ANALISIS SERANGAN WATERING HOLE SEBAGAI TEKNIK PENCURIAN DATA DIGITAL PADA WEBSITE KOPPERATI MENGGUNAKAN METODE PENETRATION TESTING

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Informatika

Disusun oleh :

Muhammad Razzy Johan Maulana

18.11.1868

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2023

ANALISIS SERANGAN WATERING HOLE SEBAGAI TEKNIK PENCURIAN DATA DIGITAL PADA WEBSITE KOPPERATI MENGGUNAKAN METODE PENETRATION TESTING

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Informatika

Disusun oleh :

Muhammad Razzy Johan Maulana

18.11.1868

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2023

HALAMAN PERSETUJUAN

SKRIPSI

Analisis Serangan Watering Hole Sebagai Teknik Pencurian Data Digital Pada Website KOPPERATI Menggunakan Metode Penetration Testing

Yang disusun dan diajukan oleh

Muhammad Razzy Johan Maulana

18.11.1868

Telah disetujui oleh Dosc Pembimbing Skripsi
pada tanggal 30 Maret 2023

Dosen Pembimbing,

Subektiningsih, M.Kom.
NIK. 190302413

HALAMAN PENGESAHAN

SKRIPSI

Analisis Serangan Watering Hole Sebagai Teknik Pencurian Data Digital Pada Website KOPPERATI Menggunakan Metode Penetration Testing

Yang disusun dan diajukan oleh

Muhammad Razzy Johan Maulana

18.11.1868

Telah dipertahankan di depan Dewan Penguji
pada tanggal 30 Maret 2023

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Ali Mustopa, M.Kom NIK. 190302192	
Banu Santoso, S.T., M.Eng NIK.190302327	
Subektiningsih, M.Kom NIK. 190302413	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta,S.Kom., M.Kom.
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Muhammad Razzy Johan Maulana
NIM : 18.11.1868

Menyatakan bahwa Skripsi dengan judul berikut:

Analisis Serangan Watering Hole Sebagai Teknik Pencurian Data Digital Pada Website KOPPERATI dengan Metode Penetration Testing

Dosen Pembimbing: Subektiningsih, M.KOM.

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 01 April 2023

Yang Menyatakan,

Muhammad Razzy Johan Maulana

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Di era digital, semua kegiatan pendukung kehidupan manusia telah dipermudah dengan adanya teknologi yang juga telah menimbulkan perubahan kebutuhan serta gaya hidup manusia yang semakin butuh dan bergantung pada teknologi. Namun kemunculan tersebut tidak semata-mata lepas dari kejahatan *cybercrime* terutama *watering hole attack* yang merupakan jenis serangan yang menargetkan kelompok tertentu dengan cara menyuntikan *malicious code* kedalam sistem dari web yang sering dikunjungi oleh target. Sehingga ketika target mengakses situs tersebut, perangkat dari target akan terinfeksi oleh payload *malicious code* yang di-*inject* oleh pelaku. Oleh karena itu, penulis bermaksud untuk menganalisis serangan *watering hole* dengan teknik XSS menggunakan metode *penetration testing* pada website KOPPERATI untuk mengetahui bagaimana cara kerja dari serangan tersebut. *Penetration Testing* merupakan sebuah metode yang digunakan untuk mengevaluasi keamanan dari suatu sistem dengan cara melakukan simulasi serangan pada sistem untuk mengetahui bagaimana sistem bereaksi terhadap serangan yang dilakukan. Sedangkan website KOPPERATI merupakan website yang berfungsi sebagai pengecekan transaksi koperasi PT. Aneka Tuna Indonesia secara mandiri. Hasil yang didapatkan dari penelitian yang dilakukan berupa serangan *watering hole* dengan teknik *cross site scripting* adalah penyerang akan menginject script hook.js kedalam sistem dari website dan menunggu hingga target mengakses website tersebut, setelah target mengakses website tersebut, maka hook.js secara otomatis akan mengirimkan respon kepada server dari *BeEF* untuk menjalankan *Command Exploitation* pada browser dari target.

Kata kunci : Serangan Watering Hole, Penetration Testing, Cross Site Scripting

ABSTRACT

In the digital era, all activities that support human life have been facilitated by technology, which has also led to changes in human needs and lifestyles that are increasingly dependent on technology. However, this emergence is not solely separated from cybercrime crimes, especially watering hole attacks which are types of attacks that target certain groups by injecting malicious code into the system from the web that is frequently visited by the target. So that when the target accesses the site, the target's device will be infected by the payload of the malicious code injected by the perpetrator. Therefore, the author intends to analyze watering hole attacks with XSS using the penetration testing method on the KOPPERATI website to find out how these attacks work. Penetration Testing is a method used to evaluate the security of a system by simulating attacks on the system to find out how the system reacts to the attacks being carried out. While the KOPPERATI website is a website that functions as a checking of PT. cooperative transactions. Various Indonesian Tuna independently. The results obtained from the research conducted in the form of a watering hole attack with a cross site scripting technique is that the attacker will inject the hook.js script into the system from the website and wait until the target accesses the website, after the target accesses the website, then hook.js will automatically send response to the server from BeEF to run an Exploitation Command on the target browser.

Keyword : *Watering Hole Attack, Penetration Testing, Cross Site Scripting*