

Computer Security (or: The Worst Internet Security Blunders, and What You Can Learn From Them)

David Wagner

i206, April 12, 2012

How Email Works



sender



recipient

```
MAIL FROM: <daw@cs.berkeley.edu>  
RCPT TO: <hearst@ischool.berkeley.edu>  
DATA  
Subject: A good one
```

```
Hey, Marti, have you heard the one about why all  
good computer programmers like Shakespeare?  
Because 2B OR NOT 2B = FF. Ha ha ha!
```

```
-- David
```

```
.
```

Demo

Important Ethics Note

- We will be discussing attacks in this class.

This is not an invitation to undertake these attacks on your own.

- Attacking systems without the consent of all affected parties is unethical, contrary to UCB policy, and a possible violation of state and federal law. *Don't do it!*

Discussion

- What are the practical consequences of this vulnerability?
- What was the blunder?
- What lessons can we learn?

Web Security

- Next, let's look at security on the web.

How the Web Works



browser

GET /index.html HTTP/1.0



web server

<HTML><HEAD>...</HEAD><BODY><P>Welcome! ...



How the Web Works



browser

GET /addcomment?msg=Hi%20mom! HTTP/1.0



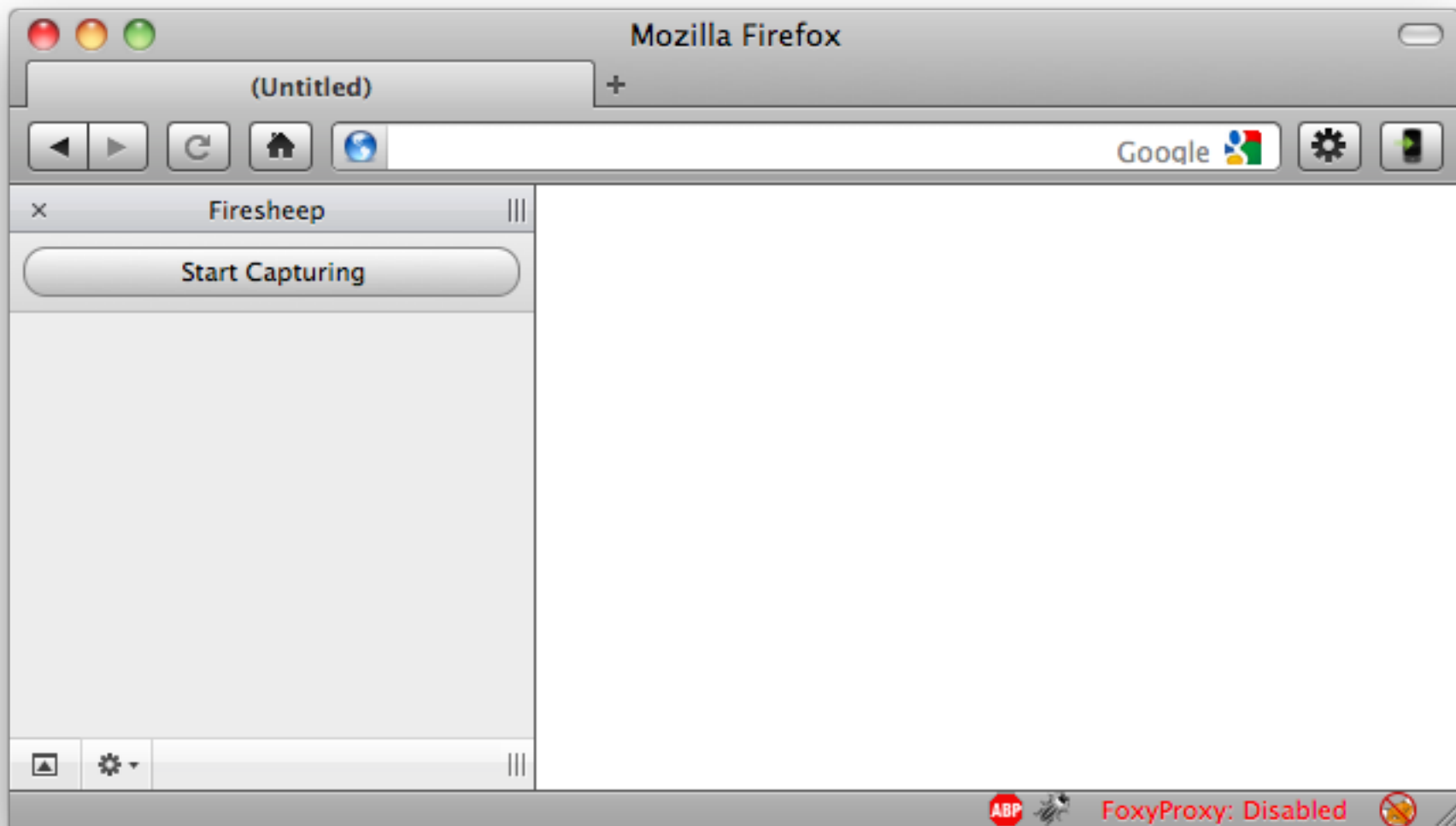
web server

<HTML> ...

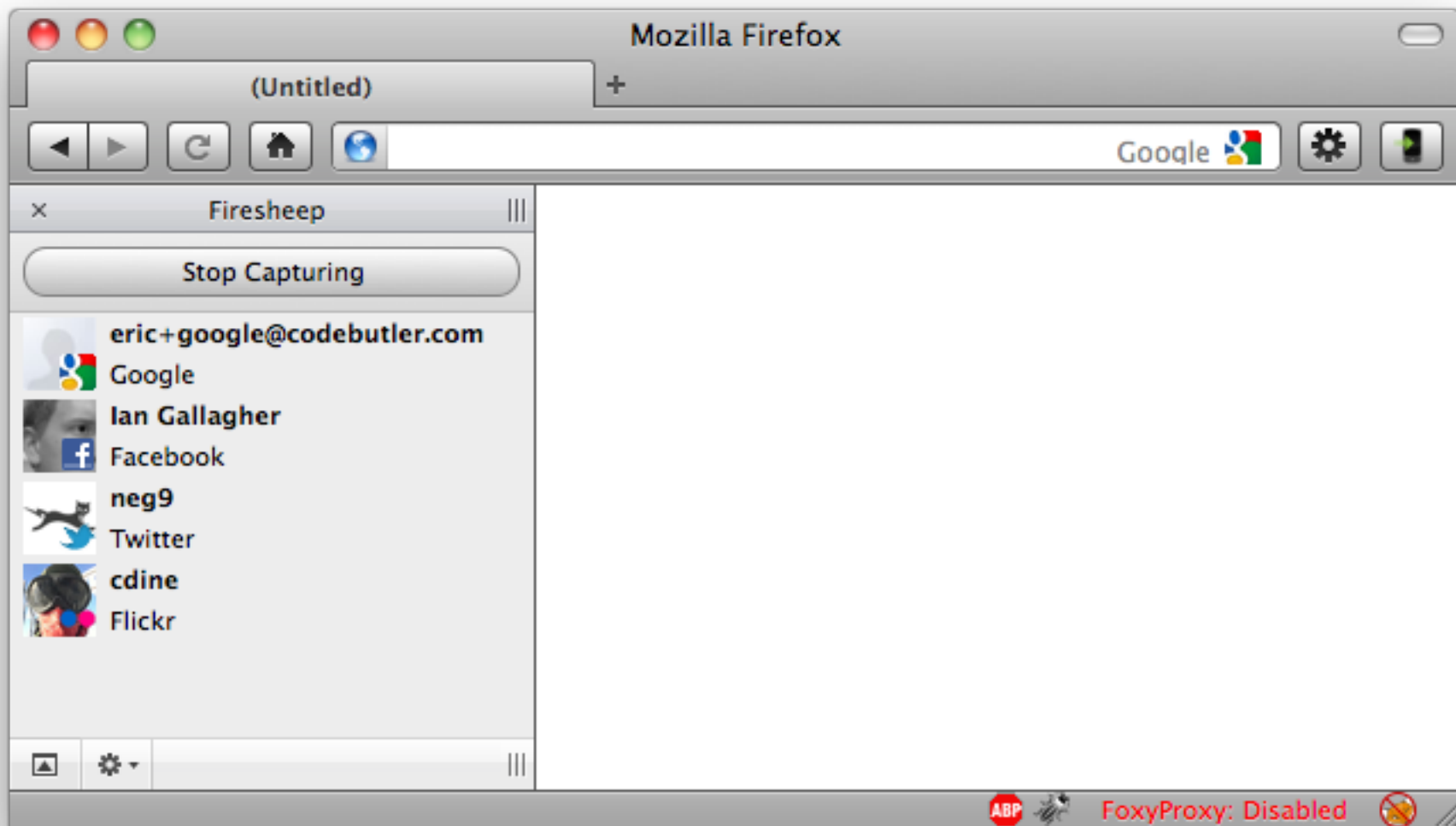


Demo

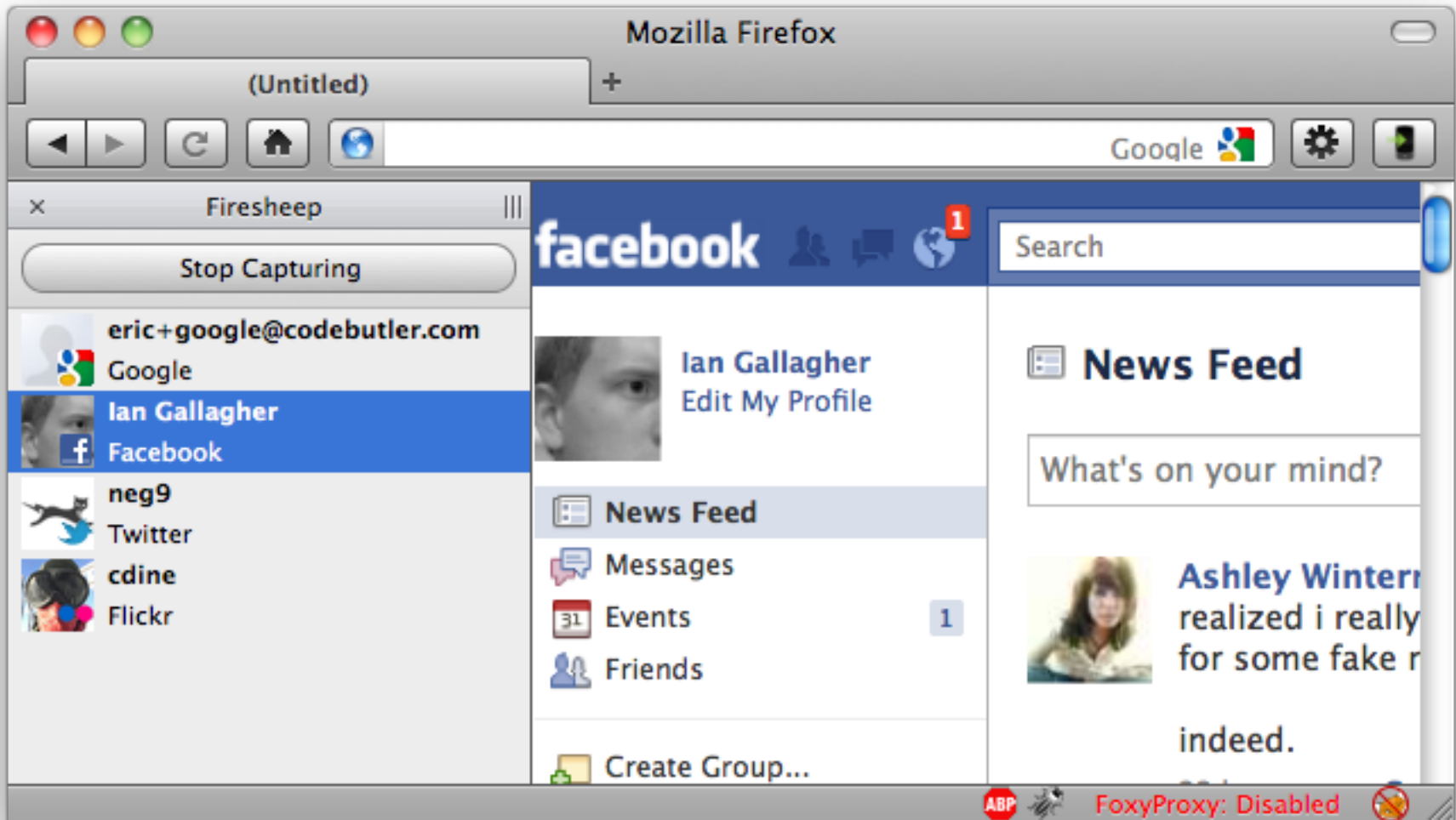
Firesheep



Firesheep



Firesheep



Stop Capturing

- kazabyte
- Wayne Yamamoto
- sagewiz
- Maria Orlova
- admin@charityblossom.org
- wayne_yamamo...
- skr325@gmail.com
- Rafael Montilla
- mrgall@mrgall.com
- fabioricotta@gmail.com
- MrGALL
- Chris Crowe
- jeremiahcitires
- LarrySwansonLMP@gmail.com
- Adrian Hall
- Merry Morud
- mrgall@mrgall.com
- Roy R Reyer
- foreclosuredataonlinecom@gmail.com
- seriocomic
- Wordpress (www.seriocomic.com)



Secure Connection Failed

An error occurred during a connection to linode.mrgall.com.
 SSL received a record that exceeded the maximum permissible length.
 (Error code: ssl_error_rx_record_too_long)

- The page you are trying to view can not be shown because the authenticity of the received data could not be verified.
- Please contact the web site owners to inform them of this problem. Alternatively, use the command found in the help menu to report this broken site.

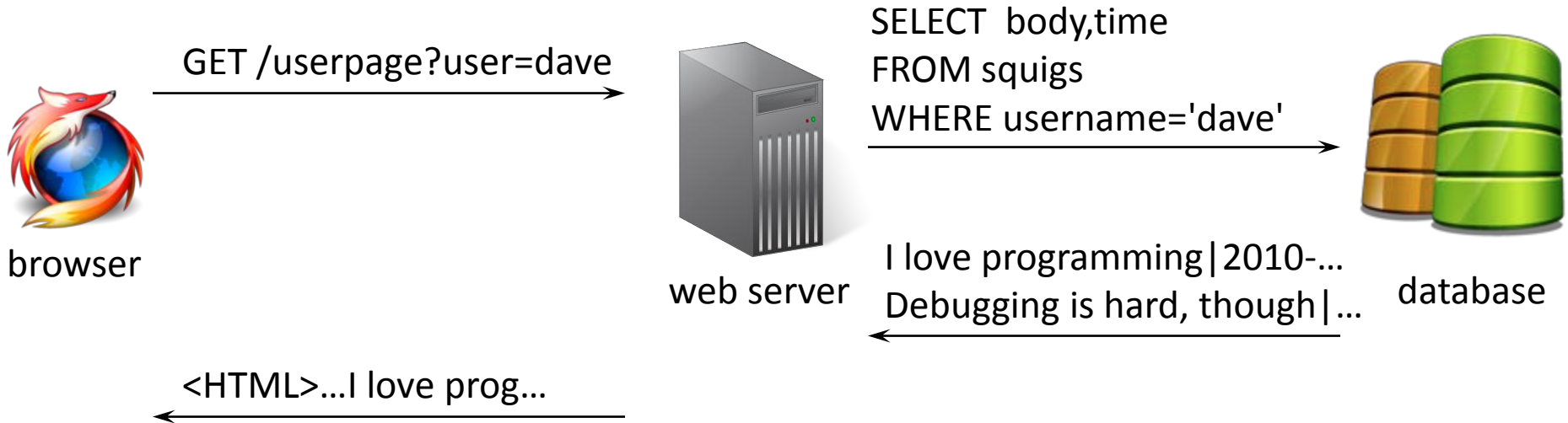
Try Again

What's the solution?

More demo

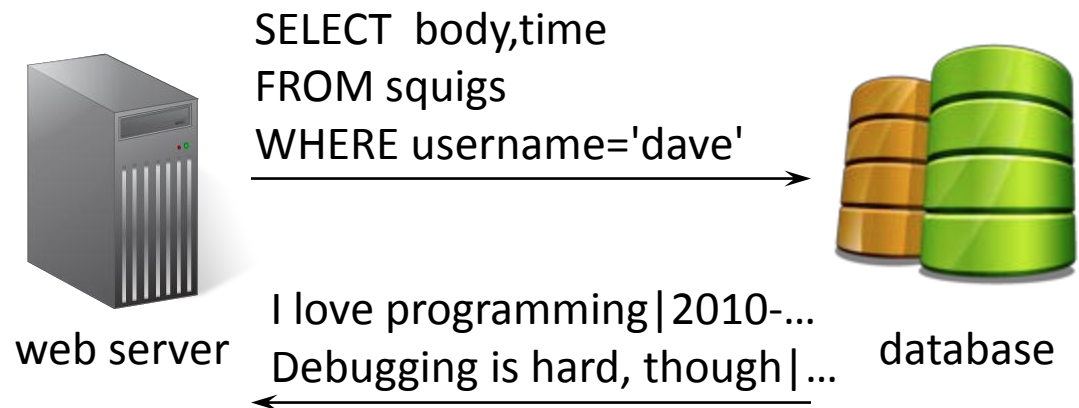


How the Web Works: Databases

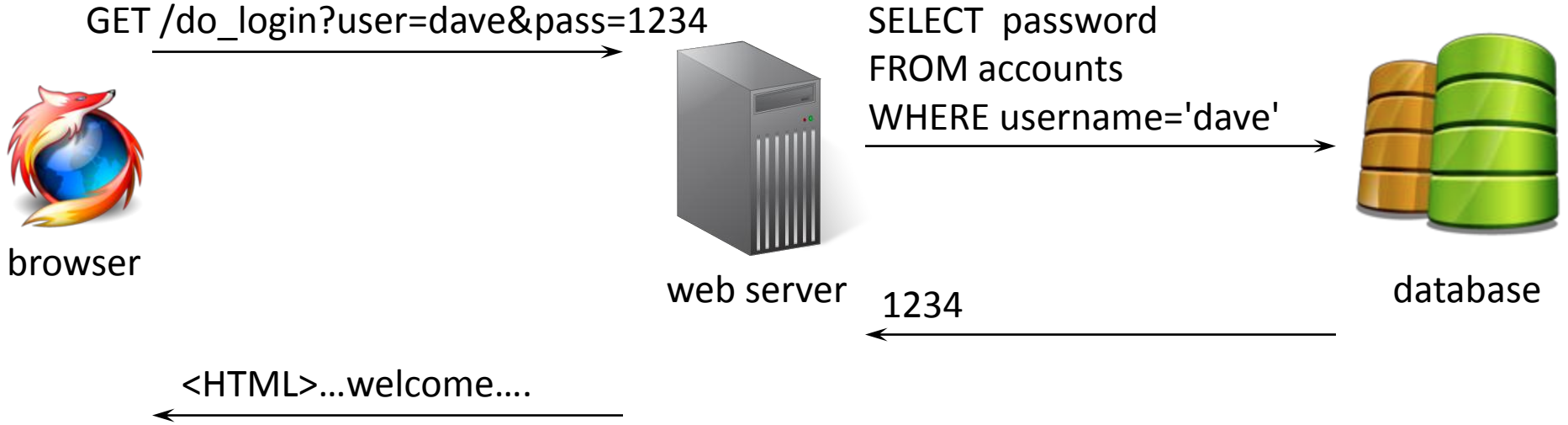


What the web server code looks like

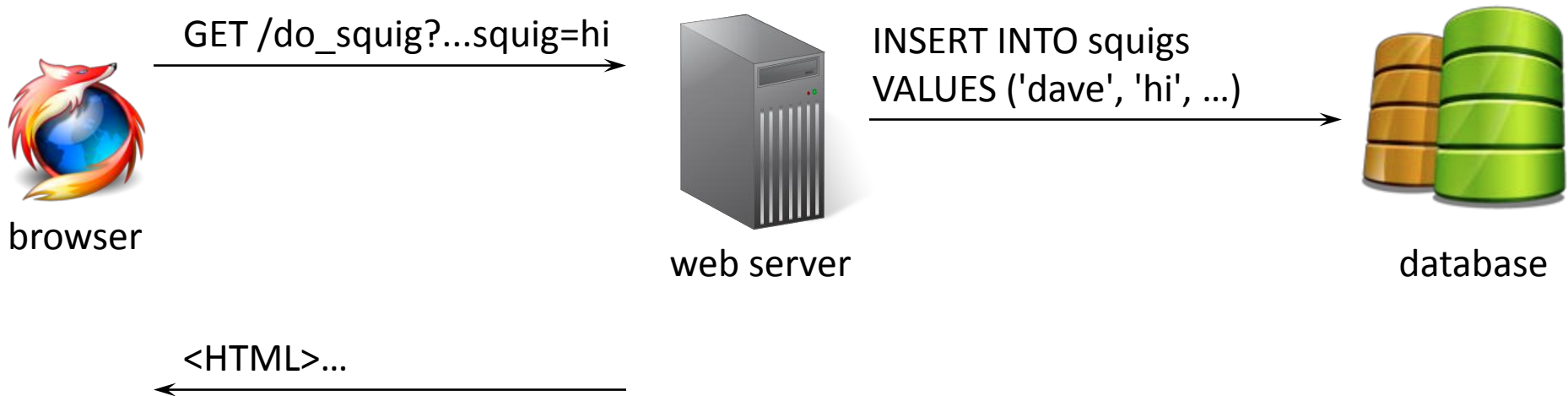
```
def get_squigs(user):  
    conn = ...  
    s = "SELECT body,time FROM squigs  
        WHERE username='%s'" % user  
    return conn.execute(s).fetchall()
```



Logging in



Posting a new squig



What the web server code looks like

```
def post_squig(user, squig):  
    conn = ...  
    s = "INSERT INTO squigs VALUES  
        ('%s', '%s', ...)" % (user, squig)  
    conn.execute(s)
```



web server

INSERT INTO squigs
VALUES ('dave', 'hi', ...)



database

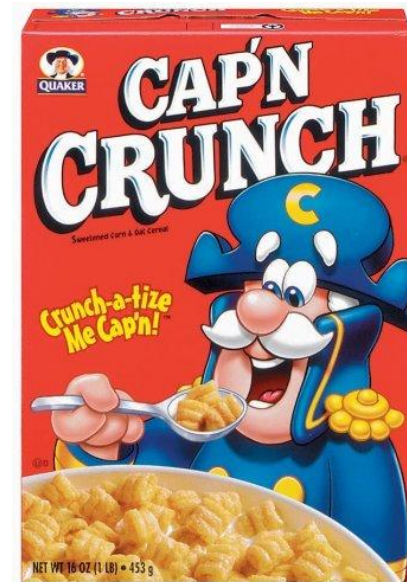
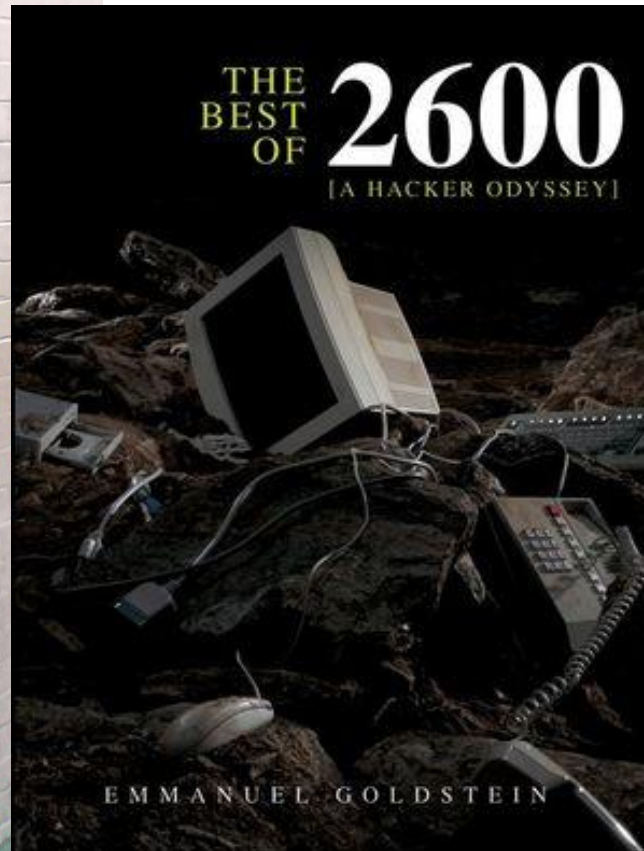
Examples

Squig SQL .

hi ... VALUES ('dave', 'hi', ...)

I'm good ... VALUES ('dave', 'I'm good', ...)

Hacking payphones (1960's)



Examples

Squig SQL .

hi ... VALUES ('dave', 'hi', ...)

I'm good ... VALUES ('dave', 'I'm good', ...)

I' || 'm go ... VALUES ('dave', 'I' || 'm go', ...)

I' || (SELECT...) || 'm

... VALUES ('dave', 'I' || (SELECT...) || 'm', ...)

Demo



SQL Injection Hack Infects 1 Million Web Pages

SANS warns of uptick in 'Lilupophilupop' attack, but Cisco said total number of infected Web pages likely lower.

By **Kelly Jackson Higgins**, Dark Reading

January 05, 2012 01:55 PM

Another SQL injection campaign is literally going viral, with some 1 million URLs possibly infected.

The SANS Internet Storm Center [over the weekend counted some 1,070,000 URLs](#) injected with the so-called lilupophilupop.com malware. That's up from 80 pages it had found in early December, according to SANS ISC handler Mark Hofman.

HI, THIS IS
YOUR SON'S SCHOOL.
WE'RE HAVING SOME
COMPUTER TROUBLE.



OH, DEAR - DID HE
BREAK SOMETHING?

IN A WAY-



DID YOU REALLY
NAME YOUR SON
Robert'); DROP
TABLE Students;-- ?



OH, YES. LITTLE
BOBBY TABLES,
WE CALL HIM.

WELL, WE'VE LOST THIS
YEAR'S STUDENT RECORDS.
I HOPE YOU'RE HAPPY.



AND I HOPE
YOU'VE LEARNED
TO SANITIZE YOUR
DATABASE INPUTS.

Discussion

- What are the practical consequences of this vulnerability?
- What was the blunder?
- What lessons can we learn?

Solution

- Use library functions that are designed for security
- Avoid mixing untrusted data with trusted control stuff

Top Internet Security Blunders

- Unencrypted email => spam, phishing
- Unencrypted web => man-in-the-middle attacks
- Mixing data and control => Vulnerable web sites

Some defenses


- Don't trust input from untrusted sources
- Use input validation: Check that inputs have the expected form
 - Check against a whitelist of known-good characters, not a blacklist of known-bad stuff
- Authenticate users
- Ensure all access attempts are checked to see whether they are authorized
- Encrypt data sent over the network

To learn more...

- Check out CS 161 (Computer Security)
- <http://security.stackexchange.com/>

Bonus Slides



 Bradesco

Tarifas de
Serviços Bancários

Preço Fixo

Preço Fixo de 100,00



Multi Expresso





Bradesco

Tarifas de
Serviços Bancários.

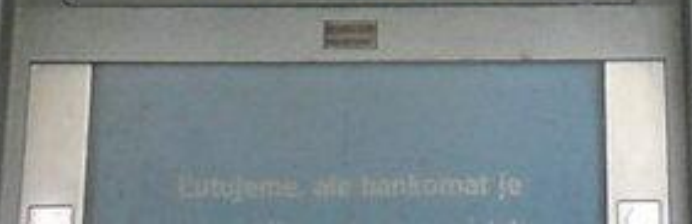
Pessoa Física

Mul

ML



Handwritten text on the right wall of the ATM enclosure, including the word "Cajero" and some illegible numbers and characters.



Handwritten text on the right wall, possibly a date or time: 100-700-500

Lessons

- Need mutual authentication (both parties authenticate each other)







RAPTORS
AHEAD
CAUTION

AMINO
DIVERSITY

MARSH

10000
10000
10000
10000



TRAPPED
IN SIGN
FACTORY



SEND
HELP!



Lessons

- Don't rely upon security through obscurity