Atitit 登录模块常见的安全措施条例与攻击行为表

目录

[1. 安全目标 1](#_Toc28051)

[2. 常见安全措施 2](#_Toc10621)

[2.1. 修改密码需要验证员密码 2](#_Toc2415)

[2.2. 密码Salt加盐机制 2](#_Toc8890)

[2.3. Sql防注入 2](#_Toc3810)

[2.4. 弱口令 防爆次数限制 2](#_Toc14333)

[2.5. 钓鱼输入各种账号密码信息 2](#_Toc29411)

[2.6. 不同权限用户(商户 管理员）隔离开ui与数据库 2](#_Toc25277)

[2.7. 权限标识等重要放入mrz区效验 2](#_Toc10238)

[2.8. Cookie加密mrz区 2](#_Toc30333)

[2.9. 防止撞库攻击 3](#_Toc23082)

[2.10. 校验ua与ip，防止Cookie重放 3](#_Toc979)

[3. 常见攻击行为 3](#_Toc569)

[3.1. Cookie重放攻击 3](#_Toc26772)

[3.2. 非法获取密码和权限 3](#_Toc21964)

[3.3. 暴力破解 3](#_Toc7797)

[3.4. 彩红标攻击 3](#_Toc32761)

[3.5. Sql注入 3](#_Toc9121)

[3.6. 拖库攻击 破解出用户的密码 3](#_Toc12286)

[3.7. 伪造登录请求 3](#_Toc29972)

[3.8. 劫持了用户的请求数据 3](#_Toc14011)

[3.9. 撞库攻击 3](#_Toc4284)

[4. 来源相关规范 4](#_Toc28871)

[4.1. 登录系统个相关标准 4](#_Toc26029)

[4.2. Atitit 登录账号管理法passport v4 4](#_Toc27224)

[4.3. Atitit 安全登录退出管理法v3 tbb.docx 4](#_Toc2797)

[4.4. Atitit 信息系统安全法v3 非法攻击行为 列表 5](#_Toc21345)

[5. Ref 5](#_Toc6558)

# 安全目标

说具体一些，我们理想中的绝对安全的系统大概是这样的：

1. 首先保障数据很难被拖库。
2. 即使数据被拖库，攻击者也无法从中破解出用户的密码。
3. 即使数据被拖库，攻击者也无法伪造登录请求通过验证。
4. 即使数据被拖库，攻击者劫持了用户的请求数据，也无法破解出用户的密码

# 常见安全措施

## 修改密码需要验证员密码

## 密码Salt加盐机制

## Sql防注入

## 弱口令 防爆次数限制

## 钓鱼输入各种账号密码信息

## 不同权限用户(商户 管理员）隔离开ui与数据库

## 权限标识等重要放入mrz区效验

## Cookie加密mrz区

非mrz区用来调试与人工识别

## 防止撞库攻击

## 校验ua与ip，防止Cookie重放

# 常见攻击行为

## Cookie重放攻击

解决方法

校验ua与ip

## 非法获取密码和权限

## 暴力破解

## 彩红标攻击

## Sql注入

## 拖库攻击 破解出用户的密码

## 伪造登录请求

## 劫持了用户的请求数据

## 撞库攻击

很多互联网公司对安全不重视，近年来密码安全事故频繁发生，导致密码泄露后被拿去撞库，用户利益受损。****应该去推动一下密码安全的业界标准，避免企业犯错用户买单****。同时，****互联网没有绝对的安全，强烈建议用户不要用同一个密码，密码定期改！****

# 来源相关规范

## 登录系统个相关标准

## Atitit 登录账号管理法passport v4

目录

1. 总则 2

1.1. 身份分类登录账号 管理员 操作人员 普通用户 2

1.2. 安全考虑，必须单独分开的账号储存表，使用不同等加密技术与秘钥 2

1.3. 第三条 登录账号登记的项目包括：acc登录账号，密码（加密存储），密码签名，acctype账号类型（uname，eml，手机），姓名、出生日期、住址、身份号码、本人相片、 有效期和签发机关。Id编码 2

1.4. 登录账号Id编码号码是每个用户唯一的、终身不变的身份代码，由 机关按照用户身份号码标准编制 2

2. 第二章 申领和发放 2

3. 第三章 使用和查验 5 2

3.1. 查验时机 2

3.2. 查验条目 3

3.3. 查验防篡改状态（账户名 密码签名等）salt机制。。 3

3.4. 黑名单（冻结名单）检查 3

3.5. 账号注销状态 3

4. 系统常用登录账号法 uname 手机号email 3

4.1. Exampl 3

5. Ref 4

## Atitit 安全登录退出管理法v3 tbb.docx

目录

1.1. 未持有效出入边界票据。。校验票据有效性 1

1.2. 从事与票据种类不符的活动的 2

1.3. 数据为数字的应该校验数字 2

2. 第三章 使用和查验 5 2

2.1. 黑名单（冻结名单）检查 2

3. 登录票据法visa 2

3.1. 1. 总则 1 2

3.2. 1.1. 身份分类 管理员 操作人员 普通用户 1 2

3.3. 1.2. 第十七条 票据的登记项目包括：种类，持有人姓名、使用次数、有效期、，签发日期、地点（ip+浏览器id），其他证件号码（登录账户，用户名，手机号码）等。 1 2

3.4. 1.3. 黑名单（冻结名单）检查 1 2

3.5. 2. 第二章 申领和发放 4 2 2

3.6. 3. 第三章 使用和查验 5 2 2

3.7. 3.1. 票据作废 2 2

4. 系统常用票据法 cookie session token 3

5. Php设置登录票据cookie法 3

6. Ref出境入境管理法100条 4

## Atitit 信息系统安全法v3 非法攻击行为 列表

# Ref

常见 Web 安全攻防总结 - zoumiaojiang.html

即使被拖库，也可以保证密码不泄露 - CoderZh Blog.html