**技术分析**

**漏洞分析**

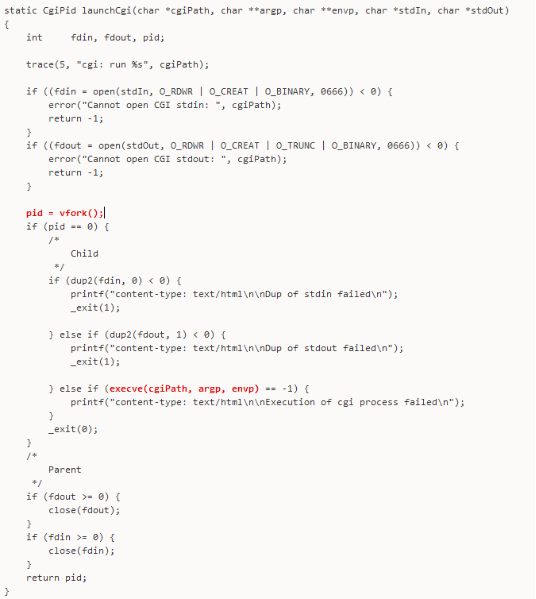
GoAhead的cgi程序在处理HTTP请求时，没有正确过滤参数，可被注入变量LD\_PRELOAD，导致远程命令执行。

goahead/src/cgi.c的cgihandler函数用于处理HTTP请求。



它会从HTTP请求的参数中提取出key-value值，代入envp数组中，作为环境变量，传递给launchCgi函数，执行cgi程序。

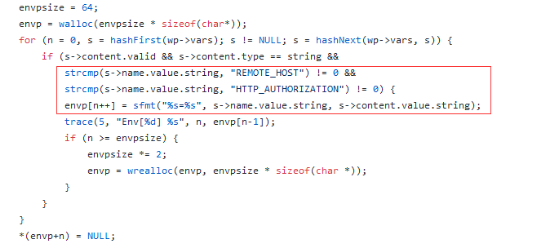
launchCgi函数中通过 execve 将之前传入的环境变量作为cgi程序的环境变量执行。



而我们知道在linux中是可以通过LD\_PRELOAD环境变量来hook，劫持函数的执行流。

在函数中可以看到只对 REMOTE\_HOST 和 HTTP\_AUTHORIZATION进行了过滤，对其他变量并没有过滤。

通过“ envp[n++] = sfmt(“%s=%s”, s->name.value.string, s->content.value.string); ”直接把HTTP请求中的参数赋值给了envp数组，而后面envp数组直接作为了cgi程序执行时的环境变量。



因此，通过恶意的HTTP请求可以让goahead的cgi程序加载执行指定的so库文件。