



WebSec: Securing Web-driven Systems



CHALMERS



Andrei Sabelfeld

Project Leader

Chalmers University of Technology



David Sands

Chalmers University of Technology



Alejandro Russo

Chalmers University of Technology



**UPPSALA
UNIVERSITET**



Philipp Rümmer

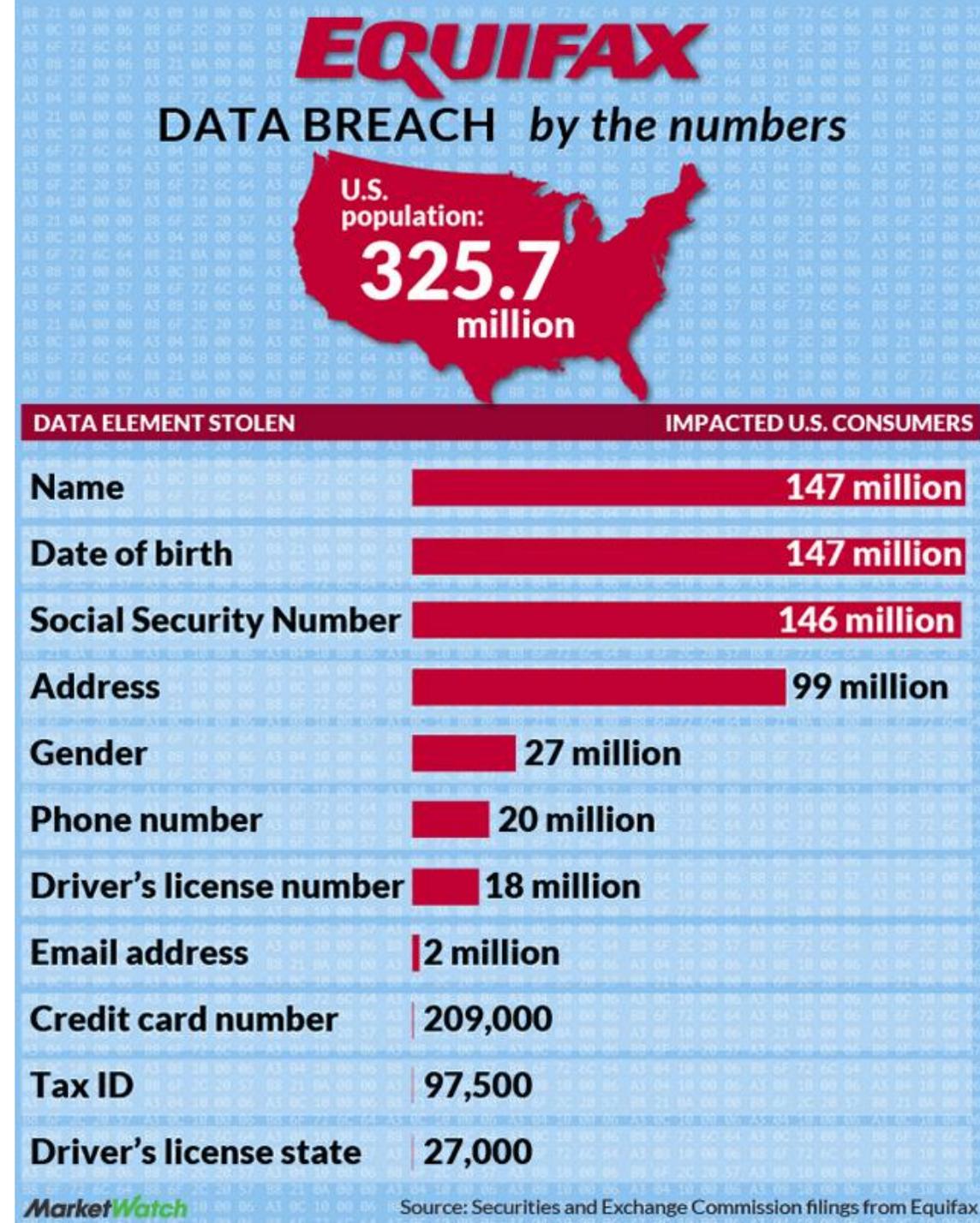
Uppsala University

December 2021

2017 Equifax data breach

- Web code injection attack
- Open-source web framework Apache Struts

Web vulnerabilities and attacks like cross-site scripting (XSS) are the lion's share for companies like Google





JavaScript at the heart of the web

- JavaScript at the heart of the modern web
 - Third-party code everywhere
 - Typical news web site: scripts from ~70 sources
 - Libraries, gadgets, ads, analytics, tracking, fingerprinting,...
- Malicious/buggy JavaScript
 - Exfiltrating private information
 - Malwartising
 - Defacing web sites
 - Phishing attacks

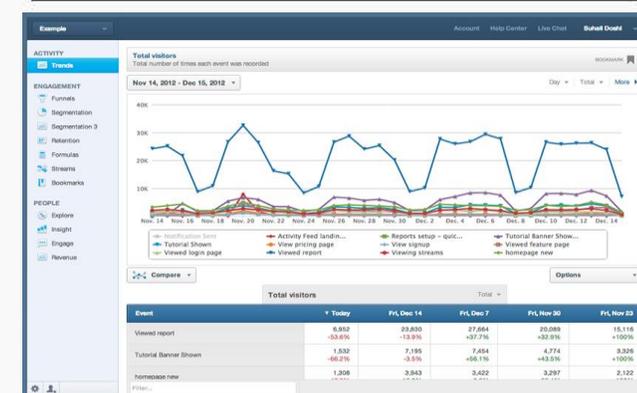


JavaScript

Securing JavaScript essential

Mixpanel analytics accidentally slurped up passwords

Posted Feb 5, 2018 by [Josh Constine \(@joshconstine\)](#)



The passwords of some people using sites monitored by popular analytics provider Mixpanel were mistakenly pulled into its software.



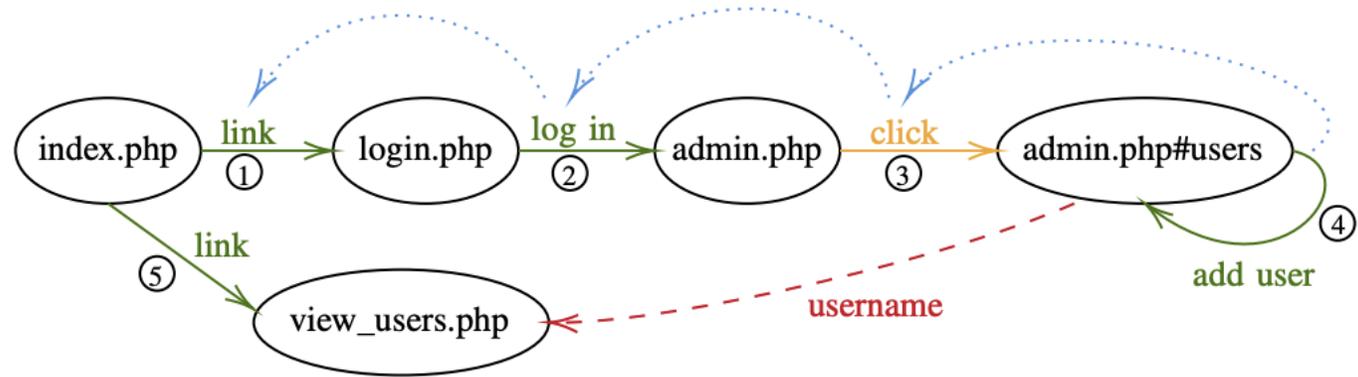
Status

- World-leading publication record
 - Published in all “Big Four” security conferences, all A*
 - IEEE Security & Privacy Symposium (S&P) 2021 (two papers), among 115 papers out of 952 (12.1%).
 - USENIX Security Symposium (USENIX Sec) 2021, among 248 papers out of 1319 (18.8%)
 - ACM Conference on Computer and Communications Security (CCS) 2018, among 134 papers out of 809 (16.6%)
 - Network and Distributed System Security Symposium (NDSS) 2019, among 149 papers out of 933 (16%)
 - Other A* publications, top in Web, Programming Languages, and Verification
 - Web Conference (WWW) 2020
 - ACM Symposium on Principles of Programming Languages (POPL) 2019
 - Computer-Aided Verification (CAV) 2019
- Putting theory to work for practice: WebSec tools
 - AutoNav <https://www.cse.chalmers.se/research/group/security/autonav>
 - Black Widow <https://github.com/SecuringWeb/BlackWidow>
 - JSFlow <https://jsflow.net>
 - OSTRICH <https://github.com/uuverifiers/ostrich>
 - SandTrap <https://github.com/sandtrap-monitor/sandtrap>
- Educational tool: Information Flow Challenge: <https://ifc-challenge.appspot.com>





Crawling 2.0

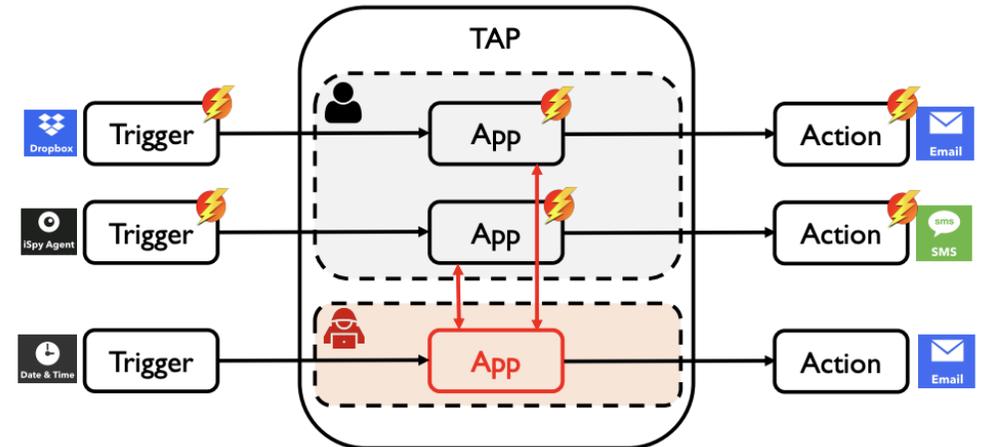


- Black Widow <https://github.com/SecuringWeb/BlackWidow>
- Navigation modeling, including clicks and form submissions
- Traversing, with global workflows
- Tracking inter-state dependencies
- Code coverage improvement: up to 280% wrt other crawlers
- Found new XSS vulnerabilities in production software
 - HotCRP, osCommerce, PrestaShop, and WordPress



Securing JavaScript

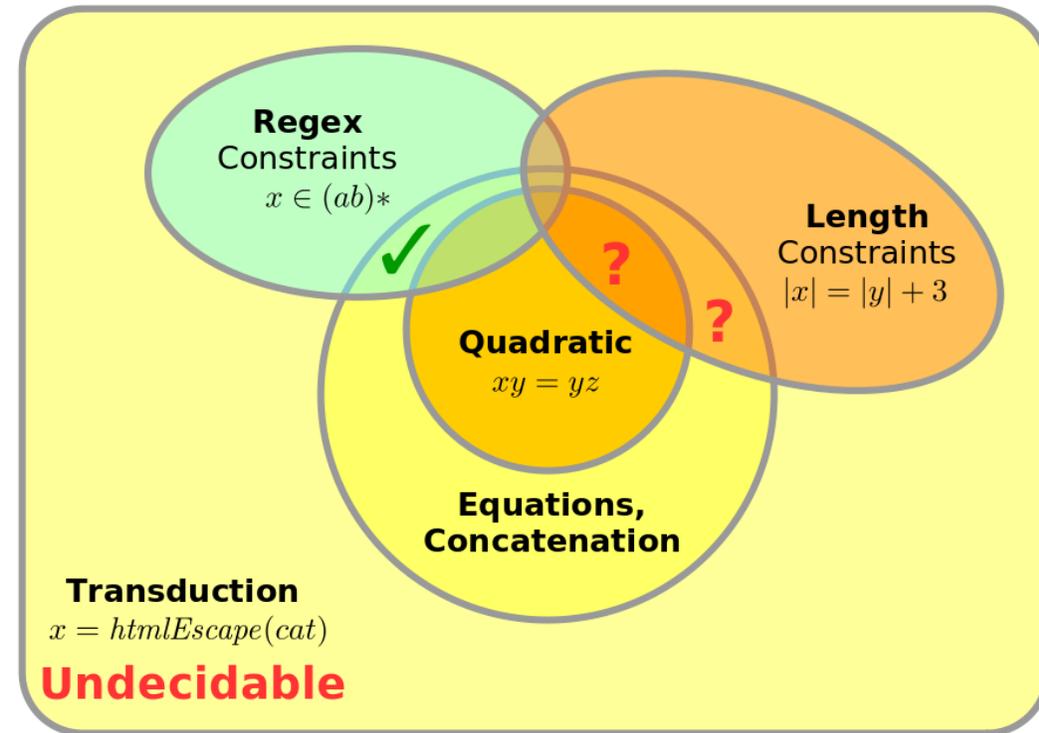
- SandTrap <https://github.com/sandtrap-monitor/sandtrap>
- JavaScript sandbox breakouts
 - IFTTT, Zapier, Node-RED
 - Coordinated disclosure
- SandTrap monitor to enforce policies
 - Baseline and advanced
 - Module-, API-, value-, and context-level
- Benchmarking on IFTTT, Zapier, Node-RED





SMT Methods for Strings

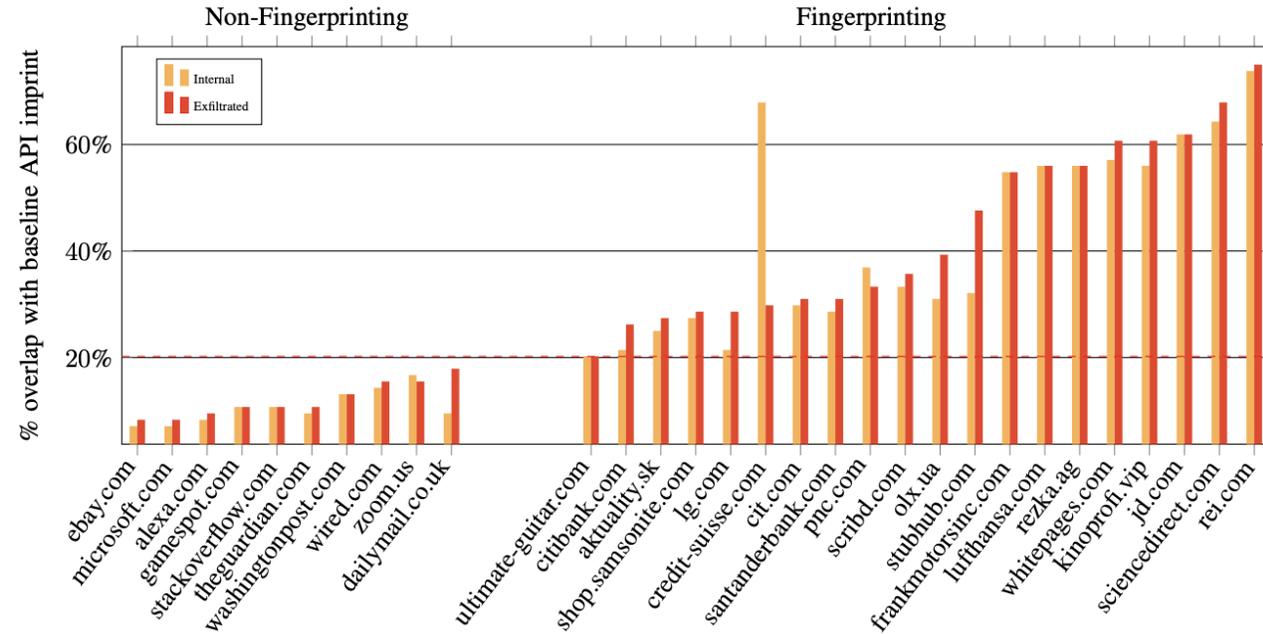
- OSTRICH <https://github.com/uuverifiers/ostrich>
- Solver for expressive combination of string constraints:
 - Word equations
 - Regular expressions
 - Transformations (e.g., escaping)
 - Length constraints
- Wide range of applications:
 - Symbolic execution, verification
 - Web crawling, scanning
 - Testing, white-box fuzzing, etc.





Browser Fingerprinting

- JSFlow <https://jsflow.net>
- Gather browser-specific info from **sources**
 - Fonts, canvas, screen resolution,...
- Combine and sent to network **sink**
- JSFlow to track the trackers!
- Analysis of categories
 - Analytics
 - Authentication (Banks)
 - Bot detection
 - Tracking by fingerprinting





Utilization and dissemination

- Patent application on securing web-driven trigger-action systems
- Acknowledged vulnerability discovery in industrial software
 - IFTTT, Zapier, Node-RED, CIVS, EasyChair, WordPress, osCommerce, HotCRP,...
- Collaboration with Chalmers Innovation System
- Utilization
 - Boost adoption potential of BlackWidow and JSFlow
 - BlackWidow and JSFlow prototypes for security testing
- Educational tool: Information Flow Challenge
<https://ifc-challenge.appspot.com>





WebSec: Securing Web-driven Systems

<https://www.cse.chalmers.se/research/group/security/websec>