Tutorial ICT

Bersama FIRKHAN
sembangict@yahoo.com

Ancaman serangan siber

APLIKASI web memerlukan beberapa saluran atau *port* yang terdapat pada prasarana rangkaian sesebuah organisasi dibuka. Perkara ini penting bagi membolehkan berlaku interaksi antara pengguna dan aplikasi web tersebut menerusi rangkaian Internet.

Namun begitu, perkara ini juga boleh mengundang ancaman serangan siber terhadap organisasi tersebut.

Berikut adalah beberapa kelompangan keselamatan siber berkait dengan aplikasi web yang perlu diberi perhatian oleh setiap organisasi.

1 Kelemahan suntikan SQL atau *SQL injection flaws*. Menurut kajian pakar, serangan suntikan SQL masih diterajui sebagai jenis serangan web paling menonjol dalam jangka masa panjang.

2 Proses *deserialization* adalah satu kaedah iaitu aplikasi mengambil objek yang bersambung dan dikodkan ke dalam format yang disimpan atau dihantar dengan mudah. Seterusnya diubah semula menjadi objek "hidup" atau aplikasi. Proses *deserialization* yang dilakukan dengan cara tidak selamat boleh menngundang ancaman keselamatan siber kepada organisasi.

3 Kebergantungan kepada risiko penggunaan komponen sumber terbuka organisasi atau *open source*. Kebanyakan pembangunan aplikasi web menggunakan perisian sumber terbuka yang boleh terdedah kepada kelemahan yang ditanam oleh pihak lain yang memahami kod atur caranya.

4 Tiada dasar keselamatan kandungan untuk mencegah serangan XSS (*Cross Site Scripting*). Dasar atau polisi ini bersifat teknikal yang mengawal keberadaan komponen atau kod sesuatu aplikasi web.

5 Kebocoran maklumat berguna yang boleh dimanipulasi oleh penceroboh menerusinya untuk membuat serangan siber. Maklumat seperti jenis sistem pengoperasian, jenis pelayan web, versi perisian, kata nama dan aspek-aspek lain perlu dilindungi keselamatan sewajarnya.

6 Kelemahan perlindungan keselamatan kental bagi API (*Application Programming Interface*). API telah menjadi lebih popular pada tahun-tahun kebelakangan ini, dengan pembangun aplikasi menggunakannya lebih kerap apabila membina aplikasi bagi membuatkan perkhidmatan atau data mereka tersedia untuk dijual kepada aplikasi lain.

7 Pengabaian pelindungan lapisan pengangkutan (*transport layer*) dalam perlaksanaan sambungan ke rangkaian atau Internet. Penggunaan protokol HTTPS dalam capaian mana-mana laman web bagi mengelak daripada masalah ini berlaku.

Boleh menggunakan protokol HSTS (*HTTP Strict Transport Security*) bagi laman web yang masih menggunakan protokol.