan layanan kepada warga negara dan bisnis lebih baik, untuk meningkatkan kualitas layanan dan untuk memberikan kesempatan lebih besar untuk berpartisipasi dalam institusi dan proses demokratis[2].

Salah satu layanan dalam E-Government adalah E-Office yang didefinisikan sebagai komponen administratif dan terpusat suatu organisasi dimana data, informasi, dan komunikasi disimpan dan disebarluaskan melalui beberapa bentuk telekomunikasi[3,4]. Salah satu layanan dalam E-Office adalah layanan dalam pembuatan dan pengelolaan surat tugas perjalanan dinas yang merupakan jenis surat tugas yang dibutuhkan oleh seorang pegawai dalam melaksanakan tugas kerja [5…8]. Dalam banyak hal, sistem informasi surat tugas dibangun dengan memanfaatkan pemrograman berbasis web.

Dalam pengembangan sistem informasi, keamanan informasi merupakan aspek penting yang perlu diperhatikan dalam membangun sistem[9]. Pada umumnya penyerang menggunakan celah-celah dalam metode POST dan GET, yang merupakan metode pengiriman data dalam sistem informasi[10], untuk menyerang sistem. Terdapat banyak teknik yang digunakan untuk menyerang sistem informasi, diantaranya SQL Injection, XSS, brute force, http request, intercept.

Brute force merupakan teknik penyerangan keamanan yang paling banyak digunakan[11]. Metode ini akan mencoba melakukan entry kode pada form yang terdapat pada sistem informasi secara berulang dengan kombinasi kode yang mungkin[12]. Biasanya ini dilakukan pada form login atau autentikasi.

Metode yang lain dapat dilakukan dengan cara melakukan scaning celah keamanan sistem informasi atau yang disebut dengan WAVs (Web Application Security Scanners). WAVs merupakan sebuah program yang digunakan untuk menemukan celah keamanan pada sistem informasi berbasis web

dengan menggunakan beberapa metode, seperti XSS, SQL Injection, Intercept dan sebagainya[13,14,15]. Celah kemanan tersebut dikelompokkan menjadi 4 jenis yaitu tinggi, menengah, rendah dan informatif[16]. Dengan melakukan scanning maka bisa ditemukan adanya celah keamanan yang ada pada sisten yang dituju.

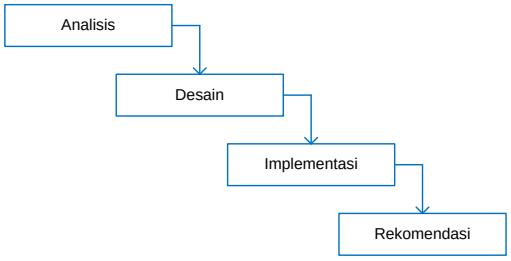
Salah satu program yang dapat digunakan adalah Burp Suite. Burp Suite merupakan aplikasi testing celah keamanan yang dikembangkan oleh Portswigger[17]. Burp Suite sering digunakan oleh auditor keamanan, peneliti, dan penguji untuk analisis dari sistem yang berbeda. Fungsionalitas inti Burp adalah untuk mencegat dan menampilkan HTTP request secara terstruktur[18,19]. Dengan menggunakan tools atau program tersebut, celah kemanan yang mungkin terdapat dalam sistem informasi dapat ditemukan, kemudian dapat dibuatkan rekomendasi kepada pengembang sistem agar dapat memperbaiki celah keamanan pada sistem informasi tersebut.

Terkait hal tersebut, Sekolah Vokasi Universitas Diponegoro telah mengembangkan sebuah sistem informasi yang digunakan untuk pengelolaan surat tugas perjalanan dinas. Pengembangan sistem informasi ini dilaksanakan dengan menggunakan aplikasi berbasis web. Namun demikian, sistem tersebut belum pernah dilakukan audit teknis pada tingkat keamanannya. Yang dilakukan pengembang adalah melakukan uji fungsionalitas sistem melalui metode black-box. Oleh karena perlu dilakukan audit teknik keamanan sistem informasi tersebut sehingga dapat dipastikan tingkat keamanan sistem informasi serta dapat dilakukan langkah perbaikan apabila terdapat celah keamanan yang ditemukan.

Penelitian ini dimaksudkan untuk melakukan audit teknis keamanan sistem informasi perjalanan dinas Sekolah Vokasi UNDIP. Audit dilakukan dengan menggunakan metode WAVs (Web Application Security Scanners) dengan aplikasi Burp Suite.

METODE PENELITIAN

Penelitian dilakukan menggunakan metode patching, dimana objek yang akan diteliti sebelumnya sudah ada namun dilakukan updating untuk menyempurnakan objek tersebut[9]. Adapun langkah-langkah metode patching dapat dilihat pada Gambar 1.



Gambar 1. Visualisasi langkah-langkah metode patching

Langkah-langkah patching dapat dibagi dalam beberapa tahapan, diantaranya tahap analisis, desain, implementasi dan rekomendasi yang diuraikan sebagai berikut:

- Analisis, tahap ini merupakan tahap untuk melakukan analisis kondisi saat ini mengenai sistem yang akan digunakan dalam penelitian ini, baik dari bagaimana sistem bekerja, alur sistem hingga payload data yang akan menjadi fokus utama pada penelitian ini. Selain itu juga percobaan mertode WAVs menggunakan tools Burpsuite, sebelum diimplementasikan konsep pengamanan yang ditawarkan. Tujuan dari tahap ini adalah mendapat semua detail dari sistem yang digunakan saat ini.
- Desain, hasil analisis tentu saja akan lebih jelas jika digambarkan dengan skema proses atau desain alur, sehingga pada tahap ini akan dipaparkan dan ditampilkan gambaran mengenai proses serangan dan pengamanan data yang dilakukan.
- Implementasi, tahap ini merupakan percobaan pengimplementasian dari hasil analisis, kerentanan yang akan terjadi ketika sistem tersebut dianalisis menggunakan WAVs.
- Rekomendasi, tahap ini merupakan tahap pendokumentasian hasil dari simulasi yang dilakukan. selain itu juga pada tahap ini dibuat rekomendasi yang akan diserahkan kepada pengembang dan pengelola sistem informasi agar dapat memperbaiki atau meningkatkan keamanan sistem informasi berdasarkan hasil simulasi yang dilakukan.

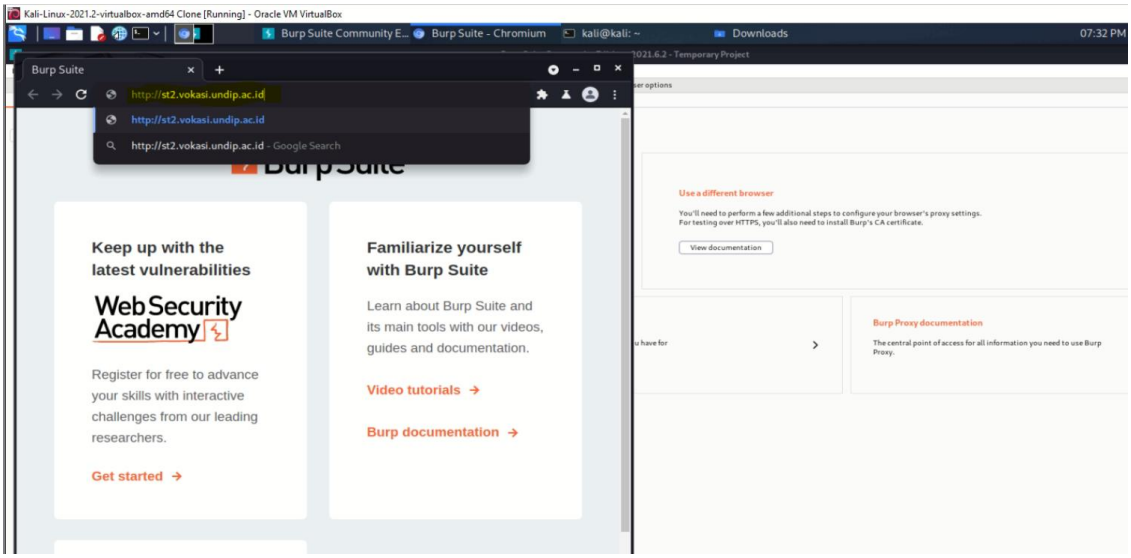
Menentukan Target

Penelitian ini menggunakan Aplikasi Surat Tugas Sekolah Vokasi sebagai target pengujian. Aplikasi ini dapat diakses melalui http://st2.vokasi.undip.ac.id pada aplikasi browser yang terdapat pada Burpsuite. Dalam penggunaannya, pada browser perlu dilakukan setting proxy ke 127.0.0.1 port 8080. Hal ini dilakukan agar paket data bisa ditangkap oleh aplikasi Burpsuite untuk mengetahui link form login aplikasi target. Ketika alamat target dieksekusi pada aplikasi browser yang proxynya sudah mengarah ke aplikasi Burp Suite, maka Proxy Burp Suite akan menginterup prosesnya dengan mengarahkan ke Proxy Burp Suite. Ilustrasinya ditunjukkan pada Gambar 2, 3 dan 4.

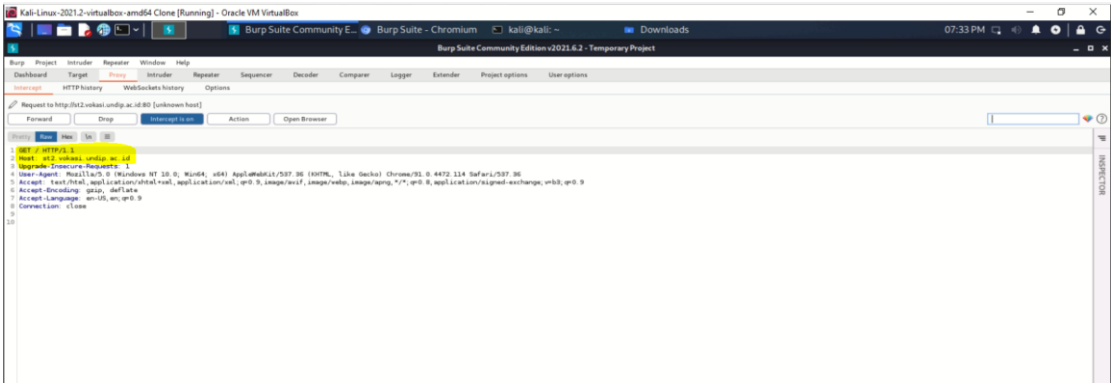
Mencari halaman login target

Halaman login target akan tampil apabila dilakukan penekanan tombol “lanjutkan” pada aplikasi surat tugas. Link halaman login yang akan digunakan untuk melakukan bruteforce didapatkan dengan cara memasukkan username dan password secara acak pada form halaman login target. Pada langkah awal pengujian ini dimasukkan username dan password “kali” seperti terlihat pada Gambar 5. Eksekusi dari proses ini akan menghasilkan beberapa

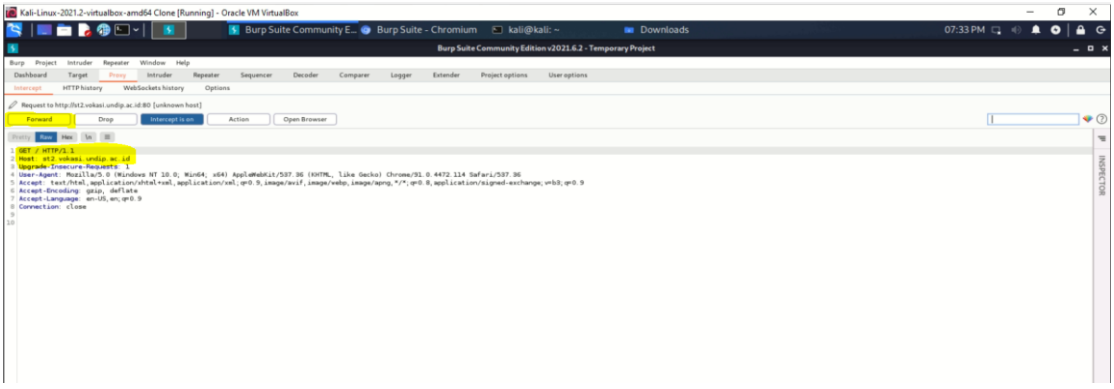
langkah eksekusi yang terekam pada Burpsuite dan dapat dilihat pada history HTTP Proxy. Dalam tampilan history tersebut, terdapat sebuah link yang mengarah pada proses eksekusi halaman login. Pengujian ini dilakukan dengan cara melakukan interupsi data pada proses ini dengan mengganti data username dan password dengan data yang telah disiapkan. Caranya adalah dengan melakukan klik kanan pada link yang di maksud kemudian pilih "Send Intruder". Pada tampilan berikutnya, dilakukan perubahan data username dan password sesuai dengan data yang telah disiapkan. Ilustrasi dari proses ini ditunjukkan pada Gambar 6, 7 dan 8.



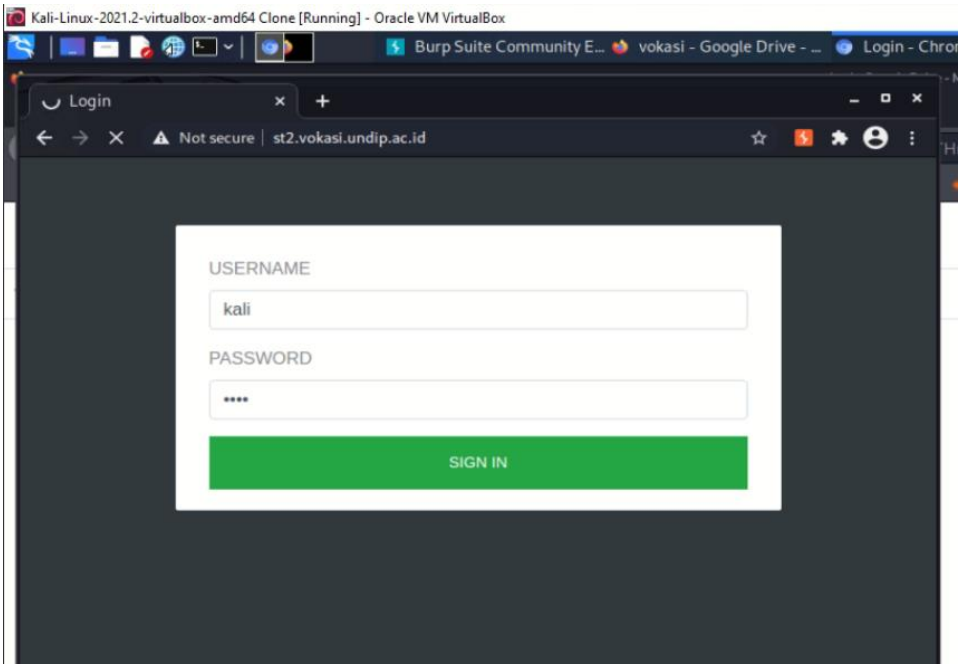
Gambar 2. Tampilan Aplikasi Browser dari Burp Suite



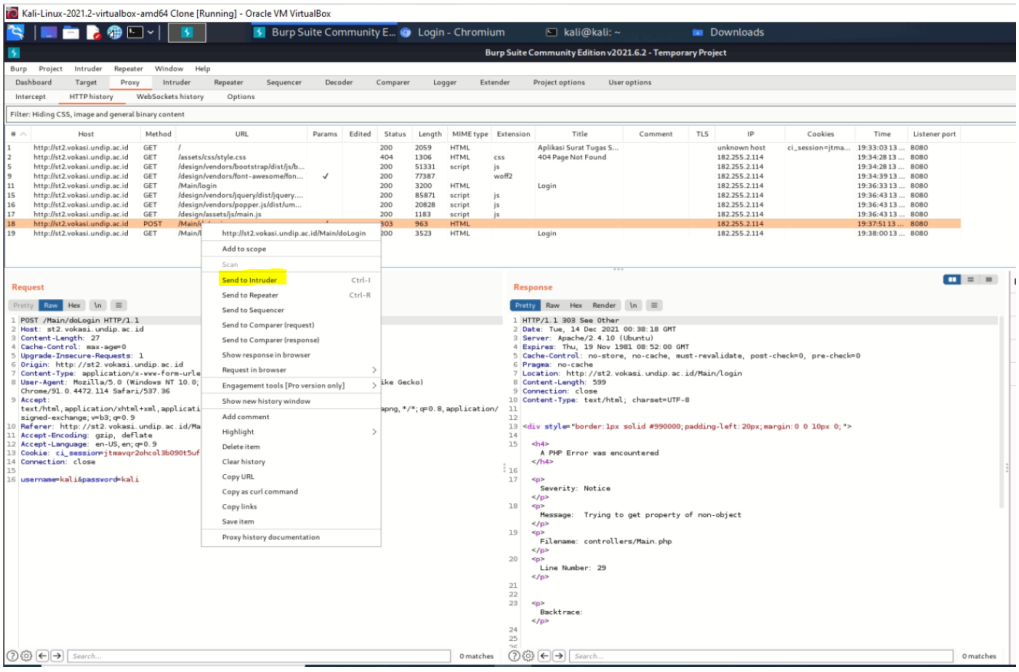
Gambar 3. Tampilan interrupt Proxy Burp Suite



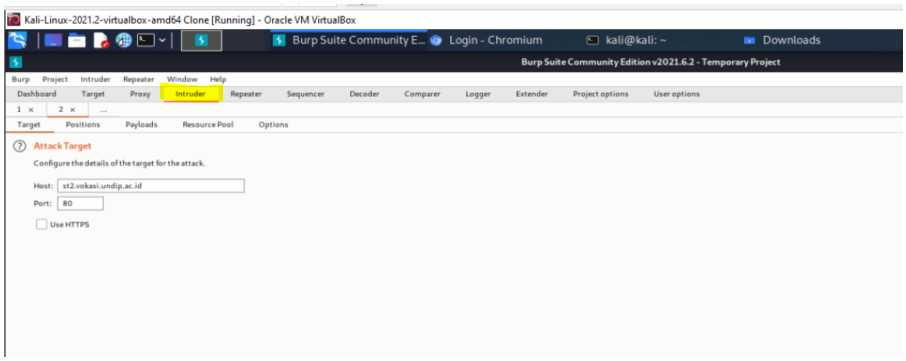
Gambar 4. Tombol Forward Aplikasi Proxy Burp Suite



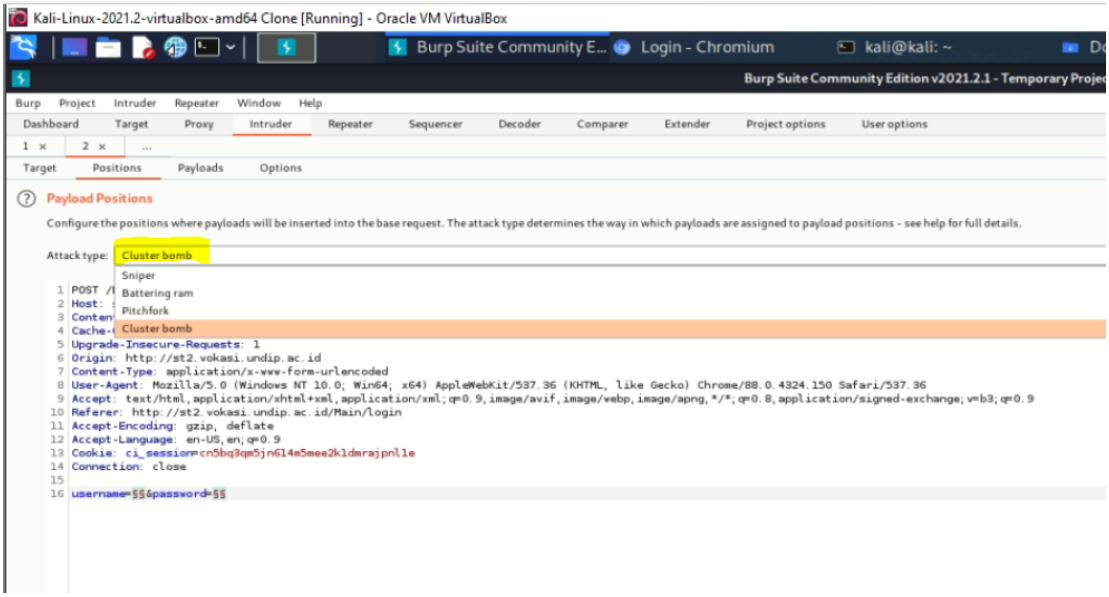
Gambar 5. Form Login Aplikasi Surat Tugas Sekola Vokasi diisi username dan password “kali”



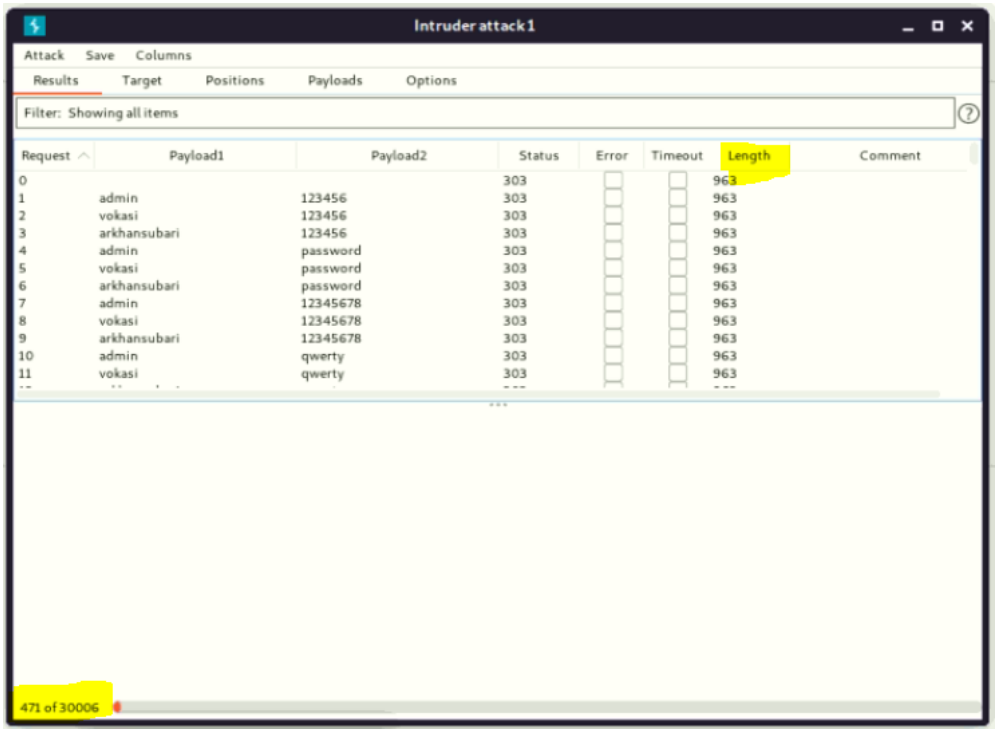
Gambar 6. Mengirimkan link ke Menu Intruder



Gambar 7. Menu Intruder Proxy Burp Suite



Gambar 8. Tampilan Edit isian username dan password Intruder Burpsuite



Gambar 9. Proses Bruteforce dengan aplikasi Burpsuite

HASIL PENGUJIAN

Pengujian dilakukan dengan cara mempersiapkan list user dan password yang akan digunakan dalam penyerangan dengan metode bruteforce. List ini dapat diunduh dari internet. Setelah itu, proses selanjutnya adalah memasukkan list tersebut ke aplikasi Burp Suite. Pilih Menu Payload pada Tab Intruder. Pada menu tersebut terdapat Payload Set dan Payload Options. Payload Set digunakan untuk mensetting text apa akan digunakan untuk dimasukkan pada form halaman login. Setelah itu maka list password akan masuk ke dalam form Payload Options. Proses pengujian dilakukan dengan menekan tombol “Start Attack” ketika list password telah siap. Dalam hal ini terdapat 10.002 list password yang dimasukkan pada Payloads Set 2. Sedangkan pada Payliad Set 1 berisi 3 list username. Sehingga aplikasi ini akan memasukkan list sebanyak 3x10.002 = 30.006 kali percobaan memasukkan user dan password pada aplikasi target, seperti yang ditunjukkan pada Gambar 9.

Hasil pengujian dengan memasukkan 3 kombinasi nama pengguna dan 10.002 kombinasi password, dihasilkan semua “length” panjangnya sama dan menunjukkan tidak ada user dan password yang sesuai. Dengan demikian dapat disimpulkan

bahwa aplikasi ini aman dari serangan bruteforce. Namun demikian fakta bahwa penyerang dapat melakukan penyerangan sebanyak 30.006 kali adalah sebuah kelemahan sehingga perlu diperbaiki.

KESIMPULAN

Audit teknis pada sistem informasi surat tugas Sekolah Vokasi undip dilakukan dengan menggunakan metode bruteforce attack memanfaatkan burp suite. Langkah pengujian adalah dengan melakukan setting burp suite untuk keperluan bruteforce suite, menyiapkan password list yang akan disimulasikan kemudian di eksekusi.

Hasil pengujian brutefoce menunjukkan tidak ada password yang sesuai. Akan tetapi, dari hasil pengujian menunjukkan bahwa metode bruteforce dengan menggunakan aplikasi Burpsuite ini terus berjalan sampai 30.006 kali memasukkan username dan password. Artinya Aplikasi Surat Tugas Sekolah Vokasi pada form login nya belum membatasi berapa kali pengguna diperbolehkan melakukan kesalahan memasukkan username dan password.

DAFTAR PUSTAKA

[1] Dewandaru, D.S, 2013, Pemanfaatan Aplikasi E-Office Untuk Mendukung Penerapan E-Government Dalam Kegiatan Perkantoran Studi Kasus: Puslitbang Jalan Dan Jembatan, Seminar Nasional Teknologi Informasi dan Komunikasi 2013 (SENTIKA 2013), pp.232-239

[2] Fang, Z., 2002, E-Government in Digital Era: Concept, Practice, and Development, International Journal of The Computer, The Internet and Management, Vol. 10, No.2, p 1-22

[3] Mohd Lokman, A., Dharmarajan, N., Zainol, Z., 2007, E-Office For UiTM: Requirements Study, Proceeding so f the CSSR, Malaysia.

[4] Robles, M., 2001, The e-Office: What Exactly it is? Office Solutions, Mt Airy 18(6), pp 43-45.

[5] Silvana, M., Fajrin, H., Danton, 2015, Analisis Proses Bisnis Sistem Pembuatan Surat Perintah Perjalanan Dinas Kantor Regional II PT.Pos Indonesia, TEKNOSI, Vol. 01, No. 01, Oktober 2015 pp. 11 – 22.

[6] Laekha, E., 2017, Rancang Bangun Sistem Informasi Surat Perintah Perjalanan Dinas, Jurnal Teknik Informatika dan Sistem Informasi Volume 3 Nomor 3 Desember 2017 pp. 598-608.

[7] Iyan Nurbayan, Asep Deddy S., 2015, Pengembangan Sistem Informasi Surat Perintah Perejalan Dinas (SPPD) di Balai Produksi Dan Pengujian Roket Pameungpeuk Menggunakan Netbeans, Sekolah Tinggi Teknologi Garut, Jurnal Algoritma Sekolah Tinggi Teknologi Garut, ISSN : 2302-7339 Vol. 12 No. 1 (2015).

[8] A Subari et al 2020 IOP Conf. Ser.: Mater. Sci. Eng. 801 012141

[9] Imam R., Rusydi U., Iqbal B., 2020, Optimasi Keamanan Autentikasi dari Man in the Middle Attack (MiTM) Menggunakan Teknologi Blockchain, Journal Information Engineering and Educational Technology, Volume 04 Nomor 01 pp. 15-19.

[10] Arkhan S., Saiful M., 2014, Implementasi Aeschipper Class Untuk Enkripsi URL Di Sistem Informasi Akademik Fakultas Teknik Universitas Diponegoro, Jurnal Sistem Komputer, 4(2).

[11] Arkhan S., Saiful M., Eko A., 2018, Implementation of Password Guessing Resistant Protocol (PGRP) in improving user login security on Academic Information System, Advanced Science Letters, Volume 24, Number 12, December 2018, pp. 9523-9525(3).

[12] Indra G., 2019, Modifikasi Keamanan File dengan Algoritma Hill Cipher Untuk Mengantisipasi Dari Serangan Brute Force, TECHSI Vol. 11 No. 2 pp. 237-246.

[13] Malik Q., Ala'a S., Tariq K., 2005, Black Box Evaluation Of Web Application Scanners: Standards Mapping Approach, Journal of Theoretical and Applied Information Technology Vol.96 No. 14 pp. 4584-4596

[14] D. Pałka, M. Zachara, and K. Wójcik, 2016, Evolutionary Scanner of Web Application Vulnerabilities, in Computer Networks, Cham, pp. 384-396.

[15] P. E. Black, E. Fong, V. Okun, and R. Gaucher, 2008, Software assurance tools: Web application security scanner functional specification version 1.0, Special Publication, pp. 500-269.

[16] R. Lepofsky, 2014, Web Application Vulnerabilities and Countermeasures, in The Manager's Guide to Web Application Security: A Concise Guide to the Weaker Side of the Web, ed Berkeley, CA: Apress, pp. 47-79.

[17] Christian M., Vladislav M., Tim G., Jörg S., 2015, Automatic Recognition, Processing and Attacking of Single Sign-On Protocols with Burp Suite, Open Identity Summit 2015 pp. 117-131.

[18] Chanchala J., Umesh K.S., 2016, Performance Evaluation of Web Application Security Scanners for More Effective Defense, International Journal of Scientific and Research Publications, Volume 6, Issue 6, pp. 660-667.

[19] Chanchala J., Umesh K.S., 2016, Security Testing and Assessment of Vulnerability Scannersin Quest of Current Information Security Landscape, International Journal of Computer Applications Volume 145 No. 2 pp. 1-7.