



Pelatihan Peningkatan Keamanan Website

Pada Aparatur Sipil Negara di Lingkungan
Pemerintah Kota Banjarbaru





Keamanan web Sistem



Hello!

Mirza Yogy K, S.Kom., M.Kom

- Dosen Fakultas Teknologi Informasi UNISKA
- Desktop Programming
- Web Programming
- Mobile Programming

1

Web Server

Layanan akses melalui [HTTP](#) atau [HTTPS](#) atas berkas-berkas yang dalam [situs.web](#)



Web Server

- IIS (untuk html & asp) di OS Windows
- APACHE webserver untuk html,php,asp,jsp, dsb). Bisa di OS Windows dan LINUX.



Exploitasi Server www

- Hijacking
- Session hijacking
- Juggernaut
- Hunt
- Replay
- Virus
- Worm
- Spyware
- Cookies
- Phising
- Pharming

2

Pengamanan Web



Membatasi Akses

● Access Control

Hanya IP tertentu yang dapat mengakses server Menggunakan enkripsi untuk menyandikan data-data

● Htaccess di apache

Batasi berbagai macam akses pada konfigurasi .htaccess



Secure Socket Layer

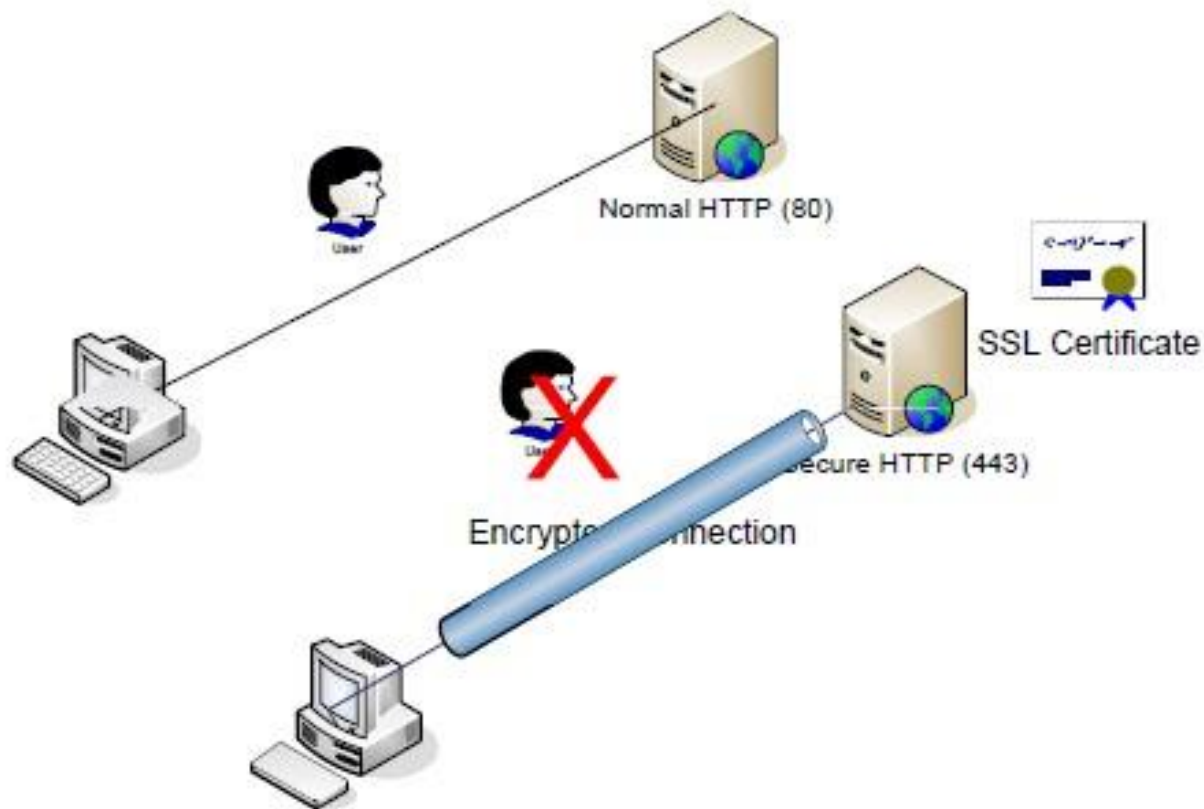
- Menggunakan enkripsi untuk mengamankan transmisi data
- Mulanya dikembangkan oleh Netscape
- Implementasi gratis pun tersedia openSSL



HTTPS pada web server

- HTTPS adalah varian dari protocol HTTP dimana user mengakses dengan https://
- Data yang dikirim ke server adalah data yang terenkripsi.
- Enkripsi yang digunakan adalah enkripsi SSL (Secure socket Layer).
- Menggunakan TCP port 443.

Ilustrasi Koneksi HTTP vs HTTPS



1

HACKERS!

Semua orang tahu Hacker?

2

HACKERS!

CRACKERS!

Sisi lain dari Hacker?

3

HACKERS!

Semua orang bilang Hackers



Keamanan web berbasis Wordpress



Hello!

Fathul Hafidh, S.Kom., M.Kom

- Dosen Fakultas Teknologi Informasi UNISKA
- Web Programming
- Networking



WordPress Hacks

- Warning! Massive Number of GoDaddy WordPress Blogs Hacked!
- DreamHost: One Million Domains Hacked; WordPress Blogs Infected
- WordPress Sites on GoDaddy, Bluehost Hacked
- Reuters Hacked Again, Outdated WordPress Blog At Fault?
- InMotion Hosting Servers Hacked, Thousands of Web Sites Affected



WordPress Hacks

- Kenyataannya sangat sedikit website “WordPress Hacks”
- “ In the vast majority of cases I see, attackers get in some other way, and then once already in the system, they go looking for WordPress installs.” -- Mark Jaquith

*Jika WordPress bukan merupakan
titik lemah, lalu siapa?*



“



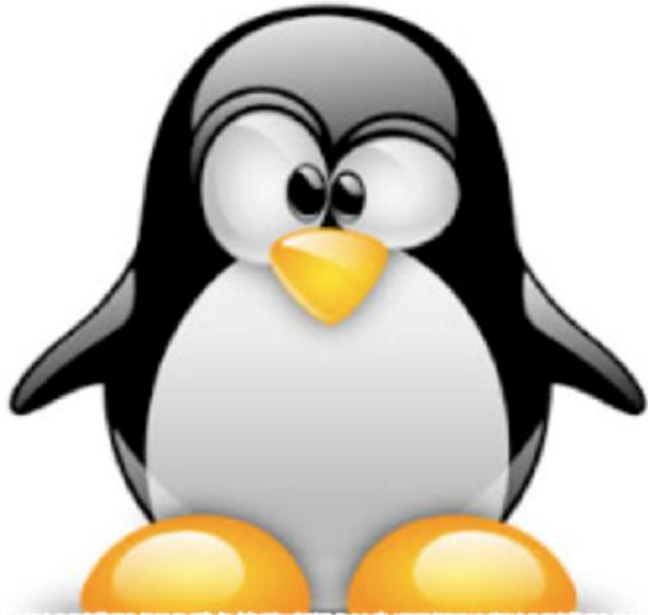
WordPress Hacks

- ❑ Most hacks that **affect** WordPress actually originate **outside** of WordPress Core.
 - ❑ TimThumb (PHP library, many themes/plugins)
 - ❑ Uploadify (jQuery plugin, many themes/plugins)
 - ❑ Adserve (plugin)
 - ❑ WassUp (plugin)
 - ❑ Is Human (plugin)

*Kita perlu melihat gambaran yang
lebih besar*



“



Komponen
LAMPP





Other Services and Apps

- SMTP (email)
- FTP
- DNS
- Other Websites Utilities
 - Drupal, Joomla, forums
 - PHPMyAdmin



Shared Hosting

- Shared hosting? Shared security!
- Pengguna lain pada server yang sama dengan Kita bias menjadi perusak keamanan yang mengganggu Kita.
- Bagaimana dengan User-user Kita? Bisa kita percaya semua user yang memiliki akses login ke web kita? Benar-benar percaya?
- “Tidak ada yang peduli tentang kelangsungan hidup bisnis Anda seperti diri Anda sendiri” -- Ron Cain, business owner



Cara Kerja Hackers

- Known exploits in vulnerable software
- Brute-force password hacking
- Network scanners
 - Firesheep
 - Wifi vulnerabilities (WEP/WPA)
- Automated tools
- Rootkits



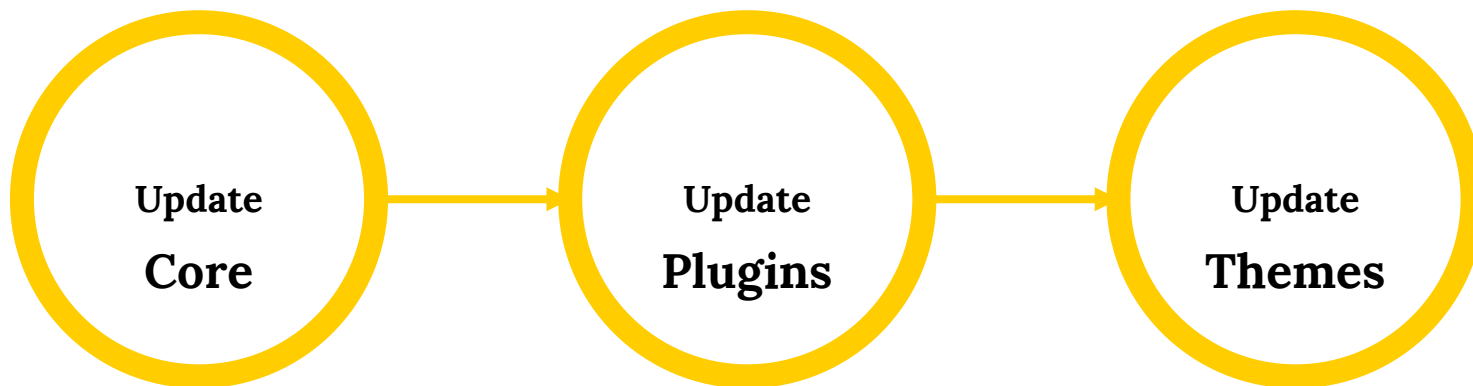
Tetap Aman

Menjaga keamanan adalah kebutuhan yang sering terabaikan.

Apa yang bisa kita lakukan?



Tiga Kata





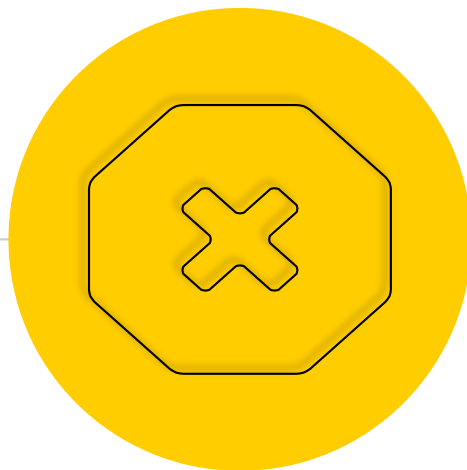
Rekomendasi lainnya?

- Hotfix Plugin
- WP Security Scanner
- Login Lockdown
- BulletProof Security
- Sucuri.net



Rekomendasi lainnya?

- Tidak menggunakan suatu plugin lagi?
- Deactivate
- DELETE!
- Hal yang sama berlaku untuk tema



HACKED!

Terlambat.. Web kita telah dihack
Apa yang kita lakukan?



Bagaimana selanjutnya?

- Anda tidak dapat lagi mempercayai koding apa pun
- Hancurkan situsnya, mulai dari awal, salinan baru
- Simpan wp-config.php dan wp-content/uploads
- Instal ulang data dari backup
- Anda punya backup, bukan?
- Punya kan?



Apa yang perlu di Backup?

- Database
- Uploaded media (wp-content/uploads)
- Custom themes and plugins
- wp-config.php
- Keep a list of your installed third-party plugins



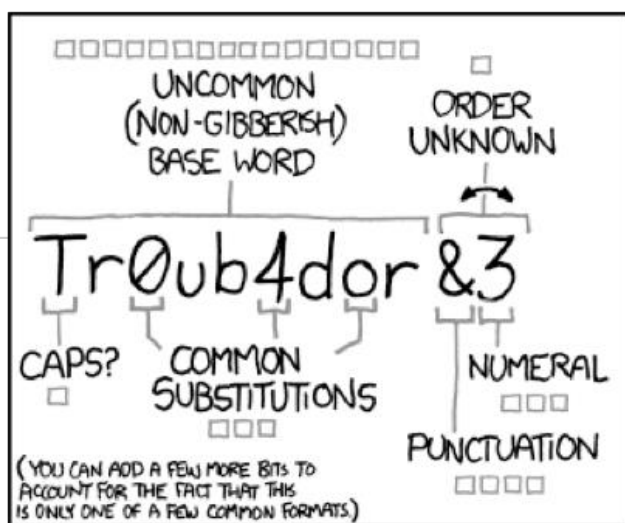
Bagaimana cara membackup?

- Backup Buddy
- VaultPress
- WordPress Backup to Dropbox



Sedikit Anjuran untuk Positif Thinking!

Mari beraman-aman ria!



~28 BITS OF ENTROPY

$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$

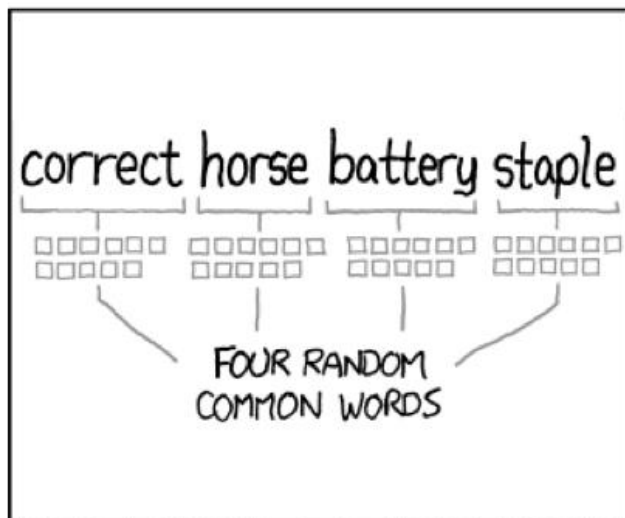
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

DIFFICULTY TO GUESS: **EASY**

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?

AND THERE WAS SOME SYMBOL...

DIFFICULTY TO REMEMBER: **HARD**



~44 BITS OF ENTROPY

$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$

DIFFICULTY TO GUESS: **HARD**

THAT'S A BATTERY STAPLE.

CORRECT!

DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT



Anjuran Keamanan

- Gunakan password yang kuat
- Samarkan link alamat login
- Limit siapa saja bisa login dan beri permisi sesuai kebutuhan
- Gunakan protokol yang aman : SSH, SFTP dsb.

*Apa? Saya tidak tahu bagaimana
cara semuanya?*

“



Dapatkan Bantuan

- ⦿ Keamanan = Asuransi
- ⦿ Bertanya kepada yang berpengalaman
- ⦿ Hosting terpercaya = Bukti dengan lihat client dan history



Terima Kasih!

Mari kita amankan web kita!

Anda dapat menghubungi saya :

- 0821 53 278 782
- havid.aide@gmail.com