Web应用程序安全诊断 摘要记录

2015/8/4

野村綜研（北京）系统集成有限公司 上海分公司

- ○ 诊断对象　上海儿童时代倍乐生文化发展有限公司 小学生酷网 （开发环境）
- ○ 诊断时间　2015年7月27日 (9：00～18：00)～2015年7月29日 (9：00～18：00)
- ○ 诊断实施地点　NRI北京上海分公司office（通过互联网实施诊断）
- ○ 诊断实施方法　主要按照弊公司的诊断手册和诊断工具(VEX&Nikto)全面实施诊断
- ○ 诊断对象功能　登录、投稿、提问

序号	指摘事项	危险度	难易度	说明	建议
1	存在XSS漏洞	中	难	**多个页面存在XSS漏洞。** 本系统的多个页面，因为从客户发送的参数没有经过无害化处理，存在XSS漏洞。通过恶意使用这个问题，存在可以在浏览器上执行恶意代码，从而取得Cookie，显示非法的错误信息等攻击的可能性。(参考另附图1) 本系统，因为Session管理使用的Cookie里含有SessionID，Cookie被诈取的情况下，存在可以伪装成第三者的可能性。 据报道，最近恶意使用这个漏洞，诱导和本系统类似站点的用户，非法取得重要信息的被称为网络钓鱼的攻击较多。	在服务器端全部检测从客户端发送的参数。对SELECT、RADIO、HIDDEN属性的值也要进行检测。 另外，生成HTML，请对HTML标签进行正确的无害化处理。
2	明文发送重要信息	中	难	**ID、密码没有经过加密被发送。** 本系统，客户端和Web服务器之间的通信都是在http状态下进行的，没有使用SSL。使用http连接的情况下，认证等信息被明文发送。这些信息被侦听的情况下，存在信息泄露、被伪装成第三者的风险。(参考另附图2)	输入、显示重要的信息的页面的情况下，请使用SSl，加密通信。 另外，推荐请只允许https连接。

序号	指摘事项	危险度	难易度	说明	建议
3	没有帐号锁定功能	中	难	**没有帐号锁定时，使用暴力破解存在ID/密码泄露的风险。** 本系统的认证处理，连续密码认证失败的情况下，也不存在帐号被锁定等类似的功能。因此，如果怀有恶意的第三者使用暴力破解的手段，存在认证信息泄露、被伪装的风险。	认证连续失败的情况下，可能会遭受暴力破解攻击。推荐连续认证失败超过一定次数以后，暂时停止该帐号的认证处理(锁定帐号)。 一般做法是经过一定的时间以后，自动解除帐号锁定。 也可以使用验证码。
4	自动登录用的Cookie里包含认证信息	中	难	**自动登录使用的Cookie里，明文保存着ID和密码。** 本系统里，为了下次访问的时候可以省略输入认证信息，设计了自动登录功能。为了实现这个功能使用的Cookie里明文保存了ID和密码。(参考另附图3) 因此，如果存在XSS漏洞等问题的话，存在认证信息被诈取的风险。另外，因为登录页面的通信没有加密(HTTP方式)，如果被侦听的话，可能遭到泄露。	请修改自动登录的功能。Cookie里不要包含认证信息，而是包含随机值。 另外，请不要发行不需要的Cookie。同时，关于此功能请对用户加以提醒。

序号	指摘事项	危险度	难易度	说明	建议
5	Cookie设置的不完备	中	难	**<u>没有对Cookie的安全进行设置，被Session攻击的可能性较高。</u>** 本系统发行的Cookie，在以下的安全问题上没有设置。(参考另附图4) **<u>1.没有设置安全属性(危险度:中)</u>** 没有对Session管理用的Cookie设置安全属性，浏览器非加密状态下(HTTP)也发送Cookie。用户非加密(http)访问URL时，攻击者侦听网络的情况下，存在被诈取Cookie里包含的SessionID，被Session攻击的风险。 **<u>2.路径为服务器全体(危险度:低)</u>** Session管理用的Cookie的请求路径为“/”，请求服务器全体里包含了Cookie。同一个服务器运行多个系统的情况下，因为其他系统的漏洞(XSS漏洞等)，可能会导致Cookie信息泄露。 **<u>3.没有设置HttpOnly属性(危险度:参考)</u>** 没有对Session管理用的Cookie设置HttpOnly属性，本系统存在XSS漏洞的情况下，存在Cookie里包含的SessionID被诈取，被Session攻击的风险。	只使用SSL通信发行Cookie的情况下，请设置安全属性。 Cookie的路径等也要设置最低的权限。 追加HttpOnly属性。
6	服务器上配置了测试页	低	难	**<u>服务器上配置了PHP的测试页。</u>** 服务器上运行着用来确认PHP是否正常运行用的程序(phpinfo.php)。使用产品的版本、设置信息遭到泄露。(参考另附图5)	请删除该文件。
7	可以同时并行登录	参考	-	**<u>一个账户，可以在两个不同的终端同时登录，并且可以进行各种各样的操作。</u>** 如果允许一个账户，在多个环境下可以同时登录的话，被第三者伪装的情况下，会使合法用户和第三者的访问记录混在一起。因此，通过日志审计来追查证据的话就会变得没有价值。(参考附录图6)	推荐禁止用户同时并行登录。

序号	指摘事项	危险度	难易度	说明	建议
8	没有显示最终访问历史	参考	-	**登录时最终访问历史等没有显示。** 登录时最终登录的时间等最终登录历史没有显示。登录后，通过显示上次登录的时间或者操作内容等，可以起到能够发现是否被第三者伪装过的效果。	从安全的观点出发，推荐显示最后登录的时间。

危险度	
高	没有权限的用户伪装成合法用户执行事务，查看重要的个人信息，危险性较高的，需要解决对策的漏洞。
中	概率较低，需要多个条件同时具备才会发生像上面所述的重大问题。希望在系统变更等适当的时机修改的指摘事项。
低	不可以直接攻击，只是可以取得主机或是网络设备相关信息等，在安全级别上不值得指摘的事项。
参考	不一定是安全上的问题，但是慎重起见还是要告知对方的指摘事项。

攻击难易度	
易	浏览器等常用的应用程序或者是网上公开的工具，不需要专业知识的攻击者都可以恶意使用的漏洞。
中	一般不怎么知道的命令，需要改造网上公开的工具，需要高级技巧，专业知识的漏洞。
难	需要在通信网络上外挂窃听程序，甚至以及知道用户的密码的前期下，需要昂贵的专业设备，需要大量资金，大量人力的漏洞。