Keamanan Web Unit Kerja IPB

Dan Upaya Peningkatannya

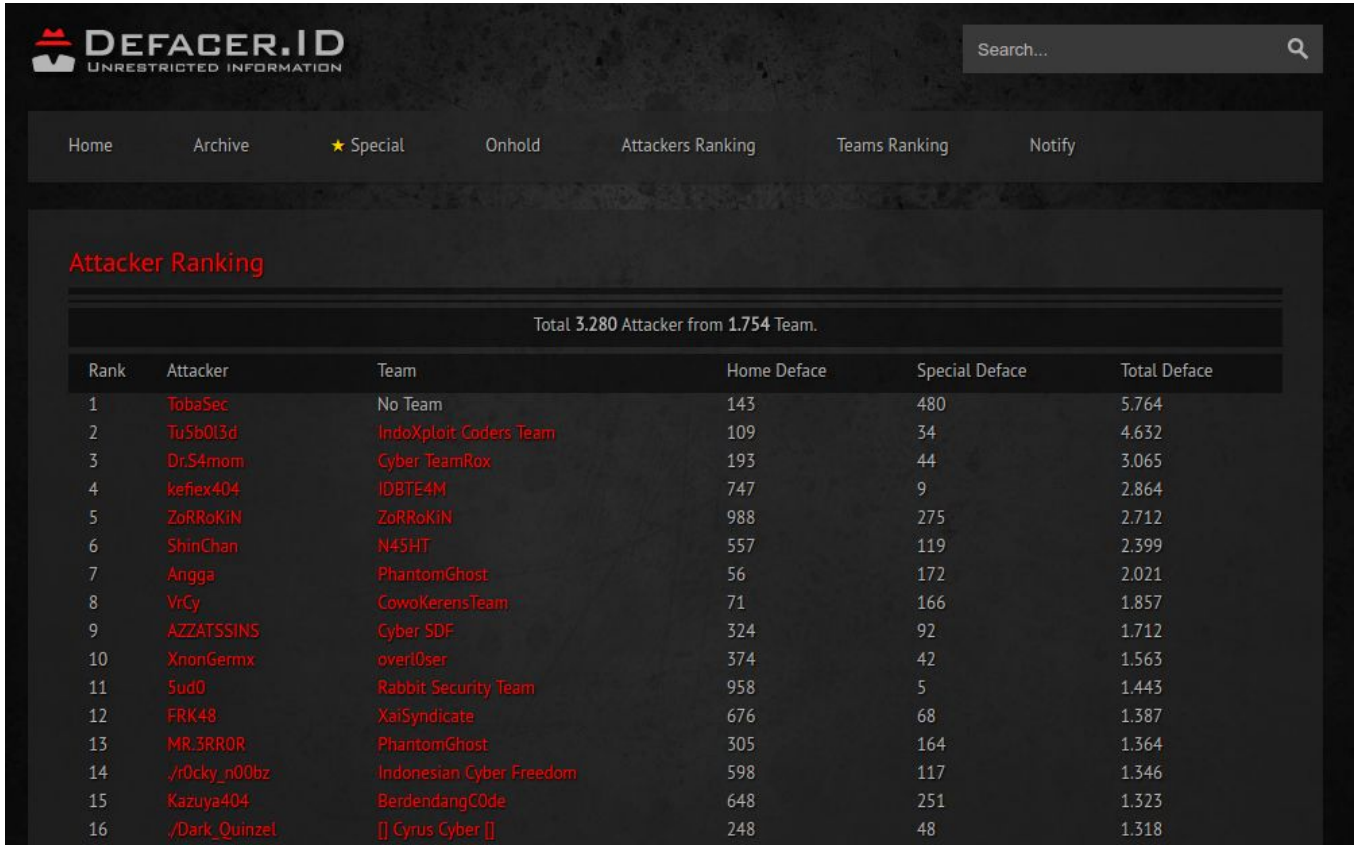
Latar Belakang

- Semakin banyaknya serangan ke web-web unit kerja di IPB.
- Web-web IPB semakin populer, namun juga semakin mengundang para penjahat.
- Peningkatan visibility harus diimbangi dengan peningkatan keamanan.

Motivasi Serangan

Mengapa mereka menyerang web Anda

- Kebanggaan



Motivasi Serangan

Mengapa mereka menyerang web Anda

- Spamming
  Penyerang menggunakan server yang sudah berhasil mereka kuasai untuk mengirim email spam
- Penyanderaan data (ransomware)
  Penyerang mengunci data di web sehingga tidak bisa dibuka dan meminta uang tebusan untuk membuka kuncinya

Pada dasarnya semua web yang sifatnya publik pasti akan mendapatkan “cobaan”. Masalahnya hanyalah apakah serangan berhasil atau tidak.

Bentuk Serangan

Apa yang biasanya mereka perbuat kepada web Anda

- Deface

Jenis-jenis Deface

Non-homepage:

- Mengupload file yang berisi pesan deface namun bukan di halaman utama. Halaman utama tetap utuh.

Homepage deface:

- Menyisipkan script kecil tapi menutupi seluruh halaman web sehingga tidak dapat dibaca.
- Mengganti halaman index web dengan halaman deface, sedangkan halaman index aslinya masih tetap ada.
- Menghapus seluruh isi web dan diganti dengan halaman deface.
- Mengunci seluruh data di web dan meminta uang tebusan.

Bentuk Serangan

Apa yang biasanya mereka perbuat kepada web Anda

- Meninggalkan “backdoor”

Penyerang bisa saja meninggalkan “backdoor” untuk kembali masuk ke web Anda di lain waktu dan merusaknya kembali. Recovery harus dilakukan dengan benar pasca-serangan.

- Mencuri data

Jika di web Anda terdapat data-data penting, bisa saja dicuri oleh penyerang yang berhasil masuk ke sistem.

Faktor Ketidakamanan

Mengapa web Anda berhasil diserang

Dari sisi pengguna

Dari sisi sistem

Dari Sisi Pengguna: Manajemen Password

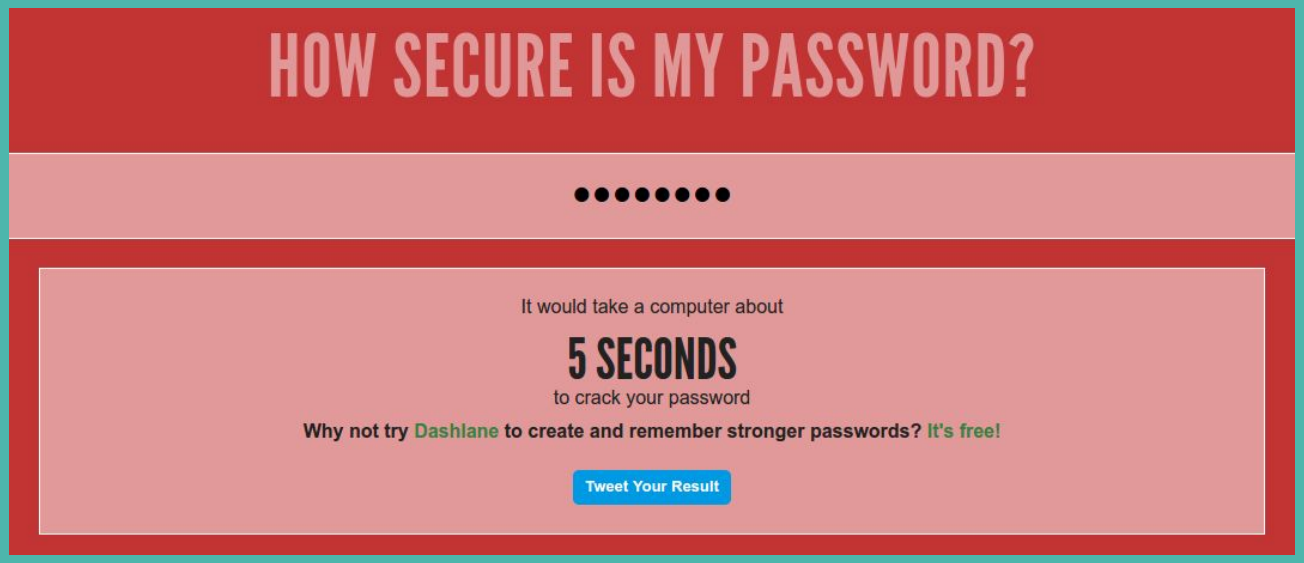
Untuk web unit kerja paling tidak ada tiga password akun:

1. Password admin web/CMS
2. Password server (FTP & SSH)
3. Password ke database

Ketiga password tersebut harus kuat:

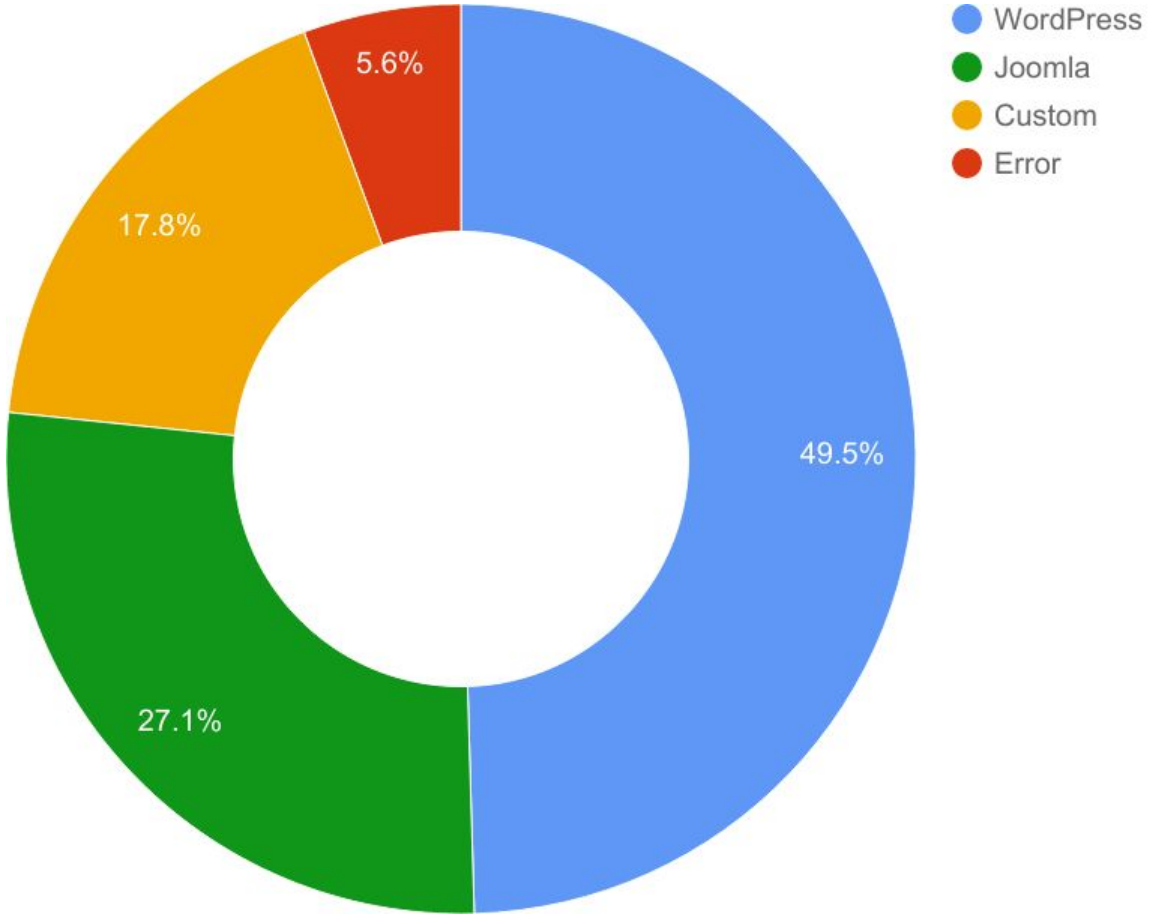
- Berbeda dengan username
- Berbeda satu sama lain
- Cukup panjang
- Tidak mudah ditebak
- Dikelola dengan baik

Cek seberapa aman password Anda di:
http://howsecureismypassword.net



Dari Sisi Sistem: Keamanan CMS

CMS yang digunakan oleh web unit IPB:

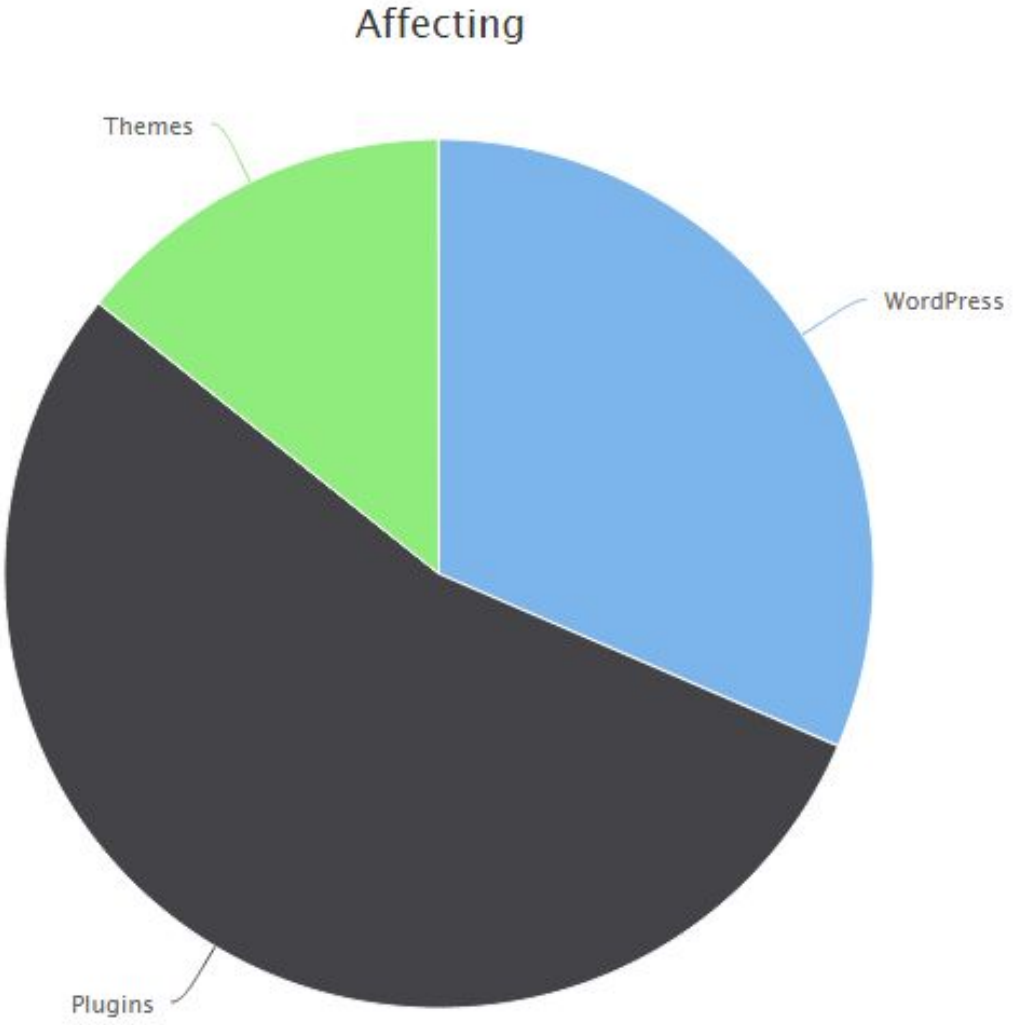


WordPress

Faktor ketidakamanan WordPress:

- WordPress-nya itu sendiri
- Plugin
- Theme

Semua terkait versi
yang tidak diperbarui (update)



https://www.wpwhitesecurity.com/wp-content/uploads/2014/11/WordPress-vulnerabilities.png

Joomla

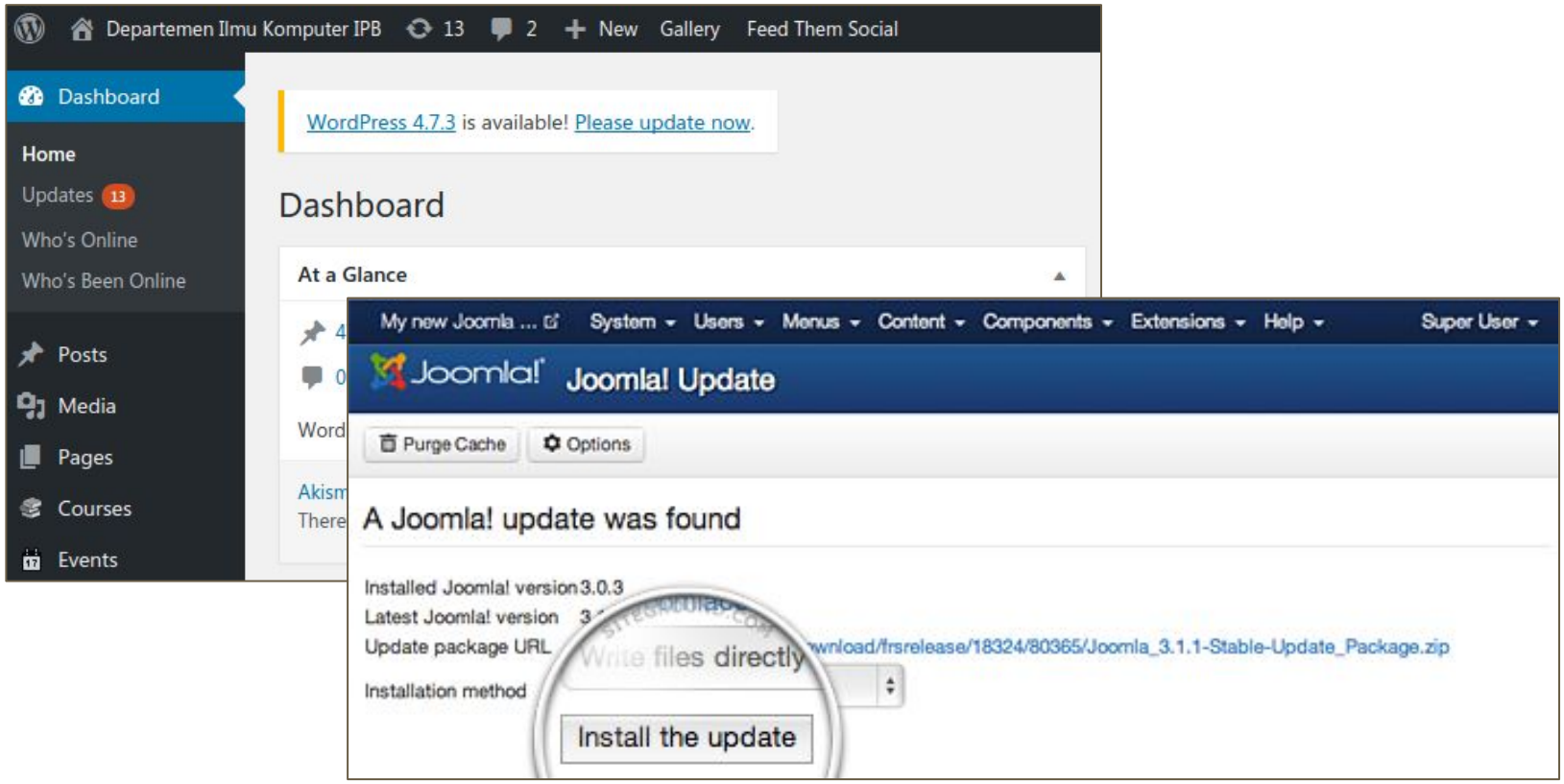
Joomla versi lama (di bawah 1.5) memiliki banyak celah sehingga mudah bagi penyerang untuk menemukan celah tersebut dan merusak web Anda

CMS Lain (Custom)

- Sebagian web unit kerja menggunakan CMS lain atau membuat CMS sendiri (outsourcing web developer dari luar).
- Keamanan web bergantung pada apakah web developer tersebut membuat CMS-nya dengan memperhatikan keamanan web atau tidak
- Tidak menutup kemungkinan CMS custom lebih rentan untuk diserang dibandingkan CMS populer seperti WordPress dan Joomla

Kiat Peningkatan Keamanan CMS

- Pastikan melakukan update core CMS jika tersedia yang baru



Kiat Peningkatan Keamanan CMS

Untuk WordPress:

- Pastikan update juga plugin yang terpasang (bukan hanya yang aktif!)
- Lakukan hal yang sama jika theme yang digunakan ada update-nya
- Tambahan: pasang plugin Wordfence untuk pemantauan keamanan

Kiat Peningkatan Keamanan CMS

Untuk Joomla:

- Instal extension **Securitycheck** versi free.
- Extension lain mayoritas berbayar. Daftarnya dapat dilihat pada alamat:

https://extensions.joomla.org/tags/site-security/

Mengamankan File Permission di Server

Untuk unit kerja yang memiliki akses ke server (FTP), pastikan file permission di server diset dengan benar:

- Untuk file: owner user dan permission 644
- Untuk folder: owner user dan permission 755
- Khusus folder tempat upload (gambar dll): owner www-data atau permission 777

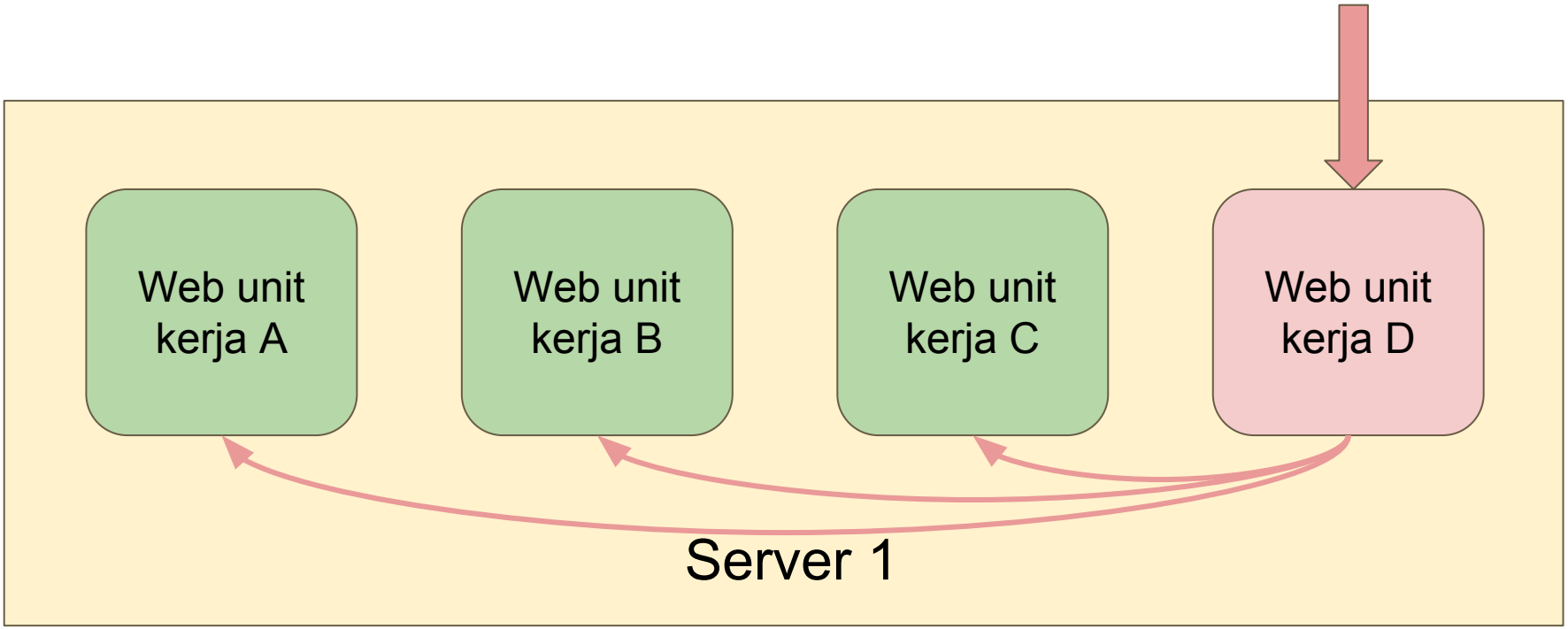
Jika permission diset dengan benar, akan mencegah penyerang untuk merusak web lebih jauh,

Bersihkan File Tidak Terpakai

- Jika update ke server dengan mengupload file ZIP misalnya, pastikan file ZIP tersebut dihapus kembali setelah di-extract isinya
- Begitu juga file backup, jangan disimpan di server karena bisa ditemukan oleh penyerang

Serangan “Tidak Langsung”

Penyerang dapat menyerang web yang sudah diperkuat melalui web lain yang masih lemah **dalam satu server yang sama**.



Serangan “Tidak Langsung”

- Serangan juga bisa dari satu web yang sama, namun terdapat beberapa aplikasi pada web tersebut.
- Jika ada satu saja sistem atau aplikasi yang lemah, web utama kemungkinan juga bisa dirusak.

Web unit kerja A

`abc.ipb.ac.id/`	Web utama
`abc.ipb.ac.id/library`	Katalog perpustakaan
`abc.ipb.ac.id/jurnal`	Publikasi (OJS)
`abc.ipb.ac.id/sisfo`	Sistem informasi internal

Jika Sudah Terlanjur Diserang...

- Kembalikan dari backup
  - **Backup wajib dimiliki** supaya jika rusak dapat dikembalikan
- Bersihkan server
  - Cek secara menyeluruh file-file di server untuk mengetahui apakah penyerang meninggalkan backdoor
- Ubah seluruh password
  - Password akun, password server, dan password database
- Analisis forensik
  - Jika memungkinkan, analisis dari celah mana penyerang bisa masuk dan perbaiki celah tersebut
  - Butuh keahlian khusus untuk analisis seperti ini

Manajemen Insiden

- Insiden keamanan web dan sistem yang pernah terjadi perlu didokumentasikan dengan baik untuk penanganan ke depan.
- Perlu dicatat misalnya:
  - Detail insiden
  - Tanggal
  - Rekaman
  - Hasil investigasi penyebab
  - Penanganan