安全小课堂第四十四期 【在线验证码的安全隐患】

京东安全应急响应中心 2017-02-10

 亲，戳上面的**蓝字**关注我们哦！

安全小课堂第四十四期——在线验证码的安全隐患

关于在线验证码大家一定不陌生，尤其是才经历了春运，12306作为中国交通枢纽最重要的网站见证了我国互联网在线验证码的技术变革。经过了本期的安全小课堂讨论，京安小妹发现原来看似简单的验证码也有那么多不简单的技术。感谢本期的讲师简单师傅的分享，以及 JSRC 白帽子Ant ， 抓的住的小伙 ， 苦逼司马，恋锋，ziwen，feng的补充。

简单：JSRC白帽子，网安全从业人员，安全经验4年，程序员开发安全经验6年，主要靠自学。现任京东安全高级安全工程师。

 京安小妹

简单师傅，你能从网络安全角度出发描述一下在线验证码的作用吗？

简单 

验证码，百度描述的信息是：（全自动区分计算机和人类的图灵测试）的缩写，是一种

区分用户是计算机还是人的公共全自动程序。

根据我近年来在网络安全方面与验证码有关的经验，验证码可以有效防止 防数据爬取 、防黄牛刷单 、 防垃圾注册 、 防恶意登录 、 防支付欺诈 、 防投票作弊.

但是，验证码也会被绕过导致验证码的作用失效。

京安小妹

那验证码实现的原理呢?

简单 

简单来说就是用户在客户端（浏览器）中输入字符，服务器端校验。校验成功后，判断当前输入的字符是否与服务器端生成的图片的字符相同，

校验通过后，可以执行下一步的操作，如：下订单，登录操作，修改密码等。

在历年来的 验证码中，实现方式多数是，服务器端随机生成了 随机数，通过绘图，添加干扰点，干扰线等方法，输出到 页面中。

京安小妹

验证码从最初的设计到现在经历了怎样的发展呢?

简单 

个人认为在线验证码的发展历程如下:

验证码1.0版本： 纯数字 或者 纯英文 （4-5）位字符验证.

验证码1.5版本：在纯数字 与英文的基础上，增加了计算运算符号。

验证码2.0版本：在纯数字与英文基础上，增加了运算功能，又增加了干扰线，干扰框。不能被轻易识别破解。

3.0版本，使用当前互联网 大家熟知的 图片对比方式。如12306使用的 就是 类似 点触科技的一套。识图功能. 其实 现在还有比较流行的，就是 验证码滑块验证。

京安小妹

做出这样的升级是因为之前的验证码容易被绕过么？

简单 

是的。而且被绕过后危害还是很大。

比如之前我曾任职的 某游戏公司，就是因为验证码被轻易识别，导致每天的账号破解数据每天在千万次数。由于识别成本较低，在淘宝上，200元就能针对 指定的验证码，进行 开发 专业的 识别插件。识别成功率可达 98.37% 。

京安小妹

那些插件的原理是什么呢？怎么绕过验证码的呢？

简单 

第1.0-2.0版本的破解成本比较低，将验证码图片保存到本地，将图片中的字符进行拆

分，将干扰点与干扰线进行屏蔽。 最终识别 图片中的单个字符。

在线验证码 3.0 不过就是在 后端，接入了3方。3方将算法，行为识别等情况 保存在后端服务器上。当同一IP，多次提交，会被识别为 恶意行为。这个时候只需要破解了第三方的算法再模拟算法，就能破解3.0验证码。这种破解方案已有人实现。

还有种方案是将出现的图片全部归类，收集整理，并按照分类存放，在发现图片后，进行数据图片对比，根据服务器要求的 分类，去做数据对比。将对比结果存在的，进行选中，则视为已经识别。相当于考试前先刷题，然后考试考到了哪一道就直接写答案。

京安小妹

之前有白帽子留言说基于谷歌识图破解验证码这种方案可行吗?

简单

其实可以，不过 这种破解成本太高了，首先 ，你要能访问谷歌。

把谷歌换成百度，效果会比较差，百度识图与谷歌识图还有一定的差距。

并且识图程序无法保证输出的内容与原图信息高保真。

京安小妹

针对在线验证码被破解，有什么补救措施么?

简单

1、针对验证码容易被绕过，现在比较常见的补救措施是双因子验证。也就是除了单纯的

验证码 + 客户的密码， 还要检测是否为常用设备，等多种因素集成的验证。如银行，现在 都是 输入密码 + 短信验证码. 多种情况加在一起，只是为了验证 这个账号属于你。

双因子验证主要是依赖个人的密码与固件信息：如令牌，指纹，手机，等情况 进行用户认证。

2、识别 浏览器的UA标识，如果发现不是浏览器，则不予通过。

3、增加了 单IP请求次数限制，发现单一IP请求次数过多，会封IP等情况。

京安小妹

简单师傅还有其他什么需要补充么？

简单

1、由于验证码的多样性，对于企业甲方与客户、用户是一竞争关系。所以现很多情况并不是直接出现验证码，而是让用户输入3-5次，后出现验证码。

2、现在已经出现了语音验证码，例如谷歌找回密码，就可以选择短信验证码或者语音验证码，选择语音验证码后会接到一个 电话验证码信息就在语音中，再讲验证码提交即可通过验证。

白帽子观点：美团、饿了么现在就使用了语音验证码。

3、还有古老的验证码过期的问题：同一个验证码 ，可以多次执行请求，导致被验证码被绕过。比如，一个四位数的验证码，服务器针对验证码没有做请求次数验证，1万次就能破出来了，用程序来实现也就1分钟，而6位数的验证码时间也就10分钟左右。

针对这种情况，企业可以在后端加入限制，例如一个验证码只允许尝试3次，3次错误后就换其他的验证码，不过这虽然能提高了攻击的难度但也增加了企业的成本。

4、有些在线验证码的问题没有设置1次失效，导致验证码失去原有的作用。比如一个post请求，账号密码+图片验证码，1个验证码可以使用N次，然后就可以进行撞库或者爆破了

这种问题的解决方案是限制错误次数、以及设置合理的短信验证码过期时间都可以防止爆破。

白帽子观点：市面上有种专业验证刷单团队，他们采用人工形式，输入一个正确的验证码给予多少钱的形式成功的绕过了各种验证机制。这种方式的绕过就暂时就没有解决方案了。

白帽子观点：现在这种团队已经很健全了。

白帽子观点：看似很安全的拼图验证码和滑动验证码也有被绕过的风险。
拼图验证码典型的例子是极验 ，极验的问题在于验证码底图相同，只是变化的地， 也就是缺失的块不同，而我们只需要稍微注册个极验api 收集全部底图 做自动化对比就可以破解，底图我上次看的时候才几十个，以后慢慢增加 可以增加破解难度 但没有本质上改变可以被破解的事实。
滑块验证码验证码的算法是计算你滑动的时间和速度，只有y轴的一个滑块从左滑到右。写一个很简单的机器学习模拟人滑动验证码的行为，然后学习一百组不同的真人滑动验证的例子 来进行破解，这个机器学习大概是学习一般人在什么地方会产生抖动 什么地方是匀速 平均速度是多少然后在平均速度区间取随机指进行破解。

最后，**小课堂持续征集讲师**，只要你在网络安全领域对有所擅长、有自己的见解、或者只是纯粹想跟大家分享个0day，都欢迎自荐成为安全小课堂讲师。

作为安全小课堂的讲师，不仅能享受分享知识的成就感与荣誉，而且通过与大家的讨论也有利于自己对知识进行梳理，完善自己的知识体系。当然，JSRC的日常福利是少不了的。

如果还有你希望出现在安全小课堂内容暂时未出现，也欢迎留言告诉我们。

安全小课堂的往期内容开通了自助查询，查询方式请点击阅读原文查看。

微信公众号：jsrc_team
新浪官方微博：京东安全应急响应中心

阅读原文