SISTEM MONITORING WEBSITE DENGAN METODE ISSAF DI DINAS KOMUNIKASI dan INFORMATIKA KABUPATEN TANGERANG

Jajang Ruhiyat[1], Angga Setiyadi[2]

[1,2] Universitas Komputer Indonesia
Jl. Dipatiukur No. 112-116, Bandung 40132
E-mail : jajangruhiyatif@gmail.com[1], angga.setyadi@email.unikom.ac.id[2]

ABSTRAK

Dinas Komunikasi dan Informatika Kabupaten Tangerang merupakan organisasi pemerintahan yang mengelola informasi, data keuangan, dan pengelolaan data untuk setiap bidang yang terlibat didalamnya. Dalam melakukan pengelolaan informasi tersebut, terdapat kekhawatiran yang memungkinkan informasi tersebut bisa jatuh ketangan pihak ketiga. Maka dari itu keamanan web aplikasi merupakan sesuatu yang harus diperhatikan. mengingat banyaknya organisasi pemerintahan yang menggunakan sistem untuk mempermudah dalam mengelola data yang mereka miliki.
Berdasarkan dari banyaknya kegiatan ilegal seperti hacking terhadap sistem yang dikelola organisasi pemerintahan tersebut, adanya kekhawatiran terhadap keamanan sistem yang mereka kelola. Hal ini mengakibatkan sistem tersebut harus terus menerus diperhatikan untuk setiap keamaan yang terdapat di dalamnya. Maka dari itu pengujian terhadap keamanan sistem perlu dilakukan guna untuk menghindari kerugian yang mungkin saja terjadi di masa depan. Pengujian terhadap keamanan sistem menggunakan metode ISSAF dengan ruang lingkup web aplikasi.
Hasil dari pengujian keamanan pada sistem ini akan berupa tabel checklist pengujian beserta kerentanan berdasarkan domain – domain yang diuji. Dan penerapan monitoring sistem berdasarkan metode ISSAF.

Kata Kunci : ISSAF , OISSG , penilaian keamanan , pemantauan sistem, penetrasi

1. PENDAHULUAN

Dinas Komunikasi dan Informatika Kabupaten Tangerang (DISKOMINFO Kab.Tangerang) berdiri sejak Februari 2014. Suatu Organisasi pemerintahan yang mengelola jalannya komunikasi dan informasi yang pada umumnya menggunakan platform berbasis website. Dengan adanya website DISKOMINFO, alur komunikasi, pengelolaan data secara online dapat dilakukan dengan mudah. Adapun fungsi utama dari website yang di kelola Dinas Komunikasi dan Informatika Kabupaten Tangerang adalah sebagai pengelolaan data secara online untuk setiap dinas dan sebagai penyedia layanan informasi resmi pemerintahan kepada masyarakat tentang kegiatan yang dilakukan pemerintah daerah, menjadi tolak ukur bagaimana aktif atau tidaknya kegiatan pemerintahan, dan memudahkan rakyat untuk mengenal sosok pemimpin Kabupaten Tangerang menggunakan website ini sebagai media informasi. Akan tetapi dibalik itu semua, adanya suatu kerentanan yang terdapat pada sistem/aplikasi yang di kelola Dinas Komunikasi dan Informatika Kabupaten Tangerang. Hal ini dapat membahayakan data dan informasi yang bersifat terbuka maupun tidak terbuka.

Berdasarkan hasil wawancara pada 2 oktober 2017 bersama Bapak Cecep khaerudin salah seorang petugas di bidang telematika Dinas Komunikasi dan Informatika Kabupaten Tangerang, beliau menegaskan bahwa sebelumnya pada tahun 2016 telah terjadi beberapa serangan yang mengakibatkan kinerja website tersebut menurun. Dan membutuhkan waktu sekitar satu bulan untuk website agar bisa pulih kembali, dalam proses maintenance yang dilakukan pada akhir mei sampai dengan pertengahan juni 2016 beliau menegaskan kembali bahwa terdapat beberapa celah keamanan berupa sql-injection,xss,ddos hal itu diketahui setelah ditemukannya artifak sisa - sisa penyerangan yang terdapat didalam sistem database dan trafik tinggi yang terdapat pada situs portal dari Dinas Komunikasi dan Informatika Kabupaten Tangerang. Akibat dari serangan ini beberapa akun admin dan user kehilangan hak istimewa (privileges) dan situs portal harus ditutup untuk sementara waktu. Berdasarkan kejadian ini pihak Dinas Komunikasi dan Informatika Kabupaten Tangerang memutuskan untuk menambah suatu keamanan berupa validasi terhadap website yang terkena serangan pada tahun 2016 dan beberapa website lainnya, hal ini dilakukan guna untuk menghindari kelanjutan dari serangan yang sudah terjadi sebelumnya. Akan tetapi meskipun

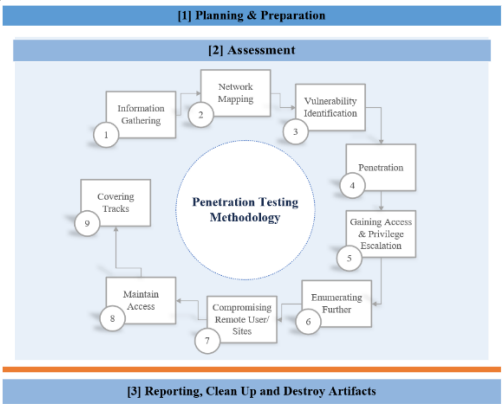
dengan adanya suatu keamanan yang sudah diterapkan pada sistem di Dinas Komunikasi dan Informatika Kabupaten Tangerang ini tidak menutup kemungkinan bahwa masih terdapat celah – celah keamanan pada sistem yang mereka kelola, hal seperti ini masih memungkinkan bagi seorang attacker memanfaatkan celah tersebut untuk medapatkan akses ilegal agar bisa masuk kedalam sistem DISKOMINFO Kabupaten Tangerang.

Berdasarkan hasil penelitian dapat dijabarkan bahwa, perlu dilakukan selftest pada website Dinas Komunikasi dan Informatika Kabupaten Tangerang yang akan mengeluarkan hasil cheklist berupa celah – celah keamanan yang masih terdapat pada sistem tersebut. Dan juga penerapan monitoring sistem berdasarkan metode Information Systems Security Assessment Framework (ISSAF). ISSAF dikeluarkan oleh Open System Security Information Group (OSSIG) adalah suatu framework terstruktur yang mengkategorikan penilaian keamanan sistem informasi berdasarkan hasil penelusuran pada domain dan rincian kriteria evaluasi atau pengujian khusus untuk masing-masing domain.

Berdasarkan masalah yang dialami Dinas Komunikas dan Informatika Kabupaten Tangerang adalah diperlukannya suatu bentuk laporan dari hasil pengujian, yaitu berupa ceklist celah – celah keamanan yang akan digunakan untuk dokumentasi guna untuk pemantauan dan meningkatkan keamanan pada website DISKOMINFO Kabupaten Tangerang.

1.1 Tahap Penelitian

Metode penetrasi *Information System Security Assessment Framework* (ISSAF) dirangkai untuk mengevaluasi suatu jaringan, sistem yang akan di uji. Terdapat tiga fase pada metode ini dan terdapat sembilan langkah pada fase *assessment.* Berikut ini adalah tahap uji penetrasi berdasarkan metode ISSAF yang dapat dilihat pada gambar 1.1 [1].



Gambar 1. *Penetration Testing Methodology*

2. ISI PENELITIAN

Pada tahap ini akan membahas mengenai masalah yang akan dianalisis, gambaran umum sistem, tahapan setiap proses dan hasil dari penelitian.

2.1 Jenis Kerentanan

Beberapa serangan berdampak pada suatu web aplikasi yang dapat merugikan pemilik dari website tersebut. Jenis serangan itu meliputi :

a. *SQL Injection*

SQL Injection adalah teknik untuk mengeksploitasi sebuah halaman web yang memakai basis data (database) seperti MySQL dengan memberikan kode kedalam *query* SQL. Terdapat 3 jenis metode serangan menggunakan *SQL Injection* diantaranya :

- *Error Based SQL Injection*

Error Based SQL Injection dalam melakukan exploitasi kedalam halaman web yang menggunakan database hanya menampilkan pesan error jika exploitasi berhasil dilakukan, pesan error tersebut memberikan beragam informasi seperti versi database yang digunakan, yang dapat dimanfaatkan oleh attacker.

- *Union Based SQL Injection*

Union Based SQL Injection adalah metode *SQL Injection* dengan memanfaatkan perintah *query UNION* dan menggabungkannya dengen beberapa perintah query lain seperti *SELECT* untuk menghasilkan informasi yang diinginkan oleh *attacker*.

- *Blind SQL Injection*

Blind SQL Injection, metode serangan menggunakan jenis ini tidak akan menampilkan pesan error pada halaman web atau tidak juga menampilkan data atau informasi yang diinginkan, karena serangan dengan menggunakan metode *Blind SQL Injection* hanya menghasilkan kondisi *True* atau *False* dari *query SQL* yang dimasukan pada sebuah halaman web yang menjadi target.

Berdasarkan jenis kerentanan SQL Injection masing – masing memiliki dampak yang berbeda – beda, namun pada akhirnya selalu memiliki hasil yang sama pada jenis kerentanan *SQL Injection*. Karena dengan adanya kerentanan ini rahasia tentang struktur database ataupun data yang ada didalamnya bisa terancam, karena seorang *attacker* bisa dengan mudah menggunakan celah ini untuk bisa mendapatkan informasi mengenai database.

b. XSS (*Cross Site Scripting*)

XSS adalah salah satu jenis serangan web yang dilakukan dengan memanfaatkan kelemahan dan kesalahan yang terletak pada penulisan *scripting* pada suatu aplikasi web sehingga memungkinkan seseorang untuk menginjeksikan

suatu tag HTML ataupun *Client Side Scrip*t pada aplikasi web tersebut dikarenakan adanya *variabel* yang tidak disanitasi dengan baik. Dari serangan XSS ini seorang *attacker* akan mencoba mendapatkan suatu hak akses berupa *session cookies* dengan adanya interaksi langsung dengan pihak korban (*victim*) dengan berbagai macam pendekatan seperti *social engineering*. Karena tanpa adanya interaksi dengan korban, mustahil bagi seorang attacker untuk bisa mendapatkan suatu hak akses yang akan digunakan untuk menyusup kedalam sistem.

c. DOS (*Denial of service*)

DOS (*Denial of service*) adalah metode untuk mencegah pengguna untuk mendapatkan layanan yang diberikan oleh server, dengan harapan metode ini dapat mematikan dan menyibukan server dengan membanjiri layanan pada server.

2.2 *Proof of Concept Exploit*

Proof of Concept Exploit atau sering disebut dengan (PoC) adalah sebuah jenis serangan terhadap sistem komputer atau jaringan. Hal ini dilakukan hanya untuk membuktikan bahwa semua itu bisa dilakukan, dan ini umumnya tidak menimbulkan kerugian, namun menunjukkan bagaimana seorang hacker dapat memanfaatkan kerentanan dalam perangkat lunak atau mungkin perangkat kerasnya[2].

2.3 *Common Weakness Enumeration* (CWE)

Common weakness enumeration ditargetkan untuk pengembang dan praktisi keamanan, merupakan daftar resmi jenis kelemahan perangkat lunak yang digunakan untuk :

1 Berfungsi sebagai bahasa yang umum untuk menggambarkan kelemahan keamanan perangkat lunak dalam hal arsitektur, Desain, atau kode.

2 Berfungsi sebagai standar yang menjadi tolak ukur alat-alat keamanan perangkat lunak penargetan kelemahan-kelemahan pada sistem.

3 Menyediakan satu standar dasar untuk identifikasi kelemahan, mitigasi dan pencegahan [3].

2.4 Nikto

Nikto merupakan suatu alat gratis (*opensource*) yang di gunakan untuk pemindaian suatu web aplikasi dengan menggunakan CLI(*command line interfaces*) karna nikto dikembangkan menggunakan bahasa pemrograman perl. meskipun tidak adanya user interface pada nikto tetapi didalamnya terdapat 6700 potensi kerentanan file/program untuk pengujian. Dengan fitur *auto scanning* yang dilakukan nikto untuk mencari kerentanan secara automatis [4].

2.5 *Web Application Security Assessment*

Keamanan suatu web aplikasi merupakan keamanan semua kompone – komponen yang digunakan oleh web aplikasi, web server yang menjalankan web aplikasi dan modul – modul pada web server. Semua trafik yang di arahkan ke web server yaitu dengan melalui protokol http/https, yang mana trafik tersebut ada yang bisa dipercaya dan ada pula yang tidak di blok oleh firewall. Web server sering menjadi sasaran untuk dijadikan target penyerangan[5].

a. *Purpose*
   Untuk membuat web aplikasi dan web server seaman mungkin dari serangan dan menutup beberapa informasi yang tidak di perlukan, yang akan mempersulit attacker untuk bisa mendapatkan informasi.
b. *Objective*
   Untuk mendapatkan akses terhadap remote-machine dengan melewati firewall dan menguasai jaringa. Mengumpulkan informasi apa saja dari jaringan dan server.
c. *Expected Result*
   Pada umumnya setiap perusahaan ataupun organisasi menempatkan firewall untuk keamanan biasanya pada port 80 untuk webserver.
d. *Pre-requisite*
   Basik pengetahuan dari HTTP Protocol.

- *Identifying web server vendor and version*

Langkah pertama ketika melakukan penilaian web aplikasi adalah mengidentifikasikan web server pada aplikasi apa yang berjalan. Untuk mendeteksi webser, hal – hal yang perlu dilakukan yaitu :

1. Banner grabbing
2. Menggunakan alat otomatis untuk mendeteksi web server
3. Default file detection
4. Mengecek ekstensi file pada server

2.6 Kali Linux

Kali Linux adalah distribusi berlandasan distribusi Debian GNU/Linux untuk tujuan forensik digital dan digunakan untuk pengujian penetrasi, yang dipelihara dan didanai oleh Offensive Security. Kali linux dikembangkan oleh pengembang Backtrack sebelumnya yaitu Mati Aharoni bersama pengembang baru bernama Devon Kearns dari Offensive Security[6]. Secara umum kali linux memiliki berbagai macam tools yang dapat dibagi ke dalam beberapa kasifikasi berdasarkan fungsi utamanya yaitu :

1. Information Gathering digunakan untuk mengumpulkan informasi dari suatu sistem

2. Reverse Enginerring digunakan untuk menganalisa suatu sistem melalui identifikasi komponen-komponennya dan keterkaitan antar komponen tersebut lalu membuat abstraksi dan informasi perancangan dari sistem yang dianalisa
3. Exploitation Tools digunakan untuk mengekspoitasi celah yang terdapat pada suatu sistem.
4. Vulnerability Assessement digunakan untuk melakukan pencarian, identifikasi, perhitungan terhadap celah keamanan suatu sistem
5. Privilege Escalation digunakan untuk melakukan serangan yang bertujuan untuk menaikkan tingkat akses didalam suatu sistem

2.4 Analisis Masalah

Berdasarkan hasil penelitian yang telah dilakukan di jelaskan bahwa sebelumnya website Dinas Komunikasi dan Informatika Kabupaten Tangerang telah terkena serangan dan menyebabkan dampak serius yang diakibatan serangan tersebut. Oleh karena itu perlu dilakukan analisis terhadap website yang terhubung dengan domain utama Diskominfo. Analisis yang dilakukan mengacu pada metode Information System Security Assessment Framework (ISSAF), adapun analisis yang dilakukan akan dibagi menjadi tiga tahap sesuai dengan metode ISSAF.

1) *Planning and Preparation*

Pada tahap ini peneliti akan melakukan pertemuan secara langsung dengan salah seorang petugas di Dinas Komunikasi dan Informatika Kabupaten Tangerang untuk meminta persetujuan melakukan penelitian dalam bentuk penetration testing research terhadap sistem yang dibagun/dikembangkan oleh pihak DISKOMINFO Kabupaten Tangerang, pada pertemuan tersebut peneliti beserta pihak DISKOMINFO melakukan persetujuan atas dasar perindungan hukum bersama. Adapun hal – hal yang menjadi topik pembicaraan pada saat melakukan pertemuan antara peneliti dengan pihak Dinas Komunikasi dan Informatika Kabupaten Tangerang adalah:

- Identifikasi kontak untuk kedua belah pihak.
- Konfirmasi ruang lingkup, pendekatan dan penjelasan metode.
- Menyetujui pengujian kasus spesifik.
- Hasil akhir dari penelitian ini akan diserahkan guna untuk proses perbaikan sistem.
- Melakukan permintaan dalam bentuk data berupa domain utama yang digunakan.
- Penjabarkan tentang kerentanan dan keamanan yang terdapat pada sistem sebelum/sesudah dilakukan maintenance.

2) *Assessment*

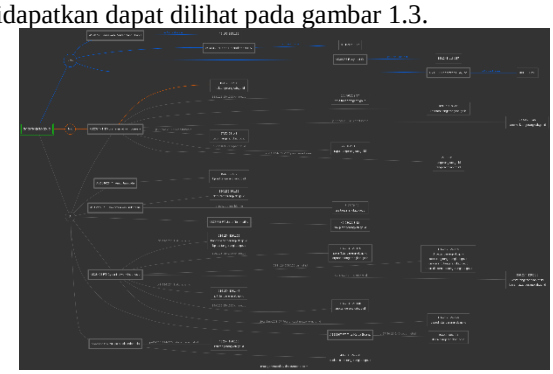
a. *Information gathering*

Peneliti mengumpulkan informasi mengenai domain yang menjadi target dalam penelitian. Informasi yang akan dikumpulkan pada tahap ini adalah *whois domain* dan *subdomain*. Berikut ini adalah informasi berdasarkan *whois domain info* yang dapat dilihat pada gambar 1.2.

tangerangkab.go.id	
WHOIS DOMAIN	Domain ID:PANDI-DO286393
	Domain Name:TANGERANGKAB.GO.ID
	Created On:19-Aug-2007 13:35:21 UTC
	Last Updated On:23-Jul-2017 03:57:05 UTC
	Expiration Date:29-Aug-2019 23:59:59 UTC
	Status:ok
	Registrant ID:abualw-4263
	Registrant Name:Abu Alwakiel
	Registrant Organization:DISKOMINFO Kabupaten Tangerang
	Registrant Street1:Jl. Somawinata No.1
	Registrant City:Kabupaten Tangerang
	Registrant State/Province:Banten
	Registrant Postal Code:15710
	Registrant Country:ID
	Registrant Phone:+62.81285920614
	Registrant Email:isa.lpse@gmail.com
	Sponsoring Registrar ID:H4964483
	Sponsoring Registrar Organization:Kementerian Komunikasi dan Informatika
	Sponsoring Registrar Street1:Jl. Medan Merdeka Barat No. 9
	Sponsoring Registrar City:Jakarta Pusat
	Sponsoring Registrar State/Province:Jakarta
	Sponsoring Registrar Postal Code:10110
	Sponsoring Registrar Country:ID
	Sponsoring Registrar Phone:622138433507
	Sponsoring Registrar Website:domain.go.id
	Name Server:NS1.DESIBLE.NET
	Name Server:NS2.DESIBLE.NET
	Name Server:DNS1.DESIBLE.NET
	Name Server:DNS2.DESIBLE.NET
	DNSSEC:Unsigned

Gambar 2. *Whois domain info*

Kemudian informasi subdomain yang didapatkan dapat dilihat pada gambar 1.3.



Gambar 3. *Subdomain*

b. *Network mapping*

Hasil uji coba *network mapping* dilakukan terhadap salah satu domain yang dikelola pihak DISKOMINFO Kab.Tangerang, hasil tersebut dapat dilihat pada tabel 1.

Tabel 1. *Network mapping*

sakip.tangerangkab.go.id		
PORT	**STATUS**	**SERVICE**
21	Open	ftp
80	Open	http
1922	Open	ssh

3306	Open	MySQL
5432	Open	Postgresql
25	Filtered	smtp

c. *Vulnerability identification*

Pada tahap ini penguji mencoba mengidentifikasi kerentanna yang terdapat pada salah satu domain yang diuji. Adapun hasil pengujian dapat dilihat pada tabel 2.

Tabel 2.*vulnerability identification*

Sakip.tangerangkab.go.id:80		
Vulnerability Type	**Parameter**	**Method**
BlindSQL Injection	filter	POST
SQL Injection	filter	POST
	/	GET
CrossSiteScripting (XSS)	filter	POST
	Gallery()	GET
	Peraturan()	GET
ApplicationError message	Host	GET
	filter	POST
Host header attack	Host	GET

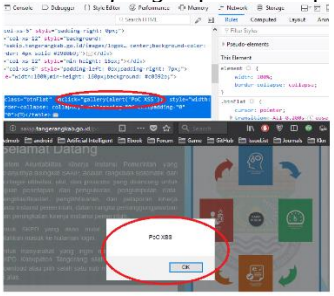
d. *Penetration*

Pada tahap ini peneliti akan melakukan uji keamanan sistem berdasarkan data yang di dapatkan dari hasil analisis. pengujian ditahap ini dibagi menjadi dua yaitu pengujian kerentanan *SQL injection* dengan menggunakan parameter filter, *payload* "'SQLinjection" sebagai inputan ditahap pengujian *SQLinjection*. Dan *cross site scripting* (XSS) dengan parameter yang terdapat didalam *event* onclick yaitu gallery(), *payload* "alert('PoC XSS')". Untuk pengujian kerentanan *SQL injection* dapat dilihat pada gambar 4.



Gambar 4. *Sql injection*

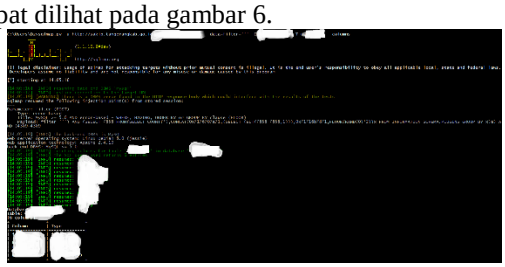
Kemudian pengujian terhadap kerentanan *cross site scripting* dapat dilihat pada gambar 5.



Gambar 5. *Cross site scripting*

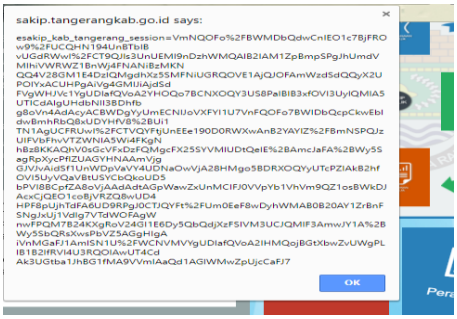
e. *Gaining access & privilege escalation*

Pada tahap ini merupakan proses yang memungkinkan penguji untuk mendapatkan suatu akun tidak sah. Adapun proses untuk mendapatkan akun tersebut akan terbagi menjadi dua bagian yaitu dengan *proof of concept* (PoC) *SQL injection* dan *cross site scripting* (XSS). Untuk pengujian terhadap PoC *SQL injection* dapat dilihat pada gambar 6.



Gambar 6. PoC *SQL injection*

Dan pengujian PoC XSS dapat dilihat pada gambar 7.



Gambar 7. PoC XSS

f. *Enumerating further*

Pada tahap ini penguji akan menyimpan data berupa *session cookie*, hasil *dump* user & pass. Data hasil *dump* dapat dilihat pada gambar 8.



Gambar 8. *Dump process*

g. *Compromise remote user/sites*

Exploitasi hubungan koneksi antara *remote user* dan *enterprise user* (peneliti). Berdasarkan data yang sudah didapatkan memungkinkan bagi peneliti untuk masuk kedalam sistem yang diuji. Tampilan penyusupan kedalam sistem dapat dilihat pada gambar 9.



Gambar 9. *Login access*

h. *Maintain access*

Dengan menggunakan sesuatu seperti *backdoor*, untuk tetap dapat masuk ke dalam sistem yang sudah di exploitasi.

i. *Covering tracks*

menghapus semua jejak dengan cara menyembunyikan file, hapus log, menghindari pengecekan integritas dan antivirus.

3) *Reporting, clean-up and destroy artefacts*

a *Reporting*

Setelah menyelesaikan semua pengujian yang berada pada ruang lingkup, menuliskan laporan yang mendeskipsikan hasil lengkap pengujian dan presentasi yang sudah di persiapkan dengan rekomendasi dan penyelesaiannya. Adapun hal – hal yang menjadi topik laporan meliputi :

- *Management Summary*

  Berdasarkan penelitian yang telah dilakukan dari tahap awal hingga tahap akhir, terdapat dua kerentanan yang sangat fatal berletak pada empat website dari tujuh website yang telah di uji. Kerentanan tersebut adalah SQLInjection dan Cross Site Scripting. jumlah in scope domain yang telah disetujui pada saat proses wawancara terdapat 35 domain yang dikelola pihak Dinas Komunikasi dan Informatika Kabupaten Tangerang.

  Berdasarkan hasil uji penetrasi yang telah dilakukan mulai dari tahap analisis sampai dengan implementasi, maka kesimpulan dari penelitian ini adalah sebagai berikut.

  a Memberikan laporan dalam bentuk kerentanan – kerentanan berdasarkan domain yang dikelola pihak Dinas Komunikasi dan Informatika Kabupaten Tangerang.

  b Laporan ini bisa menjadi acuan terhadap kerentanan sistem yang terjadi di Dinas Komunikasi dan Informatika Kabupaten Tangerang.

  Berdasarkan pengujian yang sudah diteliti terdapat kerentanan berupa cross site scripting dengan id kerentanan CWE-79 dan SQLi dengan id kerentanan CWE-89, dan ini sangat mengkhawatirkan bagi data yang terdapat didalamnya. Id kerentanan tersebut diambil dari situs cwe.mitre.org yang merupakan salah satu situs penyedia common weakness enumeration, situs tersebut berfungsi sebagai acuan terhadap kerentanan yang diteliti.

  Berdasarkan hasil penelitian, saran yang diberikan peneliti untuk menghindari kerentanan XSS yang memiliki id CWE-79 yaitu dengan memperhatikan semua potensi area dari masukan (input) yang berada pada sistem seperti : parameter, variable, cookies, request header, komponen URL, file, filename dan segala macam data external yang berhubungan dengan sistem.

  Berdasrkan hasil penelitian, saran yang diberikan peneliti untuk menghindari kerentanan SQLi yang memiliki id CWE-89 yaitu dengan melakukan whitelist terhadap masukan (input) yang diberikan, dan blacklist segala macam masukan (input) yang memungkinkan dapat merubah standar dari masukan yang telah diberikan.

- *Scope Of The Project*

  Scope of the project merupakan laporan mengenai ruang lingkup yang diambil peneliti. Ruang lingkup ini sendiri sebenarnya sudah diambil peneliti berdasarkan persetujuan dari peneliti dan pihak yang di uji. Adapun ruang lingkup yang diambil peneliti adalah web aplikasi. Dan scope domain berdasarkan data yang sudah diberikan oleh pihak Dinas Komunikasi dan Informatika Kabupaten Tangerang.

- *Vulnerability Scan Reports*

  Vulnerability scan reports merupakan tahap laporan berdasarkan proses analisis pada fase ke dua metode ISSAF ditambah dengan implementasi yang telah dilakukan. Karena pengujian kerentanan berdasarkan hasil pemindaian sangat penting untuk dilaporkan ke pihak DISKOMINFO. Berikut ini adalah laporan berupa table yang berisi domain dan disertai dengan nilai kerentanan yang terdapat/tidaknya pada suatu domain yang diuji dalam penelitian ini, nilai kerentanan tersebut diambil dari situ cwe.mitre.org. situs tersebut merupakan salah satu rekomendasi penilaian kerentanan yang terdapat pada modul ISSAF. Adapun tabel laporan kerentanan dapat dilihat pada tabel 4.

Tabel 4. *Vulnerability scann report*

CommonWeaknessEnumeration	**CWE 79**	**CWE 89**
Domain	xss	sqli
lpse.tangerangkab.go.id:443	✓	✓
mail.dinkes.tangerangkab.go.id:80	x	✓

sakip.tangerangkab.go.id:80	✓	x
Sikda.dinkes.tangerangkab.go.id:80	x	x
Sitt.dinkes.tangerangkab.go.id:80	✓	✓
Bpkad.tangerangkab.go.id:80	x	x
koperasi.tangerangkab.go.id	x	x
Sipinter.tangerangkab.go.id:80	x	✓

- *Exploit Report*

  Exploit report adalah bagian dimana peneliti melaporkan setiap tahapan yang dilakukan berhasil atau tidaknya berdasarkan tools yang diguanakan selama penelitian berlangsung. Berikut ini adalah exploit report berdasarkan domain – domain yang sudah selesai diteliti. Bentuk dari *exploit report* dapat dilihat pada gambar 10.

Domain	sakip.tangeragkab.go.id:80		
Tahapan	Source	Tools	Status
Information gathering	Domain Info	whois	✓
	Subdomain info	dnsdumpster	✓
Network Mapping	Port Mapping	zenmap	✓
Vulnerability Identification	Web Scanner Vulnerability	acunetix	✓
		vega	✓
		nikto	✓
Penetration	Cross Site Scripting	Browser (Chrome,Firefox)	x
	Sql Injection		x
Gaining Access & Privilege Escalation	Cross Site Scripting	Burpsuite	x
	Sql Injection	Sqlmap	x
Enumerating Further	Cross Site Scripting	Burpsuite	x
Compromising Remote User/Sites	Sql Injection	Sqlmap	x
Maintain Access	Backdoor	php rootkit	x
Covering Tracks	Backdoor	php rootkit	x

Gambar 10. *Exploit Report*

b *Clean-up and destroy artefacts*

Semua informasi yang dibuat/ disimpan pada pengujian sistem harus di hapus dari sistemnya, jika itu tidak bisa di lakukan dengan *remote sistem* maka harus di beritahukan ke pihak Diskominfo Kab.Tangerang, agar staff IT bisa langsung menghapus informasi tersebut setelah laporan di terima pihak tersebut.

Berdasarkan penelitian yang telah dilakukan, peneliti akan melaporkan segala macam artifacts yang tertanam selama pengujain pada sistem berlangsung. Adapun bentuk laporan mengenai artefacts akan diperlihatkan pada tabel 5.

Tabel 5. *Artefacts*

Domain	Type	Name
sitt.dinkes.tangerangkab.go.id	user/pass	4****/4****
sakip.tangerankab.go.id	user/pass	4****/4****

2.6 Analisis Perangkat Keras

Spesifikasi perangkat keras yang digunakan dalam pembangunan *monitoring system*:

Tabel 6. Analisis Kebutuhan Perangkat Keras Pembangunan Sistem

Jenis Perangkat Keras	Spesifikasi
Processor	Intel Core i3
RAM	2 GB
Harddisk	160 GB

2.7 Analisis Kebutuhan Perangkat Lunak

Berikut adalah analisis kebutuhan perangkat lunak dari sistem yang akan dibangun. Spesifikasi perangkat lunak bagi pengembang yang digunakan dalam membangun *game* edukasi peribahasa adalah:

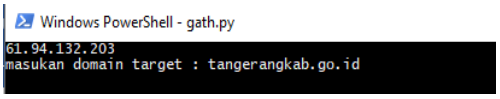
Tabel 7. Analisis Kebutuhan Perangkat Lunak

Perangkat Lunak	Spesifikasi
Sistem Operasi	Windows / linux
Python	Python digunakan sebagai interpreter bahasa pemrograman yang digunakan. Dalam penelitian ini menggunakan python 2.7
perl	Digunakan sebagai interpreter untuk bundle dari opensource nikto.
Hackertarget api	Digunakan untuk api pada *proses information gathering*
Nikto	Digunakan untuk proses identifikasi kerentanan

2.8 Perancangan Struktur Menu

Dalam perancangan struktur menu peneliti menggunakan proses otomatis untuk setiap proses yang terdapat didalamnya. Hanya saja sebelum proses dilakukan dibutuhkan masukan berupa domain yang akan diuji.

1. Tahap input domain dapat dilihat pada gambar 11.



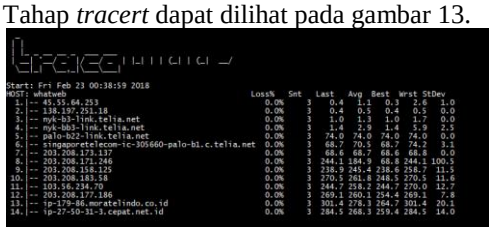
Gambar 11.*input domain*

2. Tahap pemindaian whois domain dapat dililhat pada gambar 12.



Gambar 12.*whois test*

3. Tahap *tracert* dapat dilihat pada gambar 13.



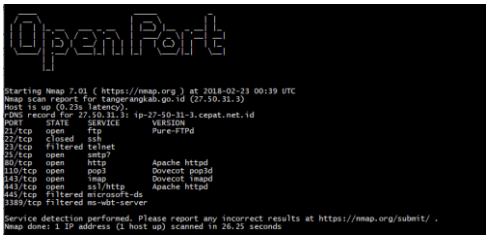
Gambar 13. *tracert*

4. Tahap *DNSLookup* dapat dilihat pada gambar 14.



Gambar 14.*DNS Lookup*

5. Tahap *Open port* dapat dilihat pada gambar 15.



Gambar 15. *Open port*

6. Tahap vulnarability identification dapat dilihat pada gambar 16.



Gambar 16. *Vulnerability identification test*

3. PENUTUP

3.1 Kesimpulan

Berdasarkan hasil analisis dan pengujian dapat disimpulkan bahwa keamanan web aplikasi pada website DISKOMINFO Kabupaten Tangerang rentan terhadap suatu serangan yang berdampak buruk bagi system yang mereka kelola. Hal ini terlihat pada kerentanan SQL injection dan Cross Site Scripting, yang memungkinkan bagi seorang attacker mengambil alih system yang dikelola pihak DISKOMINFO.

3.1 Saran

Berikut ini adalah saran – saran yang diberikan peneliti berdasarkan penelitian pada website DISKOMINFO Kab. Tangerang.

1. Melakukan uji penetrasi terhadap website DISKOMINFO kemudian memberikan laporan - laporan hasil analisis dan implementasi yang telah dilakukan pada fase *assessment* metode ISSAF.
2. Memberikan rekomendasi penanggulangan berdasarkan nilai *common weakness enumeration* (CWE), guna untuk menganggulangi kerentanan yang terdapat pada system DISKOMINFO.

DAFTAR PUSTAKA

[1] OISSG, “Penetration Testing Metodology”, p 136, 04 September 2005, 2005..

[2] ”Definition of: PoC exploit”,[Online]. Available:https://www.pcmag.com/encyclopedia/term/58148/poc-exploit. [Accessed 05 February 2018].

[3]”CommonWeaknessEnumeration”,[Online].Available:https://cwe.mitre.org/about/index.html.[Accessed 15 Februari 2018]

[4]“Nikto”,[Online].Available:https://cirt.net/Nikt2. [Accessed 16 October 2017]

[5]OISSG, ”Web Application Security Assessment”,p 719, 04 September 2005, 2005.

[6]Angga Setyadi, *Implementasi Modul Network MITM Pada Websploit sebagai Monitoring Aktifitas Pengguna dalam Mengakses Internet*, Bandung: Prosiding Seminar Nasional Komputer dan Informatika (SENASKI) , 2017.