WEB安全实验

信息安全认知实习

授课老师：颉夏青

xiexiaqing@bupt.edu.cn

网络空间安全学院实验中心

2018年9月14日

SQL注入

- SQL基础
- SQL注入原理——以表单为例
- SQL注入的危害
- 如何防范
- 实验要求

SQL注入实验

SQL基础

- SQL（Structured Query Language），一种结构化的查询语言，是关系型数据库通讯的标准语言。
- **常用的SQL语句**：
- 查询： select statement from table where condition
- 删除：delete from table where condition
- 更新：update table set field = value where condition
- 添加记录：insert into table field
- ……

自学教程推荐：http://www.w3school.com.cn/sql/

SQL注入实验

- SQL基础

table： student

No.	Name	Age
1	张三	18
2	李四	20
3	韩梅梅	19
4	李雷	20

- 查询： select * from student where Age= ‘20’
- 删除：delete from student where Age= ‘20’
- 更新：update student set Age = ‘19’ where Name= ‘张三’

SQL注入实验

什么是SQL注入

- SQL注入： SQL Injection
- 所谓SQL注入，就是通过把SQL命令插入到**Web表单**提交或**输入域名**或页面请求的查询字符串，最终达到欺骗服务器执行恶意的SQL命令。
- 域名示例：
- HTTP://www.xxx.xxx/text.asp?id=XX（带有参数的asp或者动态网页）

https://bbs.byr.cn/#!article/Security/40243?p=2#a24

SQL注入实验

- SQL注入原理——以表单为例
  - 猜想：判断语句为
  - **SELECT * From Table WHERE Name= ‘XX’ and Password= ‘YY’**

SQL注入实验

- SQL注入原理——以表单为例
  - 猜想：判断语句为
  - **SELECT * From Table WHERE Name= ‘XX’ and Password= ‘YY’**

myname’ or 1=1 --

SELECT * From Table WHERE Name=‘myname’ or 1=1 --’ and Password=‘YY’

SQL注入实验

- SQL注入原理——以表单为例
  - 猜想：判断语句为
  - **SELECT * From Table WHERE Name= ‘XX’ and Password= ‘YY’**

‘ or 1=1
“ or 1=1
‘ or ‘a’=‘a
“ or “=a

SQL注入实验

- SQL注入原理——以表单为例

- 举个例子
- http://132.232.171.13:8888/sql/index

SQL注入实验

- 实验提示（重要）

  - **通常恒等式用于获取所有数据或者测试是否能够成功。**
  - **本次实验**过程如何不用密码进入到自己的账号？
  - **输入：**
    - **学号”；#**
    - **如 2018001“;#**

SQL注入实验

- SQL注入原理——以表单为例

  - **原因分析**

  - 用户输入没有被正确地过滤：转义字符(引号、反引号、双下划线、分号、百分号)。
  - 没有进行严格类型检查：未判断输入是否预定类型。
  - **归纳：字符串拼接。**

SQL注入实验

SQL注入的危害

- 数据库信息泄漏：数据库中存放的用户的隐私信息的泄露。
- 网页篡改：通过操作数据库对特定网页进行篡改。
- 网站被挂马，传播恶意软件：修改数据库一些字段的值，嵌入网马链接，进行挂马攻击。
- 数据库被恶意操作：数据库服务器被攻击，数据库的系统管理员帐户被窜改。
- 服务器被远程控制，被安装后门。经由数据库服务器提供的操作系统支持，让黑客得以修改或控制操作系统。
- 破坏硬盘数据，瘫痪全系统。

SQL注入实验

- 针对本课程的案例，如何防范
  - 认真对表单输入进行校验，从查询变量中滤去尽可能多的可疑字符。
  - 将用户输入以参数的形式进行封装，而不是直接嵌入查询语句

请大家查阅资料，是否还有其他的防范方法?

实验二-SQL注入实验（实验要求）

- 针对提供的网站： http://132.232.171.13:8888/sql/index
- 通过测试sql注入漏洞，绕过密码并获取到个人信息管理页面（用户名为自己的学号）。(**重要提示：赋值用户名为自己的学号，直接注释掉后面的密码)**
- 在实验报告中说明：
- （1）尝试攻击的步骤与尝试、分析过程
- （2）攻击成功截图证明
- （3）针对此网站，提供可能的防护SQL注入方法
- 进阶：可通过测试发现其他有sql注入的网站并证明之，可利用sql注入检测工具如sqlmap，web扫描工具：wvs。

XSS攻击

- XSS原理
- XSS分类
- 危害
- 实验演示
- 实验要求

XSS实验

XSS原理

- Cross Site Scripting
- 为了不和层叠样式表（Cascading Style Sheets, CSS)的缩写混淆，故缩写为XSS
- 恶意攻击者往**Web页面**里插入恶意**Script代码**，当用户浏览该页之时，嵌入其中Web里面的Script代码会被执行，从而达到恶意攻击用户的目的**（在客户端浏览器执行）**。
- 跨站脚本攻击（XSS）就是常见的Web攻击技术之一，由于跨站脚本漏洞易于出现且利用成本低，所以被OWASP列为当前的头号Web安全威胁。

XSS实验

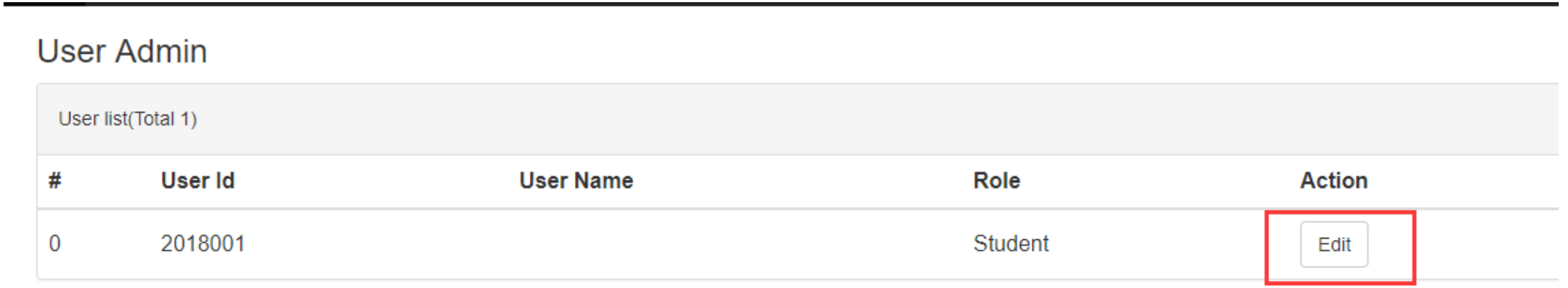
- 分类
  - 根据持续时间可以分为两种类型：
  - 持久型和非持久型
  - 根据数据流向又可以分为三种攻击类型：
  - 反射型XSS攻击：浏览器→后端→浏览器
  - 存储型XSS攻击：存储型数据流向是：浏览器→后端→**数据库**→后端→浏览器
  - DOMBasedXSS：URL-->浏览器

XSS实验

- 危害（执行JavaScript的危害）
  - 1、盗取各类用户帐号，如机器登录帐号、用户网银帐号、各类管理员帐号
  - 2、控制企业数据，包括读取、篡改、添加、删除企业敏感数据的能力
  - 3、盗窃企业重要的具有商业价值的资料
  - 4、非法转账
  - 5、强制发送电子邮件
  - 6、网站挂马
  - 7、控制受害者机器向其它网站发起攻击

XSS实验

- 实验演示
  - http://132.232.171.13:8888/sql/home
  - 入口（在sql注入成功的基础上进行本次实验）：



XSS实验

实验演示

- http://132.232.171.13:8888/sql/home
- 第一步：测试是否有xss漏洞

```
<script>alert(1)</script>
```

- 第二步：尝试运行脚本

```
<script>alert(document.cookie)</script>
```

```
<script>window.open()</script>
```

XSS

如何防范

- 目标是让代码不能正常执行
- 永远不相信用户的输入——需要对用户的输入进行处理，只允许输入合法的值，其它值一概过滤掉
- 针对本网站，具体如何防御，留作思考。

实验要求——XSS实验

- 针对提供的网站： http://132.232.171.13:8888/sql/index
- 尝试进行xss攻击，获取网站cookie，并成功打开新的链接。
- 在实验报告中说明：
- （1）尝试攻击的步骤与尝试、分析过程
- （2）攻击成功截图证明
- （3）针对此网站，思考提供可能的防御方法。
- 进阶：可通过测试发现其他有XSS漏洞的网站并证明之。