iSECpartners
part of nccgroup

Content Security Policy

Preventing Content Injection

Jake Meredith
Associate Security Engineer
iSEC Partners

Agenda

iSECpartners part of nccgroup

- The Problem
- Previous Solutions
- Content Security Policy
- Future
- Questions

iSECpartners
part of nccgroup

The Problem

- Cross-site Scripting (XSS)
  - #3 OWASP Top 10 2013
  - Possibly 70% of sites affected

XSS

iSECpartners part of nccgroup

- Inject scripts into web pages
  - Session stealing
  - Data theft
  - Cookie stealing
  - Bypass Access Control
  - Account Hijacking
  - Etc.

Prevelance of XSS

iSECpartners part of nccgroup

- Some websites affected recently
  - Suntrust.com
  - Store.apple.com
  - BarackObama.com
  - Threadless.com
  - Class.coursera.org
  - Paypal
  - Etc.

Simple Webapp

iSECpartners
part of nccgroup

Your name =

Sven

name

Code examples

iSECpartners part of nccgroup

- Simplistic XSS

```php
<?php


    if('POST' == $_SERVER['REQUEST_METHOD']) {
        $var = $_POST['name'];
        echo "<div>$var</div>\n\n";
    }
?>
```

Add in a script tag

iSECpartners part of nccgroup

Your name =

<script>alert("XSS")</s

HTTP Post Request

iSECpartners part of nccgroup

```
POST /phptest.php HTTP/1.1
Host: ec2-54-226-234-250.compute-1.amazonaws.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:23.0) Gec
Accept: text/html,application/xhtml+xml,application/xml;q=0.
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://ec2-54-226-234-250.compute-1.amazonaws.com/p
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 52

name=%3Cscript%3Ealert%28%22XSS%22%29%3C%2Fscript%3E
```

XSS!

iSECpartners
part of nccgroup

Previous Solutions

iSECpartners part of nccgroup

- Input Filtering
- Output Encoding
- Anti-XSS filters

Input Filtering

iSECpartners part of nccgroup

- Don't allow "harmful" characters
  - ', ", <, >, and &
- Also can filter against certain words
  - Alert, onerror, cookie, etc
  - Can get quite complex
- Difficult to do because of this:
  - &#60&#115&#99&#114&#105&#112&#116&#62&#97&#108&#101&#114&#116&#40&#100&#111&#99&#117&#109&#101&#110&#116&#46&#99&#111&#111&#107&#105&#101&#41&#60&#47&#115&#99&#114&#105&#112&#116&#62

Output Encoding

iSECpartners part of nccgroup

- Convert harmful characters to equivalent representations on output in order to not have them interpreted in a specific context

Character	Encoding
>	&gt;
<	&lt;
&	&amp;

- Can be tough to get correct if you have a lot of different contexts.
  - Javascript->HTML->Javascript

Anti-XSS Filters

iSECpartners part of nccgroup

- Proprietary, close-source
- Works differently in each browsers
- Could theoretically block something you want to happen

Content Security Policy 1.0

iSECpartners part of nccgroup

- White list for valid resource locations
- Scripts, media, fonts, styles, etc.
- Two forms of HTTP Response Header
  - Content-Security-Policy
  - Content-Security-Policy-Report-Only

CSP Browser Support

iSECpartners part of nccgroup

Browser	Header Name	Fully supported since version	Features supported
Firefox	Content-Security-Policy	23.0	All
Chrome	Content-Security-Policy	25.0	All
IE	X-Content-Security-Policy	Not fully supported	sandbox directive only
Safari	X-Webkit-CSP	6.0	All
Opera	Content-Security-Policy	15.0	All
Android Browser	Not Supported	N/A	None
iOS Safari	X-Webkit-CSP	6.0	All
Blackberry Browser	Not Supported	N/A	None

Other CSP Headers

iSECpartners part of nccgroup

- X-Content-Security-Policy
- X-Webkit-CSP

- Some support, but will be DIFFERENT than this standard
- Use un-prefixed header unless you NEED specific functionality

HTTP Response Header

iSECpartners part of nccgroup

- List of "Directives"
  - Each directive is resource specific
    - Default-src
    - Script-src
    - Object-src
    - Img-src
    - Media-src
    - Font-src
    - Style-src
    - Connect-src
    - Frame-src

default-src

iSECpartners part of nccgroup

```
Content-Security-Policy: default-src
isecpartners.com;
```

- Restricts all resources to domain

‘self’ keyword

iSECpartners part of nccgroup

```
Content-Security-Policy: default-src ‘self’;
```

- Does not allow “outside” resources. Restricted to domain only.

URL	Outcome	Reason
https://csp.com/test.js	Success	Same protocol and host
https://csp.com/dir/test.js	Success	Same protocol and host
http://csp.com/test.js	Failure	Different protocol
https://test.csp.com/test.js	Failure	Different host
https://www.csp.com/dir/test.js	Failure	Different host
https://csp.com:8443/test.js	Failure	Different port

‘none’ keyword

iSECpartners part of nccgroup

```
Content-Security-Policy: default-src ‘none’;
```

- No resources allowed!
- Great way to start buildling a policy

script-src

```
Content-Security-Policy: script-src
js.isecpartners.com;
```

- Restricts scripts to “js” subdomain

Default-src AND script-src

```
Content-Security-Policy: default-src
    isecpartners.com; script-src
        js.isecpartners.com;
```

- Restricts scripts to “js” subdomain and all other resources to domain.

img-src

iSECpartners part of nccgroup

```
Content-Security-Policy: img-src
images.sweetforum.net;
```

- Restricts images to “images” subdomain

style-src

iSECpartners part of nccgroup

```
Content-Security-Policy: style-src
css.sweetforum.net;
```

- Restricts styles to “css” subdomain

object-src

iSECpartners part of nccgroup

```
Content-Security-Policy: object-src
plugins.sweetforum.net;
```

- Restricts plugins to “plugins” subdomain

media-src

iSECpartners part of nccgroup

```
Content-Security-Policy: media-src
videos.sweetforum.net audio.sweetforum.net;
```

- Restricts media to “videos” or “audio” subdomains

frame-src

iSECpartners part of nccgroup

```
Content-Security-Policy: frame-src
videos.sweetforum.net youtube.com;
```

- Restricts frames to “videos” subdomain and youtube.com

font-src

```
Content-Security-Policy: font-src
fonts.sweetforum.net;
```

- Restricts fonts to “fonts” subdomain

connect-src

```
Content-Security-Policy: connect-src
    mysite.com partnersite.com;
```

- Limits connections to only partnersite.com
  - Send() method of XHR object
  - Websocket constructor
  - Eventsource constructor

More about connect-src

iSECpartners part of nccgroup

- EXAMPLES of invalid connections:
  - new WebSocket("wss://malicious.rr/");
  - (new XMLHttpRequest()).open("GET", "https://pwned.net", TRUE);
  - new EventSource("https://bankofamericac.com");

sandbox

iSECpartners part of nccgroup

```
Content-Security-Policy: sandbox
```

- Creates different origin
- Prevents plugins, scripts, and popups
- Additional parameters
  - Allow-forms
  - Allow-same-origin
  - Allow-top-navigation
  - Allow-scripts

report-uri

iSECpartners part of nccgroup

```
Content-Security-Policy: default-src 'self';
    report-uri mysite.com/report.cgi;
```

- All violations will get sent to "report.cgi" for processing

Violation Report

iSECpartners part of nccgroup

```
{
        "csp-report": {
        "document-uri": "http://csp.com/index.html",
        "referrer": "http://notorigin.com",
        "blocked-uri": "http://notorigin.com/attack.js",
        "violated directive": "script-src 'none'" ,
        "original-policy": "default-src 'self'; script-src 'none';
                report-uri
        /uri_parser"
        }
}
```

scheme

iSECpartners part of nccgroup

```
Content-Security-Policy: default-src https:;
```

- Forces only HTTPS content for all resources

More with scheme

iSECpartners part of nccgroup

```
Content-Security-Policy: default-src https:;
        script-src scripts.csp.com;
```

- Lowers the scheme of scripts!

Building a policy with 'none'

iSECpartners part of nccgroup

```
Content-Security-Policy: default-src 'none';
  script-src scripts.mysite.com; style-src
                css.mysite.com;
```

- No resources allowed by default, scripts and styles are given specific whitelists.

Unsafe-inline

iSECpartners part of nccgroup

```
Content-Security-Policy: script-src 'self'
                         unsafe-inline;
```

- Allows inline scripts
- Removes most of the benefits of CSP
- Can help with implementing a policy in a legacy application

Ridding inline code

iSECpartners part of nccgroup

- Domain csp.com

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

- csp.com/index.html:

```
<script> alert('Welcome to CSP!')</script>
```

Externalizing inline scripts

iSECpartners part of nccgroup

- csp.com/alert.js

```
function welcome()
{
      alert("Welcome to CSP!");
}
```

- index.html

```
<script src='alert.js'></script>
```

More complex

iSECpartners part of nccgroup

- Index.html

```
<a href="#" onClick="alert('you clicked
me')">Click Me</a>
```

addEventListener()

iSECpartners part of nccgroup

- events.js

```
function someEvent() {
     alert("you clicked me");
}
var obj =
document.getElementById("someElementId");
obj.addEventListener("click", someEvent);
```

Back to the html

iSECpartners part of nccgroup

- Index.html

```
<script src='events.js'</script>
<a href="#" id="someElementId">Click Me</a>
```

Evaluating your functions

iSECpartners part of nccgroup

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

- Allows following behavior:
  - Javascript operator and function eval()
  - Function() constructor
  - setTimeout() method without a function as the first argument
  - setInterval() method without a function as the first argument

Report Only

iSECpartners part of nccgroup

```
Content-Security-Policy-Report-Only:
default-src 'none'; report-uri /report.cgi;
```

- Great for monitoring
- Doesn't block behavior

Iterative Policy

iSECpartners part of nccgroup

- Use Report-Only mode to constantly monitor and improve
- Update main header with “successful” directives
- Try new Report-Only headers to try more specific and more secure settings
- Use a DB to keep track of violations

Gotchas with CSP

iSECpartners
part of nccgroup

- Use unprefixed header only

Gotchas with CSP

iSECpartners part of nccgroup

- Use unprefixed header only
- Don’t use unsafe-inline

Gotchas with CSP

iSECpartners
part of nccgroup

- Use unprefixed header only
- Don’t use unsafe-inline
- Don’t use unsafe-eval

Gotchas with CSP

iSECpartners part of nccgroup

- Use unprefixed header only
- Don’t use unsafe-inline
- Don’t use unsafe-eval
- No wildcards as default policy

Gotchas with CSP

iSECpartners part of nccgroup

- Use unprefixed header only
- Don’t use unsafe-inline
- Don’t use unsafe-eval
- No wildcards as default policy
- Always specify default-src

Gotchas with CSP

iSECpartners part of nccgroup

- Use unprefixed header only
- Don’t use unsafe-inline
- Don’t use unsafe-eval
- No wildcards as default policy
- Always specify default-src
- Always specify report-uri

Gotchas with CSP

iSECpartners part of nccgroup

- Use unprefixed header only
- Don’t use unsafe-inline
- Don’t use unsafe-eval
- No wildcards as default policy
- Always specify default-src
- Always specify report-uri
- Don’t lower scheme

Gotchas with CSP

iSECpartners part of nccgroup

- Use unprefixed header only
- Don’t use unsafe-inline
- Don’t use unsafe-eval
- No wildcards as default policy
- Always specify default-src
- Always specify report-uri
- Don’t lower scheme
- Use Report Only to your advantage

Gotchas with CSP

iSECpartners part of nccgroup

- Use unprefixed header only
- Don't use unsafe-inline
- Don't use unsafe-eval
- No wildcards as default policy
- Always specify default-src
- Always specify report-uri
- Don't lower scheme
- Use Report Only to your advantage
- No paths for CSP 1.0

CSP in Apache

iSECpartners part of nccgroup

- Main apache config
- Header set Content-Security-Policy: default-src ‘self’;

CSP in nginx

iSECpartners part of nccgroup

- add_header Content-Security-Policy default-src 'self';

CSP in IIS

iSECpartners part of nccgroup

- Features View -> HTTP Response Headers -> Actions -> Add -> Add Custom HTTP Response Header
  - Name = Content-Security-Policy
  - Value = {insert policy}

CSP header injection

iSECpartners part of nccgroup

- Django (Python)
  - response = render_to_response('app/view.html')
    response['Content-Security-Policy'] = "default-src 'self'"
    return response
- ASP.NET
  - context.Response.AddHeader("headerName", "someValue");
  - context.Response.Headers.Add("Cache-Control", "no-cache");
- PHP
  - header("Content-Security-Policy: default-src 'self'");

Future of CSP (1.1)

iSECpartners part of nccgroup

- Paths

```
Content-Security-Policy: script-src
csp.com/scripts/;
```

Future of CSP (1.1)

iSECpartners part of nccgroup

- Base-uri

```
Content-Security-Policy: base-uri 'self';
```

- Restricts the options for <base> tag use

Future of CSP (1.1)

iSECpartners part of nccgroup

- Form-action
  - restricts which URIs can be used as the action of HTML form elements
  - Is not defined by default-src

Future of CSP (1.1)

iSECpartners part of nccgroup

- Plugin-types

```
Content-Security-Policy: plugin-types
        application/pdf;
```

Future of CSP (1.1)

iSECpartners part of nccgroup

- reflected-xss
  - allows for you to turn off the user agent's XSS protection
  - Same as X-XSS-Protection header essentially

```
Content-Security-Policy: reflected-xss
                         allow;
```

Thank You

iSECpartners part of nccgroup

- Tableau Software, Inc (specifically Amanda Gray)
- Mike Warner
- Raymond Forbes
- Other folks at iSEC for their notes and assistance and the time to work on the presentation

Questions?

iSECpartners part of nccgroup

- Jake Meredith
  - Associate Security Engineer at iSEC Partners
  - jake@isecpartners.com

iSECpartners
part of nccgroup

UK Offices
Manchester - Head Office
Cheltenham
Edinburgh
Leatherhead
London
Thame

North American Offices
San Francisco
Atlanta
New York
Seattle

Australian Offices
Sydney

European Offices
Amsterdam - Netherlands
Munich – Germany
Zurich - Switzerland