Melindungi Aplikasi dari Serangan *CrossSite Scripting* (XSS) Dengan Metode *Metacharacter*

Yulianingsih*

FakultasTeknik dan MIPA Universitas Indraprasta PGRI
Jl. Nangka No.58,Tanjung Barat, Jakarta Selatan
*(corresponding author) yuliagniya@yahoo.co.id**

Abstract— **The need for the use of the internet services widespread to other places and various real of life this has resulted in also improve of crime in the internet. Unreliable application security cause important data and secrecy of users into threatened. This certainly harmful for the user and carriers. Best methods of internet security needs to be prioritized to determine measures of proper reduction first to be understood is how those crime works.**

Cross-site scripting is the type of injection attack to sites by relying on weakness of a target or internet users. Attackers will use weakness users through solicitation or inducement to follow direction to a certain condition that has been data stealing payloads, with particular secrecy or commands through code scripting by besiegers.

In this research by some experiment to find the influence of a particular treatment against another in conditions that occurs, to insert metacharacter into code scripting before and after the process of script executions. Aim to achieved through research is to function of metacharacter to protect the vulnerability.

Keyword— Internet, CrossSite Scripting, Experiment, Metacharacter, Security, Attacker.

Intisari—**Kebutuhan masyarakat atas penggunaan jasa internet semakin meluas dan mencakup berbagai bidang kehidupan hal ini mengakibatkan turut meningkatkannya kejahatan dalam dunia internet. Keamaanan aplikasi yang tidak baik mengakibatkan data penting dan kerahasiaan pengguna menjadi terancam. Hal ini tentu saja merugikan bagi pihak pengguna maupun penyelenggara. Untuk itu perlu dikedepankan metode–metode terbaik dalam keamanan berinternet dan untuk menentukan tindakan penanggulangan yang tepat terlebih dahulu harus dipahami cara kerja dari jenis kejahatan tersebu.**

CrossSite Scripting merupakan jenis serangan injection terhadap situs dengan mengandalkan kelemahan dari target atau pengguna internet. Penyerang akan memanfaatkan kelemahan pengguna melalui ajakan atau bujukan untuk mengikuti arahan menuju suatu kondisi tertentu yang telah dimuati oleh usaha untuk pencurian data, kerahasiaan atau perintah tertentu melalui code scripting oleh penyerang.

Dalam penelitian ini dilakukan Sejumlah Eksperimen untuk mencari pengaruh perlakuan tertentu terhadap yang lain dalam kondisi yang terkendalikan, yaitu dengan menanamkan metacharacter kedalam code scripting sebelum dan sesudah proses berjalan. Tujuan yang hendak dicapai melalui penelitian ini adalah pembuktian terhadap fungsi metacharacter dalam menutup celah kerentanan keamanan aplikasi.

Kata Kunci— Internet, CrossSite Scripting, Eksperimen, Metacharacter, Keamanan, Penyerang **.**

I. PENDAHULUAN

Digitalisasi merupakan era dimana informasi dapat saling bertukar dengan sangat mudah dan cepat. Perkembanganya turut andil dalam meningkatkan taraf hidup manusia untuk menjadi lebih baik pada segala bidang hehidupan. Hal ini mengakibatkan pengguna layanan internet memiliki latar belakang pendidikan dan usia yang berbeda. Dengan semakin meluasnya penggunaan maka semakin rentan keamanan jaringan terhadap serangan. Untuk menghindari dari kondisi yang tidak diharapkan maka perlu dilakukan pengawasan dan penyebaran informasi yang baik bagi pengguna layanan internet. Salah satu yang menjadi perhatian peneliti adalah bahwa beberapa serangan dilakukan dengan cara yang sederhana namun mengakibatkan kerugian yang sangat besar bagi pihak lain maupun pengguna. Dengan demikian bagi penyelenggara situs perlu melakukan tindakan pencegahan untuk menghindari adanya celah keamanan tersebut.

Keamanan aplikasi adalah tindakan pencegahan dari serangan pengguna komputer atau pengakses aplikasi yang tidak bertanggung jawab dan tujuan dari keamanan itu sendiri adalah menjaga dan menghindari hilangnya data atau kerahasiaan dari pengguna. Jenis kejahatan komputer mempunyai ciri-ciri penyerangan yang berbeda berdasarkan tujuan yang hendak dicapai oleh penyerang.

Cross-Site Scripting merupakan jenis kejahatan terhadap keamanan aplikasi yang memanfaatkan kelengahan pengguna melalui ajakan atau hasutan untuk menggunakan fasilitas email atau *Uniform Resource Locator* (URL)

tertentu yang telah ditanamkan sejumlah code oleh penyerang untuk kepentingan tertentu. Berdasarkan penelitian yang pernah dilakukan oleh Stuttard pada tahun 2007 sampai dengan 2011 terhadap 100 lebih aplikasi web, ternyata masih banyak yang memiliki celah keamanan. Celah-celah keamanan yang ditemukan dan prosentasenya yaitu: Kesalahan Otentikasi (62%), Kesalahan Akses Kontrol (71%), SQL Injection (32%), Cross-site Scripting – XSS (94%), Kebocoran Informasi (78%), dan Crosssite Request Forgery – CSRF (92%) [1]. Dengan demikian dianggap perlu melakukan pencegahan terhadap kejahatan Cross-site scripting.

Metode yang di kedepankan dalam penelitian ini adalah pemanfaatan metacharacters sebagai validasi input yang diberikan oleh pengguna melalui aplikasi web.

II. LANDASAN TEORI

Penelitian didukung oleh sejumlah teori yang relevan dengan tujuan yang hendak dicapai untuk mendapatkan hasil yang tepat.

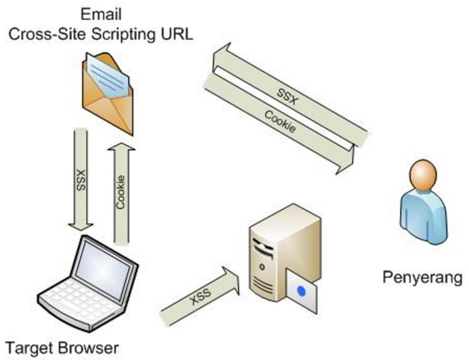
A. CrossSite Scripting (XSS)

Cross-Site Scripting merupakan salah satu kejahatan terhadap keamanan aplikasi melalui masukan pada browser. Penyerangan dilakukan dengan cara mengelabui target dan mengarahkannya untuk masuk menuju halaman tertentu yang sudah diberikan code tertentu oleh penyerang [2].

*Cross-Site Scripting*dilakukan untuk berbagai macam tujuan antara lain :

1. Mengambil alih kendali dari browser yang dimiliki target
2. Mengambil kerahasiaan data target melalui Cookie atau form data termodifikasi yang selanjutnya akan diforward kepada penyerang.
3. Penyisipan file yang tidak dikendaki.

Gambar 1 merupakan penggambaran kegiatan penyerangan dengan CrossSite Scripting melalui URL yang telah dimodifikasi untuk tujuan tertentu yang dikirimnya melalui email pada target.



Gambar 1. Penyerangan *Cross-Site Scripting*

B. Bagaimana CrossSite Scripting (XSS) dapat mempengaruhi kerentanan?

CrossSite Scripting merupakan salah satu kejahatan terhadap keamanan aplikasi melalui masukan pada browser. Penyerangan dilakukan dengan cara mengelabui target dan mengarahkannya untuk masuk menuju halaman tertentu yang sudah diberikan code tertentu oleh penyerang [2].
Dua hal yang dapat digunakan oleh penyerang dengan metode CrossSite Scripting :

1. Remote site to aplication site

   Serangan jenis ini diluncurkan dari luar, baik sebagai pesan email atau link di website lain. Pengguna masuk dengan mengklik link, loading gambar, atau mengisi form yang menyembunyikan hasil eksekusi yang berbahaya.

2. Aplication site to same or remote site

   Serangan jenis ini diluncurkan secara lokal, mengeksploitasi kepercayaan pengguna terhadap aplikasi untuk melakukan suatu tujuan jahat. Penyerang menyisipkan sebuah script berbahaya ke dalam sebuah komentar atau beberapa tulisan lainnya yang menyimpan masukan dari pengguna. Ketika halaman dengan sisipan script

tersebut dimuat dan diproses oleh seorang pengguna, browser melakukan beberapa tindakan yang tidak seharusnya dilakukan.

Kerentanan CrossSite Scripting terjadi ketika sebuah aplikasi mengirimkan data ke web browser tanpa adanya validasi yang baik. Informasi yang penting di PC yang telah di masukan oleh korban yang mengeksekusi CrossSite Scripting kemudian dikirimkan kepada hacker [3].

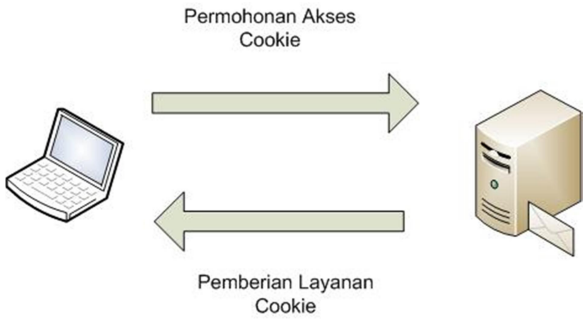
C. Metacharacter

Merupakan karakter dengan maksud khusus yang digunakan dalam sebuah *script* [4]. *Pada pemrogrman PHP fungsi html specialchars() berfungsi untuk merubah karakter-karakter khusus menjadi format HTML diantaranya:*

1. & (ampersand) menjadi &amp
2. " (double quote) menjadi &quo;
3. ' (single quote) menjadi &#039
4. < (less than) menjadi&lt
5. >(greater than) menjadi&gt

D. Cookie

Cookie merupakan fasilitas penyimpan informasi yang pengguna miliki ketika terhubung dengan suatu situs tertentu berisikan data dan segala aktifitas yang dilakukan target melalui browser. Session Cookie adalah cookie yang tersimpan dalam memory dan akan hilang ketika browser tertutup sedangkan persistent cookie adalah cookie yang tersimpan dalam bentuk file ke dalam harddisk. C*ookie* memiliki tujuan mempermudah server untuk mendapatkan identitas namun oleh penyusup *Cookie* dimanfaatkan untuk melakukan kejahatan [5].



Gambar. 2 *Cookie*

Gambar 2 memberikan gambaran mengenai *Cookie* pada browser. Dengan adanya *Cookie* identitas target dapat dikenali dengan mudah oleh server pada kunjungan selanjutnya. *Cookie* memiliki sifat Persistent dan Non Persistent.

E. Penelitian Lain Yang Relevan

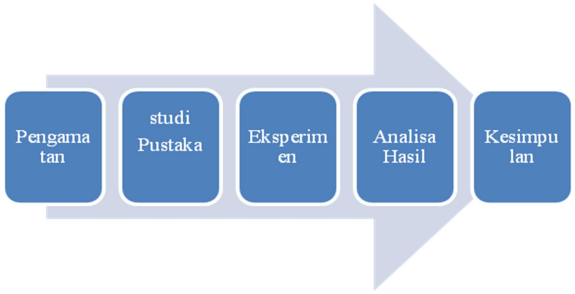
1. Menangkal Serangan *SQL Injection Dengan Parameterized Query* merupakan jurnal yang membahas tentang metode menangkal serangan terhadap situs secara *injection* melalui halaman login yang di berikan logika SQL, dengan tujuan dimana *query* yang diberikan akan dianggap selalu bernilai benar. Tujuan utama dari SQL *Injection* adalah memasuki database melalui user dan *password* yang telah diambil alih oleh penyusup untuk dikuasai [6].
2. Rancang Bangun Add-ons Deteksi *Cross Site Scripting* Pada Peramban Mozilla Firefox merupakan jurnal yang membahas secara khusus serangan Cross-Site pada browser [7].

Kedua jurnal mempertegas bahwa peningkatan keamanan harus dilakukan mulai dari pintu pertama masuknya informasi yaitu browser.

III. *METODELOGI PENELITIAN*

Sejumlah Eksperimen dilakukan dalam penelitian ini untuk mencari pengaruh perlakuan tertentu terhadap yang lain dalam kondisi yang terkendalikan [8].

Langkah-langkah penelitian yang digunakan untuk mendapatkan hasil diuraikan berdasarkan urutan proses yang ditunjukan pada gambar 3.



Gambar 3. Langkah-langkah Penelitian

Penelitian dibagi kedalam 5 langkah kegiatan, yaitu: Pengamatan, studi Pustaka, Eksperimen, Analisa Hasil dan Kesimpulan. Berikut uraian yang diberikan.

1. Pengamatan
   Merupakan kegiatan yang dilakukan diawal penelitian untuk mendapatkan permasalahan yang dianggap perlu untuk diberikan solusi yang tepat. Berdasarkan pengamatan ditemukan bahwa Cross Site Scripting merupakan jenis kejahatan didunia maya yang sering terjadi tetapi cenderung diabaikan keberadaannya tanpa memperhatikan efek negatif yang dapat ditimbulkan.
2. Studi Pustaka
   Mencari beberapa kemungkinan solusi ilmiah melalui literatur terpercaya dari sejumlah buku, jurnal dan situs yang dianggap mampu memberikan jawaban yang paling tepat. Selanjutnya melakukan penyusunan *scripting* yang akan digunakan sebagai media pengujian.
3. Eksperimen
   Dari beberapa kemungkinan solusi yang ditemukan ditentukan satu metode yang digunakan sebagai pengujian terhadap serangan *CrossSite Scripting*, yaitu *Sanitize Values Passed To Other Systems* dengan teknik *Metacharacters*yang dianggap cukup mudah dan praktis, yaitu penggunaan fungsi spesial karakter yang akan merubah karakter-karakter khusus menjadi format HTML [9].
   Langkah-langkah Pengujian:
   Pengujian Pertama:
   Memberikan serangan *CrossSite Scripting* terhadap situs sebelum blum diberikan pertahanan melalui masukan form dan URL untuk selanjutnya diamati pengaruh yang ditimbulkan.
   Pengujian Kedua :
   Memberikan serangan *CrossSite Scripting* terhadap situs sesudah diberikan pertahanan melalui masukan form dan URL untuk selanjutnya diamati pengaruh yang ditimbulkan.
4. Analisa Hasil
   Dari hasil pengujian tersebut ditentukan apakah metode yang digunakan berhasil mencapai tujuan yang diharapkan.
5. Kesimpulan

Jika ditemukan adanya perbaikan dari situs yang telah diberikan keamaan maka metode dianggap berhasil.

IV. HASIL DAN PEMBAHASAN

Pengujian terhadap *Code Scripting* dilakukan dengan dua tahapan yaitu sebelum dan sesuah pemberian metode keamanan melalui *input form dan URL* dengan hasil sebagai berikut :

Tabel 1. Ukuran Font untuk Makalah

Perbandingan Scripting

Code Scripting Tanpa Pengamanan

```
<html>
<head>
 <title>XSS Vulnerable</title>
 </head>
<body>
 <h1>Plain Search Page</h1>
<form action="" method="post">
    <input type="text" name="q_form" size="50" value="" />
    <input type="submit" value="Search" />
</form>
<?php
    if (isset($_GET['q']))
        {
            $question = $_GET['q'];
        }
    else if (isset ($_POST['q_form']))
        {
            $question = $_POST['q_form'];
        }
    else
        {
            $question = '';
        }
    echo $question;
?>
<br><br>
</body>
</html>
```

Code Scripting Dengan Pengamanan

```
<html>
<head>
 <title>XSS Secured</title>
 </head>
<body>
 <h1>XSS Secured Search Page</h1>
<form action="" method="post">
    <input type="text" name="q_form" size="50" value="" />
    <input type="submit" value="Search" />
</form>
<?php
    if (isset($_GET['q']))
        {
            $question = $_GET['q'];
        }
    else if (isset ($_POST['q_form']))
        {
            $question = $_POST['q_form'];
        }
    else
        {
            $question = '';
        }

 echo 'Kunci pencarian: '. antixss($question);

 function antixss($data)
{
    $xss = htmlspecialchars(trim($data));
    return $xss;
}
?>
<br><br>
</body>
</html>
```

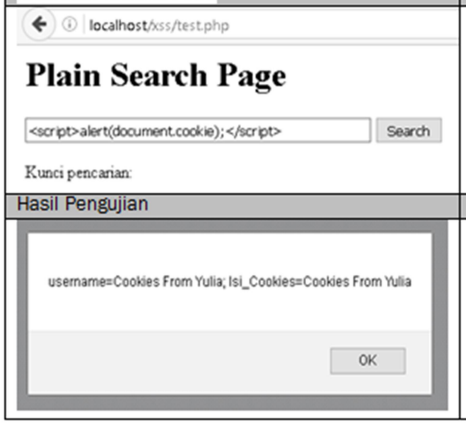
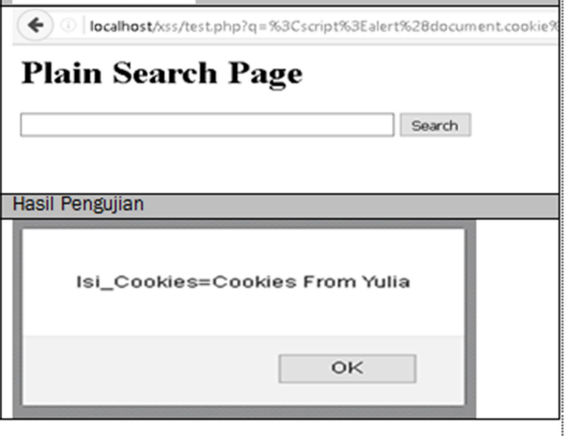
Pada pemrogrman PHP fungsi html specialchars() berfungsi untuk merubah karakter-karakter khusus menjadi format HTML diantaranya:

1. & (ampersand) menjadi &
2. " (double quote) menjadi "
3. ' (single quote) menjadi '
4. < (less than) menjadi<
5. >(greater than) menjadi>

FungsiTrim() pada pemrogramn PHP berfungsi menghilangkan spasi pada masukan.

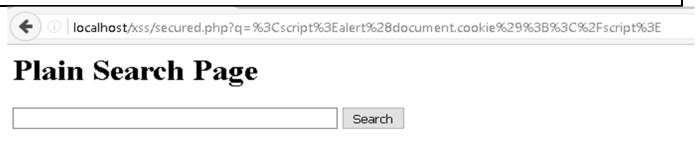
Tabel 2 merupakan hasil dari perbandingan pengujian yang dilakukan terhadap *scripting* yang belum diberikan kode pengamanan melalui input form dan URL

Tabel 2. Pengujian Pertama Tanpa Keamanan

Pengujian Pertama Scripting Sebelum Diberikan Keamanan	
Masukan Melalui Form	Masuka Melalui URL
	
Hasil Pengujian	Hasil Pengujian

Tabel 3 memberikan perbandingan hasil pengujian yang dilakukan terhadap *scripting* sesudah diberikan kode pengamanan melalui masukan form dan URL

Tabel 3. Pengujian Kedua Dengan Keamanan

Pengujian Kedua Scripting Sesudah Diberikan Keamanan	
Input Form	URL
	
Hasil Pengujian	Hasil Pengujian
	

V. KESIMPULAN

Dari hasil pengamatan selama melakukan pengujian dapat diambil kesimpulan sebagai berikut :

1. Hasil Eksperimen membuktikan bahwa metode metacharacter terbukti mampu menutup masuknya serangan *Cros Site Scripting* terhadap sebuah situs [10]
2. Metode *metacharacter* mudah untuk diimplementasikan dan efekti dalam hasil yang dicapai.
3. Menentukan konsep keamanan pada lapisan awal suatu layanan berbasis web perlu memperhatikan beberapa hal antar lain : kenyamanan pengguna layanan dan pengaruhnya terhadap kecepatan proses

REFERENSI

[1] Stuttard, Dafydd and Pinto, Marcus. 2011. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, Second Edition. John Wiley & Sons, Inc: Indianapolis.
[2] Jeremiah Grossmann, Robert Hansen, Petko. D. Petkov, Anton Rager and Seth Fogie. XSS Attack Cross Site Scripting Exploits and Defense. US: SYNGRESS. 2007
[3] Earnest Wish, Leo. Python web hacking essentials. Syngress. 2015.
[4] Stuart McClure, Joel Scambray, George Kurtz. Hacking Exposed, McGraw-Hill.2003
[5] S'to,Seni Internet Hacking, jasakom. 2004
[6] Yulianingsih. Menangkal Serangan SQL Injection Dengan Parapeterized Query. JEPIN. vol. 2. hal. 46–50. 2016.
[7] Yustiana Tri Wahyuni dan Ary Mahzaruddin Shiddiqi. Rancang Bangun Add-Ons Deteksi Cross Site Scripting (XSS) pada Peramban Mozilla Firefox. POMITS. vol. 2 2013.
[8] Sugiyono. Metode Penelitian Kuantitatif Kualitatif dan R&D. Bandung : Alfabeta. 2009.
[9] Chris Snyder, Thomas Myer and Michael Southwell. Pro PHP Security From Application Security Principles to The Implementation of XSS Defenses. 2nd ed. Ed. US: APRESS. 2010.
[10] Briony J Oates.Researching Information Systems and Computing. London: SAGE Publicatios. 2007