Metinfo 6.\* 全版本存储型XSS

Exp:

[http://127.0.0.1/admin/login/login\_check.php?url\_array[]=123&url\_array[]=123&url\_array[]=aa%22+autofocus+onfocus=alert(2)+a=%0a%0ba=&url\_array[]=123](http://127.0.0.1/admin/login/login_check.php?url_array%5b%5d=123&url_array%5b%5d=123&url_array%5b%5d=aa%22+autofocus+onfocus=alert(2)+a=%0a%0ba=&url_array%5b%5d=123)

影响版本:

6.0.0

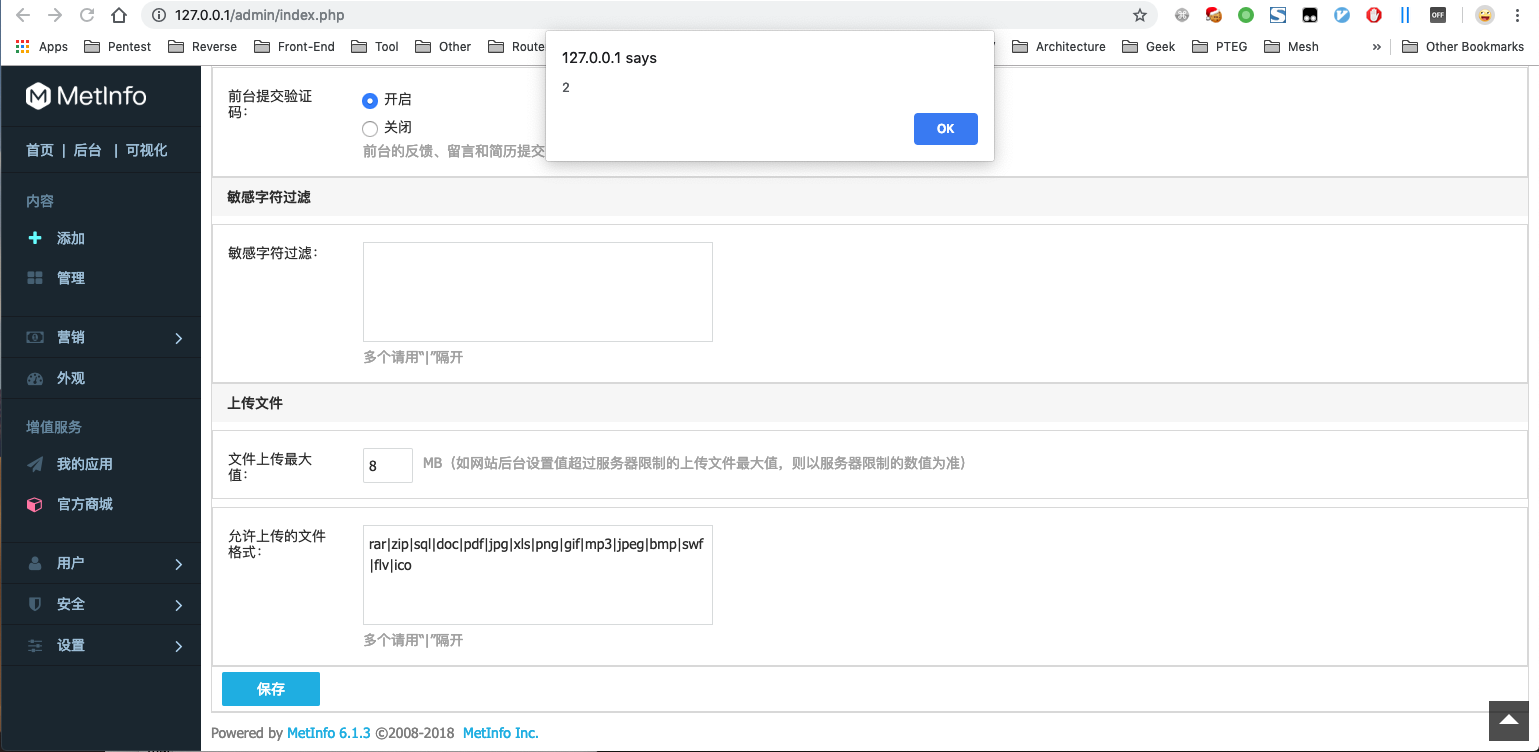
6.1.0

6.1.1

6.1.2

6.1.3

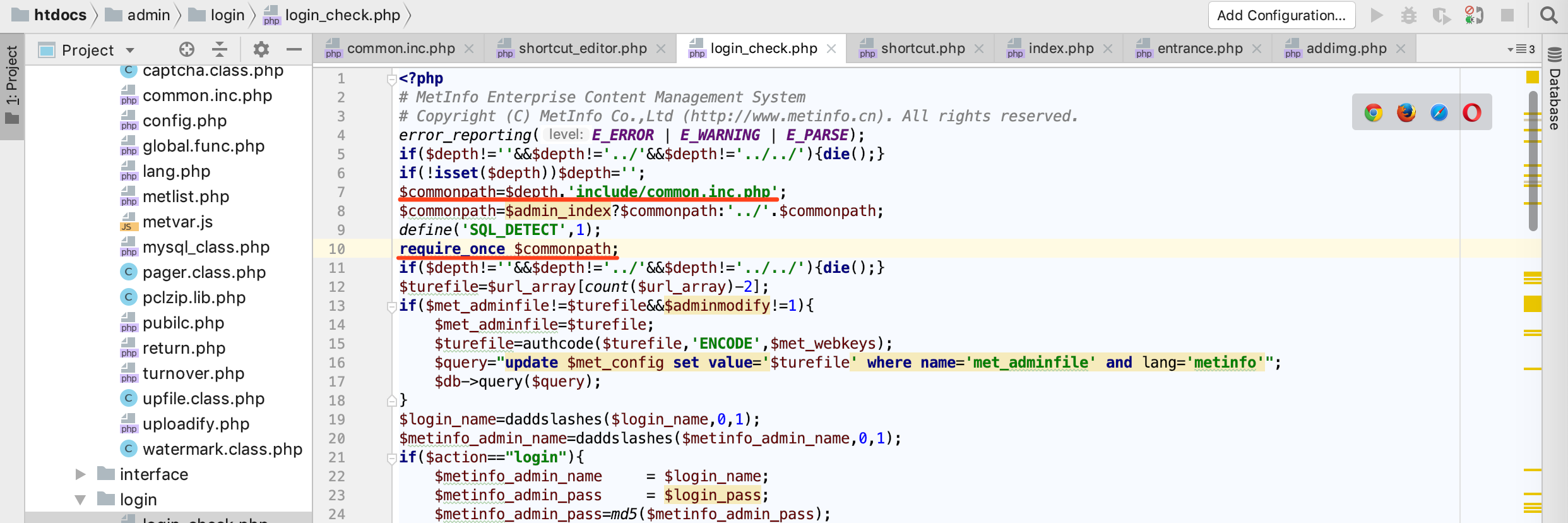
无需登录，访问上述链接可以在后台直接X。当管理登录后台时，切换到“安全与效率”界面，XSS可自动触发。



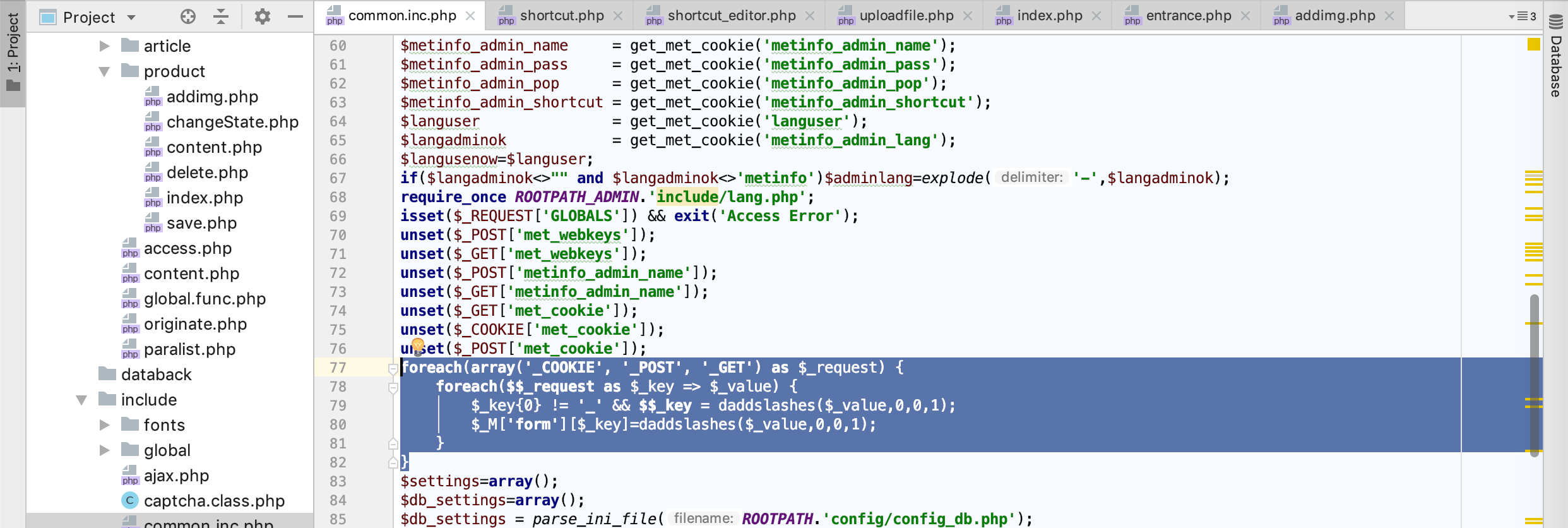
漏洞分析，以6.1.3(<https://www.metinfo.cn/upload/file/MetInfo6.1.3.zip)> 为例:

admin/login/login\_check.php

此处加载了 /admin/include/common.inc.php

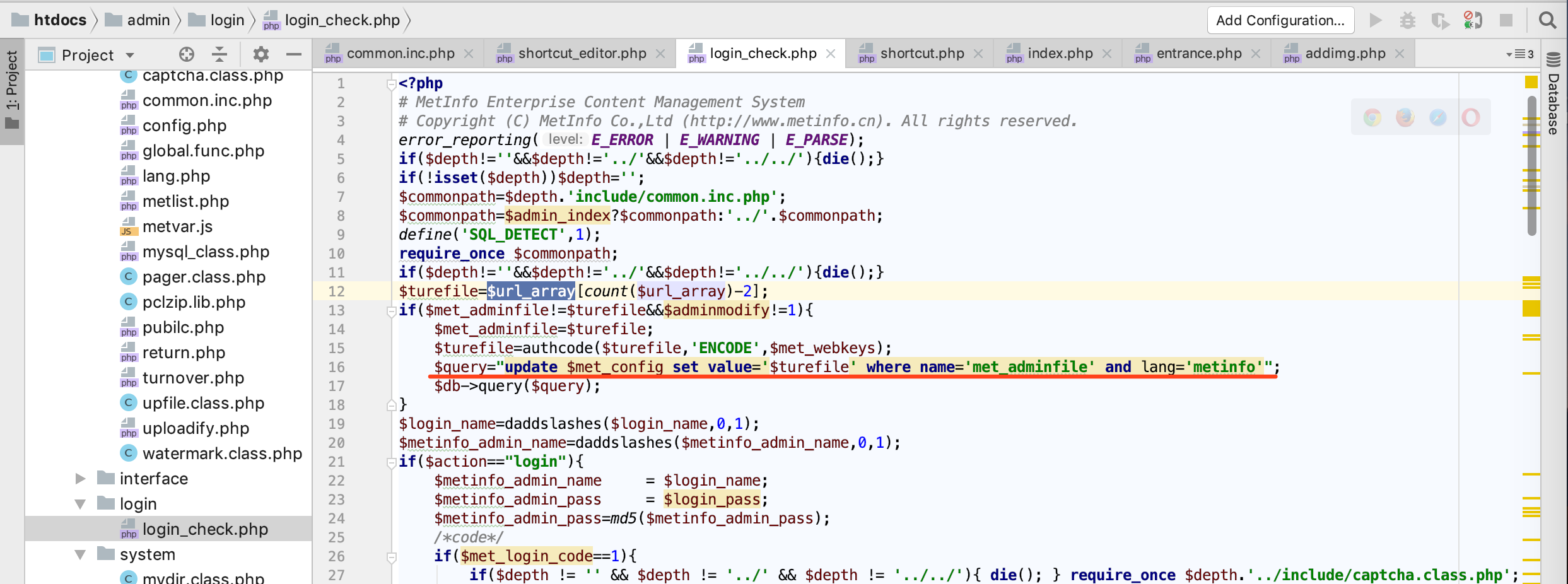


admin/include/common.inc.php



此处变量可以实现变量覆盖。

因此可以覆盖$url\_array变量



其中authcode 为其加解密算法。

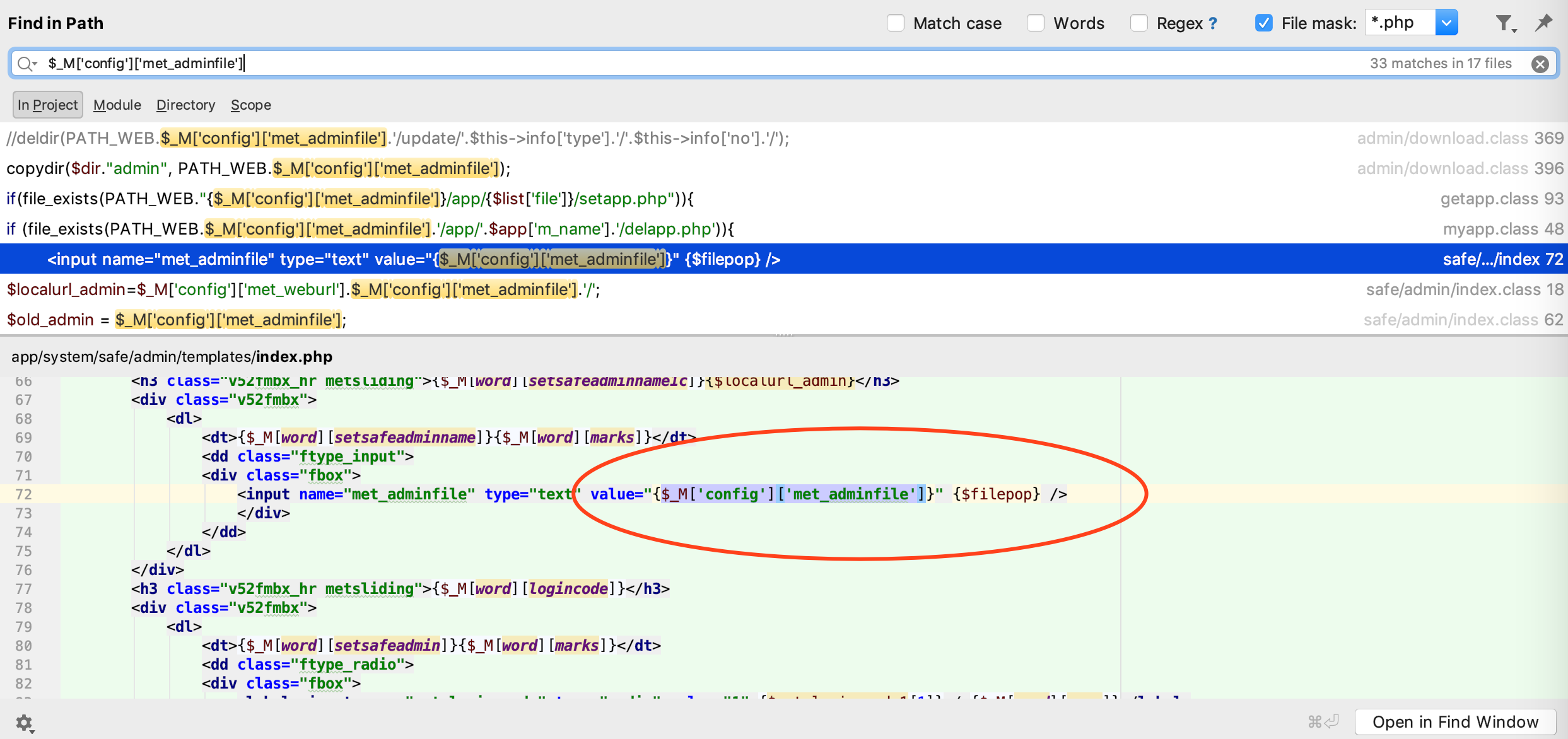
管理员正常登录后，该值会被取出并解密

app/system/include/class/common.class.php



最终直接输出在

app/system/safe/admin/templates/index.php



最终：

