安全测试思路以及实现过程。

时间关系，重点讲三个漏洞。命令注入/执行，跨站请求伪造，上传漏洞。

[http://127.0.0.0:60080/](http://124.250.31.122:60080/)

1. 命令注入

127.0.0.1

127.0.0.1;ifconfig. && |

场景：一个调用系统命令实现的功能。

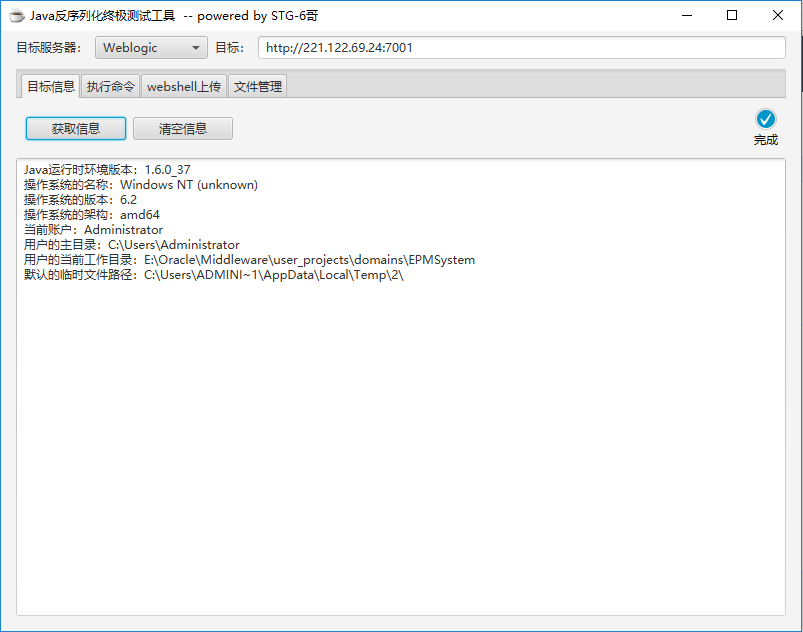
原理：功能实现调用了系统命令，参数没有限制与处理，当传入参数为系统/编程语言命令的时候，程序将命令执行。

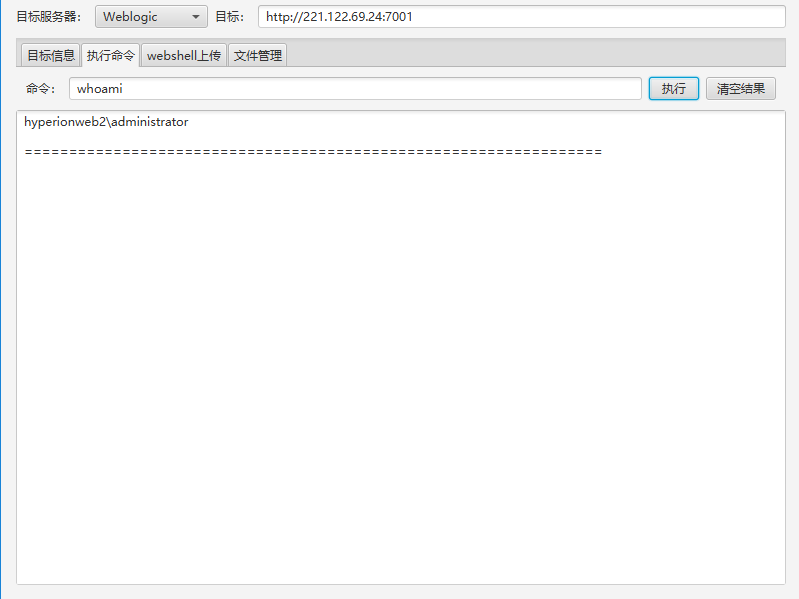
测试方法：输入系统命令或功能函数

Reboot /rm –rf / wget ‘挖矿’

防御：发现异常字符直接返回异常，不进行处理。

'&'    
';'    
'|'   
'-'    
'$'    
'('    
')'    
'`'    
'||'





1. 跨站请求伪造

Low: http://47.52.233.199/csrflow.html

漏洞位置：用户改密，添加关注等功能。

原理：请求参数是固定的。

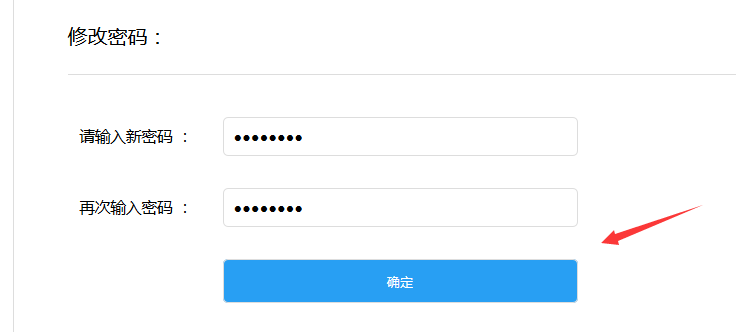
攻击场景：恶意链接或页面放到博客论坛等让你访问。

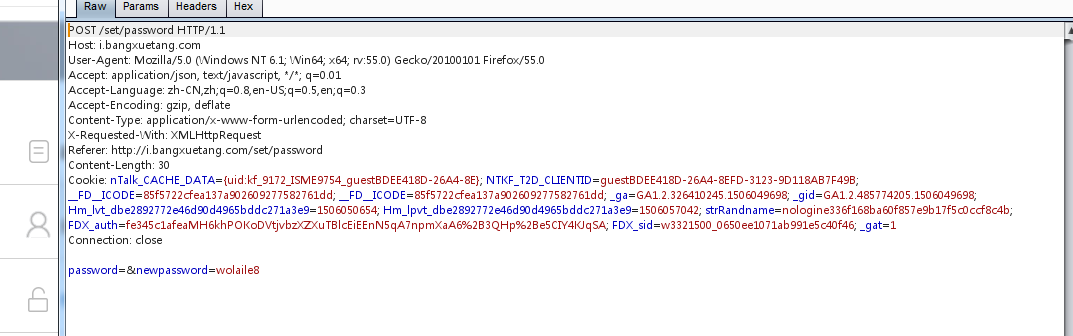
访问地址的原因： 社工。

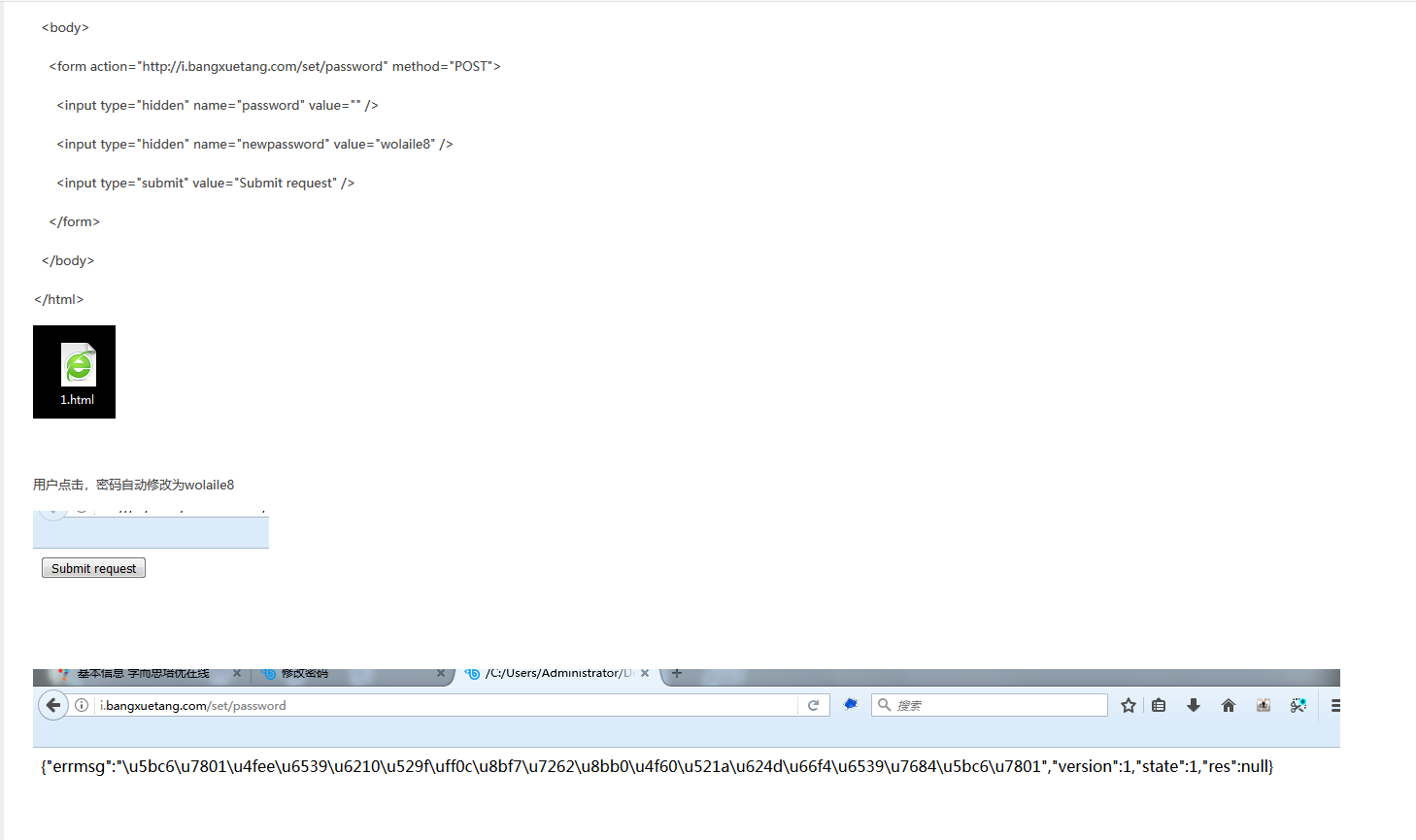
测试方法：观察功能实现参数是否固定

防御：二次校验，不固定变量。

下面是 业务发现的CSRF的例子。







1. 文件上传

漏洞场景：上传功能

原理： 上传没有限制文件类型，可以上传脚本文件

测试方法：上传脚本文件

防御：服务器后端限制文件类型。

下面是一个上传漏洞。