Infinite Connection

Build secure and reliable online services for MIT alumni
What is Infinite Connection?

A collection of online services provided for MIT Alumni Community (alum.mit.edu)

- 2,000+ web pages
- 70,000+ registered alumni
- 1,200+ mailing lists to join
- 600,000+ searches on Online Alumni Directory annually
Services in Infinite Connection

- OAD (Online Alumni Directory)
- EFL (Email Forwarding for Life)
- SmarTrans (Online Event Registration and Club Dues Payment System)
- Mailing Lists, Online Elections, Job Posting, Online Class Notes
- and many many more …
Online Alumni Directory

SEARCH RESULTS
2571 Records Found

You can start over or refine your search by using the search box or categories on the left. You can also broaden your search by removing refinement filters or search terms in the Filters section below.

Filters

Sort By

Go to Page

1. Abbott, Erik CE '00 [Update Record] [Add ICAN Advisor]
   Advance ID: 2001019320
   Department: CE - Civil Engineering
   Degrees: 2000, MNG - Master of Engg, Course 1P - Civ&Env Eng Mas Eng
   Home Address: Newport Beach CA 92663
   Company: Citini Systems
   Job Title: Senior Sales Engineer
   Work Address: Newport Beach CA 92663

2. Abiyanyar, Hari GM '00 [Update Record] [Add ICAN Advisor]
   Advance ID: 2001020271
   Department: GM - Management
   Degrees: 2000, PhD - Doctor Of Phd, Course 1SD - Management Doctoral

3. Aboumdad, Jouman CE '00 [Update Record] [Add ICAN Advisor]
   Advance ID: 2001017194
   Department: CE - Civil Engineering
   Degrees: 2000, SM - Master Of Science, Course 1M - Civ&Env Eng Sm/Eng
   Home Address: Beirut, Lebanon

4. Abu-Khail, Ramy '00 [Update Record] [Add ICAN Advisor]
   Advance ID: 1996211523
   Degrees: • 2000, SB - Bachelor Of Science, Course 2 - Mechanical Engg

Click on the figures for more information.
Email Forwarding for Life

Life long email address:
johndoe@alum.mit.edu

Up to 5 forwarding email addresses

Spam Filter, Allow List, Deny List

Send email using @alum.mit.edu address from web

Send email using @alum.mit.edu address from outgoing-alum.mit.edu server
Email Forwarding for Life

Incoming email for jdoe@alum.mit.edu

Load Balancer

Database Server

Email Server 1

Email Server 2

Application Server

Web Server

Internet

Update email settings

Alumni User

jdoe@yahoo.com

jdoe@gmail.com

jdoe@msn.com

jdoe@hotmail.com

jdoe@comcast.com

jdoe@alum.mit.edu

Internet
SmarTrans

- Online Event Creation
- Online Event Registration
- Online Club Dues Payment
- 99 Clubs and Groups signed up
- 669 Events in 2005
- $548,221 online transactions in 2005
Security Matters

- March 2005 BC (120,000 alumni)
- March 2005 UC Berkeley (98,000 students)
- April 2005 Tufts (106,000 alumni)
- June 2006 UConn (72,000 students/faculty)
- April 2006 UTexas (197,000 records)
- May 2006 VA (26.5 million veterans)
Design with Security in mind

- **Database Design:** Decouple advance and web database
- **Access Policy:** 37 different roles map to different access privileges
- **Password Policy:** at least 6 characters long, alphanumerics

Diagram:

- **Advance Database**
- **Replication**
- **Web Database**
- **Application Server**
Security Review

We hired Symantec to perform a security review of our web application in 2005.

Some of the findings:

- Weak Password: mit123, abc123, password1
- SQL Injection
- Input Validation: Cross Site Scripting (XSS)
- Verbose Error Message
SQL Injection Case

```java
PreparedStatement stmt = conn.prepareStatement("select * from user_table where username = ' ' + 
uname + ' ' and password = ' ' + pword + ' ' ');
ResultSet rs = stmt.executeQuery();

* uname = "johndoe'; -- "
```
Security Review

**SQL Injection Defense: Bind Variables**

```java
PreparedStatement stmt = conn.prepareStatement(
    "select * from user_table where username = ? " +
    "and password = ? ");
stmt.setString(1, uname);
stmt.setString(2, pword);
ResultSet rs = stmt.executeQuery();
```
Security Review

**Cross Site Scripting**

```html
<table>
<tr>
<td>Comments:</td>
<td>$comments</td>
</tr>
</table>

* $comments = <script>alert(document.cookie);</script>
Cross Site Scripting Defense: Input Validation (HTML Escaping)

```html
<table>
<tr>
<td>Comments:</td>
<td>Comments:</td>
<td>`escapeHTML($comments)`</td>
</tr>
</table>

* $comments = `<script>alert(document.cookie);</script>`
Latest Saga

Our OAD activity log showed an alum accessed 35,000 alumni records in April 2006.

We implemented a daily query quota to prevent such incidents in the future.

Moral of the Lesson:
- Log activity as much as possible
- Give info as little as possible
- Security is an ongoing battle