TÉCNICO LISBOA

Presentation

JAW: Studying Client-side Cross-Site Request Forgery with Hybrid Property Graphs and Declarative Traversals

Authors : Soheil Khodayari and Giancarlo Pellegrino– Paper from USENIX

Joseph Thachil George-PhD- Student

joseph.thachil.george@tecnico.ulisboa.pt

TÉCNICO LISBOA

OVERVIEW

- Introduction
- JAW
- Architecture and Design Of JAW
- Evaluation and Analysis of Collected Data
- Limitations and Future Work
- Conclusion and Observation

TÉCNICO LISBOA

INTRODUCTION

Cross-Site Request Forgery

- Definition

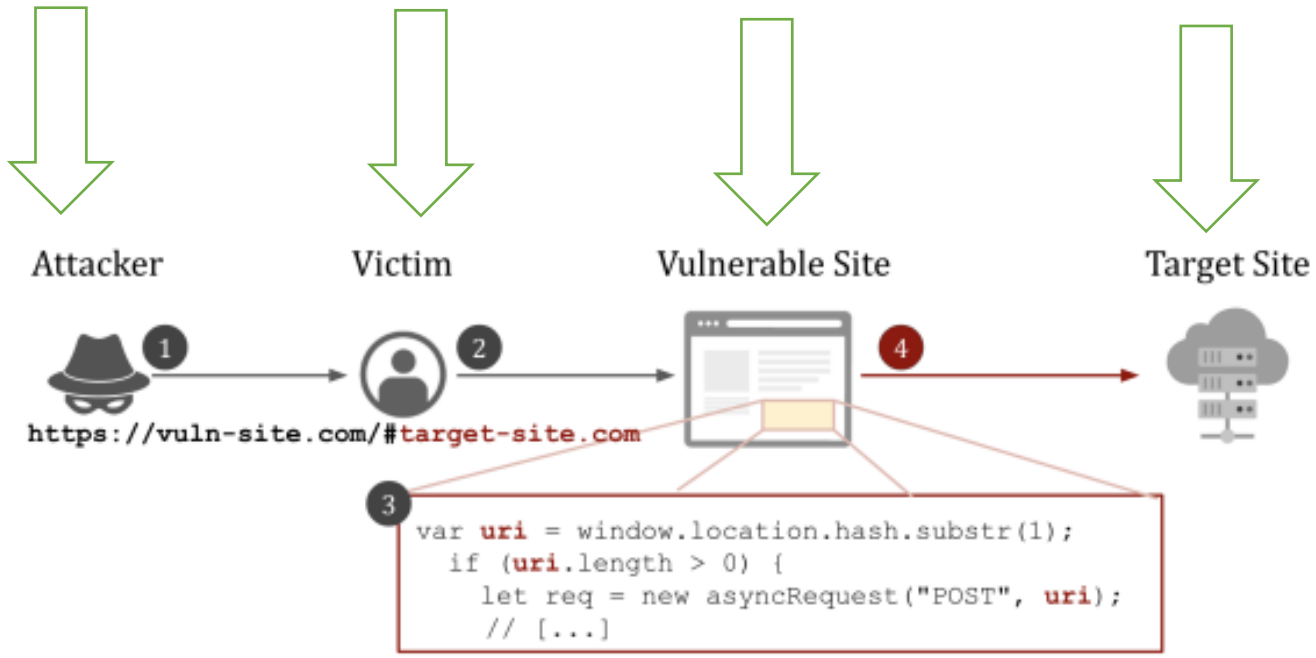
"Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated. With a little help of social engineering (such as sending a link via email or chat), an attacker may trick the users of a web application into executing actions of the attacker's choosing".

-OWASP

TÉCNICO LISBOA

INTRODUCTION- CONT.

Cross-Site Request Forgery- Attack



TÉCNICO LISBOA

INTRODUCTION

Cross-Site Request Forgery

- GET scenario

```
http://bank.com/transfer.do?acct=BOB&amount=100 HTTP/1.1

http://bank.com/transfer.do?acct=MARIA&amount=100000

<a href="http://bank.com/transfer.do?acct=MARIA&amount=100000">View my Pictures!</a>
Or as a 0x0 fake image:
<img src="http://bank.com/transfer.do?acct=MARIA&amount=100000" width="0" height="0" border="0">
```

TÉCNICO LISBOA

INTRODUCTION

Challenges

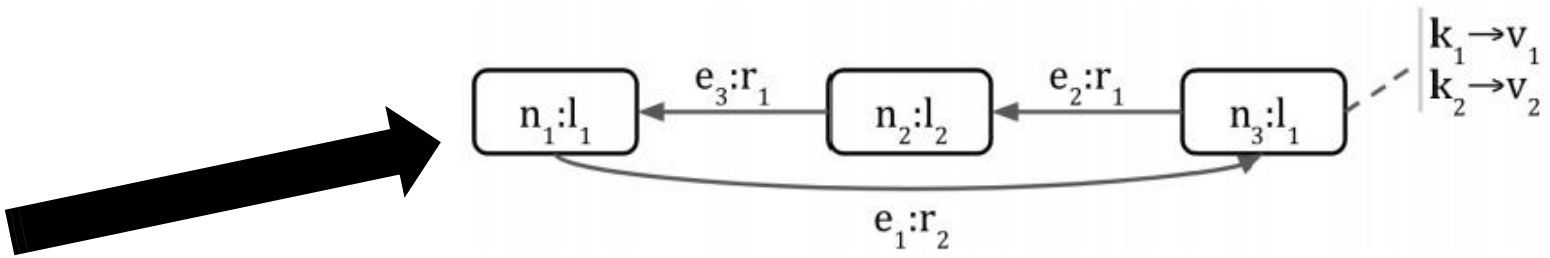
- Vulnerability-specific Analysis Tools
- Event-based Transfer of Control
- Dynamic Web Execution Environment
- Shared Third-party Code

TÉCNICO LISBOA

JAW

Why JWA ?

- ➢ Hybrid Property Graphs



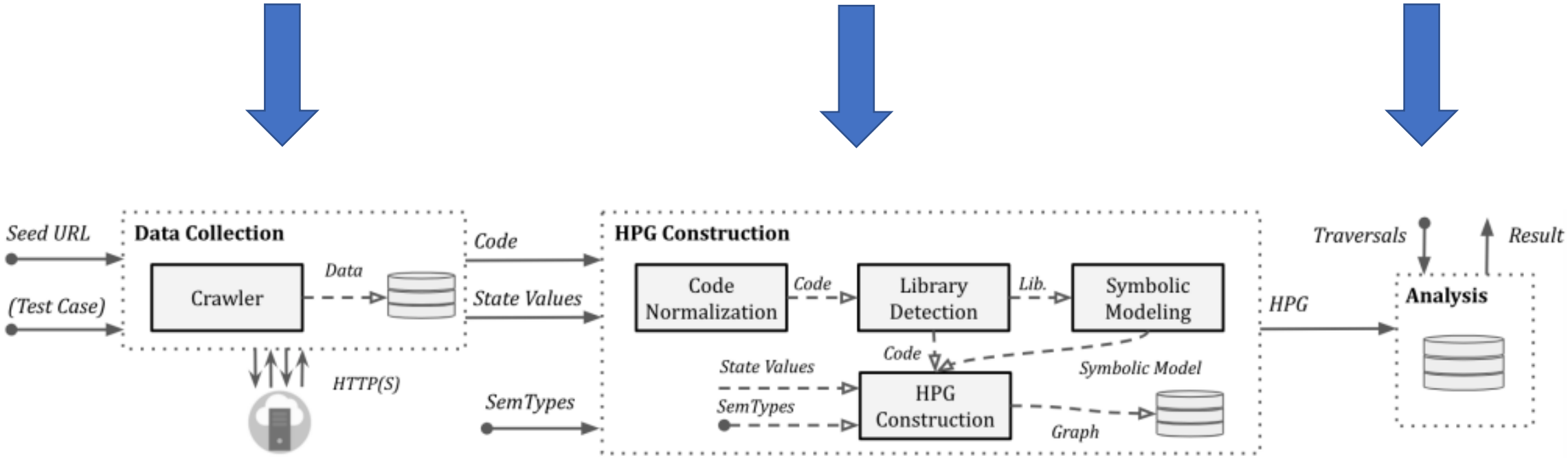
- ✓ HPGs provide a uniform canonical representation for JavaScript source code.
- ✓ Perform a variety of security tasks.
- ✓ Understand event-based transfer of control by proposing the Event Registration
- ✓ Captures the dynamics of the web execution environment of client-side JavaScript

TÉCNICO LISBOA

ARCHITECTURE AND DESIGN OF JAW

TÉCNICO LISBOA

ARCHITECTURE OF JAW



TÉCNICO LISBOA

Evaluation and analysis

TÉCNICO LISBOA

EVALUATION

Run JAW on 4,836 web pages.

- Evaluation of JAW uncovered 12,701 forgeable client-side requests affecting 87 web applications.
- For 203 of them, created a working exploit against seven applications that can be used to compromise the database integrity.
- Analyzed the forgeable requests and identified 25 different request templates.

TÉCNICO LISBOA

ANALYSIS OF COLLECTED DATA

Library	Usage %	LoC	Funcs.	*I/O*	Time (s)
JQuery	81.13%	10,872	428	238	57.54
Bootstrap	38.67%	2,377	55	55	41.07
JQuery UI	27.35%	18,706	320	320	82.33
ReactJS	9.43%	3,318	130	40	39.59
ReactDOM	9.43%	25,148	688	368	81.98
RequireJS	8.49%	1,232	50	50	35.72
AngularJS	5.66%	36,431	852	558	82.92
Analytics	5.66%	20,345	244	233	69.21
Backbone	5.66%	2,096	148	50	38.26
Modernizer	5.66%	834	292	21	34.50
Prototype	5.66%	7,764	266	243	54.10
YUI	4.71%	29,168	2,414	637	149.34
JIT	3.77%	17,163	430	255	69.11
ChartJS	2.83%	16,152	263	253	76,75
Dojo	2.83%	18,937	696	313	63.32
LeafletJS	2.83%	14,080	650	208	62.65
Scriptaculous	2.83%	3,588	97	84	46.11
HammerJS	1.88%	2,643	67	47	37.01
MomentJS	1.88%	4,602	138	138	45.44
ExtJS	1.88%	135,630	2,701	1,135	231.86
Vue	1.88%	11,965	638	288	62.77
YUI History	1.88%	789	20	10	18.41
Bootstrap Growl	0.94%	215	7	7	32.21
Bpmn-Modeler	0.94%	19,139	231	228	65.84
CookiesJS	0.94%	79	3	0	31.29
FlotChartsJS	0.94%	1,267	15	15	42.38
GWT WebStarterKit	0.94%	110	3	2	31.15
Gzip-JS	0.94%	280	4	4	31.87
Handlebars	0.94%	6,726	103	103	50.83
SpinJS	0.94%	190	4	4	31.99
SWFObject	0.94%	729	20	16	33.61
Total		412,575	11,977	5,923	1919.84

Sources	Forgeable	Apps
`DOM.COOKIES`	67	5
`DOM.READ`	12,268	83
`*-STORAGE`	76	8
`DOC.REFERRER`	1	1
`POST-MESSAGE`	8	8
`WIN.NAME`	1	1
`WIN.LOC`	280	12
Total forgeable	12,701	87
Non-reachable code	36,665	101
Total	49,366	106

TÉCNICO LISBOA

ANALYSIS OF FORGEABLE REQUESTS

- SuiteCRM and SugarCRM → violate the server's integrity 115/38
- Neos → violate the server's integrity 115/8
- Kibana → violate the server's integrity 115/1
- Modx → violate the server's integrity 115/20
- Odoo → violate the server's integrity 115/1
- Shopware → violate the server's integrity 115/20

TÉCNICO LISBOA

LIMITATIONS AND FUTURE SCOPE

TÉCNICO LISBOA

LIMITATIONS

- Static analysis tools used for the construction of the property graph.
- Checking real time vulnerability is difficult in this case.
- Crawling can not give 100 % code coverage

TÉCNICO LISBOA

FUTURE WORK OF THIS PAPER

- In future need to include dynamic analysis tools for the construction of the property graph.
- Improve the efficiency of Crawling mechanism
- Need to include additional classes for vulnerability check.

TÉCNICO LISBOA

CONCLUSION

JAW is the new concept of HPG, a canonical, static-dynamic model for clientside JavaScript programs.

TÉCNICO LISBOA

OBSERVATION

1. JAW entire model can be more efficient if we could use dynamic tools for experimental test.

2. JAW does not rely on a specific feature of JavaScript hence the methodology can be used for different programming language.

3. Need to include additional vulnerability classes.

TÉCNICO LISBOA

THANK YOU

joseph.thachil.george@tecnico.ulisboa.pt