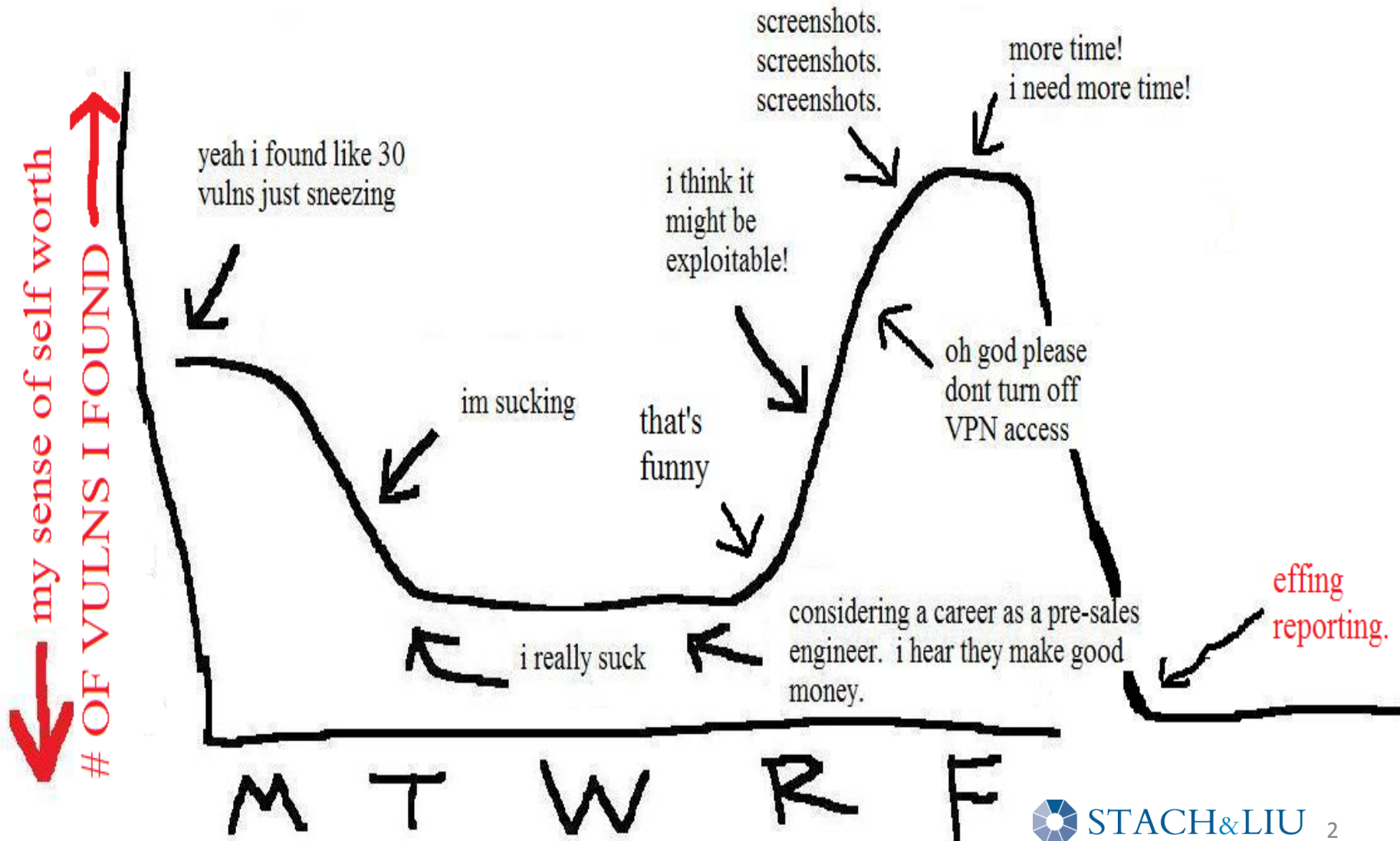


Real-world Code Review

SANS Penetration Testing and
Web Application Attacks Summit

02 JUNE 2009
Presented by Vinnie Liu
Stach & Liu, LLC

a typical week



topics

- Right Tool, Right Time, Right Place
- HQL Manipulation Attacks
- Slow State Manipulation Attacks

security questions

Answer all 3 questions and click **Next** to continue.

The questions highlighted in **red** were answered incorrectly. Please enter answers to the questions marked in **red**.

You have **1 attempt left** to correctly answer all 3 questions.

Question 1: What is the make of your first car?

Question 2: Name of Harry Potter's owl.










Question 3: Stealer of Baggins' Silver Spoons.

< Previous

Cancel

Next >

directory indexing

	opt/	14-Nov-2007 18:39	-
	pam.conf	31-Jul-2004 22:34	552
	pam.d/	17-Sep-2008 19:17	-
	papersize	04-Dec-2007 15:44	7
	passwd	30-Jul-2008 15:12	4.8K
	passwd-	25-Jul-2008 09:27	4.8K
	passwd.bak	26-Nov-2007 23:53	1.4K
	perl/	05-Feb-2008 17:12	-
	postfix/	22-Aug-2008 20:49	-

workflow SQLi

INTERESTS 1 | 2 | 3

What sort of sports and exercise do you enjoy? (Optional)

<input type="checkbox"/> Aids riding / Watercross	<input type="checkbox"/> Aerobics
<input type="checkbox"/> Baseball	<input type="checkbox"/> Basketball
<input type="checkbox"/> Billiards / Pool	<input type="checkbox"/> Bowling
<input type="checkbox"/> Cycling	<input type="checkbox"/> Football
<input type="checkbox"/> Golf	<input type="checkbox"/> Hockey
<input type="checkbox"/> Horse riding	<input type="checkbox"/> Karate arts
<input checked="" type="checkbox"/> Running	<input type="checkbox"/> Skiing
<input type="checkbox"/> Soccer	<input checked="" type="checkbox"/> Swimming
<input type="checkbox"/> Tennis / Racket sports	<input type="checkbox"/> Walking / Hiking
<input checked="" type="checkbox"/> Weight / Strength	<input type="checkbox"/> Yoga
<input type="checkbox"/> Other types of exercise	<input type="checkbox"/> Hockey
<input type="checkbox"/> Volleyball	

What do you like to do in your free time? (Optional)

Share a few of your local hot spots and travel destinations.
256 characters remaining

Fighting Crime

What are some of your favorite places? (Optional)

Share a few of your local hot spots and travel destinations.
252 characters remaining

Tree House and Export Crafts

SAVE & CONTINUE »



INTERESTS 1 | 2 | 3

What common interests would you enjoy sharing with your address? (Optional)

<input type="checkbox"/> Exploring new areas	<input type="checkbox"/> Alumni connections
<input type="checkbox"/> Book club	<input type="checkbox"/> Camping
<input type="checkbox"/> Coffee and conversation	<input type="checkbox"/> Business networking
<input type="checkbox"/> Cooking	<input type="checkbox"/> Dining out
<input checked="" type="checkbox"/> Fasting/Praying	<input type="checkbox"/> Gardening/Landscaping
<input type="checkbox"/> Hobbies and crafts	<input type="checkbox"/> Movies/Video
<input type="checkbox"/> Museums and art	<input type="checkbox"/> Music and concerts
<input type="checkbox"/> Nightclubs/Dancing	<input type="checkbox"/> Performing arts
<input type="checkbox"/> Playing cards	<input type="checkbox"/> Playing sports
<input type="checkbox"/> Political interests	<input type="checkbox"/> Religion/Spiritual
<input type="checkbox"/> Shopping/Deals	<input type="checkbox"/> Travel/Destination
<input type="checkbox"/> Video games	<input type="checkbox"/> Volunteering
<input type="checkbox"/> Watching sports	<input type="checkbox"/> Wine tasting

Share a few of your favorite things. (Optional)

Tell us about your favorite music, TV shows, books - anything goes!
256 characters remaining

I fight crime.

What's the best thing you read? (Optional)

Whether it's a novel or magazine, your best literary adventures can spark a conversation.
261 characters remaining

Crime 101

SAVE & CONTINUE »



LIFESTYLE 1 | 2

What's your current annual income? (Optional)

<input type="checkbox"/> Less than \$15,000	<input type="checkbox"/> \$25,001 to \$35,000
<input type="checkbox"/> \$35,001 to \$50,000	<input type="checkbox"/> \$50,001 to \$75,000
<input type="checkbox"/> \$75,001 to \$100,000	<input type="checkbox"/> \$100,001 to \$150,000
<input type="checkbox"/> \$100,001+	<input checked="" type="checkbox"/> No Answer

Which pets do you have (or you like but don't have)?

	I like but don't have	No opinion
Birds	<input type="checkbox"/>	<input type="checkbox"/>
Cats	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Dogs	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Exotic pets	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Fish	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Horses	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Other	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Tell us more! (Optional)

256 characters remaining

Do you want to share more about your pets? For example, if you have a dog, you might enter the breed or name.

SAVE & CONTINUE »



BACKGROUND/VALUES 1 | 2

What languages do you speak? (Optional)

<input checked="" type="checkbox"/> English	<input checked="" type="checkbox"/> Arabic	<input type="checkbox"/> Chinese
<input checked="" type="checkbox"/> Dutch	<input checked="" type="checkbox"/> French	<input type="checkbox"/> German
<input checked="" type="checkbox"/> Hebrew	<input checked="" type="checkbox"/> Hindi	<input type="checkbox"/> Italian
<input checked="" type="checkbox"/> Japanese	<input checked="" type="checkbox"/> Norwegian	<input checked="" type="checkbox"/> Portuguese
<input checked="" type="checkbox"/> Russian	<input checked="" type="checkbox"/> Spanish	<input checked="" type="checkbox"/> Swedish
<input checked="" type="checkbox"/> Tagalog	<input checked="" type="checkbox"/> Urdu	<input type="checkbox"/> Other

What's your level of education? (Optional)

<input type="checkbox"/> High school	<input type="checkbox"/> Some college
<input type="checkbox"/> Associates degree	<input type="checkbox"/> Bachelors degree
<input type="checkbox"/> Graduate degree	<input checked="" type="checkbox"/> PhD / Post Doctoral
<input type="checkbox"/> No Answer	

Tell us more! (Optional)

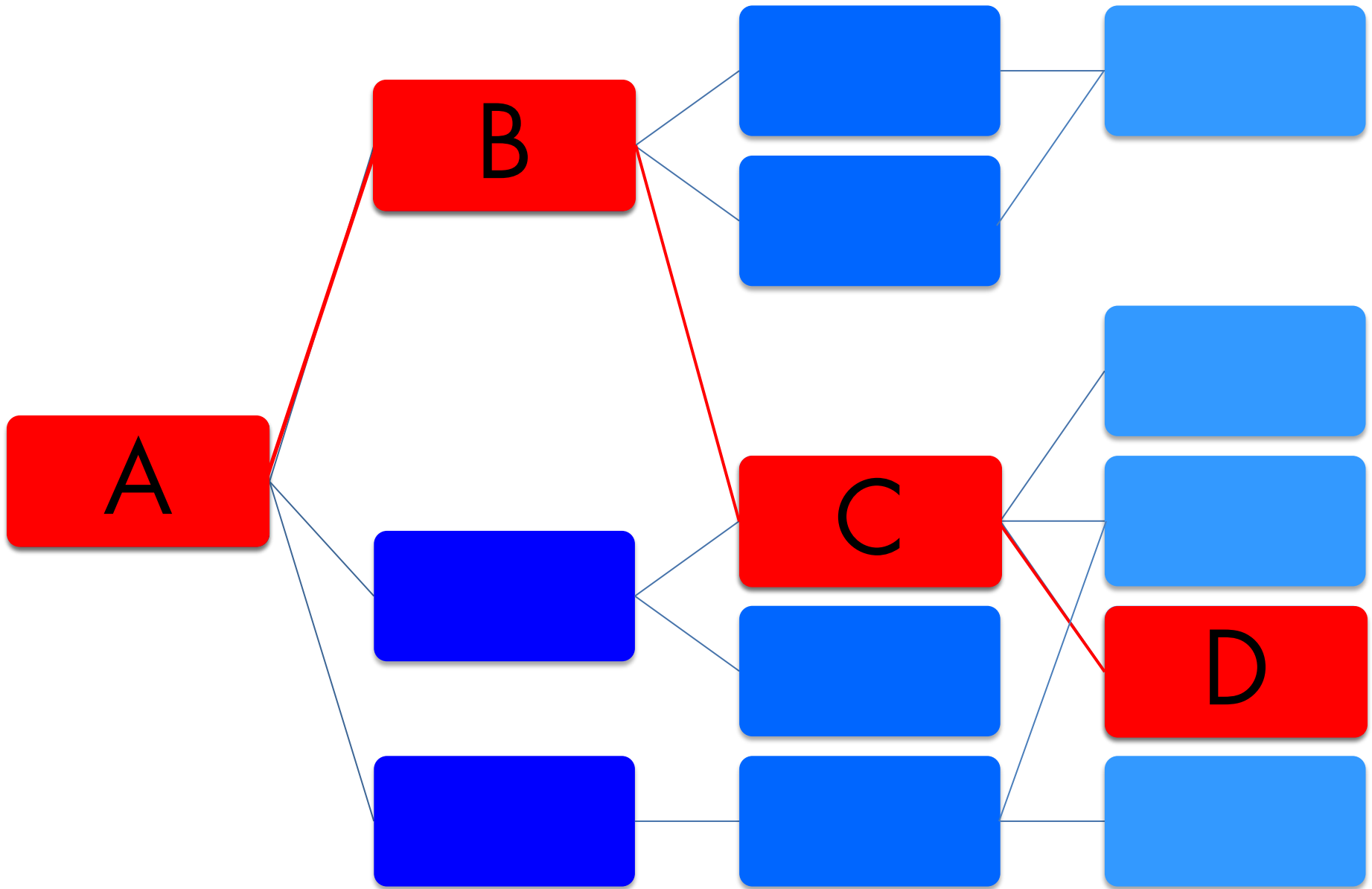
256 characters remaining

Describe your political views.

Liberal

SAVE & CONTINUE »





```
1 String sYum =  
    request.getParameter("Treat");  
  
2 if (!sYum.equals("ricekrispy"))  
    return;  
  
3 String sQuery = "  
    SELECT *  
    FROM TastySnacks  
    WHERE Treat = \""+sYum+"\"";  
  
4 executeQuery(sQuery);
```


**Security
Question**

**Directory
Indexing**

Design

Dev

QA

Release

SQLi

topics

- Right Tool, Right Time, Right Place
- HQL Manipulation Attacks
- Slow State Manipulation Attacks

“consider using persistence layers such as **Hibernate** or Enterprise Java Beans, which can provide significant protection against SQL injection if used properly”¹

HQL injection

The screenshot shows the CWE-564: SQL Injection: Hibernate page. The page header includes the CWE logo and the text "Common Weakness Enumeration A Community-Developed Dictionary of Software Weakness Types". The breadcrumb trail is "Home > CWE List > CWE- Individual Dictionary Definition (1.4)". The left sidebar contains navigation links for "CWE List", "About", "Community", "News", "Compatibility", and "Contact Us". The main content area features a blue header "SQL Injection: Hibernate" and a "Weakness ID: 564 (Weakness Variant)" label. The "Description" section includes a "Summary" stating that using Hibernate to execute a dynamic SQL statement built with user-controlled input can allow an attacker to modify data. The "Time of Introduction" section lists "Architecture and Design" and "Implementation". The "Demonstrative Examples" section provides a Java code snippet for a query that is vulnerable to HQL injection. The "Potential Mitigations" section suggests using a non-SQL style database. The "Architecture and Design" section begins with the principle of least privilege.

CWE-564: SQL Injection: Hibernate

SQL Injection: Hibernate

Weakness ID: 564 (Weakness Variant)

▼ Description

Summary

Using Hibernate to execute a dynamic SQL statement built with user-controlled input can allow an attacker to modify data.

▼ Time of Introduction

- Architecture and Design
- Implementation

▼ Demonstrative Examples

The following code excerpt uses Hibernate's HQL syntax to build a dynamic query that's vulnerable to SQL injection.

Java Example:


```
String street = getStreetFromUser();
Query query = session.createQuery("from Address a where a.street='" + street + "'");
```

▼ Potential Mitigations


Requirements specification: A non-SQL style database which is not subject to this flaw may be chosen.

Architecture and Design

Follow the principle of least privilege when setting user accounts. SQL should only be used for

 `String query = "from Users u where
u.ID = \'' + uid + '\''";`

`session.find(query);`

 `String query = "from Users u where
u.ID = ?";`

`session.find(query, uid,
StringType);`

unpublished vector



```
List users =
```

```
sess.createCriteria(User.class)  
.add(  

```

```
    Restrictions.sqlRestriction(  
        "Users.ID = `" + uid + "`")  

```

```
.list();
```

HQL manipulation

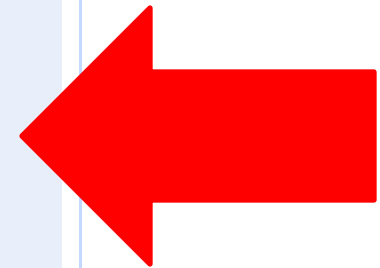
Sign in to Flight Manager X:

User ID:

Last 4
SSN:

Remember me on this
computer.

[I cannot access my account](#)



```
1 String uid = r.getParameter("uid");  
String ssn = r.getParameter("ssn");
```

```
2 String query = "  
    from Users u  
    where u.ID = :id  
    and u.SSN like :last4";
```

```
3 String[] p = {"id", "last4"};  
String[] v = {uid, '%' + ssn};
```

```
4 session.find(query, p, v);
```


simple bypass

% 0 1 2 3 4 5 6 7 8 9 5

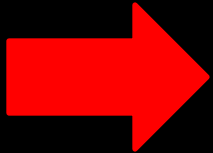
```
from Users u
where u.ID = :id
and u.SSN like %5
```

SSN enumeration

%	0	1	2	3	4	5	6	7	8	9		5
	0	1	2	3	4	5	6	7	8	9		25
	0	1	2	3	4	5	6	7	8	9		625
	0	1	2	3	4	5	6	7	8	9		0625
	0	1	2	3	4	5	6	7	8	9		10625
	0	1	2	3	4	5	6	7	8	9		810625
	0	1	2	3	4	5	6	7	8	9		5810625
	0	1	2	3	4	5	6	7	8	9		45810625
	0	1	2	3	4	5	6	7	8	9		245810625

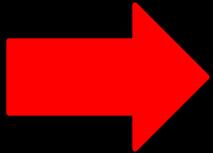
direct Criteria

```
List users =  
    sess.createCriteria(Users.class)  
        .add(  
            Restrictions.sqlRestriction(  
                "Users.SSN = ?",  
                '%' + ssn,  
                Hibernate.STRING)  
            )  
        .list();
```



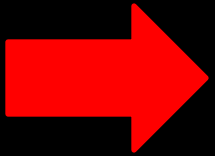
logical Criteria

```
List users =  
    sess.createCriteria(Users.class)  
        .add(  
            Restrictions.and(  
                Restrictions.eq("ID", uid),  
                Restrictions.like("SSN", '%' + ssn)  
            )  
        )  
        .list();
```



Example criteria

```
Example ex = Example.create(user)
    .ignoreCase()
    .enableLike();
```



```
List results =
    session.createCriteria(User.class)
        .add(ex)
        .list();
```

affects ASP.NET too

```
SQLi = "SELECT *  
FROM Users  
WHERE SSN  
LIKE '%\' + ssn"
```

1 sql = "SELECT *
FROM Users
WHERE SSN
LIKE '%\' + @ssn"

```
2 cmd.Parameters.Add(  
    New SqlParameter( "@ssn",  
        "% & ssn & %" ) )
```

```
3 sql = "SELECT * FROM Users  
        WHERE SSN LIKE @ssn"
```

```
cmd.Parameters.Add(  
    New SqlParameter( "@ssn", ssn ) )
```

for real

The screenshot shows the American Funds website header with the logo and navigation links: Home, Contact Us, Your Accounts, Fund Information, Retirement Planning, College Planning, Investor Resources, and About Us. The main heading is "Account Login for New Users". Below this, a message asks the user to enter their account number and the last four digits of their Social Security number (SSN). A form box contains the following fields:

Please enter your account number and the last four digits of your Social Security number (SSN) below.

Enter your login information:

Account number: [Where to find your account number](#)

SSN:
(last four digits)

topics

- Right Tool, Right Time, Right Place
- HQL Manipulation Attacks
- Slow State Manipulation Attacks

slow state manipulation

Mia
Chihuahua

11 of 484,534 dogs in random order
[resume this stroll later]

<< previous dog | next dog >>

Dogster stats for Mia
Corralled: 1 time Pals: 4 Views: 227
Paws: 🐾🐾🐾 by 3 voters
Stars: ★

🦴 Leave a bone for Mia

Nicknames:
booboosh

Doggie Dynamics:

Energy	sleepy	energetic
Intelligence	silly	serious
Friendliness	aggressive	affectionate
Playfulness	not playful	very playful
Disposition	anxious	calm

Home: CA
Age: 2 Years Sex: Female Weight: 1-10 lbs

📧 ★ 🐾 @ 🦴 📦

DOGSTER PLAY TOYS

Quick Bio:
-purebred

Likes:
Hugs & kisses, pawdicures and with my mom.

Pet Peeves:

101

Kaska
American Eskimo Dog

38 of 484,526 dogs in random order
[resume this stroll later]

<< previous dog | next dog >>

Dogster stats for Kaska
Corralled: 2 times Pals: 11 Views: 234
Stars: ★★

🦴 Leave a bone for Kaska

Nicknames:
Puppa, Sasuke, Moskaske

Doggie Dynamics:

Energy	sleepy	energetic
Intelligence	silly	serious
Friendliness	aggressive	affectionate
Playfulness	not playful	very playful
Disposition	anxious	calm

Sun Sign:
🌞 SAGITTARIUS See today's dog horoscope

Quick Bio:
-purebred

Likes:
Rubber Bones, Tennis Balls, His Baby Blanket, and Shigure [his stuffed dog], Getting rubbed on his tummy, Attention, Eating food off the ground...

Home: IN
Age: 1 Year Sex: Male Weight: 1-10 lbs

📧 ★ 🐾 @ 🦴 📦

DOGSTER PLAY TOYS

201

<http://dog.com/edit.jsp?dogID=101>

edit check

```
1 String dogID =  
    request.getParameter("dogID");  
  
2 request.getSession()  
    .setAttribute("editDogID", dogID);  
  
3 if (ownsDog() != true) return;  
  
    {...}  
  
4 request.getSession()  
    .removeAttribute("editDogID");
```

access denied

Whoa! no dog for you!!!!

There's supposed to be a dog here, but it's no where to be found. This occurs when you don't have permission to see a dog or someone removes a dog after you started your dog stroll. Though on very rare occasions extremely shy dogs have been known to crawl right under the server and refuse to come out. If only we had a treat! Here doggie doggie doggie! Who wants a treat?

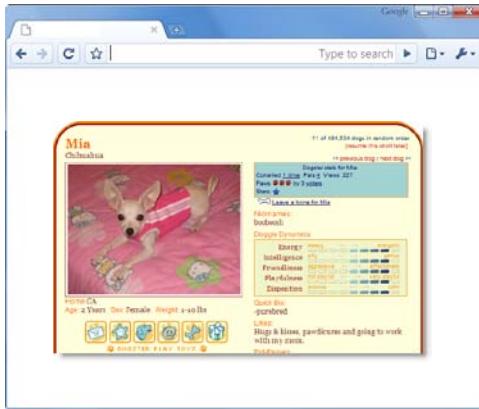
`http://dog.com/edit.jsp?dogID=201`

submit check

```
1  if ( getDogID.equals(  
2      request.getSession()  
      .getAttribute("editDogID") ) )  
    {  
3      // submission allowed  
    }  
}
```

dog theft

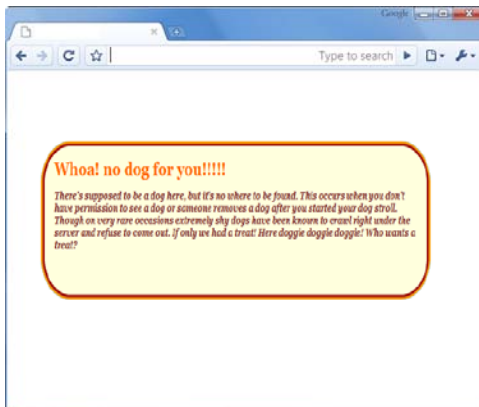
1



dogID=101



2




dogID=201



editDogID=201

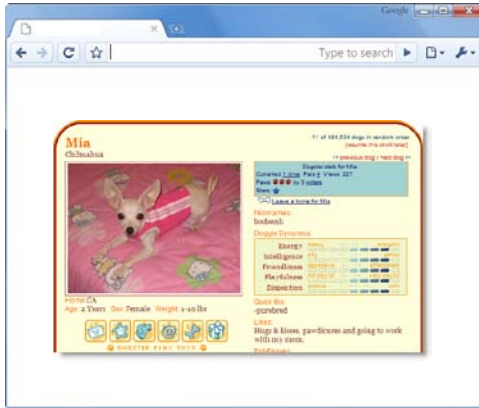
edit check

```
String dogID =  
    request.getParameter("dogID");  
  
request.getSession()  
    .setAttribute("editDogID", dogID);  
  
if (ownsDog() != true) return;  
  
{...}  
  
request.getSession()  
    .removeAttribute("editDogID");
```



dog theft

3




submit changes
w/dogID=201



editDogID=201

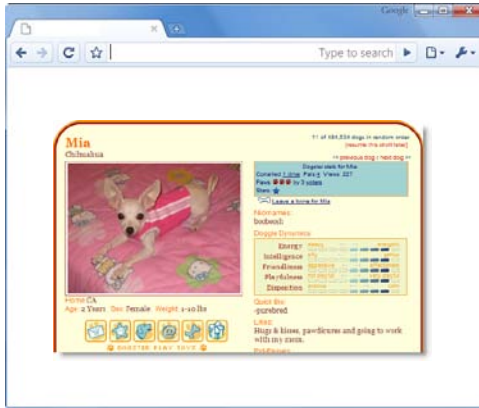
submit check

```
if ( getDogID.equals(  
    request.getSession()  
        .getAttribute("editDogID") ) )  
{  
  
    // submission allowed  
  
}
```



dog theft*

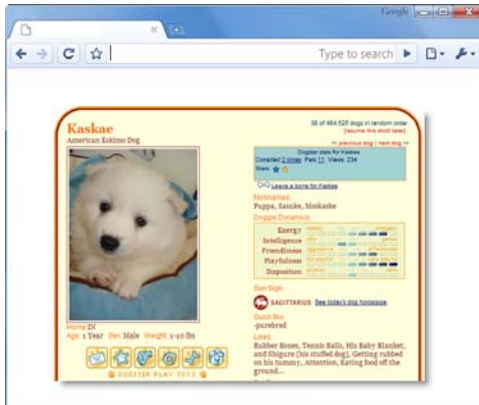
3



submit changes
w/dogID=201



4



dogID=201



summary

- Right Tool, Right Time, Right Place
- HQL Manipulation Attacks
- Slow State Manipulation Attacks

thanks!