

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)

Client Side XSS

```
1  let name = location.hash.substr(1);  
2  let greeting = "Hello, " + name;  
3  /*  
4     Application code  
5  */  
6  div.innerHTML = greeting;
```

Client Side XSS

Source: Attacker controlled data

Source

```
1 let name = location.hash.substr(1);
2 let greeting = "Hello, " + name;
3 /*
4     Application code
5 */
6 div.innerHTML = greeting;
```

Client Side XSS

Sink: Turned into (executable) code

```
1  let name = location.hash.substr(1);  
2  let greeting = "Hello, " + name;  
3  /*  
4     Application code  
5  */  
6  div.innerHTML = greeting;
```

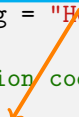
Sink

Client Side XSS

Data flow from source to sink

Source

```
1 let name = location.hash.substr(1);
2 let greeting = "Hello, " + name;
3 /*
4    Application code
5 */
6 div.innerHTML = greeting;
```



Sink

Client Side XSS

```
1  let name = location.hash.substr(1);
2  let greeting = "Hello, " + name;
3  /*
4     Application code
5  */
6  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!

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

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!

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

→ 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

	25 Million Flows	DOMsday	Our Study	Our Study (VPN)
Date	April 2013	Jan. 2017	Oct. 2020	April 2021
Vantage Point	Germany	USA	Germany	USA
Pages	504 275	44 722	390 092	876 872
Frames	4 358 031	319 481	1 111 821	4 389 872
Frames/Page	8.64	7.14	2.85	5.00

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

Nutzen Sie BILD.de ohne Tracking, Cookies und personalisierte Werbung für 3,99 EUR/Monat (rabattiert für BILDplus-Abonnenten 2,99 EUR/Monat).

Informationen zur Datenverarbeitung im BILD Pur-Abo finden Sie in unserer [Datenschutzerklärung](#) und in den [FAQ](#).

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

* 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

Sie haben bereits ein BILD Pur-Abo? [Jetzt anmelden](#)

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-IDs) gebildet und angereichert, auch außerhalb des EWR verarbeitet. Hierzu übermitteln wir an diese Drittanbieter auch Ihre Privatsphäreinstellungen bzw. Präferenz 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/loder 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

Alle akzeptieren

Details dazu finden Sie im [Privacy Center](#).

Surfing the Web today looks like this

Ohne Tracking und Cookies* nutzen

Nutzen Sie BILD.de ohne Tracking, Cookies und personalisierte Werbung für 3,99 EUR/Monat (rabattiert für BILDplus-Abonnenten 2,99 EUR/Monat).

Informationen zur Datenverarbeitung im BILD Pur-Abonnement finden Sie in unserer [Datenschutzzerklärung](#) und in unserer [FAQ](#).

Wenn Sie BILD Pur abonnieren, können Sie auch ohne Tracking die verfügbaren Inhalte ohne Tracking lesen. Sofern Sie bereits BILDplus-Abonnent sind, können Sie BILD Pur zusätzlich abonnieren und erhalten dann BILDplus-Inhalte ohne Tracking.

* 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

Sie haben bereits ein BILD Pur-Abo? [Jetzt anmelden](#)

[FAQ](#) | [Datenschutzzerklärung](#) | [Impressum](#)

FOCUS online

Einstellungen zum Datenschutz

Wenn Sie auf „Akzeptieren“ klicken, verarbeiten wir und [Drittanbieter](#) Ihre personenbezogenen Daten und speichern Informationen (z.B. durch Cookies) auf Ihrem Endgerät, bzw. greifen auf diese zu. Die Verarbeitung erfolgt zur Analyse, Personalisierung und zur Auspielung von interessengerechter Werbung. Ihre Einwilligung umfasst gem. Art. 49 Abs. 1 lit. a DSGVO auch die Übermittlung in Drittländer, bspw. in die USA. In diesem Fall ist es möglich, dass Ihre Daten ohne richterlichen Beschluss durch lokale Behörden innerhalb des jeweiligen Drittlandes verarbeitet werden.

Mit Klick auf den Button „Einstellungen“ können Sie Details zur Verarbeitung einsehen, Ihre Präferenzen jederzeit anpassen sowie Ihre Einwilligung widerrufen, indem Sie die [Datenschutzeinstellungen](#) innerhalb des Footers der Webseite aufrufen. Weitere Informationen finden Sie in unserer [Datenschutzzerklärung](#) und unserem [Impressum](#).

Eine ergänzende „FAQ“ zur Handhabung des Einwilligungsmanagers finden Sie [hier](#).

Wir verwenden Ihre Daten für:

- Informationen auf einem Gerät speichern und/oder abrufen
- Personalisierte Anzeigen und Inhalte
- Funktional, Analytik, Werbung (nicht IAB-Anbieter), Soziale Medien und unbedingt erforderliche Cookies

Verwendung der Cookies

Akzeptieren

Surfing the Web today looks like this

Datenschutz und Nutzungserlebnis

Ohne Tracking und Cookies* nutzen

Nutzen Sie BILD.de ohne Tracking, Cookies und personalisierte Werbung für 3,99 EUR/Monat (rabattiert für BILDplus-Abonnenten 2,99 EUR/Monat).

Informationen zur Datenverarbeitung im BILD Pur-App finden Sie in unserer [Datenschutzklärung](#) und in der [FAQ](#).

Wenn Sie BILD Pur abonnieren, können Sie auch auf bild.de verfügbaren Inhalte ohne Tracking und Cookies lesen. Sofern Sie bereits BILDplus haben, können Sie BILD Pur zusätzlich abonnieren und erhalten dann BILDplus-Inhalte ohne Tracking und Cookies.

Mit

Einstellungen zum Datenschutz

Wenn Sie auf „Akzeptieren“ klicken, verarbeiten wir und [Drittanbieter](#) Ihre personenbezogenen Daten und speichern Informationen (z.B. durch Cookies) auf Ihrem Endgerät, bzw. greifen auf diese zu. Die Verarbeitung erfolgt zur Analyse, Personalisierung und zur Auspielung von interessengerechter Werbung. Ihre Einwilligung umfasst gem. Art. 49 Abs. 1 lit. a DSGVO auch die Übermittlung in Drittländer, bspw. in die USA, in diesem Fall ist es möglich, dass Ihre Daten ohne richterlichen Beschluss durch lokale Behörden innerhalb des jeweiligen Drittlandes verarbeitet werden.

Mit Klick auf den Button „Einstellungen“ können Sie Details zur Verarbeitung einsehen, Ihre Präferenzen jederzeit anpassen sowie Ihre Einwilligung widerrufen, indem Sie die [Datenschutzeinstellungen](#) innerhalb des Footers der Webseite aufrufen. Weitere Informationen finden Sie in unserer [Datenschutzklärung](#) und unserem [Impressum](#).

Eine ergänzende „FAQ“ zur Handhabung des Einwilligungsmanagers finden Sie [hier](#).

Wir verwenden Ihre Daten für:

Informationen auf einem Gerät speichern und/oder abrufen
Personalisierte Anzeigen und Inhalte
Funktional, Analytik, Werbung (nicht IAB-Anbieter), Soziale Medien und unbedingt erforderliche Cookies

Verwendung der nicht

Einstellungen oder ablehnen

Akzeptieren

Cookies on FT Sites

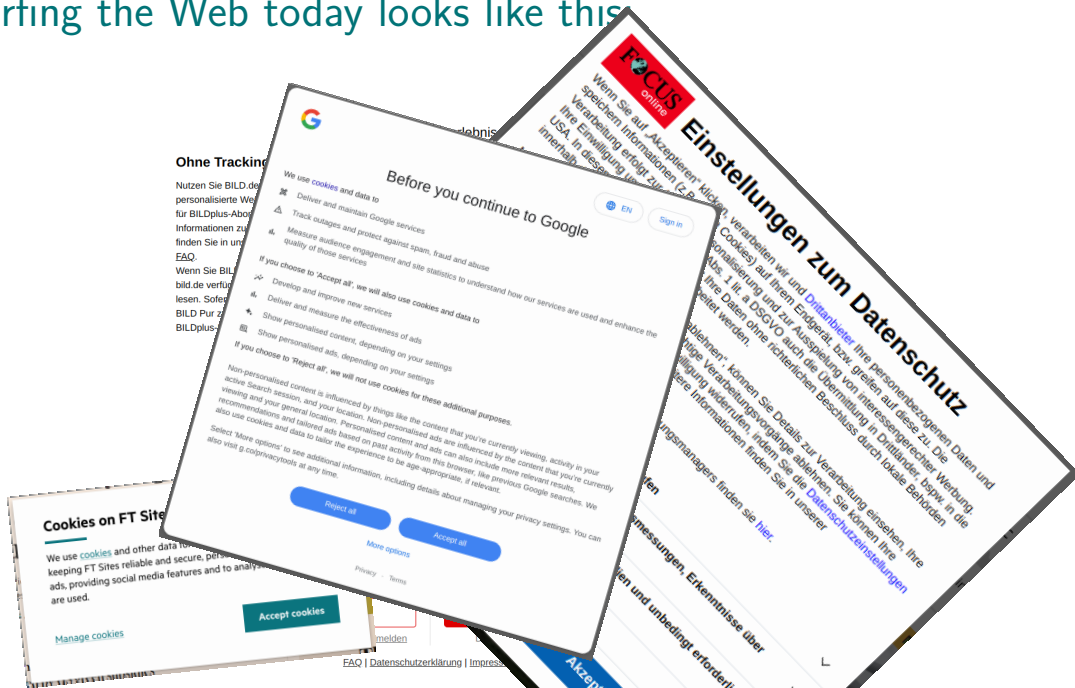
We use [cookies](#) and other data for a number of reasons, such as keeping FT Sites reliable and secure, personalising content and ads, providing social media features and to analyse how our Sites are used.

Accept cookies

[Manage cookies](#)

[FAQ](#) | [Datenschutzklärung](#) | [Impressum](#)

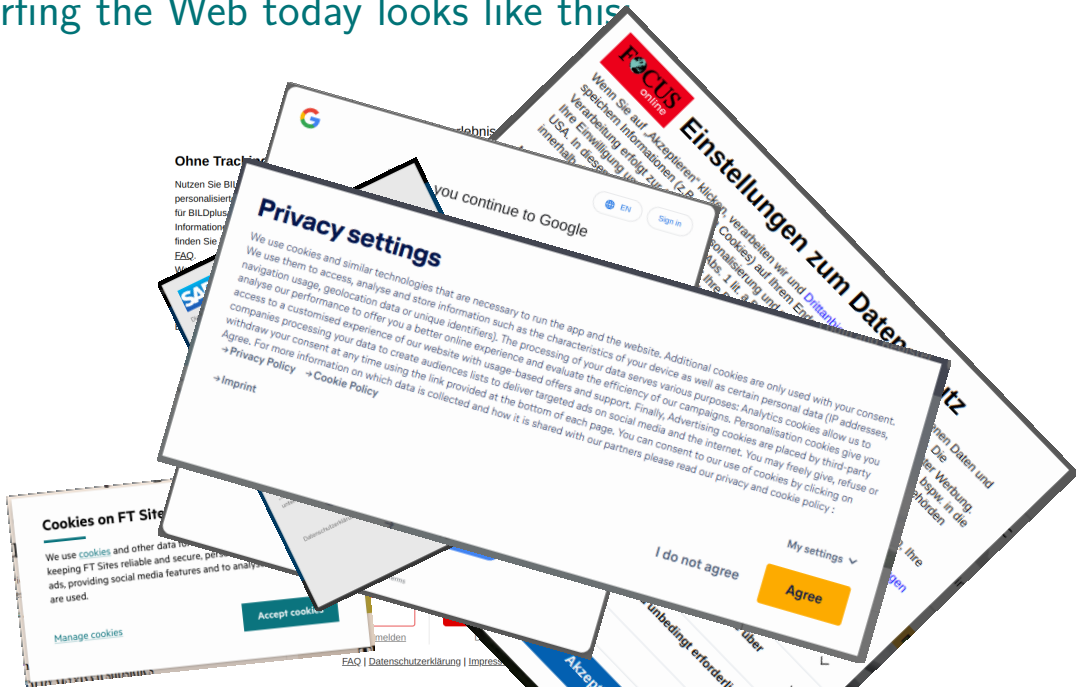
Surfing the Web today looks like this



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:

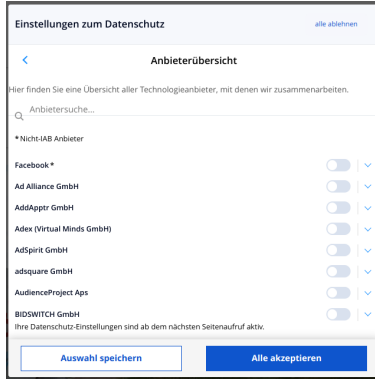
- ▶ Give people control over their private data
 - By e.g., requiring consent for tracking
- ▶ Sounds good, right?
 - Lets try it

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

```
1  __tcfapi("addEventListener", 2, function(tcData, success) {
2    if (success && tcData.uniconLoad === true) {
3      if(!window._initAds) {
4        window._initAds = true;
5        var script = document.createElement('script');
6        script.async = true;
7        script.setAttribute('data-ad-client', 'ca-pub-xxxxxxx');
8        script.src = 'https://pagead2.googlesyndication.com/...';
9        document.head.appendChild(script);
10     }
11   }
12 });
```

Cookie Banner under the hood

```
1  __tcfapi("addEventListener", 2, function(tcData, success) {
2      if (success && tcData.uniconLoad === true) {
3          if(!window._initAds) {
4              window._initAds = true;
5              var script = document.createElement('script');
6              script.async = true;
7              script.setAttribute('data-ad-client', 'ca-pub-xxxxxxx');
8              script.src = 'https://pagead2.googlesyndication.com/...';
9              document.head.appendChild(script);
10         }
11     }
12 });
```

Register event for user interaction

Cookie Banner under the hood

```
1  __tcfapi("addEventListener", 2, function(tcData, success) {  
2    if (success && tcData.uniconLoad === true) {  
3      if(!window._initAds) {  
4        window._initAds = true;  
5        var script = document.createElement('script');  
6        script.async = true;  
7        script.setAttribute('data-ad-client', 'ca-pub-xxxxxxx');  
8        script.src = 'https://pagead2.googlesyndication.com/...';  
9        document.head.appendChild(script);  
10     }  
11   }  
12 });
```

User consented?

Cookie Banner under the hood

```
1  __tcfapi("addEventListener", 2, function(tcData, success) {
2    if (success && tcData.unicLoad === true) {
3      if(!window._initAds) {
4        window._initAds = true;
5        var script = document.createElement('script');
6        script.async = true;
7        script.setAttribute('data-ad-client', 'ca-pub-xxxxxxx');
8        script.src = 'https://pagead2.googlesyndication.com/...';
9        document.head.appendChild(script);
10     }
11   }
12 });
```

Create script tag to load Google ads

Cookie Banner under the hood

```
1  __tcfapi("addEventListener", 2, function(tcData, success) {
2    if (success && tcData.unicLoad === true) {
3      if(!window._initAds) {
4        window._initAds = true;
5        var script = document.createElement('script');
6        script.async = true;
7        script.setAttribute('data-ad-client', 'ca-pub-xxxxxxx');
8        script.src = 'https://pagead2.googlesyndication.com/...';
9        document.head.appendChild(script);
10     }
11   }
12 });
```

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

Our Work

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

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: 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?

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

Acceptify

Tool to maximize consent on banners

How to do this?

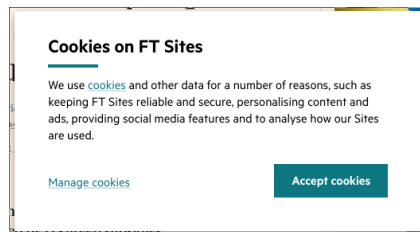
Acceptify

Tool to maximize consent on banners

How to do this?

→ Exploit combination of Dark patterns & legal requirements

Acceptify: Implementation

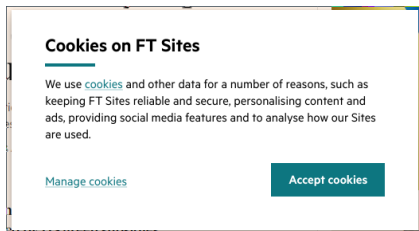


Acceptify: Implementation

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:

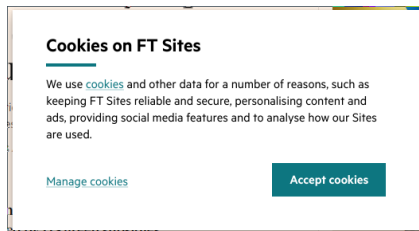
→ all DOM elements matching these criteria:

- ▶ Clickable
- ▶ Textual content contains affirmative phrase
- ▶ ≤ 6 words of text and ≤ 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:

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

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

Results: Loaded Resources

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

→ Significant increase of executed third party code!

Results: Taint Flows

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

Results: Taint Flows

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

→ Significant increase of attack surface!

Validation

Based on taint flows we can automatically generate XSS payload URLs

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:

Group	# Sites
Directly vulnerable	73
Vulnerable after giving consent	44
Overlap	9
Increase	55%

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:

Group	# Sites
Directly vulnerable	73
Vulnerable after giving consent	44
Overlap	9
Increase	55%

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

- ▶ 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

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

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

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

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!

Closing Words

Thank you for your attention!



TESTABLE

