奇安信攻防社区 – 对 SEMCMS 再一次审计

奇安信攻防社区 – 对 SEMCMS 再一次审计

前言 最近在社区看文章的时候, 发现了这一篇文章: https://forum.butian.net/share/291 感觉应该还有洞, 所以通读了下代码, 所以有了这篇文章。 # sql 注入 1 在 / Include/web_inc.php 中我们可以...

最近在社区看文章的时候, 发现了这一篇文章: https://forum.butian.net/share/291 (https://forum.butian.net/share/291) 感觉应该还有洞, 所以通读了下代码, 所以有了这篇文章。

在 / Include/web_inc.php 中我们可以发现这一串代码:

(https://shs3.b.qianxin.com/attack_forum/2021/07/attach-d3729ad17b26ba16c2840d2533b840f953bb654a.png)
我们可以看到先让 `$web_urls` 接收 `$_SERVER["REQUEST_URI"]` 的值, 然后分割后, 传进 `web_language_ml` 函数中, 所以继续跟进该函数:

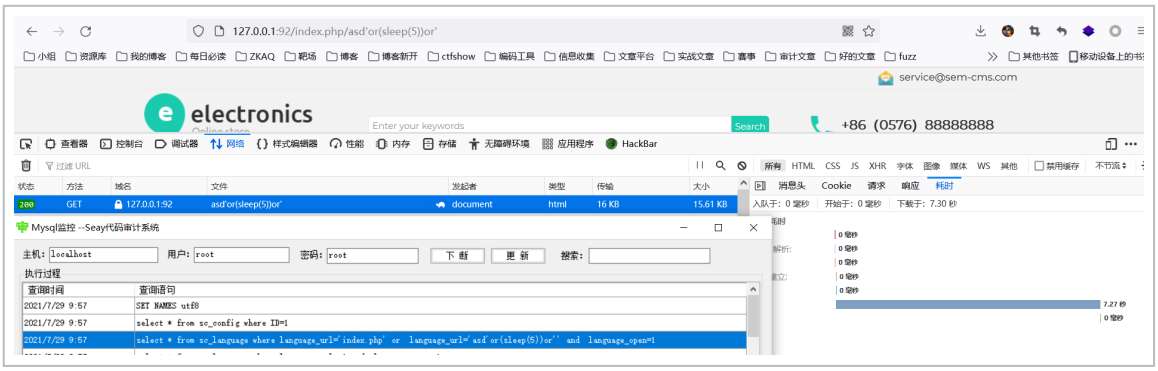
```
        $query=$db_conn->query("select * from sc_language where language_mulu=1 and  language_open=1");
        $row=mysqli_fetch_assoc($query);
        $Urlink=array('url_link'=>"",'url_ml'=>"./",'ID'=>$row['ID']);

    }

return $Urlink;
}
```

(https://shs3.b.qianxin.com/attack_forum/2021/07/attach-cb3a717950ed93a132e5012107cb464e4a3a6eb0.png)

很明显的 sql 注入, 而且是用 `$_SERVER["REQUEST_URI"]` 接收值, 而代码只过滤了传入的参数, 对这个是没有对其过滤, 所以直接注入就 ok 了



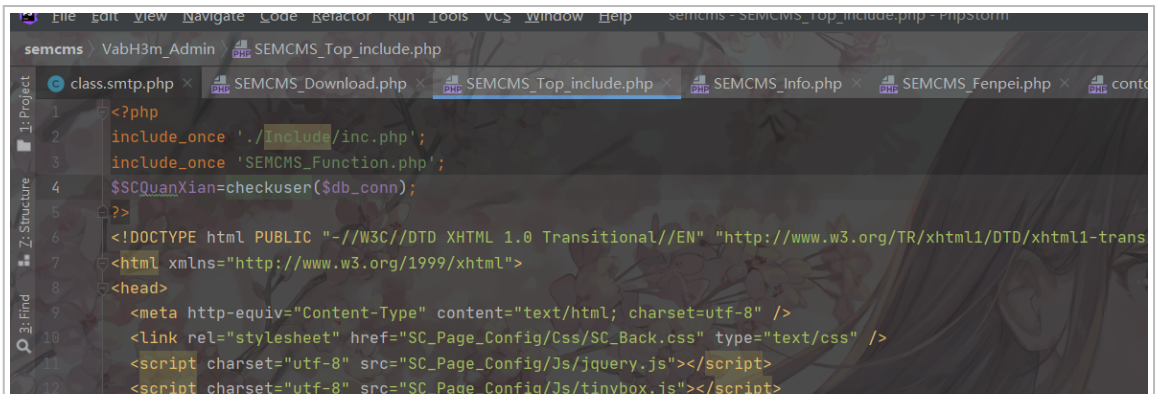
(https://shs3.b.qianxin.com/attack_forum/2021/07/attach-33dcec87919320ed09bb7a13e76fa42d6099e04e.png)

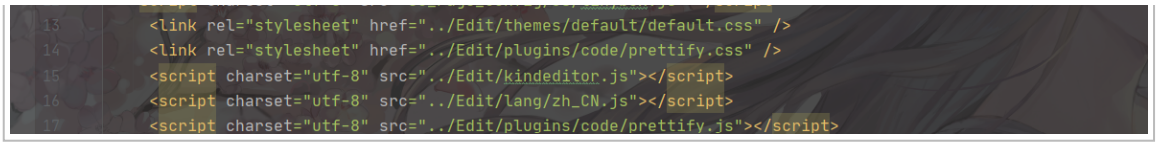
这里用的是时间盲注, 但是 `$_SERVER["REQUEST_URI"]` 接收值不会解码, 所以空格要简单的绕过一下, 不然传入的就是 %20, 后面的注释直接 `or'` 就好了!

如果想要访问后台的文件, 其所有文件都存在这段代码:

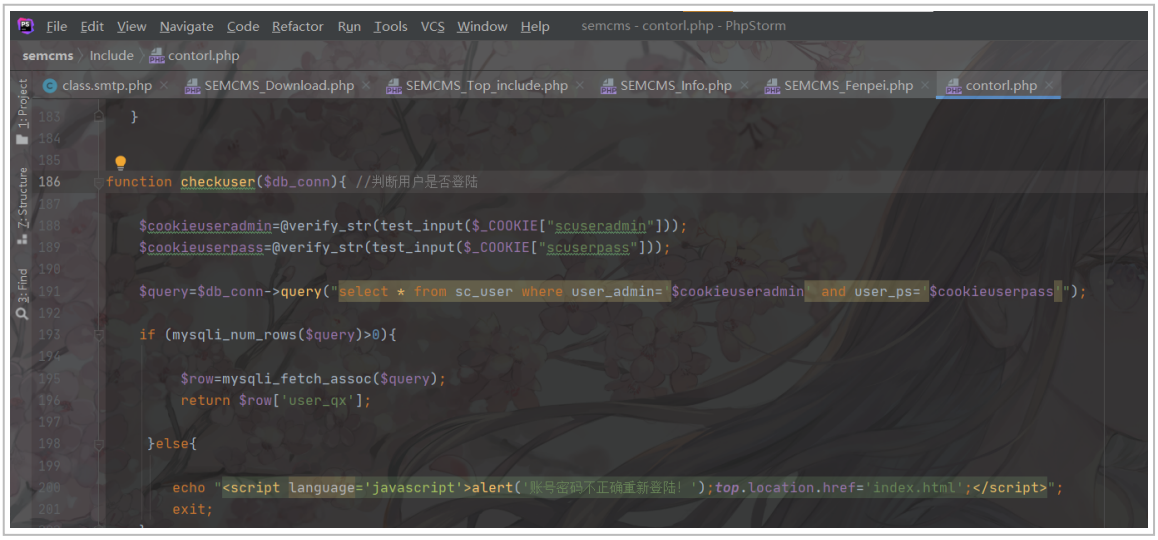
```
<?php include_once 'SEMCMS_Top_include.php'; ?>
```

所以跟进查看, 发现内容是:





(https://shs3.b.qianxin.com/attack_forum/2021/07/attach-f43efefd8357c218116fc5ae5b6762299ff421c1.png)
发现会使用 `checkuser()` 函数来进行判断, 所以继续跟进:



(https://shs3.b.qianxin.com/attack_forum/2021/07/attach-35d088a06988a9829a8fdcfebe5e33c9621d1ec9.png)
发现它是通过使用 cookie 中的值, 方入 sql 中进行执行, 这里先把 `verify_str` , `test_input` 两个函数的过滤内容奉上:
test_input:

```
function test_input($data) {
```

verify_str:

```
$data = str_replace("%", "percent", $data);
```

inject_check_sql:

```
$data = trim($data);
```

可以看到, 过滤了很多东西, 正常的 sql 注入似乎没办法搞, 但是, 这里是想要登录后台, 所以我们完全可以不用注入得到密码, 可以直接想办法构造使该 sql 语句正确就好了, 所以这里的想法是构造出 `'xxx' or 1=1` 这种形式, 所以直接上 payload:

```
$data = stripslashes($data);
```

(https://shs3.b.qianxin.com/attack_forum/2021/07/attach-d8390ab05e3d555050f6be0a89ba7a90e89f8837.png)

这个 cms 感觉漏洞挺多的, 最近有些事, 没看完, 有兴趣的小伙伴可以全篇通读一下, 不出意外还能找到一些洞...