Analisis Serangan Deface Menggunakan Backdoor Shell Pada Website

Analysis of Deface Attacks Using Backdoor Shell On Websites

Muhammad Siddik Hasibuan[1], Lipantri Mashur Gultom[2]
[1,2] Teknologi Komputer, Politeknik LP3I Medan, Jl.Amaliun No.37 Medan 061-7322649
e-mail: [1]mhdsiddikhasibuan@gmail.com, [2]lipantri@gmail.com

Abstrak

Indonesia sempat heboh dengan di retasnya situs operator seluler terkemuka, aksi peretasan ini seperti silih berganti dengan diretasnya situs operator seluler lainnya. Serangan pada website adalah hal yang sering terjadi di dunia maya, jenis serangannya pun berbeda-beda. Salah satunya deface, serangan deface membuktikan kerentanan dalam suatu website. Banyak pengembang website kurang memperhatikan hal tersebut. Seharusnya agar pengembang menerapkan sistem keamanan yang optimal dari berbagai serangan baik serangan tradisional maupun yang terbaru. Salah satunya, *Backdoor Shell* adalah tipe serangan yang baru dalam aktifitas deface, merupakan sebuah code-code yang disusun menjadi script rahasia digunakan untuk mengendalikan sebuah website/server. Serangan ini salah satu upaya untuk melakukan deface pada sebuah website. Penelitian ini menganalisi celah keamanan dari web pemerintah dan BUMN yang menggunakan domain *.go.id. Dari penelitian ini menghasilkan suatu model penanganan dari serangan deface maupun sejenisnya. Dari penelitian ini dapat menganalisis serangan deface agar menjadi alat untuk pencegahan dari hal tersebut. Model penelitian ini dilakukan dengan 2 tahapan yaitu tahapan Dorking dan Exploit.

Kata kunci*— Deface, Backdoor Shell, Dorking, Exploit*

Abstract

*Indonesia had a scene with the hacked site of leading mobile operators, this hacking action like one after another with another hacking on other mobile operator site. Attack on the website is a common thing in cyberspace, the type of attack is different. One of them deface, deface attack to prove vulnerability in a website. Many website developers pay less attention to it. It should be for developers to implement an optimal security system from various attacks both traditional and recent attacks. One of them, Backdoor Shell is a new type of attack in deface activity, is a code-code compiled into a secret script used to control a website / server. This attack is an attempt to deface a website. This study analyzes the security holes of government web and stateowned companies that use the * .go.id domain. From this research resulted a model of handling of deface attack and the like. From this research can analyze deface attacks to be a tool for prevention of it. This research model is done by 2 stages of Dorking stage and Exploit.*

Keywords*— Deface, Backdoor Shell, Dorking, Exploit*

1. PENDAHULUAN

Indonesia sempat heboh dengan di retasnya situs operator seluler terkemuka, aksi peretasan ini seperti silih berganti dengan diretasnya situs operator seluler lainnya. *Cybercrime* dapat didefinisikan sebagai perbuatan melanggar hukum yang dilakukan dengan menggunakan fasilitas internet dengan menggunakan teknologi komputer dan telekomunikasi. Ada beberapa pendapat lain mengenai definisi dari istilah *Cybercrime* seperti dibawah ini : " The U.S Department of justice " memberikan pengertian kejahatan komputer atau *Cybercrime* sebagai

berikut : " …*any illegal act requiring knowledge of computer technology for its perpetration, investigation, or prosecution* ", [1]

Menurut UU ITE No 11 tahun 2008 "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik". Dalam UU ITE tersebut dikatakan melakukan manipulasi, manipulasi disini adalah merubah halaman website atau sejenisnya menjadi tidak sesuai akan mendapatkan sanksi hukum. Aksi peretasan ini kita lihat seperti hal yang biasa terjadi untuk media website, aksi yang sering terjadi untuk meretas website adalah deface. Deface adalah melakukan perubahan pada halaman web pada situs-situs tertentu, yang dilakukan oleh para hacker atau team tertentu dengan gerakan undergroundnya sebagai sebuah *cyber gang fight* untuk mengganggu informasi yang dimunculkan pada halaman situs yang dimaksud.

Menurut [2] pentingnya aspek keamanan komputer dalam teknologi informasi membuat banyak perusahaan untuk mengembangkan perangkat lunak yang menjadikan aspek keamanan komputer sebagai bisnis utamanya.

Perkembangan jaringan, cybercrime memiliki banyak jenis kejahatan, termasuk serangan jaringan, penipuan mail, intimidasi, pelanggaran hak cipta, dan sebagainya. Untuk serangan jaringan, banyak pendekatan telah diajukan dan digunakan untuk mendeteksi dan pertahanan. Namun, setelah serangan jaringan dikonfirmasi atau kejahatan lainnya ada, masih perlu dilakukan prosedur penyidikan oleh penyidik, mengumpulkan bukti-bukti yang berkaitan dengan kejahatan tersebut, menemukan pelaku, dan mengadili mereka. [3]

Defacer adalah sebutan orang atau kelompok yang melakukan deface, defacer mencari celah keamanan website agar bisa di deface, melakukan penelitian terhadap *sourcecode* yang ada, melihat update *vulnerability* dari website-website security yang ada di jagad raya. Berdiskusi di forum untuk menemukan dan memecahkan sesuatu yang tidak bisa dipecahkan. Hal inilah yang biasanya hampir tidak pernah dilakukan oleh Webmaster & Administrator. Defacer ini bisa melakukan di lokasi manapun dan oleh banya decafer. Untuk dapat melakukan web deface, defacer melakukan beberapa tahap sebagai berikut :

1. Mencari kelemahan pada sistem security, menemukan celah yang dapat dimasuki untuk melakukan eksplorasi di server target. Dia akan melakukan scanning tentang sistem operasi, service pack, service yang enable, port yang terbuka, dan lain sebagainya. Kemudian dianalisa celah mana yang bisa dimasuki.
2. Melakukan penyusupan ke server korban. Teknik ini dia akan menggunakan beberapa tools, file yang akan disisipkan, file exploit yang dibuat sengaja untuk di-copy-kan. Setelah berhasil masuk, tangan-tangan defacer bisa mengobok-obok isi server. Tapi tidak adil kiranya jika hanya sharing tentang teknik deface web. Maka untuk pengelola situs harus waspada, karena deface bisa jadi bencana yang sangat merepotkan. Pekerjaan menata ulang dan memperbaiki bagian yang rusak, bukan pekerjaan yang mudah.

Serangan deface terhadap situs perusahaan adalah yang paling rentan terjadi, data yang tersimpan didalam sistem informasi mereka dapat berguna bagi penjahat. Mereka berfokus pada kerusakan pada aliran data dengan memcoba merusak website perusahaan. [4]

Penanganan deface perlu diatasi dengan cepat, karena kalu tidak bisa merepotkan penyedia informasi, karena informasi yang disajikan tidak bisa di gunakan oleh pihak yang membutuhkan. Oleh karena itu peneliti ingin menganalisa sistem yang digunakan untuk mendeface serta cara menangulannginya.

Menurut [5] situs olahraga adalah yang paling sering diserang oleh kelompok hacker, log yang ditemukan menunjukan secara khusus telah mengeksploitasi kerentanan SQL dalam kode Dreamweaver-generatif.

Salah satu cara untuk melakukan kejahatan deface adalah menggunakan *backdoor shell*. *Backdoor Shell* merupakan sebuah code-code yang disusun menjadi script rahasia digunakan untuk mengendalikan sebuah website/server. Backdoor dalam dunia hacker memiliki arti

membuat pintu belakang apabila akan meninggalkan host yang sudah dimasuki. Pintu ini adalah password login. Backdoor ini berguna apabila cracker ingin kembali ke host / server tersebut, karena jika password root atau admin telah diganti, kita masih bisa masuk menggunakan password backdoor yang telah dipasang. [6]

2. METODE PENELITIAN

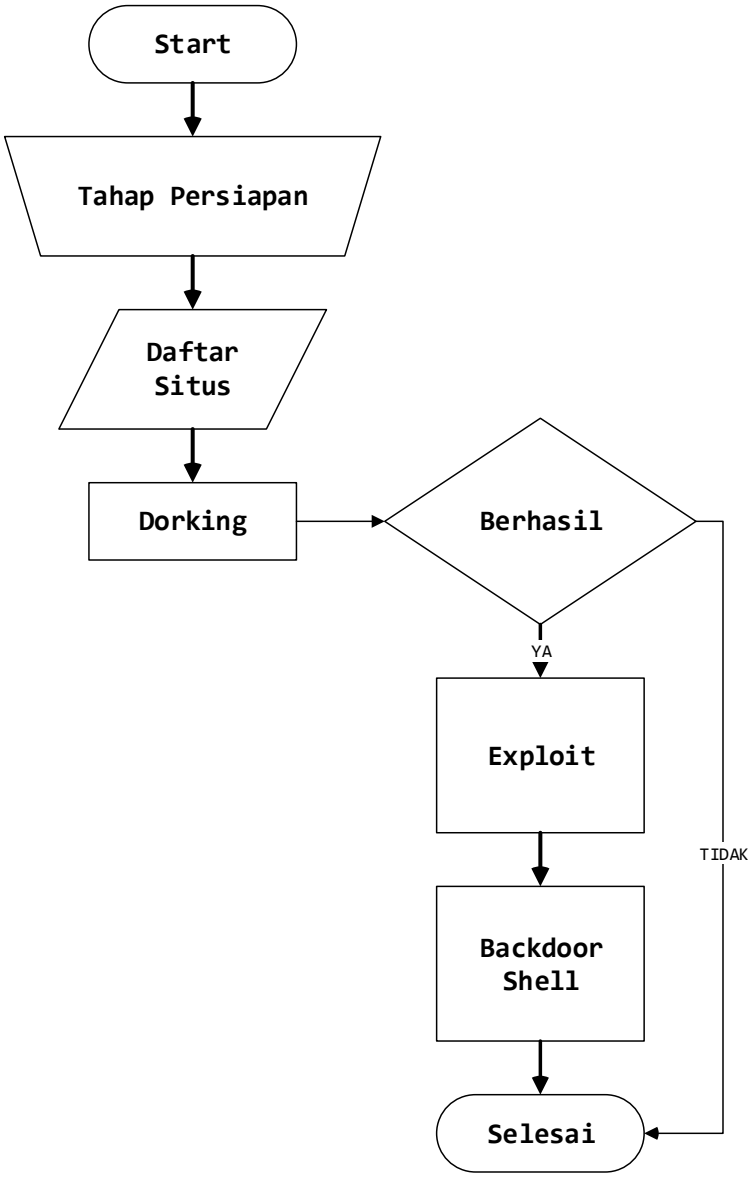
2.1. Tahapan-tahapan Penelitian

Secara umum ada 3 tahapan utama dalam penelitian yang akan dilakukan. Tahapan tersebut adalah :

1. Tahapan persiapan
   Tahapan ini dimulai dengan mengkaji permasalan yang ada kemudian melakukan kajian literature tentang penelitian sejenis yang pernah dilakukan.
2. Tahapan pengumpulan data
   Pada tahanpan ini dilakukan pengumpulan data dengan melakukan pengukuran terhadap variable-variabel yang telah ditentukan.
3. Tahapan Implementasi dan Pengujian
   i. Pre-attack phase : mengumpulkan informasi dengan footprinting dari website yang akan di uji. Website yang akan diuji diambil dari domain *.go.id yang merupakan website resmi pemerintahan dan BUMN.
   ii. Attack phase : mencoba melakukan serangan dari informasi yang didapat dari tahapan sebelumnya, misalnya menembus sistem, mendapatkan hak akses ke dalam sistem, mengekspolitasi data yang sensitif dan menanamkan kode yang berbahaya.
   iii. Post-attack phase : menghasilkan analisis dari semua serangan berdasarkan celah keamanan yang telah di uji pada tahap kedua sehingga akan ditemukan tingkat kerentanan website berdasarkan serangan yang telah dilakukan. Hasil akhir analisis berupa model penanganan celah keamanan yang akan direkomendasikan kepemilik website
4. Tahap penyelesaian

Pada tahap ini yang merupakan tahapan akhir dari proses penelitian. Dilakukan proses pengolahan dan analisis dari data yang telah diperoleh, dimulai dengan melakukan penyaringan situs (Dorking), Exloit, analisa celah keamanan, Backdoor Shell, analisa data dan merumuskan kesimpulan dari hasil yang didapat.

Rancangan penelitain yang direncanakan digambarkan dalam bentuk diagram alir seperti gambar 1.



Gambar 1. Diagram Alir Penelitian

3. HASIL DAN PEMBAHASAN

3.1 Hasil Penelitian

Dari tahapan penelitian yang penulis lakukan mengumpulkan sebanyak 33 website yang berdomain go.id dan 5 website milik BUMN yang berdomain co.id, total sebanyak 38 website yang akan di uji. Sebelum melakukan dorking peneliti menelusuri website target untuk mengetahui jenis bahasa pemrograman yang digunakan. Setelah diketahui bahasa pemrogramannya, selanjutnya website target kita coba secara acak atau mengunakan dork antara lain :

1. inurl:index.php?option=com_fabrik&view= site:co.id atau go.id
2. inurl:index.php/component/fabrik/ site:go.id atau co.id

Dari hasil uji tersebut dapat dilihat pada tabel 1.

Tabel 1. hasil Pre-attack phase

No	Nama Website	Dork	Source
1	https://www.kominfo.go.id/	safety	php+CodeIgniter
2	http://www.bulog.co.id	safety	php
3	http://www.peruri.co.id	safety	php+laravel
4	http://nad.litbang.pertanian.go.id	open	php
5	http://www.sumutprov.go.id	safety	joomla
6	http://www.bawaslu-sumutprov.go.id	safety	php
7	https://sumut.bps.go.id/	safety	yii framework
8	https://www.langkatkab.go.id	safety	php+Codeigniter
9	http://sdm.data.kemdikbud.go.id	safety	ASP
10	http://www.labuhanbatuselatankab.go.id	safety	php
11	https://bappeda.labuhanbatuselatankab.go.id	safety	php
12	http://kpu-labuhanbatuselatankab.go.id	safety	php
13	https://sumutprov.kpu.go.id	open	php
14	http://www.bumn.go.id	safety	php
15	https://labura.go.id	safety	WordPress
16	https://diskominfo.labura.go.id	safety	WordPress
17	http://bkd.labura.go.id	safety	WordPress
18	https://www.binjaikota.go.id	safety	php+Codeigniter
19	https://binjaikota.bps.go.id	safety	yii framework
20	http://pa-binjai.go.id	safety	joomla
21	http://www.pn-binjai.go.id	safety	joomla
22	https://bbkpbelawan.karantina.pertanian.go.id	safety	WordPress
23	http://www.pemkomedan.go.id	safety	php
24	http://hubla.dephub.go.id	safety	ASP
25	http://www.pajak.go.id	safety	drupal
26	http://www.beacukai.go.id	safety	j2ee
27	http://maritim.bmkg.go.id	safety	php
28	http://belawan.imigrasi.go.id	safety	WordPress
29	http://dpmpptsp.sumutprov.go.id	safety	php
30	http://kpud-medankota.go.id	safety	WordPress
31	http://pn-bandaaceh.go.id	safety	WordPress
32	http://kejari-padang.go.id/	open	joomla
33	https://pertani.co.id	safety	php+laravel
34	http://www.sucofindo.co.id	safety	php
35	http://www.banksumut.com	safety	php
36	http://belawan.pelindo1.co.id	safety	Chameleon
37	http://bict.pelindo1.co.id	safety	php
38	http://www.pt-makassar.go.id	open	Joomla

Dari hasil percobaan yang dilaukan terdapat beberapa celah (*vulnerability*) yang dimiliki oleh website target dapat dilihat pada tabel 2. Dari hasil tersebut website target dicoba dengan memasukin exploit. Exploit yang dicoba dalam penelitian ini adalah sebagai berikut :

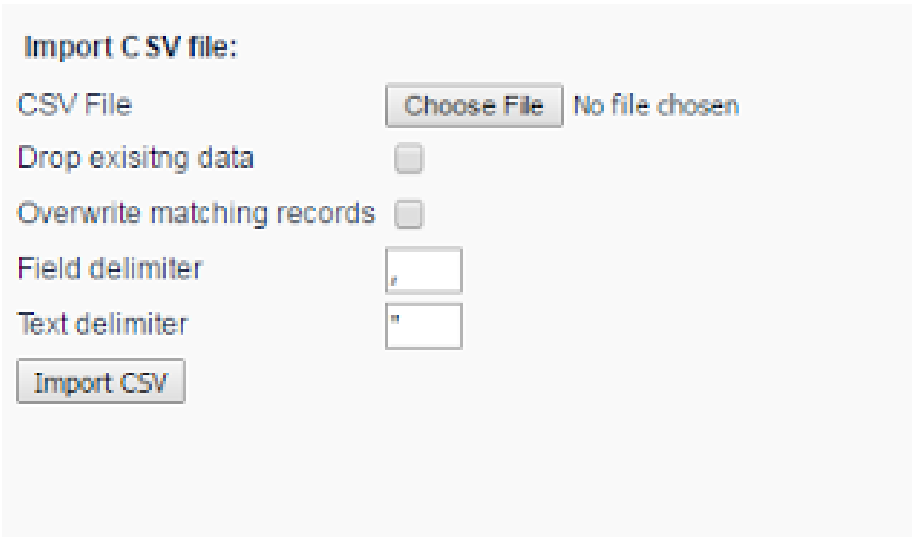
1. index.php?action=com_user&view=registration
2. index.php?option=com_fabrik&c=import&view=import&filetype=csv&table=1

Tabel 2. Hasil Exploit

No	Nama Website	Kegiatan		
		Dork	Exploit	Backdoor Shell
1	https://www.kominfo.go.id/	safety	safety	safety
2	http://www.bulog.co.id	safety	safety	safety
3	http://www.peruri.co.id	safety	safety	safety
4	http://nad.litbang.pertanian.go.id	open	open	open
5	http://www.sumutprov.go.id	safety	safety	safety
6	http://www.bawaslu-sumutprov.go.id	safety	safety	safety
7	https://sumut.bps.go.id/	safety	safety	safety
8	https://www.langkatkab.go.id	safety	safety	safety
9	http://sdm.data.kemdikbud.go.id	safety	safety	safety
10	http://www.labuhanbatuselatankab.go.id	safety	safety	safety
11	https://bappeda.labuhanbatuselatankab.go.id	safety	safety	safety
12	http://kpu-labuhanbatuselatankab.go.id	safety	safety	safety
13	https://sumutprov.kpu.go.id	open	open	open
14	http://www.bumn.go.id	safety	safety	safety
15	https://labura.go.id	safety	safety	safety
16	https://diskominfo.labura.go.id	safety	safety	safety
17	http://bkd.labura.go.id	safety	safety	safety
18	https://www.binjaikota.go.id	safety	safety	safety
19	https://binjaikota.bps.go.id	safety	safety	safety
20	http://pa-binjai.go.id	safety	safety	safety
21	http://www.pn-binjai.go.id	safety	safety	safety
22	https://bbkpbelawan.karantina.pertanian.go.id	safety	safety	safety
23	http://www.pemkomedan.go.id	safety	safety	safety
24	http://hubla.dephub.go.id	safety	safety	safety
25	http://www.pajak.go.id	safety	safety	safety
26	http://www.beacukai.go.id	safety	safety	safety
27	http://maritim.bmkg.go.id	safety	safety	safety
28	http://belawan.imigrasi.go.id	safety	safety	safety
29	http://dpmpptsp.sumutprov.go.id	safety	safety	safety
30	http://kpud-medankota.go.id	safety	safety	safety
31	http://pn-bandaaceh.go.id	safety	safety	safety
32	http://kejari-padang.go.id/	open	open	open
33	https://pertani.co.id	safety	safety	safety

34	http://www.sucofindo.co.id	safety	safety	safety
35	http://www.banksumut.com	safety	safety	safety
36	http://belawan.pelindo1.co.id	safety	safety	safety
37	http://bict.pelindo1.co.id	safety	safety	safety
38	http://www.pt-makassar.go.id	open	open	open

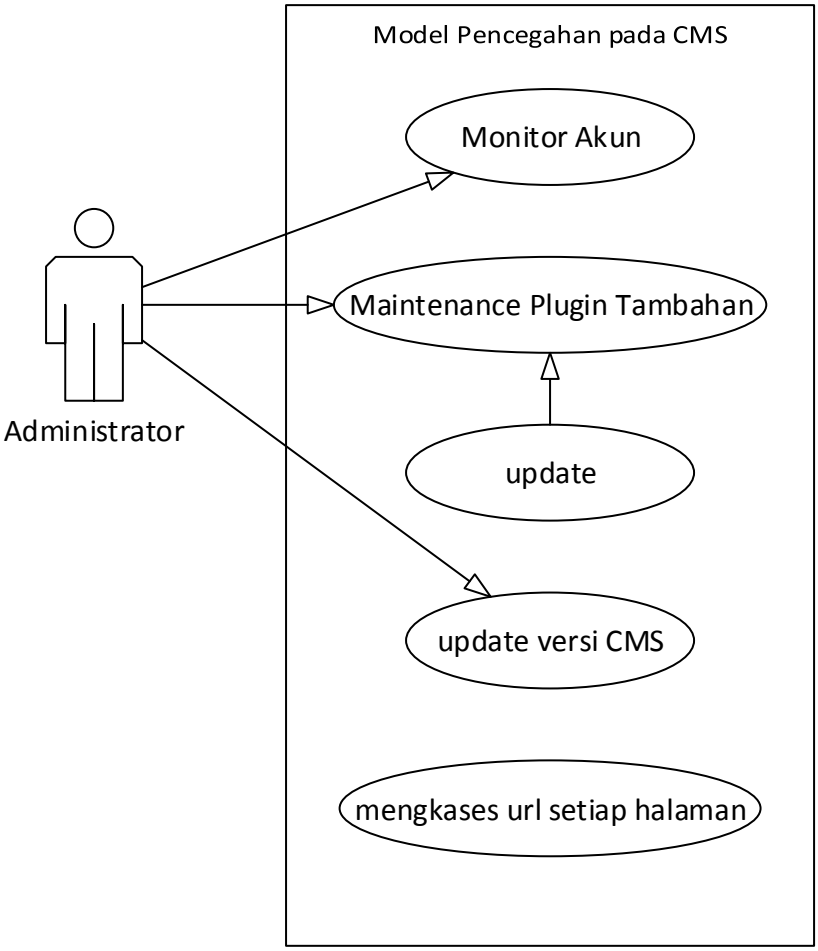
Pengujian dilakukan dengan cara *www.nama-target.com/contoh-exploit*, jika berhasil website berubah menjadi halaman seperti gambar 2.



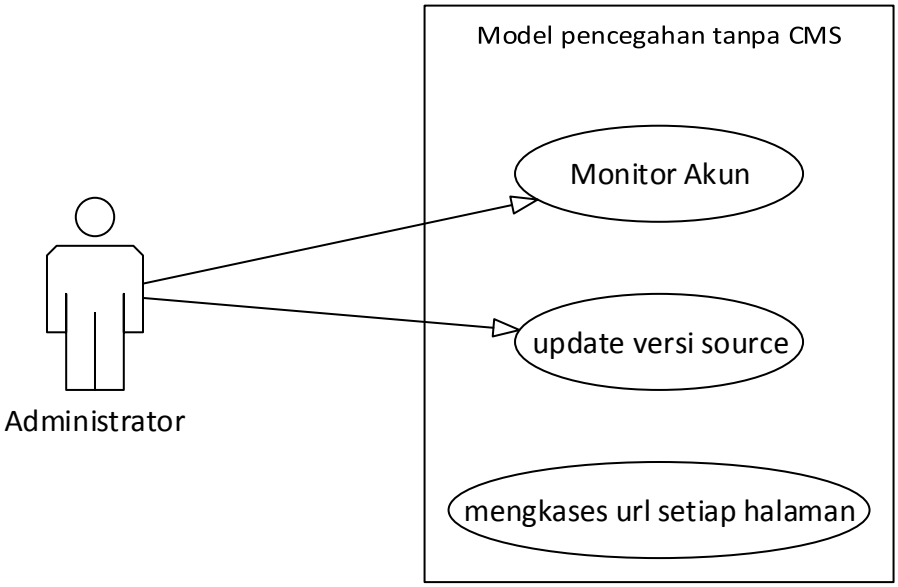
Gambar 2. Tampilan unggah Exploid pada website yang menjadi target

3.2. Pembahasan

Dari hasil penelitian yang dilakukan untuk melakukan proses deface dengan cara dorking selanjutnya adalah memanfaatkan kelemahan vuln dari website target. Dari berberapa sistem yang dibuat seperti *PHP, ASP, Joomla, Wordpress* dan *Drupal*. Website yang dibangun dari joomla yang rentang dengan celah keamanan, selanjutnya PHP. Sedangkan PHP yang dibangun dengan freamwork lebih baik keamanannya. Seperti PHP dengan Laravel atau CodeIgniter. Adapun model pengamanan dalam mengatasi serangan deface dengan exploid dapat dilihat pada gambar 3.



Gambar 3. Model Pencegahan serangan pada CMS



Gambar 4. Model Pencegahan serangan tanpa CMS

4. KESIMPULAN

Dari hasil pengujian yang didapat beberapa kelemahan yang diperoleh antara lain :

1. Celah vulnerabality yaitu www.pt-makassar.go.id, http://kejari-padang.go.id/, sumutprov.kpu.go.id, nad.litbang.pertanian.go.id. website tersebut dibuat dengan cms (*content management system*) serta murni PHP.
2. Dari banyaknya CMS yang digunakan oleh pemerintah maka joomla sangat rentang untuk di bobol

5. SARAN

Dari hasil penelitian yang dilakukan terdapat kekurangan yang perlu untuk dikembangkan antara lain :

1. Membuat suatu aplikasi khusus untuk dapat memberikan penanganan dini terhadap serangan
2. Khususnya bagi pemerintah membuat suatu sistem terpusat sebagai pengelolaan data yang periodik serta khusus memeriksa kemananan website

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Kementerian Riset, Teknologi dan Pendidikan Tinggi Republik Indonesia. yang telah memberi dukungan financial terhadap penelitian ini yang dilaksanakan pada tahun 2018.

DAFTAR PUSTAKA

[1] S. Riyanarto and I. Irsyat, "The U.S Department of justice," itspress, www.usdoj.gov/criminal/Cybercrimes, 2009.

[2] M. S. Hasibuan, "KEYLOGGER PADA ASPEK KEAMANAN KOMPUTER," *Jurnal Teknovasi: Jurnal Teknik dan Inovasi, 3(1), 8-15,* vol. III, no. 3, pp. 8-15, 2018.

[3] J. R. Sun, M. L. Shih and M. S. Hwang, "A Survey of Digital Evidences Forensic and Cybercrime Investigation Procedure," *I. J. Network Security,* vol. 17, no. 5, p. 497–509, 2015.

[4] T. A. Hemphill and P. Longstreet, "Financial data breaches in the U.S. retail economy: Restoring confidence in information technology security standards," *Technology in Society*, vol. 44, no.44 https://doi.org/10.1016/j.techsoc.2015.11.007, p. 30–38, 2016.

[5] J. B. Ullrich and J. Lam, "Defacing websites via SQL injection," *Network Security*, vol. 2008, no.1. http://doi.org/10.1016/S1353-4858(08)70007-2, pp. 9-10, 2008.

[6] C. C. Urcuqui, M. G. Peña, J. L. Osorio Quintero, and A. Navarro Cadavid, "Antidefacement," *Sist. y Telemática*, vol. 14, no. 39, pp. 9–27, 2016.