

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PENGESAHAN	iii
HALAMAN MOTTO	v
PRAKATA	vi
DAFTAR ISI	viii
DAFTAR TABEL	x
DAFTAR GAMBAR	xiii
INTISARI	xiv
ABSTRACT	xv
I PENDAHULUAN	1
1.1 Latar Belakang Masalah	1
1.2 Rumusan Masalah	3
1.3 Batasan Masalah	3
1.4 Tujuan Penelitian	3
1.5 Manfaat Penelitian	3
1.6 Metode Penelitian	4
1.7 Sistematika Penulisan	5
II TINJAUAN PUSTAKA	6
III LANDASAN TEORI	10
3.1 Kriptografi	10
3.2 Variasi Mode Operasi <i>Block Cipher</i>	11
3.3 <i>Propagating Cipher Block Chaining</i>	13
3.4 <i>Block Cipher Standard Padding</i>	14
3.5 Serangan <i>Padding Oracle</i>	15
3.5.1 <i>Padding Oracle</i>	15

3.5.2	<i>Recovering Plaintext</i>	16
3.5.3	<i>Forging Ciphertext</i>	17
IV	ANALISIS DAN RANCANGAN	19
4.1	Gambaran Umum Penelitian	19
4.2	Tahapan Penelitian	19
4.3	Perancangan Server Target	20
4.4	Perancangan Serangan	21
4.4.1	Analisis Pemrosesan <i>Cookies</i>	22
4.4.2	Perancangan <i>Proof Of Concept</i> Untuk <i>Recovering Plaintext</i>	23
4.4.3	Analisis <i>Plaintext</i> Dari <i>Cookies</i>	25
4.4.4	Perancangan <i>Proof Of Concept</i> Untuk <i>Forging Ciphertext</i>	25
4.5	Perancangan Pengujian	26
4.5.1	Evaluasi Waktu Eksekusi	26
4.5.2	Perancangan <i>Security Advisory</i>	29
V	IMPLEMENTASI	31
5.1	Alat dan Bahan	31
5.2	Implementasi Server Target	31
5.2.1	Model AES-PCBC	31
5.2.2	<i>Notes App Webservice</i>	35
5.3	Implementasi <i>Exploit</i>	51
5.3.1	Model <i>Exploit</i>	51
5.3.2	Model Evaluasi	58
5.3.3	<i>Script</i> Eksploitasi	60
VI	HASIL DAN PEMBAHASAN	65
6.1	Hasil Proses Eksploitasi	65
6.2	Hasil Proses Evaluasi	67
6.3	<i>Security Advisory</i>	70
VII	PENUTUP	72
7.1	Kesimpulan	72
7.2	Saran	72
	DAFTAR PUSTAKA	73