

作业 2 内容

基础部分：

- 部署 sqli_labs 靶机
- 尝试操作和复现课程 sql 注入相关内容 (dvwa 和 sqli_labs 等)

实践部分：

- 结合如下两个截图，自行实验，分析和解释看似相同的两个sql注入输入效果不同的原因

a. 直接在输入框输入 1'#

User ID: Submit

ID: 1'
First name: admin
Surname: admin

More Information

- <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
- https://en.wikipedia.org/wiki/SQL_injection
- <http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>
- <http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>
- https://www.owasp.org/index.php/SQL_Injection
- <http://bobby-tables.com/>

b. 在浏览器地址栏把 id 参数值设置为 1'#

Vulnerability: SQL Inject... +
localhost:18080/dvwa-master/vulnerabilities/sql/?id=1'#&Submit=Submit

DVWA DVWA2.2 SQL-labs pikachu DVWA-docker Get the pikachu upload-labs RIPS BeEF-docker Webbug Index of /Basic
Cookies CSS 表单 图片 网页信息 其他功能 标记 缩放 工具 查看源代码 选项

DVWA

Vulnerability: SQL Injection

User ID: Submit

More Information

- <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
- https://en.wikipedia.org/wiki/SQL_injection
- <http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>
- <http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>
- https://www.owasp.org/index.php/SQL_Injection
- <http://bobby-tables.com/>

- 二次注入实践，复现 sqli-labs 中 less-24 的 sql 注入实验

提交部分：

- 实践部分 1:

说明两种方式结果不同的原因，最好有分析和实验的截图过程

2. 实践部分 2:
 - a. 实践过程截图
 - b. 结合代码，说明Less-24二次注入的原理