



Ir. Budi Rahardjo, M. Sc., Ph.D

Teknik Komputer – STEI ITB

Keamanan Informasi

Keamanan Sistem World Wide Web

II3230 - Keamanan Informasi



Sejarah World Wide Web

- Dikembangkan oleh **Tim Berners-Lee** ketika sedang berada di CERN
- Kemudahan untuk mengakses informasi melalui sistem *hypertext*
- Mengembangkan standar HTML & protokol HTTP

Referensi: Tim Berners-Lee, "Weaving the Web"



Sejarah WWW (lanjutan)



- Awalnya dikembangkan di lingkungan sistem operasi **NeXTStep** (NeXT)
- Kemudian aplikasi **Mosaic** (Windows, Mac, Unix, multiplatform) dikembangkan di **NCSA** oleh mahasiswa kerja praktek (Marc Andreessen dkk.)
 - NCSA httpd (web server), kemudian Apache
- Dan ... akhirnya aplikasi **Netscape**. Kemudian meledak



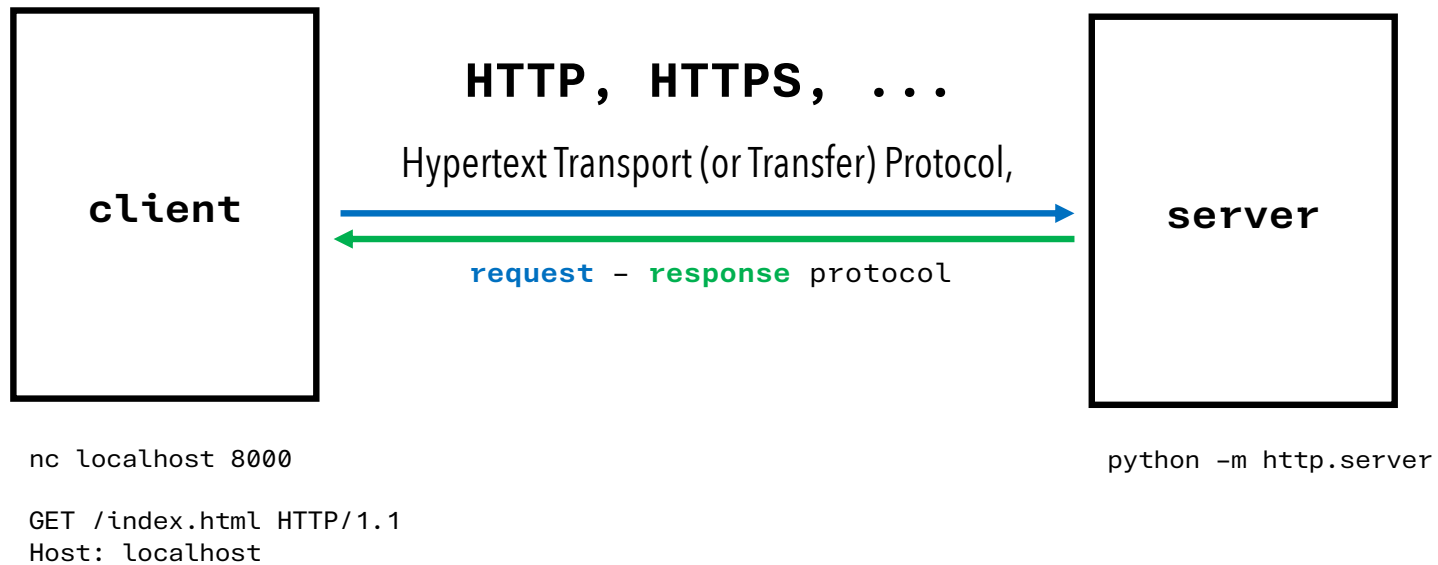
Peta Perjalanan WWW

- Memungkinkan untuk mengimplementasikan sistem secara **tersentralisasi**
 - Aplikasi di sisi server. Pembaharuan aplikasi dapat dilakukan di server saja, tanpa perlu mengubah sisi *client*. Memudahkan manajemen software/aplikasi
 - *Client* (pengguna) hanya membutuhkan web browser (yang ada di semua komputer): konsep ***thin client***
 - Browser dapat ditambah dengan “*plugin*” (extension) untuk menambahkan fitur (animasi, streaming audio & video)
 - **Java** dan **Javascript** memungkinkan menjalankan program di dalam web browser

Arsitektur Sistem WWW

- Server
 - Apache, IIS, nginx, Tomcat, Flask Python, ...
- Client
 - Firefox, Chrome, IE/Edge, Safari, Opera, Vivaldi, Brave, Galeon, kfm, lynx, links, K-meleon, wget, curl, ...
- Terhubung melalui jaringan
 - Protokol: HTTP, HTTPS, (ftp)

Arsitektur WWW



```
nc localhost 8000
```

```
GET /index.html HTTP/1.1
Host: localhost
```

```
...
```

```
python -m http.server
```

Asumsi [Sisi Pengguna / Client]

- Server dimiliki dan dikendalikan oleh organisasi yang mengaku memiliki server tersebut
 - Misal www.itb.ac.id dimiliki oleh ITB
- Dokumen yang disediakan / ditampilkan bebas dari virus (malware, malicious software) atau itikad jahat lainnya
- Server tidak mencatat atau menggunakan informasi tentang pengguna secara tidak semestinya (masalah privasi)
- Asumsi ini yang akan dilanggar dalam penyerangan

Asumsi Sisi Server

- Pengguna beritikad baik, tidak beritikad merusak server atau mengubah isinya
- Identitas pengguna benar
- Pengguna hanya mengakses dokumen yang diperkenankan diakses
 - Tidak melakukan *directory traversal* (naik ke direktori di atasnya)



Asumsi Kedua Pihak

- Jaringan dan komputer bebas dari penyadapan pihak ketiga
- Informasi yang disampaikan dari server ke pengguna (dan sebaliknya) terjamin keutuhannya dan tidak dimodifikasi oleh pihak ketiga
- Jaringan bebas dari serangan DoS
- Masalah keamanan jaringan dibahas dalam network security, bukan web security



Keamanan Server Web

- Server WWW (httpd) menyediakan informasi (statis dan dinamis)
- Halaman statis diperoleh dengan perintah GET
- Halaman dinamis diperoleh dengan
 - CGI (Common Gateway Interface)
 - Server Side Include (SSI)
 - Active Server Page (ASP), PHP
 - Servlet (seperti Java Servlet)



Serangan Terhadap Server - Confidentiality

- Account take over (weak password)
 - Setelah akun diperoleh, meningkatkan akses (eskalasi ke admin)
 - Data di server diambil (download) dan disebarkan ke tempat lain (*exfiltration*)
 - Tampilan web diubah (deface). Situs yang dideface dikoleksi di <http://www.alldas.org>, <http://www.zone-h.org>
- Menyisipkan malware (trojan)
 - Melalui aplikasi / OS yang rentan
 - Server dapat diakses dari remote (Remote Code Execution)
 - Melakukan hal-hal di atas
- Melakukan injeksi (SQL injection, XSS)
 - Mengakses (mengambil data) database
- Server web digunakan untuk tunneling ke luar

Serangan Terhadap Server - Integrity

- Menyisipkan ransomware
 - Mengambil data dan *exfiltration*
 - Mengubah berkas dengan menambahkan password, meminta tebusan
- Melakukan *injection*
 - Mengubah isi database (mengubah transaksi)
 - Terkait dengan application security

Serangan Terhadap Server - Availability

- Melakukan request secara bertubi-tubi
 - Menghabiskan resources server (slowloris attack)
 - Melakukan request ke database yang menghabiskan resources

Serangan terhadap Jaringan

- (C) Menyadap akses web
 - URLsnarf: melihat URL yang diakses. Masalah privasi
 - Menyadap data apabila tidak diproteksi dengan SSL/TLS
- (I) Melakukan Man in the middle (MiTM) attack
 - Mengubah data di tengah jalan
- (A) Melakukan request bertubi-tubi (DoS attack)
 - Menghabiskan jaringan
 - Menghabiskan session
- Pengamanan dengan WAF (Web Application Firewall)

Membatasi Akses

■ Access Control

- Hanya IP tertentu yang dapat mengakses server (konfigurasi web server atau firewall)
- Via userid & password (htaccess)
- Menggunakan token
- Menggunakan enkripsi untuk menyandikan data-data

htaccess di Apache

- Isi berkas “.htaccess”

```
AuthUserFile /home/budi/.passme
```

```
AuthGroupFile /dev/null
```

```
AuthName "Khusus untuk Tamu Budi"
```

```
AuthType Basic
```

```
<Limit GET>
```

```
    require user tamu
```

```
</Limit>
```

- Membatasi akses ke user “tamu” dan password
- Menggunakan perintah “htpasswd” untuk membuat password yang disimpan di “.passme”

Secure Socket Layer (SSL)

- Menggunakan enkripsi untuk mengamankan transmisi data
- Mulanya dikembangkan oleh Netscape
- Implementasi gratis pun tersedia
 - openSSL
- Beberapa masalah dengan SSL
 - ASN.1 compiler yang bermasalah menimbulkan masalah di beberapa implementasi SSL (sehingga server down)
 - Heartbleed, kebocoran data via SSL

Bank Mandiri - Internet Banking - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address https://it.bankmandiri.co.id/retail/Login.do?action=form&lang=in_ID Go Links

Google Search Web 295 blocked AutoFill e Options

BANK MANDIRI

HOME | SITE MAP | CONTACT US

internet banking MANDIRI

LOGIN

Masukkan USER ID Anda :

Masukkan PIN Internet Banking Anda :

BATAL KIRIM

Catatan:

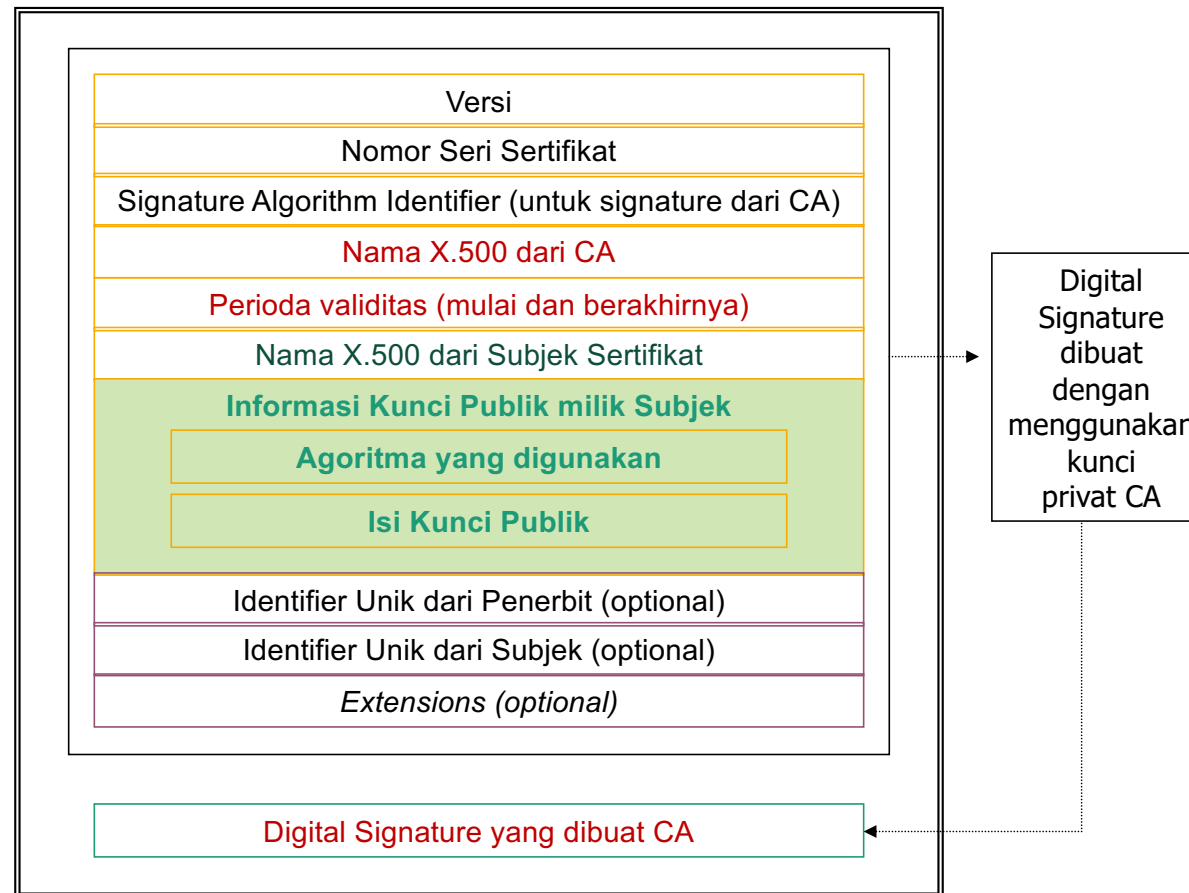
1. Isilah kolom 'Masukan USER ID Anda' dengan USER ID yang telah Anda buat (merupakan kombinasi huruf dan angka sebanyak 6-10 karakter).
2. Isilah kolom 'Masukan PIN INTERNET BANKING Anda' dengan nomor sandi rahasia yang telah Anda buat (hanya berupa angka, sebanyak 6 karakter).
3. Tekan tombol **"KIRIM"** untuk melanjutkan atau tombol **"BATAL"** untuk melakukan pembatalan.

Catatan:

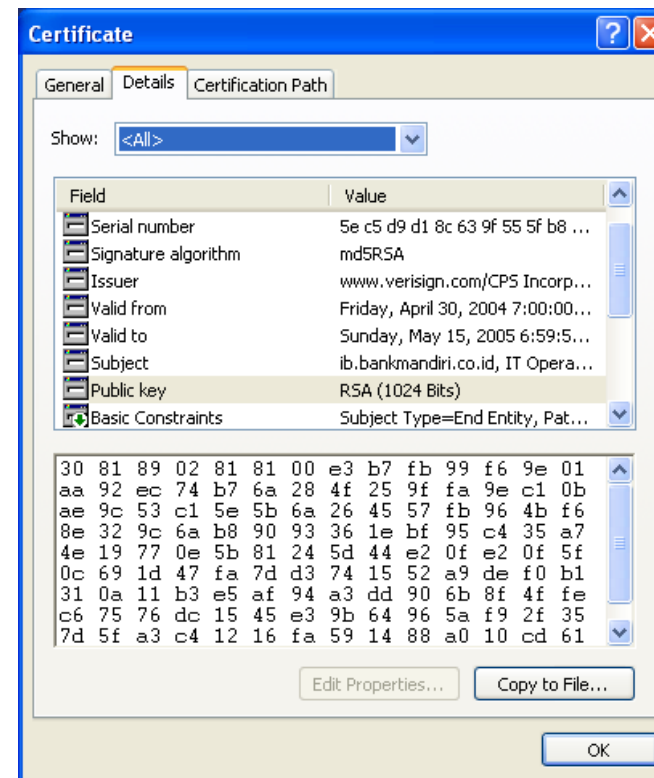
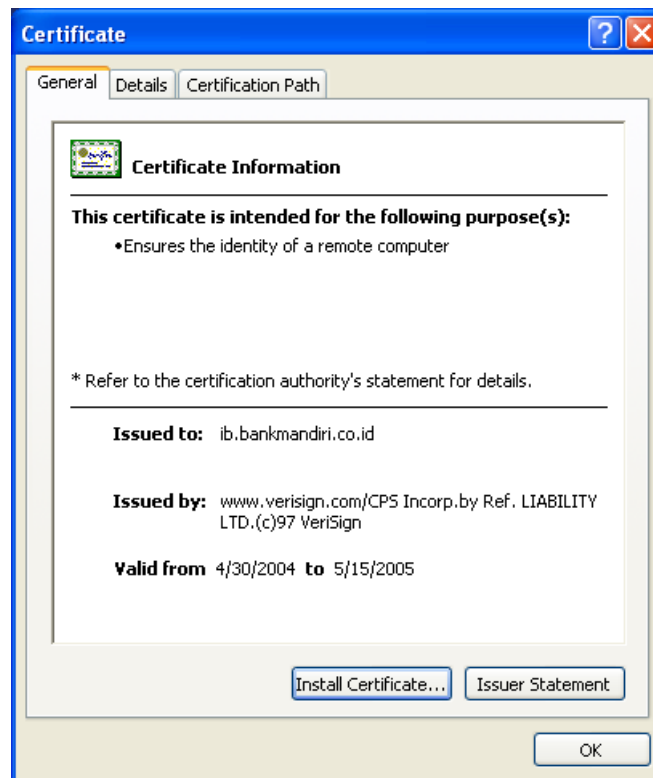
1. Untuk LOGIN kedalam layanan INTERNET BANKING MANDIRI Anda akan selalu diminta untuk memasukkan USER ID dan PIN INTERNET BANKING sebagai proses verifikasi.
2. USER ID dan PIN INTERNET BANKING merupakan sandi rahasia yang diberikan kepada Nasabah sebagai kewenangan penggunaan INTERNET BANKING MANDIRI.
3. Jagalah selalu USER ID dan PIN INTERNET BANKING untuk menghindari penyalahgunaan oleh orang lain yang tidak berhak.
4. Apabila Anda mendapatkan masalah dengan INTERNET BANKING MANDIRI Anda, silahkan hubungi CallMandiri di (021) 5299-7777

Done Internet

Sertifikat X.509 versi 3



Contoh Sertifikat



VeriSign Secure Site - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Google Search Web 295 blocked AutoFill Options

IB.BANKMANDIRI.CO.ID is a VeriSign Secure Site

Security remains the primary concern of on-line consumers. The VeriSign Secure Site Program allows you to learn more about web sites you visit before you submit any confidential information. Please verify that the information below is consistent with the site you are visiting.

Name	IB.BANKMANDIRI.CO.ID
Status	Valid
Validity Period	30-APR-04 - 14-MAY-05
Server ID Information	Country = ID State = DKI Locality = Jakarta Organization = PT Bank Mandiri (PERSERO) Organizational Unit = IT Operation Common Name = ib.bankmandiri.co.id

If the information is correct, you may submit sensitive data (e.g., credit card numbers) to this site with the assurance that:

- This site has a VeriSign Secure Server ID.
- VeriSign has verified the organizational name and that PT BANK MANDIRI (PERSERO) has the proof of right to use it.
- This site legitimately runs under the auspices of PT BANK MANDIRI (PERSERO).
- All information sent to this site, if in an SSL session, is encrypted, protecting against disclosure to third parties.

To ensure that this is a legitimate VeriSign Secure Site, make sure that:

1. The original URL of the site you are visiting comes from IB.BANKMANDIRI.CO.ID.
2. The URL of this page is <https://digitalid.verisign.com>.
3. The status of the Server ID is Valid.

HOME | SITE MAP | CONTACT US

LOGIN

HELP

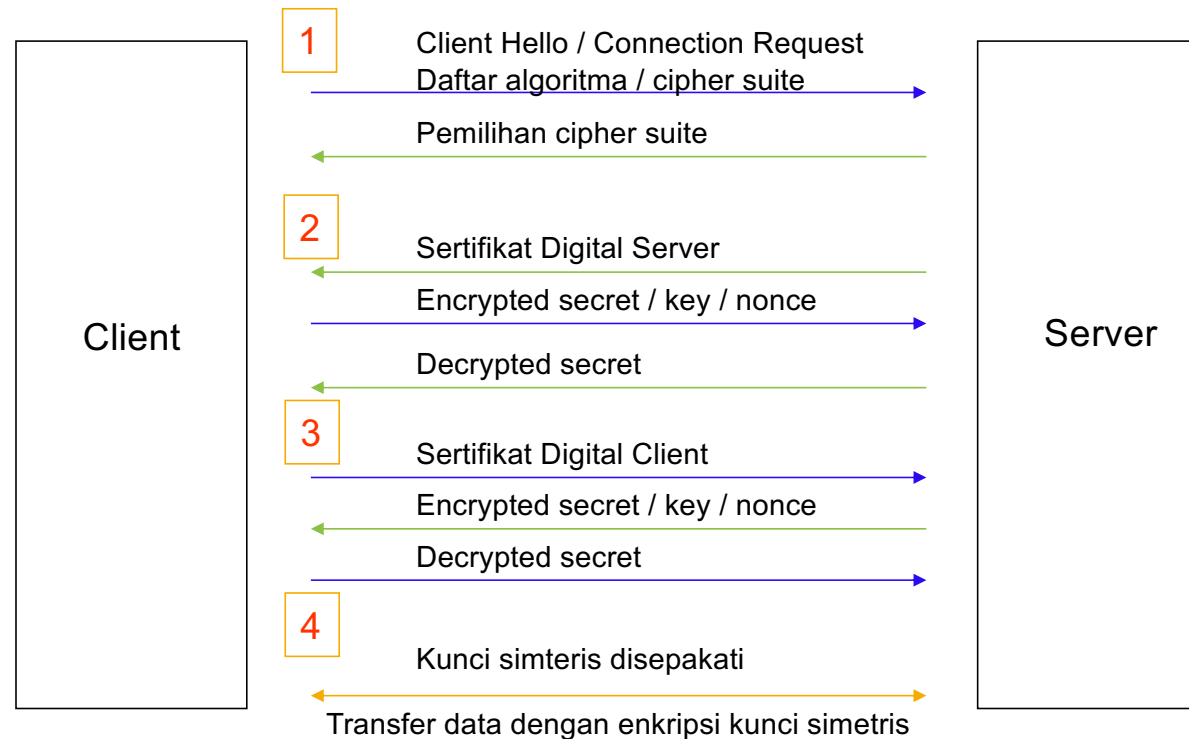
VeriSign Secure Site
Click to verify

KIRIM

an INTERNET BANKING MANDIRI Anda akan selalu diminta dan PIN INTERNET BANKING sebagai proses verifikasi. T BANKING merupakan sandi rahasia yang diberikan kepada n penggunaan INTERNET BANKING MANDIRI. PIN INTERNET BANKING untuk menghindari ain yang tidak berhak. masalah dengan INTERNET BANKING MANDIRI Anda, di (021) 5299-7777

Done Internet Internet

Protokol SSL





Cari info server

- Informasi tentang server digunakan sebagai bagian dari casing the joint
- Dapat dilakukan dengan
 - Memberikan perintah HTTP langsung via telnet
 - Menggunakan program netcat
- Ubah konfigurasi agar server tidak memberikan informasi terlalu banyak





Keamanan CGI

- Pada mulanya CGI digunakan sebagai *interface* www dengan sistem informasi lainnya (gopher, WAIS, ftp)
- Diimplementasikan dengan berbagai bahasa (perl, C, C++, python, sh)
- Skrip CGI dijalankan di server (oleh siapa saja dari jaringan) sehingga membuka potensi lubang keamanan jika skrip tidak dibuat dengan baik
 - Membocorkan informasi
 - Menggunakan resources (misal CPU) yang terlalu banyak di server sehingga server menjadi lambat





Lubang Keamanan CGI

- Beberapa contoh serangan
 - CGI dipasang oleh orang yang tidak berhak
 - CGI dijalankan berulang-ulang untuk menghabiskan resources (CPU, disk): DoS
 - Masalah *setuid* CGI di sistem UNIX, dimana CGI dijalankan oleh userid web server (atau bahkan root) sehingga ketika dijalankan maka dia memiliki rights sama dengan userid tersebut
 - Penyisipan karakter khusus untuk shell expansion
 - CGI yang lemah sehingga dapat mengambil berkas yang seharusnya tidak berhak atau mengeksekusi perintah yang seharusnya tidak dilakukan (misal: `wget trojanhorse`, eksekusi `trojanhorse`). Contoh kelemahan *awstats*
 - Guestbook abuse dengan informasi sampah (link ke pornografi atau sekedar info yang berulang dan bahkan skrip yang dijalankan di komputer pengguna)





Web & SQL

- Banyak aplikasi (transaksi) menggunakan basis web untuk mengakses database. Ini akan dibahas terpisah pada **application security**
- Umumnya database diakses melalui SQL
- Sayangnya seringkali implementasi teledor sehingga memungkinkan serangan (SQL injection attack)
 - Memasukkan perintah-perintah SQL yang nakal dengan akibat yang berbeda (server down, database berubah)
 - **; drop table**, tanda petik ' , UNION/OR
 - Tidak terdeteksi oleh firewall atau IDS karena pada level aplikasi. Mulai ada WAF (Web Application Firewall)
- Tools: Sqlmap



Keamanan Client WWW

- Berhubungan dengan masalah privacy
 - Cookies untuk tracking kemana saja browsing
 - Pencurian informasi pribadi
- Attack (via active script, javascript, java)
 - Pengiriman data komputer (program apa yang terpasang) ke luar
 - DoS attack (buka windows banyak)
 - Penyusupan virus, trojan horse, ransomware
 - Kasus: security hole di JPEG bisa mengeksekusi aplikasi di sisi client, security di MIDI player, yang pada intinya adalah mencari hal-hal yang dapat dieksekusi langsung di sisi client



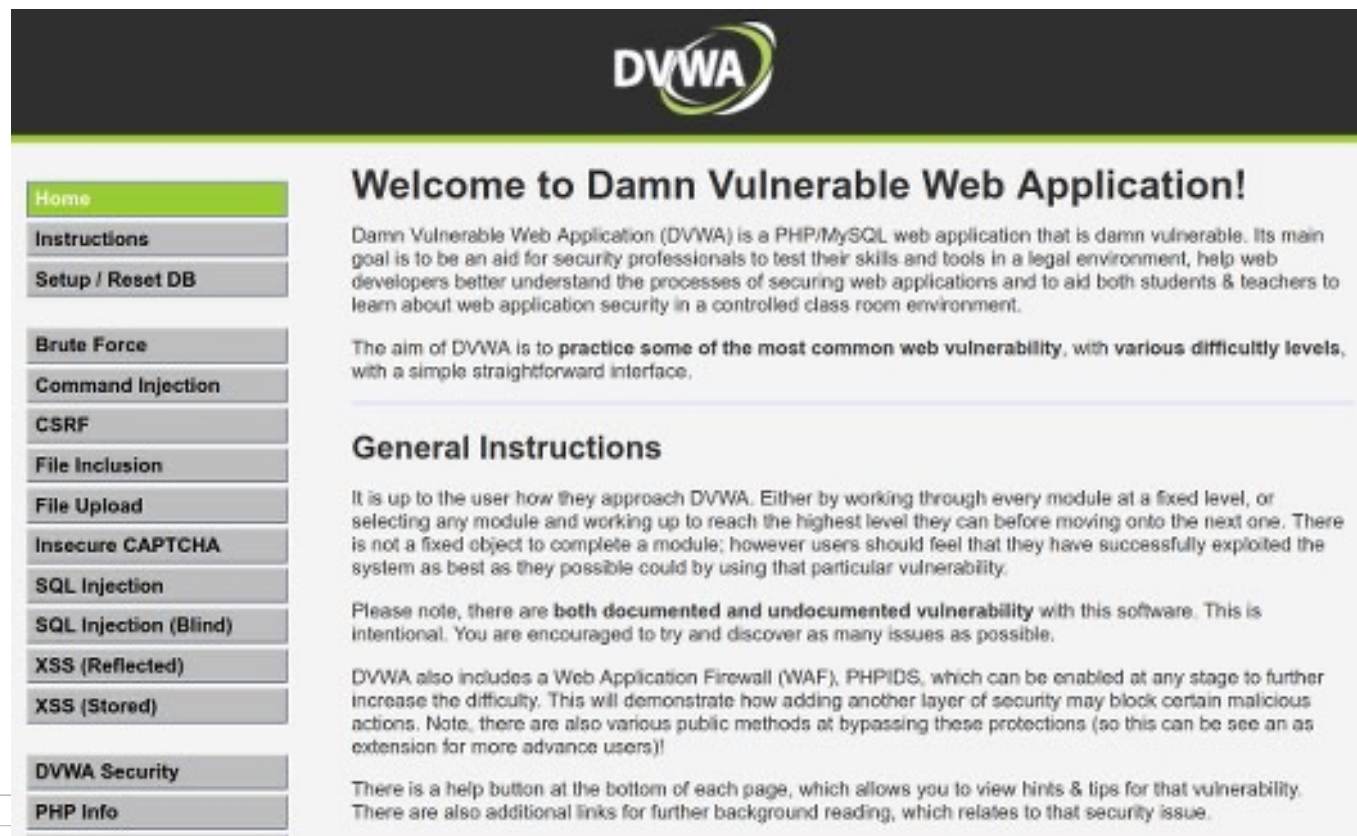
OWASP

- Open Web Application Security Project
- Top 10 web application security risks
 - <https://owasp.org/www-project-top-ten/>



* From the Survey

DVWA



The screenshot shows the DVWA homepage. At the top is a dark header with the DVWA logo. Below the header is a sidebar on the left with a green 'Home' button and several other buttons: 'Instructions', 'Setup / Reset DB', 'Brute Force', 'Command Injection', 'CSRF', 'File Inclusion', 'File Upload', 'Insecure CAPTCHA', 'SQL Injection', 'SQL Injection (Blind)', 'XSS (Reflected)', 'XSS (Stored)', 'DVWA Security', and 'PHP Info'. The main content area has a heading 'Welcome to Damn Vulnerable Web Application!' followed by a paragraph describing DVWA as a PHP/MySQL web application for testing security skills. Below this is another heading 'General Instructions' followed by two paragraphs explaining the application's purpose and usage, including a note about the included Web Application Firewall (WAF) and PHPIDS.

Welcome to Damn Vulnerable Web Application!

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.

The aim of DVWA is to **practice some of the most common web vulnerability**, with **various difficulty levels**, with a simple straightforward interface.

General Instructions

It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.

Please note, there are **both documented and undocumented vulnerability** with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

DVWA also includes a Web Application Firewall (WAF), PHPIDS, which can be enabled at any stage to further increase the difficulty. This will demonstrate how adding another layer of security may block certain malicious actions. Note, there are also various public methods at bypassing these protections (so this can be seen as an extension for more advance users!)

There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.





Penutup

- WWW merupakan salah satu aplikasi utama Internet (dan Intranet). Aplikasi berbasis web yang mendominasi internet
- Meskipun memiliki banyak manfaat, sistem berbasis web masih banyak memiliki lubang keamanan – baik di sisi server maupun di sisi client
- Banyak tools untuk melakukan otomatisasi proses pengujian aplikasi berbasis web

