

# 14. Attacking the Web II (plus more on how it works)

Blase Ur and David Cash  
February 10<sup>th</sup>, 2021  
CMSC 23200 / 33250



THE UNIVERSITY OF  
CHICAGO

# Very Basic MySQL

- Goal: Manage a database on the server
- Create a database:
  - `CREATE DATABASE cs232;`
- Delete a database:
  - `DROP DATABASE cs232;`
- Use a database (subsequent commands apply to this database):
  - `USE cs232;`

# Very Basic MySQL

- **Create a table:**

- `CREATE TABLE potluck (id INT NOT NULL PRIMARY KEY AUTO_INCREMENT, name VARCHAR(20), food VARCHAR(30), confirmed CHAR(1), signup_date DATE);`

- **See your tables:**

- `SHOW TABLES;`

- **See detail about your table:**

- `DESCRIBE cs232;`

# Very Basic MySQL

- **Create a table:**

- `INSERT INTO `potluck`  
(`id`,`name`,`food`,`confirmed`,`signu  
p_date`) VALUES (NULL, 'David  
Cash', 'Vegan Pizza', 'Y', '2020-01-  
27');`

- **See detail about your table:**

- `UPDATE `potluck` SET `food` = 'None'  
WHERE `potluck`.`name` = 'David  
Cash';`

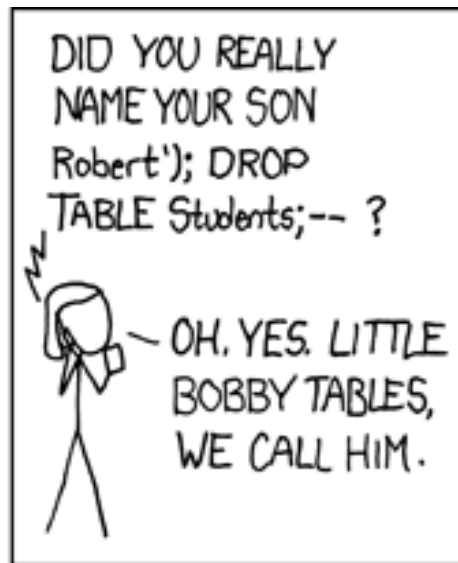
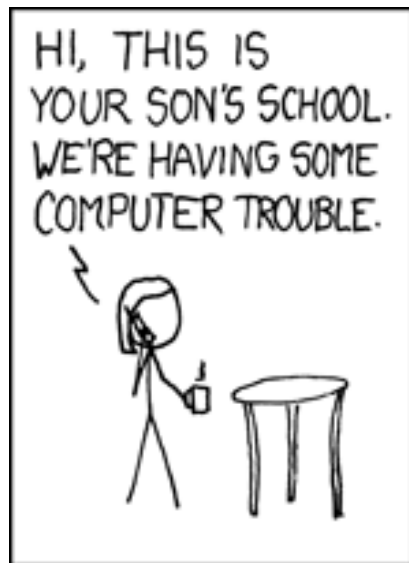
- **Get your data:**

- `SELECT * FROM potluck;`

# SQL Injection

- Goal: Change or exfiltrate info from *victim.com*'s database
- Main idea: Inject code through the parts of a query that you define

# SQL Injection



# SQL Injection

- Prerequisites:
  - Victim site uses a database
  - Some user-provided input is used as part of a database query
  - DB-specific characters aren't (completely) stripped

# SQL Injection: How?

- Enter DB logic as part of query you impact
- Back-end query
  - `SELECT * FROM USERS WHERE USER=' ' AND PASS=' ';`
- For username & password, attacker gives:
  - `' or '1'='1`
- Straightforward insertion:
  - `SELECT * FROM USERS WHERE USER=' ' or '1'='1' AND PASS=' ' or '1'='1';`



# SQL Injection: Why Does This Work?

- Database does what you ask in queries!

# SQL Injection: Key Mitigations

- Sanitize / escape user input
  - Harder than you think!
  - Different encodings
  - Use libraries to do this!
- **Prepared statements** from libraries handle escaping for you!
- Use PHP's mysqli (in place of mysql) with prepared statements
  - [https://www.w3schools.com/php/php\\_mysql\\_prepared\\_statements.asp](https://www.w3schools.com/php/php_mysql_prepared_statements.asp)

# Sending Data to a Server

- GET request
  - Data at end of URL (following “?”)
- POST request
  - Typically used with forms
  - Data *not* in URL, but rather (in slightly encoded form) in the HTTP request body
- PUT request
  - Store an entity at a location

# URL Parameters / Query String

- End of URL (GET request)
  - <https://www.cs.uchicago.edu/?test=foo&test2=bar>

The screenshot shows a web browser displaying the University of Chicago Department of Computer Science website. The address bar shows the URL `https://www.cs.uchicago.edu/?test=foo&test2=bar`. The page content includes the university logo, the text "Department of Computer Science", and a navigation menu with items: ABOUT, PEOPLE, RESEARCH, UNDERGRADUATE, GRADUATE, and ADMISSION. The browser's developer tools are open to the Network tab, showing a list of requests. The first request is highlighted, showing a 200 status, GET method, and a response size of 23.87 KB. The right-hand pane of the developer tools shows the "Params" tab for the selected request, displaying the query string parameters: `test: foo` and `test2: bar`.

Status	Method	F...	Domain	Cause	Type	Transferred	Size	0
200	GET	/?test=...	www.cs.uchi...	document	html	6.76 KB	23.87 KB	
302	GET	fonts.css	cloud.typogr...	stylesheet	css	154.58 KB	205.03 KB	
200	GET	main.cs...	www.cs.uchi...	stylesheet	css	cached	189.57 KB	
200	GET	moder...	www.cs.uchi...	script	js	cached	5.65 KB	
200	GET	jquery....	ajax.googlea...	script	js	cached	0 B	
200	GET	jquery-...	ajax.googlea...	script	js	cached	0 B	

Query string parameters:

- test: foo
- test2: bar

# Processing Data on the Server

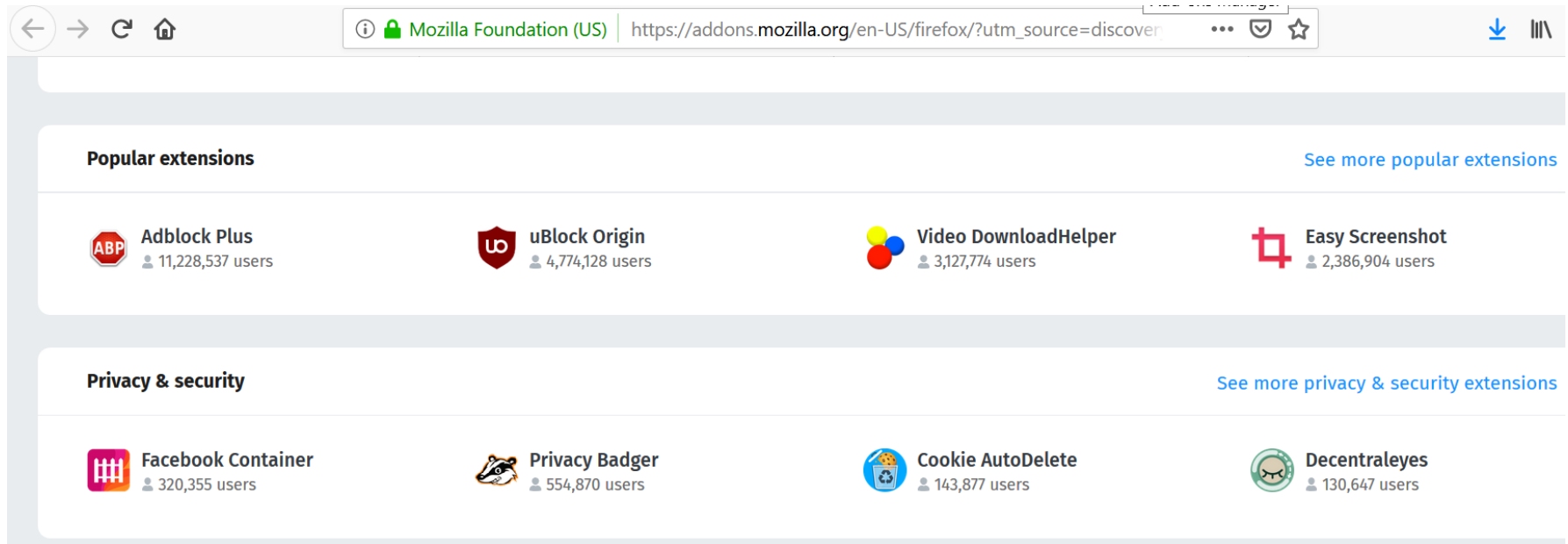
- Javascript is client-side
- Server-side you find Perl (CGI), PHP, Python (Django)
- Process data on the server
- What happens if this code crashes?

# Storing Data on the Server

- Run a database on the server
- MySQL, SQLite, MongoDB, Redis, etc.
- You probably don't want to allow access from anything other than *localhost*
- You definitely don't want human-memorable passwords for these

# Browser Extensions

- Can access most of what the browser can
- Requires permissions system
- Malicious extensions!



The screenshot shows the Mozilla Add-ons website. The browser address bar displays the URL: [https://addons.mozilla.org/en-US/firefox/?utm\\_source=discover](https://addons.mozilla.org/en-US/firefox/?utm_source=discover). The page is divided into two main sections: "Popular extensions" and "Privacy & security".

**Popular extensions** (See more popular extensions)

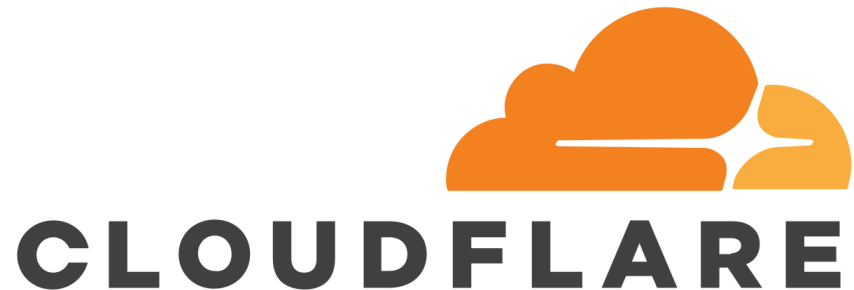
Extension Name	Users
Adblock Plus	11,228,537 users
uBlock Origin	4,774,128 users
Video DownloadHelper	3,127,774 users
Easy Screenshot	2,386,904 users

**Privacy & security** (See more privacy & security extensions)

Extension Name	Users
Facebook Container	320,355 users
Privacy Badger	554,870 users
Cookie AutoDelete	143,877 users
Decentraleyes	130,647 users

# What If You Get Lots of Traffic?

- CDNs (content delivery networks)





# What If You Don't Want To Code?

- CMS (content management system)
  - WordPress (PHP + MySQL), Drupal

The screenshot displays the WordPress dashboard interface. At the top, the site name 'Restaurant World Tou...' is visible, along with navigation links for 'Upgrade to Pro', 'New Post', and the user profile 'Dave'. The main dashboard area is titled 'Dashboard' and contains several widgets:

- Right Now:** A summary of site statistics.

CONTENT	DISCUSSION
8 Posts	9 Comments
1 Page	9 Approved
5 Categories	0 Pending
52 Tags	0 Spam
- QuickPress:** A form for creating a new post, including fields for 'Enter title here', 'Add Media', 'Tags (separate with commas)', and buttons for 'Save Draft', 'Reset', and 'Publish'.
- Storage Space:** Shows '3,072MB Space Allowed' and '0.08MB (0%) Space Used'.
- Recent Comments:** Lists comments from 'Dave' and 'Mandy' on a post titled 'Arctic Char #'. Dave's comment reads: 'Yes, it's a much less fishier fish than salmon. I've not heard of these two restaurants though. I'll have to ...'. Mandy's comment reads: 'I agree arctic char is a great fish! It's really similar looking to ...'.
- Recent Drafts:** States 'There are no drafts at the moment'.
- Stats:** States 'No stats are available for this time period.'