



链滴

# Http 响应拆分漏洞

作者: [Eddie](#)

原文链接: <https://ld246.com/article/1497802699115>

来源网站: [链滴](#)

许可协议: [署名-相同方式共享 4.0 国际 \(CC BY-SA 4.0\)](#)

## 案例分析

很多网站在登录时，为了用户体验，都会在登录连接带上登录成功后的跳转链接，这里先不谈附带链的合法性（通过改变跳转链接将用户引导到钓鱼网站），到底什么事http响应拆分漏洞（CRLF注入详）？

## 实例检验

<http://www.xxx.com/login.jsp?towhere=%0D%0A+WebScanCustomInjectedHeader%3A+Injected%5Fby%5FDBApp>

当用户登录成功，使用towhere参数进行跳转时，header被设置了非法信息。

```
HTTP/1.1 302 Found
Server: nginx/1.6.0
Date: Tue, 09 May 2017 18:35:10 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 120
Location: http://www.xxx.com/
Connection: keep-alive
WebScanCustomInjectedHeader: Injected_by_DBApp
The URL has moved <a href="http://www.xxx.com/login.jsp?towhere=%0D%0A+WebScanCustomInjectedHeader: Injected_by_DBApp">here</a>
```

## 原因

这种事情不但发生在登录跳转，而且在普通的query参数都会发生，因为参数带有：

CR = %0d = \r

LF = %0a = \n

造成网页被植入任何代码。

## 解决方法

对query参数中的CR、LF进行过滤。