

Please don't :)

~~Hack me if you can!~~

Exploring Vulnerabilities in Frontend Applications



**MEHMET
DEMIRAY**

Senior Frontend Engineer at RedRose

 mehmetdemiray

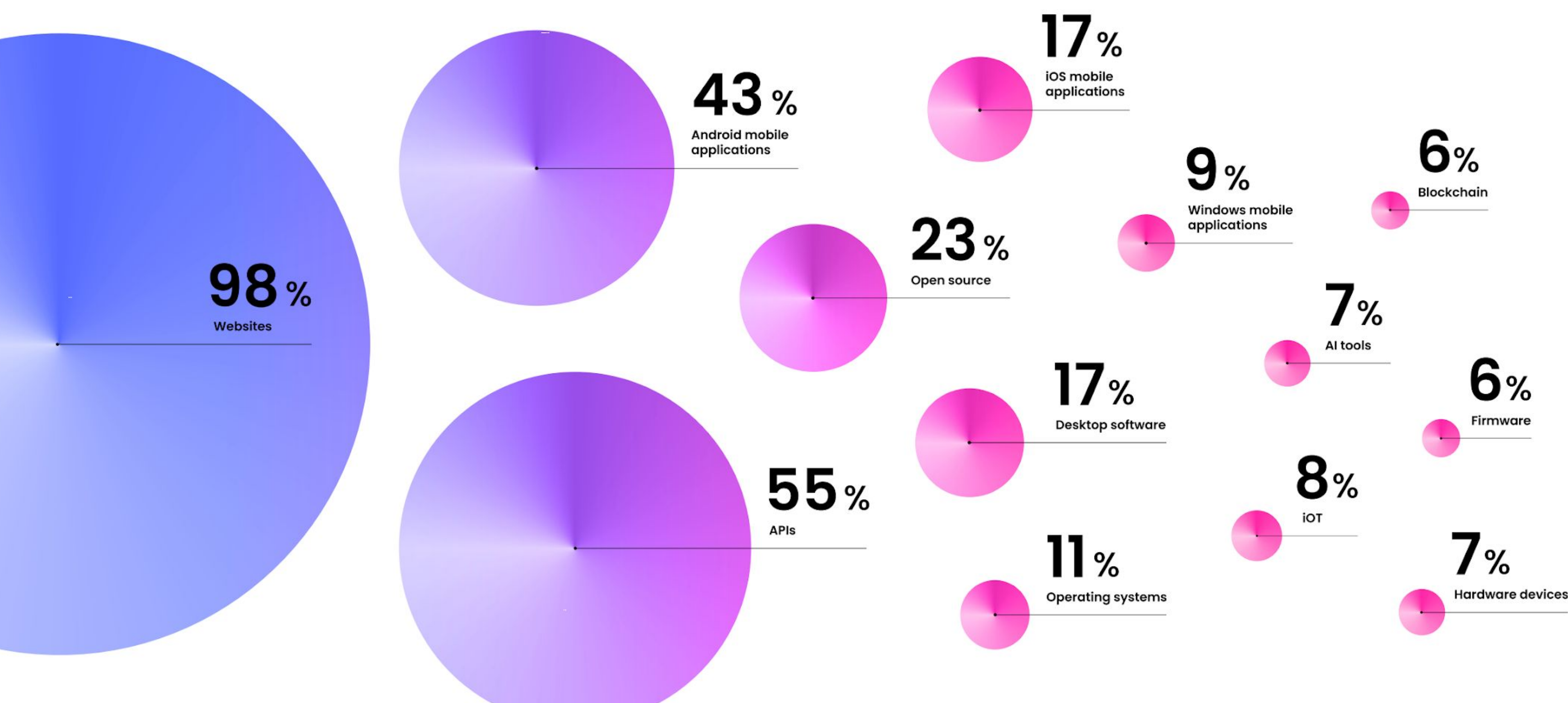
 demirayco

Awards & Recognitions



Spotlight on Frontend Security

Where Hackers Focus Their Efforts



13% Improper access control - generic

11% Information disclosure

10% Cross-site scripting (XSS) - Reflected

7% Insecure direct object reference (IDOR)

5% Privilege escalation

5% Cross-site scripting (XSS) - stored

5% Misconfiguration

3% Improper authentication - generic

3% Business logic errors

3% Cross-site scripting (XSS) - DOM

The Hidden Part of the Iceber

The Prevalence of Unreported Vulnerabilities

40%

Increase in phishing attacks
2023 - 2024

709 million

Number of blocked access attempts to
phishing and scam sites



The widespread integration of technologies featuring
built-in GPT chats has provided scammers with new avenues to exploit.









*Dall-E Prompt:
Create a Disney-style illustration with a white
background explaining phishing.*

Source: Kaspersky reports phishing attacks grow by 40 percent in 2023

Bug Bounty

Rewards and Accepted Reports from Leading Tech Companies

	Total Paid	Total Report	
	\$45,259,505	15237	https://bughunters.google.com/about/key-stats
	\$15,348,490	8500+	https://bugbounty.meta.com
	\$13,800,000	10000+	https://www.microsoft.com/en-us/msrc/bounty
	\$1,593,219	1542+	https://hackerone.com/x
	\$20,000,000	?	https://security.apple.com/bounty/
	\$4,791,150	1595+	https://bounty.github.com/

Recommended Video Series

<https://www.youtube.com/playlist?list=PL590L5WQmH8dsxxz7ooJAgmijwOz0lh2H>



HACKING GOOGLE Series

Google
9 videos 1,220,540 views Last updated on Jan 6, 2023



Five elite security teams. Six never-before-told stories. Go behind the scenes with the hacking teams at Google keeping more people safe online than anyone else in the world.

Common Frontend Vulnerabilities

Security Issue types from Unsecured Frontend Code

1	XSS	
2	NPM(DEPENDENCY) CONFUSING	
3	OPEN REDIRECT	
4	INFORMATION DISCLOSURE	
5	INSUFFICIENT SESSION MANAGEMENT	
6	BROKEN LINK HIJACKING	
7	CSS INJECTION	

XSS

Cross Site Scripting

Total unique reports (all time)

90,871

Unique reports in last 12 weeks

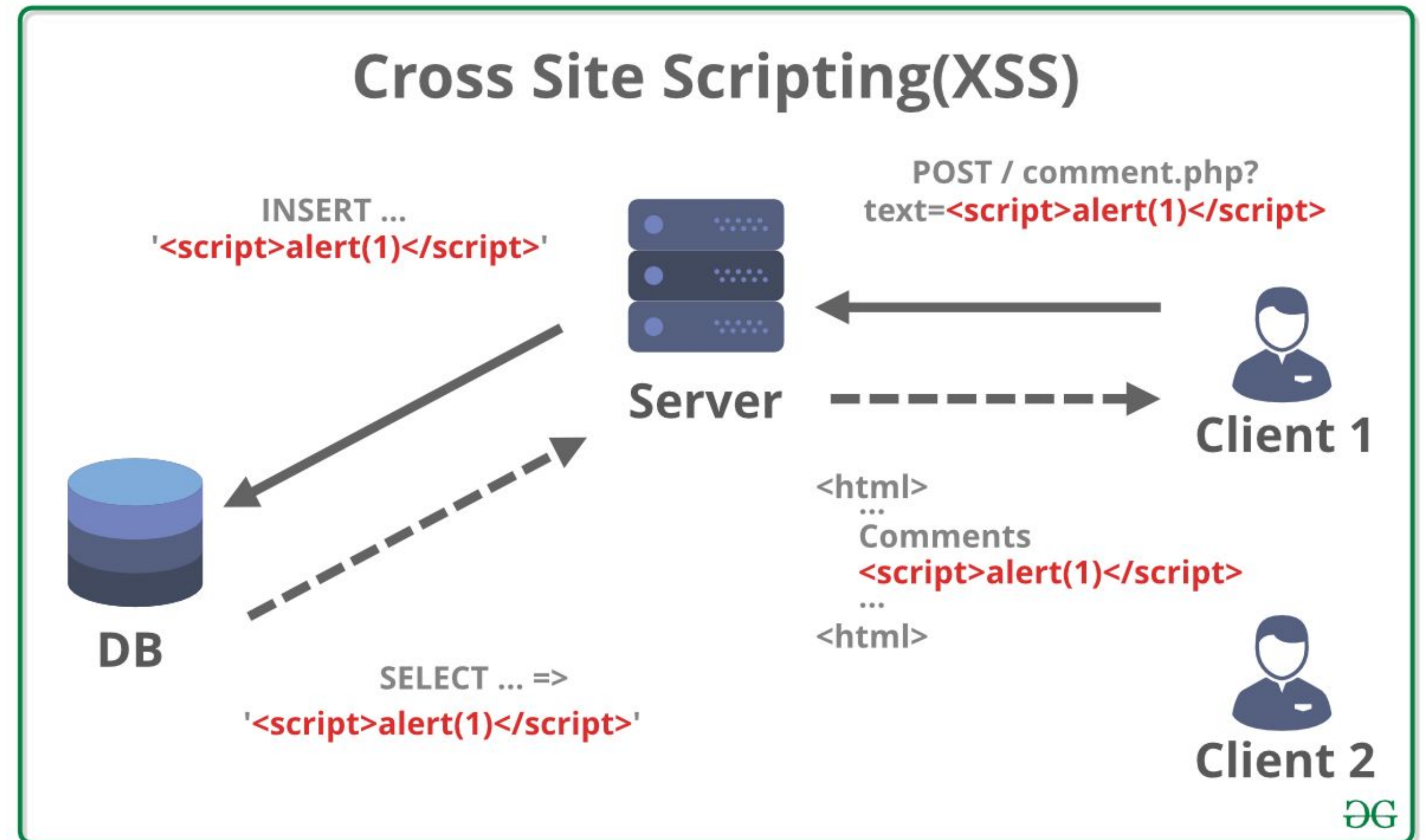
2,529

12 week change

-23%

IMPACTS

Session Hijacking,
Data Theft,
Phishing Attacks,
Keylogging ...more



XSS

Potential Sources of XSS

User Input Forms

URLs

Cookies

Third-Party Libraries

HTTP Headers

Data from External/Internal Sources

Email and Messaging Systems

WebSockets

Event Handlers

Iframes and Embedded Contents

Browser Extensions

Prevent XSS attacks

Input Validation

Output Encoding

Content Security Policy (CSP)

Escaping Data

Sanitize HTML

HTTPOnly Cookies

Secure Headers

Cross-Origin Resource Sharing(CORS)



Dall-E Prompt:

Create a Pixar-style illustration on a white background and colorful depicting a heroic character (resembling a Pixar protagonist) using a magical shield to protect a computer or website from malicious scripts, represented as dark, menacing lines of code. The character should display a confident and determined expression. Include security symbols like locks and checkmarks around the scene to emphasize protection and safety.

NPM DEPENDENCY CONFUSING

A dependency confusion attack occurs when a dependency library is downloaded from a public registry rather than the intended private/internal registry because a malicious attacker could trick the package manager (npm for NodeJs, pip for Python, rubygems for ruby) into downloading the malicious one from the public repository he controls.

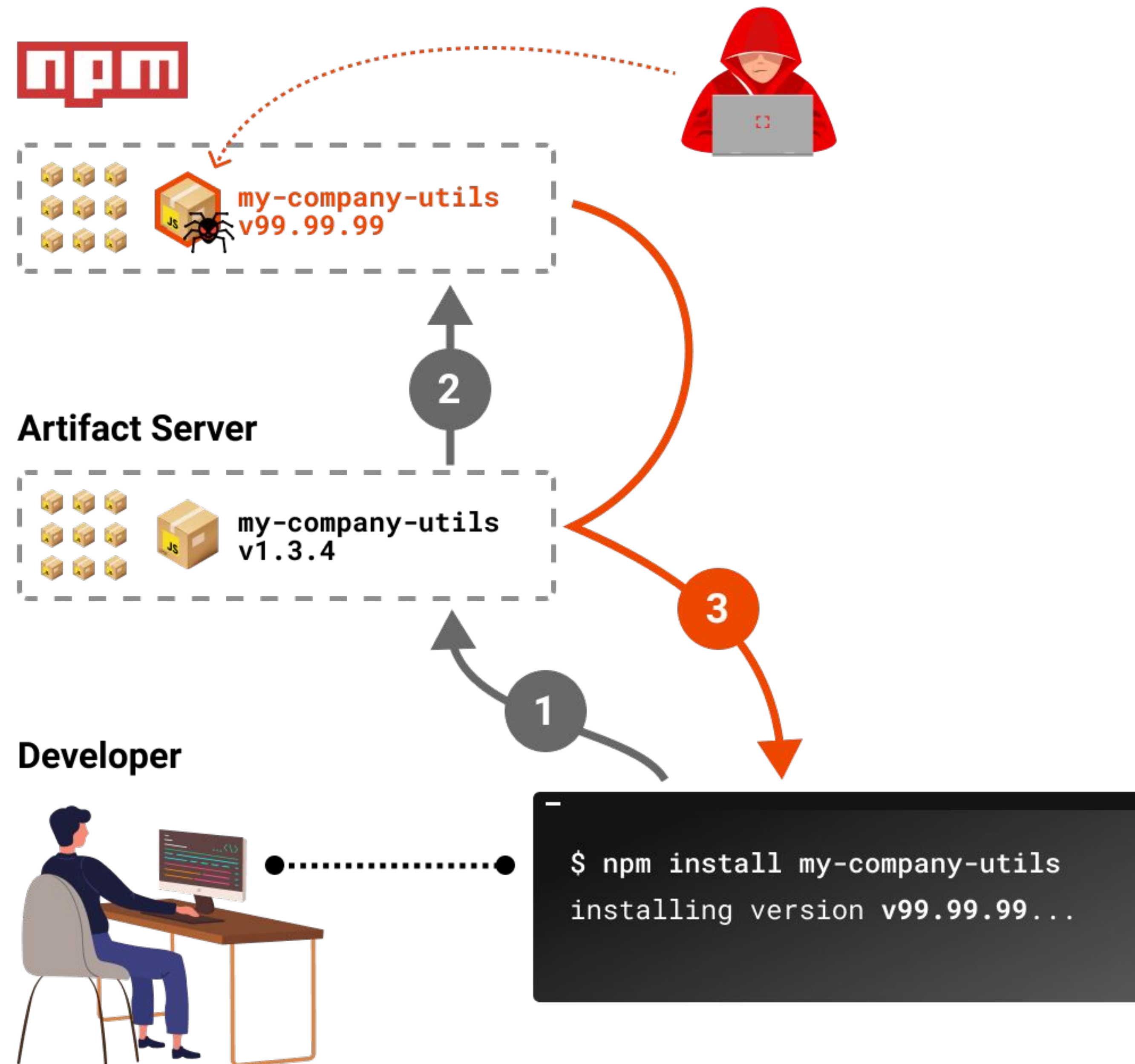
IMPACTS

Remote Code Execution

Backdoor Injection

Data Theft

+ more




NPM DEPENDENCY CONFUSING

Real Example

Dependency Confusion: How I Hacked Into Apple, Microsoft and Dozens of Other Companies

The Story of a Novel Supply Chain Attack



Alex Birsan

Follow

11 min read · Feb 9, 2021

The code was meant for internal PayPal use, and, in its `package.json` file, appeared to contain a mix of public and private dependencies — public packages from npm, as well as non-public package names, most likely hosted internally by PayPal. These names did not exist on the public npm registry at the time.

```
"dependencies": {
  "express": "^4.3.0",
  "dustjs-helpers": "~1.6.3",
  "continuation-local-storage": "^3.1.0",
  "pplogger": "^0.2",
  "auth-paypal": "^2.0.0",
  "wurfl-paypal": "^1.0.0",
  "analytics-paypal": "~1.0.0"
}
```

```
test: "yelp-js-infra test --react -- -
-watchAll", "prepublish": "make
build", "typecheck": "flow check"}, "dependencies":
{"snake-case": "^2.1.0", "yelp-bunsen-logger-
js": "^4.4.1", "yelp_sitrep": "^7.13.2"}, "devDependenci
es": {"enzyme": "^3.11.0", "flow-bin": "^0.100.0", "flow-
copy-source": "^1.2.1", "react": "^16.4.2", "react-
dom": "^16.4.2", "yelp-js-infra": "^33.39.0"}, "files":
["lib", "src"], "peerDependencies":
{"react": "^16.4.2", "react-
dom": "^16.4.2"}}' ) }, 20: function(e, t, n)
```

Time		Organization	IP Address	Package Name	Hostname	
FRI	AUG 21 2020 16:37:56 GMT	APPLE-ENGINEERING - Apple Inc.	17.149.2	@idms/idms-pmrpc	.lan	/Us
FRI	AUG 21 2020 20:14:32 GMT	APPLE-ENGINEERING - Apple Inc.	17.171.	@idms/idms-pmrpc	8faa3092cc97	
FRI	AUG 21 2020 20:15:23 GMT	APPLE-ENGINEERING - Apple Inc.	17.122.	@idms/idms-pmrpc	91c057281d0f	
MON	AUG 24 2020 17:40:43 GMT	APPLE-ENGINEERING - Apple Inc.	17.122.	@idms/idms-pmrpc	1f3cc975c67b	
MON	AUG 24 2020 17:41:38 GMT	APPLE-ENGINEERING - Apple Inc.	17.171.1	@idms/idms-pmrpc	fe01f79c7146	
MON	AUG 24 2020 17:46:06 GMT	APPLE-ENGINEERING - Apple Inc.	17.122.	@idms/idms-pmrpc	7df2bb892313	
MON	AUG 24 2020 17:46:07 GMT	APPLE-ENGINEERING - Apple Inc.	17.171.1	@idms/idms-pmrpc	c6269b74ec56	
MON	AUG 24 2020 19:55:16 GMT	APPLE-ENGINEERING - Apple Inc.	17.171.1	@idms/idms-pmrpc	580f8f68bad3	
MON	AUG 24 2020 19:55:37 GMT	APPLE-ENGINEERING - Apple Inc.	17.122.	@idms/idms-pmrpc	d7bea26b6122	
TUE	AUG 25 2020 07:15:17 GMT	APPLE-ENGINEERING - Apple Inc.	17.171.	@idms/idms-pmrpc	f507d7c91170	
TUE	AUG 25 2020 07:16:00 GMT	APPLE-ENGINEERING - Apple Inc.	17.122.	@idms/idms-pmrpc	e0b80fce2ded	
TUE	AUG 25 2020 17:04:20 GMT	APPLE-ENGINEERING - Apple Inc.	17.122.	@idms/idms-pmrpc	fab9b33c62b4	
TUE	AUG 25 2020 17:21:45 GMT	APPLE-ENGINEERING - Apple Inc.	17.122.	@idms/idms-pmrpc	dfec8557ad01	
TUE	AUG 25 2020 17:22:24 GMT	APPLE-ENGINEERING - Apple Inc.	17.171.	@idms/idms-pmrpc	23495738a747	
TUE	AUG 25 2020 17:22:33 GMT	APPLE-ENGINEERING - Apple Inc.	17.171.	@idms/idms-pmrpc	0b238c2f3792	
TUE	AUG 25 2020 17:23:34 GMT	APPLE-ENGINEERING - Apple Inc.	17.122.	@idms/idms-pmrpc	b9986c648086	
TUE	AUG 25 2020 17:23:56 GMT	APPLE-ENGINEERING - Apple Inc.	17.122.	@idms/idms-pmrpc	b44ff6b9bd5b	
TUE	AUG 25 2020 17:24:01 GMT	APPLE-ENGINEERING - Apple Inc.	17.171.1	@idms/idms-pmrpc	dbe40d2f0d7b	
TUE	AUG 25 2020 17:35:18 GMT	APPLE-ENGINEERING - Apple Inc.	17.171.1	@idms/idms-pmrpc	46ec329453e0	
TUE	AUG 25 2020 17:35:26 GMT	APPLE-ENGINEERING - Apple Inc.	17.122.	@idms/idms-pmrpc	493d6929fa02	
TUE	AUG 25 2020 17:35:31 GMT	APPLE-ENGINEERING - Apple Inc.	17.171.	@idms/idms-pmrpc	efdbc138d349	
TUE	AUG 25 2020 17:35:42 GMT	APPLE-ENGINEERING - Apple Inc.	17.122.	@idms/idms-pmrpc	c1f3c7e9dd7b	
TUE	AUG 25 2020 17:56:39 GMT	APPLE-ENGINEERING - Apple Inc.	17.151.1	@idms/idms-pmrpc	s-MacBook-Pro.local	/Users
TUE	AUG 25 2020 17:56:39 GMT	APPLE-ENGINEERING - Apple Inc.	17.150.2	@idms/idms-pmrpc	s-MacBook-Pro.local	/Users
TUE	AUG 25 2020 19:12:59 GMT	APPLE-ENGINEERING - Apple Inc.	17.122.	@idms/idms-pmrpc	ef4d6be2634f	
TUE	AUG 25 2020 19:28:51 GMT	APPLE-ENGINEERING - Apple Inc.	17.122.	@idms/idms-pmrpc	74fb58c6b33f	
TUE	AUG 25 2020 19:38:10 GMT	APPLE-ENGINEERING - Apple Inc.	17.122.	@idms/idms-pmrpc	2f0a02c2d36a	

Open Redirect

CWE-601: URL Redirection to Untrusted Site ('Open Redirect')

Total unique reports (all time)	13,486
Unique reports in last 12 weeks	392
12 week change	-13%

https://demiray.dev/login
?redirectUrl=https://demiray.dev/products

https://demiray.dev/login
?redirectUrl=https://dem1ray.com/login

https://demiray.dev/login
?redirectUrl=javascript:alert(1)

IMPACTS

Phishing Attacks

XSS

Credential Theft

Malware Distribution

Session Hijacking

Reputation Damage

Information Disclosure

+more

Information Disclosure

CWE Discovery

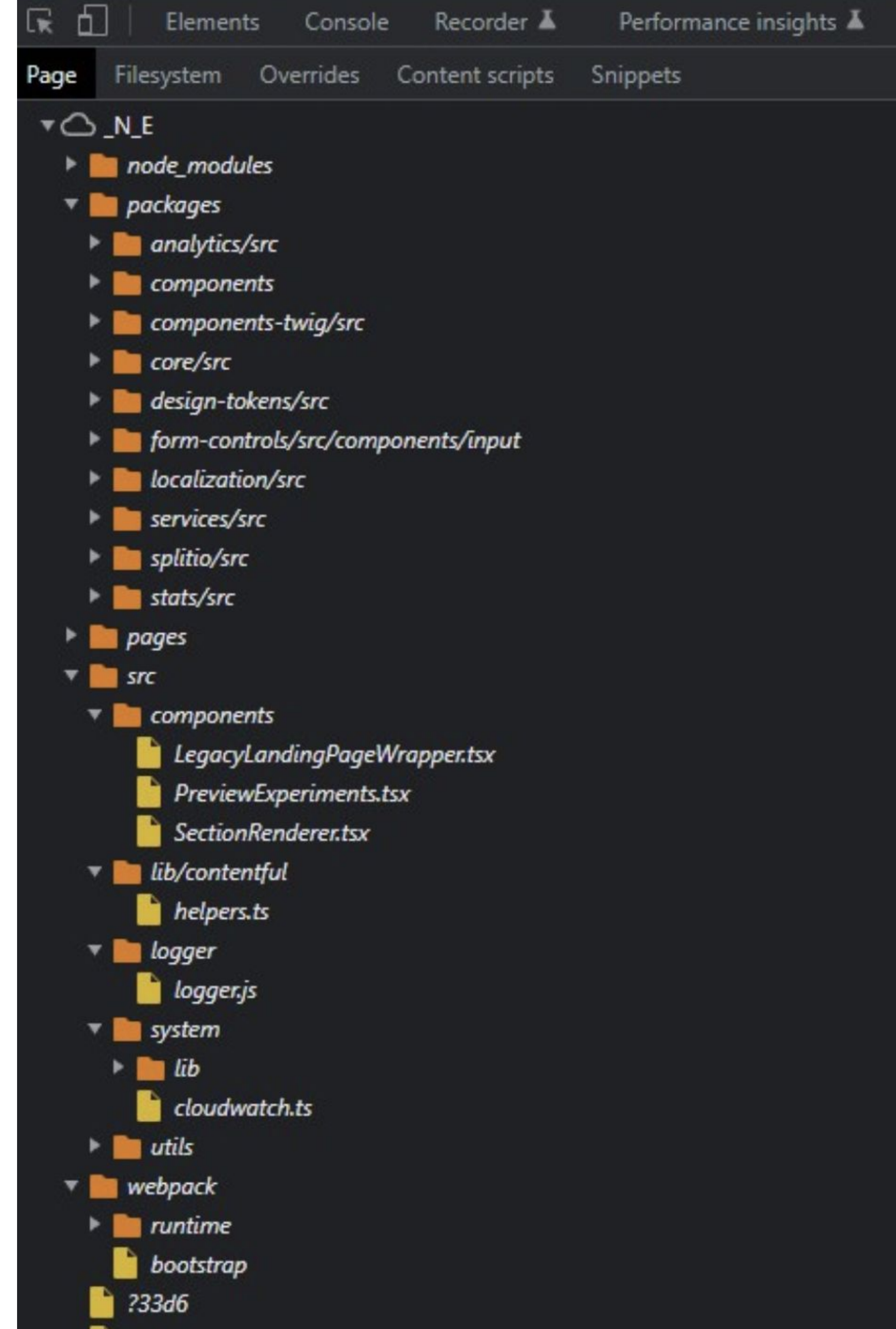
The Common Weakness Enumeration Discovery Index shows platform-wide data of instances, and severity and remediation time distributions. CWE data extracted every 24 hours.

<div><div></div><div>sensitive information</div></div>		
CWE ID	Name	Number of reports
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor	57,112
CWE-922	Insecure Storage of Sensitive Information	3,833
CWE-312	Cleartext Storage of Sensitive Information	3,179
CWE-209	Generation of Error Message Containing Sensitive Information	2,442
CWE-215	Insertion of Sensitive Information Into Debugging Code	1,975
CWE-319	Cleartext Transmission of Sensitive Information	1,925
CWE-538	Insertion of Sensitive Information into Externally-Accessible File or Directory	858
CWE-201	Insertion of Sensitive Information Into Sent Data	485
CWE-532	Insertion of Sensitive Information into Log File	94
CWE-540	Inclusion of Sensitive Information in Source Code	91

Information Disclosure

Source code disclosure

```
57
58 export const getServerSideProps: GetServerSideProps<
59   ProfileLikesPageProps,
60   { slug: string }
61 > = async ({ params }) => {
62   // * NOTE: We cast `params` as we know it will never be `undefined` because this file is under [slug]
63   // * (which catches the route w/o a parameter too).
64   const profileHandle = (params as { slug: string }).slug;
65   const [profile, createdTemplates] = await Promise.all([
66     // [REDACTED]
67     // [REDACTED]
68     // [REDACTED] 'templates' will only match the
69   ]);
70
71   if (!profile) {
72     return { notFound: true };
73   }
74
75   const likedTemplateIds = await getPublishedLikedTemplateIds([REDACTED]);
76   let initialLikedTemplates: Template[] = [];
77   const showExpertPage = [REDACTED];
78   const numberOfInitialLikes = showExpertPage ? NUMBER_PER_PAGE_EXPERT : NUMBER_PER_PAGE_STANDARD;
79
80   // [REDACTED]
81   // [REDACTED] to simplify the
82   // [REDACTED] numberOfInitialLikes
83   // [REDACTED]
84   // [REDACTED]
85   // [REDACTED]
86   // [REDACTED]
87   // [REDACTED]
88   // [REDACTED]
89   // [REDACTED] server-component
90   /*
91   const initialLikedTemplateIds = likedTemplateIds.slice(0, numberOfInitialLikes);
92   const { templates } = await getTemplatesByIds(initialLikedTemplateIds);
93   initialLikedTemplates = templates;
94   */
95 }
```



Information Disclosure

Sensitive Information into Log File
Cross-domain Referer
leakage

TOYOTA's Password reset token and Email Address leak via Referer header



Jayson Vasquez Rubio · Follow

1 min read · Feb 28, 2019



30



3

#252544



Token leakage by referrer header & analytics



31

#237262



Invitation tokens leak to Google Analytics



25

#1491127



Private invitation links/tokens leak to third-party analytics site



47

#196458




apps.shopify.com - CSRF token leakage through Google Analytics

Insufficient Session Management

Total unique reports (all time)	1,810
Unique reports in last 12 weeks	69
12 week change	+57%

- ▲

51



No Session Expiry after log-out, attacker can reuse the old cookies

By [niraj1mahajan](#) to [Shopify](#) |


●

 Resolved | Low | \$500.00 | disclosed 29 days ago

The session fixation vulnerability allowed an attacker to reuse old session cookies to log in to a victim's account on the Exchange Marketplace, even after the victim had logged out. The service has been decommissioned, and the issue has been resolved. This summary was automatically generated.

▲

60



Insufficient session expiration in the `com.shopify.ping**` android app**

By [fr4via](#) to [Shopify](#) |


●

 Resolved | Low | disclosed 3 years ago

Insufficient session expiration was identified in the com.shopify.ping android app, allowing the authentication token to remain valid even after the user logs out. This could allow an attacker to recover a fully functional session and access sensitive information. This summary was automatically generated.

▲

34



Lack of session expiration after password reset on TikTok Careers Portal

By [gnux](#) to [TikTok](#) |

●

 Resolved | Low | \$50.00 | disclosed 3 years ago

Broken Link Hijacking

milankatwal99 submitted a report to X (Formerly Twitter).

November 11, 2020, 6:59am UTC

Description

A link in <https://developer.twitter.com/en/docs/twitter-api/tools-and-libraries> was broken and anyone could create that account which leads to account impersonate

Steps To Reproduce

1) Visit <https://developer.twitter.com/en/docs/twitter-api/tools-and-libraries>
2) Scroll down to Javascript/Node.js and click on by @HunterLarco (v2)
3) Create github username HunterLarcol
4) When someone visits and scroll down to javascript/Node.js and click on @HunterLarco (v2). They are redirected to my account

similar report

<https://hackerone.com/reports/265696>

To solve this issue

put this link <https://github.com/HunterLarco>

Please let me know if you have any questions. I am happy to help

Impact

Impact
The users are coming from developer.twitter.com So, the attacker can put malicious content on the github and many users will be the victim for example <https://github.com/HunterLarco/twitter-v2>. Moreover it leads to the loss in the reputation of the company

4 attachments:

F1073585: [developer_twitter.jpg](#)
F1073586: [account.jpg](#)
F1073587: [profile1.jpg](#)
F1073588: [profile.jpg](#)

Participants

Reported to

X (Formerly Twitter) Managed

Report Id

#1031321 Resolved

Disclosed

February 4, 2021, 6:25am UTC

Severity

High (7 ~ 8.9)

Weakness

Phishing

Bounty

None

CVE ID

None

Account de...

None

SDKs / Libraries

Tools

twitter-v2

by @HunterLarco (v2)

twitter-lite

by @dandv and @peterpm

twitter-error-ha

by @shalvah

twittersignin

A wrapper around
simplify signin, by
@shalvah

https://github.com/join?ref_cta=Sign+up&ref_loc=header+logged+out&ref_page=%2F&source=header 110% ...

Create your account

Username *

HunterLarcol

Email address *

testatifalam@gmail.com

Password *

.....

Make sure it's at least 15 characters OR at least 8 characters including a number and a lowercase letter.
[Learn more.](#)

- IMPACTS
- Phishing Attacks

Malware Distribution

Session Hijacking

Reputation Damage

Information Disclosure

+more

CSS Injection

Frontend Sanitizing

```
sanitizeHtml(dirty, {
  allowedTags: ['a', 'b', 'i', 'em', 'strong'],
  allowedAttributes: {
    '*': ['class'],
  },
});
```

Attack Scenerio

```
<a href="https://evil.com">
  <div class="card--add-project-menu reading--show-actions">
    <div class="drop-zone-indicator notice--red options-menu__action reading__actions">
      <strong class="project-header__name--overview todolist-group-form__fields u-full-height">
        Your session has expired. Please log in again.
      </strong>
    </div>
  </div>
</a>
```

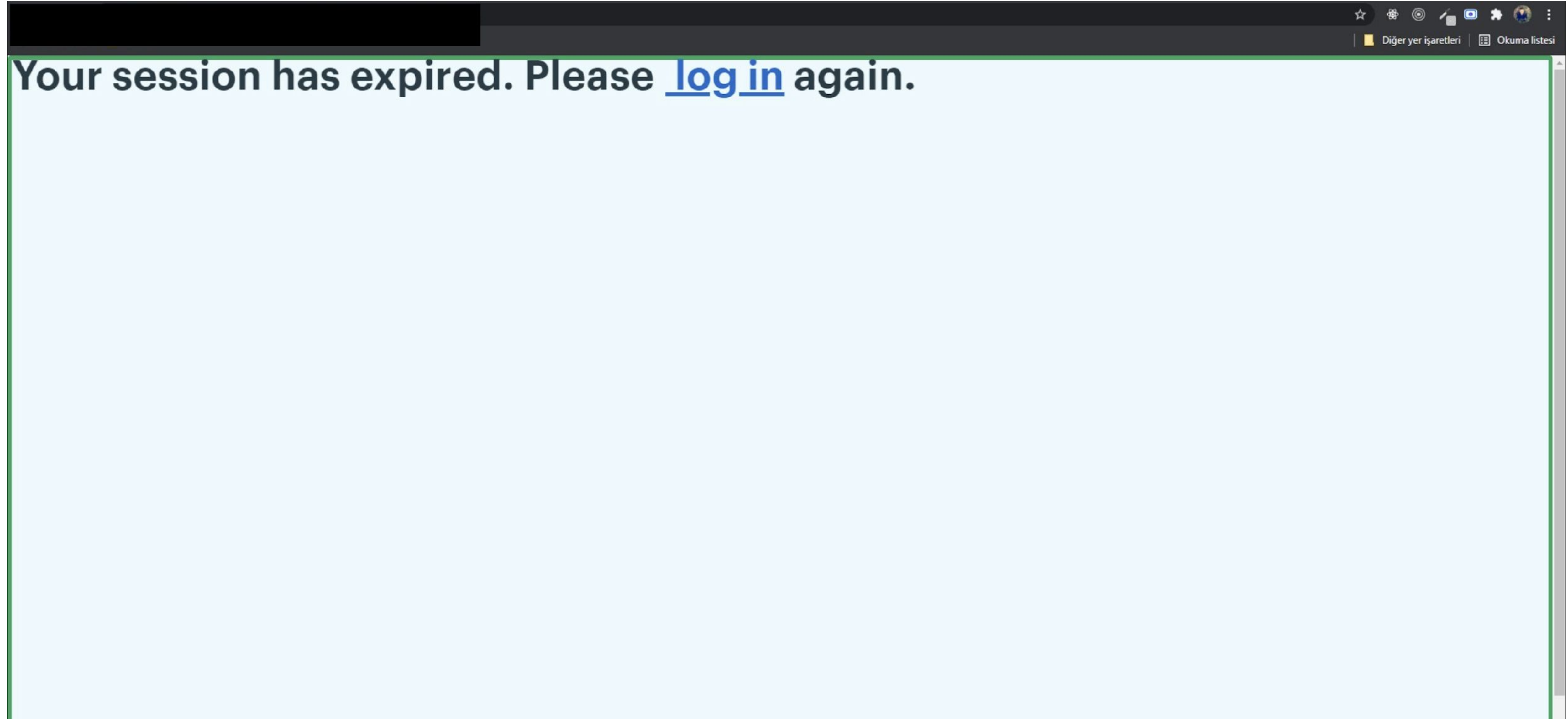
```
.card--add-project-menu .options-menu__action {
  -webkit-transition: background 0.3s;
  -moz-transition: background 0.3s;
  -ms-transition: background 0.3s;
  transition: background 0.3s;
  -webkit-flex: 1;
  -moz-flex: 1;
  -ms-flex: 1;
  flex: 1;
  pointer-events: auto
}

.drop-zone-indicator {
  position: fixed;
  top: 0;
  right: 0;
  left: 0;
  bottom: 0;
  border: 5px solid #2da562;
  z-index: 9;
  pointer-events: none
}

.notice--red {
  background-color: #ffe5e5;
  border-color: #ffc6c6
}

.camper-helper__hi {
  position: absolute;
  top: -2.5rem;
  left: 0;
  right: 0;
  font-size: 5rem
}
```

CSS Injection



Thanks!

<https://github.com/mehmetdemiray/JsKonf2024-HackMe>