INTISARI

Keamanan situs web menjadi semakin penting karena jumlah serangan, terutama serangan XSS dan DDoS, yang terus meningkat. Untuk mengatasi masalah ini, dalam penelitian ini telah dikembangkan sebuah alat forensik berbasis bash *scripting*. Alat ini menggunakan *regular expression* dan iterasi baris *log* untuk mendeteksi *payload* serangan. Fitur-fitur yang ada yaitu penanda setiap baris *log* yang teridentifikasi merupakan serangan XSS atau DDoS dan fitur lain yang terintegrasi dengan API ipdata.co memberikan informasi tentang alamat IP, termasuk geolokasi seperti kode negara, rekam jejak IP *(abusive)*, dan penggunaan VPN. Alat ini memiliki ukuran file yang lebih kecil (10 kB) dan proses instalasi yang lebih sederhana (4 langkah) dibandingkan dengan alat serupa. Pengujian dengan data yang terkumpul sekitar 8000 baris *log* dan yang terdeteksi sekitar 2300 baris *log* dengan 8 *payload* XSS dan 5 *payload* DDoS. Teridentifikasi 7 payload skrip XSS dan 2 *payload* DDoS menggunakan alat ini, sedangkan jika menggunakan cara manual teridentifikasi 8 *payload* skrip XSS dan 4 *payload* DDoS. Beberapa *payload* tidak terdeteksi karena *payload* injeksi XSS yang menggunakan huruf kapital dan non-kapital campuran, seperti "ScRiPt," serta saat payload DDoS mengandung "ST," yang tidak terbaca oleh alat. Kasus lain terjadi saat menggunakan alat MHDDoS dengan target alamat IP dan domain situs web yang sebenarnya, serta saat menggunakan alat SLOWLORIS dengan target alamat domain. Namun, ketika SLOWLORIS menggunakan target alamat IP situs web, berhasil terdeteksi dan difilter menggunakan alat yang dikembangkan. Pada pengujian menggunakan alat MHDDoS dengan metode TCP, ditemukan *payload* pola *buffer overflow* dalam *log*, yang tidak terbaca oleh *regular expression* yang dibuat peneliti. Penemuan lain terkait pembacaan informasi VPN dari ipdata.co untuk mendapatkan informasi alamat IP, terdapat kesalahan dalam membaca alamat IP, di mana saat peneliti menggunakan VPN pada saat melakukan serangan, tidak terdeteksi sebagai penggunaan VPN ketika dibaca menggunakan API ipdata.co. Oleh karena itu, alat ini dapat diperbaiki berdasarkan kekurangan dan kelebihannya agar dapat berguna bagi akademisi maupun praktisi di lapangan, dengan mempertimbangkan referensi yang sudah ada.

Kata kunci : Forensik Digital, *Bash Scripting, Regular Expression*, Layanan API Informasi IP, Log.

ABSTRACT

The security of websites has become increasingly important due to the rising number of attacks, particularly XSS and DDoS attacks. To address this issue, a bash scripting-based forensic tool has been developed in this study. The tool utilizes regular expressions and log line iterations to detect attack payloads. Its features include marking each identified log line as an XSS or DDoS attack and integration with the ipdata.co API, which provides IP address information such as country codes, IP abuse tracking, and VPN usage. The tool has a smaller file size (10 kB) and a simpler installation process (4 steps) compared to similar tools. Testing with approximately 8000 log lines, of which around 2300 were suspected attacks, detected 8 XSS payloads and 5 DDoS payloads. The tool identified 7 XSS script payloads and 2 DDoS payloads, while manual analysis identified 8 XSS script payloads and 4 DDoS payloads. Some payloads went undetected, such as XSS injection payloads with mixed capital and non-capital letters, like "ScRiPt," and DDoS payloads containing "ST," which were not recognized by the tool. Another case where detection failed was when using the MHDDoS tool targeting the actual IP address and domain of the website, as well as when using the SLOWLORIS tool targeting the domain address. However, when SLOWLORIS targeted the website's IP address, it was successfully detected and filtered using the developed tool. During testing with the MHDDoS tool using the TCP method, a buffer overflow pattern payload was found in the logs, which was not recognized by the researcher's regex. Another discovery pertained to reading VPN information from ipdata.co to retrieve IP address information. There was an error in reading the IP address, as when the researcher conducted the attack using a VPN, it was not recognized as using a VPN when read using the ipdata.co API. Therefore, the tool can be further improved based on its shortcomings and strengths to make it useful for both academics and practitioners in the field, considering the existing references.

Keywords : Digital Forensics, Bash Scripting, Regular Expression, IP Information API Service, and Log Analysis.