
WEB -

SQL

#

JSON

#

GET,POST,COOKIE,REQUEST,HTTP

SQL

',',"%),}



=>sqlilabs less 5 6

POST =>sqlilabs less 11

JSON =>

COOKIE =>sqlilabs less 20

HTTP =>sqlilabs less 18



```
# sqlilabs
<?php
header('content-type:text/html;charset=utf-8');
if(isset($_POST['json'])){
$json_str=$_POST['json'];
$json=json_decode($json_str);
if(!$json){
die('JSON ');
}
$username=$json->username;
//$passwd=$json->passwd;

$mysqli=new mysqli();
$mysqli->connect('localhost','root','root');
if($mysqli->connect_errno){
die(' '.$mysqli->connect_error);
```

```
}
$mysqli->select_db('security');
if($mysqli->errno){
    die('                '.$mysqli->error);
}
$mysqli->set_charset('utf-8');
$sql="SELECT * FROM users WHERE username='{ $username}'";
echo $sql;
$result=$mysqli->query($sql);
if(!$result){
    die('                SQL                '.$mysqli->error);
}else if($result->num_rows==0){
    die('                ');
}else {
    $array1=$result->fetch_all(MYSQLI_ASSOC);
    echo "                {$array1[0]['username']},                {$array1[0]['password']}";
}
$result->free();
$mysqli->close();
}
?>
```
