

PENCEGAHAN SERANGAN XSRF PADA APLIKASI WEB MENGGUNAKAN TOKEN IDENTIFIER

Donal F¹, Fazmah Arief Yulianto², Andrian Rakhmatsyah³

¹Teknik Informatika, Fakultas Teknik Informatika, Universitas Telkom

Abstrak

Serangan XSRF digunakan untuk mengeksploitasi celah keamanan pada aplikasi web. Serangan ini menyebabkan gangguan pada performansi sistem dan keamanan data.

Untuk mencegah serangan XSRF dibutuhkan analisis terhadap mekanisme serangan tersebut. Yang paling utama adalah mencari kelemahan pada sistem aplikasi dan bagaimana memperbaiki kelemahan tersebut. Sehingga diperlukan evaluasi terhadap sistem keamanan yang ada dan membuat rancangan baru yang mampu mencegah serangan XSRF.

Token Identifier adalah token yang berfungsi melakukan identifikasi terhadap setiap aksi pada aplikasi sebagai bagian dari proses verifikasi. Token Identifier tercipta karena kebutuhan akan pencegahan serangan XSRF. Token Identifier dapat dibuat dengan memodifikasi sistem keamanan yang sudah ada.

Kata Kunci : serangan XSRF, token identifier.

Abstract

Attack XSRF used to exploit the security gap of application web. This attack cause the trouble of system performance and data security.

To prevent the attack XSRF require the analysis of the attack mechanism. The most important need is looking for the weakness of application system and how to improve that weakness. So that needed by evaluation to existing security system and make the new device capable to prevent the attack XSRF.

Token Identifier is functioning token identify to every action at application as part of verification process. Token Identifier created because requirement of attack prevention of XSRF. Token Identifier can be made with the security system modification.

Keywords : XSRF attack, token identifier

Telkom
University

1. Pendahuluan

1.1 Latar belakang

Dalam sistem dan jaringan komputer, dikenal tujuh layer sistem OSI (*Open System Interconnection*). Pada setiap layer terdapat protokol-protokol yang mengatur sistem komunikasi, baik dengan layer yang berada di atas atau dibawahnya. Dalam bidang sistem keamanan komputer, setiap layer memiliki kelebihan dan kekurangan masing-masing jika ditinjau dari sisi *security*-nya.

Perkembangan sistem keamanan komputer berubah dari waktu ke waktu, tingkat keamanan komputer semakin lama semakin baik. Namun karena semakin kompleksnya sistem dan jaringan komputer pada masa kini, menyebabkan munculnya kelemahan-kelemahan baru bagi *security*.

Pada masa lalu pembahasan sistem keamanan jaringan komputer berbicara tentang paket data dari host ke host, bagaimana paket tersebut dapat berjalan aman pada jaringan tanpa mendapat gangguan. Protokol yang menangani ini berada pada layer *transport, network*, dan *datalink*. Protokol tersebut diantaranya TCP, IP dan Ethernet Protokol.

Kelemahan sistem keamanan yang paling banyak mendapat sorotan adalah gangguan sesi komunikasi antara client dan server, seperti pencurian paket data, kerusakan paket data atau pengelabuan sesi komunikasi. Masalah tersebut biasanya dapat diatasi dengan menggunakan firewall dan IDS. Kualitas firewall dan IDS semakin lama semakin baik, seiring dengan semakin dalamnya penelitian terhadap analisa kelemahan-kelemahan pada protokol tersebut.

Pada masa kini kelemahan sistem keamanan lebih bersifat aplikasi. Jaringan komputer tidak lagi hanya digunakan sebagai alat pertukaran data, tetapi juga sebagai sarana bisnis, komunikasi, dan sumber informasi yang komperhensif. Berbagai aplikasi dibuat untuk memfasilitasi hal tersebut. Aplikasi tersebut bekerja pada layer *application*. Salah satu protokolnya adalah HTTP.

Protokol HTTP sebenarnya adalah protokol yang sederhana. HTTP pada dasarnya tidak memiliki mekanisme sistem keamanan. Hal tersebut menyebabkan aplikasi yang berjalan di atasnya mempunyai kelemahan sistem keamanan.

Serangan-serangan yang terjadi terhadap kelemahan sistem keamanan aplikasi web kebanyakan merupakan serangan yang dikategorikan sebagai *Injection Code*. Injection code adalah suatu script yang dimasukkan oleh penyerang ke dalam form input pada aplikasi korban, yang menyebabkan gangguan pada aplikasi korban. Hal ini disebabkan script tersebut mempunyai makna yang berbeda bagi bahasa pemrograman aplikasi, dimana menyebabkan aplikasi tersebut tidak bekerja sebagaimana seharusnya diinginkan.

Script tersebut dapat berupa kode SQL (*SQL Injection Attack*), kode Javascript (*XSS Attack*), atau kode lainnya. Pada umumnya serangan ini dapat dicegah dengan membatasi karakter yang boleh diinputkan (metode *input filtering*). Rangkaian karakter yang membentuk kode bahasa pemrograman tertentu tidak akan dieksekusi sistem. Atau akan dieksekusi tetapi lebih dahulu termodifikasi oleh sistem. Kumpulan kode-kode tersebut biasanya disebut *malicious code*.

Serangan XSRF juga dikategorikan injection code. Tetapi yang berbeda adalah proses penginputan script dilakukan sendiri oleh korban. Dan script yang diinputkan tidak harus berupa kode bahasa pemrograman tertentu. Kode tersebut dapat saja merupakan kode yang valid bagi aplikasi korban.

Dibandingkan serangan injection code yang lain, munculnya XSRF masih relatif baru. Namun berdasarkan survey yang dilakukan oleh beberapa forum security online [1] menyebutkan dampak kerusakan yang disebabkan sangat fatal dan berbahaya. Polling yang dilakukan OWASP [3] dalam laporan tahunannya menempatkan XSRF selalu berada dalam 10 besar jumlah peristiwa serangan yang terjadi di internet.

Suatu aplikasi web dapat diserang menggunakan XSRF karena aplikasi tersebut mempunyai kelemahan sistem keamanan. Sehingga untuk mencegah serangan XSRF maka kelemahan tersebut harus diperbaiki. Pada banyak sistem komputer termasuk di dalamnya sistem keamanan dikenal penggunaan metode token. Token merupakan suatu nilai acak yang bersifat dinamis dan unik. Token pada sistem keamanan aplikasi perangkat lunak biasanya digunakan untuk proses otentifikasi, identifikasi dan verifikasi. Pada tugas akhir ini akan dirancang suatu mekanisme token yang digunakan untuk memperbaiki kelemahan sistem keamanan aplikasi yang dapat mencegah serangan XSRF.

Token Identifier adalah mekanisme token yang digunakan pada aplikasi perangkat lunak. Token identifier melakukan proses verifikasi terhadap nilai token yang teridentifikasi pada sistem. Rekayasa pada sistem dengan menggunakan token identifier dapat melengkapi sistem keamanan, khususnya mekanisme token yang sudah ada atau belum ada. Manfaat dari token identifier adalah untuk mencegah serangan XSRF.

1.2 Perumusan masalah

Masalah yang diteliti adalah:

1. Bagaimana menemukan cara untuk mengatasi kelemahan sistem keamanan aplikasi web terhadap serangan XSRF.
2. Bagaimana mendesain mekanisme token yang benar agar dapat mencegah serangan XSRF.

Selama penelitian, lingkup masalah dibatasi sebagai berikut:

1. Tidak melakukan perbandingan terhadap metode pencegahan serangan XSRF yang lain.
2. Pengukuran terhadap performansi sistem dilihat dari berhasil atau tidaknya serangan XSRF.
3. Tidak melakukan kajian terhadap keterlibatan serangan yang lain, seperti Social Engineering dan XSS..

1.3 Tujuan

Tujuan penelitian tugas akhir ini adalah:

1. Mendesain sistem keamanan untuk mencegah serangan XSRF pada aplikasi web.

2. Menguji coba desain yang telah dibuat untuk membuktikan berhasil mencegah serangan XSRF.

1.4 Metodologi penyelesaian masalah

Metodologi penyelesaian masalah yang dilakukan adalah:

1. Pengumpulan dan pembelajaran materi berupa:
 - a. Literatur berbagai serangan pada aplikasi web dan metode pencegahannya
 - b. Literatur konsep serangan XSRF
 - c. Literatur *Session Security* pada aplikasi web
2. Menganalisa mekanisme serangan XSRF berupa:
 - a. Eksploitasi celah keamanan proses input dalam sesi komunikasi
 - b. Kelemahan sistem keamanan yang sudah ada
 - c. Kebutuhan rekayasa sistem keamanan
3. Desain sistem keamanan berupa:
 - a. Penambahan parameter baru (lihat Gambar 3-10)
 - b. Metode pembangkitan token sebagai parameter baru (lihat Gambar 4-1)
 - c. Metode proses identifikasi dan verifikasi pada token (lihat Gambar 4-2)
4. Implementasi *token identifier* berupa:
 - a. Pengkodean untuk membuat proses pembangkitan dan verifikasi token berdasarkan desain
 - b. Penambahan pengkodean *token identifier* pada aplikasi web
5. Pengujian dan Kesimpulan berupa:
 - a. Uji coba sistem keamanan yang baru terhadap serangan XSRF
 - b. Membuat kesimpulan terhadap keberhasilan pencegahan serangan, termasuk didalamnya kelebihan dan kekurangan sistem keamanan tersebut

5. Kesimpulan

5.1 Kesimpulan

1. Serangan XSRF dapat mengganggu aplikasi web karena terdapat celah pada sistem keamanannya. Kelemahannya adalah pada aplikasi yang sama pada host yang berbeda tidak terdapat pengkodean yang berbeda. Tujuan dari pengkodean yang berbeda adalah untuk proses verifikasi pada setiap aksi, khususnya aksi pada link yang dianggap penting. Pengkodean yang berbeda dapat diperoleh dengan memanfaatkan token, dimana token yang baik harus bersifat unik, dinamis, dan memiliki nilai yang berkualitas. Token Identifier merupakan realisasi sederhana dari fungsi-fungsi tersebut.
2. Mekanisme Token Identifier telah terbukti dapat mencegah serangan XSRF pada kasus aplikasi web blog.

5.2 Saran

Perubahan pada sistem keamanan aplikasi menyebabkan gangguan terhadap kinerja sistem. Penambahan parameter token pada alamat aplikasi di URL menyebabkan browser tidak dapat bekerja sebagaimana seharusnya. Hal tersebut disebabkan mekanisme penyimpanan token yang kurang baik.

Untuk mengatasi hal tersebut dibutuhkan modul tambahan. Diperlukan penelitian lebih lanjut mengenai konsep dan desain yang baik agar dapat memperbaiki gangguan ini.

Referensi

- [1] Chuck Willis, 2008, "Preparing for the Cross Site Request Forgery Defense". Black Hat DC 2008.
- [2] Jesse Burns, 2007, "Cross Site Request Forgery". Information Security Partners LLC.
- [3] OWASP TOP 10, The Ten Most Critical Web Application Security Vulnerability, 2007, http://owasp.org/index.php/Top_10_2007.htm, didownload pada tanggal 13 Agustus 2008.
- [4] Priyadi Iman Nurcahyo, Lembur Memperbaiki Celah Keamanan CSRF, 2007, <http://priyadi.net/archives/2007/03/09/lembur-memperbaiki-celah-keamanan-csrf.htm>, didownload pada tanggal 8 Agustus 2008.
- [5] Ricky, CSRF, 2008, <http://th0r.info/csrf.htm>, didownload pada tanggal 9 September 2008.
- [6] SmitDev, CAPTCHA, 2006, <http://smitdev.com/posts/captcha83.php>, didownload pada tanggal 22 September 2008.
- [7] Thomas Satrio, 2007, "Pencegahan Serangan XSS pada Aplikasi Web PHP menggunakan Regex", Tugas Akhir Departemen Teknik Informatika Sekolah Tinggi Teknologi Telkom.
- [8] Wikipedia, Session ID, 2008, http://en.wikipedia.org/wiki/Session_ID.htm, didownload pada tanggal 22 September 2008.
- [9] Wikipedia, Token, 2008, <http://en.wikipedia.org/wiki/Token.htm>, didownload pada tanggal 28 September 2008.
- [10] Wikipedia, Verification and Validation (software), 2008, [http://en.wikipedia.org/wiki/Verification_and_Validation_\(software\).htm](http://en.wikipedia.org/wiki/Verification_and_Validation_(software).htm), didownload pada tanggal 28 September 2008.

Telkom
University