Securing Input And Output Processes On The Web to Minimize SQL-Injection and XSS Attacks Using IDS and IPS Methods

Pengamanan Proses Input Output Pada Web Untuk Meminimalisir Serangan SQL-Injection dan XSS Menggunakan Metode IDS dan IPS

Herlian Aliyasa Almaj Duddin *, Arif Senja Fitrani

Informatika, Universitas Muhammdiyah Sidoarjo, Indonesia

* *Email Penulis Korespondensi : asfjim@umsida.ac.id*

Abstract. *Some of the gaps that exist in web applications are often encountered, such as input both in the input form and input in the url. One of the attacks that are often found in data input is SQL-injection and XSS. Therefore one of the precautions is to carry out data security measures in the input and output process. Here the author uses the IDS and IPS methods as security of input forms from SQL-injection and XSS attacks. IDS is used as a detection and recording of attacks while IPS functions as a blocking access to the website if SQL-injection and XSS attacks are detected. In this case filtering uses the preg_match () function where the writer inserts the word into preg_match () as a rule which later if the user inputs what is in the preg_match () rule then the user is trying to do an injection attack. The data retrieved by the IDS script are ip_address, injected files, scripts, browsers used. IPS uses ip_address as a rule to block access from users when doing injection. It is hoped that the IDS and IPS scripts created will help secure the input output process that is on the web in order to minimize the occurrence of SQL-injection and XSS attacks.*

Keywords : Security; injection; IDS IPS; regular expression.

Abstrak. *Beberapa celah yang ada pada aplikasi web yang sering dijumpai seperti pada inputan baik pada form input yang ada maupun inputan yang ada pada url. Salah satu serangan yang sering dijumpai dalam input data adalah SQL-injection dan XSS. Maka dari itu salah satu pencegahan adalah dilakukkannya tindakan pengamanan data pada proses input output tersebut. Disini penulis menggunakan metode IDS dan IPS sebagai pengamanan form input dari serangan SQL-injection dan XSS. IDS digunakan sebagai pendeteksi dan pencatatan serangan sedangkan IPS berfungsi sebgai pemblokir akses ke website jikalau terdeteksi serangan SQL-injection dan XSS. Dalam hal ini pemfilteran menggunakan fungsi preg_match() dimana penulis menyisipkan kata kedalam preg_match() sebagai rule yang nantinya jika user menginputkan seperti apa yang ada pada rule preg_match() maka user sedang mencoba melakukan serangan injection. Data-data yang diambil oleh script IDS adalah ip_address, file yang di inject, script, browser yang digunakan. IPS menggunakan ip_address sebagai rule untuk memblokir akses dari user jika melakukan injection. Diharapkan script IDS dan IPS yang dibuat akan membantu mengamankan proses input output yang ada pada web agar meminimalisir terjadinya serangan SQL-injection dan XSS.*

Katakunci : *Keamanan; Klasifikasi; injection; IDS IPS; reguler expression.*

PENDAHULUAN

Informasi menjadi kebutuhan yang sangat penting dan bahkan menjadi kebutuhan pokok dijaman ini. Informasi juga merupakan suatu hal yang bersifat sensitif dalam hal ini informasi bisa digunakan sebagai hal baik maupun buruk. Berdasarkan data yang dibuat oleh symantec, indonesia berada di peringkat lima dunia negara yang paling banyak terserang pada tahun 2018 sebanyak 2,23% [1]. Hal ini juga dipaparkan oleh kominfo dihalaman website resminya indonesia menerima sebanyak 1,225 milyar serangan cyber setiap harinya. Salah satu serangan yang biyasa digunakan oleh hacker adalah injection. Injection sendiri adalah teknik untuk menyisipkan suatu script guna mendapat data yang di inginkan dan juga masuk ke dalam system dengan paksa. Serangan ini biyasa

dilakukkan pada inputan atau url yang ada dalam system. Maka dari itu dibutuhkan tindakan pengamanan pada proses input output data selain pada proses tersebut pengamanan data juga harus ada pada saat penyimpanan data. Banyak sekali metode yang bisa digunakan untuk mengamankan serangan dari para peretas yang ingin melakukan tindakan pencurian data. Diantara banyak metode IDS dan IPS adalah metode yang bisa digunakan untuk mengamankan proses input data . Metode ini mendeteksi serangan – serangan yang di lakukan oleh peretas. Pada kasus ini serangan yang akan di deteksi adalah SQL-injection dan XSS serangan ini dilakukan dengan cara menysipkan sesuatu script untuk menyerang suatu web [2]. Dengan adanya IDS dan IPS ini nantinya web akan difilter dengan aturan – aturan yang sudah disiapkan sehingga nanti ketika ada yang menyisipkan script – script injection maka akan dideteksi oleh IDS dan IPS.

METODE PENELITIAN

Keamanan Web

Keamanan merupakan salah satu factor penting dalam membangun sebuah web, Masalah dengan keamanan Web merupakan suatu masalah yang sangat kompleks. Proses ini berupa suatu mekanisme yang bekerja untuk mencegah akses dan modifikasi oleh user yang tidak dikenal, terhadap data-data dari web yang tersimpan secara online. Terdapat suatu metode monitoring yang digunkaan dalam melakukkan keamanan dalam suatu system yaitu Intrusion Detection System (IDS). Selanjutnya menindak lanjuti ancaman yang telah dideteksi dingan menggunakan IPS yang berfungsi sebagai pelindung untuk memblokir ip user agar user yang melakukan injeksi tidak bisa mengakses web [3].

2.1.1 Intrusion Detection System

Intrusion Detection System adalah metode atau alat yang dipasang pada system dalam suatu system guna mendeteksi dan memonitoring keamanan pada system tersebut proses monitoring event yang terjadi dalam suatu sistem computer atau jaringan dan menganalisanya untuk mengetahui adanya tanda-tanda mencurigakan yang mungkin terjadi. Tanda ini bias saja mengindikasikan adanya ancaman terhadap kebijakan keamanan computer yang diterapkan [4]. Insiden bisa terjadi karena berbagai macam sebab seperci malware contohnya worm, spyware. Didalam suatu sistem jaringan apabila ditemukan tanda-tanda yang mencurigaka berhubungan dengan traffic jaringan maka IDS akan memberikan peringatan kepada administrator jaringan ataupun sistem. Dalam beberapa kasus IDS juga merespon terhadap traffic yang tidak normal atau anomali melalui aksi pemblokiran terhadap alamat IP(Internet Protocol) atau user sumber dari usaha pengaksesan jaringan. Ada pula cara kerja yang dimiliki IDS dalam menganalisa apakah paket data yang dianggap sebagai intrusion oleh intruser [5].

Intrussion Prevention System

Intrusion Prevension system (IPS) merupakan suatu jenis pengamanan jaringan baik software maupun hardware yang dapat memonitor intruksion atau aktivitas yang tidak diinginkan serta langsung dapat beraksi untuk mencegah aktifitas tersebut. IPS Merupakan pengembangan dari Intrusion Detection System(IDS), sebagai pengembangan dari teknologi firewall, IPS melakukan control dari sebuah sistem berdasarkan aplikasi konten atau pattern, tidak hanya berdasarkan Ip address atau port seperti firewall pada umumnya. IDS selain dapat memonitoring dan mendeteksi keamanan sistem IPS dapat pula mengambil kebijakan dengan memblock paket dengan cara memberi informasi kepada firewall [6].

Injeksion

a. XSS(Cross Site Scripting)

   Cross Site Scripting merupakan serangan menggunakan mekanisme “Innjection” Dalam website, dimana dengan menggunakan metode HTTP POST ataupun memanfaatkan HTTP GET. Cross Site Scripting(XSS) biasanya digunkan oleh orang-orang yang tidak bertanggung jawab dalam upaya merusak website dengan cara menyisipkan script atau naskah program dimana script yang dipakkai menggunakan javascript sebagai mekanisme inputan, Cross Site Scripting juga dapat diartikan pula sebagai kelemahan akibat ketidakmampuan server dalam menvalidasi input yang diberikan oleh user serta algoritma yang digunakan untuk pembatan page atau halaman tidak mampu melakukan penyaringan terhadap input, XSS juga merupakan kelemahan yang popular untuk dieksploitasi [7].

b. SQL-injection

   Structured Query Language Injection(SQL-Injection) merupakan teknik serangan para peretas atau hacker dimana para hacker dapat menembus database secara illegal. Ada pula teknik dalalm SQL-Injection yaitu dengan cara memasukkan peritah SQL melalui alamat Uniform Resource Locator(URL) atau dapat melalui formulir masukan yang nantinya akan dieksekusi oleh server ketika meminta data ke dalam database. Dalam melakukan manipulasi data SQL-injection menggunakan teknik tertentu teknik yang digunakan ialah dengan menambah karakter union dan double minus (--) kedalam URL (Uniform Resource Locator) atau formulir masukan, Untuk mengetahui

bagaimana kerentanan sebuah website terhadap serangan SQL-injection terdapat bbeberapa hal yang dapat dilakukan yaitu sebagai berikut:

- Memeriksa kode apakah website telah menggunakan compiler dengan aman atau tidak.
- Verifikasi bahwa semua penggunaan compiler secara tegas memisahkan data yang tidak dapat dipercaya dari perintah atau query [8].

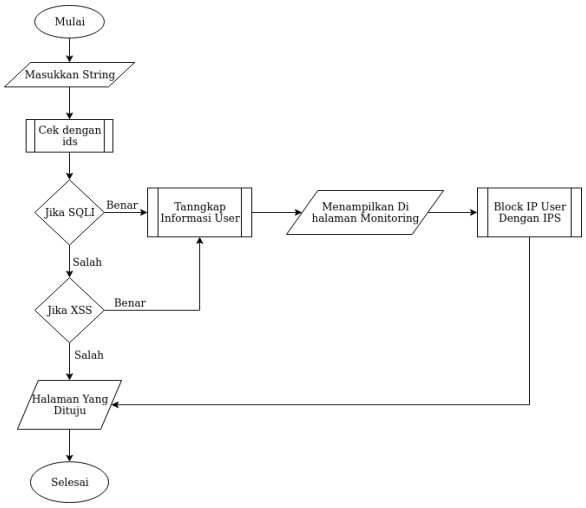
Reguler expresion

Ekspresi regular (regular Expression) yaitu sebuah bahasa mini yang mendeskrIPSikan string atau teks, yang membekadakn regex (regular expression) dengan string biasa yaitu metacharacters dimana terdapat karakter-karakter khusus, karakter-karakter ini tidak akan dicocokan secara literal dengan karakter itu sendiri, tapi mewakili sekelompok karakter lain atau pola khusus tertentu.Reguler expression biasa digunakan untuk mencocokkan dan mencari pola dalam text, mulai dari pola sederhana hingga yang sangat kompleks. Terdapat beberapa contoh karakter-karakter regular expression yang digunakan menurut Michael Fitzgerald [9]. Reguler Expression dapat dianalogikan seperti fungsi-sungsi String berikut strcmp() yang digunakan sebagai pencocokan dua string namun sctring harus memperhatikan besar dan kecilnya (case-sensitif) yang akan menghasilkan output 0 dan 1. strcasecmp() yang berfungsi sebagai pencocokan namun berbeda dengan fungsi strcmp() fungsi ini tidak memperdulikan penulisan besar dan kecil. Dan analogi terakhir adalah fungsi strops() yang berfungsi sebagai pencocokan lalu menemukan posisi string yang dicari. Namun pencocokan string dengan regex jauh lebih ampuh. Selain untuk menguji kecocokan substring dan string, regular expression juga dapat dipakai untuk mmbelah dan mensubstitusi substring dengan string [10].

HASIL DAN PEMBAHASAN

Flowchart

Flowchart sistem aplikasi ini ditunjukkan oleh Gambar 1.

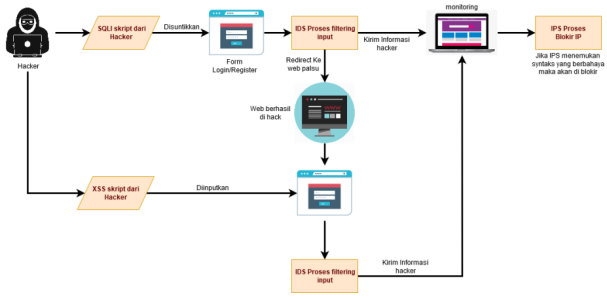


Gambar 1. Flowchart system

Pada gambar 1 dijelaskan bahwa ketika form yang di inputkan nantinya akan dicek terlebih dahulu dengan fungsi IDS apakah karakter yang di inputkan mengandung sintaks SQL- injection atau XSS. Jika nantinya inputan yang ditangkap mengandung sintak injection maka nantinya informasi seperti ip user dan halaman apa saja yang sedang dilakukan user pada web simulasi akan dikirim oleh IDS ke halaman monitoring . Setelah informasi tersebut ditangkap kemudian dilakukan pengecekan lagi terhadap aktifitas yang dilakukan oleh hacker apakah sintaks atau query yang dimasukkan didalam form input mengandung sintaks yang berbahaya. Jika terbukti melakukan serangan injection yang berbahaya maka nantinya hacker akan diblok dan tidak bisa mengakses web tersebut.

Alur Sistem

Gambar 2 akan menjelaskan alur sistem secara keseluruhan aplikasi ini.



Gambar 2. Alur System

Gambar 2 menunjukkan alur dari seranga hacker dimana langkah pertama hacker menggunakan script SQL-mjection pada form input yang sudah diberi function IDS dan IPS untuk masuk kedalam system. Kemudian string atau script SQL-injection akan di filter terlebih dulu dengan function IDS. Setelah IDS menemukan script SQL-injection kemudian hacker akan di kirim ke halaman palsu dan jika nantinya hacker melakukan tindakan berbahaya seperti memasukkan perintali hapus data kedalam form input yang ada di dalam halaman palsu tersebut maka otomatis IPS akan melakukan tindakan pemblokiran ip dan tidak bisa mengakses system tersebut. Sama halnya ketika hacker melakukan serangan injection dengan XSS jika IPS menemukan script untuk pencurian data atau perusakan data maka IPS akan memblokir ip hacker.

Pengujian Sistem

Langkah awal dalam pengujian IDS IPS ini adalah penginisialisaian dengan cara pertama memanggil file monitoring.php dan IPSFunc.php terlebih dahulu dengan cara memberi syntax include atau require pada file yang terdapat form inputannya. Selanjutna inisialisasikan class IPSFunc dan pasang fungsi IPS dengan parameter $_SERVER[‘REMOTE_ADDR’]. Hal ini digunakan untuk mengambil ip client dan nantinya akan di olah oleh fungsi IPS. Kemudian pasang fungsi IDS dengan parameter inputan tersebut bisa menggunakan $_POST atau $_GET seperti pada script inisialisasi IDS IPS.

Script Inisialisasi IDS IPS

Script inisialisasi IDS IPS ditunjukkan oleh Gambar 3 berikut.

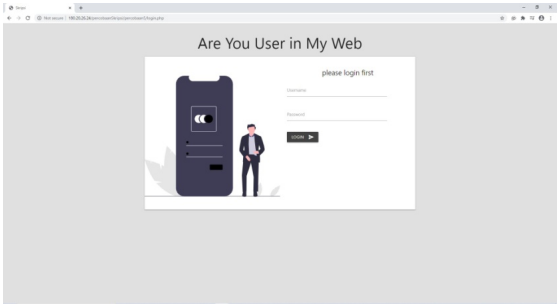
```
<?php
  require "lib/IPSFunc.php";

  $IPS = new IPSFunc;
  $IPS->cek($_SERVER['REMOTE_ADDR']);

  session_start();
  if (!empty($_SESSION['nim'])) {
     header('location:index.php');
  }

require_once(realpath(dirname(__FILE__))."/controller/logi
nController.php");

require_once(realpath(dirname(__FILE__))."/lib/monitor.ph
p");

  $login = new loginController;

  $username = IDS($_POST['username']);
  $password = IDS($_POST['password']);
```

Gambar 3. *Script inisialisasi IDS IPS*

Pengujian SQLI

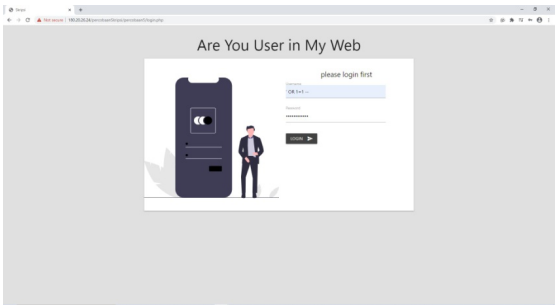
Setelah melakukan inisialisasi langkah selanjutnya melakukan pengujian terhadap script injeksi. Dimulai dengan script SQL-injection yang akan diuji dengan cara membypass form login baik itu form login user atau form login admin. Disini script yang digunakan untuk membypass login adalah ‘ OR 1=1 – – script ini jika diinputkan akan bernilai benar pada database dan nantinya jika pada login akan bisa otomatis masuk kehalaman admin dan user.

Seperti kita lihat pada gambar 3 script SQL-injection yang telah dimasukkan nantinya akan membypass login user dan ketika disubmit secara otomatis akan masuk ke halaman untuk user dan juga karena menginputkan script SQL-injection yang seblumnya inputan – inputan sudah diberi fungsi IDS. Maka kegiatan injection akan otomatis tercatat pada IDS yang telah dibuat. Tampilan *Login user* ditunjukkan oleh Gambarr 4.



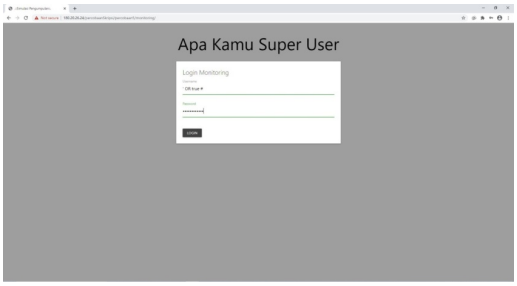
Gambar 4. *Login user*

Sedangkan untuk *login user* dengan pengujian *script SQL-injection* ditunjukkan oleh Gambar 5.



Gambar 5. *Login user dengan pengujian script SQL-injection*

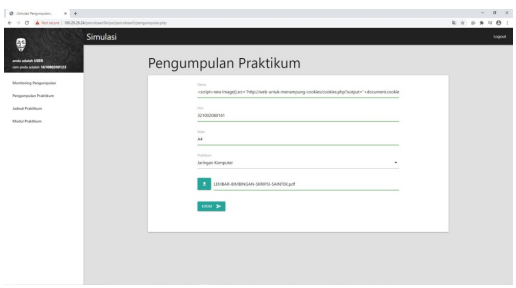
Pada Gambar 5, merupakan tampilan halaman login admin yang sama dengan halaman login user disini juga sudah di masukkan fungsi IDS. Dan ketika script IDS mendeteksi adanya inputan SQL-injection seperti yang ditunjukkan gambar 6, maka nantinya script tersebut akan mencatat dan mengirim datanya di file data.json



Gambar 6. *Login Admin dengan pengujian script SQL-injection*

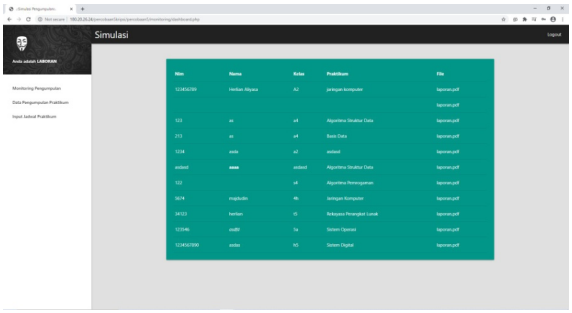
Pengujian XSS

Pengujian selanjutnya adalah pengujian XSS dimana nantinya akan ada dua pengujian XSS yang pertama store XSS dan reflected XSS. Percobaan pertama adalah store XSS dimana nantinya akan dilakukkan pengujian dengan cara menginjectkan script XSS pada inputan seperti pada contoh gambar 6 script tersebut bertujuan untuk mengambil cookie admin dan dikirim kan ke halaman yang berguna untuk menerima cookie yang dikirim ketika halaman admin dibuka. Seperti namanya store XSS akan tersimpan dalam database aplikasi dan akan berjalan terus sebelum data atau script XSS yang diinputkan dihapus. Gambar 7 menunjukkan tampilan pengumpulan praktikum dengan pengujian script XSS



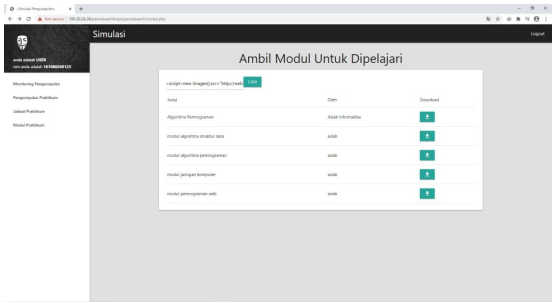
Gambar 7. *Pengumpulan Praktikum demgam pengujian script XSS*

Gambar 7 adalah halaman admin yang menampilkan data yang telah di inputkan oleh user pada halaman pengumpulan praktikum. Dan jika halaman itu dibuka maka script XSS yang di injectakan akan terus bekerja. Namun karena semua inputan sudah diberi fungsi IDS maka data-data user yang menyisipkan script XSS akan tercatat di file data.json.



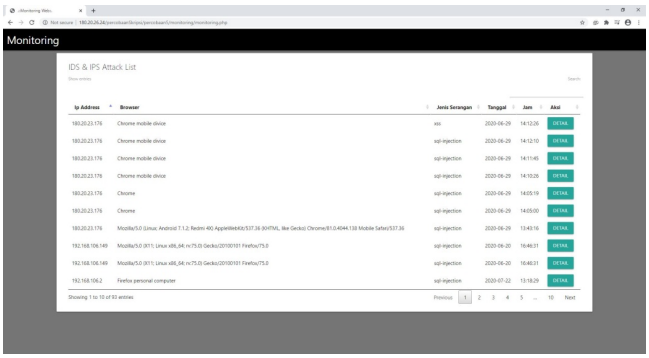
Gambar 8. *Pengumpulan Praktikum*

Pengujian XSS kedua adalah reflected XSS yang terdapat pada halaman pencarian modul. Pada halaman ini akan di uji pada form pencariannya apakah terdapat bug XSS atau tidak. Langkah pertama akan di ujikan dengan menginputkan script html seperti Hello jika pada halaman pencarian menampilkan tulisan Hello dengan huruf tebal maka pencarian tersebut bisa di injectkan script XSS. Sama halnya dengan inputan – inputan lain sebelumnya pada form pencarian ini juga terdapat fungsi IDS jadi ketika kita menginputkan script XSS maka data seperti ip address user akan tercatat dan nantinya akan ada pemblokiran terhadap ip tersebut. Tampilan pencarian modul dengan pengujian *script XSS* ditunjukkan oleh Gambar 9.



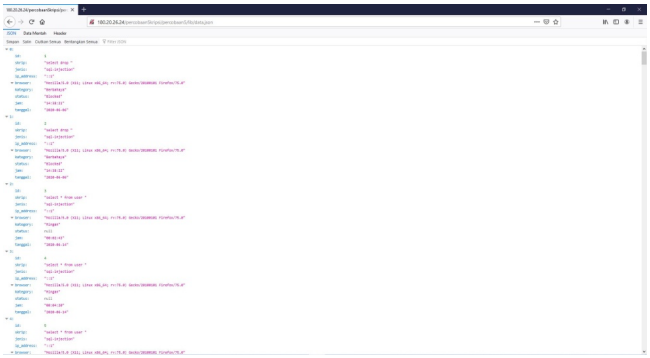
Gambar 9. *Pencarian Modul dengan Pengujian Script XSS*

Halaman monitoring pada gambar 9 ini terdapat pada halaman administrator, ini berfungsi sebagai pencatatan data-data seperti ip address , browser yang digunakan serta script yang digunakan oleh user untuk melakukan serangan injection pada inputan – inputan pada web atau aplikasi. Data – data yang ada pada halaman monitoring diambil dari file data.json dan bentuk mentahnya adalah seperti pada gambar 10.



Gambar 10. *Monitoring*

Gambar 10 merupakan hasil tampilan mentoring, sedangkan tampilan mentoring data Json nya ditunjukkan oleh Gambar 11.



Gambar 11. *Monitoring Data Json*

Seperti yang bisa dilihat dari script yang ada pada script file monitoring.php fungsi IDS menggunakan reguler expression dengan sintax preg_match sebagai pemfilteran kata dan karakter. Dengan memasukkan karakter atau kata – kata tertentu sebagai rule(pemfilter) yang menjadi ciri khas dari script XSS dan SQL-injection maka nantinya akan didapatkan sebuah pola yang nantinya dapat digunakan sebagai penentu apakah inputan tersebut benar – benar string biyasa atau kah script injection.

Dan dari proses pengujian XSS dan SQL-injection di atas bisa diketahui ip address yang digunakan oleh user yang nantinya akan digunakan sebagai pemblokiran untuk akses web jika nantinya ip tersebut terbukti menginputkan script injection yang berbahaya. Dan juga terdapat pengecekan browser yang digunakan oleh user untuk melakukan serangan. Selain ip addres dan browser fungsi IDS juga mengambil script yang diinjectkan pada inputan – inputan yang ada pada file – file tertentu.

Analisa Program

Dalam hal ini semua pengujian telah dilakukan mulai dari pengujian SQL-injection kemudian pengujian XSS semua hasil uji berjalan sesuai yang diharapkan dan sesuai dengan yang dipaparkan dalam bab I.

KESIMPULAN

Akhir dari pengujian dan analisa yang telah dilaksanakan pada bab sebelumnya dapat disimpulkan sebagai berikut:

a. Salah satu cara pencegahan serangan injection adalah dengan memfilter kata yang masuk dan karakter yang masuk karena selalu ada celah untuk menyerang selama ada inputan – inputan user.
b. Dengan reguler expression kita dapat membuat script untuk memfilter dan mengamankan form inputan yang ada pada user.

REFERENSI

[1] Symantec, “Internet Security Threat Report VOLUME 24, February 2019,” *Netw. Secur.*, vol. 21, no. February, p. 61, 2019, [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S1353485805001947.

[2] AON Cyber Solutions, “2019 Cyber Security Risk Report: What’s Now and What’s Next,” no. February, pp. 1–23, 2019.

[3] A. Tajpour and M. J. Z. Shooshtari, “Evaluation of SQL injection detection and prevention techniques,” *Proc. - 2nd Int. Conf. Comput. Intell. Commun. Syst. Networks, CICSyN 2010*, pp. 216–221, 2010, doi: 10.1109/CICSyN.2010.55.

[4] A. S. Irawan, E. S. Pramukantoro, and A. Kusyanti, “Pengembangan Intrusion Detection System Terhadap SQL Injection Menggunakan Metode Learning Vector Quantization,” *J. Pengemb. Teknol. Inf. dan Ilmu Komput. Univ. Brawijaya*, vol. 2, no. 6, pp. 2295–2301, 2018.

[5] C. Taylor and S. Sakharkar, “DROP TABLE textbooks: An argument for SQL injection coverage in database textbooks,” *SIGCSE 2019 - Proc. 50th ACM Tech. Symp. Comput. Sci. Educ.*, no. 3, pp. 191–197, 2019, doi: 10.1145/3287324.3287429.

[6] BSSN, “Mengenal SQL Injection,” *Bssn*, 2019, [Online]. Available: https://bssn.go.id/wp-content/uploads/2019/09/Proteksi-terhadap-Kerentanan-SQL-Injection-2019-

v.1.3.1_sign.pdf.
[7] A. Tajpour, M. Masrom, M. Z. Heydari, and S. Ibrahim, “SQL injection detection and prevention tools assessment,” *Proc. - 2010 3rd IEEE Int. Conf. Comput. Sci. Inf. Technol. ICCSIT 2010*, vol. 9, no. July 2014, pp. 518–522, 2010, doi: 10.1109/ICCSIT.2010.5563777.
[8] R. U. Putri and J. E. Istiyanto, “Analisis Forensik Jaringan Studi Kasus Serangan SQL Injection pada Server Universitas Gadjah Mada,” *IJCCS (Indonesian J. Comput. Cybern. Syst.*, vol. 7, no. 1, 2013, doi: 10.22146/ijccs.2157.
[9] C. Cetin, D. Goldgof, and J. Ligatti, “SQL-Identifier Injection Attacks,” *2019 IEEE Conf. Commun. Netw. Secur. CNS 2019*, pp. 151–159, 2019, doi: 10.1109/CNS.2019.8802743.
[10] I. Security and T. Report, “Internet Security Threat Report 23 Volume.”

Conflict of Interest Statement:
The author declares that the research was conducted in the absence of any commercial or financialrelation- shIPS that could be construed as a potential conflict of interest.

Article History:

Received: 2021-01-23 | Accepted: 2021-03-30 | Published: 2021-04-29