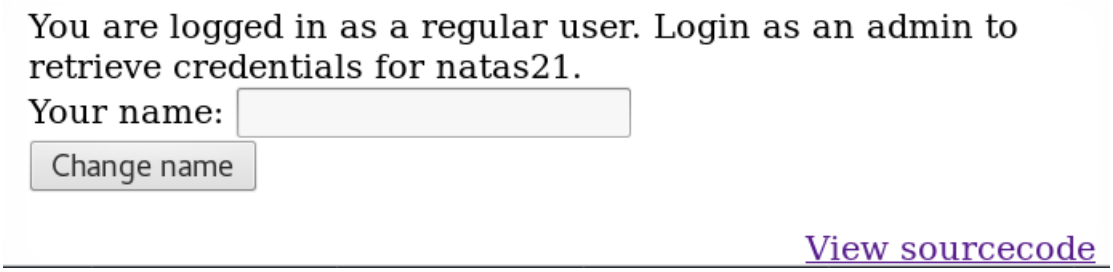
Natas Wargame Level20 Writeup（会话状态注入/篡改）

转载

a_18067 于 2017-05-20 14:35:00 发布 71 收藏
文章标签： php
原文链接：http://www.cnblogs.com/liqiuhao/p/6882068.html




```
<form action="index.php" method="POST">
  Your name:
  <input name="name" value=""></input>
  <br></br>
  <input value="Change name" type="submit"></input>
</form>
```

sourcecode核心代码：

```
<?

function debug($msg) {
    if(array_key_exists("debug", $_GET)) {
        print "DEBUG: $msg<br>";
    }
}

function print_credentials() {
    if($_SESSION and array_key_exists("admin", $_SESSION) and $_SESSION["admin"] == 1) {
    print "You are an admin. The credentials for the next level are:<br>";
    print "<pre>Username: natas21\n";
    print "Password: <censored></pre>";
    } else {
    print "You are logged in as a regular user. Login as an admin to retrieve credentials for natas21.";
    }
}


/* we don't need this */
function myopen($path, $name) {
    //debug("MYOPEN $path $name");
    return true;
}

/* we don't need this */
function myclose() {
    //debug("MYCLOSE");
    return true;
}

```

```php
function myread($sid) {
    debug("MYREAD $sid");
    if(strspn($sid, "1234567890qwertyuiopasdfghjklzxcvbnmQWERTYUIOPASDFGHJKLZXCVBNM-") != strlen($sid))
{
    debug("Invalid SID");
        return "";
    }
    $filename = session_save_path() . "/" . "mysess_" . $sid;
    if(!file_exists($filename)) {
        debug("Session file doesn't exist");
        return "";
    }
    debug("Reading from ". $filename);
    $data = file_get_contents($filename);
    $_SESSION = array();
    foreach(explode("\n", $data) as $line) {
        debug("Read [$line]");
    $parts = explode(" ", $line, 2);
    if($parts[0] != "") $_SESSION[$parts[0]] = $parts[1];
    }
    return session_encode();
}

function mywrite($sid, $data) {
    // $data contains the serialized version of $_SESSION
    // but our encoding is better
    debug("MYWRITE $sid $data");
    // make sure the sid is alnum only!!
    if(strspn($sid, "1234567890qwertyuiopasdfghjklzxcvbnmQWERTYUIOPASDFGHJKLZXCVBNM-") != strlen($sid))
{
    debug("Invalid SID");
        return;
    }
    $filename = session_save_path() . "/" . "mysess_" . $sid;
    $data = "";
    debug("Saving in ". $filename);
    ksort($_SESSION);
    foreach($_SESSION as $key => $value) {
        debug("$key => $value");
        $data .= "$key $value\n";
    }
    file_put_contents($filename, $data);
    chmod($filename, 0600);
}

/* we don't need this */
function mydestroy($sid) {
    //debug("MYDESTROY $sid");
    return true;
}
/* we don't need this */
function mygarbage($t) {
    //debug("MYGARBAGE $t");
    return true;
}

session_set_save_handler(
    "myopen",
    "myclose",
    "myread"
```

```
    "myread",
    "mywrite",
    "mydestroy",
    "mygarbage");
session_start();

if(array_key_exists("name", $_REQUEST)) {
    $_SESSION["name"] = $_REQUEST["name"];
    debug("Name set to " . $_REQUEST["name"]);
}

print_credentials();

$name = "";
if(array_key_exists("name", $_SESSION)) {
    $name = $_SESSION["name"];
}

?>

<form action="index.php" method="POST">
Your name: <input name="name" value="<?=$name?>"><br>
<input type="submit" value="Change name" />
</form>
```

关键部分已经用红色标出，mywrite和myread是两个管理会话状态的关键函数，以下是一些参考资料：

http://php.net/manual/zh/function.session-set-save-handler.php

http://php.net/manual/zh/function.strspn.php

http://www.w3school.com.cn/php/func_string_explode.asp

http://php.net/manual/zh/function.session-encode.php

简单来说，myread首先对sid（第一次由服务器自动生成并保存在cookie中）进行校验，若非字母/数字则不返回会话状态。

若sid合法，则进入相关目录寻找/读取文件，若是老的会话/文件已经删除会新建文件保存会话，文件读取完后将session的最后一对键值覆盖到第一的位置。

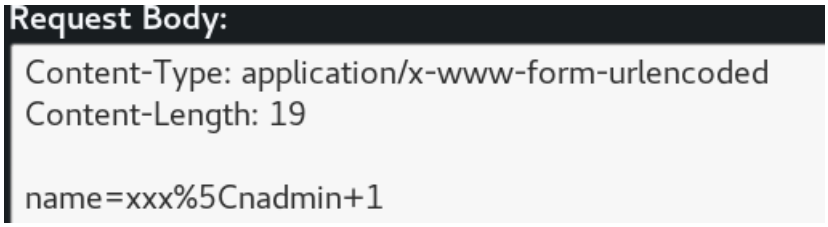
mywrite则会在会话结束的时候重新读取session，并对session进行一次ksort，将排序后的键值对重新写入文件。

一开始我的思路是通过使sid带有目录路径（改cookie），使得debug输出的时候将/etc/...../natas20的文件内容读出来，但是在myread和mywrite里面都进行了检验，所以很难通过sid进行注入。

另一个思路就是，源码里面其实没有向session里面添加admin的键值对，这也提示我们可以通过“唯一”的一个name键值对进行注入：将data里面的值变为：name xxxx\nadmin 1\n

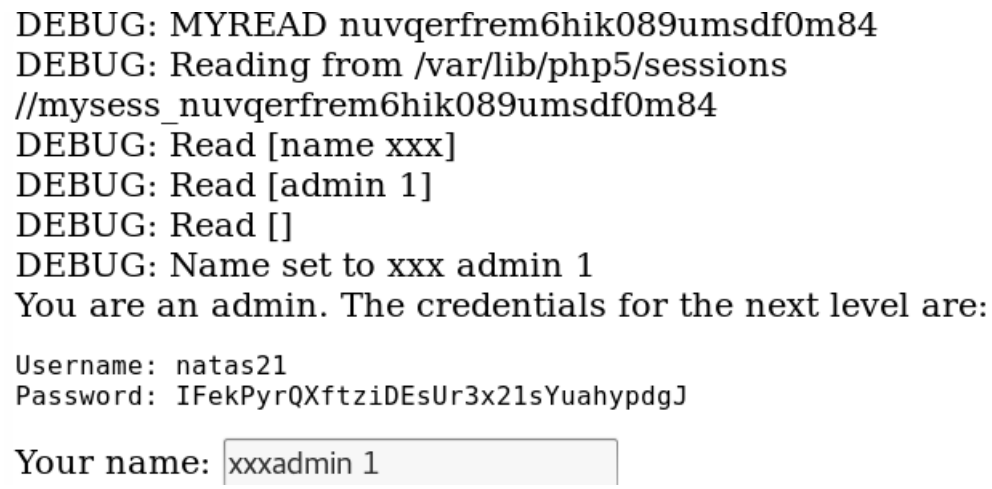
如何添加这个\n呢？既然通过get方式提交，也就要用URL编码编码后进行提交。（这里有个插曲，一开始我对mywrite的写入和myread的读取没有理解好，以为注入name xxx admin 1就可以了，实际上如果让mywrite这么写入，myread读取会话状态时$parts = explode(" ", $line, 2)，只会将这仅有的一行的第一个键值对name xxx添加到session里面）。\n对应%0A（\r对应%0D，但在linux下用换行号就够了）。所以应该输入xxx\nadmin 1，第一次会显示regular，因为没有文件/状态可以读取，session里还是没有Admin的，会话关闭后xxx\nadmin1就会被写入到状态中，下次登录后session就会被加入admin 1了。

但是，这里的输入并不能直接在form中输入并提交：



因为\n即回车并不会被编码为%0A这个字节存入到file中，可以直接url中输入并提交或者改postbody。

http://natas20.natas.labs.overthewire.org/index.php?name=xxx%0Aadmin%201&debug=1（%20为空格 直接空格也行）



总结：如果用户的输入要保存为会话状态，服务端读取和写入会话时要进行防注入处理，，否则存在提权或劫持等注入问题。

flag:**IFekPyrQXftziDEsUr3x21sYuahypdgJ**

转载于:https://www.cnblogs.com/liqiuhao/p/6882068.html