

# Ethical Hacking Penetrating Web 2.0 Security

# Contact

- Sam Bowne
- Computer Networking and Information Technology
- City College San Francisco
- Email: [sbowne@ccsf.edu](mailto:sbowne@ccsf.edu)
- Web: [samsclass.info](http://samsclass.info)

# Two Hacking Classes

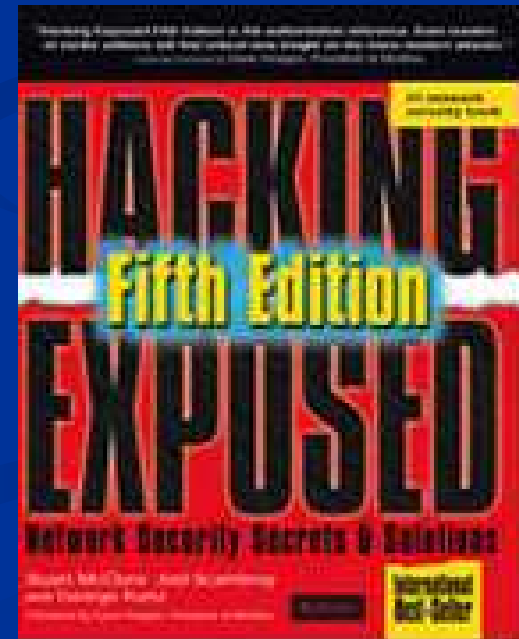
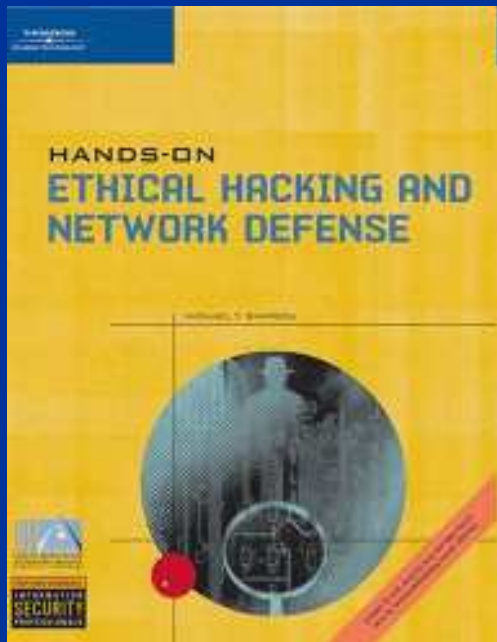
## CNIT 123: Ethical Hacking and Network Defense

Has been taught since Spring 2007 (four times)

*Face-to-face and Online sections available Fall 2008*

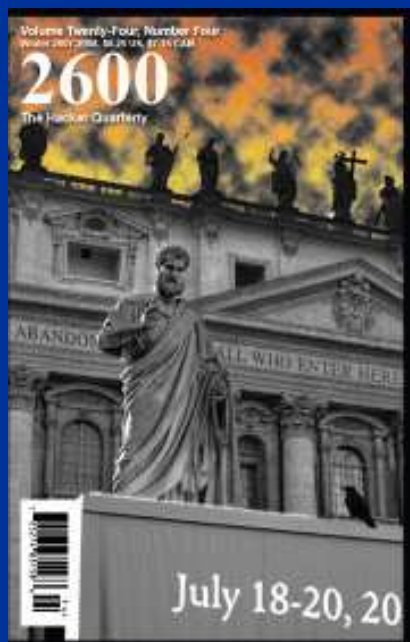
## CNIT 124: Advanced Ethical Hacking

Taught for the first time in Spring 2008



# Supplemental Materials

- Projects from recent research
- Students get extra credit by attending conferences



# Certified Ethical Hacker

- Those two classes prepare students for CEH Certification



The illustration shows a man in a white shirt and tie, carrying a large red pencil, standing next to a computer monitor. The monitor displays a globe and is labeled 'CEH'. Several dashed arrows point towards the monitor, representing different types of network threats: 'Trojans', 'DDoS Attacks', 'Virus', 'Worms', and 'Spam'. The background is a gradient of orange and blue.

**Defend your Network  
Against Hackers.**

**Master the Hacking  
Technologies.**

**Become a  
Certified Ethical Hacker.**

Ethical Hacking and Countermeasures

<http://www.eccouncil.org>

**EC-Council**

# Certificate in Network Security

## *Network Security*

This program provides instruction in the measures that must be taken to detect and prevent network security mistakes and vulnerabilities, and includes descriptions of common attacks and methods to configure the operating system, servers, routers, firewalls, and email. Preparation for the CompTIA Security+ exam.

## *Courses Required for the Certificate of Completion in Network Security*

Course	Units
<u>CNIT 106</u> Introduction to Networks or <u>CNIT 106C</u> Intro to Network Convergence or <u>CNIT 201E</u> Network Fundamentals .....	3
<u>CNIT 108</u> Wireless Networks, Advanced .....	3
<u>CNIT 120</u> Network Security .....	3
<u>CNIT 122</u> Firewalls .....	3
<u>CNIT 123</u> Ethical Hacking or <u>CNIT 221</u> Cisco PIX firewall & Router Sec or <u>CNIT 124</u> Advanced Ethical Hacking .....	3

# Associate of Science Degree

## *Courses Required for the Major in Computer Networking and Information Technology*

Core Courses	Units
<u>CNIT 103</u> Computer Hardware .....	3
<u>CNIT 106</u> Introduction to Networks	
or <u>CNIT 106C</u> Introduction to Network Convergence	
or <u>CNIT 201E</u> Network Fundamentals .....	3
<u>CNIT 131</u> Internet Basics and Beginning HTML .....	3
<u>CNIT 120</u> Network Security .....	3

## **Option in Network Security**

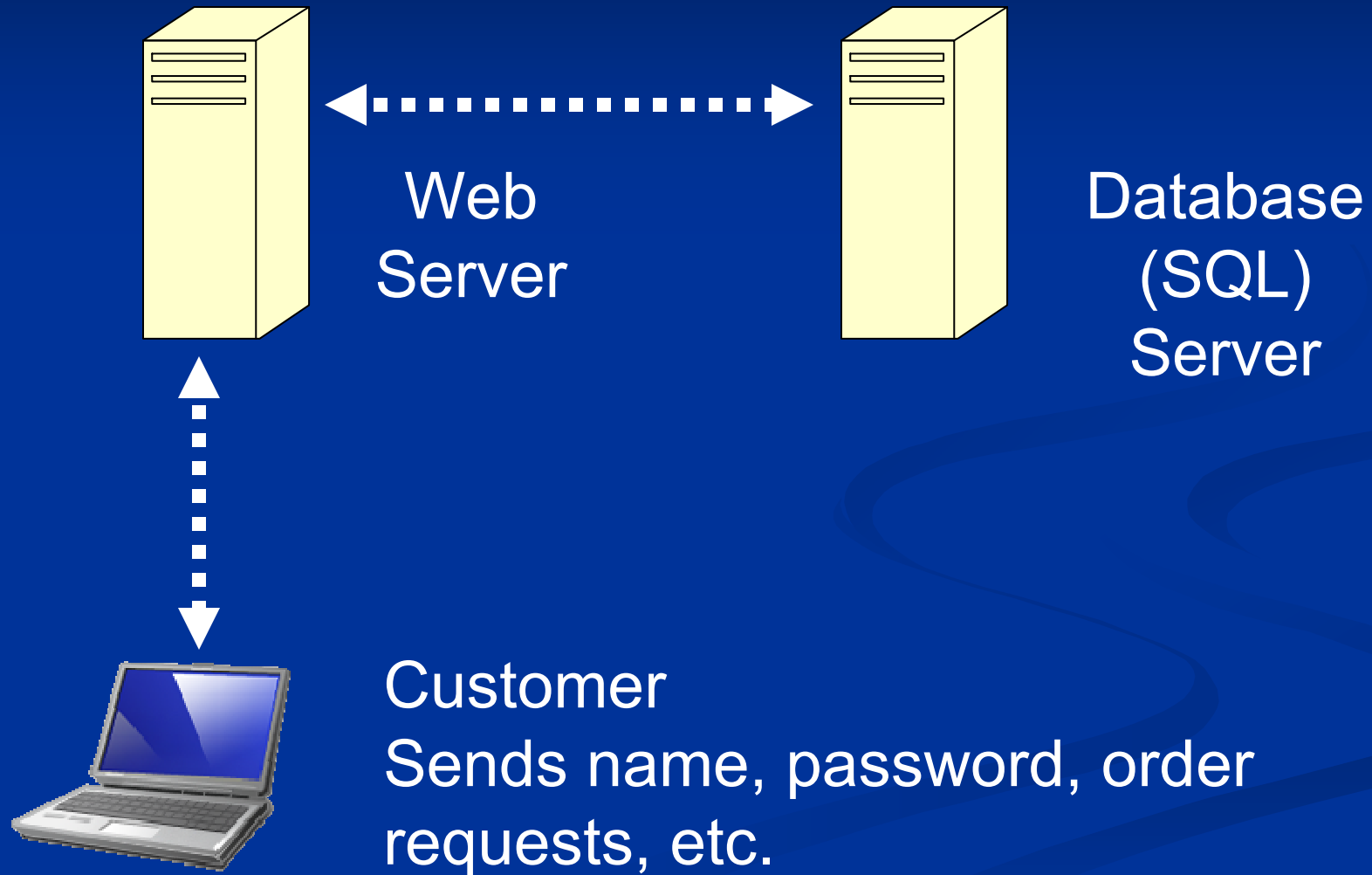
Required	
<u>CNIT 121</u> Computer Forensics .....	3
<u>CNIT 122</u> Firewalls .....	3
<u>CNIT 123</u> Ethical Hacking and Network Defense .....	3
<b>Total Units</b> .....	<b>21</b>

# Four Vulnerabilities

- SQL Injection
  - 16% of Web sites vulnerable
- Cross-Site Scripting
  - 65% of major sites vulnerable
- Cross-Site Request Forgery
  - Almost every Web site with a login is vulnerable
- Layer 7 Denial of Service
  - Every site with active content is vulnerable

# SQL Injection

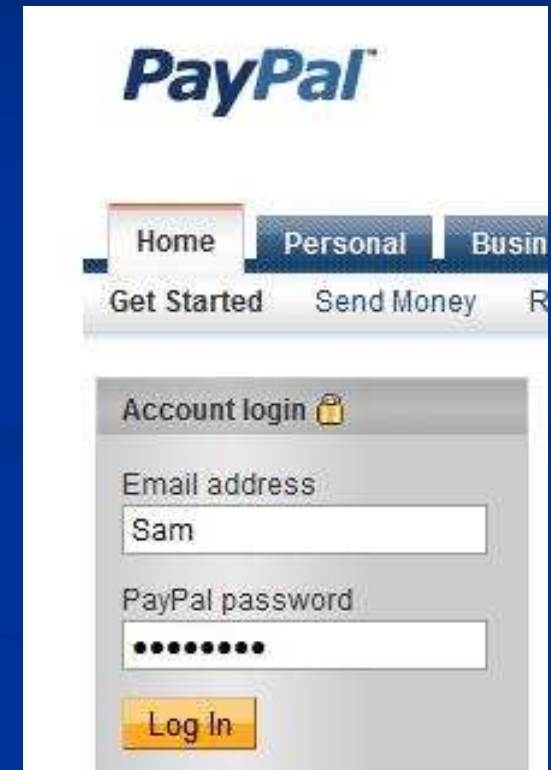
# E-Commerce Web Site



# E-Commerce Login

- HTML Form collects name and password
- It's processed at the SQL server with code like this:

```
SELECT * FROM customer WHERE  
    username = 'name' AND  
    password = 'pw'
```



The image shows a screenshot of the PayPal website's account login page. At the top, the PayPal logo is displayed. Below it, there is a navigation menu with tabs for 'Home', 'Personal', and 'Busin'. Underneath the navigation menu, there are links for 'Get Started', 'Send Money', and 'R'. The main content area features a 'Account login' section with a lock icon. It contains two input fields: 'Email address' with the text 'Sam' and 'PayPal password' with a masked password of ten dots. A yellow 'Log In' button is positioned below the password field.

# SQL Injection

If a hacker enters a name of ' OR 1=1 --

The SQL becomes:

```
SELECT * FROM customer
WHERE username = '' OR 1=1 --' AND
password = 'pw'
```

The -- ends the statement, making the rest of the line a comment

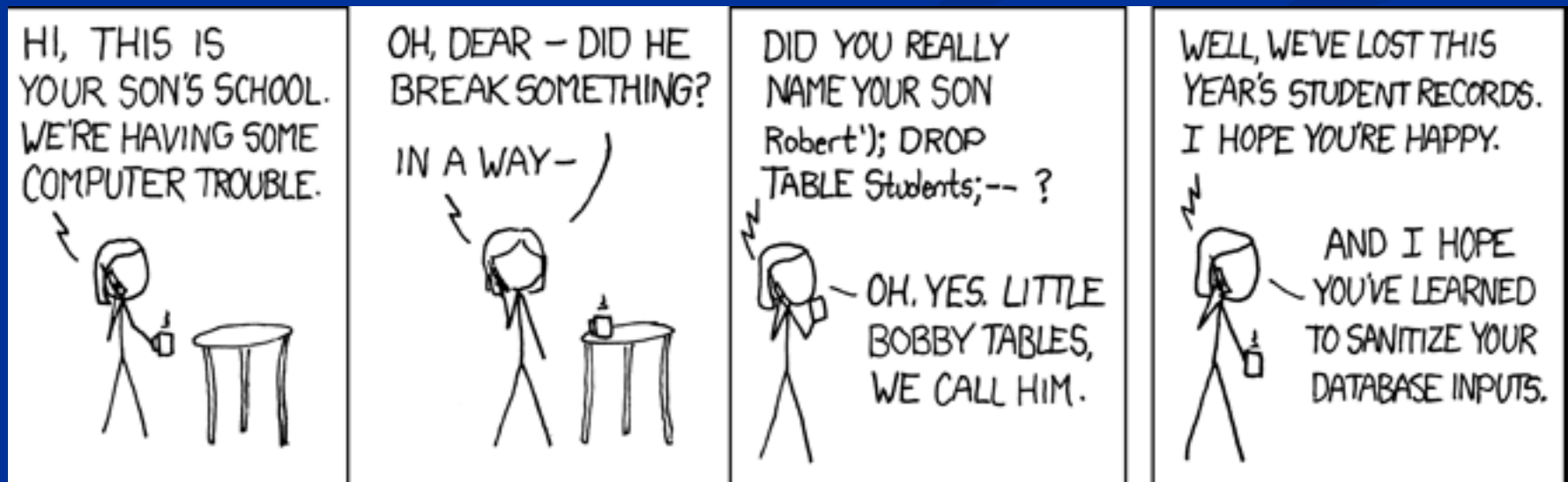
1=1 is always true, so this makes the condition true

# Demonstration



# SQL Injection Effects

- This can cause the user to be authenticated as administrator, dump the entire database, or have other drastic effects
  - Comic from [xkcd.org](http://xkcd.org)

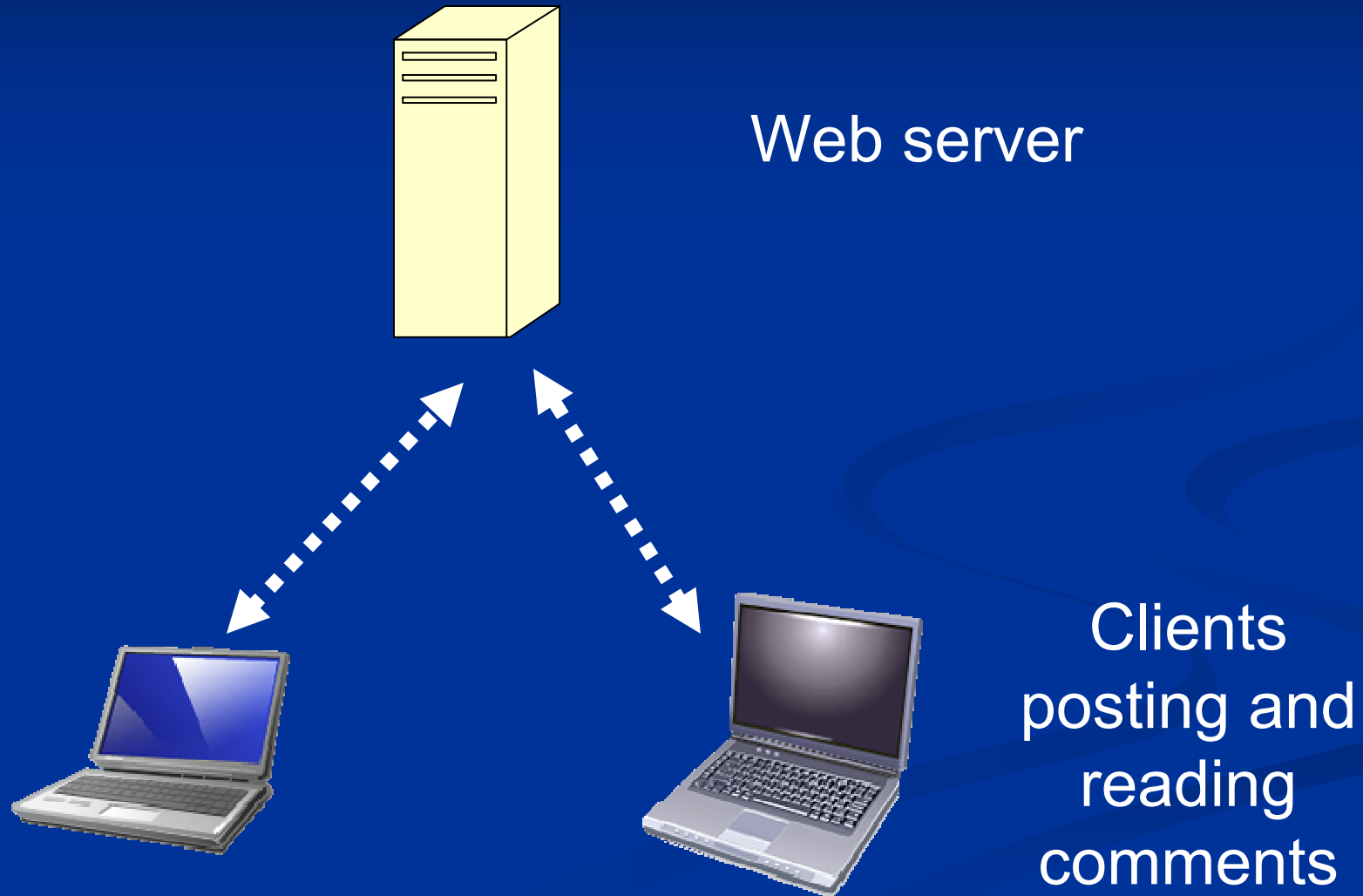


# Sanitize your Inputs

- All user input should be checked, and special characters like ' or " or < or > discarded
- That will reduce vulnerability to SQL injection
  - The typical SQL Injection vulnerability takes more than four months to locate and fix

# Cross-Site Scripting (XSS)

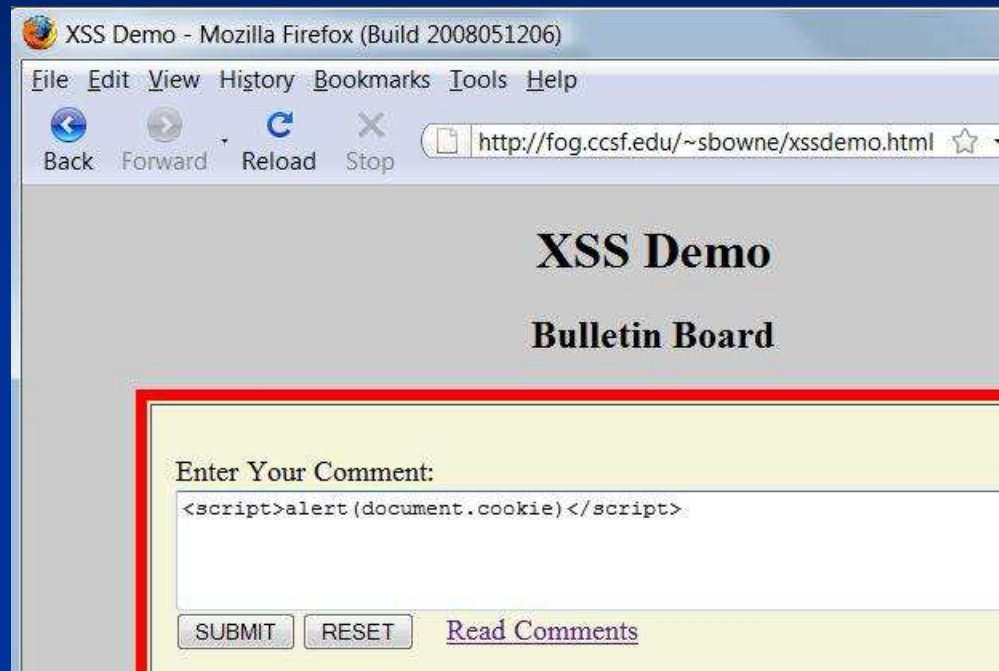
# Web Message Board



# Cross-Site Scripting (XSS)

- One client posts active content, with `<script>` tags or other programming content
- When another client reads the messages, the scripts are executed in his or her browser
- One user attacks another user, using the vulnerable Web application as a weapon

# Demonstration



- `<script>alert("XSS vulnerability!")</script>`
- `<script>alert(document.cookie)</script>`
- `<script>>window.location="http://www.ccsf.edu"</script>`

# XSS Scripting Effects

- Steal another user's authentication cookie
  - Hijack session
- Harvest stored passwords from the target's browser
- Take over machine through browser vulnerability
- Redirect Webpage
- Many, many other evil things...

# Cross-Site Request Forgery (XSRF)

# Web-based Email

To  
Internet



# Cross-Site Request Forgery (XSRF)

- Gmail sends the password through a secure HTTPS connection
  - That cannot be captured by the attacker
- But the cookie identifying the user is sent in the clear—with HTTP
  - That can easily be captured by the attacker
- The attacker gets into your account without learning your password

# Demonstration

Hamster - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://hamster/ Google

Getting Started Latest Headlines Gmail: Email from Goo... City College of San Fra...

Hamster Gmail - Inbox - s214target@gmail.c...

## 192.168.2.103

[\[cookies\]](#)

- <http://mail.google.com/mail>
- <http://google.com/>
- <http://en-us.start2.mozilla.com/firefox?client>
- <http://mail.google.com/mail/channel/bind?at>
- <http://mail.google.com/mail/channel/bind?at>
- <http://mail.google.com/mail/channel/bind?at>
- <http://mail.google.com/mail/?ui=2&ik=e858>
- <http://mail.google.com/mail/channel/test?at>
- <http://chatenabled.mail.google.com/mail/ima>
- <http://mail.google.com/mail/channel/test?at>

## HAMSTER 1.0 Side-Jacking

The following is a list of individuals we can see surfing the web. Click on one of these in order to activate this as the side-jacked session. After that point, you can either select from the list of URLs that will appear on the left, or you can type a new URL in the browser's address bar.

- [192.168.2.1](http://192.168.2.1)
- [192.168.2.103](http://192.168.2.103) - "sam.bowne@gmail.com" - "s214target@gmail.com"
- [192.168.2.100](http://192.168.2.100)

# XSRF Countermeasure

- Use <https://mail.google.com> instead of <http://gmail.com>
- No other mail service has this option at all, as far as I know

# Application-Layer Denial of Service

# Application-Layer DoS

- Find small requests that consume a lot of server resources
- Application Crashing
- Data Destruction
- Resource Depletion
  - Memory
  - CPU
  - Bandwidth
  - Disk Space

# Resource Depletion Example

- CPU Consumption
  - On a large forum
  - Create a complicated regular expression search
  - Use a script to launch the search over and over

# Real-World Test

- Hacktics, a security company, brought down a large corporate network with just three laptops in an authorized test
  - Global company with branches in Israel, Europe and the USA
  - Internet Connectivity – 3x50Mbps lines with load balancing. ISPs provide Cisco (Riverhead) based Anti DDoS solutions
  - High security network, 30+ Web servers, backend servers, Mail Relay, databases

# Hacktics Results

- DoS was successful to all systems but one
- Two applications crashed completely after a few dozen requests only
- Most other applications stopped responding after 5-15 minutes of script execution from up to three laptops (though with most a single laptop was sufficient)
- Main cause of DoS was CPU exhaustion

# References

- Where the Web is Weak
  - [http://www.forbes.com/2008/05/14/web-hacking-google-tech-security08-cx\\_ag\\_0514webhack.html](http://www.forbes.com/2008/05/14/web-hacking-google-tech-security08-cx_ag_0514webhack.html)
- Application-Layer DDoS Attacks
  - [networks.rice.edu/papers/2006-04-Infocom-final.ppt](http://networks.rice.edu/papers/2006-04-Infocom-final.ppt)