Respati Jurnal Vol 10, No 29 (2015)-1 (1)

by By Reytechno

Submission date: 11-Oct-2023 01:22PM (UTC+0700)
Submission ID: 2185301416
File name: Respati_Jurnal_Vol_10,_No_29_2015_-1_1.pdf (594.78K)
Word count: 3417
Character count: 20121

CONTINGENCY PLANNING PADA WEBSITE UNIVERSITAS WIDYA DHARMA

Agustinus Suradi[1], Hendro Joko Prasetyo[2],
E-mail: simpati2000@mailcity.com[1], hendromkom@yahoo.co.id[2],

ABSTRACT

Various information can be found on the internet by accessing the website. Information on the internet should be guaranteed integrity and service / layananya from the source to the user. In website development, technology profile, access speed, and security is a factor that must be taken to ensure that the information and services contained therein can be useful for the user.

Internet network is public and global, at the time of service of data sent from one computer to another on the Internet, the data will pass through a number of computers. Denial-of-Service Attack is one of the attacks on web security system which can inhibit the activity of the working of a service or turn it off, so the user has the right / interest can not use these services as expected.

Services web application has vulnerability to an attack. One way to detect security flaws in web applications is to use a search application security loopholes. OWASP (Open Web Application Security Project) capable of searching for security loopholes website. There are some striking technique, among others: Cross Site Scripting, Injection, Malicious File Execution, Insecure Direct Object Reference and others. Results from this study is the method of coping and prevention techniques of Denial Of Service Attack, and improved service website.

Keywords: Technology profile, OWASP, Denial Of Service Attack.

1. PENDAHULUAN

1.1. Latar Belakang

Sejalan dengan kemajuan teknologi informasi dewasa ini, kebutuhan informasi di website semakin sangat diperlukan karena sangat efektif dan efisien. Kemampuan untuk menyediakan dan mengakses informasi secara cepat dan akurat menjadi sangat esensial bagi sebuah organisasi

Kecepatan akses, *service* dan keamanan merupakan faktor penting yang perlu diperhatikan dalam pengoperasian sistem informasi lewat website. Selain itu, saat ini w*ebsite* tidak hanya dijadikan layanan untuk memberikan informasi statis, tetapi telah berkembang dengan ditambahkannya fitur-fitur untuk melakukan interaksi/ transaksi secara *on-line*.

Pemantauan terhadap keamanan sistem informasi harus selalu dilakukan meskipun sebuah sistem informasi sudah memiliki perangkat pengamanan yang cukup baik. Hal ini disebabkan oleh beberapa hal, antara lain:

1. Ditemukannya lubang keamanan *(security hole)* yang baru. Perangkat lunak dan perangkat keras biasanya sangat kompleks sehingga tidak mungkin untuk diuji secara menyeluruh. Kadang-kadang muncul lubang keamanan yang ditimbulkan oleh faktor implementasi.
2. Adanya serangan dari pihak yang tidak bertanggung jawab dengan memanfaatkan lubang keamanan atau kelemahan pada sistem yang bisa dieksploitasi, kemudian berusaha untuk mengambil informasi atau memanipulasi informasi tersebut.

Sebagai upaya yang lebih serius dan lebih *aware* terhadap keamanan, kualitas dan ketersediaan layanan teknologi informasi terhadap suatu kondisi yang tidak diinginkan

yang menyebabkan terhentinya sebagian atau keseluruhan layanan website, maka bertolak dari hal diatas penelitian ini dilaksanakan untuk melakukan analisis *contingency planning* keamanan dan kualitas sistem informasi website yang ada.

1.2. Rumusan Masalah

Dari latar belakang di atas, akan muncul beberapa permasalahan yang berkaitan dengan keamanan sistem informasi website Universitas Widya Dharma Klaten, antara lain mengenai:

1. Apa yang menjadi penyebab terjadinya serangan yang menjadi ancaman pada website Universitas Widya Dharma Klaten?
2. Bagaimana cara menganalisis bahwa pada website Universitas Widya Dharma Klaten mempunyai celah keamanan *(security hole)*?
3. Bagaimana cara untuk menentukan level resiko yang berkaitan dengan adanya celah keamanan *(security hole)* dan kebijakan apa yang arus dilakukan berkenaaan dengan *contingency planning website* Universitas Widya Dharma Klaten?

2. TINJAUAN PUSTAKA

2.1. *Content Management System*

CMS merupakan singkatan dari *Content Management System* yaitu merupakan suatu aplikasi yang bertujuan untuk memudahkan pengelolaan konten dalam sebuah website dan aplikasinya sehingga website menjadi dinamis dan interaktif. Beberapa pilihan CMS seperti: Wordperss, Joomla, XOOPs, Mambo, Vbuletin, Drupal, Opencart, atau Formulasi dan masih banyak lagi yang bermunculan dipasaran, yang dapat membantu membangun sebuah website serta fiturnya. Setiap pilihan CMS mempunyai keunggulan dan kelemahan masing-masing.

2.2. *Web Defacement*

Keamanan website rentan terhadap beberapa ancaman. Web Defacement adalah serangan dengan tujuan utama merubah tampilan sebuah website baik halaman utama maupun halaman lain terkait dengannya diistilahkan sebagai Web Defacement. Hal ini biasa dilakukan oleh para attacker atau penyerang karena berbagai hal dan memungkinkan untuk diserang sehingga website yang terkait dengannya menjadi sasaran.

Pada dasarnya *deface* dapat dibagi menjadi dua jenis berdasarkan dampak pada halaman situs yang terkena serangan terkait.

1. Jenis pertama adalah suatu serangan dimana penyerang merubah/*deface* satu halaman penuh tampilan depan alias *file index* atau *file* lainnya yang akan diubah secara utuh.
2. Jenis kedua adalah suatu serangan dimana penyerang hanya merubah sebagian atau hanya menambahi halaman yang di-deface.

2.3. *Denial of Services*

Denial of Services (DoS), serangan yang dikenal dengan istilah DoS dan D DoS (Distributed Denial of Services) ini pada dasarnya merupakan suatu aktivitas dengan tujuan utama menghentikan atau meniadakan layanan/ services sistem atau jaringan komputer sehingga pengguna tidak dapat menikmati fungsionalitas dari layanan tersebut dengan cara mengganggu ketersediaan komponen sumber daya yang terkait dengannya. Contohnya adalah dengan cara memutus koneksi antar dua sistem, membanjiri kanal akses dengan jutaan paket, menghabiskan memori dengan cara melakukan aktivitas yang tidak perlu, dan lain sebagainya.

Dengan kata lain, DOS/ D DoS merupakan serangan untuk melumpuhkan sebuah layanan dengan cara menghabiskan sumber daya yang diperlukan sistem komputer untuk melakukan kegiatan normalnya. Adapun sumber daya yang biasa diserang misalnya: kanal komunikasi/ *bandwidth*, *kernel tables*, *swap space*, *RAM*, *cache memories*, dan lain sebagainya.

Menurut *OWASP* (*The Open Web Application Security Project*) ada sepuluh macam serangan yang sering terjadi pada web application. *OWASP* adalah sebuah non profit komuniti yang bertujuan untuk mengembangkan metodologi, program program, dokumentasi dan sebagainya yang berhubungan dengan keamanan *website application*. Data dari *OWASP* menunjukkan bahwa dalam lima tahun terakhir teknik serangan tidak berubah yaitu:

A1. Cross Site Scripting (XSS)
A2 . Injection Flaws
A3 . Malicious File Execution
A4 . Insecure Direct Object Reference
A5. Cross Site Request Forgery (CSRF)
A6. Information Leakage and Improper Error Handling
A7. Broken Authentication and Session Management
A8. Insecure Cryptographic Storage
A9. Insecure Communications
A10. Failure to Restrict URL Access

3. METODE PENELITIAN

3.1 Metodologi Penelitian

Penelitian deskriptif bertujuan untuk menggambarkan fakta-fakta tentang masalah yang diteliti sebagaimana adanya, juga memberikan gambaran situasi kejadian atau memberikan hubungan antara fenomena, pengujian hipotesis-hipotesis, membuat prediksi dan implikasi suatu masalah yang ingin dipecahkan (Nawawi, 2003; Singarimbun dan Efendi, 1989).

3.2 Vulnerability Assessment Methodology

- *Adjusting Scope*
- *Information Gathering*
- *Target Identification*
- *Network Mapping/ Target enumeration*
- *Application Assessment*

4. HASIL DAN PEMBAHASAN

4.1 Profile Website.

Dengan menggunakan software IPNetInfo memungkinkan untuk menemukan semua informasi yang tersedia tentang alamat IP, Pemilik, negara / nama negara, kisaran alamat IP, informasi kontak dan informasi identifikasi lainnya. Setelah kita ping www.unwidha.ac.id kita dapat IP address: 103.23.151.119. dengan range 103.23.151.0 – 255.

Hasil identifikasi sebagai berikut
(diakses pada 22 Mei 2015)

```
% [whois.apnic.net]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html
% Information related to '103.23.151.0 - 103.23.151.255'
inetnum:        103.23.151.0 - 103.23.151.255
netname:        SCNG-ID
country:        ID
admin-c:        SWA2-AP
tech-c:         SH1746-AP
    remarks:    Send Spam & Abuse Reports to abuse.noc@scn-group.co.id
    mnt-by:     MNT-APJII-ID
```

mnt-routes: MAINT-ID-SCNG
mnt-irt: IRT-SCNG-ID
status: ASSIGNED PORTABLE
changed: hm-changed@apnic.net 20111202
abuse-mailbox: abuse.noc@scn-group.co.id
auth: # Filtered
changed: abuse.noc@scn-group.co.id 20111103
changed: hostmaster@idnic.net 20111103
source: APNIC
mail: hostmaster@scn-group.co.id
nic-hdl: SH1746-AP
mnt-by: MAINT-ID-SCNG
changed: hostmaster@idnic.net 20111101
source: APNIC
mnt-by: MAINT-ID-SCNG
source: APNIC
% Information related to '103.23.151.0/24AS58402'
route: 103.23.151.0/24
descr: Route object of PT Smart Communication Network group
descr: Corporate / Direct Member IDNIC
descr: Jawa Tengah
origin: AS58402
country: ID
mnt-by: MAINT-ID-SCNG
nged: hostmaster@idnic.net 20120106
source: APNIC
% This query was served by the APNIC Whois Service version 1.69.1-APNICv1r3 (WHOIS3)

4.2 Technology Profile

Seiring perkembangan teknologi di berbagai bidang, dalam teknologi website pun banyak terdapat perkembangan. Dibawah ini rincian teknologi profile website unwidha.ac.id : Bottom of Form

***Technology Profile* : www.unwidha.ac.id**

Web Server

Apache 2.2

Email Services

Google Apps for Business

Content Management Systems

WordPress 4.0

WordPress 4.0 Usage Statistics - Websites using WordPress 4.0

Frameworks

PHP

PHP Usage Statistics - Websites using PHP

Analytics and Tracking

Google Analytics Usage Statistics - Websites using Google Analytics

Google Universal Analytics Usage Statistics - Websites using Google Universal Analytics

JavaScript Libraries

jQuery Usage Statistics - Websites using jQuery

FlexSlider Usage Statistics - Websites using FlexSlider

Mobile

Mobile Non Scaleable Content

Mobile Non Scaleable Content Usage Statistics - Websites using Mobile Non Scaleable Content

Widgets

Google Font API Usage Statistics - Websites using Google Font API

Aggregation Functionality

Really Simple Discovery
Google FeedProxy
FeedBurner
Live Writer Support
Pingback Support

Document Information

Cascading Style Sheets
JSON-LD
HTML 5 Specific Tags
Javascript
Meta Keywords
Meta Description
Meta Robot
HTML5 DocType
X-UA-Compatible

Encoding

UTF-8

Server Information

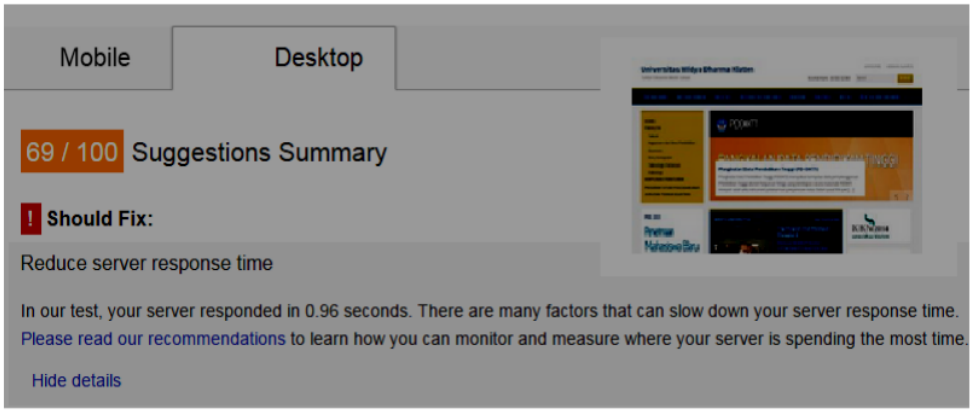
Ubuntu

CSS Media Queries

Max Width

4.3 Page speed

Pada umumnya *user* tidak menyukai halaman yang berat dan lama dalam menyajikan informasi yang dicari *user*. Mereka lebih cendrung meninggalkan halaman yang berat dari pada harus menunggu hingga informasi ditampilkan, *Speed* ketika diakses perangkat mobile ***64/100*** . *Speed page* ketika diakses perangkat *PC dekstop:* **69/100**



Gambar 4.3 Speed page dekstop

Solusi peningkatan *page speed* dengan mengubah format dan kompresi gambar agar berukuran kecil tetapi kualitas gambar harus terjaga.

Improve Server Response Time

This rule triggers when PageSpeed Insights detects that your server response time is above 200 ms.

Overview:

Server response time measures how long it takes to load the necessary HTML to begin rendering the page from your server, subtracting out the network

latency between Google and your server. There may be variance from one run to the next, but the differences should not be too large. In fact, highly variable server response time may indicate an underlying performance issue.

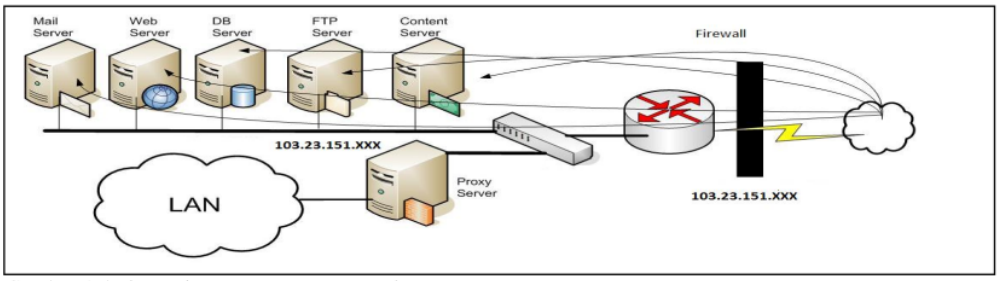
Recommendations developers.google.com/

You should reduce your server response time under 200ms. There are dozens of potential factors which may slow down the response of your server: slow application logic, slow database queries, slow routing, frameworks, libraries, resource CPU starvation, or memory starvation. You need to consider all of these factors to improve your server's response time. The first step to uncovering why server response time is high is to measure. Then, with data in hand, consult the appropriate guides for how to address the problem. Once the issues are resolved, you must continue measuring your server response times and address any future performance bottlenecks

a. *Gather and inspect existing performance and data. If none is available, evaluate using an automated web application monitoring solution (there are hosted and open source versions available for most platforms), or add custom instrumentation.*
b. *Identify and fix top performance bottlenecks. If you are using a popular web framework, or content management platform, consult the documentation for performance optimization best practices.*
c. *Monitor and alert for any future performance regressions!*

4.4 Network Mapping

Pemetaan jaringan adalah studi dari konektivitas fisik dari jaringan. Pemetaan jaringan digunakan untuk menentukan server dan sistem operasi yang berjalan di jaringan. Hal ini berfungsi untuk menemukan kemungkinan memiliki: sistem operasi, *port* terbuka, melihat layanan jaringan, dan lainya, kegiatan ini sering disebut scanning port dan lebih mirip dengan pengujian penetrasi atau kegiatan ini diibaratkan menggedor pintu jaringan kita dengan harapan ada jawaban dari dalam jaringan.



Gambar 4.5 Ilustrasi proses *scaning network*.

Hasil *network mapping* unwidha.ac.id dengan Nmap sebagai berikut :

103.23.151.119 IP address Information

The IP address 103.23.151.119 was found in . , Smart Net. Additional IP location information, as well as network tools are available below.

103.23.151.0 IP address Information

The IP address 103.23.151.0 was found in . , Smart Net. Additional IP location information, as well as network tools are available below.

IP address:	**103.23.151.0**
Organization:	Smart Net

traceroute

check latency

whois

BGP routing info

blacklist check

```
traceroute to 103.23.151.0 (103.23.151.0), 30 hops max, 60 byte packets
1  68-67-73-17.static.as19844.net (68.67.73.17)  0.227 ms  0.303 ms  0.393 ms
2  ve101.e2-17.core-a.jcvnflcq.as19844.net (198.205.127.5)  0.270 ms  0.333 ms  0.373 ms
3  ve100.e2-9.core-b.jcvnflcq.as19844.net (198.205.127.2)  0.246 ms  0.337 ms  0.373 ms
4  ix-7-1-0-56.tcore1.A56-Atlanta.as6453.net (64.86.113.65)  6.253 ms  6.262 ms  6.252 ms
5  if-15-2.tcore1.DT8-Dallas.as6453.net (66.110.56.93)  240.546 ms * *
6  if-2-2.tcore2.DT8-Dallas.as6453.net (66.110.56.6)  239.197 ms  234.642 ms  233.510 ms
7  if-8-2.tcore1.LVW-Los-Angeles.as6453.net (66.110.57.82)  234.239 ms  232.672 ms  232.993 ms
8  if-2-2.tcore2.LVW-Los-Angeles.as6453.net (66.110.59.2)  241.412 ms  243.547 ms  242.182 ms
9  if-7-2.tcore2.SVW-Singapore.as6453.net (180.87.15.25)  234.554 ms  235.064 ms  235.317 ms
10  if-2-2.tcore1.SVW-Singapore.as6453.net (180.87.12.1)  234.391 ms  232.591 ms  232.598 ms
11  180.87.12.6 (180.87.12.6)  247.087 ms  235.074 ms  233.830 ms
12  supernet-05.1-1-14.edge2-eqx-sin.moratelindo.co.id (202.43.176.222)  247.216 ms  245.839 ms  246.262 ms
13  * * *
14  103.8.63.42 (103.8.63.42)  255.403 ms  259.602 ms  249.419 ms
15  ipv4-230-33-78.as55666.net (112.78.33.230)  258.161 ms  258.156 ms  257.751 ms
16  49.128.183.102 (49.128.183.102)  259.671 ms  264.218 ms  258.489 ms
17  ipv4-6-177-128.as55666.net (49.128.177.6)  262.106 ms  260.393 ms  272.316 ms
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
```

30 * * *

103.23.151.0 IP address Information

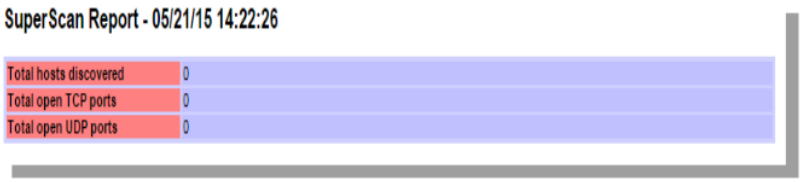
The IP address 103.23.151.0 was found in . , Smart Net. Additional IP location information, as well as network tools are available below.

Checking IP against the top SPAM source databases and Email Policy block lists... Note this may include some end-user IP address ranges which should not be delivering unauthenticated SMTP email.

103.23.151.0 is not blacklisted in SPAM/Exploits databases.

103.23.151.0 is not in any known email block lists, including ISP Policy blocks.

Hasil Superscan 4.0 sebagai berikut:



Gambar 4.6 Laporan super scan 4.0

The IP list contains 1 entries
Service TCP ports: 179
Service UDP ports: 88
Packet delay: 10
Discovery passes: 1
ICMP pinging for host discovery: Yes
Host discovery ICMP timeout: 2000
TCP banner grabbing timeout: 8000
UDP banner grabbing timeout: 8000
Service scan passes: 1
Hostname resolving passes: 1
Full connect TCP scanning for service scanning: No
Service scanning TCP timeout: 4000
Service scanning UDP timeout: 2000
TCP source port: 0
UDP source port: 0
Enable hostname lookup: Yes
Enable banner grabbing: Yes
Scan started: 05/21/15 14:22:26
------- Scan of 1 hosts started -------
Scanning 1 machines with 1 remaining.
------- Host discovery pass 1 of 1 -------
Host discovery ICMP (Echo) scan (1 hosts)...

0 new machines discovered with ICMP (Echo)

Reporting scan results...

------- Scan done -------

Discovery scan finished: 05/21/15 14:22:28

4.5 Vulnerability website

Hasil pencarian celah keamanan website unwidha.ac.id dengan OWASP akhirnya dapat diketahui tingkat resiko yang mungkin terjadi adalah sebagai berikut:

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	3
Low	31
Informational	0

Gambar 4.8 Laporan celah keamanan dan tingkat resiko

Hasil Analisa terhadap celah keamanan dan Solusi rekomendasi OWASP (Risk Level Medium)

Level Medium	**X-Frame-Options Header Not Set**
Deskripsi	X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.
Website	http://www.unwidha.ac.id
Referensi	http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx

Level Medium	**X-Frame-Options Header Not Set**
Deskripsi	X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.
Website	http://www.unwidha.ac.id/robots.txt
Referensi	http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx\

Level Medium	**X-Frame-Options Header Not Set**
Deskripsi	X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.
Website	http://www.unwidha.ac.id/sitemap.xml

Referensi	http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx
Solusi	Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (if you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. ALLOW-FROM allows specific websites to frame the web page in supported web browsers).

4.6 Contingency Plan

Pengamanan dikategorikan menjadi dua jenis: *preventif* dan *recovery*. Usaha pencegahan dilakukan agar sistem informasi tidak memiliki/ seminimal munkin memiliki celah keamanan/ vulnerability, sementara usaha-usaha perbaikan dilakukan apabila celah keamanan sudah dieksploitasi.

Selain melakukan recomendasi yang disarankan, juga perlu peningkatan pengamanan. Pengamanan sistem informasi dapat dikembangkan ke beberapa layer yang berbeda. Misalnya di layer transport, dapat digunakan *Secure Socket Layer* (SSL), selain secara fisik, sudah diamankan dengan menggunakan firewall.

Untuk usaha preventif yang lain juga perlu dilakukan peningkatan :

- Access Control berlapis
- Peningkatan autentifikasi password (program password *cracker*)
- Memasang Poteksi (misalnya *tcpwrapper)*
- Peningkatan filter Firewall
- Adanya *intruder detection system* (IDS).
- Pemantau integritas sistem (contohnya *Tripwire di unix)*
- Audit (mengamati berkas log)
- *Backup* secara rutin
- *Enkripsi* untuk keamanan
- Telnet atau shell aman

Dengan mengikuti semua tahapan diatas diharapkan segala bentuk ancaman yang mungkin akan terjadi dapat dicegah atau dapat di recovery kembali.

4.7 Kebijakan Prosedure

Setiap organisasi akan selalu memiliki pedoman (*Standart Operating Procedure*) bagi karyawannya untuk mencapai sasarannya.

Dengan adanya *Standart Operating Procedure* yang jelas dan baik diharapkan setiap komponen akan dapat menjalankan fungsinya dengan baik sehingga resiko yang mungkin akan timbul dapat ditiadakan.

5. KESIMPULAN DAN SARAN

5.1. Kesimpulan

Berdasarkan hasil identifikasi pada pembahasan, maka penyusun dapat menyimpulkan bahwa :

1. Serangan ke sistem *website* bisa terjadi karena terdapatnya *security hole*/ celah keamanan yang memungkinkan seorang attacker masuk kedalam sistem *website*.
2. Analisis celah keamanan website dapat menggunakan suatu aplikasi, *The Open Web Application Security Project* (OWASP ZAP) adalah *project open source* yang dapat dipergunakan untuk

membantu mencari *celah keamanan suatu website* dan menetapkan skor resiko/ *risk level*.

3. Usaha pencegahan terhadap serangan website dapat dilakukan dengan menutup celah keamanan seperti pemasangan proteksi, filter firewall, autentifikasi password, enkripsi, mencegah script injection masuk, adanya intruder detection system serta audit, sedangkan backup data diperlukan untuk recovery apabila celah keamanan sudah dieksploitasi.\

5.2. Saran

Saran yang dapat diberikan pada penelitian ini adalah:

1. Vulnerability perlu mendapat perhatian terhadap kemungkinan terjadi *defacement web* dan *Denial Of Service Attack*.
2. Peningkatan *technology profile*, *speed page* dan *service website* untuk peningkatan layanan pada *website* Universitas Widya Dharma.

DAFTAR PUSTAKA

1) Anley, C., 2002, Advanced SQL Injection in SQL Server Applications. AnNGSSoftware Insight Security Research (NISR) Publications: Next Generation Security Software Ltd.
2) Baryamureeba,V., Tushabe, F., 2004, The Enhanced Digital Investigation Process Model. Proceedings of the Fourth Digital Forensic Research Workshop, May 27.
3) Caroline, Yunita; Surendro, Kridanto. 2008. Pengembangan Rencana Penanggulangan Bencana (*Disaster Recovery Planning*) untuk Data Center ITB. Paper yang dipresentasikan pada Konferensi dan Temu Nasional Teknologi Informasi dan Komunikasi untuk Indonesia. Bandung: Institut Teknologi Bandung.
4) Clarke, J., 2009, SQL Injection Attacks and Defense. Burlington: Syngress Publishing and Elseiver.
5) Halfond, W.G.J., Orso, A., 2005., AMNESIA: Analysis and Monitoring for NEutralizing SQLInjection Attacks. IEEE and ACM Intern. Conf. On Automated Software Engineering (ASE 2005). Hal. 174–183, Nov. 2005.
6) M.Chandrika K., Ary Mazharuddin S., Baskoro AP, 2012, Pencari celah keamanan pada aplikasi web, Institut Teknologi Sepuluh Nopember, Surabaya.
7) OWASP. Testing for User Enumeration (Internet). https://www.owasp.org/index.php/
8) Solehudin, Usep. 2005. *"Business Continuity and Disaster Recovery Plan"*. Universitas Indonesia.

Respati Jurnal Vol 10, No 29 (2015)-1 (1)

ORIGINALITY REPORT

23%	21%	4%	10%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.awwwards.com Internet Source	2%
2	alagema.blogspot.com Internet Source	2%
3	Submitted to Fiji National University Student Paper	2%
4	whitecurant.blogspot.com Internet Source	2%
5	Submitted to De Montfort University Student Paper	2%
6	mronisob4ri.blogspot.com Internet Source	1%
7	jelajahiya.blogspot.com Internet Source	1%
8	Submitted to Universitas Nasional Student Paper	1%
9	eptikb51t6.blogspot.com Internet Source	1%

10	elearning.stmik-indonesia.ac.id Internet Source	1 %
11	digitalsinology.org Internet Source	1 %
12	text-id.123dok.com Internet Source	1 %
13	Submitted to Carnegie Mellon University Student Paper	1 %
14	cupcap.blogspot.com Internet Source	1 %
15	dittalestari.wordpress.com Internet Source	1 %
16	irfanhairis2014.wordpress.com Internet Source	1 %
17	kharismap1.blogspot.com Internet Source	1 %
18	diahafriantirahayu.blogspot.com Internet Source	1 %
19	www.ncbi.nlm.nih.gov Internet Source	1 %
20	nerd.cesnet.cz Internet Source	1 %

Exclude quotes	Off	Exclude matches	< 1%
Exclude bibliography	On		