99 Hal Penting Webiste Anda Aman Dari Serangan, Checklist...!!!
Selasa, 7 Juli 2015 | 23:05:43 WIB | **Endang Kurniawan**

Sebagai programmer ada beberapa hal yang harus diperhatikan untuk mengamankan hasil pekerjaan yang sangat "menguras" pikiran dari tangan-tangan iseng ataupun orang-orang yang memang tidak menginginkan anda "terkenal" di dunia maya. Salah satu faktor penting yang harus diperhatikan namun kadang diabaikan yaitu masalah *security* atau keamanan.

Di dalam tulisan ini, penulis memberikan beberapa tips yang dapat menambah wawasan baru bagi para pengnjung setia website ini. Karena penulis beranggapan memang tidak mudah untuk membuat aplikasi website yang bebas celah dan bebas serangan peretas, karena seperti yang kita ketahui bersama bahwa “tidak ada sistem yang sempurna”.

Meskipun begitu, bukan berarti masalah keamanan bisa diabaikan, setidaknya sang programmer bisa meminimalisir hal-hal yang bisa membahayakan apa yang telah dibuatnya.

Berikut ini adalah +99 hal yang setidaknya harus dilakukan oleh seorang programmer untuk membuat aplikasi yang *secure*, meskipun ini tidak membuat 100% aman.

BASIC
Berikut ini adalah hal-hal dasar seputar keamanan yang harus diperhatikan ketika membuat web / aplikasi dengan PHP

- Strong passwords are used.
- Passwords stored safely.
- register_globals is disabled.
- Magic_quotes is disabled.
- display_errors is disabled.
- Server(s) are physically secured.

INPUT
Ketika website atau aplikasi yang dibuat melibatkan form untuk menginput data, maka harus memperhatikan hal-hal berikut ini agar segala sesuatunya aman.

- Input form $_GET, $_POST, $_COOKIE and $_REQUEST is considerend tainted.
- Understood that only some values in $_SERVER and $_ENV are untainted.
- $_SERVER[PHP_SELF] is used where used.
- Input data is validated.
- o (null) is discardedin input.
- Length of input is bounded.
- Email addresses are validated.
- Application is aware of small, very large, zor and negative numbers. Sci. notation too.
- Application checks for invisible, look-alike, and combining characters.
- Unicode control characters stripped out when required.
- Output data is sanitized.
- User-inputted HTML is sanitized with HTMLPurifier.
- User-inputted CSS is sanitized using a white-list.
    - Abusable properties (margin, position, etc.) are handled.
    - CSS escape sequences are handled.
      Javascript in CSS is discarded (expressions, behaviors, bindings.)

- URLs are sanitized and unknown and unwanted protocols are disallowed.
- Embedded plugin files (Flash Movies) are embedded in a manner so that only the intended plugin is loaded.
- The application uses a safe encoding.

FILE UPLOAD

Ketika website yang dibuat dengan PHP melibatkan gambar atau file yang akan di input, maka agar aman perlu diperhatikan hal-hal berikut.

- Application verifies file type.
  - User provided mime type value is ignored.
  - Application analyzes the content of files to determinie their type.
  - It is understood that a perfectly valid file can still contain arbritrary data.
- Application checks the file size of uploaded files.
  - MAX_FILE_SIZE is not depended upon.
  - File uploads cannot "overtake" avaible space.
- Content is checked for malicious content.
  - Application uses a malware scanner (if req.).
  - Uploaded HTML files are displayed securely.
- Uploaded files are not moved to a web-accessisble directory.
- Extensive path checks are used when serving files.
- Uploaded files are not served with include().
- Uploaded files are served as an attachment using the Content-Disposition header.
- Application sends the X-Content-Type-Options: nosniff header.
- Files are not not served as: (Unless necessary)
  - "application/octet-stream"
  - "application/unknown"
  - "plain/text"

DATABASE

Database merupakan sasaran utama para peretas, karena pada bagian inilah informasi penting tersimpan, untuk itu ketika website melibatkan database, perhatikan hal berikut.

- Data inserted into the database is properly escaped or parameter/prepared statements are used.
  - addslashes() is not used.
- Application does not have more privileges to the database then necessary.
- Remote connections are disabled if they are unnecessary.

SERVING FILES

Ketika website melayani servis file, maka perhatikan hal-hal berikut agar website aman dari orang yang tidak berhak mengakses.

- User input is not directly used in a pathname.
  - Directory traversal is prevented.
  - Null (o) in paths are filtered.
  - Application is aware of ":"
  - PHP streams are filtered.
- Access to files is not restricted by hiding the files.
- Remote files not included with include().

AUTHENTICATION

- Ketika aplikasi atau web membutuhkan halaman yang hanya boleh diakses oleh orang tertentu yang bisa dipercaya, maka perlu proses authentication yang ketat, berikut poin-poin nya.
- Bad password throttling.
    - CAPTCHA is used.
- SSL used to prevent MITM.
- Passwords are not stored in a cookie.
- Passwords are hashed.
    - Per-user salts are used.
    - bcrypt() is used with sufficient number of rounds.
    - MD5 is not used.
- Users are warned about obvious password recovery questions.
- Account recovery forms do not reveal email existence.
- Pages that send emails are throttled.

SESSIONS

Session biasanya digunakan untuk mengatur apakah seseorang boleh untuk mengakses halaman tertentu atau tidak, session juga di gunakan untuk menyimpan data-data penting yang diperlukan oleh website, jadi perlu diamankan dengan memperhatikan hal berikut.

- Sessions only use cookies. (session.use_use_only_cookies).
- On logout session data is destroyed.
- Session is recreated on authorization level change.
- Sites on the same server use different session storage dirs.

3th-party

Bantuan pihak ketiga yang perlu juga untuk diperhatikan oleh programmer PHP adalah berikut ini.

- CSRF issues are prevented with tokens/keys.
    - Referrers are not relied upon.
    - Pages that perform action use POST.
    - Important Pages (logout, etc.) are protected.
- Your pages are not written in a way (i.e. JSON, JS-like) where they can be included and read on a remote website successfully.
- Aware that Flash can bypass referrer checks to load images and sound files.
- The following things will not reveal significant information if included remotely:
    - Images.
    - Pages that take a longer time to load.
    - CSS files.
    - Existence or ordening of frames.
    - Existence of a JS variable.
    - Detected visit of a URL.
- Inclusion of your website in an inline frame with JS disabled does not reveal a threat.
- Application uses frame bursting code and sends the X-Frame-Options header.

MISCELLANEOUS

Hal-hal umum lain yang perlu untuk diperhatikan terkait pembuatan website dan aplikasi berbasis PHP.

- A crypthographically secure PRNG is used for secret randomly-generated IDs (activation links, secret IDs? etc.).
    - Suhosin is installed or you are not using rand() for this.
- Anything that consumes a lot of resources should be throttled and limited.
    - Pages that use 3th-party APIs are throttled.
- You did not create your own encryption algorithm.
- Arguments to external programs (i.e. exec()) are validated.
- Generic intrnal and external redirect pages are secured.
- Precautions taken against the source code of you PHP pages being shown due to misconfiguration.
- Configuration and critical files are not in a web-accessible directory.

SHARE HOSTING

Ketika website yang dibuat dengan PHP di taruh di shared hosting, maka ada hal-hal yang perlu diperhatikan agar website bisa aman. Shared hosting berarti website ditaruh di server yang sama dengan website-website lain yang jumlah nya sangat banyak, website lain kena serangan, maka website kita bisa kena juga.

- Using a secure shared host where users connot access the files of other users.
- Aware that fellow shared hoting users:
    - Can, if on the same IP address, issue requests against your site with XMLHttpRequest in IE6.
    - Can access your website form 127.0.0.1 or ::1.
    - Can host a server on the same IP address.
    - Are not "remote" as far as your DB is concerned.
    - Session & file upload directories are not shared.

Dengan adanya checklist diatas, sekiranya ada beberapa hal yang perlu diperhatikan agar kerusakan website dapat diminimalisir dan menghindari orang-orang yang tidak bertanggungjawab. Untuk mendapatkan checklist diatas, bisa mengunduhnya disini. Semoga bermanfaat, terima kasih. (-dari berbagai sumber-).

All is about imagination - Endang Kurniawan
Sumber : https://endangkurniawan.com/article-99-hal-penting-webiste-anda-aman-dari-serangan-checklist.html