The DOMino Effect:









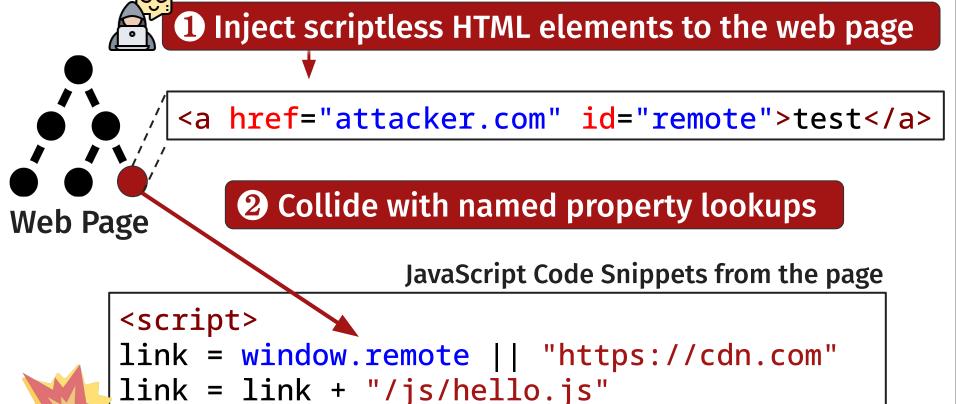




Introduction

Zhengyu Liu, Theo Lee, Jianjia Yu, Zifeng Kang, and Yinzhi Cao

DOM Clobbering: a code-reuse attack on the Web



3 Payloads flow to the dangerous sink through gadgets

Challenges

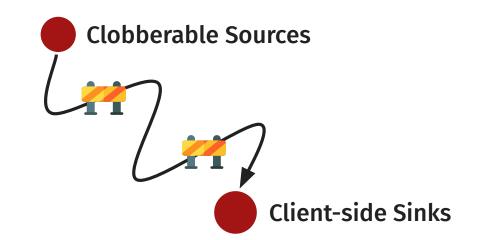
Challenge One: Gadget Detection

script.src = link //

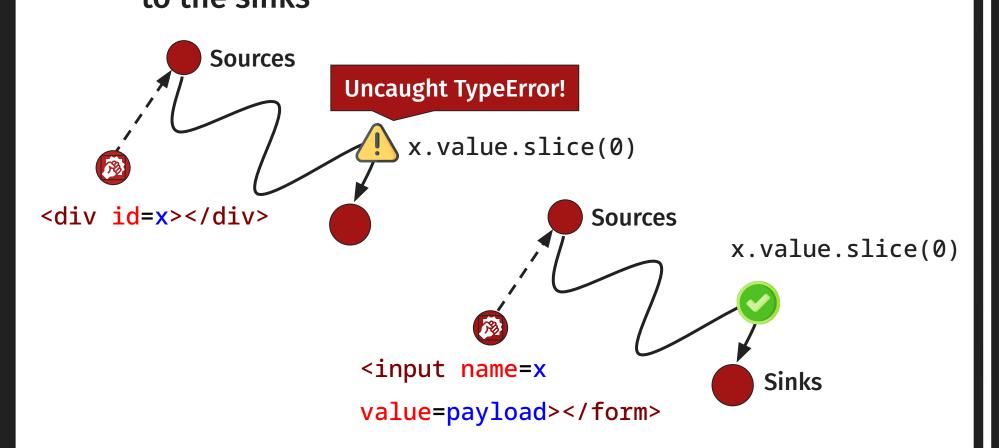
</script>

https://attacker.com/js/hello.js

 Client-side JavaScript favors dynamic behaviors and has widespread use of aliased objects.



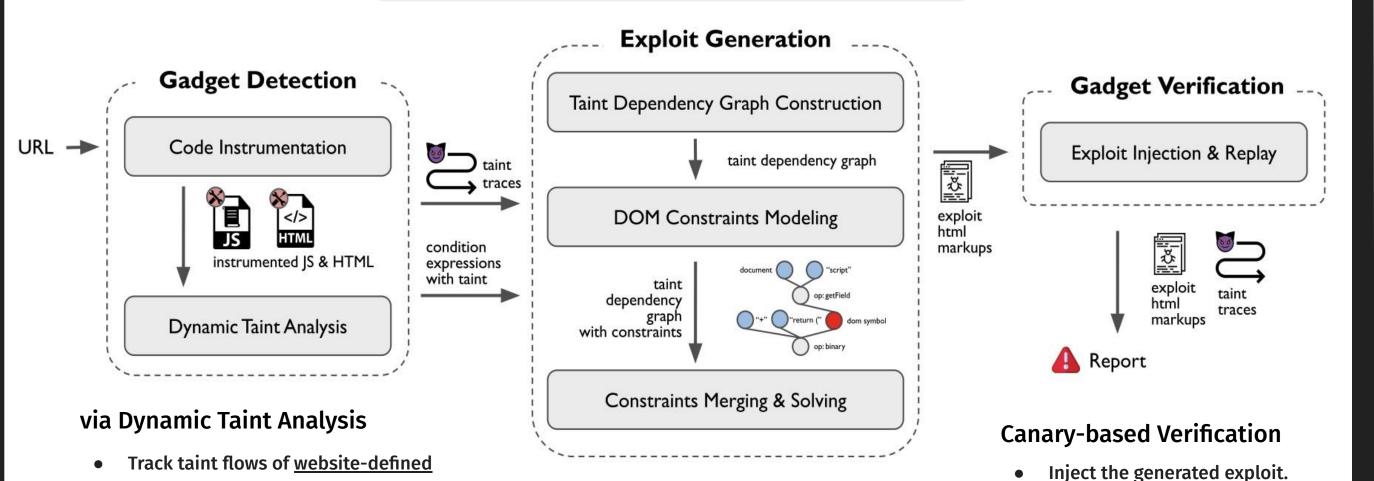
- Challenge Two: Exploit Generation
 - DOM Clobbering requires HTML markups to satisfy DOM constraints to lead attacker-controlled string to the sinks



Key Accomplishments

- Designed the first automated, dynamic analysis tool, Hulk, to detect and exploit DOM Clobbering gadgets using concolic execution with Symbolic DOM.
- Found 497 exploitable DOM Clobbering gadgets on Tranco Top 5,000 websites, including those in Google Client API, Google Closure, MathJax, and Webpack.

System Design



values from DOM clobberable sources to document.links, document.anchors

window.url ? window.url : "default" window.url || "default"

• Inject value only when there is no website-defined value available

document.getElementsByTagName("script"

k.src && 0 == k.src.indexOf(f[j]) && d.push(k)

Taint Dependency Graph

f.push.apply(f, window.___jsl["us"] || [])

for (var h = 0; h < e.length; ++h) {

for (j = 0; j < f.length; ++j) {

for (e = 0; e < d.length; ++e) {

(f = d[e]) ? h = f.nodeType,

(f = Df(f)) && b.push(f));

if (a && !/^\s+\$/.test(a)) {

Df = function(a) {

: f = void 0,

via Concolic Execution • We propose <u>Symbolic DOM</u> to define and

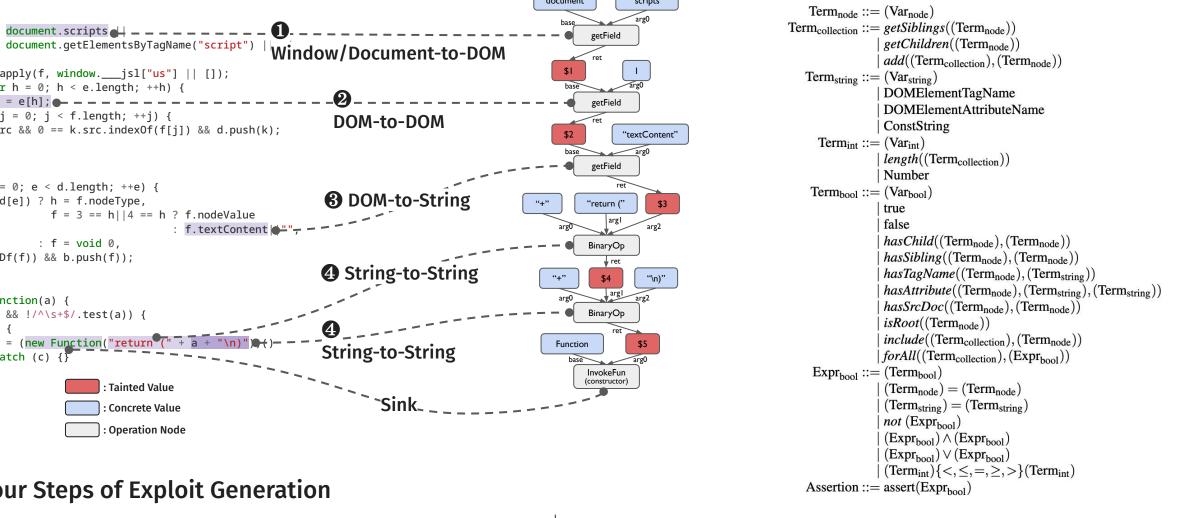
- solve DOM elements-related constraints. Based on the concrete execution trace,
- Hulk models and solves the **DOM** constraints on the Symbolic DOM and generates HTML markups as exploit.

Constraint Syntax for Symbolic DOM

Replay the web page.

• Monitor whether the

vulnerability is triggered



Four Steps of Exploit Generation

: Operation Node

Exploitation Modeling initial clobbering (window/Document-to-DOM), advanced clobbering (DOM-to-DOM), string loading (DOM-to-String), and string operations (String-to-String).

f.textContent ----

Attaching Constraints Each tainted node have two conjunctive sets of constraints, as:

■ The return value of its precedent operation

■ An argument of the subsequent operation

- Constraint Modeling
- Construct constraint of each node using the syntax E.g., isRoot(R1) Λ hasTagName (R1, "object") Λ hasAttribute(R1, "id", P)
- concretes to <object id=scripts></object> when P="scripts"

Merging and Solving Constraints C1: (declare Node R1) \wedge (R1 = \$1) \wedge (P =

C3: (declare Node R1, R2) \wedge (R1 = \$1) \wedge (R2 scripts") \land (05 \lor 06 \lor 07 \lor 08) C2: (declare Node R1) \wedge (R1 = \$1) \wedge (is-C4: (declare Node R1) \land (R1 = \$2)

Major Results

- Large-scale evaluation
 - 497 zero-day verified exploitable gadgets among Tranco top 5,000 websites
- 12 end-to-end exploitation
 - e.g., JupyterLab/Notebook and Canvas LMS.
- Gadget Case studies

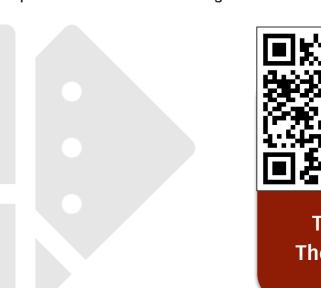
	1				[4]	
Library	# Stars	Version	Impact	Status	TheThing ^[1]	Hulk
				Status	Det./Exp.	Det./Exp
Vite	67.2K	v5.4.5	XSS	CVE-2024-45812	0	•
Webpack	64.4K	v5.93.0	XSS	CVE-2024-43788	0	•
Astro	45.7K	v4.5.9	XSS	CVE-2024-47885	0	•
plausible-analytics	19.7K	v2.1.0	CSRF	Reported	0	•
plotly.js	16.9K	v2.35.2	CSRF	Reported	0	•
Prism	12.2K	v1.29.0	XSS	CVE-2024-53382	0	•
MathJax2	10.1K	v2.7.9	XSS	Acknowledged	0	•
MathJax3	10.1K	v3.2.2	XSS	Acknowledged	0	•
tsup	8.9K	v8.2.4	XSS	CVE-2024-53384	0	•
rspack	8.6K	v1.0.0-rc.0	XSS	Patched	0	•
seajs	8.3K	v3.0.3	XSS	CVE-2024-51091	0	•
Google Closure	4.9K	v20230103	XSS	Acknowledged	0	•
pagefind	3.3K	v1.1.0	XSS	CVE-2024-45389	0	•
Google Client API	3.2K	5Blk7BglYEE	XSS	Patched	0	•
Mavo	2.8K	v0.3.2	XSS	CVE-2024-53388	0	•
Stage.js	2.4K	v1-alpha	XSS	CVE-2024-53386	0	•
cusdis	2.6K	v1.3.0	XSS	CVE-2024-49213	0	•
inspire.js	1.7K	v1.10	XSS	CVE-2024-53385	0	•
steal	1.4K	v2.3.0	XSS	CVE-2024-45939	0	•
UMeditor	1.4K	v1.2.2	XSS	CVE-2024-53387	0	•
doomcaptcha	1K	latest	XSS	Reported	•	•

- indicates that the gadget cannot be detected or exploited by the tool. : indicates successful detection but failed exploit generation.
- : indicates successful detection and verification.



		TheThing ^[1]			Hulk		
	GT	Reported	TP/FP	FN	Reported	TP/FP	FN
Tranco Top 500	33 ^[2]	6	6/0	27	33	33/0	0
Known Gadgets	12	4	4/0	8	5	5/0	7

1] It's (dom) clobbering time: Attack techniques, prevalence, and defenses, Khodayari S, Pellegrino G, (S&P '23) Ground Truth of Tranco Top 500 dataset = TP from TheThing ∩ TP from Hulk







Collection



The DOMino Effect