Web Security
Historical Web

- Historically, the web was just a request response protocol
- HTTP is stateless, which means that the server essentially processes a request independent of prior history
- Envisioned as a way for exchanging information
Current Web

• Evolving into a platform for executing programs that support day-to-day tasks
• A lot of state needs to be maintained
• Distributed computation, and trust model
HTTP Requests

• A request has the form:

```plaintext
<METHOD> /path/to/resource?query_string HTTP/1.1
<header>*
</BODY>
```

• HTTP supports a variety of methods, but only two matter in practice:
  – **GET**: intended for information retrieval
    • Typically the BODY is empty
  – **POST**: intended for submitting information
    • Typically the BODY contains the submitted information
Structure of HTTP GET request

- **Connect to:** www.example.com
  - TCP Port 80 is the default for http, others may be specified explicitly in the URL.
- **Send:** GET /index.html HTTP/1.1
- **Server Response:**
  ```
  HTTP/1.1 200 OK
  Date: Mon, 23 May 2005 22:38:34 GMT
  Server: Apache/1.3.3.7 (Unix) (Red-Hat/Linux)
  Etag: "3f80f-1b6-3e1cb03b"
  Content-Length: 438
  Connection: close
  Content-Type: text/html; charset=UTF-8
  ```
GET with parameters

- GET /submit_order?sessionid=79adjadf888888768&pay=yes
  HTTP/1.1
- User inputs sent as parameters to the request
POST Requests

- Another way of sending requests to HTTP servers
- Commonly used in FORM submissions
- Message written in the BODY of the request
- Sending links with malicious parameter values is difficult when a web site accepts only POST requests.
- But a script running on a malicious web site can as easily send a POST request (as a GET request) to another web site.
HTTP Responses

• A response has the form

```
HTTP/1.1 <STATUS CODE> <STATUS MESSAGE>
<header>*
<BODY>
```

• Important response codes:
  – 2XX: Success, e.g. 200 OK
  – 3XX: Redirection, e.g. 301 Moved Permanently
  – 4XX: Client side error, e.g. 404 Not Found
  – 5XX: Server side error, e.g. 500 Internal Server Error
HTTP response

HTTP/1.1 200 OK
Date: Tue, 21 Oct 2014 16:21:44 GMT
Server: Apache/2.2.25 (Unix) mod_ssl/2.2.25 OpenSSL/1.0.1h PHP/5.2.17
Last-Modified: Tue, 21 Oct 2014 15:37:09 GMT
ETag: "3aaa5c-850-505f09ab7f211"
Accept-Ranges: bytes
Content-Length: 2128
Content-Type: text/html

<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html><head>
<title>Is The Internet On Fire?</title>
<meta http-equiv="content-type" content="text/html; charset=UTF-8">
<link rev="made" href="mailto:jschauma@netmeister.org">

<title>Is The Internet On Fire?</title>
<meta http-equiv="content-type" content="text/html; charset=UTF-8">
<link rev="made" href="mailto:jschauma@netmeister.org"
Cookies

• HTTP is stateless, therefore client needs to remember state and send this with every request
• Cookies are the common way of keeping state
  – Client:
    GET /index.html HTTP/1.1
  – Server:
    HTTP/1.1 200 OK
    Content-type: text/html
    Set-Cookie: sess-id=3773777adbdad

(content of page)
Cookies...

• Browsers send cookie with every subsequent request
  –GET /spec.html HTTP/1.1
    Host: www.example.org
    Cookie: sess-id=3773777adbdad

• Now server can look up stored state through sess-id

• Alternative to cookies: hidden form fields.
What Are Cookies Used For?

• Authentication
  – The cookie proves to the website that the client previously authenticated correctly

• Personalization
  – Helps the website recognize the user from a previous visit

• Tracking
  – Follow the user from site to site; learn his/her browsing behavior, preferences, and so on
Sessions

• As long as different users have different session identifiers (present in their cookies), the web server will be able to tell them apart
  – Regardless of their IP address

• When users delete their cookies, the browsers no longer send out the appropriate session identifier, and thus the web server “forgets” about them
Session Identifiers

• Long pseudo-random strings
• Unique per visiting client
• Each identifier is associated with a specific visitor
  – ID A → User A
• As sensitive as credentials (per session)
One missing piece

• We can create websites
• And we can have state, enabling us to have a personalized web
  – Banking, Email, Social networks, etc.

• But our pages are still static
  – The server sent some HTML, the browser drew it on the screen, and that’s it
JavaScript

• “The world’s most misunderstood programming language”
• Language executed by the Web browser
  – Scripts are embedded in webpages
  – Can run before HTML is loaded, before page is viewed, while it is being viewed, or when leaving the page
• Used to implement “active” webpages and Web applications
• A potentially malicious webpage gets to execute some code on user’s machine
JavaScript History

• Developed by Brendan Eich at Netscape
  – Scripting language for Navigator 2
• Later standardized for browser compatibility
  – ECMAScript Edition 3 (aka JavaScript 1.5)
• Related to Java in name only
  – Name was part of a marketing deal
  – “Java is to JavaScript as car is to carpet”
• Various implementations available
  – SpiderMonkey, RhinoJava, others
Aside: Java Security

• With binary code, memory and type safety issues complicate the problem of untrusted code

• Java and Javascript rely on safe languages
  • avoid low-level issues arising in C, C++ and binary code
    • No buffer overflows.
  • code can be created and executed only through sanctioned pathways, e.g., class loader
  • access-control restrictions associated with classes will be strictly and fully enforced
    • Can’t circumvent public/private restrictions by casting etc.
Java Vs JavaScript

• Java originally developed to support “active web pages”
  • Applets were intended to allow local execution of untrusted code
  • Security was achieved by restricting access to local resources, e.g., files

• Drawbacks
  • did not provide good integration with the browser environment
  • focus was more on (OS) integrity rather than confidentiality
  • these factors led to the development of Javascript
  • Today, Adobe flash is closer in many ways to Java than Javascript
Java Vs JavaScript

• Javascript takes a different approach
  • Language safety is still the basis
  • Use this basis to provide safe interface to the browser environment
  • The security model is object-oriented
  • What are the browser resources, which ones are accessible to untrusted code

• Browser is the platform, not the underlying OS
• It is not about whether untrusted code can access local files, but whether the browser permits it to do so ("trusted dialogs")
• Cookie-based model of browser security evolved in conjunction with Javascript, leading to excellent support for the same.
Common Uses of JavaScript

• Page embellishments and special effects
• Dynamic content manipulation
• Form validation
• Navigation systems
• Hundreds of applications
  – Google Docs, Google Maps, dashboard widgets
    in Mac OS X, Philips universal remotes ...
JavaScript in Webpages

• Embedded in HTML as a `<script>` element
  – Written directly inside a `<script>` element
    • `<script>` alert("Hello World!") `</script>`
  – In a file linked as `src` attribute of a `<script>` element
    `<script type="text/JavaScript" src="functions.js"></script>`

• Event handler attribute
  `<a href="http://www.yahoo.com" onmouseover="alert('hi');">`

• Pseudo-URL referenced by a link
  `<a href="javascript: alert(‘You clicked’);">Click me</a>`
Document Object Model (DOM)

• HTML page is structured data
• DOM is object-oriented representation of the hierarchical HTML structure
  – Methods: `document.write(document.referrer)`
    • These change the content of the page!
• Also Browser Object Model (BOM)
  – `Window`, `Document`, `Frames[]`, `History`, `Location`, `Navigator` (type and version of browser)
Browser and Document Structure

- **navigator object**
- **window object**
- **frame object**
- **document object**
- **<p> paragraph object**
- **<h2> heading object**
Reading Properties with JavaScript

Sample script

1. document.getElementById('t1').nodeName
2. document.getElementById('t1').nodeValue
3. document.getElementById('t1').firstChild.nodeName
4. document.getElementById('t1').firstChild.firstChild.nodeName
5. document.getElementById('t1').firstChild.firstChild.nodeValue

- Example 1 returns "ul"
- Example 2 returns "null"
- Example 3 returns "li"
- Example 4 returns "text"
  - A text node below the "li" which holds the actual text data as its value
- Example 5 returns " Item 1 "

Sample HTML

```html
<ul id="t1">
  <li>Item 1</li>
</ul>
```
Page Manipulation with JavaScript

• Some possibilities
  – createElement(elementName)
  – createTextNode(text)
  – appendChild(newChild)
  – removeChild(node)

• Example: add a new list item

```javascript
var list = document.getElementById('t1')
var newitem = document.createElement('li')
var newtext = document.createTextNode(text)
list.appendChild(newitem)
newitem.appendChild(newtext)
```

Sample HTML

```html
<ul id="t1">
  <li>Item 1</li>
</ul>
```
All the functional pieces are in place

• Now we can create personalized and dynamic websites. Yay!

• But what about security?
  – How do we stop websites from snooping around in each other’s business?
Goals of Web Security

• Safely browse the Web
  – A malicious website cannot steal information from or modify legitimate sites or otherwise harm the user...
  – ... even if visited concurrently with a legitimate site - in a separate browser window, tab, or even iframe on the same webpage

• Support secure Web applications
  – Applications delivered over the Web should have the same security properties we require for standalone applications (what are these properties?)
All of These Should Be Safe

• Safe to visit an evil website

• Safe to visit two pages at the same time

• Safe delegation
Web Security Concerns

- Web Security is concerned with ensuring the following 3 properties for web applications:
  - **Authentication**: securely identify users on top of HTTP, which is a stateless protocol.
  - **Confidentiality**: protect any sensitive data that websites serve to the browser from other websites, and the user's own sensitive data outside the browser from any website.
  - **Integrity**: ensure that the data and the code served to users cannot be tampered with.
HTTP Request Authentication

• HTTP is stateless, so web apps have to associate requests with users themselves
  – HTTP authentication: username/passwd automatically supplied in HTTP header
  – Cookie authentication: credentials requested in form, after POST app issues session token
    • Browser returns session cookie for each request
  – Hidden-form authentication: hidden form fields transfer session token
• Http & cookie authentication credentials are cached, so they don’t have to be supplied with each request
HTTP is a stateless protocol.

- User Authentication: Use cookies and send them implicitly for convenience.
- Server Authentication: SSL + Certification Authorities
Lifetime of Cached Cookies and HTTP Authentication Credentials

• Temporary cookies cached until browser shut down, persistent ones cached until expiry date

• HTTP authentication credentials cached in memory, shared by all browser windows of a single browser instance

• Caching depends only on browser instance lifetime, not on whether original window is open
Confidentiality (Browser)

- No mutual trust among parties.
- Confidentiality through Isolation: Same-Origin Policy (SOP)
  - Partition the Web into domains and isolate sensitive data such as cookie, network data and DOM nodes.
Confidentiality Example

• If there are no restrictions, securitee.org could use the DOM to dive into https://www.cs.stonybrook.edu/members-only and
  1. Extract details
  2. Make requests in the name of the user
  3. Inspect the responses
My name is Nick Nikiforakis and I am an Associate Professor of Computer Science at Stony Brook University.

While I am interested in all sorts of practical scientific problems, my interests are currently focused on computer security and privacy. I am most interested in developing new and practical solutions to existing problems, both for computer systems, as well as for the greater good of society.
The SOP partitions the web into domains (according to their DNS origin) and isolates sensitive data from scripts running in other domains.

What is sensitive data?
- Cookies
- Web page content (DOM isolation)
- Web site response (Network isolation)
SOP: Cookie Isolation

- Each domain has its own set of independently managed cookies, and these are embedded only in requests to the same domain.
- Only scripts running from the same domain and responses from the same domain can read and write cookies
- HTTP-Only cookies
SOP: Page content isolation

- Basic unit of isolation in a browser is a `<frame>`
  - `document.write` – refers to the current frame

- DOM Isolation
  - Scripts only have access to DOM elements on the same domain.
  - Frames embedded in a page are part of the DOM tree of the parent, but the policy still applies:
    - `document.frames[0].title`
  - Only accessible if the parent is from the same origin.
Domains vs Subdomains

• Subdomains
  – E.g. `private.example.com` vs `forum.example.com`
  – Considered different origin
  – Possibility to relax the origin to `example.com` using `document.domain`
  – Possibility to use cookies on `example.com`

• Completely separate domains
  – E.g. `private.example.com` vs `exampleforum.com`
  – Considered different origin, without possibility of relaxation
  – No possibility of shared cookies
SOP: Network isolation

- Script can send requests to arbitrary sites
- But scripts cannot read responses from any server
  - They can still send blind requests to other domains.
  - Is it safe for a malicious script to issue a request if it cannot read the response?
  - CSRF (discussed later)
- Exception: XmlHttpRequests permit a script to read from its origin server
Embedding and SOP: Caveats

- For embedded content, origin of the content may be different from the domain used for SOP checks
  - Scripts retrieved from B and embedded in A run with A privileges.
  - Akin to user A running an executable written by B in a UNIX environment.
    - Cross-site scripting attacks exploit this!
    - as do script inclusion attacks!
- Plugins implement their own SOP-like policies.
  - Flash keeps its server origin.
Same-Origin Policy: Exceptions

- Some resources are not considered sensitive and can be accessed across domains
- Browser History: CSS allows website to use different rules for visited and unvisited links.
- CSS rules: they can be read even when importing a cross-origin stylesheet
- Unsurprisingly, two attacks use these exceptions for information leaks
- Cross-origin CSS and CSS history hacks exploit these exceptions
Limitations of SOP

- A very rigid policy that imposes an all-or-nothing approach:
- The developer can embed the resource (allow all) or open it in an iframe (allow none).
- Cannot import script libraries without trusting them blindly.
Mashup

- A highly dynamic web application that embeds resources from different web applications to combine data and create new services.
Coping with SOP Limitations

- How to interact with cross-origin resources?
  - Network requests:
    - CORS (Cross-Origin Request Sharing)
  - JavaScript access: postMessage API
    - Allows interaction through a generic message-passing interface.
    - Suited to access components with a limited interface.

- Other alternatives for cross-origin script interaction
  - Embed scripts from other origin, but enforce policies to ensure security
    - Example: AdJail, AdSafe, FBJS
  - Technically feasible for full Javascript, but policy specification is difficult
  - Lighter-weight solutions possible if user is restricted to a subset of Javascript
Confidentiality (OS)

- Users do not trust the websites they visit.
- Again: Confidentiality through Isolation
- Sandboxing: only expose a safe API to web application that limits their interaction with the operating system
Integrity

- Network data integrity: HTTPS/DNSSEC
  - Also used to authenticate the server (e.g. Banks) and ensure network confidentiality.
  - Public-key protocol used to establish a session key to encrypt traffic.
- Browser data integrity: SOP
  - Think of integrity as write access on confidential resources. SOP protects from read as well as write accesses
Despite the same origin policy

• Many things can go wrong at the client-side of a web application

• Popular attacks
  – Cross-site Scripting
  – Cross-site Request Forgery
  – Session Hijacking
  – Session Fixation
  – SSL Stripping
  – Clickjacking
Weaknesses Leading to Attacks

- Trusting embedded content
  - Embedded scripts have same privilege as surrounding page (XSS)
  - Embedded content can target browser flaws, e.g., buffer overflows
- Not restricting outgoing network requests
  - Unauthorized requests to third-party sites (CSRF)
  - Include trusted party content in a frame
    - Abuse trust in third party, e.g., to improve odds of successful phishing
    - Clickjacking
  - Attacking third-party sites, e.g., portscanning or launching exploits
  - Ease of leaking sensitive data acquired (e.g., send cookie to attacker)
- Allowing Turing-complete computation for arbitrary sites
  - Bitcoin mining
  - Side-channel attacks
  - JIT-ROP attacks
- Weaknesses in lower layers
  - In-network attacks, e.g., man-in-the-middle
  - DNS compromise
- Application development environments that blur trust boundaries
  - Trusting client-side: browser and/or scripts running on a web page (Parameter tampering, ...)
- Good old application logic or implementation vulnerabilities
  - SQL injection, command injection, HTTP parameter pollution, ...
Two Sides of Web Security

• Web browser
  – Responsible for securely confining Web content presented by visited websites

• Web applications
  – Online merchants, banks, blogs, Google Apps …
  – Mix of server-side and client-side code
    • Server-side code written in PHP, Ruby, ASP, JSP… runs on the Web server
    • Client-side code written in JavaScript… runs in the Web browser
  – Many potential bugs: XSS, CSRF, SQL injection
Where Does the Attacker Live?

Browser

Malware attacker

Network attacker

website

Web attacker
Web Threat Models

• Web attacker
• Network attacker
  – Passive: wireless eavesdropper
  – Active: evil Wi-Fi router, DNS poisoning
• Malware attacker
  – Malicious code executes directly on victim’s computer
  – To infect victim’s computer, can exploit software bugs (e.g., buffer overflow) or convince user to install malicious content (how?)
    • Masquerade as an antivirus program, video codec, etc.
Web Attacker

• Controls a malicious website (attacker.com)
  – Can even obtain an SSL/TLS certificate for his site ($0)
• User visits attacker.com – why?
  – Phishing email, enticing content, search results, placed by an ad network, blind luck …
  – Attacker’s Facebook app
• Attacker has no other access to user machine!
• Variation: “iframe attacker”
  – An iframe with malicious content included in an otherwise honest webpage
    • Syndicated advertising, mashups, etc.
Dangerous Websites

• Microsoft’s 2006 “Web patrol” study identified hundreds of URLs that could successfully exploit unpatched Windows XP machines
  – Many interlinked by redirection and controlled by the same major players

• “But I never visit risky websites”
  – 11 exploit pages are among top 10,000 most visited
  – Trick: put up a page with popular content, get into search engines, page then redirects to the exploit site
    • One of the malicious sites was providing exploits to 75 “innocuous” sites focusing on (1) celebrities, (2) song lyrics, (3) wallpapers, (4) video game cheats, and (5) wrestling
Threat model 1: Web Attacker

• In these scenarios:
  – The server is benign
  – The client is benign
  – The attacker is either:
    • A website attacker (someone who can send you links that you follow and setup websites)
    • A network attacker (someone who is present on the network and can inspect and potentially modify unencrypted packets) (Passive/Active)
Attacks on Authentication

- CSRF and Clickjacking
  - Confused deputy attacks that cause the victim browser to send authenticated requests for the attacker's benefit
  - CSRF: Cross-site request forgery: attacker sends requests to another web site, impersonating browser user
  - Clickjacking: User intends to click on one link, but the browser recognizes a link on another site
    - Achieved using overlaid frames and by manipulating visibility related attributes
Cross-site Request Forgery (CSRF)

• Is an attack where the attacker tricks the browser into injecting a request into an authenticated session
  – E.g. by means of scripting
  – E.g. by means of remote resource inclusion

• Attacker can perform requests/operations in the name of the user
Cross-site Request Forgery (CSRF)

```html
<form method="POST" action="/changepass">
...
New Password: <input type="password" name="password">
</form>
```

- Browser makes the following request:
  ```
  GET http://www.example.site.com/changepass?password=newpassword HTTP 1.1
  ```
- Let’s say the application didn’t authenticate password change request using any means other than cookies
- An attacker can easily forge request!
- Attack works because (a) cookies are sent by default, and (b) SOP does not restrict cross-origin submissions
POST Example

- POST requests can also be forged
- Attacker lures the client to visit his/her web page

```html
<iframe name="hiddenframe" style="display:none">
<form method="POST" name="evilform" target="hiddenframe" action="http://wwwexamplesite.com/update_password">
  <input type="hidden" name="password" value="evilhax0r">
</form>
<script>document.evilform.submit();</script>
</iframe>
```
CSRF and Authentication status

• The classic CSRF attack abuses a user’s existing session cookies with a victim website
• Does that mean that CSRF is a non-issue when a user is logged out?
  • No! (although many still think “yes”)
  • In certain cases, an attacker can log in a victim with his credentials using an unprotected login form and still manage some sort of abuse
    • Login CSRF
Possible targets of CSRF

- Banks
  - Attacker can issue a request to transfer money from victim’s bank account to attacker’s
- E-commerce sites
  - Purchase items using victim’s account, ship to attacker
- Forums and Social network sites
  - Post articles using victim’s identity
- Home/Intranet firewall
  - Reconfigure firewall to permit connections from the Internet to a host behind the firewall
- Note that victim user’s location is exploited: the attacker (typically) cannot communicate with the firewall, but the user’s browser can.
CSRF Impacts

• Malicious site can’t read info, but can make write requests to our app!
• In Alice’s case, attacker gained control of her account with full read/write access!
Preventing CSRF

- HTTP requests originating from user action are indistinguishable from those initiated by attacker

- Need own methods to distinguish valid requests
  - Inspecting Referrer Headers
  - Validation via User-Provided Secret
  - Validation via Action Token
Inspecting Referer Headers

• Referer header specifies the URI of document originating the request

• Assuming requests from our site are good, don’t serve requests not from our site

• Unfortunately, Referrer information may be suppressed by browsers (or firewalls) for privacy reasons
Validation via User-Provided Secret

• Can require user to enter secret (e.g. login password) along with requests that make server-side state changes or transactions

• Example: The change password form could ask for the user’s current password

• Security vs convenience: use only for infrequent, “high-value” transactions
  – Password or profile changes
  – Expensive commercial/financial operations
Validation via Action Token

- Add special action tokens as hidden fields to “genuine” forms to distinguish from forgeries
- Need to generate and validate tokens so that malicious 3rd party can’t guess or forge token
  - Same-origin policy prevents 3rd party from inspecting the form to find the token
- This token can be used to distinguish genuine and forged forms
Clickjacking

Win a free iphone!
Just click on red and green!

Quick while the offer lasts!
So you click...

• Nothing happens.
  – Or something happens
  – But you don’t get that free iphone that you were promised

• Continue browsing

• Time to check email
  – Go to GMail
Where are my mails bro?!?

Your inbox is empty
Win a free iphone!
Just click on red and green!

Quick while the offer lasts!
Win a free iphone!
Just click on red and green!
Quick while the offer lasts!
What can be done?

• Websites that don’t want to be framed can say so...

• X-Frame-Options header
  – SAMEORIGIN;
  – Allow-from <uri>;
  – DENY;
Cross-Site Scripting (XSS)

• Different types of script injection
  – **Persistent**: stored data used in the response
  – **Reflected**: part of the URI used in the response
  – **DOM-based**: data used by client-side scripts

/http://www.example.com/search?q=<script>alert('XSS');</script>

<h1>You searched for<script>alert('XSS');</script></h1>
What can an attacker do with XSS?

• Long answer (non exhaustive):
  – Exfiltrate your cookies (session hijacking)
  – Make arbitrary changes to the page (phishing)
  – Steal all the data available in the web application
  – Make requests in your name
  – Redirect your browser to a malicious page
  – Tunnel requests to other sites, originating from your IP address (BEEF)

• Short demo:
  http://securitee.tk/files/search.php?a=hi
A web site vulnerable to XSS

- **Host:** www.vulnerable.site
  
  GET /welcome.cgi?name=value HTTP/1.0

- Displays name submitted in the web page

- Example
  
  GET /welcome.cgi?name=Joe%20Hacker HTTP/1.0
<HTML>
>Title>Welcome!</Title>
Hi Joe Hacker
<br>
Welcome to our system
...
</HTML>

• How can this be abused??
Reflected XSS Summary

• Attacker causes victim to click on maliciously crafted link
  • Typically contains a malicious script as a parameter
• request goes to vulnerable web site
• web site does not properly check its input
• returns a page that contains the malicious script
  • which operates with privileges of the vulnerable site can perform any action that the user can perform
  • send the cookie (or other private info) to the attacker
  • perform sensitive action, e.g., withdraw money
Attack details

• Above attack requires victim to click on attacker link
  • Easy way: use email messages with enticing information
    • victim clicks on link
  • Variation: Attacker provides scripting code as input to vulnerable web application
Persistent XSS

• Malicious script permanently stored on server
• Still requires
  • An attacker that causes the script to be stored
  • Script should be used in a page visited by victim user
• User totally unaware of the vulnerability/exploit
  • More stealthy, damaging and long-lasting
  • How can this be possible?
  • Think of a blog, or social networking web site: input from one user is rendered in the page shown to another
Preventing XSS

- Never send untrusted data to browser
- Such that data could cause execution of script
- Usually can just suppress certain characters

- We show examples of various contexts in HTML document as template snippets
- Variable substitution placeholders: % (var)
- evil-script; will denote what attacker injects
- Contexts where XSS attack is possible
General Considerations

- **Input Validation vs. Output Sanitization**
  - XSS is not just a input validation problem
  - Strings with HTML metachars not a problem until they’re displayed on the webpage
  - Might be valid elsewhere, e.g. in a database, and thus not validated later when output to HTML
  - Sanitize: check strings as you insert into HTML doc

- **HTML Escaping**
  - a.k.a entity reference encoding
    - & to &amp;
    - < to &lt;
    - > to &gt;
Most straightforward, common situation

Example Context:

Error: Your query '%(query)' did not return any results.

- Attacker sets `query = <script>evil-script;</script>`
- HTML snippet renders as

```
Error: Your query '<script>evil-script;</script>' did not return any results.
```

Prevention: HTML-escape untrusted data

Rationale: If not escaped
- `<script>` tags evaluated, data may not display as intended
Tag Attributes (e.g., Form field values)

- Contexts where data is inserted into tag attribute
- Attacker able to “close the quote”, insert script
- Example HTML Fragment:

```html
<form ...
<input name="city" value="%(city)"/>
<script>evil-script;</script>
</form>
```

- Attacker sets
  ```html
  city = xyz"<script>evil-script;</script>
  ```

- Renders as
  ```html
  <form ...>
  <input name="city" value="xyz">
  <script>evil-script;</script>
  </form>
  ```
More Attribute Injection Attacks

- **Image Tag:** `<img src=%(image_url)>`

- **Attacker sets** `image_url = http://www.example.com/ onerror=evil-script;`

- **After Substitution:** `<img src=http://www.example.com/ onerror=evil-script;>

  - **Lenient browser:** first whitespace ends `src` attribute
  
  - **onerror** attribute sets handler to be desired script
  
  - **Attacker forces error** by supplying URL w/o an image

  - **Can similarly use** `onload, onmouseover` **to run scripts**

  - **Attack string didn’t use** any HTML metacharacters!
URL Attributes (href and src)

- Dynamic URL attributes vulnerable to injection
- Script/Style Sheet URLs: `<img src="%(script_url)">
  - Attacker sets `script_url = http://hackerhome.org/evil.js`

- `javascript: URLS` - `<img src="%(img_url)">
  - By setting `img_url = javascript:evil-script;` we get `<img src="javascript:evil-script;">`
  - And browser executes script when loading image
Style Attributes

- Dangerous if attacker controls style attributes
  - Attacker injects:
  - Browser evaluates:

    ```html
    <div style="background: %(color)">I like colors.</div>
    ```
    
    ```javascript
    color = green; background-image: url(javascript:evil-script;)
    
    <div style="background: green; background-image: url(javascript:evil-script;)">I like colors. </div>
    ```

- In IE 6 (but not Firefox 1.5), script is executed!

- Prevention: whitelist through regular expressions
  - Ex: `^[a-z]+|[#0-9a-f]+$` specifies safe superset of possible color names or hex designation
In JavaScript Context

Be careful embedding dynamic content

- `<script>` tags or handlers (onclick, onload, ...)

Attacker injects:

```javascript
var msg_text = '%(msg_text)';
// do something with msg_text
</script>
msg_text = 'oops'; evil-script; //
```

And evil-script; is executed!
Another JavaScript Injection Example

- From previous example, if attacker sets

```html
msg_text = 'foo</script><script>evil-script;</script><script>
```

the following HTML is evaluated:

```html
<script>var msg_text = 'foo</script> 
<script>evil-script;</script>
<script>' // do something with msg_text</script>
```

- Browser parses document as HTML first
- Divides into 3 `<script>` tokens before interpreting as JavaScript
- Thus 1st & 3rd invalid, 2nd executes as evil-script
How would you stop this attack?

• Blacklisting
  – E.g. No <, >, script, document.cookie, etc.
  – Intuitively correct, but it should **NOT** be relied upon
• Whitelisting whenever possible
  – E.g. this field should be a number, nothing more nothing less
• Always escape user-input
  – Neutralize “control” characters for all contexts
• Content Security Policy
  – Whitelist for resources
  – Belongs in the “if-all-else-fails” category of defense mechanisms
Content Security Policy

• Example

Content-Security-Policy: default-src https://cdn.example.net; frame-src 'none'; object-src 'none'; image-src self;

• CSP is very powerful
  – Great if you are writing something from scratch
  – Not so great if you have to rewrite something to CSP
    • E.g. Convert all inline JavaScript code to files
Content Security Policy v2

• CSP was great in theory but still hasn’t caught up in practice

• CSP v2.0 supports two new features to help adopt CSP
  – Script nonces for inline scripts
  – Hashes for inline scripts
  – Read more here:
    • https://blog.mozilla.org/security/2014/10/04/csp-for-the-web-we-have/
Content Security Policy v2

Script nonces for inline scripts

[HTTP Header] Content-security-policy: default-src 'self'; script-src 'nonce-2726c7f26c'

[HTML] <script nonce="2726c7f26c">... </script>

Hashes for inline scripts

[HTTP Header] content-security-policy: script-src 'sha256-cLuU6nVzrYJIo7rUa6TMmz3nylPFrPQrEUpOHllb5ic='

[HTML] <script> ... </script>
Some browsers try to help by attempting to detect *reflected XSS* and stop them

- Internet Explorer was the first to introduce this
- Chrome followed a bit later, with a more complete approach that addressed some of IEs problems
  - Unfortunately, over the years, Chrome’s filter seems to have gone back on some of the improvements. Its filter stops fewer attacks than IE in our experiments
- Firefox invested in an XSS filter for some time, but then seems to have abandoned its efforts
  - PaleMoon, a Firefox clone, imported the XSS filter for Firefox developed at Stony Brook.
Browser XSS filters

Attempt 1: Use string (or regexp) matching to identify suspicious content within request parameters (NoScript)
Example: excise “<script>”, “data:”, etc. from parameters
Problem: High False Positives make it unsuitable for general use

Attempt 2: Filter only if suspicious parameter is reflected, i.e., its value appears in the HTML response (IE/Edge)
FPs can still be too high
Mitigate using very strict matching rules (IE/Edge, Chrome)
Unfortunately, this leads to false negatives and filter evasion

Attempt 3: Filter if suspicious reflected content is used in a dangerous context in the HTML response (Firefox filter)
Example: “data:” can safely appear outside HTML tags
In our filter, this reduces FPs sufficiently to enable use of approximate matching
Result: Evasion resistant XSS filtering
Script Inclusion

• What if an attacker can’t find an XSS vulnerability in a website
  – Can he somehow still get to run malicious JavaScript code?

• Perhaps... by abusing existing trust relationships between the target site and other sites
JavaScript libraries

• Today, a lot of functionality exists, and all developers need to do is link it in their web application
  – Social widgets
  – Analytics
  – JavaScript programming libraries
  – Advertising
  – ...
Remote JavaScript libraries

\[
\text{mybank.com}
\]

\[
\text{<html>}
\]

\[
\text{...}
\]

\[
\text{<script src=\texttt{http://www.foo.com/a.js}> </script>}
\]

\[
\text{...}
\]

\[
\text{</html>}
\]

- The code coming from \textit{foo.com} will be incorporated in \textit{mybank.com}, as if the code was developed and present on the servers of \textit{mybank.com}
Remote JavaScript libraries

- This means that if, foo.com, decides to send you malicious JavaScript, the code can do anything in the mybank.com domain

- Why would foo.com send malicious code?
  - Why not?
  - Change of control of the domain
  - Compromised
Timing attacks

• Because of the same-origin policy, scripts cannot access most resources in a cross-domain
  – Can still make the requests though, that’s why CSRF is a problem

• An attacker can still abuse the time it takes for a page to load, as a side-channel
Timing attacks

• Scenario: I want to know if you are logged-in to your Gmail
  – I may, or may not be able to load the page in an iframe, depending on the Xframe-options
  – Even if I can load it, I still can’t peek in it

• What if I try to load mail.google.com as an image?
  – `<img src="https://mail.google.com" onError="func()"/>
  – The browser will fetch the page with your cookies and then the parser will at some point throw an error that this is not an image
Timing attacks

• The size of a page is often dependent on whether you are logged in or not

• Hence, for a large image, the browser will take a longer time to give you an error

• Oversimplified attack:
  – Fast error: not-logged in
  – Slow error: logged-in
Getting one measurement

```html
<html><body><img id="test" style="display: none">
<script>
    var test = document.getElementById('test');
    var start = new Date();
    test.onerror = function() {
        var end = new Date();
        alert("Total time: " + (end - start));
    }
    test.src = "http://www.example.com/page.html";
</script>
</body></html>

Figure 3: Example JavaScript timing code

Code sample from: Exposing Private Information by Timing Web Applications
By Bortz et al.
Redirects, Cookies, and Header Injection

- Need to filter and validate user input inserted into HTTP response headers
- Ex: servlet returns HTTP redirect

```
HTTP/1.1 302 Moved
Content-Type: text/html; charset=ISO-8859-1
Location: %(redir_url)s

<html>
<head><title>Moved</title></head>
<body>Moved <a href='%(redir_url)s'>here</a></body>
</html>
```

- Attacker Injects: (URL-encodes newlines)

```
oops:foo\r\n\nSet-Cookie: SESSION=13af..3b;
domain=mywwwservice.com\r\n\n<script>evil()</script>
```
Threat Model 2: Network Attacker
Quiz:

• Suppose that a website only exists over HTTPS
  – E.g. paypal.com

• Does the website need to explicitly mark its session (or otherwise sensitive) cookies as “Secure”?
  – If yes, why yes?
  – If not, why not?
SSL Stripping

• Let’s say that a website exists only over HTTPS
  – No HTTP pages

• Two scenarios
  1. User types https://www.securesite.com and the browser directly tries to communicate the remote server over a secure channel
  2. User types http://www.securesite.com (or just securesite.com) and the site will redirect the user to the secure version (using an HTTP redirection/Meta header)
SSL Stripping

• Let’s say that a website exists only over HTTPS
  – No HTTP pages

• Two scenarios
  1. User types https://www.securesite.com and the browser directly tries to communicate the remote server over a secure channel
  2. User types http://www.securesite.com (or just securesite.com) and the site will redirect the user to the secure version (using an HTTP redirection/Meta header)
Normal page load
Page load when attacker is present
SSL Stripping

• Let’s say that a website exists only over HTTPS
  – No HTTP pages

• Two scenarios
  1. User types https://www.securesite.com and the browser directly tries to communicate the remote server over a secure channel
  2. User types http://www.securesite.com (or just securesite.com) and the site will redirect the user to the secure version (using an HTTP redirection/Meta header)
SSL Stripping

• Same thing can happen when sites deliver HTTPS-targeted forms over an HTTP connection (typically for performance or outsourcing purposes)

```html
<form action=https://example.com/login>
    <input .... username>
    <input .... password>
</form>
```
Defenses

• Use full-site SSL in combination with Secure cookie and HTTP-only Cookie

• HSTS: HTTP Strict Transport Security
  – Force the browser to always contact the server over an encrypted channel, regardless of what the user asks

HTTP Header

**Strict-Transport-Security**: max-age=31536000
Defenses

• What about the very first time you visit a website?
  – What if a MITM is located on your network and will therefore strip SSL and suppress HSTS?

• Answer:
  – Preloaded HSTS: Websites can ask browsers to mark them as HSTS in a special browser-vendor-updated database
Threat model 3: Malicious Client

• In these scenarios:
  – The server is benign
  – The client is malicious
    • The client can send arbitrary requests to the server, not bound by the HTML interfaces

• The attacker is after information at the server-side
  – Steal databases
  – Gain access to server
  – Manipulate server-side programs for gain
## OWASP Top 10

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>Injection</td>
</tr>
<tr>
<td>A2</td>
<td>Broken Auth and Session Management</td>
</tr>
<tr>
<td>A3</td>
<td>Cross-site Scripting</td>
</tr>
<tr>
<td>A4</td>
<td>Insecure Direct Object References</td>
</tr>
<tr>
<td>A5</td>
<td>Security misconfiguration</td>
</tr>
<tr>
<td>A6</td>
<td>Sensitive Data Exposure</td>
</tr>
<tr>
<td>A7</td>
<td>Missing function level access control</td>
</tr>
<tr>
<td>A8</td>
<td>Cross-site Request Forgery</td>
</tr>
<tr>
<td>A9</td>
<td>Using components with kn. vulnerabilities</td>
</tr>
<tr>
<td>A10</td>
<td>Unvalidated redirects and Forwards</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>A1</strong></td>
<td>Injection</td>
</tr>
<tr>
<td><strong>A2</strong></td>
<td>Broken Auth and Session Management</td>
</tr>
<tr>
<td><strong>A3</strong></td>
<td>Cross-site Scripting</td>
</tr>
<tr>
<td><strong>A4</strong></td>
<td>Insecure Direct Object References</td>
</tr>
<tr>
<td><strong>A5</strong></td>
<td>Security misconfiguration</td>
</tr>
<tr>
<td><strong>A6</strong></td>
<td>Sensitive Data Exposure</td>
</tr>
<tr>
<td><strong>A7</strong></td>
<td>Missing function level access control</td>
</tr>
<tr>
<td><strong>A8</strong></td>
<td>Cross-site Request Forgery</td>
</tr>
<tr>
<td><strong>A9</strong></td>
<td>Using components with kn. vulnerabilities</td>
</tr>
<tr>
<td><strong>A10</strong></td>
<td>Unvalidated redirects and Forwards</td>
</tr>
</tbody>
</table>
Imagine a server-side calendar

```php
$year = $_GET['year'];
print "<pre>
system("cal $year");
print "</pre>
?>
```

system("cal 2012");
http://example.com/cal.php?year=2012;cat /etc/passwd

What if we, as the script programmers, blacklist the semicolon? Will it solve our problems?
http://example.com/cal.php?year=2012%26%26cat /etc/passwd

```
system("cal 2012 && cat /etc/passwd");
```
Injected commands does the following:

- Downloads backdoor script from attacker’s server
- Makes it executable
- Executes it

Backdoor is now running with the permissions of the web server user on the web server
Remote Command Execution

• These were examples of a vulnerability belonging to the class of “Remote Command Execution”

• One of the more deadly attacks
  – Attacker has foothold on server
  – This foothold can be used to (among others): steal data, connect to other machines internal to the network, or try to become root
Defenses

• Defense should not be blacklisting
  – Hard to do comprehensively (&,*`,$,( ... )
  – Problems with applications that need access to the things that you blacklist

• Sanitization is the correct step (but not foolproof)
  – We saw this again in XSS where we said that the characters needed to be properly escaped
  – E.g. Place parameters in single quotes and escape existing single quotes that are part of the payload
  – Frameworks provide functions to help, e.g., `escapeshellarg()` in PHP
Question

• Can we rely on sanitization of the arguments using JavaScript at the client-side?
  – E.g. use JavaScript to add quotes to the value of the year variable, as the attacker types it in a specific HTML input field

• NO!!!!!!
  – The attacker is the client, and can send arbitrary input to us (e.g. remove JavaScript, or just create requests by hand/through another program)
## OWASP Top 10

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>A1</strong> – Injection</td>
<td></td>
</tr>
<tr>
<td><strong>A2</strong> – Broken Auth and Session Management</td>
<td></td>
</tr>
<tr>
<td><strong>A3</strong> – Cross-site Scripting</td>
<td></td>
</tr>
<tr>
<td><strong>A4</strong> – Insecure Direct Object References</td>
<td></td>
</tr>
<tr>
<td><strong>A5</strong> – Security misconfiguration</td>
<td></td>
</tr>
<tr>
<td><strong>A6</strong> – Sensitive Data Exposure</td>
<td></td>
</tr>
<tr>
<td><strong>A7</strong> – Missing function level access control</td>
<td></td>
</tr>
<tr>
<td><strong>A8</strong> – Cross-site Request Forgery</td>
<td></td>
</tr>
<tr>
<td><strong>A9</strong> – Using components with known vulnerabilities</td>
<td></td>
</tr>
<tr>
<td><strong>A10</strong> – Unvalidated redirects and Forwards</td>
<td></td>
</tr>
</tbody>
</table>
Different name, same beast

```php
$user = $_POST['username'];
$pass = $_POST['password'];

$res = mysql_query("SELECT * from members where username = '{$user}' and password = 'pass'");  

[...]

?>
```
Different name, same beast

If the user submits:

- **Username**: Jack
- **Password**: letmein

Then the query becomes

```sql
SELECT * from members where username = 'Jack' and password = 'letmein'
```
SQL Injection

What if an attacker submits:

• **Username**: administrator’--
• **Password**: doesnotmatter

Then the query becomes

```
SELECT * from members where
username = 'administrator'--' and password =
'doesnotmatter'
```
SQL Injection

In an eShop with the following:

```sql
SELECT * from products where pid = $_GET['pid']
```

An attacker could construct the following input:

```
Pid= -9999 UNION ALL SELECT 
username,password,3,4,5 from members;
```

Allowing him to list credentials from different tables in the SQL database
Compulsory XKCD cartoon

http://xkcd.com/327/
Defenses

• As before, sanitization should be used to stop the attack
  – E.g. knowing that a value should only be an integer, allows you to wrap it in the intval() function

• More generically, for SQL, prepared statements are considered the best way of defending
Prepared statements

`mysql_query("SELECT * from members where
username = '{$user}' and password = '{$pass}'");`

Now becomes

```
$stmt = $conn->prepare("SELECT * from members
where username=? and password=?");
$stmt->bind_param("ss", username,password);
$stmt->execute();
$res = $stmt->get_result();
```
## OWASP Top 10

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>A1</strong> – Injection</td>
<td></td>
</tr>
<tr>
<td><strong>A2</strong> – Broken Auth and Session Management</td>
<td></td>
</tr>
<tr>
<td><strong>A3</strong> – Cross-site Scripting</td>
<td></td>
</tr>
<tr>
<td><strong>A4</strong> – Insecure Direct Object References</td>
<td></td>
</tr>
<tr>
<td><strong>A5</strong> – Security misconfiguration</td>
<td></td>
</tr>
<tr>
<td><strong>A6</strong> – Sensitive Data Exposure</td>
<td></td>
</tr>
<tr>
<td><strong>A7</strong> – Missing function level access control</td>
<td></td>
</tr>
<tr>
<td><strong>A8</strong> – Cross-site Request Forgery</td>
<td></td>
</tr>
<tr>
<td><strong>A9</strong> – Using components with known vulnerabilities</td>
<td></td>
</tr>
<tr>
<td><strong>A10</strong> – Unvalidated redirects and Forwards</td>
<td></td>
</tr>
</tbody>
</table>
Injection (still)

• Web servers, in addition to sending SQL requests to internal SQL servers can also send HTTP requests to internal (or external) servers

• If these requests contain user-controlled input, an attacker could trick the server to:
  – Send requests to arbitrary internal/external servers (Server-side redirection)
  – Overwrite existing parameters in those internal requests (HTTP Parameter Pollution)
Injection (Server-side Redirection)

• In a server-side redirection attack, attackers are able to specify an arbitrary resource or URL that is then requested by the front-end web application

```
POST /account/home HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Host: vulnerable.com
Content-length: 65

view=default&loc=online.foo.net/css/style.css
```
Injection (Server-side Redirection)

- In a server-side redirection attack, attackers are able to specify an arbitrary resource or URL that is then requested by the front-end web application.

```
POST /account/home HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Host: vulnerable.com
Content-length: 65
view=default&loc=online.foo.net/css/style.css
```
Injection (Server-side Redirection)

• In a server-side redirection attack, attackers are able to specify an arbitrary resource or URL that is then requested by the front-end web application.

```
POST /account/home HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Host: vulnerable.com
Content-length: 65

view=default&loc=192.168.0.1:22
```
Injection (HTTP Parameter Pollution)

- HTTP Parameter Injection (HPI) can occur when user-supplied parameters are used as parameters in new HTTP requests towards backends
  - These requests are done by the web server (not by the user/attacker)

- The goal is to confuse the backend webserver and get it to use the parameter controlled by the attacker instead of the one sent by the application
Injection (HTTP Parameter Pollution)

• The reason why HPI exists is because the HTTP specification is not explicit about what servers should do when they receive a request having two parameters with the same name

• http://www.example.com?foo=1&bar=yes&foo=2

• At the server-side, what should the value of the foo variable be?
  – 1, 2, “12”, [1,2]?

• It turns out that different combinations of web server/server-side languages do different things
Injection (HTTP Parameter Pollution)

• Depending on the configuration, an attacker may be able to override the value specified in the backend HTTP request
Injection (HTTP Parameter Pollution)

1. **Attacker to public-facing webserver**
   
   POST /bank/52/Default.aspx HTTP/1.1
   Content-Type: application/x-www-form-urlencoded
   Host: acmebank.com
   Content-length: 65

   fromAcc=123456&amount=1000&toAcc=654321&Submit=Submit

2. **Public-facing webserver to internal webserver**
   
   POST /doTransfer.asp HTTP/1.1
   Host: internal.acmebank.com
   Content-length: 72

   FROM=123456&clearedfunds=false&AMOUNT=1000&TO=654321
Injection (HTTP Parameter Pollution)

1. **Attacker to public-facing webserver**

   POST /bank/52/Default.aspx HTTP/1.1
   Content-Type: application/x-www-form-urlencoded
   Host: acmebank.com
   Content-length: 65

   fromAcc=123456%26clearedfunds=true&amount=1000&toAcc=654321&Submit=Submit

2. **Public-facing webserver to internal webserver**

   POST /doTransfer.asp HTTP/1.1
   Host: internal.acmebank.com
   Content-length: 72

   FROM=123456&clearedfunds=true&clearedfunds=false&AMOUNT=1000&TO=654321
HTTP Parameter Tampering Vulnerabilities

• In all of these attacks, it’s important to remember that the client is the attacker, and the server is the potential victim

• In HTTP Parameter tampering, an attacker can arbitrarily change the values of parameters that are exposed to him
  – E.g. prices of products, current auth level, etc.
Welcome to A Clean Well-Lighted Place for Books

Your Shopping Cart

<table>
<thead>
<tr>
<th>Qty</th>
<th>Description</th>
<th>Price</th>
<th>Remove</th>
</tr>
</thead>
<tbody>
<tr>
<td>-1</td>
<td>Linux Security for Large-Scale Enterprise Networks, Becker, Jamieson</td>
<td>$-59.99</td>
<td>Remove</td>
</tr>
<tr>
<td></td>
<td>1555582923 Paperback Special Order</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Total: $-59.99

Insecure software

Secure communications
Logic Vulnerabilities

• HTTP parameter tampering vulnerabilities are a subset of logic vulnerabilities in web applications

• Logic vulnerabilities typically rely on breaking assumptions made by architects and developers

• Assumptions
  – Step 2 can only be performed after Step 1
  – The web application controls the navigation steps
  – Users cannot change parameters that they cannot see
  – Etc.
Examples of logic vulnerabilities

• Unlike vulnerabilities discussed so far, logic vulnerabilities don’t have a clear, narrow definition
• This makes them hard to identify, especially by automated vulnerability discovery tools
• We will see a few real-world examples based on the book “The Web Application Hackers Handbook”
Case Study: Password change

• A website allows its users to change their password, by filling out a form with their current password, and their new password

• Administrators can also change a user’s password but they don’t need to provide a user’s current password

```java
String existingPassword = request.getParameter("existingPassword");
if (null == existingPassword)
{
    trace("Old password not supplied, must be an administrator");
    return true;
}
else
{
    trace("Verifying user's old password");
    ...
}
Case Study: Password change

• The code that handles these two cases is the same and the developer assumes that if the “existingPassword” parameter is not present, this must be because the current request came from an administrative UI.

• All the attackers have to do is drop the “existingPassword” HTTP parameter from the outgoing request.
Case Study: Business Limit

• A business does not want its finance personnel to be able to transfer funds between accounts that exceed a certain threshold, without approval

```cpp
bool CAuthCheck::RequiresApproval(int amount)
{
    if (amount <= m_apprThreshold)
        return false;
    else return true;
}
```
Case Study: Business Limit

• The code allows negative transfers from A to B which the transaction module interprets as a positive transfer from B to A

• Therefore a malicious employee (or an attacker who has stolen his credentials) can initiate a transfer for say -$20,000 and bypass the transfer limit
Case Study: Bulk Discounts

• An online shop gives users discounts when they buy some products together
  – E.g. If you purchase an antivirus solution, and a personal firewall, and antispam software then you are entitled to 25% discount on each product

• Abuse
  – Add all products in your basket to get the discount and then remove the ones you don’t want
Case Study: Escaping from escaping

• A web application has to pass user-controllable input as an argument to an operating system command.

• The developer creates a list of special shell metacharacters that need escaping
  – ; | & < > ‘ space and newline

• If any of these are present in the input, the code escapes them by prepending them with a backslash
  – \
Case Study: Escaping from escaping

- If an attacker types
  - `foo;ls`
- The code converts it to
  - `foo\;ls`
- What if an attacker types an escape character
  - `foo\;ls`
- Will become
  - `foo\\;ls`
- Which amounts to escaping the backslash but not the semicolon
Case Study: Invalidating input validation

• A web application has two filtering mechanisms aimed at stopping abuse
  – Filter 1: Escape single quotes with an additional quote as a means of invalidating SQL injections
    • ‘admin– becomes “admin–"
  – Filter 2: Prune all user inputs to 128 characters

• Abuse
  – Submit 128 character SQL injection with the last character being a single quote
  – Filter 1 will escape the single quote by adding another quote, thereby making the string 129 bytes long
  – Filter 2 will prune the string to 128 bytes and remove the extra escaping quote, making the SQL injection valid again
Credits

• Many of the slides here are the courtesy of Nick Nikiforakis and Venkat Venkatakrishnan