OWASP Russia Meetup #3

Web Application Security: future standards and technologies


W3C®

Web Application Security Working Group

The mission of the Web Application Security Working Group, part of the Security Activity, is to develop security and policy mechanisms to improve the security of Web Applications, and enable secure cross-origin communication.

http://www.w3.org/2014/12/webappsec-charter-2015

Agenda

- CSP2 (very shortly)
- Subresource Integrity
- Referrer Policy
- Credential Management API
- Confinement with Origin Web Labels
- Entry Point Regulation for Web Applications

CSP2

- www.w3.org/TR/CSP2/
- `nonces` & `hashes`!!!11111
- `frame-ancestors` to replace `X-Frame-Options`
- `unsafe-redirect`
- The CSP HTTP Request Header
- More information in violation reports

CSP2 nonces

```
Content-Security-Policy: default-src 'self'; script-src 'self' https://example.com 'nonce-Nc3n83cn...9hc3'
```

```
<script nonce="Nc3n83cn...9hc3">
alert("Allowed because nonce is valid.")
</script>
```

Subresource Integrity

- www.w3.org/TR/SRI/
- Integrity verification via cryptographic hash

```
<script
src="https://example.com/example-
framework.js" integrity="sha256-
C6CB9UYIS9UJeq...5Twh+Y5qFQmYg="
crossorigin="anonymous"></script>
```

What about RequireJS?

RefeRRer Policy

- www.w3.org/TR/referrer-policy/
- `<meta name="referrer" content="origin">`
- None, None when downgrade, Origin Only, Origin when cross-origin, Unsafe URL

Credential Management API

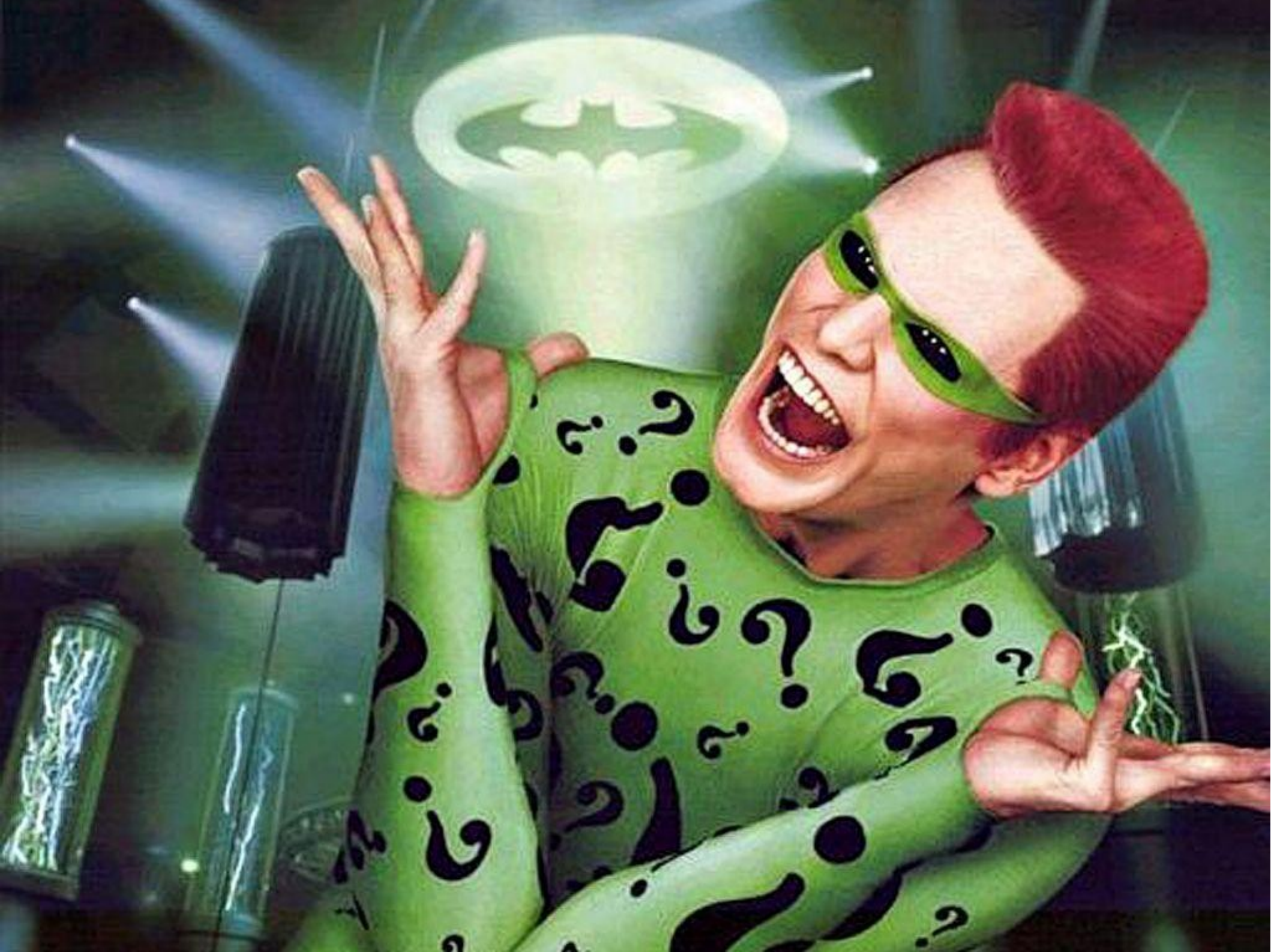
- www.w3.org/TR/credential-management-1/
- Allow websites to more directly interact with the user agent’s credential manager
- Help to detect sign-in via a third-party
- Changing Password

Password-based Sign-in

```
navigator.credentials.get({
  "types": [ "password" ]
}).then(
    function(credential) {
      if (!credential) {
        // show basic form
        return;
      }
      if (credential.type == "PasswordCredential") {
        credential.send("https://example.com/login")
          .then(function (response) {
            // signin succeeded!
          });
      } else {
        // See the Federated Sign-in example
      }
    });
```

And the last...

- Confinement with Origin Web Labels
- Entry Point Regulation for Web Applications
- Permissions API
- Suborigin Namespaces
- Mixed Content
- User Interface Security Directives for Content Security Policy



Thanks!

mailto:oxdef@oxdef.info