Accept All Exploits
Exploring the Security Impact of Cookie Banners

David Klein, Marius Musch, Thomas Barber, Moritz Kopmann, Martin Johns

david.klein@tu-braunschweig.de
How we came up with the idea for this paper

In 2020 we looked for websites susceptible to Client-Side Cross Site Scripting (XSS)
let name = location.hash.substr(1);
let greeting = "Hello, " + name;
/*
 * Application code
 */
div.innerHTML = greeting;
Client Side XSS

**Source:** Attacker controlled data

```javascript
let name = location.hash.substr(1);
let greeting = "Hello, " + name;
/*
 Application code
 */
div.innerHTML = greeting;
```
Client Side XSS

**Sink:** Turned into (executable) code

```
let name = location.hash.substr(1);
let greeting = "Hello, " + name;
/*
   Application code
*/
div.innerHTML = greeting;
```

Sink
Client Side XSS

Data flow from source to sink

Source

```javascript
let name = location.hash.substr(1);
let greeting = "Hello, " + name;
/*
  Application code
*/
div.innerHTML = greeting;
```

Sink
```javascript
let name = location.hash.substr(1);
let greeting = "Hello, " + name;

/*
 Application code
 */
div.innerHTML = greeting;
```

Automated detection of Client-Side XSS via e.g., taint tracking enabled browser
How we came up with the idea for this paper

In 2020 we looked for websites susceptible to Client-Side Cross Site Scripting (XSS)

Initial sanity check of our setup:
How we came up with the idea for this paper

In 2020 we looked for websites susceptible to Client-Side Cross Site Scripting (XSS)

Initial sanity check of our setup: compare results with literature!
How we came up with the idea for this paper

In 2020 we looked for websites susceptible to Client-Side Cross Site Scripting (XSS)

Initial sanity check of our setup: compare results with literature!

<table>
<thead>
<tr>
<th></th>
<th>25 Million Flows</th>
<th>DOMsday</th>
<th>Our Study</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td>April 2013</td>
<td>Jan. 2017</td>
<td>Oct. 2020</td>
</tr>
<tr>
<td>Vantage Point</td>
<td>Germany</td>
<td>USA</td>
<td>Germany</td>
</tr>
<tr>
<td>Pages</td>
<td>504 275</td>
<td>44 722</td>
<td>390 092</td>
</tr>
<tr>
<td>Frames</td>
<td>4 358 031</td>
<td>319 481</td>
<td>1 111 821</td>
</tr>
<tr>
<td>Frames/Page</td>
<td>8.64</td>
<td>7.14</td>
<td>2.85</td>
</tr>
</tbody>
</table>
How we came up with the idea for this paper

In 2020 we looked for websites susceptible to Client-Side Cross Site Scripting (XSS)

Initial sanity check of our setup: compare results with literature!

<table>
<thead>
<tr>
<th>Date</th>
<th>25 Million Flows</th>
<th>DOMsday</th>
<th>Our Study</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td>April 2013</td>
<td>Jan. 2017</td>
<td>Oct. 2020</td>
</tr>
<tr>
<td>Vantage Point</td>
<td>Germany</td>
<td>USA</td>
<td>Germany</td>
</tr>
<tr>
<td>Pages</td>
<td>504 275</td>
<td>44 722</td>
<td>390 092</td>
</tr>
<tr>
<td>Frames</td>
<td>4 358 031</td>
<td>319 481</td>
<td>1 111 821</td>
</tr>
<tr>
<td>Frames/Page</td>
<td><strong>8.64</strong></td>
<td><strong>7.14</strong></td>
<td><strong>2.85</strong></td>
</tr>
</tbody>
</table>

→ Less than one third frames per page compared with 25 Million Flows!
Debugging time

Initial thought: Less XSS is believable, but less frames sounds really strange
Debugging time

Initial thought: Less XSS is believable, but less frames sounds really strange

Are we counting them wrong? window.frames.length
Debugging time

Initial thought: Less XSS is believable, but less frames sounds really strange

Are we counting them wrong? `window.frames.length`

Yes, but that did not really matter
Debugging time

Initial thought: Less XSS is believable, but less frames sounds really strange

Are we counting them wrong? `window.frames.length`

Yes, but that did not really matter

### Explanation

It’s “wrong” due to missing dynamically added frames

However, we took that into account and got: **2.95**
Debugging time

Initial thought: Less XSS is believable, but less frames sounds really strange

Are we counting them wrong? window.frames.length

Yes, but that did not really matter

Once someone tested with a VPN the issue became clear: German IP address
Debugging time

Initial thought: Less XSS is believable, but less frames sounds really strange

Are we counting them wrong? `window.frames.length`

Yes, but that did not really matter

Once someone tested with a VPN the issue became clear: German IP address

VPN to server in the US to the rescue!
## Result

<table>
<thead>
<tr>
<th>Date</th>
<th>25 Million Flows</th>
<th>DOMsday</th>
<th>Our Study</th>
<th>Our Study (VPN)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td>April 2013</td>
<td>Jan. 2017</td>
<td>Oct. 2020</td>
<td>April 2021</td>
</tr>
<tr>
<td>Vantage Point</td>
<td>Germany</td>
<td>USA</td>
<td>Germany</td>
<td>USA</td>
</tr>
<tr>
<td>Pages</td>
<td>504 275</td>
<td>44 722</td>
<td>390 092</td>
<td>876 872</td>
</tr>
<tr>
<td>Frames</td>
<td>4 358 031</td>
<td>319 481</td>
<td>1 111 821</td>
<td>4 389 872</td>
</tr>
<tr>
<td>Frames/Page</td>
<td><strong>8.64</strong></td>
<td><strong>7.14</strong></td>
<td><strong>2.85</strong></td>
<td><strong>5.00</strong></td>
</tr>
</tbody>
</table>
Surfing the Web today looks like this:
Surfing the Web today looks like this:

Datenschutz und Nutzungserlebnis auf BILD.de

**Ohne Tracking und Cookies* nutzen**


Wenn Sie BILD Pur abonnieren, können Sie die auf bILD.de verfügbaren Inhalte ohne Tracking und Cookies* lesen. Sofern Sie bereits BILDplus-Abonnement sind und BILD Pur zusätzlich abonnieren, können Sie auch die BILDplus-Inhalte ohne Tracking und Cookies* lesen.

**Mit Tracking und Cookies nutzen**

Sie können unser Angebot auch nutzen, ohne einen Vertrag abzuschließen. Wir übermitteln in diesem Fall personenbezogene Daten an Drittanbieter, die uns helfen, unser Webangebot zu verbessern und zu finanzieren. In diesem Zusammenhang werden auch Nutzungsprofile (u.a. auf Basis von Cookie-ID) gebildet und angereichert, auch außerhalb des EWR verarbeitet. Hierzu übermitteln wir an diese Drittanbieter auch Ihre Privatsphäreinstellungen bzw. Präferenzen in Form einer codierten Zeichenfolge (so. TC-String). Hierfür und um bestimmte Dienste zu nachfolgend aufgeführten Zwecken verwenden zu dürfen, benötigen wir Ihre Einwilligung. Indem Sie "Alle akzeptieren" klicken, stimmen Sie diesen (jederzeit widerruflich) zu. Dies umfasst auch Ihre Einwilligung in die Übermittlung bestimmter personenbezogener Daten in Drittländer, u.a. die USA, nach Art. 49 (1) (a) DSGVO. Sie können Ihre Auswahl jederzeit unter "Widerruf Tracking" am Seitenende mit Wirkung für die Zukunft widerrufen.

- Informationen auf einem Gerät speichern und/oder abrufen
- Personalisierte Anzeigen und Inhalte, Anzeigen- und Inhaltsmessungen, Erkenntnisse über Zielgruppen und Produktentwicklungen
- Fremdinhalte anzeigen (Soziale Netzwerke, Videos)
- Verwendung und Weitergabe von Nutzerkennungen zu Werbezwecken

* In BILD Pur werden keine einwilligungspflichtigen Datenverarbeitungen vorgenommen und nur solche Cookies und ähnliche Technologien verwendet, die zur Erbringung dieses Dienstes unbedingt erforderlich sind.

Jetzt BILD Pur abonnieren

Alle akzeptieren

Details dazu finden Sie im Privacy Center.

FAQ | Datenschutzerklärung | Impressum
Surfing the Web today looks like this:
Surfing the Web today looks like this:

We can collect and store data for a number of reasons, with the purposes of personalization and keeping our services free. As a result, we use cookies and similar technologies to track and analyze website usage. To manage your cookie settings, please click on the "Manage cookies" button.
Surfing the Web today looks like this:
Surfing the Web today looks like this:
Surfing the Web today looks like this:
Cookie Banners: Background

Result of privacy regulations by the European Union
- ePrivacy Directive
- General Data Protection Regulation (GDPR)
Cookie Banners: Background

Result of privacy regulations by the European Union
▶ ePrivacy Directive
▶ General Data Protection Regulation (GDPR)

Goal:
▶ Give people control over their private data
Cookie Banners: Background

Result of privacy regulations by the European Union

- ePrivacy Directive
- General Data Protection Regulation (GDPR)

Goal:
- Give people control over their private data
  - By e.g., requiring consent for tracking
Cookie Banners: Background

Result of privacy regulations by the European Union
▶ ePrivacy Directive
▶ General Data Protection Regulation (GDPR)

Goal:
▶ Give people control over their private data
  – By e.g., requiring consent for tracking
▶ Sounds good, right?
Cookie Banners: Background

Result of privacy regulations by the European Union
▶ ePrivacy Directive
▶ General Data Protection Regulation (GDPR)

Goal:
▶ Give people control over their private data
  – By e.g., requiring consent for tracking
▶ Sounds good, right?
  – Let's try it
Controlling your privacy

Once you found the (well hidden) button to interact with it:
Controlling your privacy

Once you found the (well hidden) button to interact with it:

Over **150** third parties, had to include a search feature because the list is so huge!
Cookie Banner under the hood

```javascript
__tcfapi("addEventListener", 2, function(tcData, success) {
  if (success && tcData.unicLoad === true) {
    if(!window._initAds) {
      window._initAds = true;
      var script = document.createElement('script');
      script.async = true;
      script.setAttribute('data-ad-client', 'ca-pub-xxxxxxxxx');
      script.src = 'https://pagead2.googlesyndication.com/...';
      document.head.appendChild(script);
    }
  }
});
```
Cookie Banner under the hood

```javascript
__tcfapi("addEventListner", 2, function(tcData, success) {
  if (success && tcData.unicLoad === true) {
    if(!window._initAds) {
      window._initAds = true;
      var script = document.createElement('script');
      script.async = true;
      script.setAttribute('data-ad-client', 'ca-pub-xxxxxxxx');
      script.src = 'https://pagead2.googlesyndication.com/...';
      document.head.appendChild(script);
    }
  }
});
```

Register event for user interaction
Cookie Banner under the hood

```javascript
__tcfapi("addEventListener", 2, function(tcData, success) {
    if (success && tcData.unicLoad === true) {
        if(!window._initAds) {
            window._initAds = true;
            var script = document.createElement('script');
            script.async = true;
            script.setAttribute('data-ad-client', 'ca-pub-xxxxxxxxx');
            script.src = 'https://pagead2.googlesyndication.com/...';
            document.head.appendChild(script);
        }
    }
});
```

User consented?
Cookie Banner under the hood

```javascript
__tcfapi("addEventListener", 2, function(tcData, success) {
    if (success && tcData.unicLoad === true) {
        if(!window._initAds) {
            window._initAds = true;

            var script = document.createElement('script');
            script.async = true;
            script.setAttribute('data-ad-client', 'ca-pub-xxxxxxxx');
            script.src = 'https://pagead2.googlesyndication.com/...';
            document.head.appendChild(script);
        }
    }
});
```

Create script tag to load Google ads
Cookie Banner under the hood

```javascript
__tcfapi("addEventListener", 2, function(tcData, success) {
    if (success && tcData.unicLoad === true) {
        if(!window._initAds) {
            window._initAds = true;
            var script = document.createElement('script');
            script.async = true;
            script.setAttribute('data-ad-client', 'ca-pub-xxxxxxxxx');
            script.src = 'https://pagead2.googlesyndication.com/...';
            document.head.appendChild(script);
        }
    }
});
```

Add script to DOM and execute it in websites security domain!
Our Work

Basic idea: Consenting leads to additional and complex code being executed

Research Questions:
1) Can we automate consenting and measure its effect?
2) Does this additional code actually make the user more vulnerable?
Our Work

Basic idea: Consenting leads to additional and complex code being executed
→ This will become the default view of the user after consenting!
Our Work

Basic idea: Consenting leads to additional and complex code being executed
→ This will become the default view of the user after consenting!

Research Questions:
Our Work

Basic idea: Consent ing leads to additional and complex code being executed → This will become the default view of the user after consenting!

Research Questions:
1) Can we automate consenting and measure its effect?
Our Work

Basic idea: Consenting leads to additional and complex code being executed
→ This will become the default view of the user after consenting!

Research Questions:
1) Can we automate consenting and measure its effect?
2) Does this additional code actually make the user more vulnerable?
Acceptify

Tool to maximize consent on banners
Tool to maximize consent on banners

How to do this?
Tool to maximize consent on banners

How to do this?

→ Exploit combination of Dark patterns & legal requirements
Acceptify: Implementation
Acceptify: Implementation

**Candidate Selection:**

→ all DOM elements matching these criteria:

▶ Clickable
▶ Textual content contains affirmative phrase
▶ ≤ 6 words of text and ≤ 200 characters of text
Acceptify: Implementation

Candidate Selection:
→ all DOM elements matching these criteria:
  ▶ Clickable
  ▶ Textual content contains affirmative phrase
  ▶ \( \leq 6 \) words of text and \( \leq 200 \) characters of text

Candidate Pruning:
→ Drop all elements matching one filter:
  ▶ Invisible
  ▶ Require the user to scroll
  ▶ Textual content contains negation
  ▶ Not on top
Acceptify: Efficacy

Automated Verification:

Transparency & Consent Framework as verification oracle

88.4% Success Rate

Manual Verification:

Save screenshot of banner before consenting & manually inspect them

19.2% False Negatives

1.2% False Positives
Acceptify: Efficacy

**Automated Verification:**

- Transparency & Consent Framework as verification oracle
- **88.4%** Success Rate
Acceptify: Efficacy

Automated Verification:
→ Transparency & Consent Framework as verification oracle
→ 88.4% Success Rate

Manual Verification:
Acceptify: Efficacy

**Automated Verification:**
- Transparency & Consent Framework as verification oracle
- **88.4%** Success Rate

**Manual Verification:**
- Save screenshot of banner before consenting & manually inspect them
- **19.2%** False Negatives
- **1.2%** False Positives
Experiment

**List selection:**
For each European and generic TLD: First 1000 entries of Tranco 1M list.
→ **28 718 Websites to visit**

**Execution:**

1. Visit each URL with “Project Foxhound”, our taint tracking enabled Firefox fork
Experiment

List selection:
For each European and generic TLD: First 1000 entries of Tranco 1M list.
→ 28 718 Websites to visit

Execution:
1. Visit each URL with “Project Foxhound”, our taint tracking enabled Firefox fork
2. Record information about cookies, frames, loaded scripts
Experiment

**List selection:**
For each European and generic TLD: First 1000 entries of Tranco 1M list.
→ **28 718** Websites to visit

**Execution:**
1. Visit each URL with “Project Foxhound”, our taint tracking enabled Firefox fork
2. Record information about cookies, frames, loaded scripts
3. Run Acceptify and iff successful:
Experiment

List selection:
For each European and generic TLD: First 1000 entries of Tranco 1M list.
→ 28 718 Websites to visit

Execution:

1. Visit each URL with “Project Foxhound”, our taint tracking enabled Firefox fork
2. Record information about cookies, frames, loaded scripts
3. Run Acceptify and iff successful:
   - Record information again
Experiment

**List selection:**
For each European and generic TLD: First 1000 entries of Tranco 1M list.
→ **28 718** Websites to visit

**Execution:**

1. Visit each URL with “Project Foxhound”, our taint tracking enabled Firefox fork
2. Record information about cookies, frames, loaded scripts
3. Run Acceptify and iff successful:
   - Record information again
   - Queue 20 sub pages to explore further
Experiment

List selection:
For each European and generic TLD: First 1000 entries of Tranco 1M list.
→ 28 718 Websites to visit

Execution:

1. Visit each URL with “Project Foxhound”, our taint tracking enabled Firefox fork
2. Record information about cookies, frames, loaded scripts
3. Run Acceptify and iff successful:
   - Record information again
   - Queue 20 sub pages to explore further
Experiment

List selection:
For each European and generic TLD: First 1000 entries of Tranco 1M list.
→ 28 718 Websites to visit

Execution:
1. Visit each URL with “Project Foxhound”, our taint tracking enabled Firefox fork
2. Record information about cookies, frames, loaded scripts
3. Run Acceptify and iff successful:
   - Record information again
   - Queue 20 sub pages to explore further

→ Acceptify detected and interacted with a Consent Button on 8149 (35.3%) websites
### Results: Loaded Resources

<table>
<thead>
<tr>
<th>Resource</th>
<th># Sites</th>
<th>Initial Visit</th>
<th>After Accept</th>
<th>Increase</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cookies</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>First Party</td>
<td>8085</td>
<td>71 538</td>
<td>119 318</td>
<td>66.8%</td>
</tr>
<tr>
<td>Third Party</td>
<td>7181</td>
<td>38 260</td>
<td>167 814</td>
<td>338.6%</td>
</tr>
<tr>
<td>Scripts</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>First Party</td>
<td>7699</td>
<td>97 953</td>
<td>98 739</td>
<td>0.8%</td>
</tr>
<tr>
<td>Third Party</td>
<td>7931</td>
<td>117 165</td>
<td>169 352</td>
<td>44.5%</td>
</tr>
</tbody>
</table>

→ Significant increase of executed third party code!
### Results: Loaded Resources

<table>
<thead>
<tr>
<th>Resource</th>
<th># Sites</th>
<th>Initial Visit</th>
<th>After Accept</th>
<th>Increase</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cookies</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>First Party</td>
<td>8085</td>
<td>71 538</td>
<td>119 318</td>
<td><strong>66.8%</strong></td>
</tr>
<tr>
<td>Third Party</td>
<td>7181</td>
<td>38 260</td>
<td>167 814</td>
<td><strong>338.6%</strong></td>
</tr>
<tr>
<td><strong>Scripts</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>First Party</td>
<td>7699</td>
<td>97 953</td>
<td>98 739</td>
<td><strong>0.8%</strong></td>
</tr>
<tr>
<td>Third Party</td>
<td>7931</td>
<td>117 165</td>
<td>169 352</td>
<td><strong>44.5%</strong></td>
</tr>
</tbody>
</table>

→ Significant increase of executed third party code!
## Results: Taint Flows

<table>
<thead>
<tr>
<th>Taint Flows</th>
<th>#Sites</th>
<th>Initial Visit</th>
<th>After Accept</th>
<th>Increase</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Taint Flows</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>URL → HTML</td>
<td>452</td>
<td>1970</td>
<td>2657</td>
<td>34.9%</td>
</tr>
<tr>
<td>URL → JavaScript</td>
<td>112</td>
<td>1480</td>
<td>3024</td>
<td>104.3%</td>
</tr>
<tr>
<td>URL → URL</td>
<td>7474</td>
<td>451808</td>
<td>740733</td>
<td>63.9%</td>
</tr>
<tr>
<td><strong>Reflected XSS:</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>URL → cookie</td>
<td>2645</td>
<td>20444</td>
<td>31942</td>
<td>56.2%</td>
</tr>
<tr>
<td>URL → LocalStorage</td>
<td>1542</td>
<td>17723</td>
<td>24743</td>
<td>39.6%</td>
</tr>
<tr>
<td><strong>Generic</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>URL → postMessage</td>
<td>499</td>
<td>2625</td>
<td>5863</td>
<td>123.4%</td>
</tr>
<tr>
<td><strong>Stored XSS:</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Total Increase:</strong></td>
<td></td>
<td></td>
<td></td>
<td>63.1%</td>
</tr>
</tbody>
</table>
## Results: Taint Flows

<table>
<thead>
<tr>
<th></th>
<th>#Sites</th>
<th>Initial Visit</th>
<th>After Accept</th>
<th>Increase</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Taint Flows</strong></td>
<td>7577</td>
<td>496 050</td>
<td>808 962</td>
<td>63.1%</td>
</tr>
<tr>
<td>Reflected XSS:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>URL → HTML</td>
<td>452</td>
<td>1970</td>
<td>2657</td>
<td>34.9%</td>
</tr>
<tr>
<td>URL → JavaScript</td>
<td>112</td>
<td>1480</td>
<td>3024</td>
<td>104.3%</td>
</tr>
<tr>
<td>URL → URL</td>
<td>7474</td>
<td>451 808</td>
<td>740 733</td>
<td>63.9%</td>
</tr>
<tr>
<td>Generic</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>URL → postMessage</td>
<td>499</td>
<td>2625</td>
<td>5863</td>
<td>123.4%</td>
</tr>
<tr>
<td>Stored XSS:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>URL → cookie</td>
<td>2645</td>
<td>20 444</td>
<td>31 942</td>
<td>56.2%</td>
</tr>
<tr>
<td>URL → localStorage</td>
<td>1542</td>
<td>17 723</td>
<td>24 743</td>
<td>39.6%</td>
</tr>
</tbody>
</table>

→ Significant increase of attack surface!
Validation

Based on taint flows we can automatically generate XSS payload URLs

Successful for 1395 domains

Validate by visiting twice:
1. With clean browser
2. After restoring cookies

Results:

<table>
<thead>
<tr>
<th>Group #</th>
<th>Sites</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directly vulnerable</td>
<td>73</td>
</tr>
<tr>
<td>Vulnerable after giving consent</td>
<td>44</td>
</tr>
<tr>
<td>Overlap</td>
<td>9</td>
</tr>
</tbody>
</table>

Increase 55%

Giving consent leads to more exploitable vulnerabilities!
Validation

Based on taint flows we can automatically generate XSS payload URLs

→ Successful for 1395 domains
Validation

Based on taint flows we can automatically generate XSS payload URLs

→ Successful for 1395 domains

Validate by visiting twice:
1. With clean browser
2. After restoring cookies
Validation

Based on taint flows we can automatically generate XSS payload URLs

→ Successful for 1395 domains

Validate by visiting twice:
  1. With clean browser
  2. After restoring cookies

Results:

<table>
<thead>
<tr>
<th>Group</th>
<th># Sites</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directly vulnerable</td>
<td>73</td>
</tr>
<tr>
<td>Vulnerable after giving consent</td>
<td>44</td>
</tr>
<tr>
<td>Overlap</td>
<td>9</td>
</tr>
<tr>
<td>Increase</td>
<td>55%</td>
</tr>
</tbody>
</table>
Validation

Based on taint flows we can automatically generate XSS payload URLs

→ Successful for 1395 domains

Validate by visiting twice:
  1. With clean browser
  2. After restoring cookies

Results:

<table>
<thead>
<tr>
<th>Group</th>
<th># Sites</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directly vulnerable</td>
<td>73</td>
</tr>
<tr>
<td>Vulnerable after giving consent</td>
<td>44</td>
</tr>
<tr>
<td>Overlap</td>
<td>9</td>
</tr>
<tr>
<td>Increase</td>
<td>55%</td>
</tr>
</tbody>
</table>

Giving consent leads to more exploitable vulnerabilities!
Key Takeaways

▶ Consenting to tracking has a profound impact on attack surface
Key Takeaways

- Consenting to tracking has a profound impact on attack surface
- Problematic for vulnerability scanning tools
Key Takeaways

▶ Consent to tracking has a profound impact on attack surface
▶ Problematic for vulnerability scanning tools
  – Unless they interact with consent banners they only see a subset of code

Difficult to compare and reproduce results
– High possibility the web security landscape looks even worse than reported!
Key Takeaways

▶ Consent to tracking has a profound impact on attack surface
▶ Problematic for vulnerability scanning tools
  – Unless they interact with consent banners they only see a subset of code
▶ Challenge for academic measurement studies
Key Takeaways

- Consent to tracking has a profound impact on attack surface
- Problematic for vulnerability scanning tools
  - Unless they interact with consent banners they only see a subset of code
- Challenge for academic measurement studies
  - Vantage point rarely stated in literature
Key Takeaways

▶ Consent ing to tracking has a profound impact on attack surface
▶ Problematic for vulnerability scanning tools
  – Unless they interact with consent banners they only see a subset of code
▶ Challenge for academic measurement studies
  – Vantage point rarely stated in literature
  ▶ Difficult to compare and reproduce results

High possibility the web security landscape looks even worse than reported!
Key Takeaways

▶ Consenting to tracking has a profound impact on attack surface
▶ Problematic for vulnerability scanning tools
  – Unless they interact with consent banners they only see a subset of code
▶ Challenge for academic measurement studies
  – Vantage point rarely stated in literature
    ▶ Difficult to compare and reproduce results
  – High possibility the web security landscape looks even worse than reported!
Thank you for your attention!