自动化测试验证码解决方案

http://www.uml.org.cn/Test/200709134.asp

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **技术性方法** | | **非技术性方法** | |
|  | **识别法** | **服务端插入法** | **屏蔽法** | **后门法** |
| **优点** | 不需要修改代码，也不需要在代码中增加额外的接口和后门，在服务端代码不可接触到的情况下，是唯一的选择 | 理论上来说可以解决任何验证码的问题，而且不需要修改已有的服务端代码 | 简单修改现有代码就能让自动测试顺利进行，开销小 | 实现方式不复杂，对现有代码改动小，安全性相对有保证 |
| **缺点** | 存在技术限制，只能对相对简单的验证码图片进行分析识别，对复杂的图片无法进行识别 | 存在一定的安全隐患，如果被攻击者获知测试接口，验证码就会失去作用 | 存在很大的安全问题，对于未上线应用还可应用，对于已上线的实际应用，该方法不可行；况且，由于该方法需要对代码修改的内容太多，导致发布时可能发生某些验证码被不正确屏蔽的情况 | 如果被攻击者探测得到万能验证码，则验证码会失去作用 |
| **适用场合** | <!--[if !supportLists]-->1、  <!--[endif]-->服务端代码不可接触到或是不可进行任何修改  <!--[if !supportLists]-->2、  <!--[endif]-->验证码采用xbm等较简单的方式实现 | 未上线系统，或是在测试条件下安全性要求不是特别高的系统； | 开发阶段，未实际上线的系统 | 可在实际应用系统上应用 |
| **应用建议** | 纯粹的客户端识别解决方案成本较高，建议主要采用服务端方式实现 | 在管理上需要增加对测试接口的管理，系统在发布时需要保证去掉测试接口 | 在发布管理时，一定要有合理的方案保证发布时所有被屏蔽的验证码能够得到恢复 | 为了保证上线系统的安全，该方法一般需要结合密码管理方法使用，通过定期更换万能验证码、控制其知晓范围等手段保证安全 |