APPSEC engineer

Content-Security-Policy

An Introduction

What we're looking at

- Why you need `Content-Security-Policy`
- Introduction to `Content-Security-Policy`
- Bypassing CSP
- CSP Success Factors

Why you need CSP

```
<html>
 <head>
 <title>{{ title }} - My Site</title>
<!--html entities context -->
 <style>
 body {
 color: {{ theme['color'] }};
 }
 </style>
<!--css context -->
 </head>
 <body>
 <script type="text/javascript">
 var init = {{ data }};
 </script>
<!--javascript context -->
 <a href={{ home_url }}>Home</a>
<!--html attribute context -->
 </body>
</html>
```

XSS is still hard to fix

- Auto-escaping deals mostly with HTML Entities
- CSS, JavaScript, HTML Attribs can still be used for XSS
- You need all the help you can get

Enter CSP

- Set by the Application (Server)
- Enforced by the Browser
- Meant to prevent XSS payloads from being rendered on the client

CSP

Set via **HTTP header**, by the **web server**, for the **browser** to enforce

```
Content-Security-Policy: default-src 'self' *.trusted.com
```

Nature of CSP

- CSP rules are additive. Example `default-src: 'self'` means that **all** content, comes from the origin server
- You can define more fine-grained rules for other content-types

Bypassing CSP

- CSP Whitelist Bypass - Control execution from wildcard domain like `*.amazonaws.com` or `*.marketo.com`
- Bypass based on poorly generated CSP rules on specific content-types

Additional CSP Protections

- Nonce: where you use a one-time random token to work with client-side content.
- Hash: Hash of client-side content that will load only if the

CSP with Hashes

```
content-security-policy: default-src 'self';
                         script-src 'sha256-
U15iTVPSeNNxQzawfmi5aUkcP7JxgjVuecsYsVs5aPE='
```

CSP with Nonce

```
content-security-policy: default-src 'self';
                         script-src 'nonce-
                         12898842bb6a42e4934312f237ffe45a'
```

Useful resources

- Report-URI
- CSP is Awesome
- Mozilla

Like this video?

- Follow @abhaybhargav on Twitter
- Subscribe to this channel for more videos
- abhaybhargav.com