What does Tala solve

- XSS (Cross-Site Attacking)
- Magecart (Supply Chain Attacking)
- Session re-directs
- Browser-Based Malware

XSS (Cross-Site Attacking)

184 **#84601** **XSS and cache poisoning via upload.twitter.com on ton.twitter.com**

State	Resolved (Closed)	Severity	No Rating (---)
Disclosed	May 2, 2019 7:05am +0800	Participants	
Reported To	Twitter	Visibility	Disclosed (Full)
Weakness	Cross-site Scripting (XSS) - Generic		
Bounty	$2,520		

40 **#330008** **[dev.twitter.com] XSS and Open Redirect Protection Bypass** Share:

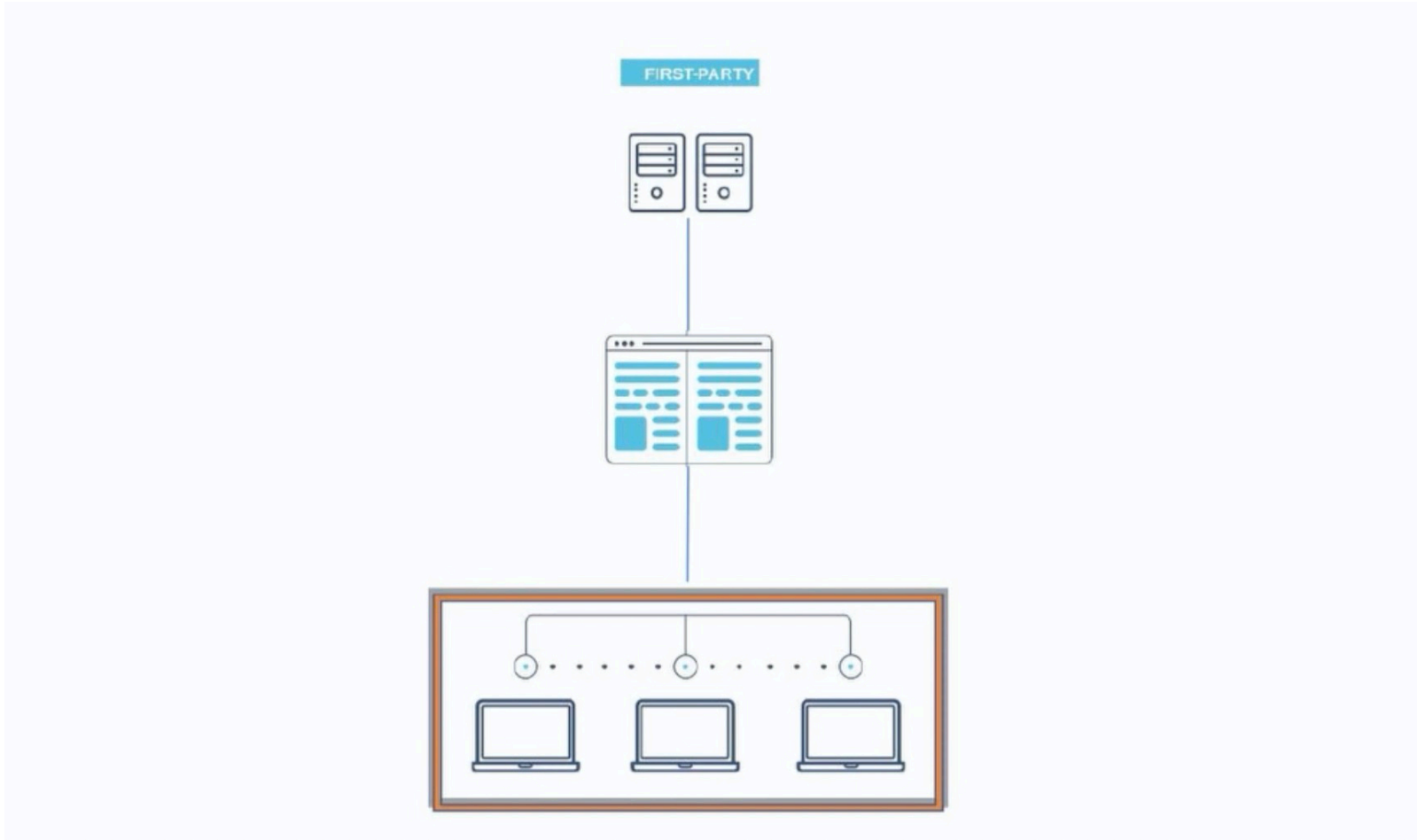
State	Resolved (Closed)	Severity	Medium (4 ~ 6.9)
Disclosed	February 8, 2019 12:32am +0800	Participants	
Reported To	Twitter	Visibility	Disclosed (Full)
Asset	*.twitter.com (Domain)		
Weakness	None		
Bounty	$1,120		

- Formjacking
- Inject malicious JavaScript
- Redirection

Steal Customer Information

Magecart

Evolution of Web Architecture – Last Decade

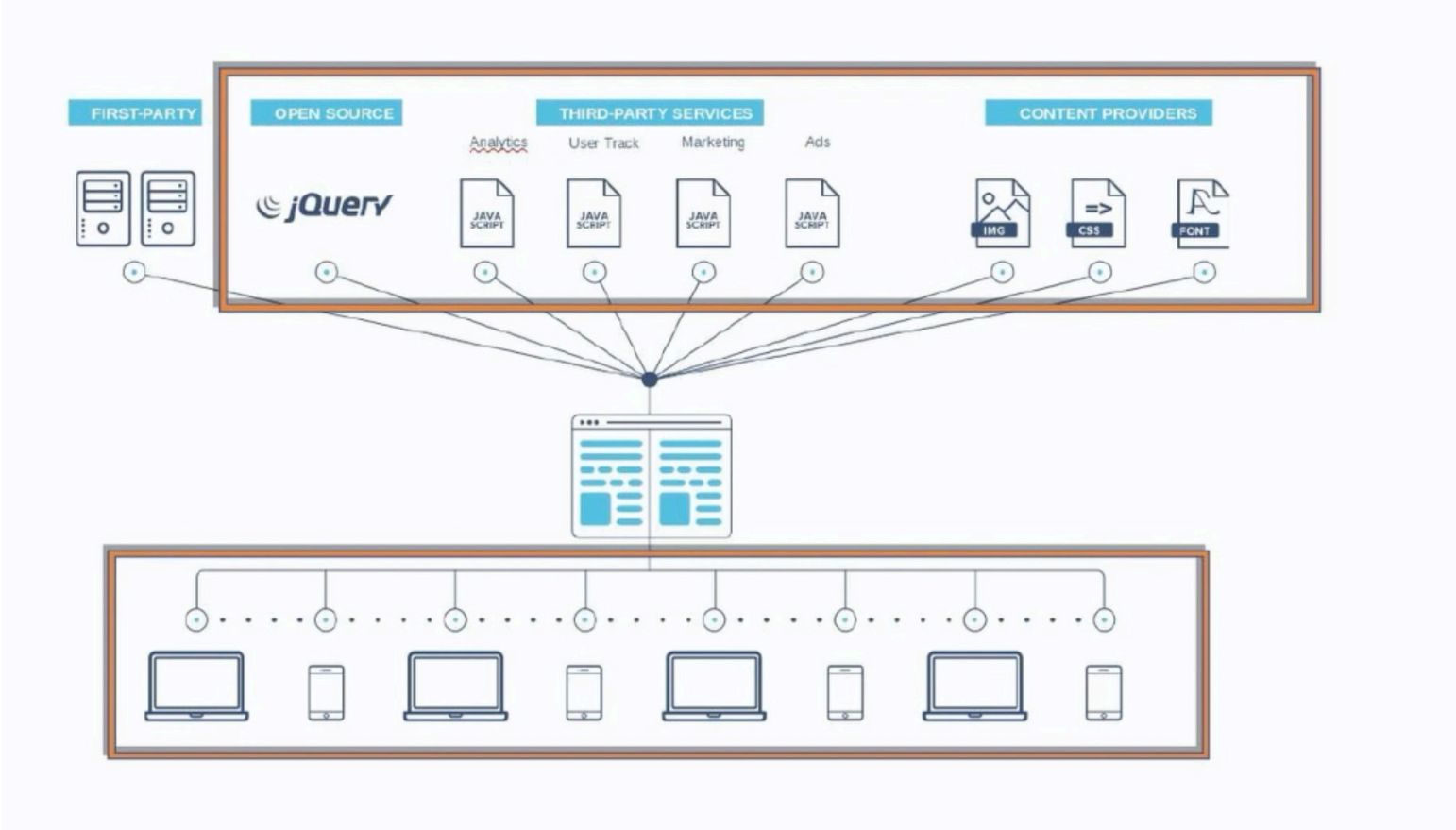


HTML Content served by 1st party Server

Server heavy applications run on desktop computers

Magecart

Evolution of Web Architecture – Today

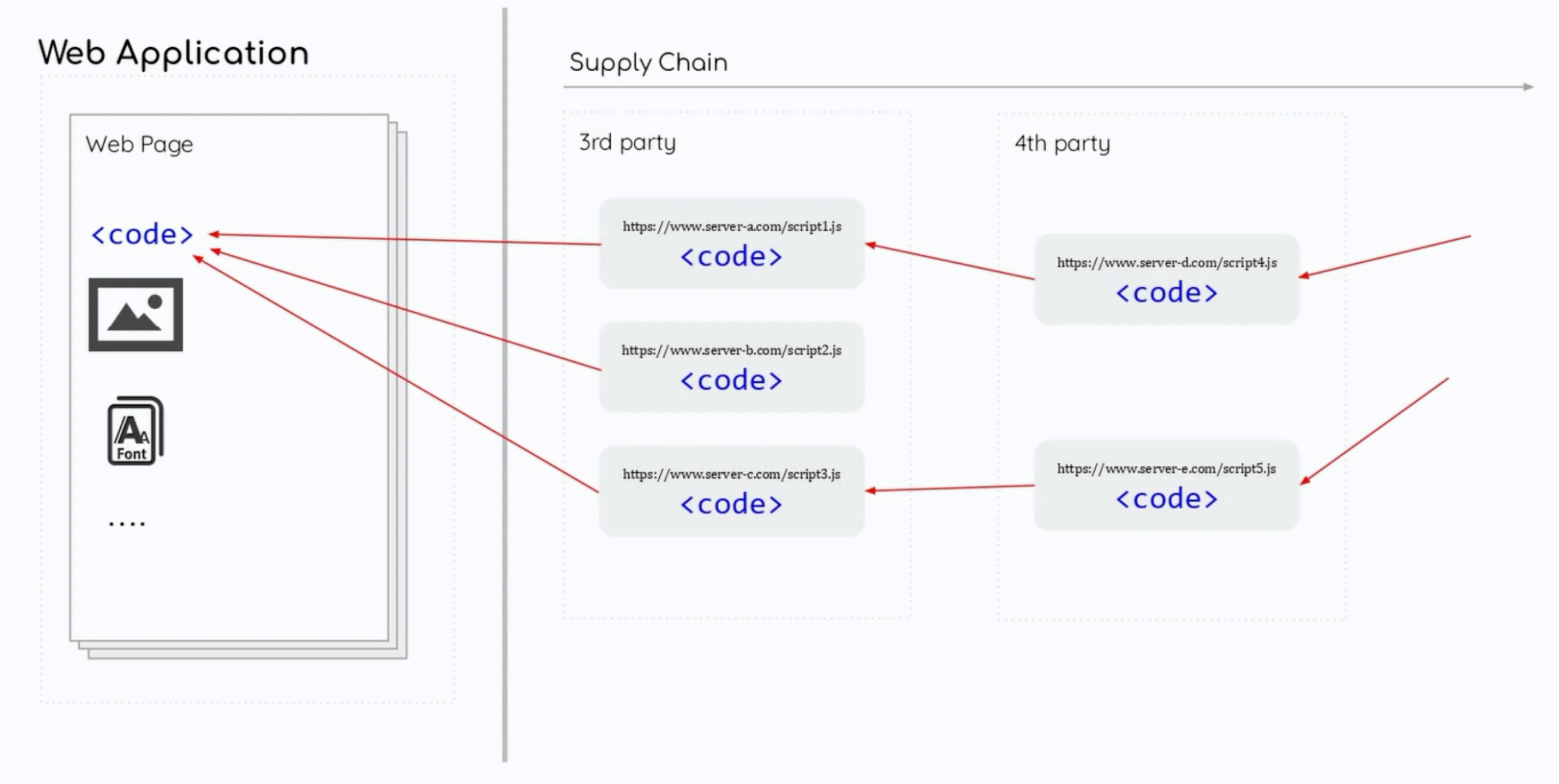


Increased use of 3rd parties, enabled by tag management

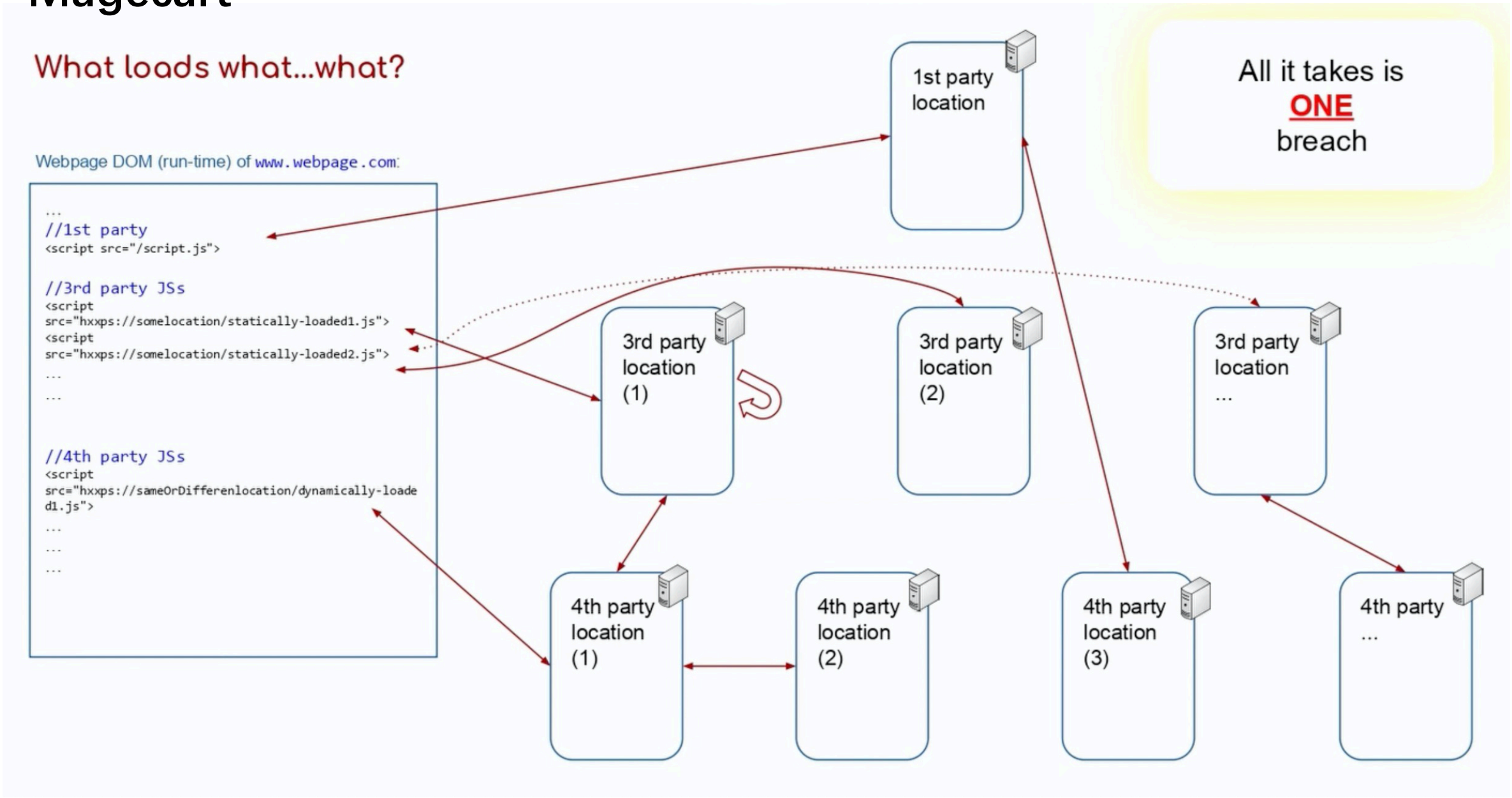
Client-heavy applications, which run on browser executed JavaScript

React
Angular
Backbone

Magecart


Web Application
Web Page
<code>
Font
....
Supply Chain
3rd party
https://www.server-a.com/script1.js
<code>
https://www.server-b.com/script2.js
<code>
https://www.server-c.com/script3.js
<code>
4th party
https://www.server-d.com/script4.js
<code>
https://www.server-e.com/script5.js
<code>

Magecart


What loads what...what?
Webpage DOM (run-time) of www.webpage.com:
...
//1st party
<script src="/script.js">
//3rd party JSs
<script
src="hxxps://somelocation/statically-loaded1.js">
<script
src="hxxps://somelocation/statically-loaded2.js">
...
...
//4th party JSs
<script
src="hxxps://sameOrDifferenlocation/dynamically-loade
d1.js">
...
...
...
1st party location
3rd party location (1)
3rd party location (2)
3rd party location ...
4th party location (1)
4th party location (2)
4th party location (3)
4th party ...
All it takes is ONE breach

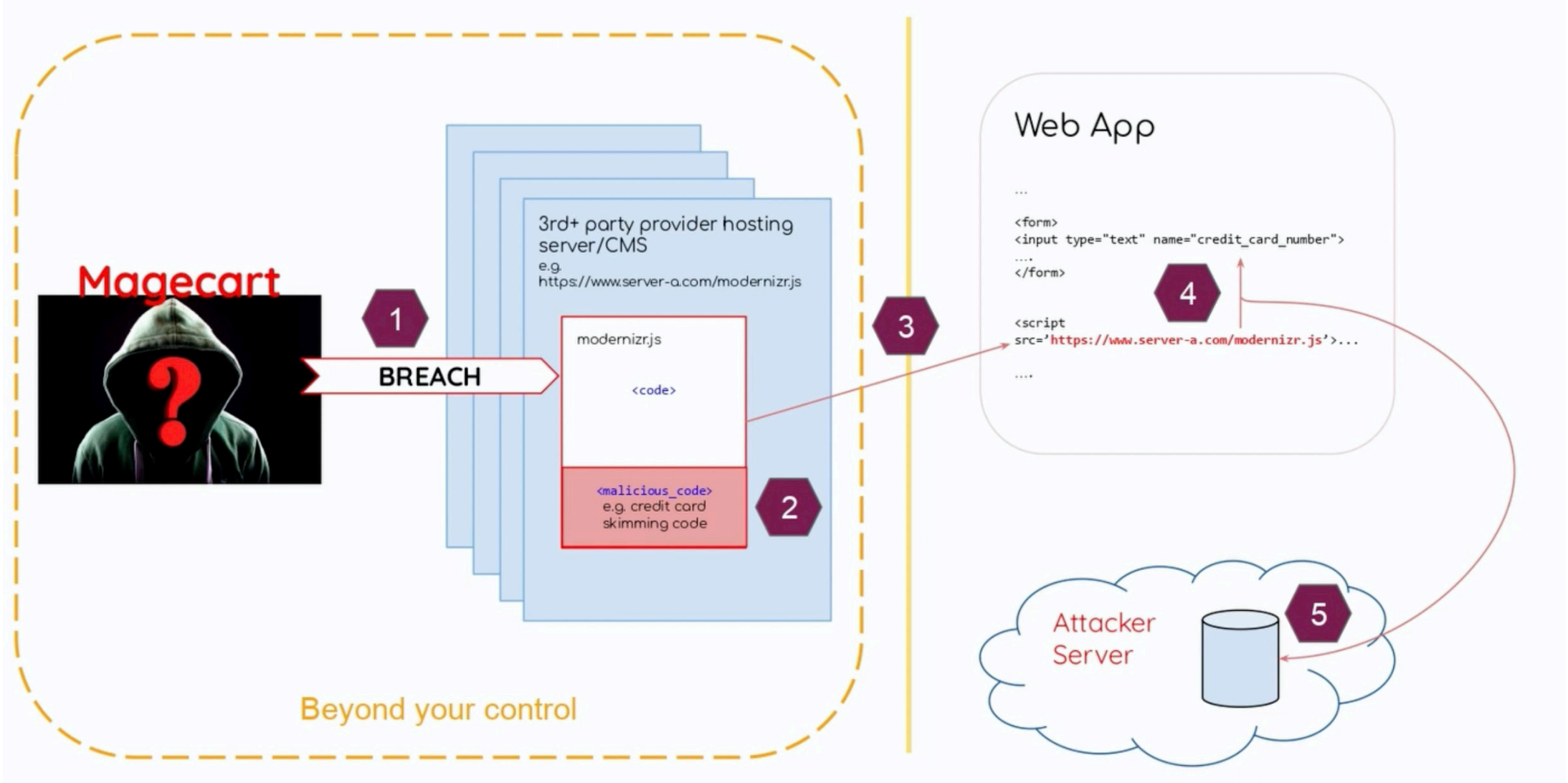
Magecart Victims

Victims of 3rd party compromise

Who is Magecart

- Hacker Groups
- Formjacking/Web Skimmer
- Steal Payment Information
- eCommerce/Airline as target

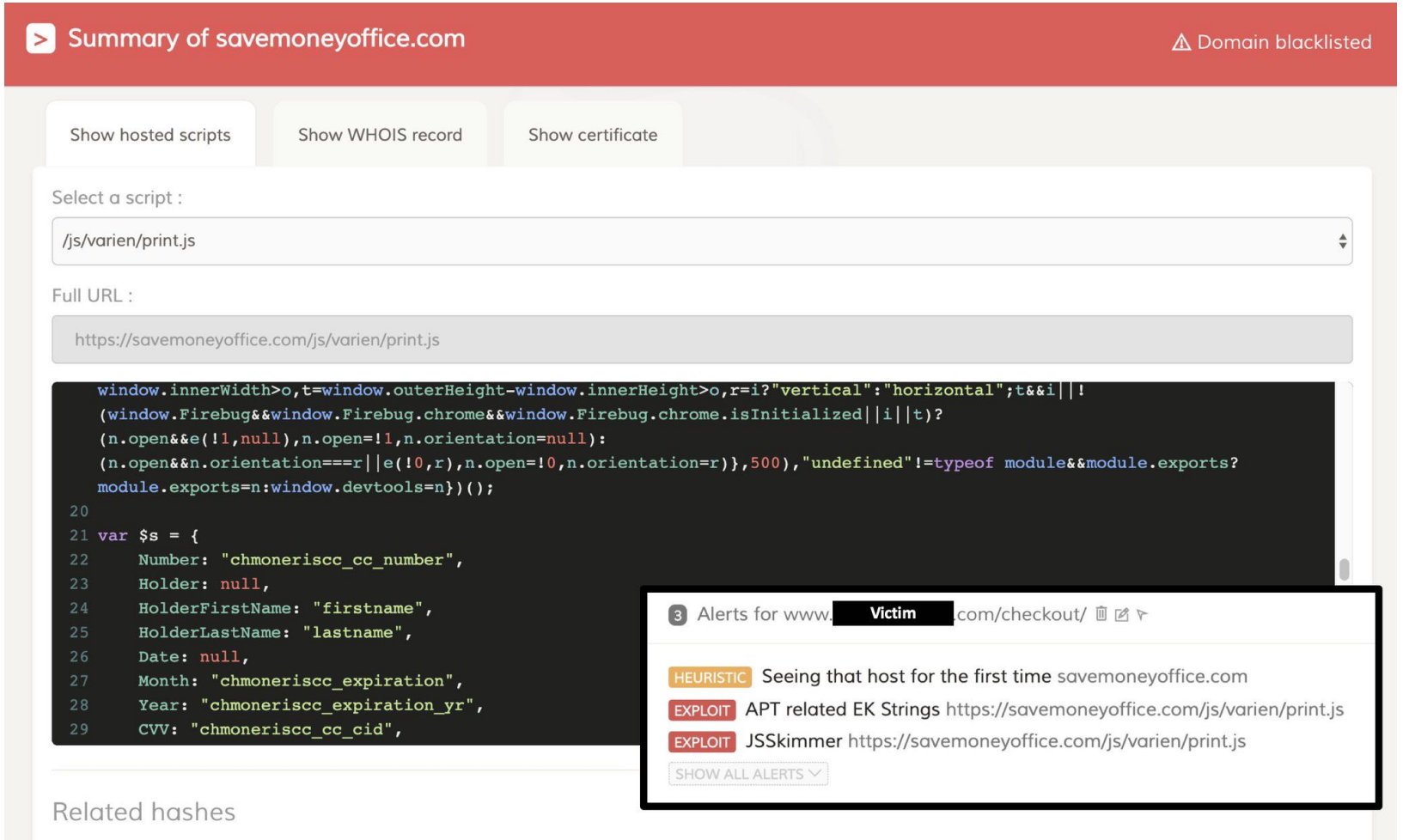
How Magecart Works



Magecart

Inject Malicious JavaScript Code into 3rd part library

JSSkimmer



Tala Security Solution

- Content Security Policy (CSP)
- Subresource Integrity (SRI)
- Strict Transport (HSTS)
- Sandboxing (iFrame rules)
- Referrer Policy
- Trusted Types
- Certificate Stapling
- Clear Site Data

Tala Security Solution

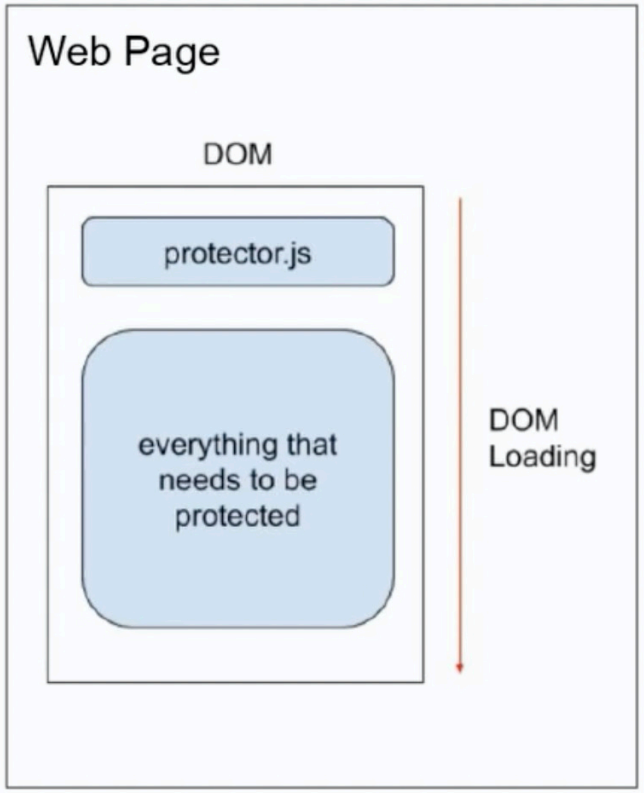
Protections against Magecart

HTTP Security Headers

*Recommended

Cross origin iframe

Javascript vs Javascript



HTTP Security Headers

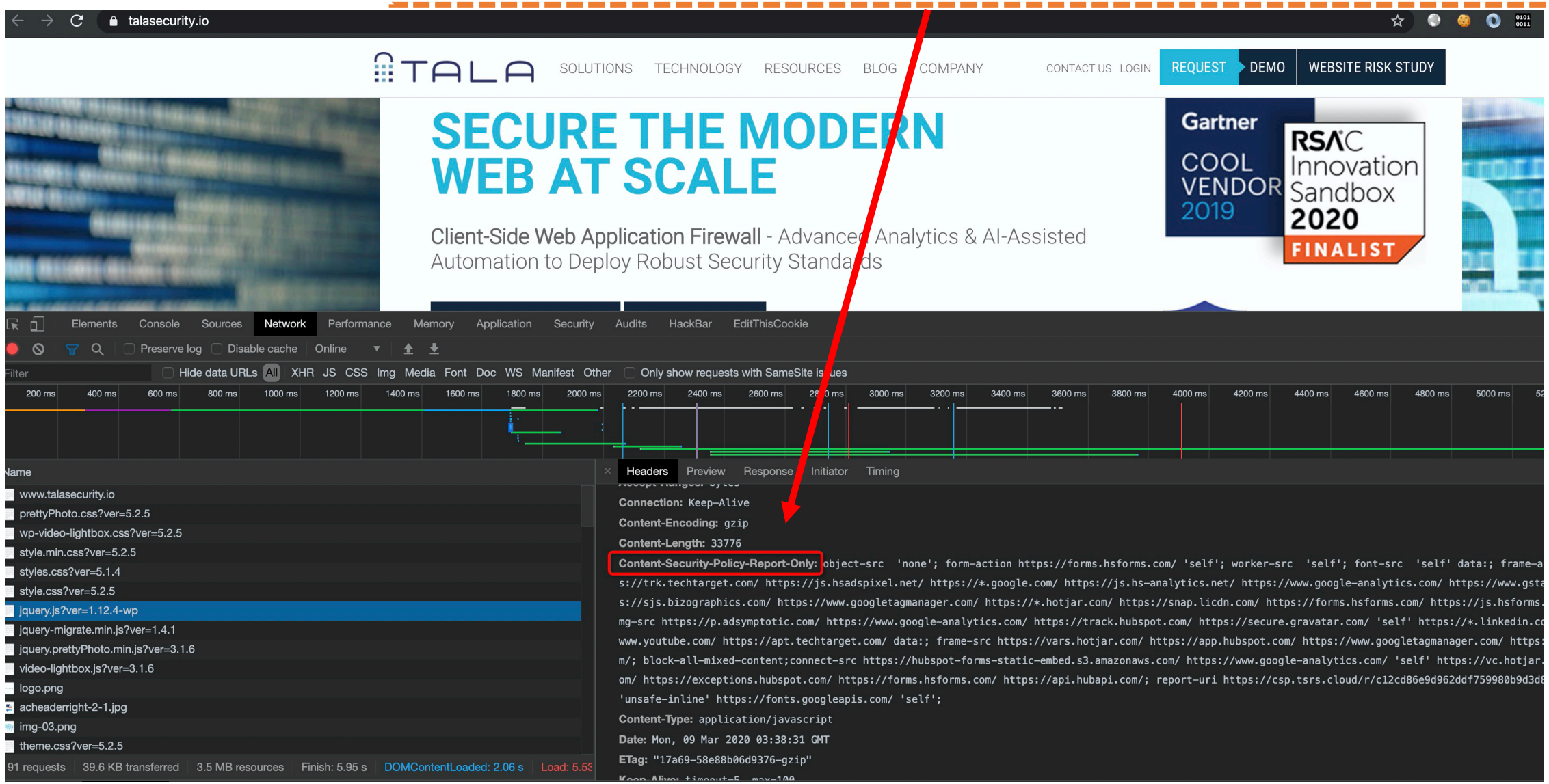
Content Security Policy

- W3C Security Standard
- Implemented as a HTTP header and enforced by browsers
- Locks down web resource origins and content
- Prevents execution of **unintended content** in web context
- Implemented and supported by most browsers

CSP Policy

Content-Security-Policy-Report-Only

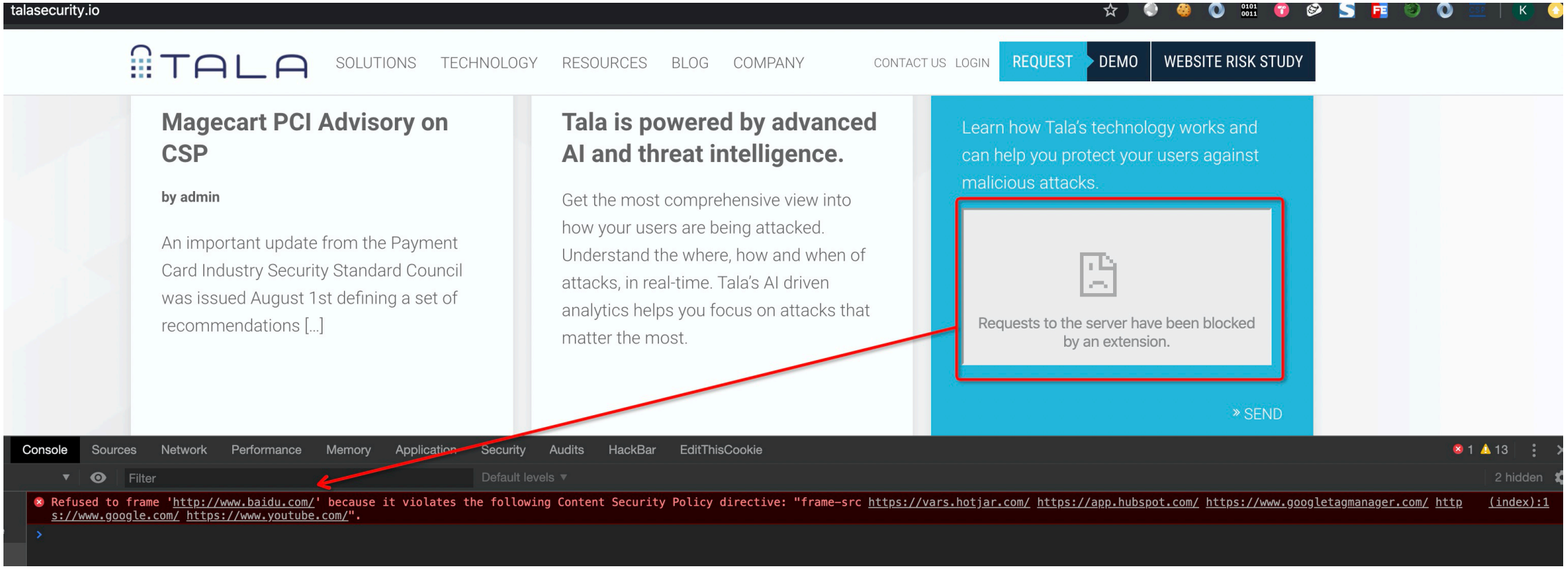
report-uri https://csp.tsrs.cloud/r/c12cd86e9d962ddf759980b9d3d8436e1887c8b7



CSP Policy

frame-src https://vars.hotjar.com/ https://app.hubspot.com/ https://www.googletagmanager.com/ https://www.google.com/ https://www.youtube.com/;

http://www.baidu.com → **Block**



HTTP Security Headers

SRI Example

$ curl https://example.com/example-framework.js | openssl dgst -sha384 -binary | openssl enc -base64 -A

```
<script src="https://example.com/example-framework.js"
integrity="sha384-oqVuAfXRKap7fdgcCY5uykM6+R9GqQ8K/uxy9rx7HNQlGYl1kPzQho1wx4JwY8wC"
crossorigin="anonymous"> <!-- endpoint must support CORS -->
</script>
```

Endpoint must support **CORS**

Response Header

Access-Control-Allow-Origin: <domain>

Access-Control-Allow-Credentials: true

Access-Control-Allow-Methods: GET, POST, PUT

HTTP Security Headers

Referrer-Policy

```
Referrer-Policy: no-referrer
Referrer-Policy: no-referrer-when-downgrade
```

HTTP Strict Transport Security (HSTS)

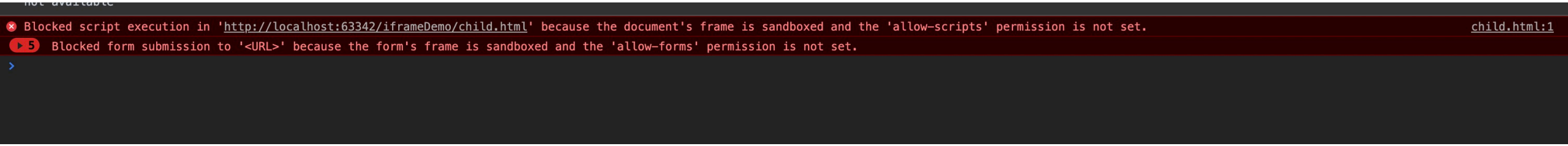
Response Header

```
Strict-Transport-Security: max-age=<expire-time>

Strict-Transport-Security: max-age=<expire-time>; includeSubDomains

Strict-Transport-Security: max-age=<expire-time>; preload
```

Cross Origin Iframe

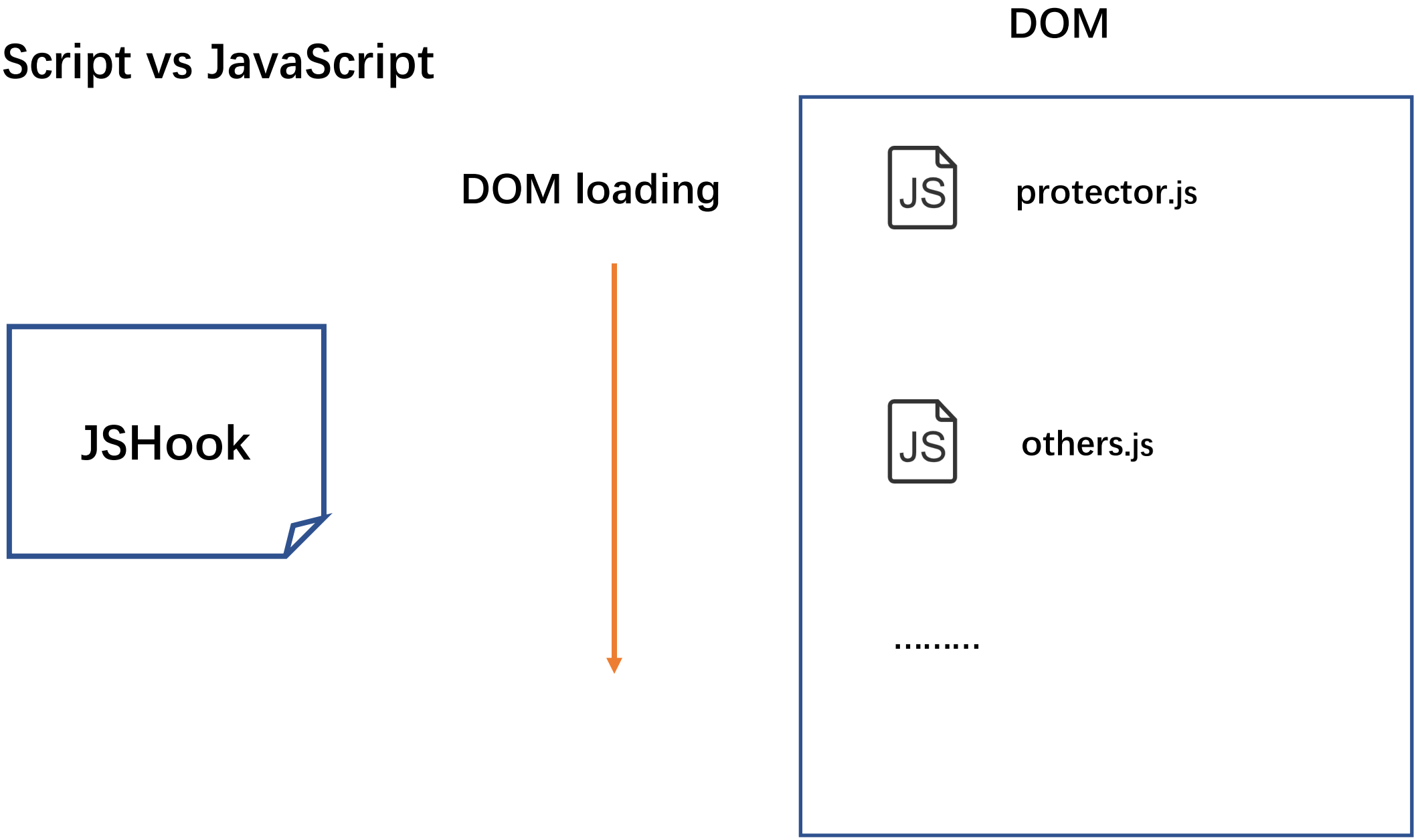
<iframe> tag supports cross domain

```
<iframe src='www.baidu.com' sandbox=''></iframe>
```



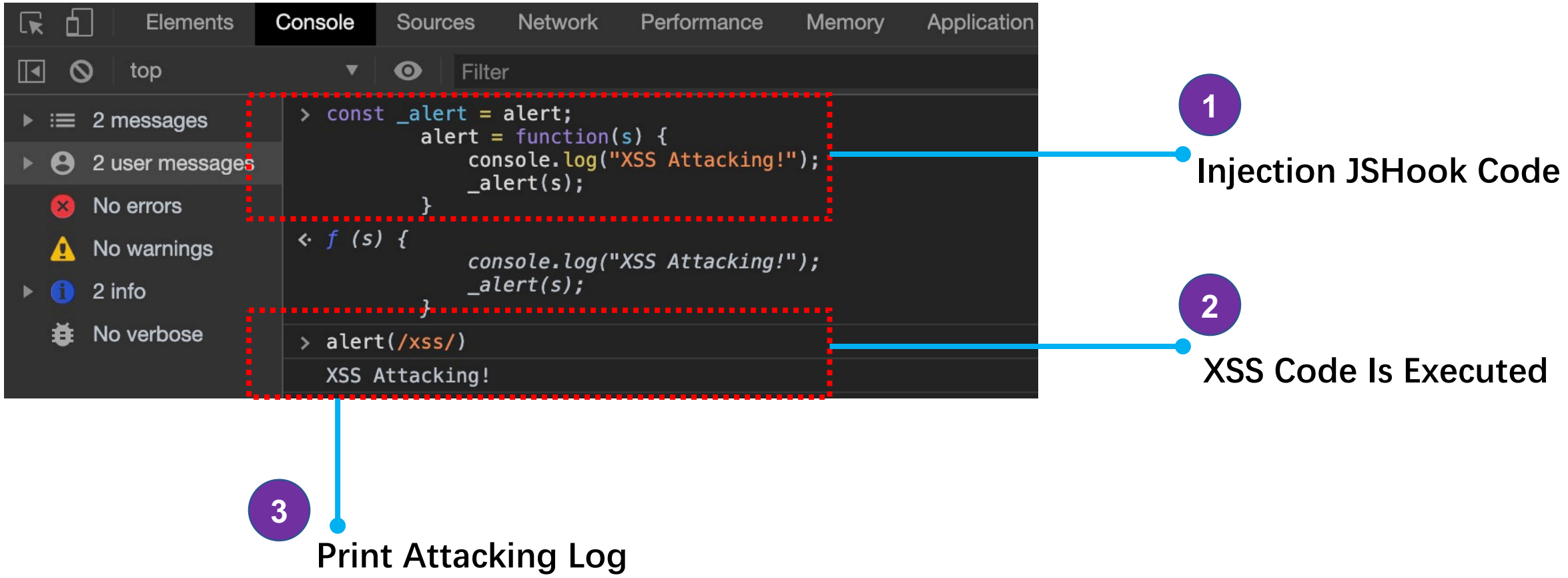
sandbox=''	Deny All
sandbox='allow-same-origin'	All Same Site Resource
sandbox='allow-forms'	All Forms
sandbox='allow-scripts'	All Scripts

JavaScript vs JavaScript



JavaScript vs JavaScript

JSHook Simple Sample

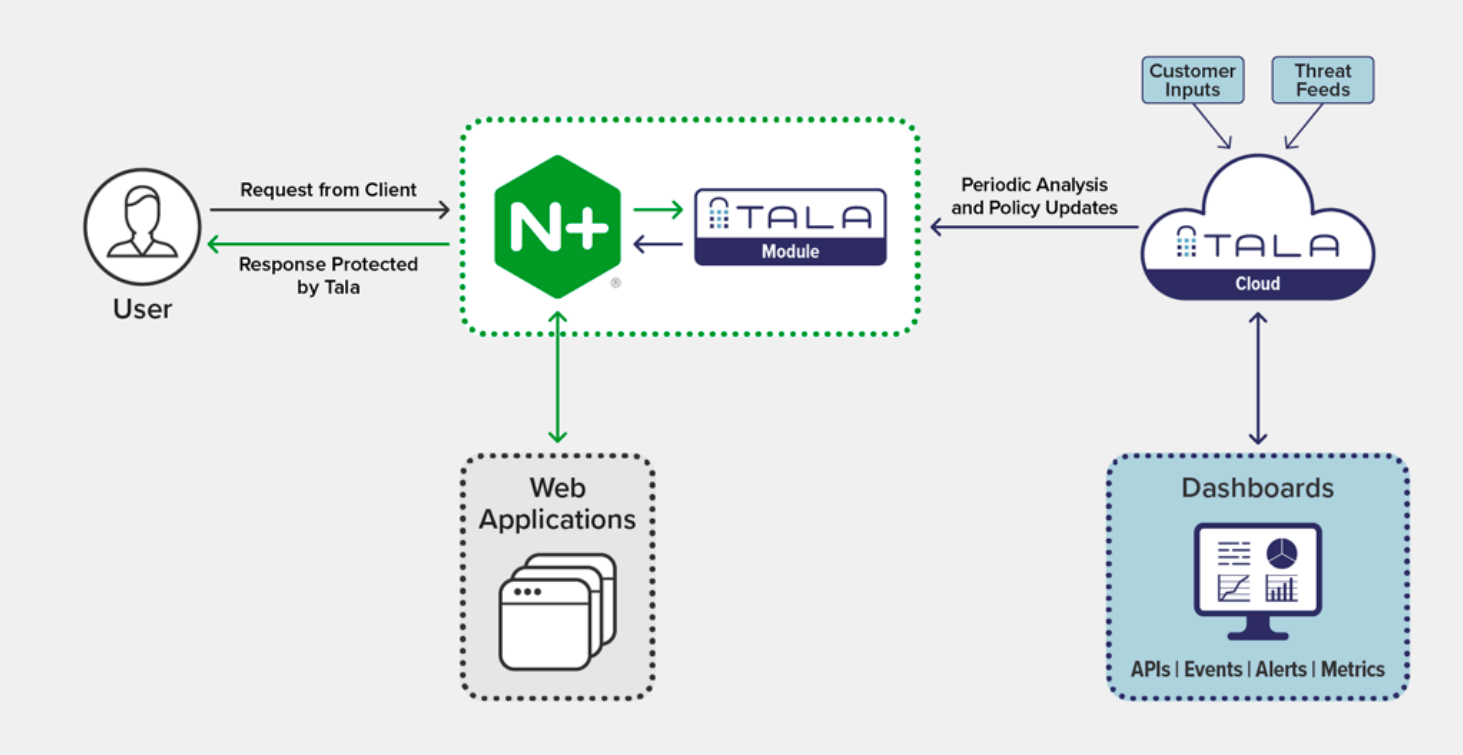


Tala Security Solutions

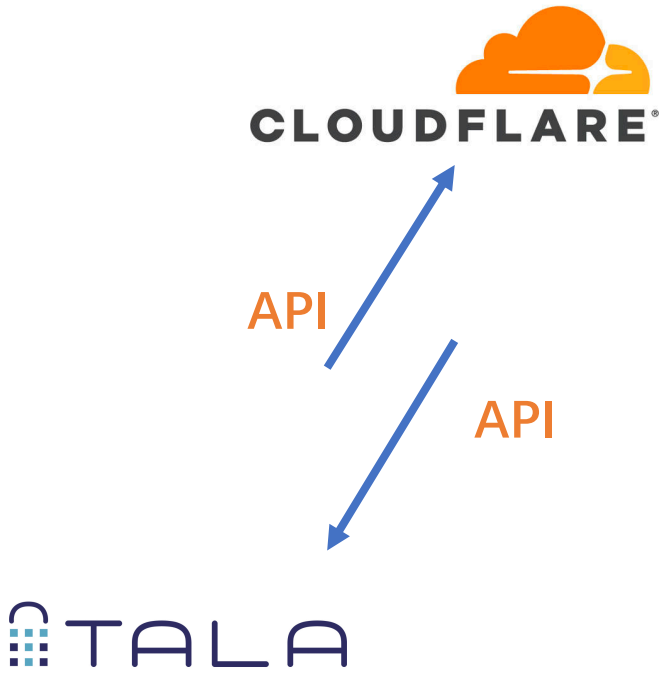
Technology	Advantages	Challenges
HTTP Security Headers (CSP/SRI)	- Specifications by w3c standards, implemented by most browsers - Enforcement happens at highest privilege - Averse to code obfuscations - Mobile browser coverage	- No DOM XSS protection - Hard to implement over large assets - Post policy domain compromise - Domain reputation - First party compromise - Too much noise from violation reporting (csp-wtf analysis)
Cross Origin iframe	- Nothing noteworthy	- Requires restructuring of the code - Not foolproof: Attack code present in 3rd party can prevent the iframe from loading, and skin it with attacker's iframe (no src attribute)
Javascript vs Javascript	- Nothing noteworthy	- Needs to load first, hence performance is a problem - Operates at the same privilege as the attacker

Tala Security Deployment

Tala & NGINX Plus



Tala & Cloudflare



Tala Security Solutions

Advantage

- Generate client-side policy involvling AI automaticlly
- Collect CSP Report and monitor event
- Collect JSHook Report and monitor event