Input to your Website

• How does a user input information to your site?

• How does your server-side code process the input?

• How do you store the input?

• Does the input later appear on your site? Verbatim?
Status Updates

• What is a status update?

• Do you have any constraints on an update?

Lab Exercise

• Teams of 3

• Visit this website, and post a message!
  – http://intranet.cs.usna.edu/~nchamber/hack/it350-team3/bufftalk.pl
Lab Exercise

• Teams of 3

• Visit this website, and post a message!
  – http://intranet.cs.usna.edu/~nchamber/hack/bufftalk.pl

• Now break it.

Displaying User Content

** Dangerous, but necessary in all social media!

Bare Minimum Security Options
1. Check all strings for HTML tags, reject them
2. Replace < > characters with &gt; and &lt;
3. (need a lot more if databases are involved)
Injection: HTML vs Javascript

• HTML injection can ruin a page’s display, but not much else

• Javascript injection can *steal* information
  – It can read your cookies
  – Redirect to other (fake) websites
  – AJAX: ‘redirects’ *without the user knowing*

Lab Exercise

1. Inject Javascript, but do not break the page.
   – Why would a malicious hacker not want to visibly break it?

2. Find out what cookies are stored for the page

3. Inject Javascript to display the user’s name to the screen (“I see you X!!”).

Adapted from © 2004 Prentice Hall, Inc. All rights reserved.
Let’s just block <script>!!

- Easy enough: check all input strings for <script> and reject them

- Is that good enough?

Samy is my hero.

- MySpace during the heyday of MySpace: **2005**
- A 19 year old with too much time on his hands.

*Simple Javascript injection that eventually forced MySpace to shut its servers down.*
**MySpace Basics**

- MySpace has always been “customizable” from its early beginnings.
- You can submit biographical information as raw text, but HTML tags are allowed.
- Many tags are blocked, but CSS is fair game.

---

**Samy’s Original Goal**

*When someone visits your profile…*

1. The visitor sends Samy a friend request
   - Javascript sent a POST
2. The visitor adds text to his/her profile
   - “but most of all, Samy is my hero”
3. The visitor copies the javascript code to his/her profile
   - All visitors to their page will now repeat this process
Injecting into MySpace

• Already blocked:
  – <script>, onclick, onhover, onmouseover, …

• Some browsers allowed Javascript in CSS!
  – <div style="background:url('javascript:alert(1)')">

• The injection begins:
  <div id="mycode" expr="alert('hah!')" style="background:url('javascript:eval(document.all.mycode.expr)')">

• But MySpace blocked all “javascript” strings!
  – Insert an innocuous newline

  <div id="mycode" expr="alert('hah!')" style="background:url('java
  script:eval(document.all.mycode.expr)')">

Adapted from © 2004 Prentice Hall, Inc. All rights reserved.
Escaped Quotes Blocked

- MySpace stripped out escaped quotes \" and \'
- Solution?
  
  ```
  String.fromCharCode(34)
  ```

```html
<div id="mycode" expr="alert('double quote: ' + String.fromCharCode(34))"
style="background:url('javascript:eval(document.all.mycode.expr))">
</div>
```

Doing real damage

- Injection attacks are fun until the injection actually gets access to personal data.

- Samy accesses the user’s ID from the page itself.
  - `document.body.innerHTML`

- MySpace blocks “innerHTML” from input
  - Samy appends strings: `<document.body.inne` + `<rHTML>`
How do we add code to a profile?

• Goal: add “samy is my hero” and new javascript to the visitor’s own profile page

1. Grab your visitor’s unique ID.
2. Use AJAX to do a GET on the user’s personal profile.
3. Search the returned profile’s text for “heroes”
4. Use AJAX to do a POST to update the user’s profile

Summary

1. The visitor sends Samy a friend request
   – Javascript sent a POST
2. The visitor adds text to his/her profile
   – “Samy is my hero”
3. The visitor adds the entire javascript code to his/her profile
   – All visitors to their page will now repeat this process
What Happened (Oct 4, 2005)

• 12:34am posted code to his profile

• 1:30am 1 friend request
  – “One of my friends’ girlfriend looks at my profile. She’s obviously checking me out.”

• 8:35am 221 friend requests
  – “Woah”

• 10:30am 561 friend requests
  – “I’m getting messages from people pissed off”

• 1:30pm 6,373 friend requests

• 6:20pm 918,268 friend requests

• 20 hours: 1/35th of all of myspace

• 7:05pm MySpace shuts down
Aftermath

- **January 2007**: Samy pleads guilty to a felony computer hacking charge
- 3 year probation from touching a computer
- Now works for a security company
  - He discovered that iPhones sent GPS data back to Apple

- **Full technical details**: [http://namb.la/popular/tech.html](http://namb.la/popular/tech.html)

Adapted from © 2004 Prentice Hall, Inc.  All rights reserved.