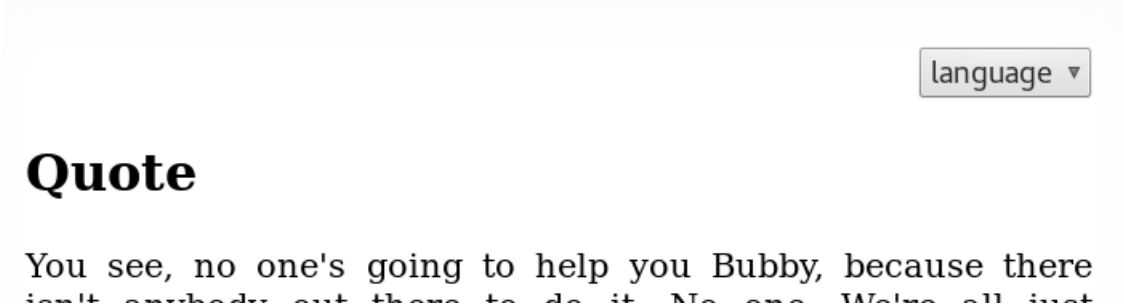
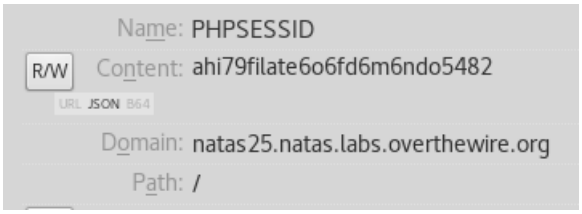
Natas Wargame Level25 Writeup(头部注入+POST/GET注入)

转载

a_18067 于 2017-05-20 22:05:00 发布 57 收藏
文章标签： php
原文链接：http://www.cnblogs.com/liqiuhao/p/6883356.html





sourcecode核心代码：

```php
<?php
    // cheers and <3 to malvina
    // - morla

    function setLanguage(){
        /* language setup */
        if(array_key_exists("lang",$_REQUEST))
            if(safeinclude("language/" . $_REQUEST["lang"] ))
                return 1;
        safeinclude("language/en");
    }

    function safeinclude($filename){
        // check for directory traversal
        if(strstr($filename,"../")){
            logRequest("Directory traversal attempt! fixing request.");
            $filename=str_replace("../","",$filename);
        }
        // dont let ppl steal our passwords
        if(strstr($filename,"natas_webpass")){
            logRequest("Illegal file access detected! Aborting!");
            exit(-1);
        }
        // add more checks...

        if (file_exists($filename)) {
            include($filename);
            return 1;
        }
        return 0;
    }
```

```
    }

    function listFiles($path){
        $listoffiles=array();
        if ($handle = opendir($path))
            while (false !== ($file = readdir($handle)))
                if ($file != "." && $file != "..")
                    $listoffiles[]=$file;

        closedir($handle);
        return $listoffiles;
    }

    function logRequest($message){
        $log="[". date("d.m.Y H::i:s",time()) ."]";
        $log=$log . " " . $_SERVER['HTTP_USER_AGENT'];
        $log=$log . " \"" . $message ."\"\n";
        $fd=fopen("/var/www/natas/natas25/logs/natas25_" . session_id() .".log","a");
        fwrite($fd,$log);
        fclose($fd);
    }
?>

<h1>natas25</h1>
<div id="content">
<div align="right">
<form>
<select name='lang' onchange='this.form.submit()'>
<option>language</option>
<?php foreach(listFiles("language/") as $f) echo "<option>$f</option>"; ?>
</select>
</form>
</div>

<?php
    session_start();
    setLanguage();

    echo "<h2>$__GREETING</h2>";
    echo "<p align=\"justify\">$__MSG";
    echo "<div align=\"right\"><h6>$__FOOTER</h6><div>";
?>
```

首先要将注入点分析清楚：一共有三个注入点

1.$_REQUEST["lang"] 即get/post注入

2.$_SERVER['HTTP_USER_AGENT'] http头部信息注入

3.session_id() cookie注入

23条注入能够发生的条件是safeinclude函数检测到了非法输入，而且必须是“../”这种非法输入，若是“web_pass”这种的话会直接exit(-1)。

这里第一条过滤非法输入语句存在漏洞，例如..././将../去掉后就变成了../，根本原因就在于没有使用while语句，没有想到过滤一次后依然（助攻）存在../，所以过滤应该持续检测直到非法字符不再出现。

第一条直接注入比较困难，原因在于即使用..././绕过了第一条检测，第二条检测也很难直接将"web_pass"下的密码给include进来，所以应该思考利用23两个注入，23两个注入必须触发“../”检测，随后logRequest($message)将信息写入/var/www/natas/natas25/logs/natas25_session_id().log。

很容易得到新思路，将“密码”或者能够显示密码的php语句写入到session_id().log之中，随后在safeinclude中将其include进来，由于这里是$_SERVER['HTTP_USER_AGENT']（通过字符串串联起来），所以没法执行命令做字符串替换，可以考虑写入php语句：

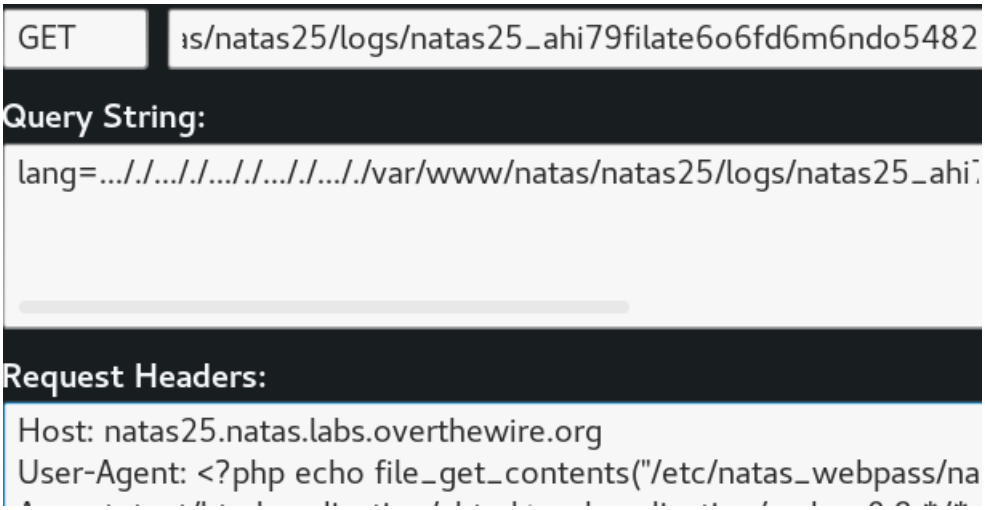
```
<?php echo file_get_contents("/etc/natas_webpass/natas26")?>
```

参考：http://php.net/manual/zh/function.file-get-contents.php

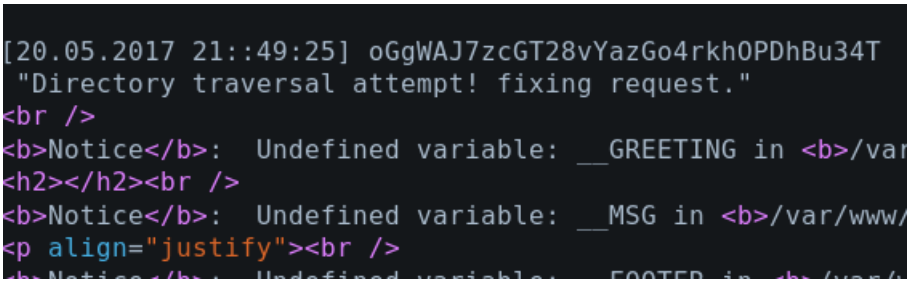
这样做以后，只要触发第一条过滤机制，密码就会在.log被include进来时显示，考虑如何即触发../又能够将.log包含进来：GET: lang=..././..././..././..././..././var/www/natas/natas25/logs/natas25_session_id().log即可

流程：GET输入触发第一次过滤，开始记录日志，headers中http-agent的php执行语句被记录到/var/www/natas/natas25/logs/natas25_session_id().log。同时输入被过滤为../../../../../var/www/natas/natas25/logs/natas25_session_id().log。file_exists()检测正确，将其include进来，触发php echo 语句，显示flag。

有两个地方需要注入，即get/post 和 headers。



注：如果想要注入session_id的话（虽然这没什么用。。），记得改cookie，Firefox里面发送http请求时会自动将headers中的cookie该回为真实的值。



总结：1.过滤机制一定要达到在任何情况下确定不包含非法字符（考虑周全）2.对用户的输入（不一定是真的“输入”，只要是用户传过来的信息）都要做防注入或过滤处理。3.做题的思路很重要，一是要注意过滤机制是否不够严格，而是碰壁后应该全局思考所有的注入点，只要是自己能篡改的信息都要思考能否注入，而且可能是多个注入点联合使用。

flag:**oGgWAJ7zcGT28vYazGo4rkhOPDhBu34T**

转载于:https://www.cnblogs.com/liqiuhao/p/6883356.html