Analisis Deteksi Vulnerability Pada Webserver Open Jurnal System Menggunakan OWASP Scanner

Yunanri. W[*1], Imam Riadi[2], Anton Yudhana[3]
[1,2]Teknik Informatika; Jalan.Prof.Dr. Soepomo.S.H.,M.H.Telpon. 0274-563515, 511830
Magister Teknologi Informasi, Universitas Ahmad Dahlan, Yogyakarta
e-mail: *[1]yunanriw@gmail.com, [2]imamriadi@is.uad.ac.id, [3]eyudhana@ee.uad.ac.id

Abstrak

Keamanan merupakan suatu usaha yang dilakukan untuk melindungi informasi yang terdapat didalamnya yang mengacu pada kerahasiaan. Sebuah sistem yang terhubung dengan jaringan internet, akan memiliki tingkat kerawanan tinggi akan menjadi sebuah polemik bagi pemilik layanan sebuah informasi. Metode yang dilakukan adalah mengaudit webserver Open Jurnal System (O.J.S). Kegiatan ini bertujuan untuk mengidentifikasi dan mengekploitasi kerentanan pada webserver Open Jurnal Sistem (O.J.S). Pada penelitian ini menggunakan tool Open Web Aplication Security Project (OWASP). Pengujian ini bertujuan mencari vulnerability pada webserver Open Jurnal Sistem (OJS) adapun tingkatan vulnerability yang dideteksi dalam pengujian ini antara lain high risk, medium risk, low risk. tujuan mengamankan dari serangan SQL Injection maupun Cross Site Scripting XSS, karena akan membawa dampak kegagalan sistem. Manfaat dari pengujian ini sebagai alert atau peringatan. adanya serangan SQl Injection maupun serangan Cross Site Scripting XSS, oleh tool OWASP dalam mengaudit secara mandiri pada webserver Open Jurnal System sendiri.

***Kata kunci**: Audit Security, SQL Injection, Cross-site Scripting, Vulnerability, OWASP.*

1. PENDAHULUAN

Aplikasi *webserver* sering sekali mendapatkan serangan dari bergai pihak yang tidak bertanggung jawab yang seringkali di sebut *hacker* atau peretas. Berbagai macam alasan *hacker* mencari celah pada *webserver* bertujuan untuk mendapatkan informasi pada sebuah organisasi dan perusahaan untuk kepentingan-kepentingan yang membuat kerugian pada pihak lain.

Hacker dengan kemampuan tinggi dapat *remote* setelah mendapatkan celah dengan melakukan serangan menggunakan *SQL Injection*. Dimana *hacker* dapat menngirimkan *Script* dengan cara memasukkan *script* khusus ke *website* dengan cara teknik rekayasa system.serangan *Cross Site Scripting (XSS)* adalah jenis *injeksi*, dengan mengirimkan kode-kode *script* berbahaya, umumnya dalam bentuk skrip ke sisi *browser* pada pengguna akhir yang berbeda. Hacker dengan kemampuan tinggi dapat meremote setelah mendapatkan celah dengan melakukan serangan menggunakan *SQL Injection* Dimana *hacker* dapat menngirimkan skrip dengan cara memasukkan script khusus ke *website* dengan cara teknik rekayasa system.

Serangan *Cross Site Scripting* (*XSS*) adalah jenis injeksi, dengan mengirimkan kode-kode *script* berbahaya,umumnya dalam bentuk skrip ke sisi *browser* pada pengguna akhir yang berbeda.Aplikasi *Webserver Open Jurnal Sistem* (*OJS*), memiliki informasi pada Akademis yang berupaya dalam menyampaikan karya ilmiah ke masyarakat *global*. Dimana sebuah perangkat lunak dengan rekayasa sistem yang di bangun tidaklah semurna, oleh karena itu, sering sekali ada pihak yang tidak bertanggung jawab untuk membobol sistem.

Keamanan yang telah di buat, dari gambaran yang berupa tampilan sebuah informasi untuk ditampilkan di halaman *web*. Buat sebuah organisasi yang membayar

Seorang penyerang atau *hacker*. Agar dapat engeksploitasi, *hacker* menggunakan *software* semacam *program JavaScript* berbahaya yang dapat dieksekusi untuk menyebabkan kerusakan. Tujuan *hacker* atau peretas agar bias *login* seperti User atau *admin* pada sebuah *webserver.Cross Situs Scripting* (*XSS*), salah satu serangan keamanan paling umum saat ini, aplikasi web harus membersihkan data yang tidak tepercaya menggunakan fungsi pengkodean keluaran sebelum menampilkannya di halaman web [1] pada Gambar 1.

Gambar 1. Serangan *hacker* pada setiap *server* pada setiap negara.[1]

Teknik Serangan *Cross Site Attacks* adalah serangan Jaringan yang paling umum di *web* tempat kami menyuntikkan *Payload* (Kode Berbahaya) sisi klien ke *situs web*. Itu adalah kelemahan yang ditemukan dengan buruk situs kode yang dieksploitasi dan dicoba penyerang [2]. *SQL Injection* merupakan hanyalah satu dari sekian banyak jenis serangan injeksi atau *Injection,* yang terutama terjadi pada *database webserver. Hecker* dapat mengeksploitasi *SQL* yang tidak disetujui dengan mengeksploitasi kode-kode *Script*, melewati sebuah sistem *firewall* yang aktif [3]. Aplikasi *web* terdiri dari sisi *server hypertext protocol* (*PHP*), *Active Server Pages* (*ASP*) dan *Java Server Pages* (*JSP*) dan sisi klien (disandikan ke *JavaScript, Visual Basic Script (VBScript), Hyper Text Markup Language (HTML), ActiveX*).Sisi klien termasuk halaman *web* statis dengan scripting bahasa seperti JavaScript dijalankan dalam browser oleh Permintaan *HyperText Transfer Protocol* (*HTTP*) [4]. *Cross Site Scripting* (*XSS*) menyerang pada system komunikasi antar perangkat protocol *HTTPS* serta antara orang dengan orang lain. Hanya kemungkinkan komunikasi di antara domain dan subdomain yang diizinkan, yang membawa hasil dari sebuah *requesting* [5].

Laporan statistik keamanan terbaru mengungkapkan bahwa sekitar 55% aplikasi *webserver* yang dinilai memiliki kerentanan keamanan. Pada tahun 2013, *Open Web Aplikasi Security Projeject* (*OWASP*) menginformaikan adanya Kerentanan. Baik secara Umum atau *Exposures* (CWE) bahwa *Cross-Site Scripting* (*XSS*) sebagai satu kerentanan paling serius dalam aplikasi *web*. Yang paling Utama merupakan alasan kerentanan *XSS* adalah kerentanan yang terdapat pada source kode pada *webserver validasi* apa pun [6].

2. METODE PENELITIAN

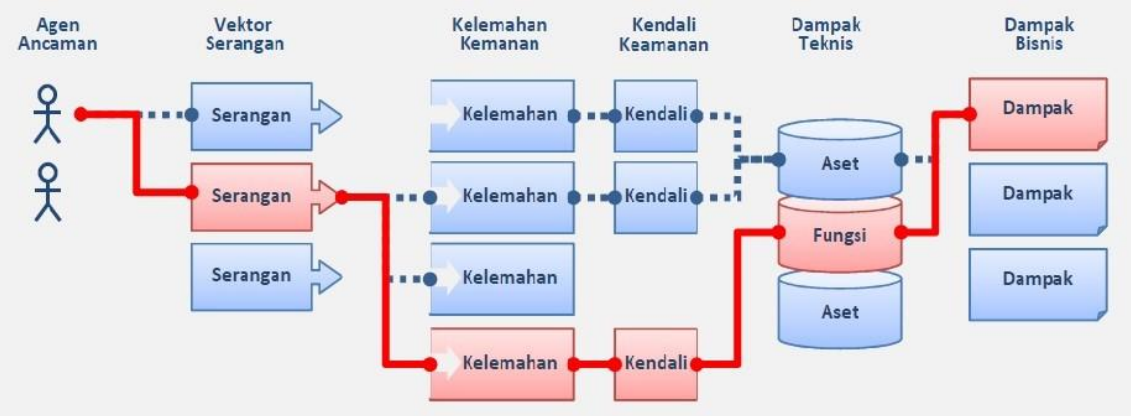
2.1 Pengumpulan data

Penelitian yang dilakukan termasuk dalam bidan security management. Metode pengumpulan data dilakukan dengan mengadopsi teknik Penetrasi Testing. Adapun

alur sistematika ini terdiri dari studi literature, analisis dan ujicoba pada webserver Open Jurnal System, secara localnetwork.

2. 2. Metodologi yang digunakan

Kelemahan XSS terjadi ketika aplikasi mengambil data yang tidak dapat dipercaya dan mengirimnya ke suatu web browser tanpa validasi yang memadai. XSS memungkinkan penyerang mengeksekusi script-script di dalam browser korban, yang dapat membajak sesi pengguna, mengubah tampilan website, atau mengarahkan pengguna ke situs-situs jahat. Mengaudit sistem dapat dilihat dalam Gambar 2.

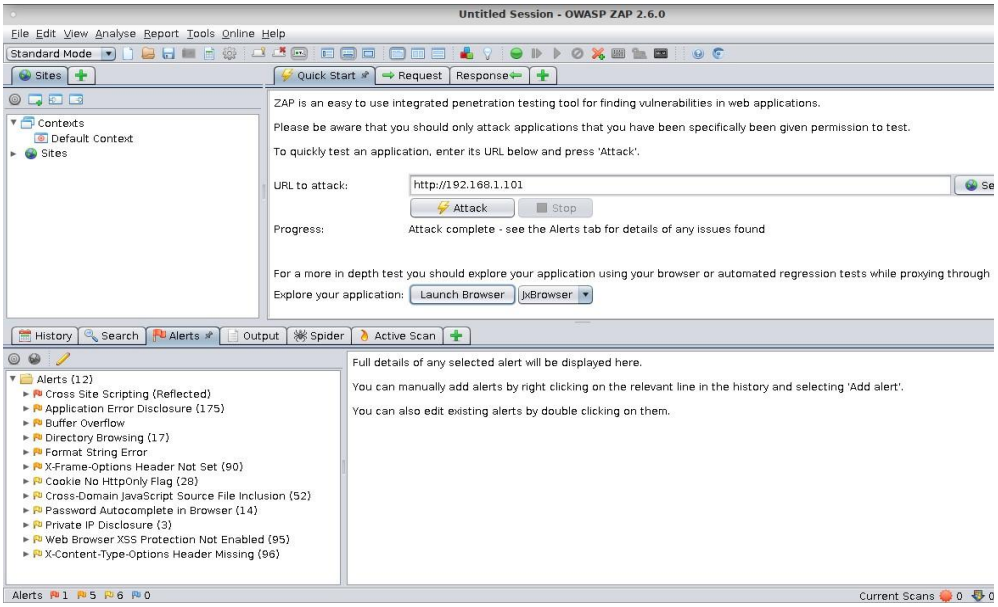


Gambar 2. Mengaudit sistem yang mengandung Vulneability

3. HASIL DAN PEMBAHASAN

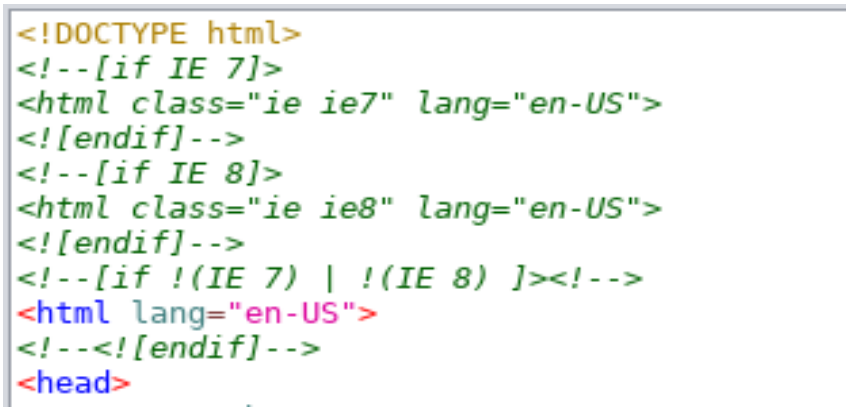
Dari hasil diagnosa yang di lakukan pada *webserver Open Jurnal System* (*OJS*) menemukan beberapa sub file system yang terindikasi memliki *Vulnerability*. Adapun aplikasi *webserver* yang di pakai untuk penelitian ini adalah *Ubuntu*.

a. Tool OWASP Scanning pada Open jurnal system dapat dilihat pada Gambar 3:



Gambar 3. Hasil Scanning Open jurnal system OJS [6]

b. Hasil Scanner oleh OWASP terhadap Open Jurnal System Local Network dapat dilihat pada Gambar 4:



```
<!DOCTYPE html>
<!--[if IE 7]>
<html class="ie ie7" lang="en-US">
<![endif]-->
<!--[if IE 8]>
<html class="ie ie8" lang="en-US">
<![endif]-->
<!--[if !(IE 7) | !(IE 8) ]><!-->
<html lang="en-US">
<!--<![endif]-->
<head>
```

Gambar 4. Vulnerability pada Remote OS Command Injector.

c. Hasil Scanner oleh OWASP terhadap Open Jurnal System Local Network dapat dilihat pada Gambar 5:

```
.download-box{width:250px;border:1px solid #ccc;-moz-border-radius:4px;-webkit-border-radius:4px;border-radius:4px;text-align:center
;position:relative;margin:1em auto;box-shadow:0 2px 4px rgba(0,0,0,.1),inset 0 1px 0 rgba(255,255,255,.4)}.download-box h1{margin:.
5em 0!important}.download-box img.wp-post-image{margin:0;padding:0;display:block;width:100%;-moz-border-radius:0;
-webkit-border-radius:0;-moz-border-top-left-radius:3px;-moz-border-top-right-radius:3px;-webkit-border-top-left-radius:3px;
-webkit-border-top-right-radius:3px;border-radius:0;border-top-left-radius:3px;border-top-right-radius:3px;box-shadow:inset 0 1px 0
rgba(255,255,255,.4)}.download-box .download-box-content{padding:0 1em 1em}.download-box .download-count{-moz-border-radius:1em;
-webkit-border-radius:1em;border-radius:1em;color:#777;text-shadow:0 1px 0 rgba(255,255,255,.5);background:#ddd;box-shadow:0 2px 4px
rgba(0,0,0,.1),inset 0 1px 0 rgba(255,255,255,.4);position:absolute;top:0;right:0;padding:.6em;width:auto;min-width:1em;font-size:
1em;text-align:center;vertical-align:middle;line-height:1em;border:1px solid #bbb;margin:-.5em -.5em 0 0}.download-button{text-align
:center;text-decoration:none;padding:.75em 1em;color:#fff;display:block;font-size:1.2em;line-height:1.5em;background-color:#09c;
background-image:-webkit-linear-gradient(#009fd4,#09c,#0086b2);background-image:-moz-linear-gradient(#009fd4,#09c,#0086b2);
-moz-border-radius:4px;-webkit-border-radius:4px;border-radius:4px;text-shadow:0 -1px 0 rgba(0,0,0,.5);box-shadow:0 2px 4px rgba(0,0
```

Gambar 5. Vulnerability pada Remote OS Command Injector

d. Hasil Scanner oleh OWASP terhadap Open Jurnal System Local Network dapat dilihat pada Gambar 6:

```
<head>
<title>IIS 8.5 Detailed Error - 500.52 - URL Rewrite Module Error.</title>
<style type="text/css">
<!--
body{margin:0;font-size:.7em;font-family:Verdana,Arial,Helvetica,sans-serif;}
code{margin:0;color:#006600;font-size:1.1em;font-weight:bold;}
.config_source code{font-size:.8em;color:#000000;}
pre{margin:0;font-size:1.4em;word-wrap:break-word;}
ul,ol{margin:10px 0 10px 5px;}
ul.first,ol.first{margin-top:5px;}
fieldset{padding:0 15px 10px 15px;word-break:break-all;}
.summary-container fieldset{padding-bottom:5px;margin-top:4px;}
legend.no-expand-all{padding:2px 15px 4px 10px;margin:0 0 0 -12px;}
legend{color:#333333;;margin:4px 0 8px -12px;_margin-top:0px;
```

Gambar 6. Vulnerability pada Remote OS Command Injector

e. Hasil Scanner oleh OWASP terhadap Open Jurnal System Local Network, dapat dilihat pada Gambar 7.

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<html>
<head>
<title>732</title>
<meta http-equiv="Cache-Control" content="no-cache"/>
</head>
<body>
<p>
Internal Server Error
</p>
</body>
</html>
```

Gambar 7. Vulnerability pada Remote OS Command Injector

f. Hasil Scanner oleh OWASP terhadap Open Jurnal System Local Network, dapat dilihat pada Gambar 8:

```
<!DOCTYPE html>
<!--[if IE 7]>
<html class="ie ie7" lang="en-US">
<![endif]-->
<!--[if IE 8]>
<html class="ie ie8" lang="en-US">
<![endif]-->
<!--[if !(IE 7) | !(IE 8) ]><!-->
<html lang="en-US">
<!--<![endif]-->
<head>
      <meta charset="UTF-8">
      <meta name="viewport" content="width=device-width"
      <link rel="pingback" href="http://irdp.info/xmlrpc
      <title>IRDP &#8211; Group of Journals</title>
<link rel='dns-prefetch' href='//fonts.googleapis.com'
```

Gambar 8. Vulnerability pada Remote OS Command Injector

g. Hasil Scanner oleh OWASP terhadap Open Jurnal System Local Network, dapat dilihat pada Gambar 9:

```
HTTP/1.1 200 OK
Cache-Control: no-cache, must-revalidate, max-age=0
Content-Type: text/html; charset=UTF-8
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Server: Microsoft-IIS/8.5
Set-Cookie: wordpress_test_cookie=WP+Cookie+check; path=/
X-Frame-Options: SAMEORIGIN
Set-Cookie: wordpress_cb63cd9a0e24f6a1a059205bd1b37da7=+; expires=Thu, 25-May-2017 04:35:31 GMT; Max-Age=-31536000;
Set-Cookie: wordpress_sec_cb63cd9a0e24f6a1a059205bd1b37da7=+; expires=Thu, 25-May-2017 04:35:31 GMT; Max-Age=-315360
```

Gambar 9. Vulnerability pada Remote OS Command Injector

h. Hasil Scanner oleh OWASP terhadap Open Jurnal System Local Network, dapat dilihat pada Gambar 10:

```
</p>
<p>
    <label for="user_pass">Password<br />
    <input type="password" name="pwd" id="user_pass" class="input" value="" size="20" /></label>
</p>
    <p class="forgetmenot"><label for="rememberme"><input name="rememberme" type="checkbox" id="rememberme
Remember Me</label></p>
 <p class="submit">
    <input type="submit" name="wp-submit" id="wp-submit" class="button button-primary button-large" value=
    <input type="hidden" name="redirect_to" value="http://irdp.info/wp-admin/" />
    <input type="hidden" name="testcookie" value="1" />
```

Gambar 10. Vulnerability pada Remote OS Command Injector

i. Hasil Scanner oleh OWASP terhadap Open Jurnal System Local Network:

```
<![endif]-->
<!--[if IE 8]>
<html class="ie ie8" lang="en-US">
<![endif]-->
<!--[if !(IE 7) | !(IE 8) ]><!-->
<html lang="en-US">
<!--<![endif]-->
<head>
     <meta charset="UTF-8">
     <meta name="viewport" content="width=device-width">
     <link rel="pingback" href="http://irdp.info/xmlrpc.php">
     <title>IRDP &#8211; Group of Journals</title>
<link rel='dns-prefetch' href='//fonts.googleapis.com' />
```

Gambar 11. Vulnerability pada Remote OS Command Injector

j. Hasil Scanner oleh OWASP terhadap Open Jurnal System Local Network:

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=UTF-8
Server: Microsoft-IIS/8.5
Link: <http://irdp.info/wp-json/>; rel="https://api.w.org/"
Link: <http://irdp.info/>; rel=shortlink
X-Powered-By: ASP.NET
X-Powered-By-Plesk: PleskWin
Date: Fri, 25 May 2018 04:34:41 GMT
Content-Length: 38987
```

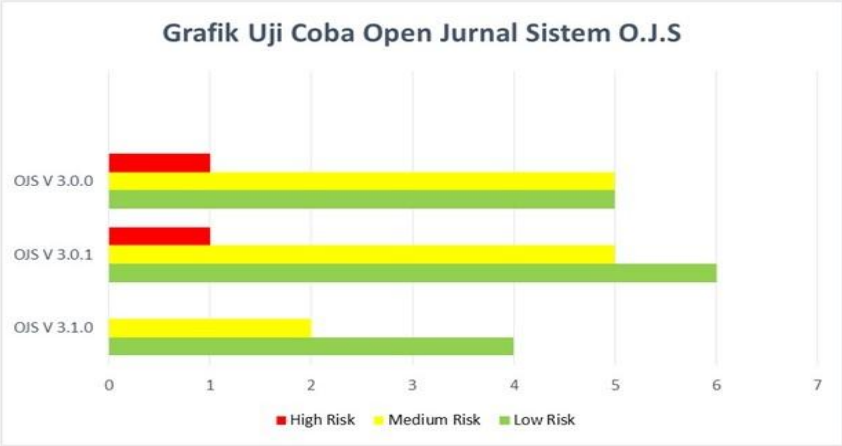
```
<!DOCTYPE html>
<!--[if IE 7]>
<html class="ie ie7" lang="en-US">
<![endif]-->
<!--[if IE 8]>
<html class="ie ie8" lang="en-US">
<![endif]-->
<!--[if !(IE 7) | !(IE 8) ]><!-->
<html lang="en-US">
<!--<![endif]-->
<head>
     <meta charset="UTF-8">
     <meta name="viewport" content="width=device-width">
     <link rel="pingback" href="http://irdp.info/xmlrpc.php">
     <title>IRDP &#8211; Group of Journals</title>
<link rel='dns-prefetch' href='//fonts.googleapis.com' />
```

Gambar 12. Vulnerability pada Remote OS Command Injector

Perbandingan Open Jurnal System pada webserver, dapat dilihat pada Gambar 13.

NO	Open Jurnal System Versi	Alert												RISK		
		Cross Site Scripting	Application Error Disclosure	Buffer OverFlow	Directory Browsing	Format String Error	X-Frame Option Header	Cookie No HttpOnly Flag	Cross-Domain Java Script File Inclusion	Password Autocomplete in Browser	Private IP Disclosure	Web Browser Xss Protection Not Enable	X-Content-Type Options Header Missing	High	Medium	Low
1	3.0.0	Reflected	1045	-	108	-	889	27	50	12	-	900	900	1	2042	1889
2	3.0.1	Reflected	175	-	17	-	90	28	52	14	3	95	96	1	282	288
3	3.1.0	-	239	-	-	-	239	18	-	9	173	175	83	-	316	458
4	Server 1 Realtime	2	-	-	-	-	934	1110	2589	2903	-	951	1002	11	934	8555
5	Server 2 Realtime	-	2	-	-	2	146	10	-	3	-	163	180	29	150	356

Gambar 13. Tabel Perhitungan dari Pengujian Baik LocalNetwork dan RealTime Penelitian pada Open Jurnal System pada 3 (Tiga) versi yang berbeda, dapat dilihat pada Gambar 14



Gamba 14. Grafik perbandingan pada Open Jurnal System (OJS)

4. KESIMPULAN

Pada pengujian di lab Informatika di temukan beberapa kerentanan dalam *open jurnal system* yang dapat menanipulasi file lokal, mengunggah file dengan melakukan serangan *Cross- Site Scripting* (*XSS*).

Pastikan filter XSS browser web diaktifkan, dengan mengatur *header respons X-XSS-Protection* HTTP ke '1'.

5. SARAN

Semoga penelitian selanjutnya dapat mengembangkan sistem lebih sempurna, dengan menggunakan metode yang baru, demi mendapatkan hasil yang lebih sempurna.

UCAPAN TERIMA KASIH

Saya mengucapkan terimakasih banyak atas dukungan nya pada pihak-pihak yang telah banyak membantu dalam penyusunan penelitian ini:

1. Allah SWT.
2. Kedua Orang tua saya. Anwar dan Siti Raodah
3. Dosen pembimbing saya: Bapak Dr. Imam Riadi, M.Kom, dan Bapak Anton Yudhana, M.T., Ph.D
4. Tim IT. Abdul Djalil Djayali, Om Handoko, Fazrul Rahman, Kelas Pagi Yogyakarta
5. Kedua Anak saya, Beserta Istri yang berada di kampang halaman.

DAFTAR PUSTAKA

[1] Shaimaa Khalifa Mahmoud, Marco Alfonse , Mohamed Ismail Roushdy, Abdel-Badeeh M.Salem., 2017, Acomparative Analysis of Cross Site Scripting (XSS) Detecting and Defensive Techniques, Vol. 8, Ed.2, IEEE / ICICIS International Conference on Intelligent Computing and Information Systems. Cairo,Egypt.

[2] Hua Zhang, Fang Lou, Yunsheng Fu, Zhihoung Tian,. 2017, A Conditional Probability Computation Method For Vulnerability Exploitation Based On CVSS, IEEE / Second International Conference on Data Science in Cyberspace. Institut of Computer Application, China Academy of Enginerring Physics, Mianyang, Sinhcuan, 621900, RRC.

[3] Angkita Gupta, Kavita, Kirandeep Kaut " Vulnerability Assesment and Penetration Testing" Computer Science Departemen, PEC University of Technology, India IJETT Vol 4 Issue3- 2013.

[4] Ahmad Budi Setiawan " peningkatan keamanan supervisiory control and Acquisiti (SCADA) Padasmart grid sebagai infastruktur kritis. kementrian komunikasi dan informatika JJPI Vol.6 No. 1 (2016) 59-78.

[5] Shaimaa Khalifa Mahmoud, Mohamed Ismail Roushdy, Marco Alfonse, Abdel-Badeeh M.Salem. *Acomparative Analysis of Cross Site Scripting (XSS) Detecting and Defensive Techniques*. Computer Science Department, Faculty of Computer and Information Sciences. Ain Shams University. Cairo, Egypt. 2017, Vol 8.

[6] J. Breckling, Ed., *The Analysis of Directional Time Series: Applications to Wind Speed and Direction*, ser. Lecture Notes in Statistics. Berlin, Germany: Springer, 1989, vol. 61.

[7] S. Zhang, C. Zhu, J. K. O. Sin, and P. K. T. Mok, “A novel ultrathin elevated channel low-temperature poly-Si TFT,” *IEEE Electron Device Lett.*, vol. 20, pp. 569–571, Nov. 1999.

[8] M. Wegmuller, J. P. von der Weid, P. Oberson, and N. Gisin, “High resolution fiber distributed measurements with coherent OFDR,” in *Proc. ECOC’00*, 2000, paper 11.3.4, p. 109.

[9] Maryana Yevdokymenko, Elsayed Mohamed, Paul Onwuakpa Arinze.2017. Ethical Hacking and Penetration Testing Using Raspberry PI. International Scientific-Pactical Conference, Problems of Infocommunications. Science and Technology.(PIC S&T 2017).Kharkiv National University of Radio Electronics Kharkiv, Ukraine.

[10] Da-Yu KAO, Yu-Siang WANG, Fu-Ching TSAI, Chien-Hung CHEN.2018. Forensic Analysis of Network packets from Penetration Test Toolkits. ICACT2018. Ferbruari 11-14, 2018. International Conference on Advanced Communications Technology (ICACT). Departemen of Information Management, Central police University, Taiwan.