DAFTAR ISI

PERS	ETUJUAN DOSEN PEMBIMBING TUGAS AKHIRiv
PERS	ETUJUAN TIM PENGUJI TUGAS AKHIRv
ABST	RACTvi
ABST	'RAK vii
KATA	A PENGANTAR viii
DAFT	AR ISI
DAF I	AK GAMBARXIII VAD TAREI
DAFI	'AR LAMPIRAN xxiii
BAB I	I PENDAHULUAN1
1.1	Latar Belakang1
1.2	Rumusan Masalah7
1.3	Batasan Masalah7
1.4	Tujuan Penelitian9
1.5	Metodologi9
1.6	Sistematika Penulisan10
BAB I	II LANDASAN TEORI13
2.1	Cloud Computing
	2.1.1 Cloud Computing Definition13
	2.1.2 Cloud Computing Characteristics14
	2.1.3 Cloud Computing Service Models17
	2.1.4 Cloud Computing Deployment Models
2.2	Penetration Testing
2.3	Penetration Testing Methodology24
	2.3.1 Planning25
	2.3.2 Discovery
	2.3.3 Attack
	2.3.4 Reporting
2.4	CSA Top Threats to Cloud Computing 202427
	2.4.1 Misconfiguration & Inadequate Change Control
	2.4.2 Identity and Access Management
	2.4.3 Insecure Interfaces and APIs
	2.4.4 Inadequate Cloud Security Strategy
2.5	Google Cloud Platform

	2.5.1 GCP Project	
	2.5.2 Layanan Google Cloud	
	2.5.3 Shared Responsibility di Google Cloud	40
	2.5.4 Berinteraksi dengan Google Cloud	43
2.6	Terraform	45
	2.6.1 File Konfigurasi Terraform	46
	2.6.2 Otomatisasi Penyediaan Cloud dengan Terraform	49
BAB 1	III ANALISIS DAN PERANCANGAN SISTEM	51
3.1	GCPGoat	51
3.2	Arsitektur sistem GCPGoat dan Komponen	53
3.3	Design Web Service pada Exploitasi XSS	60
	3.3.1 Introduksi Web Service "XSS Server"	61
	3.3.2 Garis besar Arsitektur XSS Server	63
	3.3.3 Implementasi XSS Server	65
BAB 1	IV IMPLEMENTASI DAN PENGUJIAN	110
4.1	Garis Besar Implementasi	110
4.2	Planning	123
4.3	Server-Side Request Forgery (SSRF) Attack	
	4.3.1 Discovery	125
	4.3.2 Vulnerability Analysis	
	4.3.3 Attack	134
4.4	Storage Bucket IAM Misconfiguration	144
	4.4.1 Discovery	144
	4.4.2 Vulnerability Analysis	
	4.4.3 Attack	156
4.5	VM Misconfiguration	
	4.5.1 Discovery	
	4.5.2 Vulnerability Analysis	
	4.5.3 Attack	165
4.6	Cross-Site Scripting	174
	4.6.1 Discovery	174
	4.6.2 Vulnerability Analysis	176
	4.6.3 Attack	
4.7	Reporting	190
	4.7.1 Kesimpulan	
	4.7.2 Rekomendasi	
4.8	Kesimpulan Implementasi	

BAB V	PENUTUP	289
5.1	Kesimpulan	289
5.2	Saran	290
DAFTA	AR PUSTAKA	291
LAMP	IRAN A. VIDEO-VIDEO PROSES PENETRATION TESTING	. A-1
INDEX	Χ	a



DAFTAR GAMBAR

		halaman
Gambar 2.1	NIST Four-Stage Penetration Testing Methodology	
Gambar 2.2	Hasil Survei CSA Top Threats to Cloud Computing 2024 Top 11	
Gambar 2.3	Diagram menggambarkan Shared Responsibility masing-masing	
	Cloud Service antara Cloud Provider dengan customer	40
Gambar 2.4	Tampilan dari Google Cloud Console	44
Gambar 2.5	Alur mengotomatisasi penyediaan sumber daya menggunakan	
	Terraform Sumber : (Hashimoto 2024)	50
Gambar 3.1	Attack Path yang dapat diikuti dalam melakukan Penetration	
	Testing sistem GCPGoat Sumber: (Litesh 2023)	51
Gambar 3.2	Output dari penyediaan sumber daya yang digunakan	
	infrastruktur GCPGoat menyediakan URL dari Aplikasi Web	
	GCPGoat	53
Gambar 3.3	Tampilan pertama dari Aplikasi Web GCPGoat setelah selesai	
	penyediaan infrastruktur GCPGoat oleh Terraform	53
Gambar 3.4	Arsitektur GCPGoat berdasarkan File Konfigurasi Terraform	54
Gambar 3.5	Use Case Diagram dari Aplikasi Web GCPGoat	55
Gambar 3.6	Alur dari menggunakan Blog Aplikasi Web GCPGoat untuk	
	membuat dan membaca Post	55
Gambar 3.7	Alur dari penggunaan Web Service "XSS Server" dalam	
	pengujian eksploitasi XSS dalam Aplikasi Web GCPGoat	62
Gambar 3.8	Use Case Diagram dari Web Service yang digunakan dalam	
	eksploitasi vulnerability XSS	62
Gambar 3.9	Google Cloud Platform (GCP) Architecture dari Web Service	
	yang digunakan untuk eksploitasi vulnerability XSS	63
Gambar 3.10	Directory Structure dari source code Web Service "XSS Server"	66
Gambar 3.11	Isi dari file ".env" dari source code Web Service "XSS Server"	68
Gambar 3.12	Isi dari file ".gitignore" dari source code Web Service "XSS	
	Server"	70
Gambar 3.13	Isi dari file "package-lock.json" dari source code Web Service	
	"XSS Server"	71
Gambar 3.14	Isi dari file "package.json" dari source code Web Service "XSS	
	Server"	72
Gambar 3.15	Isi dari file "server.js" dari source code Web Service "XSS	
	Server"	
Gambar 3.16	Isi dari file "routes.js" dari source code Web Service "XSS	
	Server"	79
Gambar 3.17	Isi dari file "handler.js" dari source code Web Service "XSS	
	Server"	83
Gambar 3.18	Diagram Alur dari handler function "getRootHandler"	85
Gambar 3.19	Diagram Alur dari handler function "getTokensPageHandler"	86
Gambar 3.20	Diagram Alur dari handler function "saveTokenHandler"	87
Gambar 3.21	Diagram Alur dari handler function "getAllTokensHandler"	88
Gambar 3.22	Isi dari file "InsertionError.js"	89
Gambar 3.23	Isi dari <i>file</i> "NotFoundError.js"	90
Gambar 3.24	Isi dari file "tokens.ejs" dari source code Web Service "XSS	
	Server"	91

Gambar 3.25	Bagian dari file "tokens.ejs" yang menyertakan setiap JWT Token	
	yang diterima dari database pada HTML Document yang	
	dikembalikan ke <i>requester</i>	91
Gambar 3.26	Diagram Alur cara kerja function "getTokens"	94
Gambar 3.27	Isi dari file "getTokens.js"	94
Gambar 3.28	Diagram Alur cara kerja function "saveToken"	98
Gambar 3.29	Isi dari file "saveToken.js"	99
Gambar 3.30	Dockerfile untuk membuat <i>Container Image</i> dari Web Service "XSS Server".	. 102
Gambar 3.31	URL yang disediakan oleh Cloud Build dari <i>Container Image</i> Web Service "XSS Server" yang selesai dibuat	108
Gambar 3 32	Container Image Web Service "XSS Server" denat diakses	. 100
Gambai 5.52	melalui dashboard Artifacta Registry di Google Cloud Console	108
Combor 2 22	IIPL yang disadiakan alah Claud Pun untuk danat mangirim	. 108
Gambai 5.55	request be Web Service "YSS Server"	100
Combor 2 24	Mangalesas Wah Sarvia "YSS Sarvar" yang sudah di danlay	. 109
Gambal 5.54	mengauseken Cloud Run	100
Combon 1 1	Tempilen Coogle Cloud Concele untuk and neint UTTD your	. 109
Gambar 4.1	diaunakan alah Anlikasi Wah CCDC ast	125
Combon 12	Tampilan Dartama Anlikasi Web CCPGoat	123
Gambar 4.2	In Address deri Hest Anlikesi Web CCPGoat wang diter alter	. 120
Gambar 4.5	IP Address dari Host Aplikasi web GCPGoal yang dilangkap	
	olen wiresnark melalul paket TCP SYN yang dikirim ke Host	107
Combon 4.4	Apiikasi web.	. 127
Gambar 4.4	IP Address dari Host Aplikasi web GCPGoat yang ditangkap	100
Cambra 15	Olen Firetox Dev Loois	. 128
Gambar 4.5	Hasil Port Scanning dengan nmap	. 128
Gambar 4.6	GCPGoat	. 129
Gambar 4.7	HTTP Header yang digunakan untuk berinteraksi dengan backend	
	mengindikasikan penggunaan JWT Token untuk otentikasi	. 129
Gambar 4.8	Input Field dengan fungsionalitas mengunggah gambar melalui	
	URL	. 130
Gambar 4.9	Mendapatkan URL dari Gambar Online untuk melihat cara kerja	
	dari fungsionalitas tersebut	. 130
Gambar 4.10	HTTP Response dari Backend Server setelah mengunggah URL	
	Gambar	. 131
Gambar 4.11	Browser segera mengunduh file yang tercantum pada URL yang	
	dikirim dalam HTTP Response dari Backend Server	. 131
Gambar 4.12	Gambar yang terunggah dari URL tersebut sama dengan URL	
	Gambar yang diberikan ke Backend Server	. 131
Gambar 4.13	Mencoba membuat Backend Server mengunggah file "/etc/hosts"	. 132
Gambar 4.14	File "/etc/hosts" yang tersimpan secara lokal di Host dan berhasil	
	diunggah, mengindikasikan adanya vulnerability terhadap SSRF	. 133
Gambar 4.15	Mencoba membuat Backend Server mengunggah file	
	"/proc/self/environ" yang mengandung Environment Variables	
	yang digunakan oleh Host	. 135
Gambar 4.16	Backend Server benar mengunggah file "/proc/self/environ"	. 135
Gambar 4.17	Isi dari <i>file "/proc/self/environ"</i>	. 136

Gambar 4.18	Fuzzing nama <i>file</i> dan <i>directory</i> dalam <i>directory</i> "workspace" dan "root".	. 138
Gambar 4.19	Hasil Fuzzing nama <i>file</i> dan <i>directory</i> dalam <i>directory</i> "workspace" dan "root"	138
Gambar 4.20	Membuat Backend Server mengunggah <i>file</i> "main.py" dalam	. 150
	directory "workspace"	. 139
Gambar 4.21	Isi dari <i>file</i> "main.py"	. 140
Gambar 4.22	Endpoint dalam Backend Server yang dapat mengirim semua data	1 / 1
Cambra 4 22	<i>user</i> dan Post yang terdapat dalam <i>database</i>	. 141
Gambar 4.23	Mendapatkan semua data <i>user</i> dan Post yang digunakan oleh	140
Combon 1 21	Sistem metalul <i>enapoint</i> dump-db-321423341325	. 142
Gambar 4.24	Data dari <i>user</i> dengan miai autinLevel yang berbeda dengan	140
Combon 1 25	Mongoungkon fungsionalitas "Forget Dessuard" untuk manguhah	. 142
Gailloar 4.23	Deserverd deri user	1/2
Combor 1 26	Parhasil Log In dan manamukan bahwa ugar adalah Admin Usar	143
Cambar 4.20	Monomukan Storago Bucket untuk monyimpon filo gember yang	. 143
Gailibal 4.27	digunakan oleh Anlikasi Wah CCPCoat	145
Combor 1 28	Manamukan Storaga Rucket untuk manyimpan fila gambar yang	. 145
Gailloal 4.20	diunggah melalui UPL oleh Anlikasi Web GCPGoat	1/6
Gambar 1 20	Peneliti mencoha mengakses Storage Bucket "prod-blogapp-	. 140
Gainbar 4.27	c213c27ef30/b802" namun gagal karena tidak memiliki	
	narmission yang cukup	1/6
Gambar 4 30	Peneliti mencoha mengakses Storage Bucket "function-bucket-	. 170
Gambar 4.50	c213c27ef304b80?" namun gagal karena tidak memiliki	
	permission vang cukup	146
Gambar 4.31	Hasil dari HTTP Request yang dikirim ke URL yang digunakan	. 1 10
	untuk memeriksa Permission yang dimiliki Peneliti (dan Publik)	
	pada Storage Bucket "function-bucket-c213c27ef304b802"	. 148
Gambar 4.32	Hasil dari HTTP Request vang dikirim ke URL vang digunakan	
	untuk memeriksa Permission yang dimiliki Peneliti (dan Publik)	
	pada Storage Bucket "prod-blogapp-c213c27ef304b802"	. 148
Gambar 4.33	Fuzzing nama Storage Bucket berdasarkan Pola Penamaan yang	
	ditemukan	. 149
Gambar 4.34	Hasil Fuzzing nama Storage Bucket berdasarkan Pola Penamaan	
	yang ditemukan	. 150
Gambar 4.35	Hasil dari HTTP Request yang dikirim ke URL yang digunakan	
	untuk memeriksa Permission yang dimiliki Peneliti (dan Publik)	
	pada Storage Bucket dev-blogapp-c213c27ef304b802	. 150
Gambar 4.36	Menggunakan gcloud untuk mendapatkan IAM Policy dari	
	Storage Bucket "dev-blogapp-c213c27ef304b802"	. 152
Gambar 4.37	Penambahan Binding pada IAM Policy Storage Bucket "dev-	
	blogapp-c213c27ef304b802"	. 154
Gambar 4.38	Hasil dari HTTP Request yang dikirim ke URL yang digunakan	
	untuk memeriksa Permission yang dimiliki Peneliti (dan Publik)	
	pada Storage Bucket "dev-blogapp-c213c27ef304b802" setelah	
	menambahkan Role "Storage Object Admin" pada publik	. 155

Gambar 4.39	Hasil mengakses Storage Bucket "dev-blogapp- c213c27ef304b802" setelah menambahkan Role "Storage Object	
	Admin" untuk publik	. 155
Gambar 4.40	Isi dari Storage Bucket "dev-blogapp-c213c27ef304b802"	
~	mengandung Identity File dan Public Key untuk SSH	. 157
Gambar 4.41	Isi dari <i>file</i> "/shared/files/.ssh/config.txt" mengandung informasi	
	dari <i>user</i> dan Identity File yang dapat digunakan untuk	
	melakukan SSH dengan Host tertentu	. 157
Gambar 4.42	Hasil dari ICMP Ping dengan Host pada 34.169.30.41	150
C 1 4 42	IL I I TODD (S	. 139
Gambar 4.43	Hasil dari TCP Port Scanning menggunakan nmap menunjukkan	150
Combor 1 11	Polt ICF 22 (SSR) telbuka	. 139
Gambal 4.44	untuk SSH dengen Host pada 34 169 30 41	160
Gambar 4 45	Hasil unava melakukan SSH dengan Host nada 34 169 30 41	. 100
Gambar 4.45	gagal karena konfigurasi akses dari Identity File yang digunakan	
	kurang aman	160
Gambar 4 46	Koneksi SSH berhasil dibentuk dengan Host pada 34 169 30 41	. 100
Sumbur 1.10	setelah mengulang SSH dengan mengubah konfigurasi akses dari	
	Identity File vang digunakan.	. 160
Gambar 4.47	Informasi mengenai konfigurasi gcloud dari Host "34.169.30.41"	100
	menunjukkan bahwa Host merupakan bagian dari GCP Project	
	GCPGoat	. 161
Gambar 4.48	Memeriksa Service Account yang digunakan oleh VM dan	
	menemukan menggunakan Default Compute Engine Service	
	Account yang secara default memiliki Role "Editor" dalam	
	sebuah GCP Project	. 163
Gambar 4.49	Memeriksa Scope yang diberikan pada VM Instance tersebut dan	
	ternyata VM tersebut memiliki Scope untuk pengaturan penuh	
	untuk sumber daya komputasi dalam GCPGoat	. 165
Gambar 4.50	Menggunakan VM pada 34.169.30.41 untuk mendaftarkan semua	
	VM Instance dalam GCPGoat	. 166
Gambar 4.51	Melakukan ICMP Ping dengan VM Instance "admin-vm"	. 167
Gambar 4.52	Melakukan Port Scanning dengan nmap untuk memeriksa Port	
	TCP yang terbuka pada "admin-vm" dan mendapatkan Port TCP	
	22 (SSH) terbuka.	. 167
Gambar 4.53	Hasil dari membuat SSH Key-Pairs, di mana terbuatnya Public	4 40
~	Key "christia2_key.pub" dan Private Key "christia2_key"	. 169
Gambar 4.54	Hasil dari Private Key (Identity File) yang dibuat dengan	1.60
a 1 455	command ssh-keygen	. 169
Gambar 4.55	Hasil dari Public Key yang dibuat dengan <i>command</i> ssh-keygen	. 170
Gambar 4.56	Mengubah Format dari Public Key sesuai dengan format Public	
	Key yang digunakan oleh VM yang disediakan oleh Google	170
Combox 457	Uloud	. 170
Gamoar 4.5/	wienandankan Public Key pada Wietadata V M Instance "admin-	170
Combor 1 50	Viii menggunakan <i>commana</i> geloud	. 170
Gambar 4.38	vanuasi proses bernasii dan dapat SSH dengan VIVI Instance "admin ym"	171
	au111111-v111	. 1/1

Gambar 4.59	Memeriksa Service Account yang digunakan oleh VM Instance "admin-vm"	172
Gambar 4.60	Service Account yang digunakan oleh VM Instance "admin-vm" memiliki Role "Project Owner" yaitu level akses tertinggi dalam	150
Gambar / 61	sebuah GCP Project	172
Gainoar 4.01	platform" vaitu Access Scope vang memberikan akses penuh	
	terhadap sumber dava sebuah GCP Project	172
Gambar 4.62	Service Account vang digunakan oleh VM Instance "admin-vm"	
	dapat digunakan untuk mengakses isi dari Storage Bucket " prod-	
	blogapp-c213c27ef304b802"	173
Gambar 4.63	Memindahkan SSH Public Key dari VM Instance "developer-vm"	
	ke directory lokal peneliti	173
Gambar 4.64	Input Field "Post Headline" dalam halaman "New Post"	175
Gambar 4.65	Input Field "Post Content" dalam halaman "New Post"	175
Gambar 4.66	HTTP Request yang dikirim ke Backend Server setelah mengisi	
	Input Field pada "New Post" dengan nilai yang biasa	176
Gambar 4.67	Nilai dari "Post Content" yang dimasukkan ke dalam HTML	
	Document pada Post yang dibuat	176
Gambar 4.68	Memasukkan Input dengan HTML Tag ke dalam Input Field	1 7 7
C 1 1 CO	"Post Content"	177
Gambar 4.69	HI IP Request yang dikirim ke Backend Server menguban	170
Combon 170	Niloi dari "Dest Content" una menormalian hamiltan mesial	178
Gambar 4.70	HTML membuat HTML Tag che untuk ditempilkan dan bukan	
	mancetak tehal tulisan "This should be Bold"	178
Gambar 4 71	HTTP Request yang sama dengan percohaan sebelumnya namun	170
Gambar 4.71	ditangkan oleh Burn Proxy sebelum dikirim ke Backend Server	180
Gambar 4 72	Mengubah nilai "nostContent" dengan mengubah kembali	100
Sumour 1.72	karakter spesial HTML menjadi karakter "<" dan ">" sebelum	
	dikirim ke Backend Server	180
Gambar 4.73	HTML Tag berhasil mencetak tebal tulisan di dalamnya.	
	mengindikasikan dapat melakukan HTML Injection	181
Gambar 4.74	Memasukkan HTML Element yang mengandung JavaScript	
	untuk mencuri JWT Token ke dalam Input Field "Post Content"	183
Gambar 4.75	Mengubah kembali karakter spesial HTML menjadi karakter "<"	
	dan ">" pada HTTP Request yang mengandung HTML Element	
	untuk mencuri JWT Token	183
Gambar 4.76	HTML Element yang menjalankan JavaScript untuk mengirim	
	JWT Token dari browser ke XSS Server terlihat pada halaman	
	Post yang di buat	184
Gambar 4.77	JWT Token dari user berhasil ditangkap dan disimpan oleh XSS	
	Server	184
Gambar 4.78	JWT Token yang ditangkap oleh XSS Server sama dengan JWT	
a	Token yang disimpan oleh <i>browser user</i>	185
Gambar 4.79	Menggunakan Burp Suite untuk membuat dan mengirim HTTP	
	Request ke Backend Server untuk membuat sebuah Post yang	10-
	mengandung HTML Element yang disembunyikan	186

Gambar 4.80	HTML Element yang menjalankan JavaScript untuk mengirim JWT Token dari <i>browser</i> ke XSS Server tidak lagi terlihat pada	
	halaman Post	187
Gambar 4.81	JWT Token dari <i>user</i> berhasil ditangkap dan disimpan oleh XSS Server walaupun HTML Element tidak terlihat pada halaman Post	187
Gambar 4.82	Peneliti berusaha mengakses halaman "Dashboard" namun selalu gagal karena belum melakukan Log In	188
Gambar 4.83	Peneliti menggunakan JWT Token yang ditangkap oleh XSS Server untuk digunakan oleh <i>browser</i> peneliti saat berinteraksi	100
Gambar 4.84	Peneliti menambahkan Key-Value pair pada Session Storage pada browser yang digunakan oleh peneliti dan menggunakan JWT Token dari XSS Server	188
Gambar 4.85	Peneliti mencoba untuk membuka halaman "Dashboard" setelah menambahkan JWT Token dari XSS Server pada Session Storage	107
Gambar 4.86	Peneliti berhasil mengakses halaman "Dashboard" dengan hanya menggunakan JWT Token milik <i>user</i> lain yang ditangkap dan disimpan oleh XSS Server	189
Gambar 4.87	Karena tidak menggunakan metode Log In yang biasa, ada beberapa data yang belum dimiliki oleh <i>browser</i> untuk	107
	ditampilkan pada halaman tertentu	189
Gambar 4.88	Tampilan halaman "User" pada Dashboard sebagai user biasa	190
Gambar 4.89	Tampilan halaman "User" pada Dashboard sebagai Super User	190
Gambar 4.90	Tampilan halaman "User" pada Dashboard dengan JWT Token milik Super User	190
Gambar 4 91	source code endpoint "/save-content"	199
Gambar 4.92	Diagram Alur dari <i>endpoint</i> "/save-content"	200
Gambar 4.92	source code function "upload file"	200
Gambar 4.93	source code function "download url"	200
Gambar 4.94	Depembehan pada function "download url" untuk mitigasi	200
Gainbai 4.93	vulnerability SSRF	202
Gambar 4.96	Penambahan <i>function</i> untuk digunakan oleh <i>function</i>	202
	"download_url" untuk mengimplementasi sebuah mekanisme	
	Allowlist terhadap URL yang diterima sebagai Input dari user	203
Gambar 4.97	Mendapatkan URL dari Gambar Online untuk melihat cara kerja	
	dari fungsionalitas setelah menambahkan Input Validation untuk	
	Input URL	204
Gambar 4.98	HTTP Response dari Backend Server setelah mengunggah URL	
	Gambar	204
Gambar 4.99	Browser segera mengunduh file yang tercantum pada URL yang	
	dikirim dalam HTTP Response dari Backend Server	205
Gambar 4.100	Gambar yang terunggah dari URL tersebut tetap sama dengan	
	URL Gambar yang diberikan ke Backend Server setelah	
	menambahkan Input Validation untuk Input URL	205
Gambar 4.101	Mencoba membuat Backend Server mengunggah file "/etc/hosts"	
	tetapi menampilkan Error	206
Gambar 4.102	Detail Error tertangkap oleh Error Reporting	206
Gambar 4.103	source code endpoint "/save-post"	207

Gambar 4.104	source code function "create"	. 208
Gambar 4.105	Diagram Alur dari endpoint "/save-post"	. 209
Gambar 4.106	WYSIWYG Editor dalam halaman "New Post" dalam Aplikasi	010
Combor 4 107	Denombahan nada andnoint "/anya nast" untuk mitigasi	212
Gambar 4.107	vulnerability XSS	213
Gambar 4.108	Memberikan Input dengan Styling dan Struktur sederhana pada	
	WYSIWYG Editor untuk konten sebuah Post	. 215
Gambar 4.109	Hasil yang ditampilkan pada halaman Post sama persis dengan	
	Styling dan Struktur yang dirancang menggunakan WYSIWYG	
	Editor	215
Gambar 4.110	Memberikan Input yang mengandung karakter-karakter yang	
	direservasi HTML pada WYSIWYG Editor untuk konten sebuah	
	Post	215
Gambar 4.111	Output dari WYSIWYG yang melakukan Output Encoding	
	(HTML Entity Encoding)	216
Gambar 4.112	Hasil yang ditampilkan pada halaman Post sama persis dengan	
	Styling dan Struktur yang dirancang menggunakan WYSIWYG	
	Editor walaupun Input mengandung karakter-karakter yang	
	direservasi oleh HTML.	216
Gambar 4.113	Menggunakan Burp Proxy untuk memberikan Input yang	
	digunakan untuk eksploitasi vulnerability XSS pada Backend	
	Server tanpa melalui WYSIWYG Editor	217
Gambar 4.114	Hasil yang ditampilkan pada halaman Post menghapus (<i>strip</i>)	
	HTML Element dari Input yang diberikan karena HTML Element	
	tersebut menggunakan HTML Tag yang tidak termasuk dalam	
a 1 1 1 1	daftar Allowed Tags yang ditentukan	218
Gambar 4.115	Menggunakan Burp Proxy untuk memberikan Input yang	
	digunakan untuk eksploitasi vulnerability XSS pada Backend	
	Server tanpa melalui WYSIWYG Editor namun juga	
	mengandung HTML Element yang menggunakan HTML Tag	010
0 1 1110		218
Gambar 4.116	Hasil yang ditampilkan pada halaman Post menghapus (<i>strip</i>)	
	HIML Element dari input yang diberikan karena HIML Element	
	tersebut menggunakan HTML Tag <irrame> yang tidak termasuk</irrame>	
	dalam daftar Allowed Tags yang ditentukan, sedangkan HTML	010
Combon 4 117	Element yang menggunakan HTML Tag tetap ditampilkan	219
Gambar 4.11/	Alur dari penggunaan web Service "ASS Server" dalam	
	pengujian ekspionasi XSS dalam Aplikasi web GCPGoat setelan	220
Combon 4 110	Deskhoord ashush Case dalam SCC	220
Gambar 4.118	Lashboard sedual Case dalam SCC	224
Gambar 4.119	Fungsionalitas Dick Engine SCC	220
Gambar 4.120	Puligsionanias Kisk Eligine SCC	221
Gainual 4.121	Cases yang ditemukan Risk Engine seteleh melekukan Virtuel	
	Cases yang unemukan Kisk Engine Seletah melakukan vintual Red Teaming terhadan Asat dan lingkungan Cloud austamar	$\gamma\gamma$
Gambar 4 122	Case Dashboard dari salah satu Cases yang dihasilkan oleh Pisk	220
Gainual 4.122	Engine setelah menemukan kesalahan konfigurasi aksas untuk	
	Service Account sebuah VM yang dapat diaksas oleh publik yang	
	Service Account section vivi yang dapat diakses oleh publik yang	

	memungkinkan terjadinya Privilege Escalation dan Exposure	
	terhadap aset kritis	. 228
Gambar 4.123	Attack Path Visualization dari salah satu Cases yang dihasilkan	
	oleh Risk Engine menemukan kesalahan konfigurasi terhadap	
	Service Account sebuah VM yang menyebabkan terjadinya	
	Privilege Escalation untuk dapat mengakses dan memodifikasi	
	dataset sensitif dalam BigOuery	229
Gambar 4,124	4 komponen utama Zero Trust dari BevondCorp	243
Gambar 4 125	4 lavanan inti dalam BeyondCorn untuk masing-masing	213
Guinour 1.125	komponen Zero Trust	243
Gambar 4 126	Role "Dev role" dihubungkan (<i>bind</i>) dengan <i>principal</i> "allUsers"	213
Guillour 1.120	dalam Storage Bucket "dev-blogann-c213c27ef304b802"	245
Gambar 4 127	Daftar parmission dalam Role "Dev role"	245
Gambar 4 127	Manambahkan IAM Policy Binding yang menghubungkan (hind)	. 273
Gainbai 4.120	nringing l'abristion know amail com? (untuk moron resentesikan	
	amail dari tim dayalanar) dangan Rala "Day rala"	216
Cambon 4 120	Manghilangkan IAM Deligu Dinding yang menghuhungkan (<i>kin l</i>)	. 240
Gainbar 4.129	i i 1% III January Languary Data "Describe"	247
C 1 1 120	principal "all'Users" dengan Role "Dev role"	. 247
Gambar 4.130	Hasil dari HTTP Request yang dikirim ke URL yang digunakan	
	untuk memeriksa Permission yang dimiliki Peneliti (dan Publik)	
	pada Storage Bucket dev-blogapp-c213c2/ef304b802 setelah	• • •
	mengubah konfigurasi IAM Storage Bucket tersebut	. 248
Gambar 4.131	Menghentikan VM "developer-vm" agar dapat mengubah	
	konfigurasi VM tersebut	. 250
Gambar 4.132	Mengubah konfigurasi Access Scope dari VM "developer-vm"	
	untuk menggunakan Access Scope	
	"https://www.googleapis.com/auth/cloud-platform"	250
Gambar 4.133	IAM Permission yang dimiliki Role "Editor" terhadap sumber	
	daya VM Instance Compute Engine dalam sebuah GCP Project	251
Gambar 4.134	IAM Permission yang dimiliki Role "Compute Viewer" terhadap	
	sumber daya VM Instance Compute Engine dalam sebuah GCP	
	Project.	252
Gambar 4.135	Membuat Service Account "developer-vm-sa" khusus untuk	
	digunakan VM "developer-vm"	253
Gambar 4.136	Membuat sebuah IAM Policy Binding untuk mengasosiasikan	
	Service Account "developer-vm" dengan Role "Compute	
	Viewer"	254
Gambar 4.137	IAM Policy Binding antara Service Account "developer-ym-sa"	
Current inter	dengan Role "Compute Viewer" berhasil ditambahkan	254
Gambar 4 138	Menguhah Service Account vang digunakan VM "developer-vm"	231
Guinoar 4.150	untuk menggunakan Service Account "developer-vm-sa"	255
Gambar 4 139	Memulai kembali VM "developer-vm" dengan konfigurasi	. 233
Gainbai 4.139	Access Scope dan Service Account yang baru	255
Gambar 4 140	Memeriksa Service Account yang digunakan oleh VM	
Janibal 4.140	"developer ym" setelab perubahan konfigurasi	756
Combor 4 141	Momenikan A apage Soona yang digyaalaga alah VM "dayalaga"	0
Gambar 4.141	weinenksa Access Scope yang digunakan oleh v Mi "developer-	DEC
	vm selelan perubanan konfigurasi melalui geloud	236

Memeriksa Access Scope yang digunakan oleh VM "developer-	
vm" setelah perubahan konfigurasi melalui Compute Metadata	
Server Google Cloud	257
Menambahkan Public Key pada Metadata VM Instance "admin-	
vm" setelah perubahan konfigurasi menggunakan command	
gcloud, namun tidak berhasil karena tidak lagi memiliki	
permission yang cukup	257
Standar pengamanan Web Services untuk setiap aspek	
implementasi Web Services	267
Struktur dari CSF Core	270
CSF Functions	272
Tabel Core Function serta Category masing-masing Function dari	
CSF 2.0	273
Langkah-langkah membuat dan menggunakan CSF	
Organizational Profile	274
CSF Tiers dalam Cybersecurity Risk Management	277
Tahap-tahap dalam CSA SSDLC	279
Klasifikasi ancaman STRIDE serta security requirement yang	
terdampak	283
	Memeriksa Access Scope yang digunakan oleh VM "developer- vm" setelah perubahan konfigurasi melalui Compute Metadata Server Google Cloud Menambahkan Public Key pada Metadata VM Instance "admin- vm" setelah perubahan konfigurasi menggunakan <i>command</i> gcloud, namun tidak berhasil karena tidak lagi memiliki <i>permission</i> yang cukup Standar pengamanan Web Services untuk setiap aspek implementasi Web Services Struktur dari CSF Core CSF Functions Tabel Core Function serta Category masing-masing Function dari CSF 2.0 Langkah-langkah membuat dan menggunakan CSF Organizational Profile CSF Tiers dalam Cybersecurity Risk Management Tahap-tahap dalam CSA SSDLC Klasifikasi ancaman STRIDE serta <i>security requirement</i> yang terdampak.



DAFTAR TABEL

		halaman
Tabel 2.1	Pengelompokan layanan Google Cloud dalam kategori layanan	
	Cloud	37
Tabel 2.2	Penjelasan Shared Responsibility masing-masing kategori layanan	
	Cloud	40
Tabel 2.3	Penjelasan 3 Block yang diperlukan untuk sebuah File	
	Konfigurasi Terraform	46
Tabel 2.4	Penjelasan dari Variable Block, Data Block, dan Locals Block	47
Tabel 3.1	Penjelasan layanan-layanan Google Cloud yang digunakan oleh	
	Aplikasi Web GCPGoat	55
Tabel 3.2	Penjelasan layanan-layanan Google Cloud yang digunakan dalam	
	CI/CD Pipeline GCPGoat	59
Tabel 3.3	Pengelompokan File dan drectory dalam Directory Structure Web	
	Service "XSS Server"	66
Tabel 3.4	Penjelasan setiap Route dalam kategori "Route yang bersifat	
	sebagai Utilitas dari HTTP Server"	80
Tabel 3.5	Penjelasan setiap Route dalam kategori "Route yang bersifat	
	sebagai API Endpoint"	81
Tabel 3.6	Penjelasan setiap Route dalam kategori "Route yang	
	mengembalikan Halaman"	81
Tabel 3.7	Garis Besar function dalam directory "services"	92
Tabel 4.1	Garis Besar Implementasi Penetration Testing	110
Tabel 4.2	Teknik Penetration Testing serta tools yang digunakan	120
Tabel 4.3	Penjelasan Tools yang digunakan	121
Tabel 4.4	Hasil Pengujian pada infrastruktur GCPGoat	191
Tabel 4.5	Garis besar rekomendasi untuk mengimplementasi masing-	
	masing strategi mitigasi untuk infrastruktur GCPGoat	196
Tabel 4.6	Rangkuman rekomendasi peneliti untuk mengimplementasi setiap	
	prinsip Zero Trust dalam lingkungan Cloud GCPGoat	263
Tabel 4.7	Isu-isu "Top Threats to Cloud Computing 2024" yang	
	ditunjukkan dalam pengujian terhadap infrastruktur GCPGoat	285
Tabel 4.8	Daftar kumpulan kesalahan kecil/sederhana yang menyebabkan	
	kerugian besar yang ditemukan dalam pengujian terhadap	
	infrastruktur GCPGoat	286

DAFTAR LAMPIRAN

halaman

