security
iPhone Tracker

http://petewarden.github.com/iPhoneTracker/
obvious threats

Telnet
FTP
HTTP
MySQL
...

session hijacking

physical access
packet sniffing
session fixation
XSS
...

...
SSL

SSL Certificates
Secure data and transactions!
public-key crypto
Diffie-Hellman (DLP)

Alice
choose random A

agree on g,p

Bob
choose random B

\[ T_A = g^A \mod p \]

compute \( T_B^A \)

\[ T_B = g^B \mod p \]

compute \( T_A^B \)

agree on \( g^{AB} \mod p \)
Log in

You must have cookies enabled to log in to CS164.

Username: 
Password: 

☐ Remember my login on this browser (for a maximum of 30 days)

Log in
Log in

You must have cookies enabled to log in to CS164.

Username: 
Password: ' OR '1'='1

☐ Remember my login on this browser (for a maximum of 30 days)

Log in
$sql = sprintf("SELECT uid FROM users WHERE username='\%s' AND password='\%s'", $_POST["username"], $_POST["password"]);
SELECT uid FROM users WHERE username='' AND password='' OR '1'='1'
$sql = sprintf("SELECT uid FROM users WHERE username='\%s' AND password='\%s'", mysql_real_escape_string($_POST["username"]), mysql_real_escape_string($_POST["password"]));
SELECT uid FROM users WHERE username='\' AND password='\' OR \'1\'='\'1'
2. You then visit a bad guy’s website.
4. You unwittingly buy the penny stock!
CSRF

<img src="etrae.com/buy.php?symbol=INFX.PK">
<script src="etrae.com/buy.php?symbol=INFX.PK"></script>
<iframe src="etrae.com/buy.php?symbol=INFX.PK">
...

1. You click a link like


or, really,


2. vulnerable.com writes value of foo to its body.

3. badguy.com gets your cookies.
SEAS Design Fair
Tue 5/1, 11am - 4pm
the end