Blind OS command injection with output redirection

Herkese merhaba,

Bu gün portswigger'da bulunan Command injection başlığının altındaki Blind OS command injection with output redirection lab'ının çözümünü anlatacağım.

İlk olarak submit feedback kısmını doldurup isteğimizi yakalıyoruz.

```
POST /feedback/submit HTTP/2

Most: Oal1004C04044746E18a0c00000000b0. web-security-academy.net
Content-length: 105

Sec-Ch-Ua-Chrosium-ye-127*, "Mot)A.Brand";v=-59*

Sec-Ch-Ua-Chrosium-ye-127*, "Mot)A.Brand";v=-59*

Sec-Ch-Ua-Chrosium-ye-127*, "Mot)A.Brand";v=-59*

Accept-language: tr-10-chrosium-ye-127*, "Mot)A.Brand";v=-59*

Sec-Ch-Ua-Chrosium-ye-127*, "Mot)A.Brand";v=-59*

Sec-Ch-Ua-Chrosium-ye-127*, "Mot)A.Brand";v=-59*

Sec-Ch-Ua-Chrosium-ye-127*, "Mot)A.Brand";v=-59*

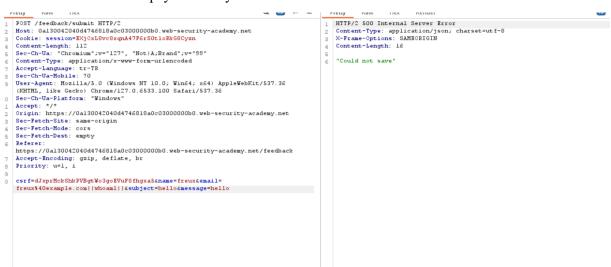
Sec-Ch-Ua-Chrosium-ye-127*, "Mot)A.Brand";v=-59*

Sec-Ch-Ua-Chrosium-ye-127*, "Mot)A.Brand";v=-59*

Accept-Rench-Ua-Language: tr-10-chrosium-ye-127*, "Mot)A.Brand";v=-59*

Sec-Ch-Ua-Chrosium-ye-127*, "Mot)A.Brand";v=-
         csrf=YzeUJQgAVgBpkG7PlbQTFi0OnH6eobc7&name=freux&email=freux%40example.com&subject=qwewqe&message=wqeqweq
```

Ardından email kısmına payload deniyoruz.



Doğru yolda olduğumuzu anlamış olduk .yakaladığımız istekler arasında image istekleri'de vardı /var/www/images/ dizini altına bir txt dosyası oluşturalım.,

```
GRT /image?filename=21.jpg HTTP/2

Host: Oal3004C040d4746818aOc03000000b0.web-security-academy.net

Cookie: session=rAkqeVCTcc9iloA609mCcgjKTsn77b54

Sec-Ch-Ua-"Chronium';v"=127", "Not)A;Brand";v"=99"
Accept-Language: tr-TR
Sec-Ch-Ua-Phobile: 70

User-Agent: Hozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36

(MRHML, like Gecho: Chrome/127.0.6533.100 Safari/537.36

Sec-Ch-Ua-Platform: "Windows"
Accept: image/avif,image/webp,image/apng,image/syg*xml,image/*,*/*;q=0.8

Sec-Fetch-Site: same-origin
Sec-Fetch-Dest: image
Refere: https://oal3004204044746818aOc0300000b0.web-security-academy.net/
Accept-Encoding: gsip, deflate, br
Priority: u=2, i
                                                                                                                                                                                                                                                                                                                                                         yθyálExifMM*DDx~(1$^200ii$

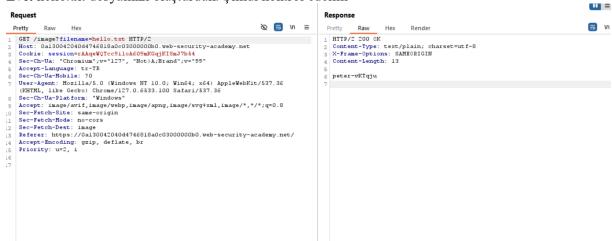
10' WlAdobe Photoshop CC 2019 (Hacintosh)2019:03:01

16:19:1600221 γγ ¼ ότα (ΠΟΗΗγθγίλΑdobe_CMγίλΑdobedDyÖD

γλλ "γΫ́ γλλ
```



Evet hello.txt dosyamızı oluşturduk. Şimdi kontrol edelim



Dosyamız oluşmuş durumda ve Lab'ımızı da tamamlamış bulunmaktayız.

