OWASP

Open Web Application Security Project

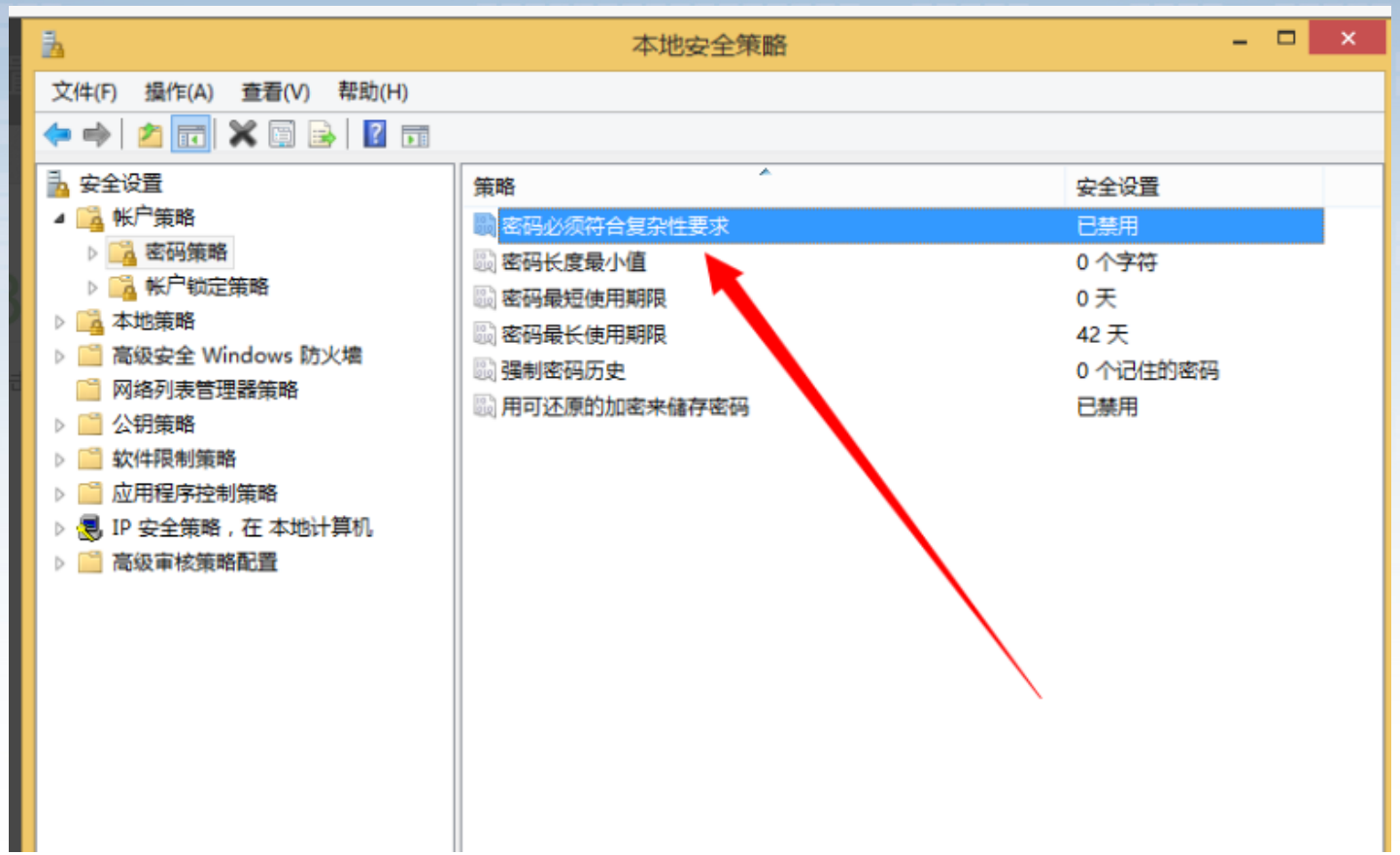
等级保护测评之应用安全高风险判定

李海涛

分享议题

1、密码复杂度策略不足会是高风险？
2、有弱密码就一定是高风险？
3、只要设置了复杂口令就不是高风险？
4、无双因素认证什么情况下会是高风险？
5、判定系统漏洞是否为高风险的原则？
6、数据完整性和保密性方面如何预防高风险项？
7、剩余信息和个人信息保护方面高风险判定？

1、密码复杂度策略不足会是高风险？



1、密码复杂度策略不足会是高风险？

判例内容：应用系统无任何用户口令复杂度校验机制，校验机制包括口令的长度、复杂度等，可判定为高风险。

适用范围：所有系统。

满足条件（同时）：

a) 应用系统无口令长度、复杂度校验机制；

b) 可设置 6 位以下，单个数字或连续数字或相同数字等易猜测的口令。

补偿措施：

a) 如应用系统采用多种身份鉴别认证技术的，即使有口令也无法直接登录应用系统的，可酌情降低风险等级。

b) 如应用系统仅为内部管理系统，只能内网访问，且访问人员相对可控，可酌情降低风险等级。

c) 如应用系统口令校验机制不完善，如只有部分校验机制，可根据实际情况，酌情降低风险等级。

d) 特定应用场景中的口令（如 PIN 码）可根据相关要求，酌情判断风险等级。

整改建议：建议应用系统对用户的账户口令长度、复杂度进行校验，如要求系统账户口令至少8位，由数字、字母或特殊字符中2种方式组成；对于如PIN码等特殊用途的口令，应设置弱口令库，通过对比方式，提高用户口令质量。

2、有弱密码就一定是高风险么？

7.2.1.2 应用系统存在弱口令

对应要求：应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换。

判例内容：应用系统存在易被猜测的常用/弱口令帐户，可判定为高风险。

适用范围：所有系统。

满足条件：

通过渗透测试或常用/弱口令尝试，发现应用系统中存在可被登录弱口令帐户。

补偿措施：如该弱口令帐号为前台自行注册，自行修改的普通用户帐户，被猜测登录后只会影响单个用户，而不会对整个应用系统造成安全影响的，可酌情降低风险等级。

整改建议：建议应用系统通过口令长度、复杂度校验、常用/弱口令库比对等方式，提高应用系统口令质量。

3、只要设置了复杂口令就不是高风险？

7.2.1.3 应用系统无登录失败处理机制

对应要求：应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施。

判例内容：可通过互联网登录的应用系统未提供任何登录失败处理措施，攻击者可进行口令猜测，可判定为高风险。

适用范围：3级及以上系统。

满足条件：

a) 3级及以上系统；

b) 可通过互联网登录，且对帐号安全性要求较高，如帐户涉及金融、个人隐私信息后台管理等

c) 对连续登录失败无任何处理措施；

d) 攻击者可利用登录界面进行口令猜测。

3、只要设置了复杂口令就不是高风险？

补偿措施：

a) 如应用系统采用多种身份鉴别认证技术的，可酌情降低风险等级。

b) 仅通过内部网络访问的内部/后台管理系统，如访问人员相对可控，可酌情降低风险等级。

c) 如登录页面采用图像验证码等技术可在一定程度上提高自动化手段进行口令暴力破解难度的，可酌情降低风险等级。

d) 可根据登录帐户的重要程度、影响程度，可酌情判断风险等级。但如果登录帐户涉及到金融行业、个人隐私信息、信息发布、后台管理等，不宜降低风险等级。

整改建议：建议应用系统提供登录失败处理功能（如帐户锁定、多重认证等），防止攻击者进行口令暴力破解。

4、无双因素认证什么情况下会是高风险？

7.2.1.4 互联网可访问系统未实现双因素认证

对应要求：应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。

判例内容：通过互联网方式访问，且涉及大额资金交易、核心业务等操作的系统，在进行重要操作前应采用两种或两种以上方式进行身份鉴别，如只采用一种验证方式进行鉴别，可判定为高风险。

适用范围：3级及以上系统。

满足条件（同时）：

a) 3 级及以上系统；

b) 通过互联网方式访问的系统，在进行涉及大额资金交易、核心业务等重要操作前未启用两种或两种以上鉴别技术对用户身份进行鉴别；4 级系统多种鉴别技术中未用到密码技术或生物技术。

4、无双因素认证什么情况下会是高风险？

补偿措施：

a) 采用两重用户名/口令认证措施，且两重口令不可相同等情况，可酌情降低风险等级。

b) 如应用服务访问的网络环境安全可控，网络窃听、违规接入等隐患较小，口令策略和复杂度、长度符合要求的情况下，可酌情降低风险等级。

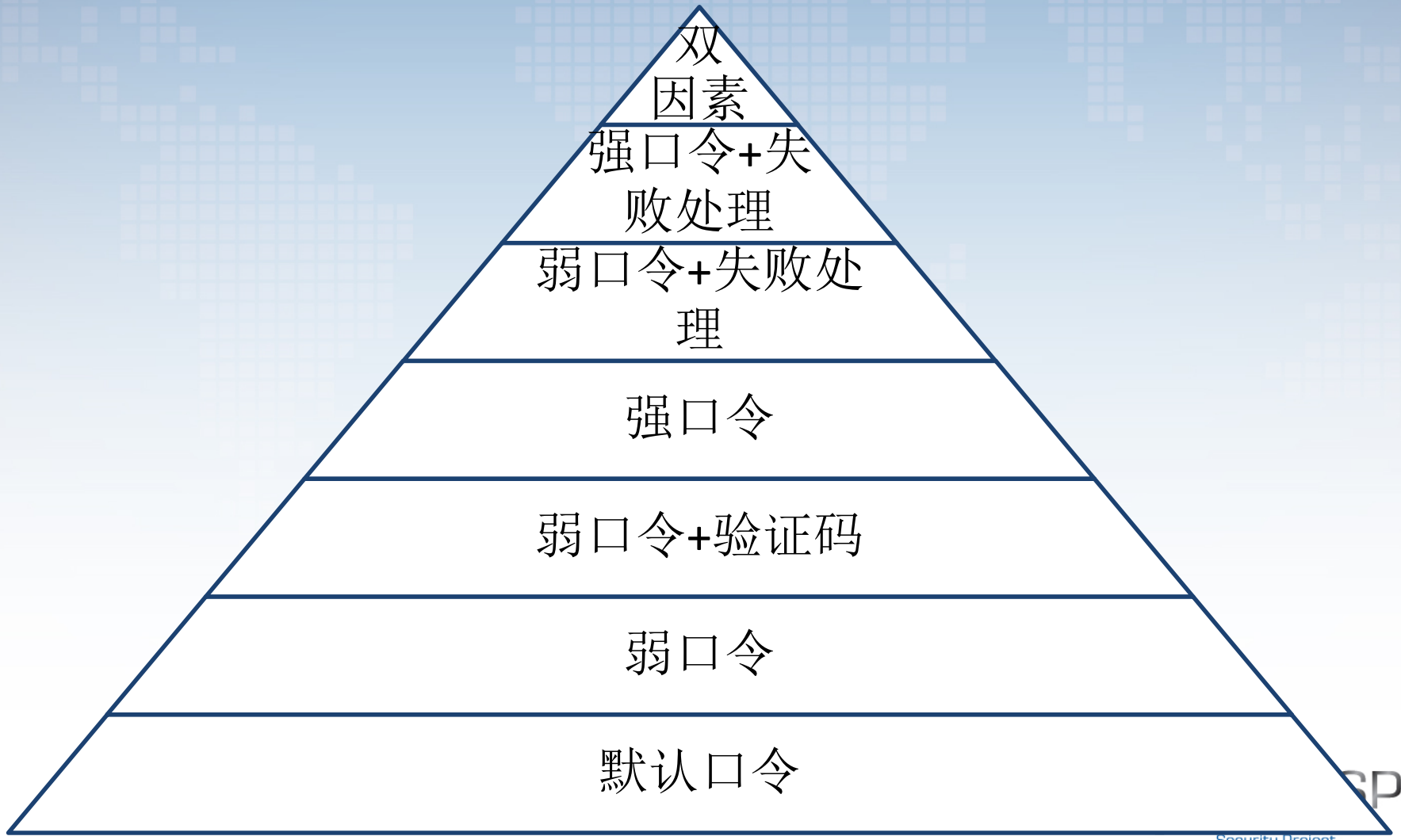
c) 在完成重要操作前的不同阶段两次或两次以上使用不同的方式进行身份鉴别，可根据实际情况，酌情降低风险等级。

d) 涉及到主管部门认可的业务形态，例如快捷支付、小额免密支付等，可酌情降低风险等级。

e) 可根据被测对象中用户的作用以及重要程度，在口令策略和复杂度、长度符合要求的情况下，可根据实际情况，酌情判断风险等级。

f) 系统用户群体为互联网用户，且冒名登录、操作不会对系统或个人造成重大恶劣影响或经济损失的，可酌情判断风险等级。

身份鉴别强度层级



5、判定系统漏洞是否为高风险的原则？

7.2.4 入侵防范

7.2.4.1 数据有效性检验功能存在缺陷

对应要求：应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求。

判例内容：由于校验机制缺失导致的应用系统存在如SQL注入、跨站脚本、上传漏洞等高风险漏洞，可判定为高风险。

适用范围：所有系统。

满足条件：

a) 应用系统存在如 SQL 注入、跨站脚本、上传漏洞等可能导致敏感数据泄露、网页篡改、服务器被入侵等安全事件的发生，造成严重后果的高风险漏洞；

b) 无其他技术手段对该漏洞进行防范。

补偿措施：

c) 如应用系统存在 SQL 注入、跨站脚本等高风险漏洞，但是系统部署了 WAF、云盾等应用防护产品，在防护体系下无法成功利用，可酌情降低风险等级。

d) 不与互联网交互的内网系统，可根据系统重要程度、漏洞危害情况等，酌情判断风险等级。

5、判定系统漏洞是否为高风险的原则？

7.2.4.3 应用系统存在严重逻辑缺陷类漏洞

对应要求：应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。

判例内容：如应用系统的业务功能（如密码找回功能等）存在高风险安全漏洞或严重逻辑缺陷，可能导致修改任意用户密码、绕过安全验证机制非授权访问等情况，可判定为高风险。

适用范围：所有系统。

满足条件：

通过测试，发现应用系统的业务功能（如密码找回功能等）存在高风险安全漏洞或严重逻辑缺陷，可能导致修改任意用户密码、绕过安全验证机制非授权访问等情况。

补偿措施：无。

整改建议：建议通过修改应用程序的方式对发现的高风险/严重逻辑缺陷进行修补，避免出现安全隐患。

6、数据完整性和保密性方面如何预防高风险项？

5.2.1 数据传输无完整性保护措施

对应要求：应采用密码技术保证通信过程中数据的完整性。

判例内容：对数据传输完整性要求较高的系统，数据在网络层传输无完整性保护措施，一旦数据遭到篡改，可能造成财产损失的，可判定为高风险。

适用范围：对数据传输完整性要求较高的3级及以上系统。

a) 3 级及以上系统；

b) 系统数据传输完整性要求较高；

c) 数据在网络层传输无任何完整性保护措施。

补偿措施：如应用层提供完整性校验等措施，或采用可信网络传输，可酌情降低风险等级。

6、数据完整性和保密性方面如何预防高风险项？

7.2.6 数据保密性

7.2.6.1 敏感信息明文传输

对应要求：应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。

判例内容：用户鉴别信息、公民敏感信息数据或重要业务数据等以明文方式在不可控网络中传输，可判定为高风险。

适用范围：3级及以上系统。

满足条件（同时）：

a) 3 级及以上系统；

b) 用户身份认证信息、个人敏感信息数据或重要业务数据等以明文方式在不可控网络中传输。

补偿措施：

a) 如使用网络加密的技术确保数据在加密通道中传输，可根据实际情况，视为等效措施，判为符合。

b) 如敏感信息在可控网络中传输，网络窃听等风险较低，可酌情降低风险等级。

7、剩余信息和个人信息保护方面高风险判定？

7.2.8 剩余信息保护

7.2.8.1 鉴别信息释放措施失效

对应要求：应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。

判例内容：身份鉴别信息释放或清除机制存在缺陷，如在正常进行释放或清除身份鉴别信息操作后，仍可非授权访问系统资源或进行操作，可判定为高风险。

适用范围：所有系统。

满足条件（同时）：

a) 身份鉴别信息释放或清除机制存在缺陷；

b) 利用剩余鉴别信息，可非授权访问系统资源或进行操作。

补偿措施：无。

整改建议：建议完善鉴别信息释放/清除机制，确保在执行释放/清除相关操作后，鉴别信息得到完全释放/清除。

7、剩余信息和个人信息保护方面高风险判定？

7.2.9 个人信息保护

7.2.9.1 违规采集、存储个人信息

对应要求：应仅采集和保存业务必需的用户个人信息。

判例内容：在采集和保存用户个人信息时，应通过正式渠道获得用户同意、授权，如在未授权情况下，采取、存储用户个人隐私信息，可判定为高风险。

适用范围：所有系统。

满足条件（任意条件）：

a) 在未授权情况下，采取、存储用户个人隐私信息，无论该信息是否是业务需要。

b) 采集、保存法律法规、主管部门严令禁止采集、保存的用户隐私信息。

补偿措施：如在用户同意、授权的情况下，采集和保存业务非必需的用户个人信息，可根据实际情况，酌情判断风险等级。

急招渗透测试工程师！！！

OWASP
Open Web Application Security Project