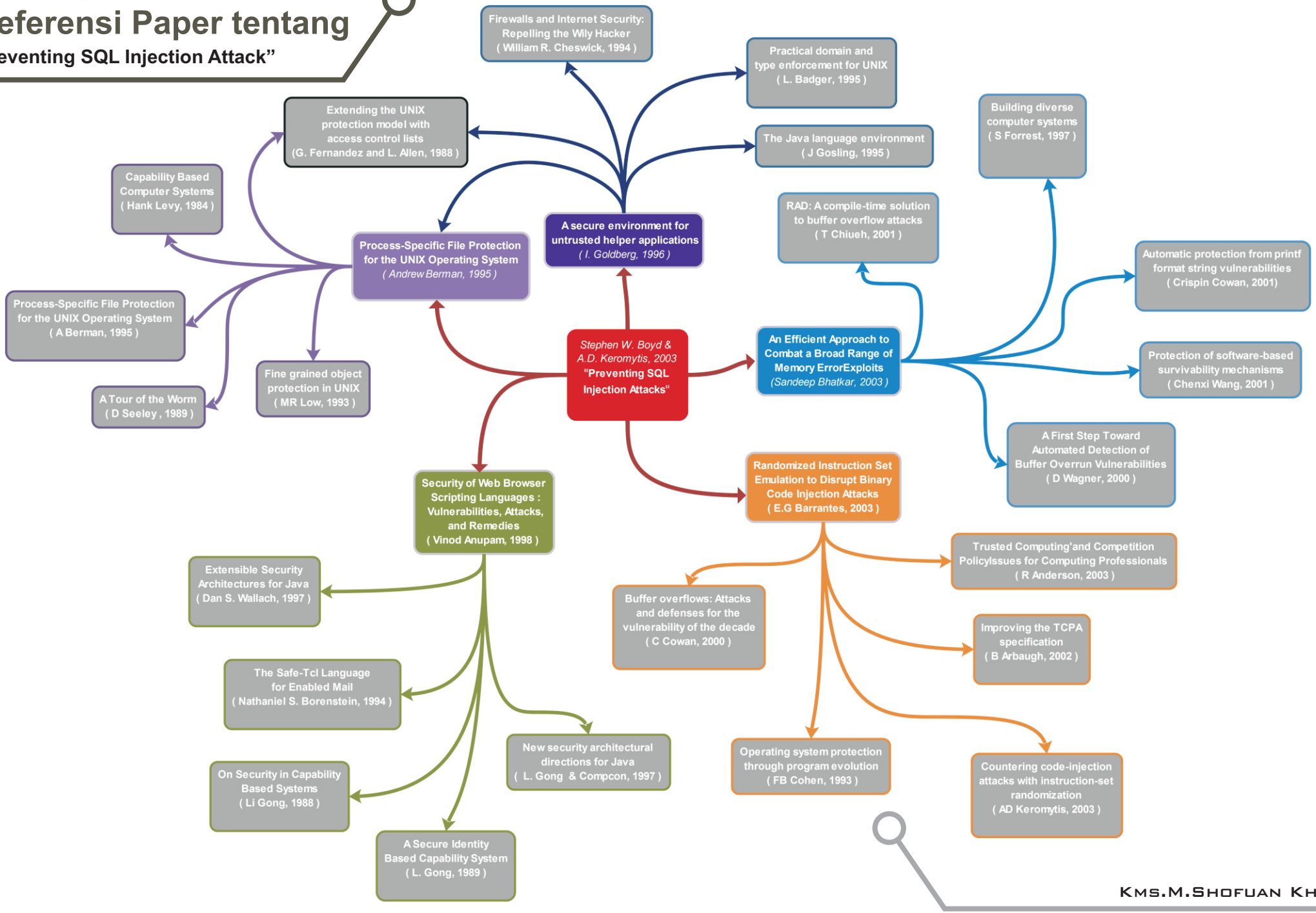
Sitemap :
Referensi Paper tentang
"Preventing SQL Injection Attack"



KMS.M.SHOFUAN KHOIRI

09011181520018

A. Penjelasan isi Sitemap dan jurnal "Preventing SQL Injection Attacks"

Pada Sitemap diatas menggambarkan berbagai jurnal yang telah dijadikan referensi oleh Steven W. Boyd dan Angelos D. Keromytis dalam penulisan jurnal mereka yang berjudul "Preventing SQL Injection Attacks".

Dalam jurnal ini membahas tentang beragam metode yg telah dikembangkan dan di uji untuk mencegah dan mendeteksi serangan system tipe SQL yg saat ini sudah marak terjadi, sasaran utama SQL yaitu website database yg bersifat vulnurable (rentan / rapuh) dimana website tersebut dimafaatkan untuk mencuri sejumlah informasi user seperti pada serangan database yang diperoleh melalui antarmuka web, lalu sipelaku mengambil kesempatan dari kelemahan dalam komponen web tersebut agar dapat mencuri informasi usernya. SQL sering di gunakan untuk tindakan CARDING atau pencurian id kartu kredit. Selain itu, pada jurnal ini juga menjelaskan tentang mekanisme perlindungan yang secara praktis dilakukan terhadap serangan SQL. Untuk itu, jurnal ini mengambil berbagai referensi-referensi pada jurnal sebelumnya.

Berikut merupakan lima dari beberapa jurnal yang telah dijadikan referensi oleh Steven W. Boyd dan Angelos D. Keromytis dalam menulis jurnal tentang pencegahan terhadap serangan SQL ini :

1. A secure environment for untrusted helper applications
(I. Goldberg, 1996)

Dalam jurnal yang ditulis oleh I. Goldberk dan rekan-rekannya ini membahas tentang bagaimana merancang dan mengimplementasikan suatu lingkungan system yang aman digunakan untuk aplikasi pembantu yang tidak terpercaya. Sebab saat ini banyak sekali program – program populer seperti netscape yang menggunakan aplikasi pembantu tersebut. Mereka yakin bahwa aplikasi pembantu tersebut dapat membantu mereka dalam mengolah data dari internet. Namun, banyak dari aplikasi pembantu tersebut dapat mengancam keamaanan system pada suatu program. Dari lingkungan system inilah diharapkan dapat mengurangi pelanggaran keamanan system dengan membatasi akses program tersebut ke sistem operasinya.

Untuk membuat jurnal ini, I. Goldberg dan rekan-rekannya mengambil referensi-

referensi berikut :

a) Process-Specific File Protection for the UNIX Operating System (Andrew Berman, 1995)
b) Firewalls and Internet Security: Repelling the Wily Hacker (William R. Cheswick, 1994)
c) Extending the unix protection model with access control lists, (G. Fernandez and L. Allen, 1988)
d) Practical domain and type enforcement for UNIX (L. Badger, 1995)
e) The Java language environment (J Gosling, 1995)

2. Process-Specific File Protection for the UNIX Operating System (Andrew Berman, 1995)

Pada jurnal yang ditulis oleh Andrew Berman dan rekan-rekannya membahas tentang proses apa saja yang secara spesifik dapat dilakukan dalam pengamanan data khususnya pada sistem operasi UNIX. Sebab pada mekanisme pengamanan data yang disediakan oleh UNIX tidak cukup untuk lingkungan komputasi saat ini. Ketika kita mencoba melakukan pengamanan data pada sitem operasi UNIX dari serangan pengguna lain, hal ini tidak secara langsung diatasi oleh sistem yang menghancurkan serangan dari pengguna lain tersebut. Karena hal itu lah jurnal ini ditulis, dimana dalam jurnal ini mengenalkan kita istilah TRON yaitu suatu tingkat proses yang mengakses sistem kontrol pada sistem operasi UNIX. Dengan menggunakan TRON, program pada UNIX dapat dijalankan tanpa kompilasi ulang sehingga dengan demikian TRON dapat meningkat keamanan pada sistem operasi UNIX.

Untuk membuat jurnal ini, Andrew Berman dan rekan-rekannya mengambil referensi-referensi berikut :

a) Extending the unix protection model with access control lists, (G. Fernandez and L. Allen, 1988)
b) Capability Based Computer Systems (Hank Levy, 1984)
c) A Tour of the Worm (D Seeley , 1989)
d) Fine grained object protection in UNIX (MR Low, 1993)
e) Process-Specific File Protection for the UNIX Operating System (A Berman,

1995)

3. An Efficient Approach to Combat a Broad Range of Memory Error Exploits (Sandeep Bhatkar, 2003)

Dalam jurnal ini membahas cara yang efisien untuk memberantas serangan sistem yang memanfaatkan error pada memory sistem tersebut. Sebab serangan system yang memanfaatkan error pada memory merupakan salah satu hal yang paling serius dalam ancaman keamanan system. Pada serangan ini, membutuhkan sistem penyerang yang digunakan untuk mendapatkan pemahaman secara mendalam tentang rincian internal program korban termasuk lokasi data-data penting si korban. Untuk menghadapi hal tersebut digunakanlah suatu teknik pengacakan program agar si pelaku tersebut sulit untuk memperoleh pemahaman dan informasi yang rinci pada program korban tersebut. Dalam jurnal ini dikembangkanlah study sistematis tentang pengacakan program, ini dimana dalam jurnal ini juga membahas berbagai strategi untuk melakukan pengacakan program pada lokasi data / kode penting serta jarak relatif antar lokasi data tersebut. Dengan menggunakan teknik pengacakan program ini diharapkan dapat mengurangi keberhasilan dari serangan system oleh si pelaku. Selain itu, jika si pelaku berhasil menyerang system pada salah satu korban, maka hal tersebut mungkin tidak akan terjadi pada korban lainnya dan berkemungkinan tidak akan terjadi pada kedua kalinya sebab jika serangan si pelaku itu lolos pada suatu system milik korban, maka hal tersebut dapat dengan mudah mendeteksi upaya pencegahan terhadap serangan tersebut.

Untuk membuat jurnal ini, Sandeep Bhatkar bersama rekan-rekannya mengambil referensi-referensi berikut :

a) RAD: A compile-time solution to buffer overflow attacks (T Chiueh, 2001)
b) Automatic protection from printf format string vulnerabilities(Crispin Cowan, 2001)
c) Building diverse computer systems (S Forrest, 1997)
d) A First Step Towards Automated Detection of Buffer Overrun Vulnerabilities. (D Wagner, 2000)
e) Protection of software-based survivability mechanisms (Chenxi Wang, 2001)

4. Randomized Instruction Set Emulation to Disrupt Binary Code Injection Attacks (E.G Barrantes, 2003)

Pada jurnal ini membahas tentang bagaimana membuat suatu instruksi acak untuk mengatasi serangan dari kode biner asing pada suatu program. Serangan dengan metode kode biner ini merupakan bentuk serangan yang secara umum dilakukan para pelaku untuk menghancurkan suatu program. Kebanyakan pertahanan system saat melawan bentuk serangan ini menggunakan sebuah strategi "Penjagaan semua pintu" dimana sistem keamanan ini mencoba memblokir jalan yang akan dilalui oleh bentuk serangan ini sehingga dalam jjurnal ini juga menjelaskan sebuah metode pelengkap perlindungan program yang juga dapat mengacaukan kinerja serangan dari kode-kode biner asing.

Untuk membuat jurnal ini, E.G. Barrantes bersama rekan-rekannya mengambil referensi-referensi berikut :

a) Trusted Computing'and Competition Policy–Issues for Computing Professionals (R Anderson, 2003)
b) Operating system protection through program evolution (FB Cohen, 1993)
c) Buffer overflows: Attacks and defenses for the vulnerability of the decade (C Cowan, 2000)
d) Countering code-injection attacks with instruction-set randomization (AD Keromytis, 2003)
e) Improving the TCPA specification (B Arbaugh, 2002)

5. Security of Web Browser Scripting Languages: Vulnerabilities, Attacks, and Remedies (Vinod Anupam, 1998)

Dalam jurnal ini membahas tentang bagaimana mencegah kelemahan pada keamanan web agar terhindar dari serangan yang berhasil masuk dalam keamanan data privasi pengguna web tersebut. Untuk menghadapi hal ini digunakanlah langkah-langkah yang merujuk pada kerangka keamanan dalam bahasa scripting web tersebut. Pada jurnal ini menunjukkan bahwa jika dari awal kerangka keamanan telah diintegrasikan ke dalam masing-masing bahasa scripting, berkemungkinan pencegahan

kelemahan pada keamanan data dapat dilakukan.

Untuk membuat jurnal ini Vinod Anupam dan rekan-rekannya mengambil referensi dari jurnal-jurnal berikut :

a) Extensible Security Architectures for Java (Dan S. Wallach, 1997)
b) The Safe-Tcl Language for Enabled Mail (Nathaniel S. Borenstein, 1994)
c) On Security in Capability-Based Systems (Li Gong, 1988)
d) A Secure Identity-Based Capability System (L. Gong, 1989)
e) New security architectural directions for Java (L. Gong & Compcon, 1997)