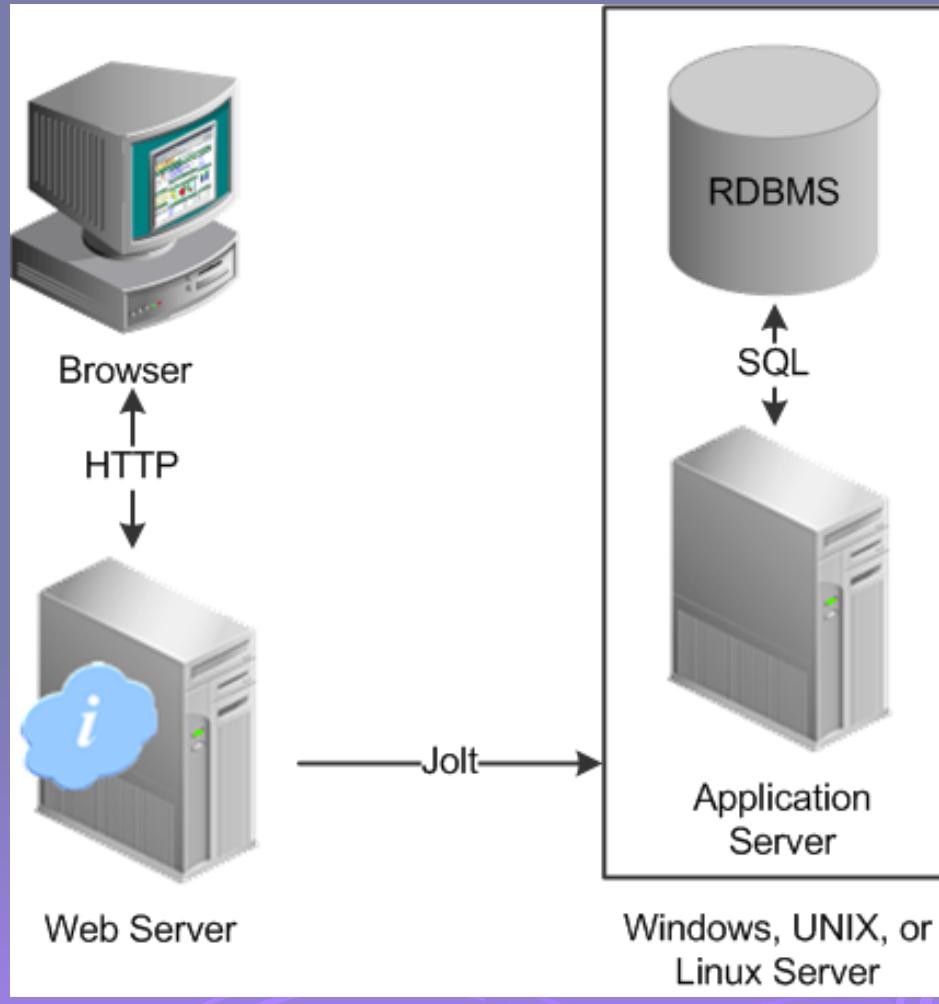


TTM4536 - Ethical Hacking - Information Security, Specialization Course

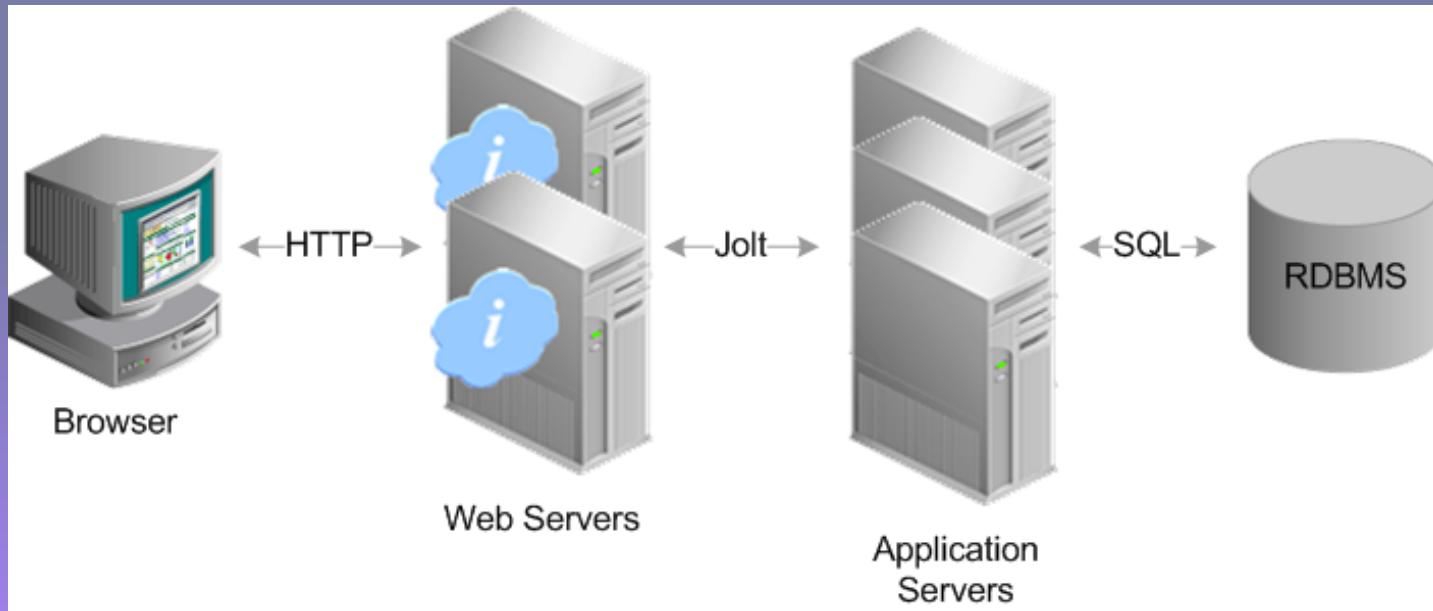
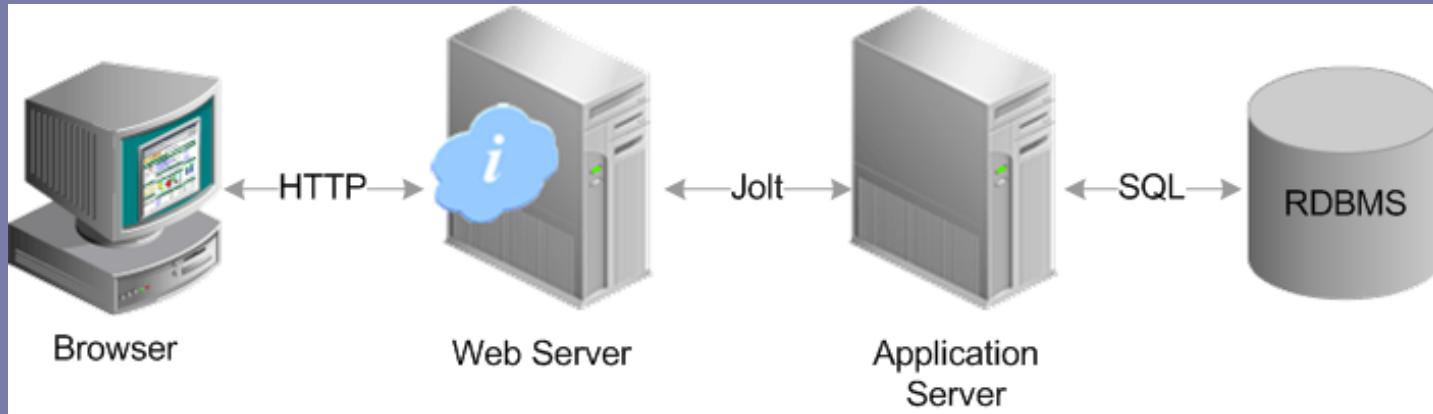
- Plan for 24 Oct 2017
- SQL Injections

Logical and physical relation between web servers and relational database servers



Logical relation

Logical and physical relation between web servers and relational database servers



Physical relation

What is a SQL Injection Attack?

- Many web applications take user input from a form
- Often this user input is used literally in the construction of a SQL query submitted to a database. For example:
 - `SELECT productdata FROM table WHERE productname = ‘user input product name’ ;`
- A SQL injection attack involves placing SQL statements in the user input

An Example SQL Injection Attack

Product Search: **blah ' OR 'x' = 'x**

- This input is put directly into the SQL statement within the Web application:
 - \$query = "SELECT prodinfo FROM prodtable WHERE proddname = '' .
\$_POST['prod_search'] . " " ;
- Creates the following SQL:
 - SELECT prodinfo FROM prodtable WHERE proddname = **'blah ' OR 'x' = 'x'**
 - Attacker has now successfully caused the entire database to be returned.

A More Malicious Example

- What if the attacker had instead entered:
 - **blah ';** **DROP TABLE prodinfo;** **--**
- Results in the following SQL:
 - **SELECT prodinfo FROM prodtble WHERE prodname = 'blah' ; DROP TABLE prodinfo; --**
 - Note how comment (--) consumes the final quote
- Causes the entire database to be deleted
 - Depends on knowledge of table name
 - This is sometimes exposed to the user in debug code called during a database error
 - Use non-obvious table names, and never expose them to user
- Usually data destruction is not your worst fear, as there is low economic motivation

Other injection possibilities

- Using SQL injections, attackers can:
 - Add new data to the database
 - Could be embarrassing to find yourself selling politically incorrect items on an eCommerce site
 - Perform an INSERT in the injected SQL
 - Modify data currently in the database
 - Could be very costly to have an expensive item suddenly be deeply ‘discounted’
 - Perform an UPDATE in the injected SQL
 - Often can gain access to other user’s system capabilities by obtaining their password

Defenses

- Use provided functions for escaping strings
 - Many attacks can be thwarted by simply using the SQL string escaping mechanism
 - Instead of ‘ use \’
 - and
 - Instead of “ use \”
 - Or use `mysql_real_escape_string()` as the preferred function for this
- Not a silver bullet!
 - Consider:
 - `SELECT fields FROM table WHERE id = 23 OR 1=1`
 - No quotes here!

More Defenses

- Check syntax of input for validity
 - Many classes of input have fixed languages
 - Email addresses, dates, part numbers, etc.
 - Verify that the input is a valid string in the language
 - Sometime languages allow problematic characters (e.g., '*' in email addresses); may decide to not allow these
 - If you can exclude quotes and semicolons that's good
 - Not always possible: consider the name Bill O' Reilly
 - Want to allow the use of single quotes in names
- Have length limits on input
 - Many SQL injection attacks depend on entering long strings

Even More Defenses

- Insert code that scans query string for undesirable word combinations that indicate SQL statements
 - INSERT, DROP, etc.
 - If you see these, can check against SQL syntax to see if they represent a statement or valid user input
- Limit database permissions and segregate users
 - If you're only reading the database, connect to database as a user that only has read permissions
 - Never connect as a database administrator in your web application

More Defenses

- Configure database error reporting
 - Default error reporting often gives away information that is valuable for attackers (table name, field name, etc.)
 - Configure so that this information is never exposed to a user
- If possible, use bound variables
 - Some libraries allow you to bind inputs to variables inside a SQL statement
 - PERL example (from <http://www.unixwiz.net/techtips/sql-injection.html>)

```
$sth = $dbh->prepare("SELECT email, userid FROM members WHERE  
email = ?;");  
$sth->execute($email);
```

https://www.codebashing.com/sql_demo

FIND OUT MORE [Tweet](#)

Exercise Instructions

Start Here

Each lesson starts here. Read the explanation, then follow the instructions underneath.

Next

In this interactive tutorial you will understand how SQL injection attacks are used to compromise the security of a web application, and how to write code more securely to protect against this type of attack.

START

https://trade_portal.codebashing.com/log_in

BROWSER LOCKED

Login

TradePORTAL Login

Username:

Password:

Vulnerable Application

Go through all the demo instructions
on this web site

Remember Web Security Dojo?

Installing Web Security Dojo with VirtualBox

File Edit View History Bookmarks Tools Help

http://dojo.mavensecurity.com/ Google

Most Visited Getting Started Latest Headlines

Maven Security ... Downloads - Virt... Browse Web Sec... 3341956878_13e2... hro_1004_019.jpg... snapshot2007020... YouTube - Mave... mavensecurity o...

SECURITY CONSULTING

maven (noun): a trusted expert who seeks to pass knowledge on to others

Home Services News & Events Resources About Us Contact Us Maven Security Consulting Inc

Web Security Dojo

A free open-source self-contained training environment for Web Application Security penetration testing. Tools + Targets = Dojo

What?
Various web application security testing tools and vulnerable web applications were added to a clean install of Ubuntu v9.10.

Why?
The Web Security Dojo is for learning and practicing web app security testing techniques. It is ideal for training classes and conferences since it does not need a network connection. The Dojo contains everything needed to get started - tools, targets, and documentation.

Where?
Download Web Security Dojo from <http://sourceforge.net/projects/websecuritydojo/files/>.

How?
To install Dojo you can install and run VirtualBox, then "Import Appliance" using the Dojo's OVF file. Go here for Virtual Box instructions. As of version 1.0 a VMware version is also provided.

Who?
Sponsored by Maven Security Consulting Inc (performing web app security testing & training since 1996).

Announcements

- * Check out our YouTube channel for videos about Web Security Dojo (more videos coming soon).
- * Current version of Web Security Dojo is v1.0, released Feb. 21, 2010.
- * Web Security Dojo v0.4 was released Feb. 2, 2010.
- * Web Security Dojo v0.3 was released Jan. 27, 2010.
- * Web Security Dojo v0.2 was released Nov. 4, 2009.
- * Public debut of v0.1 on Nov. 3, 2009 at USENIX LISA 2009 conference in Baltimore, Maryland.

- * The project needs contributors! Get involved.

Current Features (v1.0) Upcoming Features

Convenient virtual machine image

Done 0:35 / 6:04 CC HD Fiddle Disabled

Before starting Kali and Dojo do the following in VirtualBox

- 1. In Preferences go to Network**
- 2. Change Network adapters for both Kali
and Dojo to be Bridged**

- 1. Start Dojo and find out its IP address**
- 2. Start Firefox and open localhost**
- 3. Start the vulnerable web server
Insecure Web App.**
- 4. See that the port that the server is
listening is 8080**



American Services

[Products](#)
 [Customer Login](#)

[Instructions](#)

InsecureWebApp

Sponsored By
The logo features two blue interlocking shapes forming a stylized letter 'G'.
ISTHMUSGROUP

OWASP
The Open Web Application Security Project

> Customer Login

Name :

Password :

[I need a new password](#)

- On Kali machine in a browser put the address of the web site of the dojo Insecure Web App

The screenshot shows a web browser window with the following details:

- Address Bar:** 192.168.1.13:8080/insecure/public/Login.jsp
- Page Title:** American Services
- Left Sidebar:** AS logo, navigation links: Products, Customer Login, Instructions, and InsecureWebApp.
- Sponsored By:** ISTHMUSGROUP logo.
- Content Area:**
 - Customer Login Form:** A black header bar with white text reads > Customer Login. Below it are two input fields: Name : [text input] and Password : [text input]. To the right of the password field is a "Login" button. Below the form is a link: I need a new password.

- Try the username admin to break the login access by injecting some SQL query for the password field

192.168.1.13:8080/insecure/public/Login.jsp

American Services

[Products](#)
[Customer Login](#)

[Instructions](#)
InsecureWebApp

Sponsored By

ISTHMUSGROUP

 OWASP
The Open Web
Application Security Project

> Customer Login

Name :

Password :

I need a new password

- Try the username admin to break the login access by injecting some SQL query for the password field

The screenshot shows a web browser window with the URL `192.168.1.13:8080/insecure/public/Login.jsp?login=admin&pass=` in the address bar. The page title is *American Services*. On the left, there's a sidebar with links for [Products](#), [Customer Login](#), and [Instructions](#). Below that, it says **InsecureWebApp**. A logo for **ISTHMUSGROUP** is shown with the text "Sponsored By". At the bottom left is the **OWASP** logo with the text "The Open Web Application Security Project". The main content area contains a "Customer Login" form with fields for Name and Password, and a "Login" button. There's also a link "I need a new password".

192.168.1.13:8080/insecure/public/Login.jsp?login=admin&pass=

American Services

Products

Customer Login

Instructions

InsecureWebApp

Sponsored By

ISTHMUSGROUP

OWASP

The Open Web Application Security Project

> Customer Login

Name :

Password : Login

[I need a new password](#)

- Try the username admin to break the login access by injecting some SQL query for the password field

The screenshot shows a web browser window with the URL `192.168.1.13:8080/insecure/public/Login.jsp?login=admin&pass=` in the address bar. The page title is *American Services*. On the left, there's a sidebar with links for [Products](#), [Customer Login](#), and [Instructions](#). Below these is the text **InsecureWebApp**. Underneath that, it says **Sponsored By** with the **ISTHMUSGROUP** logo. At the bottom left is the **OWASP** logo with the text **The Open Web Application Security Project**. The main content area contains a **> Customer Login** form with fields for **Name :** and **Password :**, a **Login** button, and a link [I need a new password](#).

Bypass the authentication by gluing to pass= some of the following
'OR 1=1--

or

') OR 1=1--

or

' OR '1'='1>--

- Try the username admin to break the login access by injecting some SQL query for the password field

The screenshot shows a web browser window with the URL `192.168.1.13:8080/insecure/public/Login.jsp?login=admin&pass='OR 1=1--`. The page title is "American Services". On the left, there's a sidebar with links for "Products", "Customer Login", "Instructions", and "InsecureWebApp". The main content area displays a "Customer Login" form with fields for "Name" and "Password", and a link "I need a new password". A purple arrow points from the text at the bottom of the slide to the "Password" input field.

Bypass the authentication by gluing to pass= some of the following
'OR 1=1--
or
) OR 1=1--
or
' OR '1'='1'-- or try something else

- Try the username admin to break the login access by injecting some SQL query for the password field

192.168.1.13:8080/insecure/secure/index.jsp

AS American Services

Products
Hello Administrator.
Logout
Home
Preferences
Admin

Instructions
InsecureWebApp

Sponsored By
 Isthmus Group

 OWASP The Open Web Application Security Project

> Account Information for Administrator

| | | |
|-----------|----------|----------------------|
| Account # | Invoiced | Instructions / Notes |
|-----------|----------|----------------------|

> New Payment Wizard

| | |
|------------------|--|
| Credit Card # | <input type="text"/> |
| Expiration MM/YY | <input type="text"/> |
| Amount | <input type="text"/> <input type="button" value="Submit"/> |

The power of sqlmap

- In a web browser in Kali go to the web page <http://sqlmap.org>
- Install the latest sqlmap tool:
 - Download the tarball
 - tar zxvf sqlmap*
 - Go to the sqlmap folder
 - Run: python sqlmap.py

- There are 1 + 12 videos (around 1 minute each) demonstrating the work with sqlmap
- Repeat the demos presented in the videos on <http://sqlmap.org>