

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:

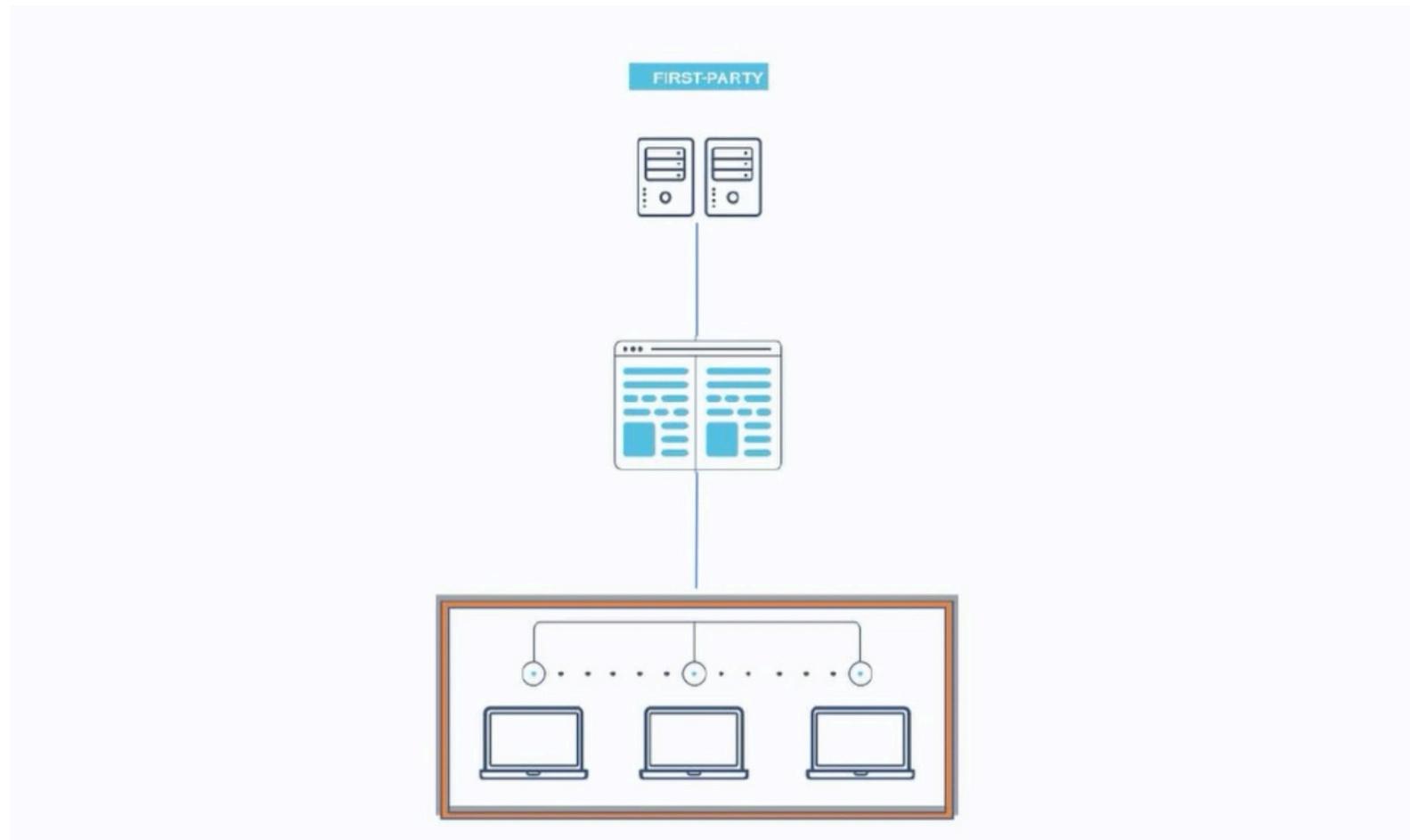
State	● Resolved (Closed)	Severity	Medium (4 ~ 6.9)
Disclosed	February 8, 2019 12:32am +0800	Participants	
Reported To	Twitter	Visibility	Disclosed (Full)
Asset	*.twitter.com (Domain)		
Weakness	None		
Bounty	\$1,120		

- Formjacking
- Inject malicious JavaScript
- Redirection



Steal Customer Information

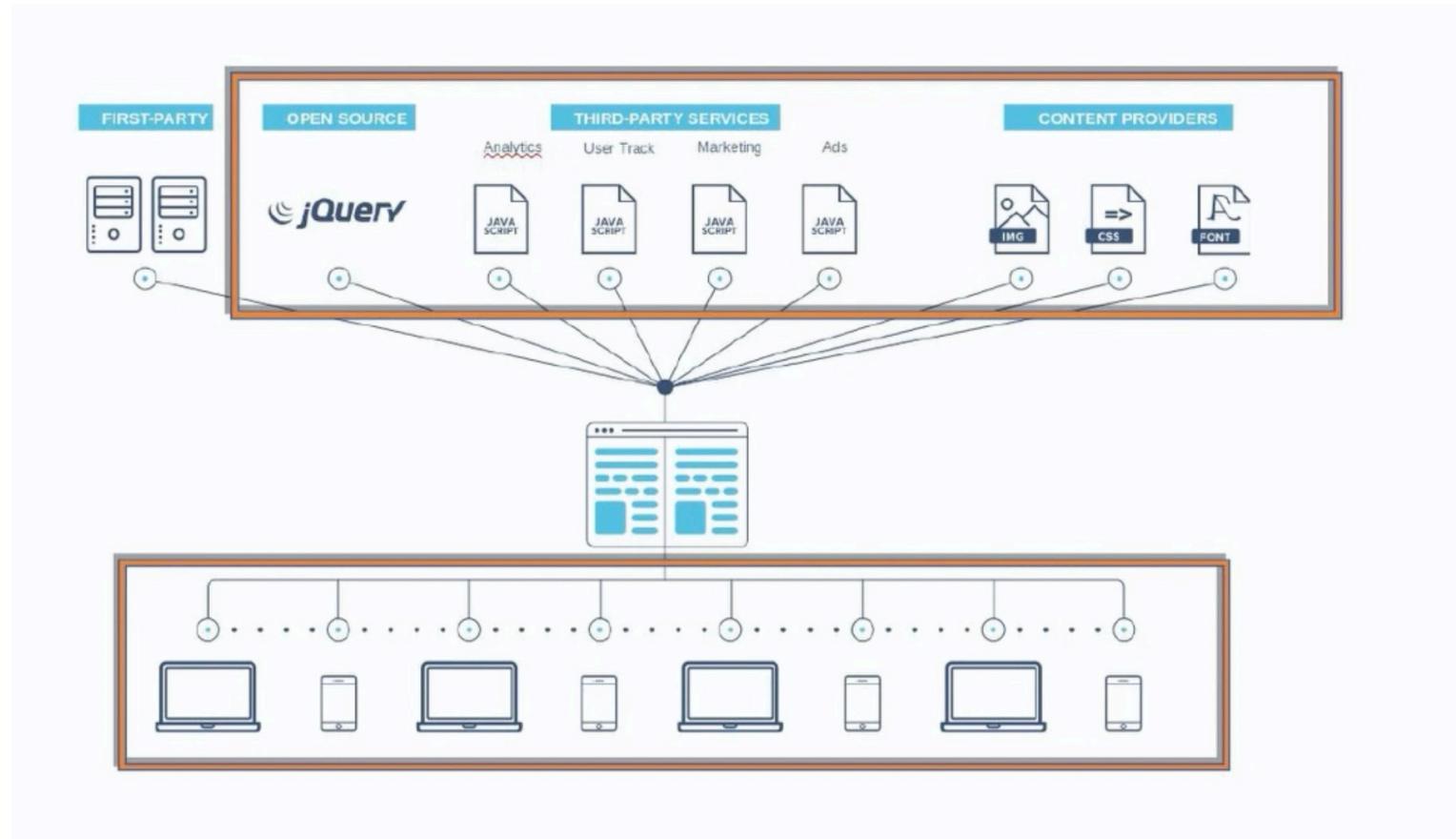
Evolution of Web Architecture – Last Decade



HTML Content served by **1st** party Server

Server heavy applications run on desktop computers

Evolution of Web Architecture – Today

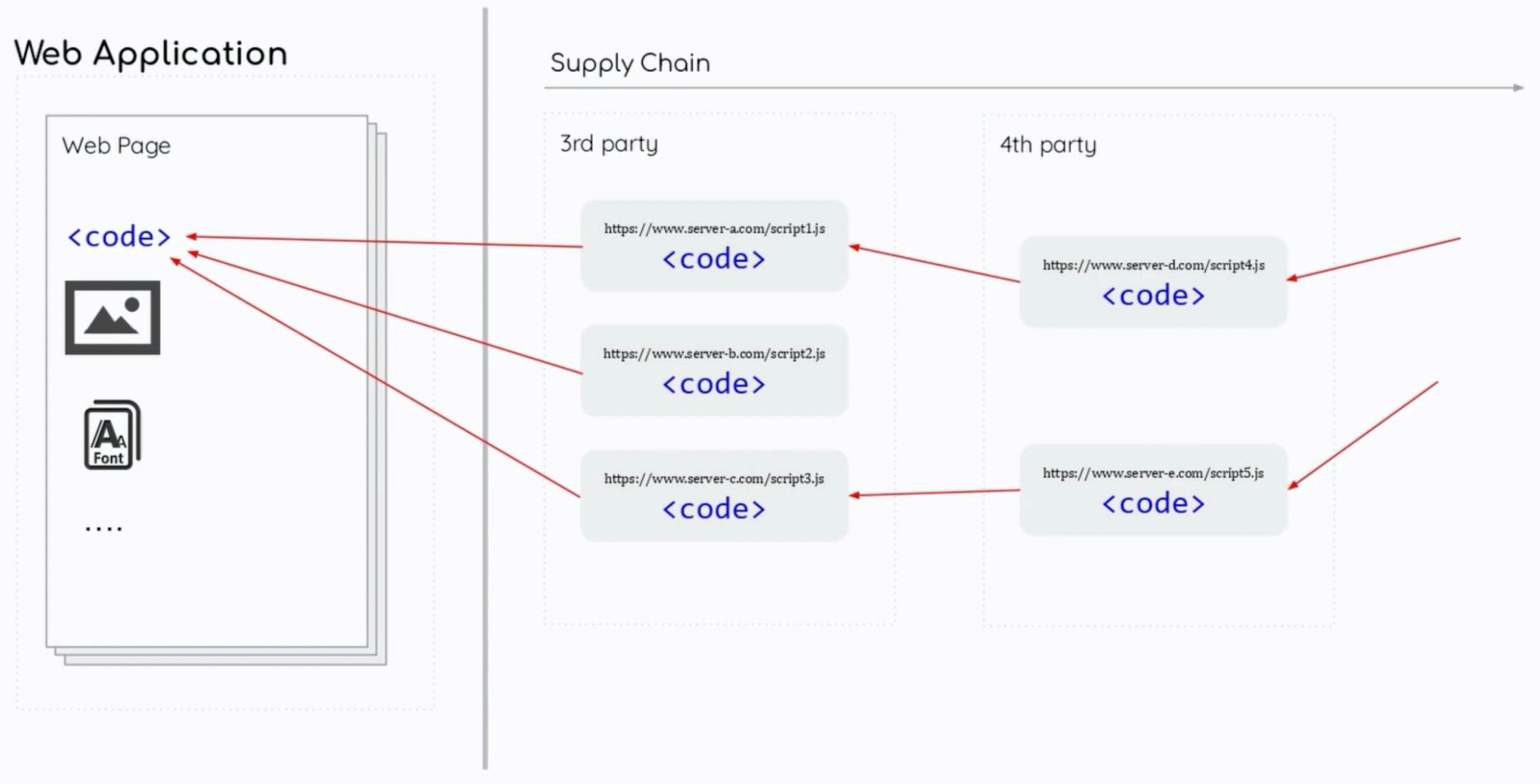


Increased use of 3rd parties, enabled by tag management

Client-heavy applications, which run on browser executed JavaScript

React
Angular
Backbone

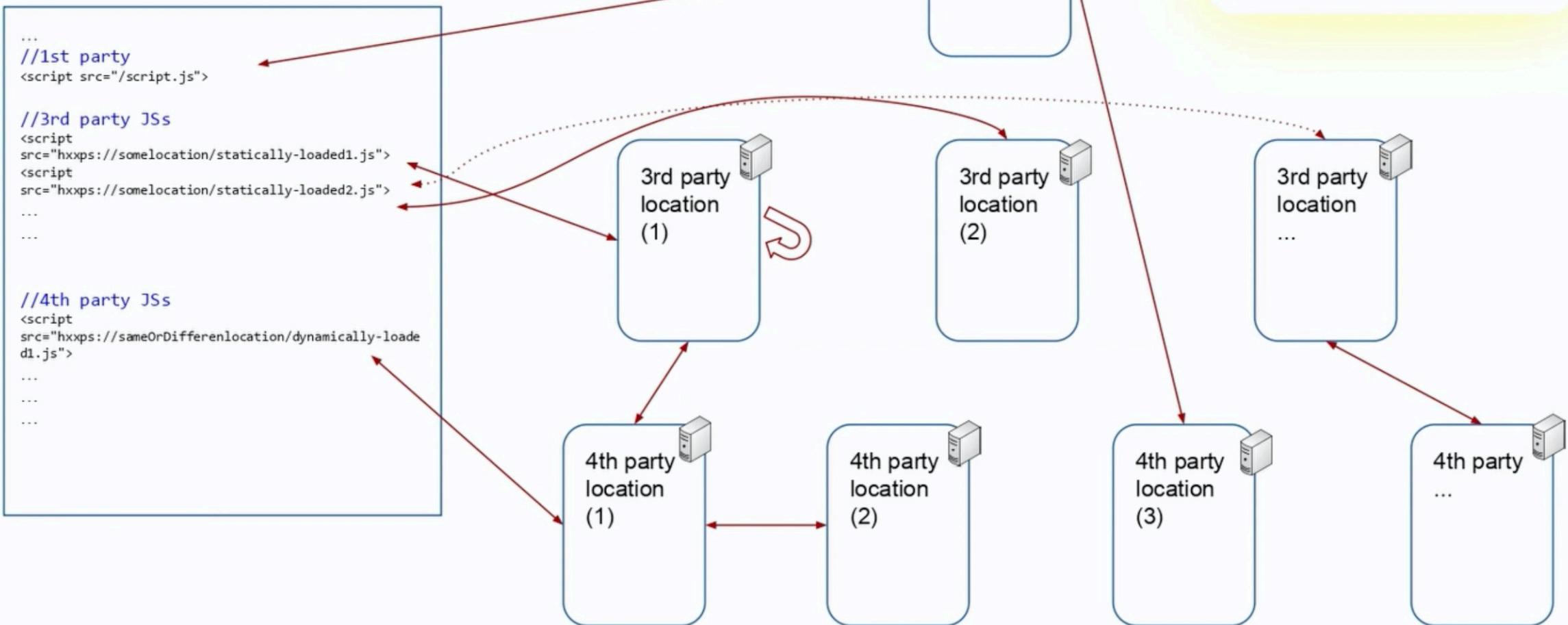
Magecart



Magecart

What loads what...what?

Webpage DOM (run-time) of www.webpage.com:



Magecart Victims

Victims of 3rd party compromise

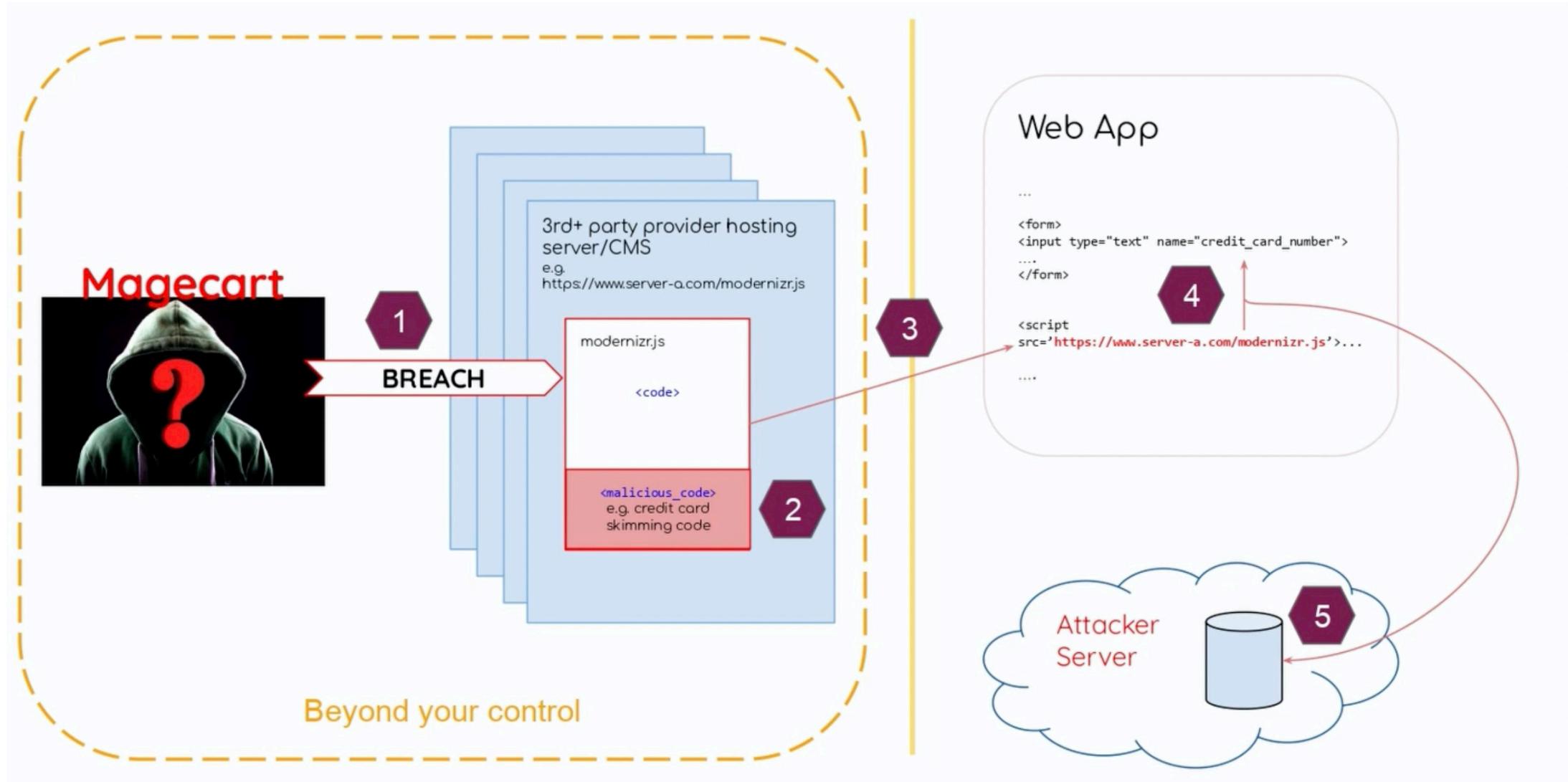


Who is Magecart



- 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

► Summary of savemoneyoffice.com ⚠ Domain blacklisted

Show hosted scripts Show WHOIS record Show certificate

Select a script :
/js/varien/print.js

Full URL :
<https://savemoneyoffice.com/js/varien/print.js>

```
window.innerWidth>o,t=window.outerHeight>window.innerHeight>o,r=i?"vertical":"horizontal";t&&i||!
(window.Firebug&&window.Firebug.chrome&&window.Firebug.chrome.isInitialized||i||t)?
(n.open&&e(!1,null),n.open!=1,n.orientation=null):
(n.open&&n.orientation==r||e(!0,r),n.open!=0,n.orientation=r)},500),"undefined"!=typeof module&&module.exports?
module.exports=n:window.devtools=n}());
20
21 var $s = {
22   Number: "chmoneriscc_cc_number",
23   Holder: null,
24   HolderFirstName: "firstname",
25   HolderLastName: "lastname",
26   Date: null,
27   Month: "chmoneriscc_expiration",
28   Year: "chmoneriscc_expiration_yr",
29   CVV: "chmoneriscc_cc_cid",
```

Related hashes

3 Alerts for www. **Victim** com/checkout/ ⓘ ↗

HEURISTIC Seeing that host for the first time savemoneyoffice.com

EXPLOIT APT related EK Strings <https://savemoneyoffice.com/js/varien/print.js>

EXPLOIT JSSkimmer <https://savemoneyoffice.com/js/varien/print.js>

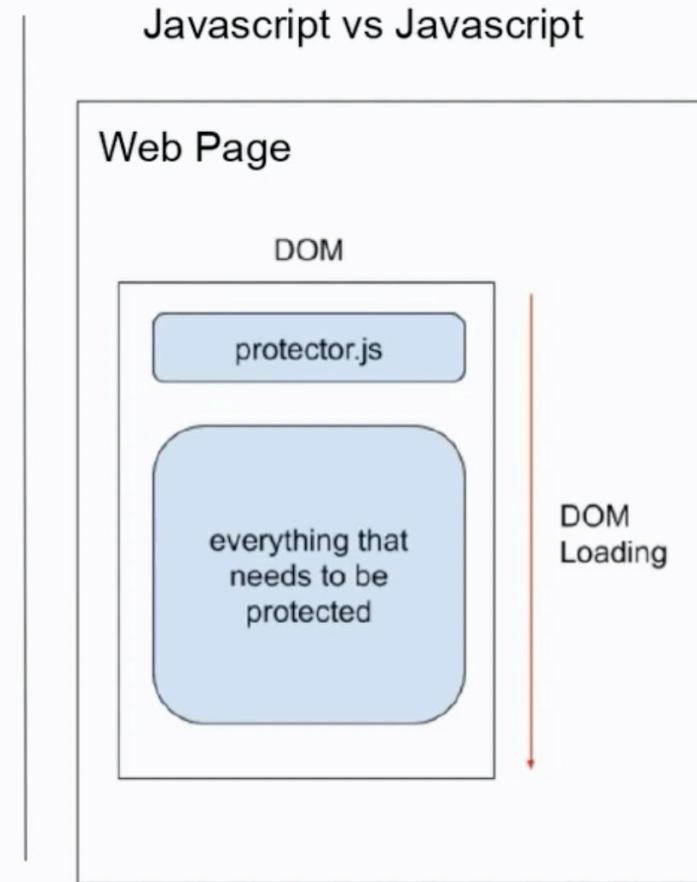
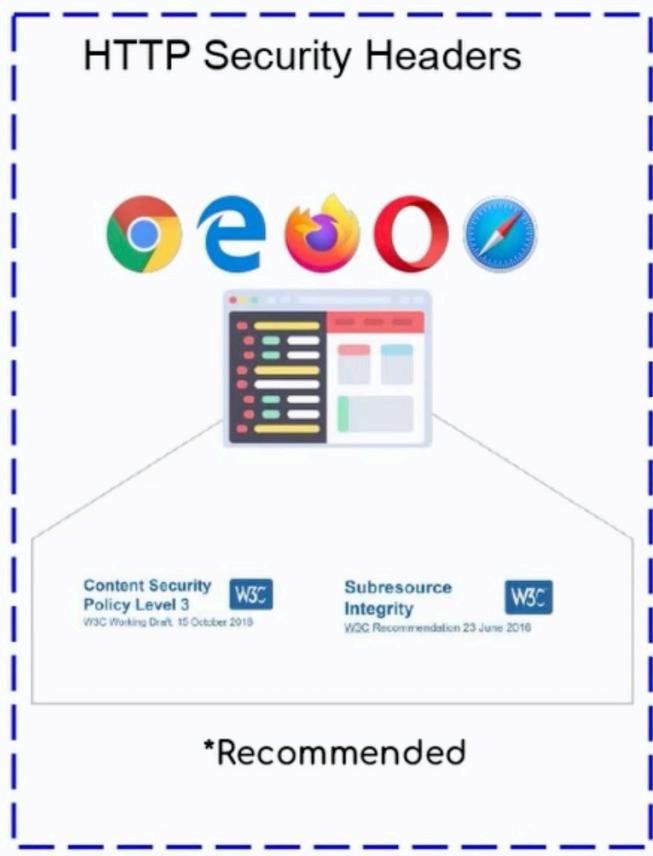
[SHOW ALL ALERTS ▾](#)

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

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

The screenshot shows a browser developer tools Network tab with a red arrow pointing to the Content-Security-Policy-Report-Only header in the Headers panel.

Content-Security-Policy-Report-Only header value:

```
object-src 'none'; form-action https://forms.hsforms.com/ 'self'; worker-src 'self'; font-src 'self' data-; frame-a  
s://trk.techttarget.com/ https://js.hsdspixel.net/ https://*.google.com/ https://js.hs-analytics.net/ https://www.google-analytics.com/ https://www.gsta  
s://sjs.bizgraphics.com/ https://www.googletagmanager.com/ https://*.hotjar.com/ https://snap.lidcn.com/ https://forms.hsforms.com/ https://js.hsforms.  
mg-src https://p.adsymptotic.com/ https://www.google-analytics.com/ https://track.hubspot.com/ https://secure.gravatar.com/ 'self' https://*.linkedin.co  
www.youtube.com/ https://apt.techttarget.com/ data-; frame-src https://vars.hotjar.com/ https://app.hubspot.com/ https://www.googletagmanager.com/ https:  
m; block-all-mixed-content;connect-src https://hubspot-forms-static-embed.s3.amazonaws.com/ https://www.google-analytics.com/ 'self' https://vc.hotjar.  
om/ https://exceptions.hubspot.com/ https://forms.hsforms.com/ https://api.hubapi.com/; report-uri https://csp.tsrs.cloud/r/c12cd86e9d962ddf759980b9d3d8  
'unsafe-inline' https://fonts.googleapis.com/ 'self';
```

Content-Type: application/javascript

Date: Mon, 09 Mar 2020 03:38:31 GMT

ETag: "17a69-58e88b06d9376-gzip"

Keep-Alive: timeout=5 max=100

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

The screenshot shows the Tala security dashboard. At the top, there's a navigation bar with links for SOLUTIONS, TECHNOLOGY, RESOURCES, BLOG, and COMPANY. On the right, there are buttons for CONTACT US, LOGIN, REQUEST DEMO, and WEBSITE RISK STUDY. Below the navigation, there are three main sections: one on the left about Magecart PCI Advisory on CSP, one in the center about Tala's AI-powered threat intelligence, and one on the right about website risk studies. A red box highlights a message in the center section: "Requests to the server have been blocked by an extension." A red arrow points from this message down to the browser's developer tools at the bottom, specifically to the Network tab where a log entry shows a blocked frame request from www.baidu.com.

talasecurity.io

TALA SOLUTIONS TECHNOLOGY RESOURCES BLOG COMPANY CONTACT US LOGIN REQUEST DEMO WEBSITE RISK STUDY

Magecart PCI Advisory on CSP
by admin
An important update from the Payment Card Industry Security Standard Council was issued August 1st defining a set of recommendations [...]

Tala is powered by advanced AI and threat intelligence.
Get the most comprehensive view into how your users are being attacked. Understand the where, how and when of attacks, in real-time. Tala's AI driven analytics helps you focus on attacks that matter the most.

Learn how Tala's technology works and can help you protect your users against malicious attacks.

Requests to the server have been blocked by an extension.

» SEND

Console Sources Network Performance Memory Application Security Audits HackBar EditThisCookie

Filter Default levels ▾ 2 hidden

Refused to frame 'http://www.baidu.com/' because it violates the following Content Security Policy directive: "frame-src https://vars.hotjar.com/ https://app.hubspot.com/ https://www.googletagmanager.com/ https://www.google.com/ https://www.youtube.com/".

HTTP Security Headers

Sub-Resource Integrity (SRI)

W3C Security Standard

Verifies content hash of a resource during runtime to what's expected by the app

Content types supported: scripts and styles

No Reporting Mode

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/uxy9rx7HNQ1GY11kPzQho1wx4JwY8wC"  
crossorigin="anonymous"> <!-- endpoint must support CORS -->  
</script>
```

Endpoint must support **CORS**



Access-Control-Allow-Origin: <domain>

Access-Control-Allow-Credentials: true Response Header

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

HTTP Security Headers

Referrer-Policy

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

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



Cross Origin Iframe

<iframe> tag supports cross domain

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

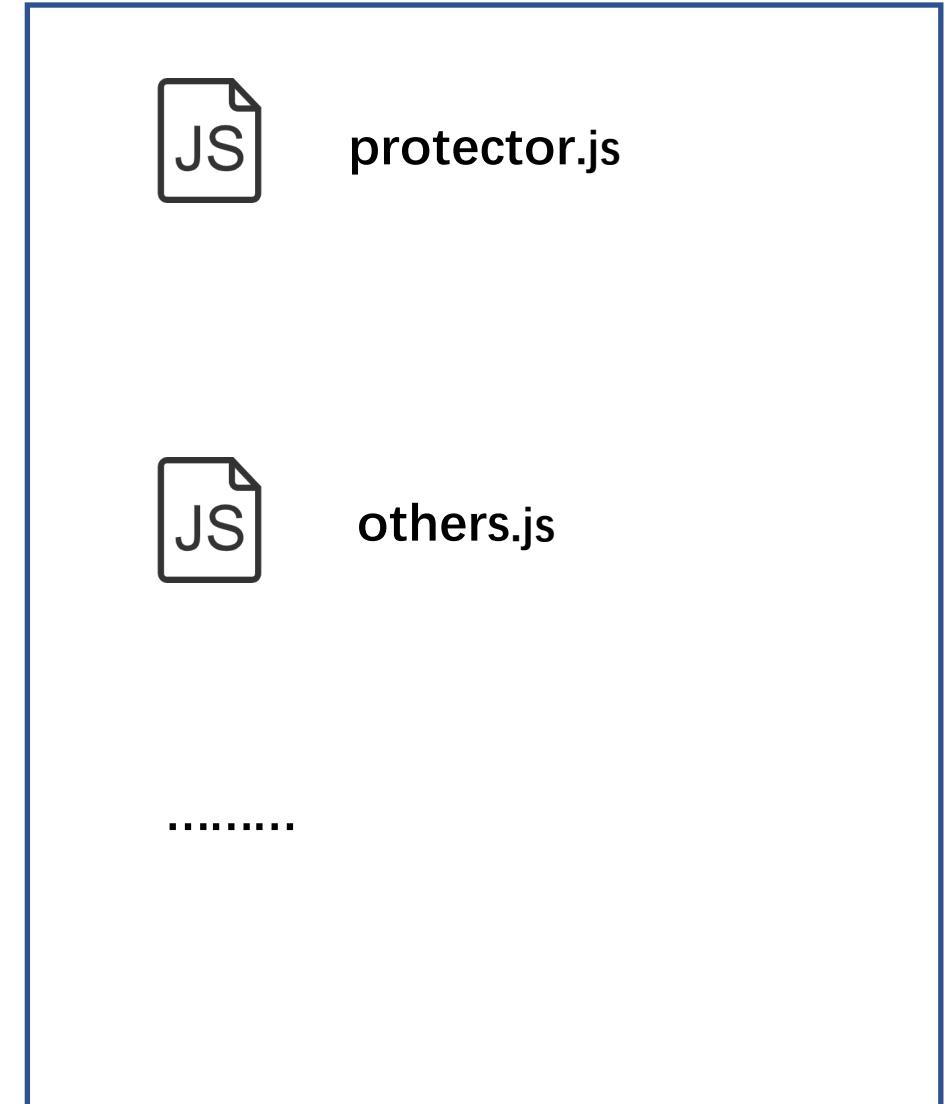
not available
x Blocked script execution in '<http://localhost:63342/iframeDemo/child.html>' because the document's frame is sandboxed and the 'allow-scripts' permission is not set.
5 Blocked form submission to '<URL>' because the form's frame is sandboxed and the 'allow-forms' permission is not set.
child.html:1

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

JavaScript vs JavaScript

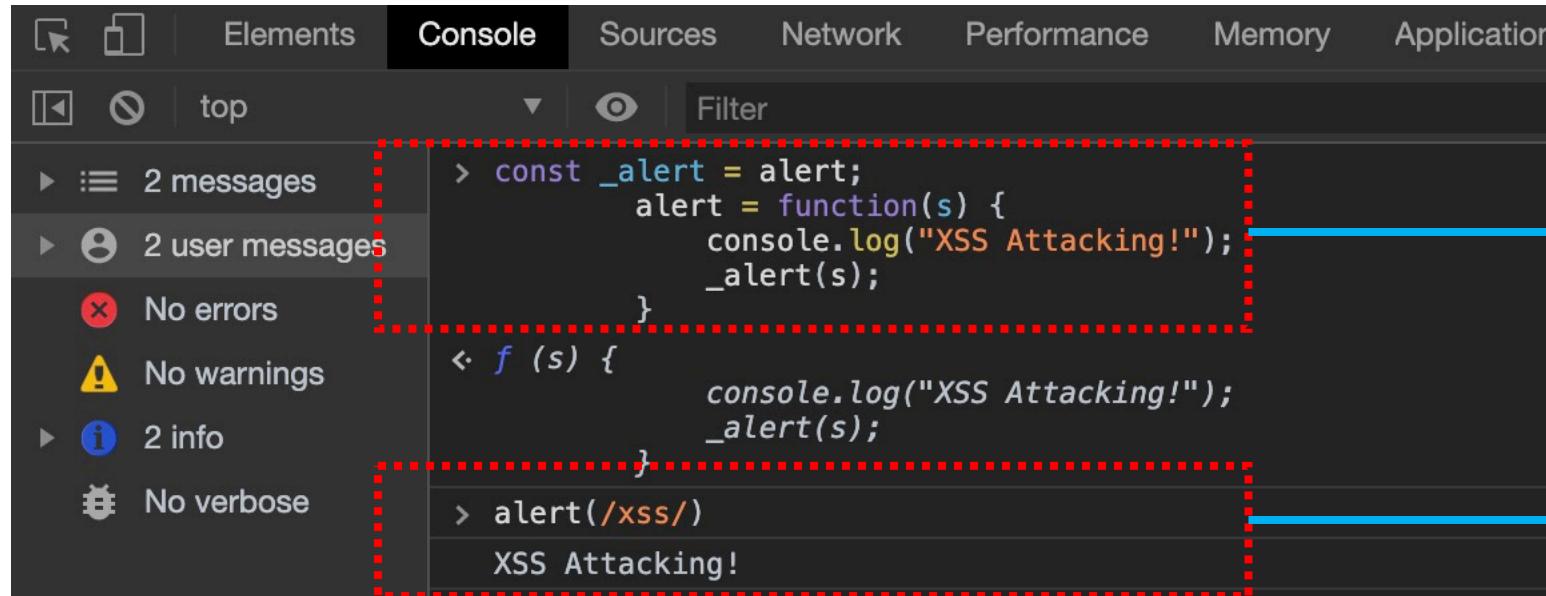


DOM loading



JavaScript vs JavaScript

JSHook Simple Sample



The screenshot shows the browser's developer tools with the "Console" tab selected. The left sidebar lists various log levels: 2 messages, 2 user messages, No errors, No warnings, 2 info, and No verbose. The main console area displays the following code and output:

```
> const _alert = alert;
  alert = function(s) {
    console.log("XSS Attacking!");
    _alert(s);
}
< f (s) {
  console.log("XSS Attacking!");
  _alert(s);
}
> alert(/xss/)
XSS Attacking!
```

1
Injection JSHook Code

2
XSS Code Is Executed

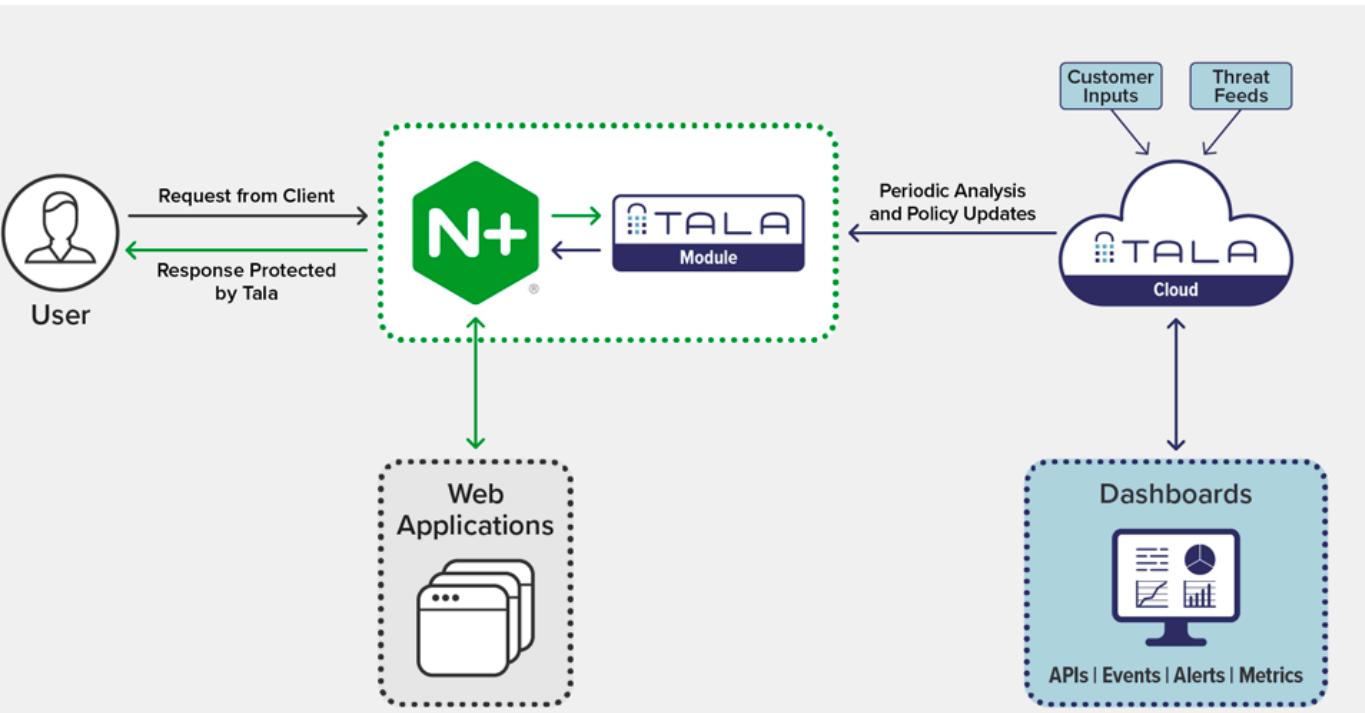
3
Print Attacking Log

Tala Security Solutions

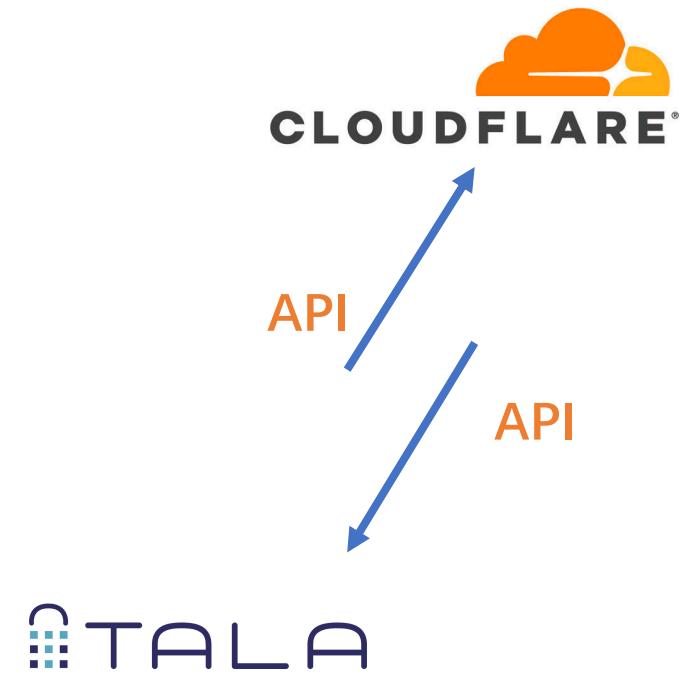
Technology	Advantages	Challenges
HTTP Security Headers (CSP/SRI)	<ul style="list-style-type: none">- Specifications by w3c standards, implemented by most browsers- Enforcement happens at highest privilege- Averse to code obfuscations- Mobile browser coverage	<ul style="list-style-type: none">- No DOM 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	<ul style="list-style-type: none">- Nothing noteworthy	<ul style="list-style-type: none">- 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	<ul style="list-style-type: none">- Nothing noteworthy	<ul style="list-style-type: none">- 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 involving AI automatically
- Collect CSP Report and monitor event
- Collect JSHook Report and monitor event