

DAFTAR ISI

HALAMAN PERNYATAAN KEASLIAN	ii
HALAMAN PENGESAHAN TUGAS AKHIR	iii
HALAMAN PERSETUJUAN PUBLIKASI KARYA ILMIAH	iv
KATA PENGANTAR	v
ABSTRAK	vi
DAFTAR ISI.....	viii
DAFTAR TABEL	x
DAFTAR GAMBAR	xi
BAB I PENDAHULUAN	1
1.1 Latar Belakang Masalah	1
1.2 Identifikasi Masalah	3
1.3 Tujuan Masalah	3
1.4 Batasan Masalah.....	3
1.5 Manfaat Penelitian.....	4
1.6 Kerangka Berfikir.....	4
1.7 Sistematika Penulisan.....	6
BAB II LANDASAN TEORI	7
2.1 <i>Content Management System (CMS)</i>	7
2.1.1 Wordpress	7
2.1.2 Plugin Wordpress.....	7
2.2 PHP.....	8
2.2.1 PHPShell	8
2.3 LINUX.....	9
2.3.1 Kelebihan Linux.....	10
2.3.2 Kekurangan Linux.....	10
2.4 <i>Websserver</i>	10
2.5 <i>Unrestricted File upload</i>	11
2.6 <i>Vulnerability Research</i>	11

2.7	<i>Penetration Testing</i>	11
2.7.1	Teknik <i>Penetration testing</i>	11
2.8	<i>Wordpress Vulnerability Scanner (WPScan)</i>	12
2.9	<i>Common Vulnerability and Exposure (CVE)</i>	13
2.10	Google Dork	13
2.11	<i>Open Web Application Security Project (OWASP)</i>	14
BAB III METODE PENELITIAN.....		16
3.1	Perumusan Masalah.....	16
3.2	Metode Pengujian.....	16
3.2.1	<i>Information Gathering</i>	16
3.2.2	<i>Vulnerability Analysis</i>	17
3.2.3	<i>Exploitation</i>	17
3.2.4	<i>Privilege Escalation</i>	17
3.2.5	<i>Reporting</i>	17
3.3	Teknik Pengumpulan Data	17
3.4	Kebutuhan Perangkat Lunak	18
BAB IV HASIL DAN PEMBAHASAN		19
4.1	<i>Target</i>	19
4.2	<i>Information Gathering</i>	19
4.3	<i>Vulnerability Analysis</i>	21
4.4	<i>Exploitation</i>	22
4.5	<i>Privilege Escalation</i>	25
4.6	<i>Reporting</i>	28
BAB V SARAN DAN KESIMPULAN.....		29
5.1	Kesimpulan	29
5.2	Saran.....	30
DAFTAR PUSTAKA		31

DAFTAR TABEL

Tabel 2. 1 Fungsi –fungsi PHP *shell* 2

Table 3. 1 Perangkat Lunak17

Tabel 4. 1 Target berdasarkan *Dork*18

Tabel 4.2 Tabel CVE wp-file-manager.....20

DAFTAR GAMBAR

Gambar 1. 1 Persentase jenis serangan terhadap Wordpress	2
Gambar 1. 2 Kerangka Berfikir	5
Gambar 2. 1 Tampilan utama WPScan pada Kali linux	12
Gambar 2. 2 Dork wp file manager.....	14
Gambar 2. 3 celah keamanan OWASP Top 10.....	15
Gambar 3. 1 Metodologi OWASP Penetration Testing	15
Gambar 4.1 Tampilan web target	19
Gambar 4.2 Hasil Scanning WPScan	19
Gambar 4.3 Directory Listing	20
Gambar 4.4 Upload PHPShell	21
Gambar 4.5 Directory file exploit	22
Gambar 4.6 Directory server target	22
Gambar 4.7 wp-config.php	23
Gambar 4.8 Login phpmyadmin	24
Gambar 4.9 akun admin Wordpress target	24
Gambar 4.10 mengubah password admin	25
Gambar 4.11 Password berhasil diubah	25
Gambar 4.12 Percobaan login Wordpress target	26
Gambar 4.13 Dashboard Wordpress target	26