Delivering Javascript to World+Dog
Background

Enterprise SaaS Third party javascript Functional Spec

Include JS on site, increase biz

What could go wrong?
The Problem

Javascript - delivering code + data in one

Browser can’t always tell the difference

3rd party js - Hack once, pwn everywhere
Syrian Electronic Army in news site 'hack' POP-UP MAYHEM

Gigya redirect exploit blamed for pop-rageous ploy

By Jasper Hamill 27 Nov 2014 at 13:31

The Syrian Electronic Army has compromised a number of news websites – apparently through DNS redirects via Gigya, a customer identity management platform used by all the sites.

The Pro-Assad javascript popup appeared across several websites, including The Telegraph, The Independent, Forbes, Time Out, PC World and The Evening Standard.
Pwn any of these to have your Gigya moment

- Customer
- App admin
- App developer
- AWS Admin
- CDN developer or admin
- CDN
- DNS
- Staging
- Vuln in payload
Humans - the Weakest Link

Even after you get your shizz together, your customers won’t
Startup developers want to move fast, unencumbered by big company bureaucracy. They ship code daily. More access means less headaches getting their job done.

Least Privilege

Managing Secrets
Good- modern password best practices

Better - 2FA

Best - SAML SSO
Safely Creating Business Value

No custom js
Output encode everything
Absolutely minimize attack surface
Log, publish HMAC of builds
HTTPS build fn
HTTPS to stage bucket
HTTPS to CDN
Third Party Library Management
HTTPS everywhere
Minimize admins
Logging
Change Management
SSO, 2FA
HTTPS everywhere
Have a backup ready
DNS CAA
Secure DNS?
TLS

Cert Transparency
Pinning
Pinning Preload
HTTP2
Server Push
SHA-2 certs
Update ciphersuites regularly
Cookies, HTML5 Local Storage

Data **will** be scrutinized and tampered with

Integrity checks first

Don’t store sensitive data
<table>
<thead>
<tr>
<th>Colliding with Performance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Load first on page</td>
</tr>
<tr>
<td>TLS latency</td>
</tr>
<tr>
<td>TLS tuning</td>
</tr>
<tr>
<td>Can’t break up javascript</td>
</tr>
<tr>
<td>Can’t break up data</td>
</tr>
</tbody>
</table>
Great idea
Least worst, allow unsafe
Hardly any customers ask for it
CSPv3?
Integrity Check
Static
Ties your hands
Self Hosted

Not sustainable

Need rigorous agile release

See server side
Bug Bounty

What finds legit high severity bugs in the JS?

$1000 Bounty - Nope
$5000 Bounty - Nope
$10000 Bounty - ?

10k/1 week of a $300/hr consultant? Yup
Availability

Have backup:

- DNS
- CDN
- Origin
- Build
- Configuration
Looking Ahead

Anomaly detection

Privacy

Insurance?
@kylerandolph
about.me/kylerandolph

Like this? Optimizely is Hiring!
optimizely.com/careers
TLS is essential

Javascript integrity must be ensured end-to-end

Don’t give your customers the opportunity to make insecure choices
Delivering Javascript to World+Dog