PENINGKATAN KEAMANAN *WEBSITE* DARI SERANGAN *CROSS SITE SCRIPTING* (XSS) DENGAN METODE METACHARACTER DAN *FORM VALIDATION*

Fuad Bawazir Alatas

ABSTRAK

Cross Site Scripting (XSS) merupakan salah satu teknik penyerangan yang umum terjadi pada suatu *website*. Dikarenakan teknik ini merupakan teknik yang lumayan *simple* dimana penyerang hanya memasukan injeksi kode yang nantinya akan memunculkan atau merefleksikan data dari *user*. Dikarenakan sekarang banyak muncul *website* baru maka penggunaan akan teknik XSS (*Cross Site Scripiting*) semakin meningkan dan sudah ada beberapa kasus yang terjadi sepanjang tahun 2020. Solusi yang ditawarkan didalam penelitian ini adalah membuat pengamanan yang dapat mendeteksi dan mencegah serangan *Cross Site Scripting* (XSS). Sistem ini dapat mencegah terjadinya serangan XSS (*Cross Site Scripting*) . Sistem ini dapat mendeteksi dan mencegah terjadinya serangan *Cross Site Scripting* (XSS) dengan melakukan *filter* pada inputan. Metacharacter digunakan untuk mereplace inputan yang dimasukan user agar mencegah terjadinya *bug* XSS yang disebabkan oleh *payload* yang berasal dari inputan *user*. *Form validation* digunakan untuk melengkapi kekurangan yang ada di metacharacter untuk meningkatkan keamanan *website*. Setelah dilakukan pengujian didapatkan dengan menggabungkan dua filter dapat mencegah payload yang diberikan, sehingga tidak memunculkan *bug* XSS. Kesimpulanya adalah menggunakan metacharacter saja belum cukup dikarenakan masih ada beberapa *payload* yang tidak ter*filter* maka dengan begitu jika digabungkan dengan *form validation* dapat memfilter semua pengujian *payload* yang diberikan.

Kata kunci : XSS , inputan , *filter,* injeksi, *form validation, metacharacter, payload*.

IMPROVING WEBSITE SECURITY FROM CROSS SITE SCRIPTING (XSS) ATTACKS WITH METACHARACTER AND FORM VALIDATION METHODS

Fuad Bawazir Alatas

ABSTRACT

Cross Site Scripting (XSS) is a common attack technique on a website. Because this technique is a fairly simple technique where the attacker only enters code injection which will later display or reflect data from the user. Because there are now many new websites, the use of the XSS (Cross Site Scripting) technique is increasing and there have been several cases that occurred throughout 2020. The solution offered in this research is to create security that can detect and prevent Cross Site Scripting (XSS) attacks. . This system can prevent XSS (Cross Site Scripting) attacks. This system can detect and prevent Cross Site Scripting (XSS) attacks by filtering the input. Metacharacter is used to replace input entered by the user in order to prevent XSS bugs caused by the payload originating from user input. Form validation is used to complete the deficiencies in the metacharacter to improve website security. After testing, it is found that combining the two filters can prevent the given payload, so it doesn't cause XSS bugs. The conclusion is that using metacharacters alone is not enough because there are still some unfiltered payloads so that when combined with form validation it can filter all the given payload tests.

Keywords: XSS, input, filter, injection, form validation, metacharacter, payload.