CRLF Injection : Carriage Return [ASCII 13, \r , Line Feed [ASCII 10,\n]

Description:
CRLF is a sequence that is used to terminate a line in HTTP Protocol. CRLF injection vulnerability occurs when any application does not have proper user input sanitization, which allows attackers for insertion of carriage returns and linefeeds

CRLF Injection can be used by attackers for Log Poisoning and HTTP response splitting.

1. Log Poisoning: In Log Poisoning the attacker can falsify the log file entries by inserting an end of a line and extra line. This will create confusion when someone will analyze the logs.

2. HTTP Response Splitting : Attackers add extra header which can be further exploited for performing XSS and Information Disclosure . HTTP headers uses CRLF to signify where one headers ends and other starts.

Normal Search Request:

GET /search.asp?search=abc

Below payload will set malicious cookie.
GET /search.asp?search=/%0d%0aSet-Cookie:attacker=yash

Let's say an attacker is able to inject a Location header , So **redirection attack** can be carried out.

Sample Payload: /%od%oaLocation:%20https://malicious.com

XSS using CRLF Injection attack :

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

Mitigation:
1. Strip any new line characters before passing content into the header
2. Code Review : User supplied data is sanitized, and user inputs are not passed directly in http headers
3. Encode the data which is passed into the headers, this will scramble the CR and LF codes