

公告

【公告】SRC行业安全测试规范

由 Pa0er 于 2019-11-08 11:12:03 发表

SRC行业安全测试规范

参与此标准制定的组织:

小米SRC、蚂蚁金服SRC、ASRC、阿里云先知、菜鸟SRC、本地生活SRC、同舟共测-企业安全响应联盟、腾讯SRC、百度SRC、360SRC、小米SRC、滴滴SRC、苏宁SRC、唯品会SRC、微博SRC、美丽联合SRC、网易SRC、VIPKID SRC、WiFi万能钥匙SRC、完美世界SRC、京东SRC、vivoSRC、爱奇艺SRC、陌陌src。

感谢以下白帽子对此规范提供的建议和认可:

hackbar、SToNe、无心、、mmmark、ayound、算命先生、泳少、离兮、lakes、Adam、羽_、小笼包（随机排名，不分先后）

一、测试规范:

1、注入漏洞，只要证明可以读取数据就行，严禁读取表内数据。对于UPDATE、DELETE、INSERT等注入类型，不允许使用自动化工具进行测试。

2、越权漏洞，越权读取的时候，能读取到的真实数据不超过5组，严禁进行批量读取。

3、帐号可注册的情况下，只允许用自己的2个帐号验证漏洞效果，不要涉及线上正常用户的帐号，越权增删改，请使用自己测试帐号进行。

帐号不可注册的情况下，如果获取到该系统的账密并验证成功，如需进一步安全测试，请咨询管理员(或发邮件到 security@xiaomi.com)得到同意后进行测试。

4、存储xss漏洞，正确的方法是插入不影响他人的测试payload，严禁弹窗，推荐使用console.log，再通过自己的另一个帐号进行验证，提供截图证明。对于盲打类xss，仅允许外带domain信息。所有xss测试，测试之后需删除插入数据，如不能删除，请在漏洞报告中备注插入点。

5、如果可以shell或者命令执行的，推荐上传一个文本证明，如纯文本的1.php、1.jsp等证明问题存在即可，禁止下载和读取服务器上任何源代码文件和敏感文件，不要执行删除、写入命令，如果是上传的webshell，请注明shell文件地址和连接口令。

6、在测试未限制发送短信或邮件次数等扫号类漏洞，测试成功的数量不超过50个。如果用户可以感知，例如会给用户发送登陆提醒短信，则不允许对他人真实手机号进行测试。

7、如需要进行具有自动传播和扩散能力漏洞的测试（如社交蠕虫的测试），只允许使用和其他账号隔离的小号进行测试。不要使用有社交关系的账号，防止蠕虫扩散。

8、禁止对网站后台和部分私密项目使用扫描器。

9、除特别获准的情况下，严禁与漏洞无关的社工，严禁进行内网渗透。

10、禁止进行可能引起业务异常运行的测试，例如：IIS的拒绝服务等可导致拒绝服务的漏洞测试以及DDOS攻击。

- 11、请不要对未授权厂商、未分配给自己的项目、超出测试范围的列表进行漏洞挖掘，可与管理员联系(或发邮件到 security@xiaomi.com)确认是否属于资产范围后进行挖掘，否则未授权的法律风险将由漏洞挖掘者自己承担。
- 12、禁止拖库、随意大量增删改他人信息，禁止可对服务稳定性造成影响的扫描、使用漏洞进行黑灰产行为等恶意行为。
- 13、敏感信息的泄漏会对用户、厂商及上报者都产生较大风险，禁止保存和传播和业务相关的敏感数据，包括但不限于业务服务器以及Github 等平台泄露的源代码、运营数据、用户资料等，若存在不知情的下载行为，需及时说明和删除。
- 14、尊重《中华人民共和国网络安全法》的相关规定。禁止一切以漏洞测试为借口，利用安全漏洞进行破坏、损害用户利益的行为，包括但不限于威胁、恐吓SRC要公开漏洞或数据，请不要在任何情况下泄露漏洞测试过程中所获知的任何信息，漏洞信息对第三方披露请先联系SRC获得授权。企业将对违法违规者保留采取进一步法律行动的权利。

以下是小米针对违反测试规范的处罚措施：

- 1、对于干扰业务等违规测试的行为（包括但不限于“一、测试规范”），
 - A. 在MiSRC 违反一次，视情节严重程度：较轻者，警告处理；严重者，取消MiSRC 所有奖励（包括荣誉奖励）；
 - B. 在MiSRC 违反第二次，无论情节轻重，取消MiSRC 所有奖励（包括荣誉奖励）
- 2、如触犯测试规范第 14 条，将取消MiSRC 所有奖励（包括荣誉奖励）同时，我们将保留法律追责权力。

— 联系我们 —



专用邮箱



新浪微博



公众号

小米网|MIUI|米聊|多看书城|小米路由器|视频电话|小米后院|小米天猫店|小米淘宝直营店|小米网盟|问题反馈
©mi.com 京ICP证110507号 京ICP备10046444号 京公网安备11010802020134号 京网文[2014]0059-0009号
违法和不良信息举报电话：185-0130-1238

