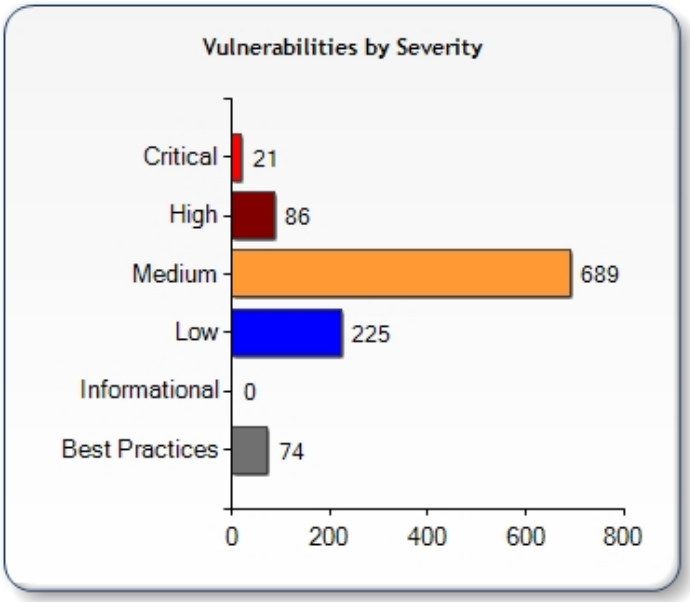
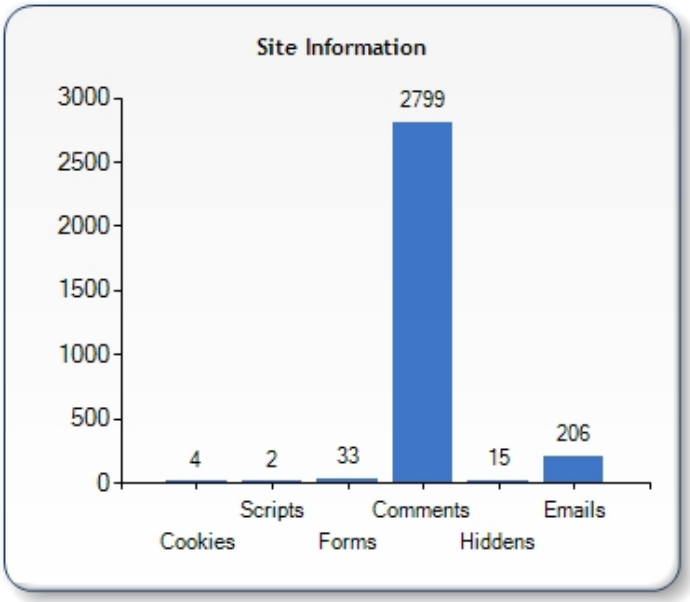
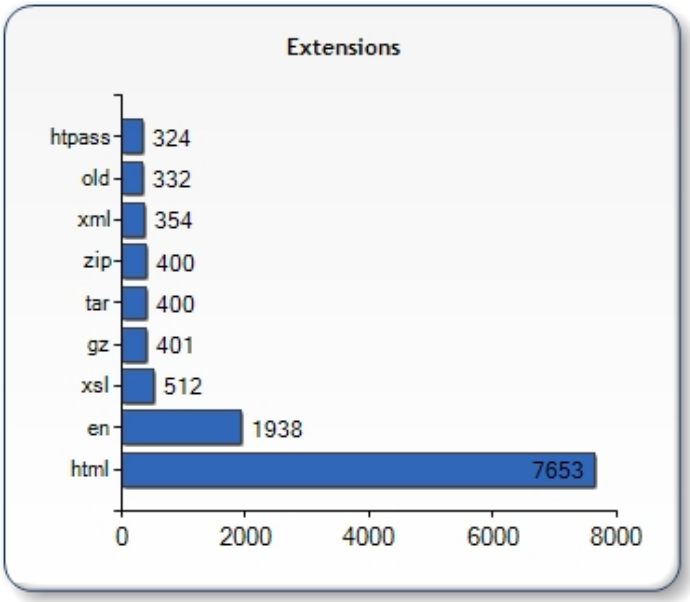
Web Application Assessment Report

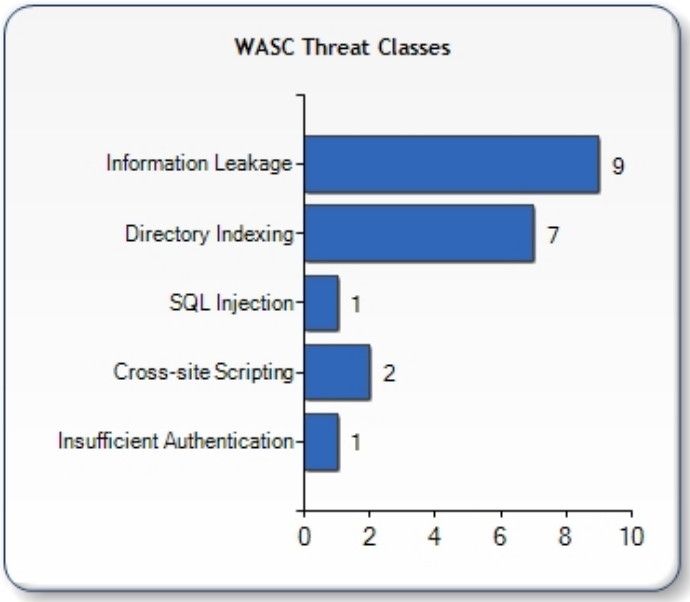
Scan: http://129.105.46.118/
Policy: Standard

Scan Date: Tuesday, August 28, 2007 9:39:55 AM
Scan Version: 7.5.35.1





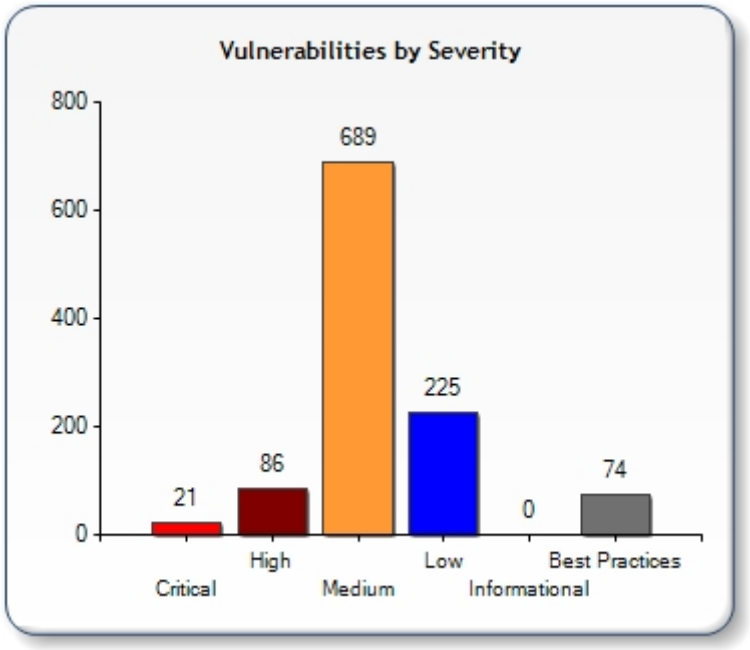




Scan: http://129.105.46.118/
Policy: Standard

Scan Date: Tuesday, August 28, 2007 9:39:55 AM
Scan Version: 7.5.35.1

Server: 129.105.46.118



Critical **Database Server Error Message**

File Names:
- http://129.105.46.118:80/sql/index.php
- http://129.105.46.118:80/sql/index.php
- http://129.105.46.118:80/authskip/login.php
- http://129.105.46.118:80/authskip/login.php
- http://129.105.46.118:80/sql/
- http://129.105.46.118:80/sql/

Summary: Critical database server error message vulnerabilities were identified in the web application, indicating that an unhandled exception was generated in your web application code. Unhandled exceptions are circumstances in which the application has received user input that it did not expect and does not know how to handle. When successfully exploited, an attacker can gain unauthorized access to the database by using the information recovered from seemingly innocuous error messages to pinpoint flaws in the web application and to discover additional avenues of attack. Recommendations include designing and adding consistent error-handling mechanisms that are capable of handling any user input to your web application, providing meaningful detail to end-users, and preventing error messages that might provide information useful to an attacker from being displayed.

Description

The most common cause of an unhandled exception is a failure to properly sanitize client-supplied data that is used in SQL statements. They can also be caused by a bug in the web application's database communication code, a misconfiguration of database connection settings, an unavailable database, or any other reason that would cause the application's database driver to be unable to establish a working session with the server. The problem is not that web applications generate errors. All web applications in their normal course of operation will at some point receive an unhandled exception. The problem lies not in that these errors were received, but rather in how they are handled. Any error handling solution needs to be well-designed, and uniform in how it handles errors. For instance, assume an attacker is attempting to access a specific file. If the request returns an error File not Found, the attacker can be relatively sure the file does not exist. However, if the error returns "Permission Denied," the attacker has a fairly good idea that the specific file does exist. This can be helpful to an attacker in many ways, from determining the operating system to discovering the underlying architecture and design of the application.

The error message may also contain the location of the file that contains the offending function. This may disclose the webroot's absolute path as well as give the attacker the location of application "include" files or database configuration information. A fundamental necessity for a successful attack upon your web application is reconnaissance. Database server error messages can provide information that can then be utilized when the attacker is formulating his next method of attack. It may even disclose the portion of code that failed.

Be aware that this check is part of unknown application testing which seeks to uncover new vulnerabilities in both custom and commercial software. Because of this, there are no specific patches or remediation information for this issue. Please note that this vulnerability may be a false positive if the page it is flagged on is technical documentation relating to a database server.

Execution: The ways in which an attacker can exploit the conditions that caused the error depend on its cause. In the case of SQL injection, the techniques that are used will vary from database server to database server, and even query to query. An in-depth guide to SQL Injection attacks is available at http://www.spidynamics.com/papers/SQLInjectionWhitePaper.pdf, or in the SQL Injection vulnerability information, accessible via the Policy Manager. Primarily, the information gleaned from database server error messages is what will allow an attacker to conduct a successful attack after he combines his various findings.

Implication: The severity of this vulnerability depends on the reason that the error message was generated. In most cases, it will be the result of the web application attempting to use an invalid client-supplied argument in a SQL statement, which means that SQL injection will be possible. If so, an attacker will at least be able to read the contents of the entire database arbitrarily. Depending on the database server and the SQL statement, deleting, updating and adding records and executing arbitrary commands may also be possible. If a software bug or bug is responsible for triggering the error, the potential impact will vary, depending on the circumstances. The location of the application that caused the error can be useful in facilitating other kinds of attacks. If the file is a hidden or include file, the attacker may be able to gain more information about the mechanics of the web application, possibly even the source code. Application source code is likely to contain usernames, passwords, database connection strings and aids the attacker greatly in discovering new vulnerabilities.

Fix:

For Development:

From a development perspective, the best method of preventing problems from arising from database error messages is to adopt secure programming techniques that prevent problems that might arise from an attacker discovering too much information about the architecture and design of your web application. The following recommendations can be used as a basis for that.

- Stringently define the data type (for instance, a string, an alphanumeric character, etc) that the application will accept.
- Use what is good instead of what is bad. Validate input for improper characters.
- Do not display error messages to the end user that provide information (such as table names) that could be utilized in orchestrating an attack.
- Define the allowed set of characters. For instance, if a field is to receive a number, only let that field accept numbers.
- Define the maximum and minimum data lengths for what the application will accept.
- Specify acceptable numeric ranges for input.

For Security Operations:

The following recommendations will help in implementing a secure database protocol for your web application. Be advised each database has its own method of secure lock down.

- **ODBC Error Messaging:** Turn off ODBC error messaging in your database server. Never display raw ODBC or other errors to the end user. See Removing Detailed Error Messages below, or consult your database server's documentation, for more information.
- **Uniform Error Codes:** Ensure that you are not inadvertently supplying information to an attacker via the use of inconsistent or "conflicting" error messages. For instance, don't reveal unintended information by utilizing error messages such as Access Denied, which will also let an attacker know that the file he seeks actually exists. Have consistent terminology for files and folders that do exist, do not exist, and which have read access denied.
- **Informational Error Messages:** Ensure that error messages do not reveal too much information. Complete or partial paths, variable and file names, row and column names in tables, and specific database errors should never be revealed to the end user. Remember, an attacker will gather as much information as possible, and then add pieces of seemingly innocuous information together to craft a method of attack.
- **Proper Error Handling:** Utilize generic error pages and error handling logic to inform end users of potential problems. Do not provide system information or other data that could be utilized by an attacker when orchestrating an attack.
- **Stored Procedures:** Consider using stored procedures. They require a very specific parameter format, which makes them less susceptible to SQL Injection attacks.
- **Database Privileges:** Utilize a least-privileges scheme for the database application. Ensure that user accounts only have the limited functionality that is actually required. All database mechanisms should deny access until it has been granted, not grant access until it has been denied.

Removing Detailed Error Messages

Find instructions for turning off detailed error messaging in IIS at this link:

http://www.microsoft.com/windows2000/en/server/iis/default.asp?url=
/windows2000/en/server/iis/htm/core/iierrcst.htm

Use the following syntax to suppress error messages on an Apache server.

Syntax: ErrorDocument <3-digit-code>
Example: ErrorDocument 500 /webserver_errors/server_error500.txt

For QA:

In reality, simple testing can usually determine how your web application will react to different input errors. More expansive testing must be conducted to cause internal errors to gauge the reaction of the site. If the unhandled exception occurs in a piece of in-house developed software, consult the developer. If it is in a commercial package, contact technical support.

The best course of action for QA associates to take is to ensure that the error handling scheme is consistent. Do you receive a different type of error for a file that does not exist as opposed to a file that does? Are phrases like "Permission Denied" utilized which could reveal the existence of a file to an attacker?

Reference:

SQL Injection Whitepaper
http://www.spidynamics.com/papers/SQLInjectionWhitePaper.pdf

Web Application Security Whitepaper
http://www.spidynamics.com/whitepapers/webappwhitepaper.pdf

Attack Request:

```
POST /sql/index.php HTTP/1.1
Referer: http://129.105.46.118:80/sql/index.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 35
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)
```

Pragma: no-cache
Host: 129.105.46.118
Connection: Keep-Alive
Cookie:
CustomCookie=WebInspect15804ZX5968C937BF2F4C00B8CA168F18502748YF85E;PHPSESSID=3e0922905
5471e85751910dd5b91c5ca;

search='&showquery=on&Submit=Submit

Attack Response:
HTTP/1.1 200 OK
Date: Tue, 28 Aug 2007 09:40:00 GMT
Server: Apache/2.0.54 (Unix) mod_ssl/2.0.54 OpenSSL/0.9.7e DAV/2 PHP/4.3.10
X-Powered-By: PHP/4.3.10
Content-Length: 483
Connection: close
Content-Type: text/html

<HTML>
<HEAD>
<TITLE>SQL Injection Exercise</TITLE>
<STYLE type="text/css">
BODY
{
font-family: arial;
}
</STYLE>
</HEAD>
<BODY>
<h2>SANS Web Application Security Workshop - SQL injection exercise </h2>
The query sent to the database is:
SELECT name, price, qty FROM products WHERE name like
'%'%'

Cannot submit query:You have an error in your SQL syntax; check the manual that corresponds to your
MySQL server version for the right syntax to use near ''' at line 1

Critical **Password Field Masked**

File Names:
- http://129.105.46.118:80/authskip/login.php

Summary:
Basic web application security measures include "masking" all passwords to ensure they are not easily visible/recovered. This includes both passwords typed in by the user (which may be viewed by someone looking over the user's shoulder), as well as hidden passwords returned by the server (which may be viewed by looking at the HTML source code in the browser). Recommendations include requiring all password fields in your web application be masked to prevent other users from seeing this information.

Implication:
Not masking password fields would give anyone within physical proximity easy access to sensitive information.

Fix:
Ensure that passwords entered by users on a site are not displayed in clear text. Also, do not return passwords to the user within hidden form fields.

Attack Request:
GET /authskip/login.php HTTP/1.1
Referer: http://129.105.46.118:80/
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)
Pragma: no-cache
Host: 129.105.46.118
Connection: Keep-Alive
Cookie: CustomCookie=WebInspect15804ZX5968C937BF2F4C00B8CA168F18502748YF85E

Attack Response:
HTTP/1.1 200 OK
Date: Tue, 28 Aug 2007 09:39:26 GMT
Server: Apache/2.0.54 (Unix) mod_ssl/2.0.54 OpenSSL/0.9.7e DAV/2 PHP/4.3.10
X-Powered-By: PHP/4.3.10
Content-Length: 1271
Connection: close
Content-Type: text/html

<html>
<head>
<title>Login Page</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
</head>

<body bgcolor="#FFFFFF" text="#000000">

<table width="257" border="0" height="367" cellspacing="0" cellpadding="0">
<tr>
<td colspan="2" height="104"><img src="intro-image-welcome.gif" width="298"
height="104"></td>

</tr>
<tr>
<td height="33"> </td>
<td height="33"> </td>
</tr>

```
        <tr>
          <td width="192" align="right" ><img src="intro-image-login.gif" width="112"></td>
          <td height="46"> <form method="post">
            <input type="text" name="login">
          </td>

        </tr>
        <tr>
          <td width="192" align="right" ><img src="intro-image-password.gif" width="112"></td>
          <td width="198" >
            <input type="text" name="pass">
          </td>
        </tr>
        <tr>
          <td width="192" height="22" valign="middle"> </td>
          <td height="22" width="198">

            <input type="image" border="0" name="imageField" src="intro-button-enter.gif">
           </form>
          </td>
        </tr>
  <tr><td></td><td><BR><Br><br><br><br></td></tr>
      </table>
</body>
</html>
```

Critical **Cross-Site Scripting**

File Names:
- http://129.105.46.118:80/sql/index.php
- http://129.105.46.118:80/session1/seecookie.php
- http://129.105.46.118:80/session2/page2.php
- http://129.105.46.118:80/session2/page2.php
- http://129.105.46.118:80/session2/page2.php
- http://129.105.46.118:80/session1/page2.php
- http://129.105.46.118:80/input/page2.php
- http://129.105.46.118:80/sql/

Summary: Cross-Site Scripting vulnerabilities were verified as executing code on the web application. Cross-Site Scripting occurs when dynamically generated web pages display user input, such as login information, that is not properly validated, allowing an attacker to embed malicious scripts into the generated page and then execute the script on the machine of any user that views the site. In this instance, the web application was vulnerable to an automatic payload, meaning the user simply has to visit a page to make the malicious scripts execute. If successful, Cross-Site Scripting vulnerabilities can be exploited to manipulate or steal cookies, create requests that can be mistaken for those of a valid user, compromise confidential information, or execute malicious code on end user systems. Recommendations include implementing secure programming techniques that ensure proper filtration of user-supplied data, and encoding all user supplied data to prevent inserted scripts being sent to end users in a format that can be executed.

Execution: View the attack string included with the request to check what to search for in the response. For instance, if "(javascript:alert('XSS')" is submitted as an attack (or another scripting language), it will also appear as part of the response. This indicates that the web application is taking values from the HTTP request parameters and using them in the HTTP response without first removing potentially malicious data.

Implication: XSS can generally be subdivided into two categories: stored and reflected attacks. The main difference between the two is in how the payload arrives at the server. Stored attacks are just that...in some form stored on the target server, such as in a database, or via a submission to a bulletin board or visitor log. The victim will retrieve and execute the attack code in his browser when a request is made for the stored information. Reflected attacks, on the other hand, come from somewhere else. This happens when user input from a web client is immediately included via server-side scripts in a dynamically generated web page. Via some social engineering, an attacker can trick a victim, such as through a malicious link or "rigged" form, to submit information which will be altered to include attack code and then sent to the legitimate server. The injected code is then reflected back to the user's browser which executes it because it came from a trusted server. The implication of each kind of attack is the same.

The main problems associated with successful Cross-Site Scripting attacks are:

- Account hijacking - An attacker can hijack the user's session before the session cookie expires and take actions with the privileges of the user who accessed the URL, such as issuing database queries and viewing the results.
- Malicious script execution - Users can unknowingly execute JavaScript, VBScript, ActiveX, HTML, or even Flash content that has been inserted into a dynamically generated page by an attacker.
- Worm propagation - With Ajax applications, XSS can propagate somewhat like a virus. The XSS payload can autonomously inject itself into pages, and easily re-inject the same host with more XSS, all of which can be done with no hard refresh. Thus, XSS can send multiple requests using complex HTTP methods to propagate itself invisibly to the user.
- Information theft - Via redirection and fake sites, attackers can connect users to a malicious server of the attacker's choice and capture any information entered by the user.
- Denial of Service - Often by utilizing malformed display requests on sites that contain a Cross-Site Scripting vulnerability, attackers can cause a denial of service condition to occur by causing the host site to query itself repeatedly .
- Browser Redirection - On certain types of sites that use frames, a user can be made to think that he is in fact on the original site when he has been redirected to a malicious one, since the URL in the browser's address bar will remains the same. This is because the entire page isn't being redirected, just the frame in which the JavaScript is being executed.

- Manipulation of user settings - Attackers can change user settings for nefarious purposes.

For more detailed information on Cross-Site Scripting attacks, see the SPI Dynamics Cross-Site Scripting whitepaper.

Fix:

For Development:

Cross-Site Scripting attacks can be avoided by carefully validating all input, and properly encoding all output. Validation can be done using standard ASP.NET Validation controls, or directly in your code. Always use as strict a pattern as you can possibly allow.

Encoding of output ensures that any scriptable content is properly encoded for HTML before being sent to the client. This is done with the function HttpUtility.HtmlEncode, as shown in the following Label control sample:

Label2.Text = HttpUtility.HtmlEncode(input)

Be sure to consider all paths that user input takes through your application. For instance, if data is entered by the user, stored in a database, and then redisplayed later, you must make sure it is properly encoded each time it is retrieved. If you must allow free-format text input, such as in a message board, and you wish to allow some HTML formatting to be used, you can handle this safely by explicitly allowing only a small list of safe tags. Here are examples of how to do this safely:

C# Example:

```
StringBuilder sb = new StringBuilder(
    HttpUtility.HtmlEncode(input));
sb.Replace("&lt;b&gt;", "<b>");
sb.Replace("&lt;/b&gt;", "<b>");
sb.Replace("&lt;i&gt;", "<i>");
sb.Replace("&lt;/i&gt;", "</i>");
Response.Write(sb.ToString());
```

VB.NET Example:

```
Dim sb As StringBuilder = New StringBuilder( _
    HttpUtility.HtmlEncode(input))
sb.Replace("&lt;b&gt;", "<b>")
sb.Replace("&lt;/b&gt;", "<b>")
sb.Replace("&lt;i&gt;", "<i>")
sb.Replace("&lt;/i&gt;", "</i>")
Response.Write(sb.ToString())
```

Java Example:

```
public static String HTMLEncode(String aTagFragment){
final StringBuffer result = new StringBuffer();
final StringCharacterIterator iterator = new StringCharacterIterator(aTagFragment);
char character = iterator.current();
while (character != StringCharacterIterator.DONE ){
if (character = = '<') {
result.append("&lt;");
}
else if (character = = '>') {
result.append("&gt;");
}
else if (character = = '\"') {
result.append("&quot;");
}
else if (character = = '\') {
result.append("&#039;");
}
else if (character = = '\\') {
result.append("&#092;");
}
else if (character = = '&') {
result.append("&amp;");
}
else {
//the char is not a special one
//add it to the result as is
result.append(character);
}
character = iterator.next();
}
return result.toString();
}
```

The following recommendations will help you build web applications capable of withstanding Cross-Site Scripting attacks.

- Define what is allowed. Ensure that the web application validates all input parameters (cookies, headers, query strings, forms, hidden fields, etc.) against a stringent definition of expected results.

- Check the responses from POST and GET requests to ensure what is being returned is what is expected, and is valid.
- Remove conflicting characters, brackets, and single and double quotes from user input by encoding user supplied data. This will prevent inserted scripts from being sent to end users in a form that can be executed.
- Whenever possible, limit all client-supplied data to alphanumeric data. Using this filtering scheme, if a user entered " <script>alertdocumentcookie('aaa') </script>", it would be reduced to "scriptalertdocumentcookiescript". If non-alphanumeric characters must be used, encode them as HTML entities before using them in an HTTP response, so that they cannot be used to modify the structure of the HTML document.
- Use two-factor customer authentication mechanisms as opposed to single-factor authentication.
- Verify the origin of scripts before you modify or utilize them.
- Do not implicitly trust any script given to you by others (whether downloaded from the web, or given to you by an acquaintance) for use in your own code.

Most server side scripting languages provide built in methods to convert the value of the input variable into correct, non-interpretable HTML. These should be used to sanitize all input before displayed to the client.

PHP: string htmlspecialchars (string string [, int quote_style])

ASP / ASP.NET: Server.HTMLEncode (strHTML String)

For Security Operations:

Server-side encoding, where all dynamic content is first sent through an encoding function where Scripting tags will be replaced with codes in the selected character set, can help to prevent Cross-Site Scripting attacks. The drawback to server-side encoding is that it can be resource intensive, and may have a negative performance impact on some web servers.

If site users must be allowed to use HTML tags, such as a bulletin board where the user would be allowed to use formatting tags, limit the ones that can be used. Create a list of acceptable tags, such as bold, italic or underline, and only allow those to be used. Any other tags should be rejected. Below are a few regular expressions that will help detect Cross-Site Scripting.

Regex for a simple CSS attack:

/((\%3C)|<)((\%2F)|\/)*[a-z0-9\%]+((\%3E)|>)/ix

The above regular expression would be added into a new Snort rule as follows:

alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"NII Cross-Site Scripting attempt"; flow:to_server,established; pcre:"/((\%3C)|<)((\%2F)|\/)*[a-z0-9\%]+((\%3E)|>)/i"; classtype:Web-application-attack; sid:9000; rev:5;)

Paranoid regex for CSS attacks:

/((\%3C)|<)[^\n]+((\%3E)|>)/I

This signature simply looks for the opening HTML tag, and its hex equivalent, followed by one or more characters other than the new line, and then followed by the closing tag or its hex equivalent. This may end up giving a few false positives depending upon how your Web application and Web server are structured, but it is guaranteed to catch anything that even remotely resembles a Cross-Site Scripting attack. From a public perspective, you can also strengthen educational programs to help consumers avoid online scams, such as phishing, that can be utilized in account hijackings and other forms of identity theft.

For QA:

Fixes for Cross-Site Scripting defects will ultimately require code based fixes. The steps detailed in the Developer and Security Operations section will provide any developer with the information necessary to remediate these issues. The following steps outline how to manually test an application for Cross-Site Scripting.

Step 1. Open any Web site in a browser, and look for places on the site that accept user input such as a search form or some kind of login page. Enter the word test in the search box and send this to the Web server.

Step 2. Look for the Web server to respond back with a page similar to something like "Your search for 'test' did not find any items" or "Invalid login test." If the word "test" appears in the results page, you are in luck.

Step 3. To test for Cross-Site Scripting, input the string "<script>alert('hello')</script>" without the quotes in the same search or login box you used before and send this to your Web server.

Step 4. If the server responds back with a popup box that says "hello", then the site is vulnerable to Cross-Site Scripting.

Step 5. If Step 4 fails and the Web site does not return this information, you still might be at risk. Click the 'View Source' option in your browser so you can see the actual HTML code of the Web page. Now find the <script> string that you sent the server. If you see the entire "<script>alert('hello')</script>" text in this source code, then the Web server is vulnerable to Cross-Site Scripting.

Reference:

SPI Dynamics Cross-Site Scripting Whitepaper

http://www.spidynamics.com/spilabs/education/whitepapers/CrossSiteScripting.html

OWASP Cross-Site Scripting Information

http://www.owasp.org/documentation/topten/a4.html

Microsoft

http://support.microsoft.com/default.aspx?scid=kb;EN-US;q252985

Microsoft Anti-Cross-Site Scripting Library V1.0

http://www.microsoft.com/downloads/details.aspx?familyid=9a2b9c92-7ad9-496c-9a89-af08de2e5982&displaylang=en

CERT

http://www.cert.org/advisories/CA-2000-02.html

Apache

http://httpd.apache.org/info/css-security/apache_specific.html

Netscape

http://channels.netscape.com/ns/browsers/security.jsp

SecurityFocus.com

http://www.securityfocus.com/infocus/1768

Attack Request:

```
POST /sql/index.php HTTP/1.1
Referer: http://129.105.46.118:80/sql/index.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 106
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)
Pragma: no-cache
Host: 129.105.46.118
Connection: Keep-Alive
Cookie:
CustomCookie=WebInspect15804ZX5968C937BF2F4C00B8CA168F18502748YF85E;PHPSESSID=d5a9350fa1
40374074819389271b3bb8;

search=777-777-1911form%2540value777.com%3cscript%3ealert(25568)%3c%2fscript%3e&showquery=o
n&Submit=Submit
```

Attack Response:

```
HTTP/1.1 200 OK
Date: Tue, 28 Aug 2007 09:40:00 GMT
Server: Apache/2.0.54 (Unix) mod_ssl/2.0.54 OpenSSL/0.9.7e DAV/2 PHP/4.3.10
X-Powered-By: PHP/4.3.10
Content-Length: 566
Connection: close
Content-Type: text/html

<HTML>
<HEAD>
<TITLE>SQL Injection Exercise</TITLE>
<STYLE type="text/css">
BODY
{
font-family: arial;
}
</STYLE>
</HEAD>
<BODY>
<h2>SANS Web Application Security Workshop - SQL injection exercise </h2>
  The query sent to the database is: <BR>SELECT name, price, qty FROM products WHERE name like
'%777-777-1911form%40value777.com<script>alert(25568)</script>%'<BR><BR><BR>
  <FONT COLOR=RED FACE="Arial"><B>
  0   rows returned</FONT></B><P>
  <TABLE
BGCOLOR="LightSteelBlue"><TR><TD>Name</TD><TD>Price</TD><TD>Quantity</TD></TR>
    </TABLE>
  </BODY>
</HTML>
```

Critical

SQL Injection (confirmed)

File Names:

- http://129.105.46.118:80/sql/
- http://129.105.46.118:80/sql/
- http://129.105.46.118:80/authskip/login.php
- http://129.105.46.118:80/authskip/login.php
- http://129.105.46.118:80/sql/index.php
- http://129.105.46.118:80/sql/index.php

Summary: Critical SQL Injection vulnerabilities have been identified in the web application. SQL injection is a method of attack where an attacker can exploit vulnerable code and the type of data an application will accept, and can be exploited in any application parameter that influences a database query. Examples include paramaters within the url itself, post data, or cookie values. If successful, SQL Injection can give an attacker access to backend database contents, the ability to remotely execute system commands, or in some circumstances the means to take control of the server hosting the database. Recommendations include employing a layered approach to security that includes utilizing parameterized queries when accepting user input, ensuring that only expected data is accepted by an application, and hardening the database server to prevent data from being accessed inappropriately.

Execution: Consider a login form for a web application. If the user input from the form is directly utilized to build a dynamic SQL statement, then there has been no input validation conducted, giving control to an attacker who wants access to the database. Basically, an attacker can use an input box to send their own request to the server, and then utilize the results in a malicious manner. This is a very typical scenario considering that HTML pages often use the POST command to send parameters to another ASP page. The number in bold might be supplied by the client in an HTTP GET or POST parameter, like in the following URL:

http://www.server.com/GetItemPrice?ItemNumber=**12345**

In the example above, the client-supplied value, **12345**, is simply used as a numeric expression to indicate the item that the user wants to obtain the price of an item. The web application takes this value and inserts

it into the SQL statement in between the single quotes in the WHERE clause. However, consider the following URL:

http://www.server.com/GetItemPrice?ItemPrice?ItemNumber=0' UNION SELECT CreditCardNumber FROM C
ustomers WHERE '1'='1

In this case, the client-supplied value has actually modified the SQL statement itself and 'injected' a statement of his or her choosing. Instead of the price of an item, this statement will retrieve a customer's credit card number.

Implication: Fundamentally, SQL Injection is an attack upon the web application, not the web server or the operating system itself. As the name implies, SQL Injection is the act of adding an unexpected SQL commands to a query, thereby manipulating the database in ways unintended by the database administrator or developer. When successful, data can be extracted, modified, inserted or deleted from database servers that are used by vulnerable web applications. In certain circumstances, SQL Injection can be utilized to take complete control of a system.

Fix: Each method of preventing SQL injection has its own limitations. Therefore, it is wise to employ a layered approach to preventing SQL injection, and implement several measures to prevent unauthorized access to your backend database. The following are recommended courses of action to take to prevent SQL Injection and Blind SQL Injection vulnerabilities from being exploited in your web application.

For Development:

Use the following recommendations to code web applications that are not susceptible to SQL Injection attacks.

- **Parameterized Queries:** SQL Injection arises from an attacker's manipulation of query data to modify query logic. The best method of preventing SQL Injection attacks is thereby to separate the logic of a query from its data. This will prevent commands inserted from user input from being executed. The downside of this approach is that it can have an impact on performance, albeit slight, and that each query on the site must be structured in this method for it to be completely effective. If one query is inadvertently bypassed, that could be enough to leave the application vulnerable to SQL Injection. The following code shows a sample SQL statement that is SQL injectable.

```
sSql = "SELECT LocationName FROM Locations ";
sSql = sSql + " WHERE LocationID = " + Request["LocationID"];
oCmd.CommandText = sSql;
```

The following example utilizes parameterized queries, and is safe from SQL Injection attacks.

```
sSql = "SELECT * FROM Locations ";
sSql = sSql + " WHERE LocationID = @LocationID";
oCmd.CommandText = sSql;
oCmd.Parameters.Add("@LocationID", Request["LocationID"]);
```

The application will send the SQL statement to the server without including the user's input. Instead, a parameter-@LocationID- is used as a placeholder for that input. In this way, user input never becomes part of the command that SQL executes. Any input that an attacker inserts will be effectively negated. An error would still be generated, but it would be a simple data-type conversion error, and not something which a hacker could exploit.

The following code samples show a product ID being obtained from an HTTP query string, and used in a SQL query. Note how the string containing the "SELECT" statement passed to SqlCommand is simply a static string, and is not concatenated from input. Also note how the input parameter is passed using a SqlParameter object, whose name ("@pid") matches the name used within the SQL query.

C# sample:

```
    string connString = WebConfigurationManager.ConnectionStrings["myConn"].ConnectionStrin
g;
    using (SqlConnection conn = new SqlConnection(connString))
    {
        conn.Open();
        SqlCommand cmd = new SqlCommand("SELECT Count(*) FROM Products WHERE ProdID=
@pid", conn);
        SqlParameter prm = new SqlParameter("@pid", SqlDbType.VarChar, 50);
        prm.Value = Request.QueryString["pid"];
        cmd.Parameters.Add(prm);
        int recCount = (int)cmd.ExecuteScalar();
    }
```

VB.NET sample:

```
    Dim connString As String = WebConfigurationManager.ConnectionStrings("myConn").Connecti
onString
    Using conn As New SqlConnection(connString)
        conn.Open()
        Dim cmd As SqlCommand = New SqlCommand("SELECT Count(*) FROM Products WHERE
ProdID=@pid", conn)
        Dim prm As SqlParameter = New SqlParameter("@pid", SqlDbType.VarChar, 50)
        prm.Value = Request.QueryString("pid")
        cmd.Parameters.Add(prm)
        Dim recCount As Integer = cmd.ExecuteScalar()
    End Using
```

- **Validate input:** The vast majority of SQL Injection checks can be prevented by properly validating user input for both type and format. The best method of doing this is via "white listing". This is defined as only accepting specific account numbers or specific account types for those relevant fields, or only accepting integers or letters of the English alphabet for others. Many developers will try to validate input by "black listing" characters, or "escaping" them. Basically, this entails rejecting known bad data, such as a single quotation mark, by placing an "escape" character in front of it so that the item that follows will be treated as a literal value. This approach is not as effective as white listing because it is impossible to know all forms of bad data ahead of time.

For Security Operations:

Use the following recommendations to help prevent SQL Injection attacks upon your web applications.

- **Restrict Application Privileges:** Limit user credentials so that only those rights the application needs to function are utilized. Any successful SQL Injection attack would run in the context of the user's credential. While limiting privileges will not prevent SQL Injection attacks outright, it will make them significantly harder to enact.
- **Strong SA Password Policy:** Often, an attacker will need the functionality of the administrator account to utilize specific SQL commands. It is much easier to "brute force" the SA password when it is weak, and will increase the likelihood of a successful SQL Injection attack. Another option is not to use the SA account at all, and instead create specific accounts for specific purposes.
- **Consistent Error Messaging Scheme:** Ensure that you provide as little information to the user as possible when a database error occurs. Don't reveal the entire error message. Error messages need to be dealt with on both the web and application server. When a web server encounters a processing error it should respond with a generic web page, or redirect the user to a standard location. Debug information, or other details that could be useful to a potential attacker, should never be revealed.

  Find instructions for turning off detailed error messaging in IIS at this link:

  http://www.microsoft.com/windows2000/en/server/iis/default.asp?url=
  /windows2000/en/server/iis/htm/core/iierrcst.htm

  Use the following syntax to suppress error messages on an Apache server.

  Syntax: ErrorDocument <3-digit-code>

  Example: ErrorDocument 500 /webserver_errors/server_error500.txt

  Application servers, like WebSphere, often install with error messages or debug settings enabled by default. Consult your application server's documentation for information on suppressing those error messages.
- **Stored Procedures:** If unused, delete SQL stored procedures such as master..Xp_cmdshell, xp_startmail, xp_sendmail, and sp_makewebtask.

SQL Injection vulnerabilities are inherently tied to the actual code of your web application. While not a fix, you can implement an emergency measure by adding a rule that incorporates a regular expression to your IDS to check for SQL Injection attacks. While this will not resolve all possible SQL injection vulnerabilities, it is simple to implement, and will require an attacker to escalate his methodology to achieve a successful attack. Regular expressions that can be utilized to do this follow.

Regex for detection of SQL meta-characters:

/(\%27)|(\')|(\-\-)|(\%23)|(#)/ix

The above regular expression would be added into a Snort rule as follows:

alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"SQL Injection - Paranoid"; flow:to_server,established;uricontent:".pl";pcre:"/(\%27)|(\')|(\-\-)|(%23)|
(#)/i"; classtype:Web-application-attack; sid:9099; rev:5;)

Regex for typical SQL Injection attacks:

/\w*((\%27)|(\'))((\%6F)|o|(\%4F))((\%72)|r|(\%52))/ix

Regex for detecting SQL Injection with the UNION keyword:

/(((\%27)|(\'))union/ix

(\%27)|(\')

the single-quote and its hex equivalent union - the keyword union

Similar expressions can be written for other SQL queries such as select, insert, update, delete, drop, and so on.

Regex for detecting SQL Injection attacks on a MS SQL Server:

/exec(\s|\+)+(s|x)p\w+/ix

For QA:

Fixes for SQL Injection defects will ultimately require code based fixes. The steps detailed in the Developer and Security Operations section will provide any developer with the information necessary to remediate these issues. The following steps outline how to manually test an application for SQL Injection.

How to manually test applications for SQL Injection:

1. Open the web application you wish to test for SQL Injection defects in a browser.

2. Mouse over the links of the Web site with your cursor while paying attention to the bottom status bar. You will notice the URLs that the links point to. Try to find a URL with parameters in it. Ex. http://www.site.com/articleid.asp?id=42.

Note: If you don't see any URL's in the status bar, then just click on links and watch the address bar until you find a URL that has parameters.

3. Once a URL with parameters has been found, click the link and go to that page. In the Address bar you should now see the URL that was seen in the status bar.

4. There are two methods for testing scripts for SQL injection. Be sure to test each parameter value one at a time with both methods.

Method 1. Go to the address bar, click your cursor, and highlight a parameter value Ex. Highlight the word value in "name=value" and replace it with a single quote (').It should now look like "name=' "

Method 2. Go to the address bar, click your cursor, and put a single quote (') in the middle of the value. It should now look like "name=val'ue"

5. Click the 'GO' button. This will send your request to the Web server.

6. Analyze the response from the Web server for any error messages. Most database error messages will look similar to the examples below:

Example error 1:
Microsoft OLE DB Provider for SQL Server error '80040e14'
Unclosed quotation mark before the character string '51 ORDER BY
some_name'. /some_directory/some_file.asp, line 5

Example error 2:
ODBC Error Code = S1000 (General error)
[Oracle][ODBC][Ora]ORA-00933: SQL command not properly ended

Example error 3:
Error: 1353 SQLSTATE: HY000 (ER_VIEW_WRONG_LIST)
Message: View's SELECT and view's field list have different column counts

7. Sometimes the error message is not obvious and is hidden in the source of the page. To look for it, you must view the HTML source of the page and search for the error. To do this in Internet Explorer, click the 'View' menu, and select the 'Source' option. This will cause notepad to open with the HTML source of the page. In notepad, click the 'Edit' menu and select 'Find'. A dialog box will appear that will ask you to 'Find What'. Type the phrase 'Microsoft OLE DB' or '[ODBC]' and click 'Find Next'.

8. If either step 6 or 7 is successful, then the Web site is vulnerable to SQL injection.

Reference:
SPI Dynamics SQL Injection Whitepaper
http://www.spidynamics.com/whitepapers/WhitepaperSQLInjection.pdf
SPI Dynamics Blind SQL Injection Whitepaper
http://www.spidynamics.com/support/whitepapers/Blind_SQLInjection.pdf
Microsoft
http://msdn.microsoft.com/msdnmag/issues/04/09/SQLInjection/default.aspx
http://support.microsoft.com/default.aspx?scid=kb;en-us;302570
SQLSecurity.com
http://www.sqlsecurity.com/DesktopDefault.aspx
OWASP
http://www.owasp.org/index.php/SQL_Injection

Attack Request:
```
POST /sql/ HTTP/1.1
Referer: http://129.105.46.118:80/sql/
Content-Type: application/x-www-form-urlencoded
Content-Length: 119
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)
Pragma: no-cache
Host: 129.105.46.118
Connection: Keep-Alive
Cookie:
CustomCookie=WebInspect15804ZX5968C937BF2F4C00B8CA168F18502748YF85E;PHPSESSID=6ea4a2f4f8
85719ef23b18117ac21c1a;

search=777-777-1911form%2540value777.com'+OR+(select+count(*)+from+spitable)+%3e0+OR+'4'%3d
'&showquery=on&Submit=Submit
```

Attack Response:
```
HTTP/1.1 200 OK
Date: Tue, 28 Aug 2007 09:40:26 GMT
Server: Apache/2.0.54 (Unix) mod_ssl/2.0.54 OpenSSL/0.9.7e DAV/2 PHP/4.3.10
X-Powered-By: PHP/4.3.10
Content-Length: 449
Connection: close
Content-Type: text/html

<HTML>
<HEAD>
<TITLE>SQL Injection Exercise</TITLE>
<STYLE type="text/css">
BODY
{
font-family: arial;
}
</STYLE>
</HEAD>
<BODY>
<h2>SANS Web Application Security Workshop - SQL injection exercise </h2>
  The query sent to the database is: <BR>SELECT name, price, qty FROM products WHERE name like
'%777-777-1911form%40value777.com' OR (select count(*) from spitable) >0 OR '4'='%'<BR><BR><BR>
Cannot submit query:Table 'sans.spitable' doesn't exist
```

High **Directory Listing**

File Names:

- http://129.105.46.118:80/manual/es/howto/ssi.html
- http://129.105.46.118:80/manual/en/howto/ssi.html
- http://129.105.46.118:80/manual/de/howto/ssi.html
- http://129.105.46.118:80/session2/
- http://129.105.46.118:80/input/
- http://129.105.46.118:80/authskip/
- http://129.105.46.118:80/icons/
- http://129.105.46.118:80/icons/small/
- http://129.105.46.118:80/manual/howto/ssi.html
- http://129.105.46.118:80/manual/mod/mod_autoindex.html
- http://129.105.46.118:80/session1/
- http://129.105.46.118:80/manual/style/
- http://129.105.46.118:80/manual/images/
- http://129.105.46.118:80/manual/howto/ssi.html.en
- http://129.105.46.118:80/manual/style/css/
- http://129.105.46.118:80/manual/de/mod/mod_autoindex.html
- http://129.105.46.118:80/manual/en/mod/mod_autoindex.html
- http://129.105.46.118:80/manual/es/mod/mod_autoindex.html
- http://129.105.46.118:80/manual/ru/howto/ssi.html
- http://129.105.46.118:80/manual/fr/howto/ssi.html
- http://129.105.46.118:80/manual/de/images/
- http://129.105.46.118:80/manual/en/images/
- http://129.105.46.118:80/manual/es/images/
- http://129.105.46.118:80/manual/fr/images/
- http://129.105.46.118:80/manual/ja/images/
- http://129.105.46.118:80/manual/ko/images/
- http://129.105.46.118:80/manual/ru/images/
- http://129.105.46.118:80/manual/ru/mod/mod_autoindex.html
- http://129.105.46.118:80/manual/mod/mod_autoindex.html.en
- http://129.105.46.118:80/manual/de/style/css/
- http://129.105.46.118:80/manual/de/style/
- http://129.105.46.118:80/manual/de/howto/ssi.html.en
- http://129.105.46.118:80/manual/en/style/css/
- http://129.105.46.118:80/manual/en/style/
- http://129.105.46.118:80/manual/es/style/css/
- http://129.105.46.118:80/manual/es/style/
- http://129.105.46.118:80/manual/en/howto/ssi.html.en
- http://129.105.46.118:80/manual/fr/mod/mod_autoindex.html
- http://129.105.46.118:80/manual/fr/style/css/
- http://129.105.46.118:80/manual/fr/style/
- http://129.105.46.118:80/manual/ko/style/css/
- http://129.105.46.118:80/manual/ko/style/
- http://129.105.46.118:80/manual/es/howto/ssi.html.en
- http://129.105.46.118:80/manual/fr/howto/ssi.html.en
- http://129.105.46.118:80/manual/ja/style/css/
- http://129.105.46.118:80/manual/ja/style/
- http://129.105.46.118:80/manual/ru/style/css/
- http://129.105.46.118:80/manual/ru/style/
- http://129.105.46.118:80/manual/ru/howto/ssi.html.en
- http://129.105.46.118:80/manual/style/lang/
- http://129.105.46.118:80/manual/style/latex/
- http://129.105.46.118:80/manual/style/xsl/
- http://129.105.46.118:80/manual/de/mod/mod_autoindex.html.en
- http://129.105.46.118:80/manual/en/mod/mod_autoindex.html.en
- http://129.105.46.118:80/manual/es/mod/mod_autoindex.html.en
- http://129.105.46.118:80/manual/ru/mod/mod_autoindex.html.en
- http://129.105.46.118:80/manual/de/style/lang/
- http://129.105.46.118:80/manual/de/style/latex/
- http://129.105.46.118:80/manual/de/style/xsl/
- http://129.105.46.118:80/manual/en/style/lang/
- http://129.105.46.118:80/manual/en/style/latex/
- http://129.105.46.118:80/manual/en/style/xsl/
- http://129.105.46.118:80/manual/es/style/lang/
- http://129.105.46.118:80/manual/es/style/latex/
- http://129.105.46.118:80/manual/es/style/xsl/
- http://129.105.46.118:80/manual/fr/mod/mod_autoindex.html.en
- http://129.105.46.118:80/manual/fr/style/lang/
- http://129.105.46.118:80/manual/fr/style/latex/
- http://129.105.46.118:80/manual/fr/style/xsl/
- http://129.105.46.118:80/manual/ja/style/lang/
- http://129.105.46.118:80/manual/ja/style/latex/
- http://129.105.46.118:80/manual/ja/style/xsl/
- http://129.105.46.118:80/manual/ko/style/lang/
- http://129.105.46.118:80/manual/ko/style/latex/
- http://129.105.46.118:80/manual/ko/style/xsl/
- http://129.105.46.118:80/manual/ru/style/lang/
- http://129.105.46.118:80/manual/ru/style/latex/
- http://129.105.46.118:80/manual/ru/style/xsl/
- http://129.105.46.118:80/manual/style/xsl/util/

- http://129.105.46.118:80/manual/de/style/xsl/util/
- http://129.105.46.118:80/manual/en/style/xsl/util/
- http://129.105.46.118:80/manual/es/style/xsl/util/
- http://129.105.46.118:80/manual/fr/style/xsl/util/
- http://129.105.46.118:80/manual/ja/style/xsl/util/
- http://129.105.46.118:80/manual/ko/style/xsl/util/
- http://129.105.46.118:80/manual/ru/style/xsl/util/

Summary: A serious Directory Listing vulnerability was discovered within your web application. Risks associated with an attacker discovering a Directory Listing, which is a complete index of all of the resources located in that directory, result from the fact that files that should remain hidden, such as data files, backed-up source code, or applications in development, may then be visible. The specific risks depend upon the specific files that are listed and accessible. Recommendations include restricting access to important directories or files by adopting a "need to know" requirement for both the document and server root, and turning off features such as Automatic Directory Listings that could expose private files and provide information that could be utilized by an attacker when formulating or conducting an attack.

Execution: http://129.105.46.118:80/manual/es/howto/ssi.html

Implication: Risks associated with an attacker discovering a Directory Listing on your application server depend upon what type of directory is discovered, and what types of files are contained within it. The primary threat from an accessible Directory Listing is that hidden files such as data files, source code, or applications under development will then be visible to a potential attacker. In addition to accessing files containing sensitive information, other risks include an attacker utilizing the information discovered in that directory to perform other types of attacks.

Fix: **For Development:** Unless you are actively involved with implementing the web application server, there is not a wide range of available solutions to prevent problems that can occur from an attacker finding a Directory Listing. Primarily, this problem will be resolved by the web application server administrator. However, there are certain actions you can take that will help to secure your web application.

- Restrict access to important files or directories only to those who actually need it.
- Ensure that files containing sensitive information are not left publicly accessible, or that comments left inside files do not reveal the locations of directories best left confidential.

For Security Operations:

One of the most important aspects of web application security is to restrict access to important files or directories only to those individuals who actually need to access them. Ensure that the private architectural structure of your web application is not exposed to anyone who wishes to view it as even seemingly innocuous directories can provide important information to a potential attacker.

The following recommendations can help to ensure that you are not unintentionally allowing access to either information that could be utilized in conducting an attack or propriety data stored in publicly accessible directories.

- Turn off the Automatic Directory Listing feature in whatever application server package that you utilize.
- Restrict access to important files or directories only to those who actually need it.
- Ensure that files containing sensitive information are not left publicly accessible.
- Don't follow standard naming procedures for hidden directories. For example, don't create a hidden directory called "cgi" that contains cgi scripts. Obvious directory names are just that...readily guessed by an attacker.

Remember, the harder you make it for an attacker to access information about your web application, the more likely it is that he will simply find an easier target.

For QA:

For reasons of security, it is important to test the web application not only from the perspective of a normal user, but also from that of a malicious one. Whenever possible, adopt the mindset of an attacker when testing your web application for security defects. Access your web application from outside your firewall or IDS. Utilize Google or another search engine to ensure that searches for vulnerable files do not return information from regarding your web application. For example, an attacker will utilize a search engine, and search for directory listings such as the following: "index of / cgi-bin". Make sure that your directory structure is not obvious, and that only files that are necessary are capable of being accessed.

Reference: **Apache:**

Security Tips for Server Configuration

Protecting Confidential Documents at Your Site

Securing Apache - Access Control

IIS:

Implementing NTFS Standard Permissions on Your Web Site

Netscape:

Controlling Access to Your Server

General:

Password-protecting web pages

Web Security

Attack Request:

```
GET /manual/es/howto/ssi.html HTTP/1.1
Referer: http://129.105.46.118:80/manual/es/
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)
Pragma: no-cache
Host: 129.105.46.118
Connection: Keep-Alive
Cookie:
CustomCookie=WebInspect15804ZX5968C937BF2F4C00B8CA168F18502748YF85E;PHPSESSID=0286af493a
```

cdaf996469d378e8cb3ea1;

Attack Response:

```
HTTP/1.1 200 OK
Date: Tue, 28 Aug 2007 09:44:07 GMT
Server: Apache/2.0.54 (Unix) mod_ssl/2.0.54 OpenSSL/0.9.7e DAV/2 PHP/4.3.10
Content-Location: ssi.html.en
Vary: negotiate,accept-language,accept-charset
TCN: choice
Last-Modified: Fri, 04 Feb 2005 22:50:17 GMT
ETag: "1cb0-5e98-4e689c40;1caf-fe-a64a7c40"
Accept-Ranges: bytes
Content-Length: 24216
Connection: close
Content-Type: text/html
Content-Language: en

<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" lang="en" xml:lang="en"><head><!--
      XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
           This file is generated from xml source: DO NOT EDIT
      XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
    -->
<title>Apache Tutorial: Introduction to Server Side Includes - Apache HTTP Server</title>
<link href="../style/css/manual.css" rel="stylesheet" media="all" type="text/css" title="Main stylesheet" />
<link href="../style/css/manual-loose-100pc.css" rel="alternate stylesheet" media="all" type="text/css"
title="No Sidebar - Default font size" />
<link href="../style/css/manual-print.css" rel="stylesheet" media="print" type="text/css" />
<link href="../images/favicon.ico" rel="shortcut icon" /></head>
<body id="manual-page"><div id="page-header">
<p class="menu"><a href="../mod/">Modules</a> | <a href="../mod/directives.html">Directives</a> |
<a href="../faq/">FAQ</a> | <a href="../glossary.html">Glossary</a> | <a
href="../sitemap.html">Sitemap</a></p>
<p class="apache">Apache HTTP Server Version 2.0</p>
<img alt="" src="../images/feather.gif" /></div>
<div class="up"><a href="./"><img title="&lt;-" alt="&lt;-" src="../images/left.gif" /></a></div>
<div id="path">
<a href="http://www.apache.org/">Apache</a> &gt; <a href="http://httpd.apache.org/">HTTP
Server</a> &gt; <a href="http://httpd.apache.org/docs-project/">Documentation</a> &gt; <a
href="../"> ... {content removed}
```

Medium **Possible Server Path Disclosure (win32)**

File Names:

- http://129.105.46.118:80/manual/mod/mod_cache.html.en
- http://129.105.46.118:80/manual/ru/mod/mod_isapi.html
- http://129.105.46.118:80/manual/mod/mod_isapi.html.en
- http://129.105.46.118:80/manual/ru/mod/mod_cache.html
- http://129.105.46.118:80/manual/ru/mod/mod_disk_cache.html
- http://129.105.46.118:80/manual/ko/mod/mod_cache.html
- http://129.105.46.118:80/manual/ko/mod/mod_disk_cache.html
- http://129.105.46.118:80/manual/ko/mod/mod_isapi.html
- http://129.105.46.118:80/manual/mod/mod_disk_cache.html.en
- http://129.105.46.118:80/manual/fr/platform/windows.html
- http://129.105.46.118:80/manual/fr/platform/netware.html
- http://129.105.46.118:80/manual/es/platform/windows.html
- http://129.105.46.118:80/manual/es/platform/netware.html
- http://129.105.46.118:80/manual/ru/platform/windows.html
- http://129.105.46.118:80/manual/ru/platform/netware.html
- http://129.105.46.118:80/manual/ja/platform/netware.html
- http://129.105.46.118:80/manual/ja/platform/windows.html
- http://129.105.46.118:80/manual/ko/platform/windows.html
- http://129.105.46.118:80/manual/ko/platform/netware.html
- http://129.105.46.118:80/manual/es/mod/mod_cache.html
- http://129.105.46.118:80/manual/es/mod/mod_disk_cache.html
- http://129.105.46.118:80/manual/es/mod/mod_isapi.html
- http://129.105.46.118:80/manual/ja/mod/mod_cache.html
- http://129.105.46.118:80/manual/ja/mod/mod_disk_cache.html
- http://129.105.46.118:80/manual/ja/mod/mod_isapi.html
- http://129.105.46.118:80/manual/en/mod/mod_cache.html
- http://129.105.46.118:80/manual/en/mod/mod_disk_cache.html
- http://129.105.46.118:80/manual/en/mod/mod_isapi.html
- http://129.105.46.118:80/manual/de/mod/mod_cache.html
- http://129.105.46.118:80/manual/de/mod/mod_disk_cache.html
- http://129.105.46.118:80/manual/de/mod/mod_isapi.html
- http://129.105.46.118:80/manual/platform/windows.html.en
- http://129.105.46.118:80/manual/platform/netware.html.en
- http://129.105.46.118:80/manual/mod/mod_cache.html
- http://129.105.46.118:80/manual/mod/mod_disk_cache.html
- http://129.105.46.118:80/manual/mod/mod_isapi.html
- http://129.105.46.118:80/manual/platform/windows.html

- http://129.105.46.118:80/manual/platform/netware.html
- http://129.105.46.118:80/manual/de/platform/windows.html
- http://129.105.46.118:80/manual/de/platform/netware.html
- http://129.105.46.118:80/manual/en/platform/windows.html
- http://129.105.46.118:80/manual/en/platform/netware.html
- http://129.105.46.118:80/manual/fr/mod/mod_isapi.html.en
- http://129.105.46.118:80/manual/fr/mod/mod_cache.html.en
- http://129.105.46.118:80/manual/fr/mod/mod_disk_cache.html.en
- http://129.105.46.118:80/manual/ko/mod/mod_disk_cache.html.ko.euc-kr
- http://129.105.46.118:80/manual/ko/mod/mod_isapi.html.ko.euc-kr
- http://129.105.46.118:80/manual/ru/mod/mod_cache.html.en
- http://129.105.46.118:80/manual/ru/mod/mod_disk_cache.html.en
- http://129.105.46.118:80/manual/ru/mod/mod_isapi.html.en
- http://129.105.46.118:80/manual/es/mod/mod_disk_cache.html.en
- http://129.105.46.118:80/manual/es/mod/mod_isapi.html.en
- http://129.105.46.118:80/manual/ja/mod/mod_cache.html.en
- http://129.105.46.118:80/manual/ja/mod/mod_disk_cache.html.en
- http://129.105.46.118:80/manual/ja/mod/mod_isapi.html.en
- http://129.105.46.118:80/manual/ko/mod/mod_cache.html.ko.euc-kr
- http://129.105.46.118:80/manual/es/mod/mod_cache.html.en
- http://129.105.46.118:80/manual/en/mod/mod_cache.html.en
- http://129.105.46.118:80/manual/en/mod/mod_disk_cache.html.en
- http://129.105.46.118:80/manual/en/mod/mod_isapi.html.en
- http://129.105.46.118:80/manual/de/mod/mod_cache.html.en
- http://129.105.46.118:80/manual/ko/platform/netware.html.ko.euc-kr
- http://129.105.46.118:80/manual/ko/platform/windows.html.ko.euc-kr
- http://129.105.46.118:80/manual/de/mod/mod_disk_cache.html.en
- http://129.105.46.118:80/manual/de/mod/mod_isapi.html.en
- http://129.105.46.118:80/manual/ru/platform/windows.html.en
- http://129.105.46.118:80/manual/ru/platform/netware.html.en
- http://129.105.46.118:80/manual/ja/platform/windows.html.en
- http://129.105.46.118:80/manual/ja/platform/netware.html.en
- http://129.105.46.118:80/manual/fr/platform/windows.html.en
- http://129.105.46.118:80/manual/fr/platform/netware.html.en
- http://129.105.46.118:80/manual/es/platform/windows.html.en
- http://129.105.46.118:80/manual/es/platform/netware.html.en
- http://129.105.46.118:80/manual/fr/mod/mod_isapi.html
- http://129.105.46.118:80/manual/fr/mod/mod_cache.html
- http://129.105.46.118:80/manual/fr/mod/mod_disk_cache.html
- http://129.105.46.118:80/manual/en/platform/windows.html.en
- http://129.105.46.118:80/manual/en/platform/netware.html.en
- http://129.105.46.118:80/manual/de/platform/windows.html.en
- http://129.105.46.118:80/manual/de/platform/netware.html.en

Summary: A serious vulnerability has been detected within your web application due to the discovery of a fully qualified path name to the root of your system. This most often occurs in context of an error being produced by the web application. Fully qualified server path names allow an attacker to know the file system structure of the web server, which is a baseline for many other types of attacks to be successful. Recommendations include adopting a consistent error handling scheme and mechanism that prevents fully qualified path names from being displayed.

Fix:

For Development:

Don't display fully qualified pathnames as part of error or informational messages. At the least, fully qualified pathnames can provide an attacker with important information about the architecture of web application.

For Security Operations:

The following recommendations will help to ensure that a potential attacker is not deriving valuable information from any error message that is presented.

- Uniform Error Codes: Ensure that you are not inadvertently supplying information to an attacker via the use of inconsistent or "conflicting" error messages. For instance, don't reveal unintended information by utilizing error messages such as Access Denied, which will also let an attacker know that the file he seeks actually exists. Have consistent terminology for files and folders that do exist, do not exist, and which have read access denied.
- Informational Error Messages: Ensure that error messages do not reveal too much information. Complete or partial paths, variable and file names, row and column names in tables, and specific database errors should never be revealed to the end user. Remember, an attacker will gather as much information as possible, and then add pieces of seemingly innocuous information together to craft a method of attack.
- Proper Error Handling: Utilize generic error pages and error handling logic to inform end users of potential problems. Do not provide system information or other data that could be utilized by an attacker when orchestrating an attack.

For QA:

In reality, simple testing can usually determine how your web application will react to different input errors. More expansive testing must be conducted to cause internal errors to gauge the reaction of the site.

The best course of action for QA associates to take is to ensure that the error handling scheme is consistent. Do you receive a different type of error for a file that does not exist as opposed to a file that does? Are phrases like "Permission Denied" utilized which could reveal the existence of a file to an attacker? It is often a seemingly innocuous piece of information that provides an attacker with the means to discover something else which he can then utilize when conducting an attack.

Attack Request:

```
GET /manual/mod/mod_cache.html.en HTTP/1.1
Referer: http://129.105.46.118:80/manual/mod/mod_cache.html
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)
Pragma: no-cache
Host: 129.105.46.118
Connection: Keep-Alive
Cookie:
CustomCookie=WebInspect15804ZX5968C937BF2F4C00B8CA168F18502748YF85E;PHPSESSID=0286af493a
cdaf996469d378e8cb3ea1;
```

Attack Response:

```
HTTP/1.1 200 OK
Date: Tue, 28 Aug 2007 09:50:11 GMT
Server: Apache/2.0.54 (Unix) mod_ssl/2.0.54 OpenSSL/0.9.7e DAV/2 PHP/4.3.10
Last-Modified: Mon, 11 Apr 2005 15:10:57 GMT
ETag: "1cfb-67ce-953b2240"
Accept-Ranges: bytes
Content-Length: 26574
Connection: close
Content-Type: text/html
Content-Language: en

<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" lang="en" xml:lang="en"><head><!--
      XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
            This file is generated from xml source: DO NOT EDIT
      XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
    -->
<title>mod_cache - Apache HTTP Server</title>
<link href="../style/css/manual.css" rel="stylesheet" media="all" type="text/css" title="Main stylesheet" />
<link href="../style/css/manual-loose-100pc.css" rel="alternate stylesheet" media="all" type="text/css"
title="No Sidebar - Default font size" />
<link href="../style/css/manual-print.css" rel="stylesheet" media="print" type="text/css" />
<link href="../images/favicon.ico" rel="shortcut icon" /></head>
<body>
<div id="page-header">
<p class="menu"><a href="../mod/">Modules</a> | <a href="../mod/directives.html">Directives</a> |
<a href="../faq/">FAQ</a> | <a href="../glossary.html">Glossary</a> | <a
href="../sitemap.html">Sitemap</a></p>
<p class="apache">Apache HTTP Server Version 2.0</p>
<img alt="" src="../images/feather.gif" /></div>
<div class="up"><a href="./"><img title="&lt;-" alt="&lt;-" src="../images/left.gif" /></a></div>
<div id="path">
<a href="http://www.apache.org/">Apache</a> &gt; <a href="http://httpd.apache.org/">HTTP
Server</a> &gt; <a href="http://httpd.apache.org/docs-project/">Documentation</a> &gt; <a
href="../">Version 2.0</a> &gt; <a href="./">Modules</a></div>
<div id="page-content">
<div id="preamble"><h1>Apache Module mod_cache</h1>
<div class="toplang">
<p><span>Available  ... {content removed}
```

Medium **Possible Server Path Disclosure (unix)**

File Names:

- http://129.105.46.118:80/manual/fr/glossary.html
- http://129.105.46.118:80/manual/es/logs.html
- http://129.105.46.118:80/manual/es/urlmapping.html
- http://129.105.46.118:80/manual/es/misc/security_tips.html
- http://129.105.46.118:80/manual/de/sections.html
- http://129.105.46.118:80/manual/es/install.html
- http://129.105.46.118:80/manual/es/invoking.html
- http://129.105.46.118:80/manual/es/stopping.html
- http://129.105.46.118:80/manual/es/mod/quickreference.html
- http://129.105.46.118:80/manual/fr/invoking.html
- http://129.105.46.118:80/manual/fr/stopping.html
- http://129.105.46.118:80/manual/es/suexec.html
- http://129.105.46.118:80/manual/es/vhosts/
- http://129.105.46.118:80/manual/es/howto/auth.html
- http://129.105.46.118:80/manual/es/howto/cgi.html
- http://129.105.46.118:80/manual/fr/install.html
- http://129.105.46.118:80/manual/fr/logs.html
- http://129.105.46.118:80/manual/fr/urlmapping.html
- http://129.105.46.118:80/manual/fr/misc/security_tips.html
- http://129.105.46.118:80/manual/fr/suexec.html
- http://129.105.46.118:80/manual/ja/glossary.html
- http://129.105.46.118:80/manual/fr/vhosts/
- http://129.105.46.118:80/manual/fr/howto/auth.html
- http://129.105.46.118:80/manual/fr/howto/cgi.html
- http://129.105.46.118:80/manual/en/install.html
- http://129.105.46.118:80/manual/en/invoking.html
- http://129.105.46.118:80/manual/en/stopping.html

- http://129.105.46.118:80/manual/en/mod/quickreference.html
- http://129.105.46.118:80/manual/en/vhosts/
- http://129.105.46.118:80/manual/en/howto/auth.html
- http://129.105.46.118:80/manual/en/howto/cgi.html
- http://129.105.46.118:80/manual/en/sections.html
- http://129.105.46.118:80/manual/en/logs.html
- http://129.105.46.118:80/manual/en/urlmapping.html
- http://129.105.46.118:80/manual/en/misc/security_tips.html
- http://129.105.46.118:80/manual/en/suexec.html
- http://129.105.46.118:80/manual/de/logs.html
- http://129.105.46.118:80/manual/de/urlmapping.html
- http://129.105.46.118:80/manual/de/misc/security_tips.html
- http://129.105.46.118:80/manual/de/suexec.html
- http://129.105.46.118:80/manual/de/vhosts/
- http://129.105.46.118:80/manual/de/howto/auth.html
- http://129.105.46.118:80/manual/de/howto/cgi.html
- http://129.105.46.118:80/manual/de/mod/quickreference.html
- http://129.105.46.118:80/manual/misc/descriptors.html
- http://129.105.46.118:80/manual/mod/directive-dict.html
- http://129.105.46.118:80/manual/install.html
- http://129.105.46.118:80/manual/invoking.html
- http://129.105.46.118:80/manual/stopping.html
- http://129.105.46.118:80/manual/mod/quickreference.html
- http://129.105.46.118:80/manual/glossary.html
- http://129.105.46.118:80/manual/mod/mod_alias.html
- http://129.105.46.118:80/manual/mod/mod_proxy.html
- http://129.105.46.118:80/manual/sections.html
- http://129.105.46.118:80/manual/logs.html
- http://129.105.46.118:80/manual/urlmapping.html
- http://129.105.46.118:80/manual/misc/security_tips.html
- http://129.105.46.118:80/manual/suexec.html
- http://129.105.46.118:80/manual/vhosts/
- http://129.105.46.118:80/manual/howto/auth.html
- http://129.105.46.118:80/manual/howto/cgi.html
- http://129.105.46.118:80/manual/faq/all_in_one.html
- http://129.105.46.118:80/manual/faq/support.html
- http://129.105.46.118:80/manual/mod/mod_rewrite.html
- http://129.105.46.118:80/manual/mod/mod_ext_filter.html
- http://129.105.46.118:80/manual/mod/mod_dav.html
- http://129.105.46.118:80/manual/mod/mod_vhost_alias.html
- http://129.105.46.118:80/manual/de/glossary.html
- http://129.105.46.118:80/manual/en/glossary.html
- http://129.105.46.118:80/manual/es/glossary.html
- http://129.105.46.118:80/manual/ko/glossary.html
- http://129.105.46.118:80/manual/programs/apxs.html
- http://129.105.46.118:80/manual/programs/httpd.html
- http://129.105.46.118:80/manual/custom-error.html
- http://129.105.46.118:80/manual/programs/configure.html
- http://129.105.46.118:80/manual/ssl/ssl_faq.html
- http://129.105.46.118:80/manual/programs/htpasswd.html
- http://129.105.46.118:80/manual/de/install.html
- http://129.105.46.118:80/manual/de/invoking.html
- http://129.105.46.118:80/manual/de/stopping.html
- http://129.105.46.118:80/manual/glossary.html.en
- http://129.105.46.118:80/manual/mod/mod_ssl.html
- http://129.105.46.118:80/manual/mod/mod_file_cache.html
- http://129.105.46.118:80/manual/dns-caveats.html
- http://129.105.46.118:80/manual/ssl/ssl_howto.html
- http://129.105.46.118:80/manual/developer/thread_safety.html
- http://129.105.46.118:80/manual/vhosts/index.html.en
- http://129.105.46.118:80/manual/howto/auth.html.en
- http://129.105.46.118:80/manual/howto/cgi.html.en
- http://129.105.46.118:80/manual/de/mod/mod_proxy.html
- http://129.105.46.118:80/manual/de/mod/mod_ext_filter.html
- http://129.105.46.118:80/manual/de/mod/mod_dav.html
- http://129.105.46.118:80/manual/de/mod/mod_alias.html
- http://129.105.46.118:80/manual/en/mod/mod_proxy.html
- http://129.105.46.118:80/manual/en/mod/mod_ext_filter.html
- http://129.105.46.118:80/manual/en/mod/mod_dav.html
- http://129.105.46.118:80/manual/de/mod/mod_rewrite.html
- http://129.105.46.118:80/manual/de/mod/mod_ssl.html
- http://129.105.46.118:80/manual/de/mod/mod_vhost_alias.html
- http://129.105.46.118:80/manual/de/mod/mod_file_cache.html
- http://129.105.46.118:80/manual/en/mod/mod_alias.html
- http://129.105.46.118:80/manual/ja/mod/mod_proxy.html
- http://129.105.46.118:80/manual/ja/mod/mod_rewrite.html
- http://129.105.46.118:80/manual/de/mod/directive-dict.html
- http://129.105.46.118:80/manual/ja/mod/mod_ext_filter.html
- http://129.105.46.118:80/manual/ja/mod/mod_dav.html

- http://129.105.46.118:80/manual/es/mod/mod_vhost_alias.html
- http://129.105.46.118:80/manual/ja/mod/mod_alias.html
- http://129.105.46.118:80/manual/es/mod/mod_rewrite.html
- http://129.105.46.118:80/manual/es/mod/mod_ssl.html
- http://129.105.46.118:80/manual/es/mod/mod_proxy.html
- http://129.105.46.118:80/manual/es/mod/mod_ext_filter.html
- http://129.105.46.118:80/manual/en/mod/mod_file_cache.html
- http://129.105.46.118:80/manual/es/mod/mod_file_cache.html
- http://129.105.46.118:80/manual/en/mod/mod_vhost_alias.html
- http://129.105.46.118:80/manual/es/mod/mod_dav.html
- http://129.105.46.118:80/manual/es/mod/mod_alias.html
- http://129.105.46.118:80/manual/en/mod/mod_rewrite.html
- http://129.105.46.118:80/manual/en/mod/mod_ssl.html
- http://129.105.46.118:80/manual/ru/mod/quickreference.html
- http://129.105.46.118:80/manual/ru/logs.html
- http://129.105.46.118:80/manual/ru/urlmapping.html
- http://129.105.46.118:80/manual/ru/misc/security_tips.html
- http://129.105.46.118:80/manual/ru/suexec.html
- http://129.105.46.118:80/manual/ru/vhosts/
- http://129.105.46.118:80/manual/ru/howto/auth.html
- http://129.105.46.118:80/manual/ru/howto/cgi.html
- http://129.105.46.118:80/manual/ko/howto/auth.html
- http://129.105.46.118:80/manual/ko/howto/cgi.html
- http://129.105.46.118:80/manual/es/sections.html
- http://129.105.46.118:80/manual/fr/sections.html
- http://129.105.46.118:80/manual/ja/sections.html
- http://129.105.46.118:80/manual/install.html.en
- http://129.105.46.118:80/manual/invoking.html.en
- http://129.105.46.118:80/manual/stopping.html.en
- http://129.105.46.118:80/manual/mod/quickreference.html.en
- http://129.105.46.118:80/manual/ru/sections.html
- http://129.105.46.118:80/manual/suexec.html.en
- http://129.105.46.118:80/manual/sections.html.en
- http://129.105.46.118:80/manual/logs.html.en
- http://129.105.46.118:80/manual/urlmapping.html.en
- http://129.105.46.118:80/manual/misc/security_tips.html.en
- http://129.105.46.118:80/manual/fr/mod/quickreference.html
- http://129.105.46.118:80/manual/ja/install.html
- http://129.105.46.118:80/manual/ja/invoking.html
- http://129.105.46.118:80/manual/ja/stopping.html
- http://129.105.46.118:80/manual/ko/install.html
- http://129.105.46.118:80/manual/ja/mod/quickreference.html
- http://129.105.46.118:80/manual/ko/invoking.html
- http://129.105.46.118:80/manual/ko/stopping.html
- http://129.105.46.118:80/manual/ko/mod/quickreference.html
- http://129.105.46.118:80/manual/ru/glossary.html
- http://129.105.46.118:80/manual/ja/logs.html
- http://129.105.46.118:80/manual/ko/sections.html
- http://129.105.46.118:80/manual/ja/urlmapping.html
- http://129.105.46.118:80/manual/ja/misc/security_tips.html
- http://129.105.46.118:80/manual/ja/suexec.html
- http://129.105.46.118:80/manual/ko/logs.html
- http://129.105.46.118:80/manual/ko/urlmapping.html
- http://129.105.46.118:80/manual/ja/vhosts/
- http://129.105.46.118:80/manual/ja/howto/auth.html
- http://129.105.46.118:80/manual/ko/misc/security_tips.html
- http://129.105.46.118:80/manual/ja/howto/cgi.html
- http://129.105.46.118:80/manual/ru/install.html
- http://129.105.46.118:80/manual/ru/invoking.html
- http://129.105.46.118:80/manual/ru/stopping.html
- http://129.105.46.118:80/manual/ko/suexec.html
- http://129.105.46.118:80/manual/ko/vhosts/
- http://129.105.46.118:80/manual/mod/mod_ext_filter.html.en
- http://129.105.46.118:80/manual/mod/mod_ssl.html.en
- http://129.105.46.118:80/manual/de/dns-caveats.html
- http://129.105.46.118:80/manual/de/faq/support.html
- http://129.105.46.118:80/manual/en/custom-error.html
- http://129.105.46.118:80/manual/de/ssl/ssl_howto.html
- http://129.105.46.118:80/manual/de/ssl/ssl_faq.html
- http://129.105.46.118:80/manual/en/dns-caveats.html
- http://129.105.46.118:80/manual/en/ssl/ssl_howto.html
- http://129.105.46.118:80/manual/es/dns-caveats.html
- http://129.105.46.118:80/manual/en/ssl/ssl_faq.html
- http://129.105.46.118:80/manual/es/faq/support.html
- http://129.105.46.118:80/manual/de/programs/configure.html
- http://129.105.46.118:80/manual/es/ssl/ssl_howto.html
- http://129.105.46.118:80/manual/de/programs/htpasswd.html
- http://129.105.46.118:80/manual/en/programs/configure.html
- http://129.105.46.118:80/manual/en/programs/htpasswd.html

- http://129.105.46.118:80/manual/de/misc/descriptors.html
- http://129.105.46.118:80/manual/es/programs/httpd.html
- http://129.105.46.118:80/manual/en/misc/descriptors.html
- http://129.105.46.118:80/manual/es/programs/configure.html
- http://129.105.46.118:80/manual/es/programs/htpasswd.html
- http://129.105.46.118:80/manual/es/misc/descriptors.html
- http://129.105.46.118:80/manual/programs/httpd.html.en
- http://129.105.46.118:80/manual/ko/programs/httpd.html
- http://129.105.46.118:80/manual/ko/custom-error.html
- http://129.105.46.118:80/manual/es/ssl/ssl_faq.html
- http://129.105.46.118:80/manual/ja/dns-caveats.html
- http://129.105.46.118:80/manual/ja/faq/support.html
- http://129.105.46.118:80/manual/ko/dns-caveats.html
- http://129.105.46.118:80/manual/custom-error.html.en
- http://129.105.46.118:80/manual/ja/ssl/ssl_howto.html
- http://129.105.46.118:80/manual/ja/ssl/ssl_faq.html
- http://129.105.46.118:80/manual/ko/ssl/ssl_howto.html
- http://129.105.46.118:80/manual/ko/ssl/ssl_faq.html
- http://129.105.46.118:80/manual/ja/programs/httpd.html
- http://129.105.46.118:80/manual/ja/programs/apxs.html
- http://129.105.46.118:80/manual/ja/programs/configure.html
- http://129.105.46.118:80/manual/ja/programs/htpasswd.html
- http://129.105.46.118:80/manual/ko/programs/configure.html
- http://129.105.46.118:80/manual/ko/programs/htpasswd.html
- http://129.105.46.118:80/manual/ja/misc/descriptors.html
- http://129.105.46.118:80/manual/ko/misc/descriptors.html
- http://129.105.46.118:80/manual/fr/custom-error.html
- http://129.105.46.118:80/manual/dns-caveats.html.en
- http://129.105.46.118:80/manual/mod/mod_file_cache.html.en
- http://129.105.46.118:80/manual/ko/mod/mod_proxy.html
- http://129.105.46.118:80/manual/ko/mod/mod_ext_filter.html
- http://129.105.46.118:80/manual/ko/mod/mod_rewrite.html
- http://129.105.46.118:80/manual/ko/mod/mod_ssl.html
- http://129.105.46.118:80/manual/ko/mod/mod_dav.html
- http://129.105.46.118:80/manual/ja/mod/mod_file_cache.html
- http://129.105.46.118:80/manual/ko/mod/mod_alias.html
- http://129.105.46.118:80/manual/ja/mod/mod_ssl.html
- http://129.105.46.118:80/manual/ja/mod/mod_vhost_alias.html
- http://129.105.46.118:80/manual/ru/mod/mod_file_cache.html
- http://129.105.46.118:80/manual/ru/mod/mod_dav.html
- http://129.105.46.118:80/manual/ru/mod/mod_ext_filter.html
- http://129.105.46.118:80/manual/ru/mod/mod_alias.html
- http://129.105.46.118:80/manual/ko/mod/mod_vhost_alias.html
- http://129.105.46.118:80/manual/en/mod/directive-dict.html
- http://129.105.46.118:80/manual/es/mod/directive-dict.html
- http://129.105.46.118:80/manual/ko/mod/directive-dict.html
- http://129.105.46.118:80/manual/ru/mod/directive-dict.html
- http://129.105.46.118:80/manual/ja/mod/directive-dict.html
- http://129.105.46.118:80/manual/en/faq/all_in_one.html
- http://129.105.46.118:80/manual/en/faq/support.html
- http://129.105.46.118:80/manual/ko/faq/all_in_one.html
- http://129.105.46.118:80/manual/ko/faq/support.html
- http://129.105.46.118:80/manual/faq/all_in_one.html.en
- http://129.105.46.118:80/manual/faq/support.html.en
- http://129.105.46.118:80/manual/mod/mod_rewrite.html.en
- http://129.105.46.118:80/manual/mod/mod_vhost_alias.html.en
- http://129.105.46.118:80/manual/de/glossary.html.de
- http://129.105.46.118:80/manual/en/glossary.html.en
- http://129.105.46.118:80/manual/de/programs/apxs.html
- http://129.105.46.118:80/manual/en/programs/apxs.html
- http://129.105.46.118:80/manual/de/programs/httpd.html
- http://129.105.46.118:80/manual/en/programs/httpd.html
- http://129.105.46.118:80/manual/ko/glossary.html.ko.euc-kr
- http://129.105.46.118:80/manual/es/programs/apxs.html
- http://129.105.46.118:80/manual/ko/programs/apxs.html
- http://129.105.46.118:80/manual/programs/apxs.html.en
- http://129.105.46.118:80/manual/de/custom-error.html
- http://129.105.46.118:80/manual/mod/directive-dict.html.en
- http://129.105.46.118:80/manual/ru/mod/mod_proxy.html
- http://129.105.46.118:80/manual/ru/mod/mod_rewrite.html
- http://129.105.46.118:80/manual/ru/mod/mod_ssl.html
- http://129.105.46.118:80/manual/mod/mod_dav.html.en
- http://129.105.46.118:80/manual/mod/mod_alias.html.en
- http://129.105.46.118:80/manual/mod/mod_proxy.html.en
- http://129.105.46.118:80/manual/ko/mod/mod_file_cache.html
- http://129.105.46.118:80/manual/ru/mod/mod_vhost_alias.html
- http://129.105.46.118:80/manual/de/developer/thread_safety.html
- http://129.105.46.118:80/manual/programs/htpasswd.html.en
- http://129.105.46.118:80/manual/de/install.html.de

- http://129.105.46.118:80/manual/de/invoking.html.de
- http://129.105.46.118:80/manual/de/stopping.html.de
- http://129.105.46.118:80/manual/de/mod/quickreference.html.de
- http://129.105.46.118:80/manual/misc/descriptors.html.en
- http://129.105.46.118:80/manual/en/install.html.en
- http://129.105.46.118:80/manual/en/invoking.html.en
- http://129.105.46.118:80/manual/en/stopping.html.en
- http://129.105.46.118:80/manual/en/mod/quickreference.html.en
- http://129.105.46.118:80/manual/ssl/ssl_faq.html.en
- http://129.105.46.118:80/manual/en/sections.html.en
- http://129.105.46.118:80/manual/en/logs.html.en
- http://129.105.46.118:80/manual/de/faq/all_in_one.html
- http://129.105.46.118:80/manual/programs/configure.html.en
- http://129.105.46.118:80/manual/fr/dns-caveats.html
- http://129.105.46.118:80/manual/ssl/ssl_howto.html.en
- http://129.105.46.118:80/manual/de/sections.html.en
- http://129.105.46.118:80/manual/de/logs.html.en
- http://129.105.46.118:80/manual/de/urlmapping.html.en
- http://129.105.46.118:80/manual/de/misc/security_tips.html.en
- http://129.105.46.118:80/manual/de/suexec.html.en
- http://129.105.46.118:80/manual/de/vhosts/index.html.de
- http://129.105.46.118:80/manual/de/howto/auth.html.en
- http://129.105.46.118:80/manual/de/howto/cgi.html.en
- http://129.105.46.118:80/manual/en/developer/thread_safety.html
- http://129.105.46.118:80/manual/fr/mod/mod_ext_filter.html
- http://129.105.46.118:80/manual/fr/mod/mod_dav.html
- http://129.105.46.118:80/manual/en/urlmapping.html.en
- http://129.105.46.118:80/manual/en/misc/security_tips.html.en
- http://129.105.46.118:80/manual/es/faq/all_in_one.html
- http://129.105.46.118:80/manual/en/suexec.html.en
- http://129.105.46.118:80/manual/en/vhosts/index.html.en
- http://129.105.46.118:80/manual/en/howto/auth.html.en
- http://129.105.46.118:80/manual/en/howto/cgi.html.en
- http://129.105.46.118:80/manual/fr/mod/mod_alias.html
- http://129.105.46.118:80/manual/fr/mod/mod_file_cache.html
- http://129.105.46.118:80/manual/fr/mod/directive-dict.html
- http://129.105.46.118:80/manual/fr/mod/mod_proxy.html
- http://129.105.46.118:80/manual/fr/mod/mod_rewrite.html
- http://129.105.46.118:80/manual/fr/mod/mod_ssl.html
- http://129.105.46.118:80/manual/fr/mod/mod_vhost_alias.html
- http://129.105.46.118:80/manual/fr/faq/all_in_one.html
- http://129.105.46.118:80/manual/fr/faq/support.html
- http://129.105.46.118:80/manual/fr/glossary.html.en
- http://129.105.46.118:80/manual/fr/programs/apxs.html
- http://129.105.46.118:80/manual/fr/programs/httpd.html
- http://129.105.46.118:80/manual/fr/mod/quickreference.html.en
- http://129.105.46.118:80/manual/es/developer/thread_safety.html
- http://129.105.46.118:80/manual/fr/ssl/ssl_howto.html
- http://129.105.46.118:80/manual/fr/ssl/ssl_faq.html
- http://129.105.46.118:80/manual/es/sections.html.en
- http://129.105.46.118:80/manual/fr/programs/configure.html
- http://129.105.46.118:80/manual/fr/programs/htpasswd.html
- http://129.105.46.118:80/manual/fr/misc/descriptors.html
- http://129.105.46.118:80/manual/es/urlmapping.html.en
- http://129.105.46.118:80/manual/es/misc/security_tips.html.en
- http://129.105.46.118:80/manual/es/suexec.html.en
- http://129.105.46.118:80/manual/es/howto/auth.html.en
- http://129.105.46.118:80/manual/es/howto/cgi.html.en
- http://129.105.46.118:80/manual/fr/install.html.en
- http://129.105.46.118:80/manual/fr/developer/thread_safety.html
- http://129.105.46.118:80/manual/fr/invoking.html.en
- http://129.105.46.118:80/manual/fr/stopping.html.en
- http://129.105.46.118:80/manual/fr/sections.html.en
- http://129.105.46.118:80/manual/fr/logs.html.en
- http://129.105.46.118:80/manual/fr/urlmapping.html.en
- http://129.105.46.118:80/manual/fr/suexec.html.en
- http://129.105.46.118:80/manual/ja/faq/all_in_one.html
- http://129.105.46.118:80/manual/fr/vhosts/index.html.en
- http://129.105.46.118:80/manual/ja/glossary.html.en
- http://129.105.46.118:80/manual/fr/howto/auth.html.en
- http://129.105.46.118:80/manual/fr/howto/cgi.html.en
- http://129.105.46.118:80/manual/fr/misc/security_tips.html.en
- http://129.105.46.118:80/manual/ru/dns-caveats.html
- http://129.105.46.118:80/manual/ru/ssl/ssl_howto.html
- http://129.105.46.118:80/manual/ru/ssl/ssl_faq.html
- http://129.105.46.118:80/manual/ja/logs.html.ja.euc-jp
- http://129.105.46.118:80/manual/ko/sections.html.ko.euc-kr
- http://129.105.46.118:80/manual/ja/urlmapping.html.ja.euc-jp
- http://129.105.46.118:80/manual/ja/misc/security_tips.html.en

- http://129.105.46.118:80/manual/ja/suexec.html.ja.euc-jp
- http://129.105.46.118:80/manual/ko/logs.html.ko.euc-kr
- http://129.105.46.118:80/manual/ko/urlmapping.html.ko.euc-kr
- http://129.105.46.118:80/manual/ja/invoking.html.ja.euc-jp
- http://129.105.46.118:80/manual/ja/install.html.ja.euc-jp
- http://129.105.46.118:80/manual/ja/stopping.html.ja.euc-jp
- http://129.105.46.118:80/manual/ko/install.html.ko.euc-kr
- http://129.105.46.118:80/manual/ko/invoking.html.ko.euc-kr
- http://129.105.46.118:80/manual/ja/mod/quickreference.html.ja.euc-jp
- http://129.105.46.118:80/manual/ko/stopping.html.ko.euc-kr
- http://129.105.46.118:80/manual/ru/faq/all_in_one.html
- http://129.105.46.118:80/manual/ko/mod/quickreference.html.ko.euc-kr
- http://129.105.46.118:80/manual/ru/faq/support.html
- http://129.105.46.118:80/manual/ru/glossary.html.en
- http://129.105.46.118:80/manual/ru/programs/apxs.html
- http://129.105.46.118:80/manual/ru/programs/httpd.html
- http://129.105.46.118:80/manual/ru/custom-error.html
- http://129.105.46.118:80/manual/ru/mod/quickreference.html.ru.koi8-r
- http://129.105.46.118:80/manual/ko/howto/auth.html.ko.euc-kr
- http://129.105.46.118:80/manual/ko/howto/cgi.html.ko.euc-kr
- http://129.105.46.118:80/manual/ja/developer/thread_safety.html
- http://129.105.46.118:80/manual/ru/programs/configure.html
- http://129.105.46.118:80/manual/ru/programs/htpasswd.html
- http://129.105.46.118:80/manual/ru/misc/descriptors.html
- http://129.105.46.118:80/manual/ja/sections.html.ja.euc-jp
- http://129.105.46.118:80/manual/ja/vhosts/index.html.ja.euc-jp
- http://129.105.46.118:80/manual/ja/howto/auth.html.ja.euc-jp
- http://129.105.46.118:80/manual/ko/misc/security_tips.html.ko.euc-kr
- http://129.105.46.118:80/manual/ja/howto/cgi.html.ja.euc-jp
- http://129.105.46.118:80/manual/ru/install.html.ru.koi8-r
- http://129.105.46.118:80/manual/ru/invoking.html.ru.koi8-r
- http://129.105.46.118:80/manual/ru/stopping.html.ru.koi8-r
- http://129.105.46.118:80/manual/ko/suexec.html.ko.euc-kr
- http://129.105.46.118:80/manual/ko/vhosts/index.html.ko.euc-kr
- http://129.105.46.118:80/manual/ru/developer/thread_safety.html
- http://129.105.46.118:80/manual/developer/thread_safety.html.en
- http://129.105.46.118:80/manual/ru/sections.html.en
- http://129.105.46.118:80/manual/ko/developer/thread_safety.html
- http://129.105.46.118:80/manual/ru/logs.html.en
- http://129.105.46.118:80/manual/ru/urlmapping.html.en
- http://129.105.46.118:80/manual/ru/misc/security_tips.html.en
- http://129.105.46.118:80/manual/ru/suexec.html.en
- http://129.105.46.118:80/manual/ru/vhosts/index.html.ru.koi8-r
- http://129.105.46.118:80/manual/ru/howto/auth.html.en
- http://129.105.46.118:80/manual/ru/howto/cgi.html.en
- http://129.105.46.118:80/manual/de/mod/mod_proxy.html.en
- http://129.105.46.118:80/manual/de/mod/mod_rewrite.html.en
- http://129.105.46.118:80/manual/de/mod/mod_ssl.html.en
- http://129.105.46.118:80/manual/de/mod/mod_vhost_alias.html.en
- http://129.105.46.118:80/manual/de/mod/mod_ext_filter.html.en
- http://129.105.46.118:80/manual/de/mod/mod_alias.html.en
- http://129.105.46.118:80/manual/de/mod/mod_file_cache.html.en
- http://129.105.46.118:80/manual/de/mod/mod_dav.html.en
- http://129.105.46.118:80/manual/en/mod/mod_proxy.html.en
- http://129.105.46.118:80/manual/en/mod/mod_ext_filter.html.en
- http://129.105.46.118:80/manual/en/mod/mod_dav.html.en
- http://129.105.46.118:80/manual/en/mod/mod_vhost_alias.html.en
- http://129.105.46.118:80/manual/es/mod/mod_dav.html.en
- http://129.105.46.118:80/manual/en/mod/mod_alias.html.en
- http://129.105.46.118:80/manual/en/mod/mod_file_cache.html.en
- http://129.105.46.118:80/manual/es/mod/mod_alias.html.en
- http://129.105.46.118:80/manual/en/mod/mod_rewrite.html.en
- http://129.105.46.118:80/manual/ko/mod/mod_dav.html.ko.euc-kr
- http://129.105.46.118:80/manual/ja/mod/mod_vhost_alias.html.en
- http://129.105.46.118:80/manual/ja/mod/mod_rewrite.html.en
- http://129.105.46.118:80/manual/ja/mod/mod_ssl.html.en
- http://129.105.46.118:80/manual/ja/mod/mod_proxy.html.en
- http://129.105.46.118:80/manual/es/mod/mod_file_cache.html.en
- http://129.105.46.118:80/manual/ja/mod/mod_file_cache.html.en
- http://129.105.46.118:80/manual/de/mod/directive-dict.html.en
- http://129.105.46.118:80/manual/ja/mod/mod_ext_filter.html.en
- http://129.105.46.118:80/manual/ja/mod/mod_dav.html.ja.euc-jp
- http://129.105.46.118:80/manual/es/mod/mod_vhost_alias.html.en
- http://129.105.46.118:80/manual/ja/mod/mod_alias.html.ja.euc-jp
- http://129.105.46.118:80/manual/es/mod/mod_rewrite.html.en
- http://129.105.46.118:80/manual/es/mod/mod_ssl.html.en
- http://129.105.46.118:80/manual/es/mod/mod_proxy.html.en
- http://129.105.46.118:80/manual/es/mod/mod_ext_filter.html.en
- http://129.105.46.118:80/manual/en/mod/mod_ssl.html.en

- http://129.105.46.118:80/manual/ru/mod/mod_rewrite.html.en
- http://129.105.46.118:80/manual/ru/mod/mod_proxy.html.en
- http://129.105.46.118:80/manual/ru/mod/mod_file_cache.html.en
- http://129.105.46.118:80/manual/ru/mod/mod_dav.html.en
- http://129.105.46.118:80/manual/ru/mod/mod_ext_filter.html.en
- http://129.105.46.118:80/manual/ru/mod/mod_vhost_alias.html.en
- http://129.105.46.118:80/manual/en/faq/all_in_one.html.en
- http://129.105.46.118:80/manual/en/faq/support.html.en
- http://129.105.46.118:80/manual/ko/faq/all_in_one.html.ko.euc-kr
- http://129.105.46.118:80/manual/ko/faq/support.html.ko.euc-kr
- http://129.105.46.118:80/manual/de/programs/apxs.html.en
- http://129.105.46.118:80/manual/en/programs/apxs.html.en
- http://129.105.46.118:80/manual/de/programs/httpd.html.en
- http://129.105.46.118:80/manual/en/programs/httpd.html.en
- http://129.105.46.118:80/manual/es/programs/apxs.html.en
- http://129.105.46.118:80/manual/ko/programs/apxs.html.ko.euc-kr
- http://129.105.46.118:80/manual/de/custom-error.html.en
- http://129.105.46.118:80/manual/ko/mod/mod_proxy.html.en
- http://129.105.46.118:80/manual/ko/mod/mod_rewrite.html.en
- http://129.105.46.118:80/manual/ko/mod/mod_ext_filter.html.ko.euc-kr
- http://129.105.46.118:80/manual/ko/mod/mod_alias.html.ko.euc-kr
- http://129.105.46.118:80/manual/ko/mod/mod_file_cache.html.ko.euc-kr
- http://129.105.46.118:80/manual/ru/mod/mod_alias.html.en
- http://129.105.46.118:80/manual/ko/mod/mod_ssl.html.en
- http://129.105.46.118:80/manual/ko/mod/mod_vhost_alias.html.en
- http://129.105.46.118:80/manual/en/mod/directive-dict.html.en
- http://129.105.46.118:80/manual/ja/mod/directive-dict.html.ja.euc-jp
- http://129.105.46.118:80/manual/ko/mod/directive-dict.html.ko.euc-kr
- http://129.105.46.118:80/manual/ru/mod/directive-dict.html.en
- http://129.105.46.118:80/manual/fr/mod/mod_ext_filter.html.en
- http://129.105.46.118:80/manual/fr/mod/mod_alias.html.en
- http://129.105.46.118:80/manual/fr/mod/mod_file_cache.html.en
- http://129.105.46.118:80/manual/fr/mod/mod_dav.html.en
- http://129.105.46.118:80/manual/fr/custom-error.html.fr
- http://129.105.46.118:80/manual/fr/mod/directive-dict.html.en
- http://129.105.46.118:80/manual/fr/mod/mod_proxy.html.en
- http://129.105.46.118:80/manual/fr/mod/mod_rewrite.html.en
- http://129.105.46.118:80/manual/fr/mod/mod_ssl.html.en
- http://129.105.46.118:80/manual/ja/faq/all_in_one.html.en
- http://129.105.46.118:80/manual/fr/developer/thread_safety.html.en
- http://129.105.46.118:80/manual/ru/faq/all_in_one.html.en
- http://129.105.46.118:80/manual/ru/faq/support.html.en
- http://129.105.46.118:80/manual/ru/programs/apxs.html.en
- http://129.105.46.118:80/manual/ru/programs/httpd.html.en
- http://129.105.46.118:80/manual/ru/custom-error.html.en
- http://129.105.46.118:80/manual/fr/mod/mod_vhost_alias.html.en
- http://129.105.46.118:80/manual/fr/faq/all_in_one.html.en
- http://129.105.46.118:80/manual/fr/faq/support.html.en
- http://129.105.46.118:80/manual/fr/programs/apxs.html.en
- http://129.105.46.118:80/manual/fr/programs/httpd.html.en
- http://129.105.46.118:80/manual/fr/ssl/ssl_howto.html.en
- http://129.105.46.118:80/manual/fr/ssl/ssl_faq.html.en
- http://129.105.46.118:80/manual/ru/programs/configure.html.en
- http://129.105.46.118:80/manual/ru/programs/htpasswd.html.en
- http://129.105.46.118:80/manual/ru/misc/descriptors.html.en
- http://129.105.46.118:80/manual/ja/developer/thread_safety.html.en
- http://129.105.46.118:80/manual/ko/developer/thread_safety.html.en
- http://129.105.46.118:80/manual/ru/developer/thread_safety.html.en
- http://129.105.46.118:80/manual/fr/programs/configure.html.en
- http://129.105.46.118:80/manual/fr/programs/htpasswd.html.en
- http://129.105.46.118:80/manual/fr/misc/descriptors.html.en
- http://129.105.46.118:80/manual/es/developer/thread_safety.html.en
- http://129.105.46.118:80/manual/ru/dns-caveats.html.en
- http://129.105.46.118:80/manual/ru/ssl/ssl_howto.html.en
- http://129.105.46.118:80/manual/ru/ssl/ssl_faq.html.en
- http://129.105.46.118:80/manual/es/faq/all_in_one.html.en
- http://129.105.46.118:80/manual/en/developer/thread_safety.html.en
- http://129.105.46.118:80/manual/de/faq/all_in_one.html.en
- http://129.105.46.118:80/manual/de/developer/thread_safety.html.en
- http://129.105.46.118:80/manual/ko/ssl/ssl_howto.html.en
- http://129.105.46.118:80/manual/ko/ssl/ssl_faq.html.en
- http://129.105.46.118:80/manual/ja/dns-caveats.html.ja.euc-jp
- http://129.105.46.118:80/manual/ja/faq/support.html.en
- http://129.105.46.118:80/manual/ko/dns-caveats.html.ko.euc-kr
- http://129.105.46.118:80/manual/ja/ssl/ssl_howto.html.en
- http://129.105.46.118:80/manual/ja/ssl/ssl_faq.html.en
- http://129.105.46.118:80/manual/ja/programs/httpd.html.en
- http://129.105.46.118:80/manual/ja/programs/apxs.html.en
- http://129.105.46.118:80/manual/ja/programs/configure.html.en

- http://129.105.46.118:80/manual/ja/programs/htpasswd.html.en
- http://129.105.46.118:80/manual/ko/programs/configure.html.ko.euc-kr
- http://129.105.46.118:80/manual/ko/programs/htpasswd.html.ko.euc-kr
- http://129.105.46.118:80/manual/ja/misc/descriptors.html.en
- http://129.105.46.118:80/manual/ko/misc/descriptors.html.en
- http://129.105.46.118:80/manual/fr/dns-caveats.html.fr
- http://129.105.46.118:80/manual/ru/mod/mod_ssl.html.en
- http://129.105.46.118:80/manual/de/dns-caveats.html.en
- http://129.105.46.118:80/manual/de/faq/support.html.en
- http://129.105.46.118:80/manual/en/custom-error.html.en
- http://129.105.46.118:80/manual/de/ssl/ssl_howto.html.en
- http://129.105.46.118:80/manual/de/ssl/ssl_faq.html.en
- http://129.105.46.118:80/manual/en/dns-caveats.html.en
- http://129.105.46.118:80/manual/en/ssl/ssl_howto.html.en
- http://129.105.46.118:80/manual/es/dns-caveats.html.en
- http://129.105.46.118:80/manual/es/faq/support.html.en
- http://129.105.46.118:80/manual/de/programs/configure.html.en
- http://129.105.46.118:80/manual/es/ssl/ssl_howto.html.en
- http://129.105.46.118:80/manual/en/ssl/ssl_faq.html.en
- http://129.105.46.118:80/manual/es/ssl/ssl_faq.html.en
- http://129.105.46.118:80/manual/de/programs/htpasswd.html.en
- http://129.105.46.118:80/manual/en/programs/configure.html.en
- http://129.105.46.118:80/manual/en/programs/htpasswd.html.en
- http://129.105.46.118:80/manual/de/misc/descriptors.html.en
- http://129.105.46.118:80/manual/es/programs/httpd.html.en
- http://129.105.46.118:80/manual/en/misc/descriptors.html.en
- http://129.105.46.118:80/manual/es/programs/configure.html.en
- http://129.105.46.118:80/manual/es/programs/htpasswd.html.en
- http://129.105.46.118:80/manual/es/misc/descriptors.html.en
- http://129.105.46.118:80/manual/ko/programs/httpd.html.ko.euc-kr
- http://129.105.46.118:80/manual/ko/custom-error.html.ko.euc-kr
- http://129.105.46.118:80/test.php?=,`@^*$;#
- http://129.105.46.118:80/test.php?="
- http://129.105.46.118:80/test.php?=%0aA:B
- http://129.105.46.118:80/test.php?='
- http://129.105.46.118:80/test.php?=%00
- http://129.105.46.118:80/test.php?=%2500
- http://129.105.46.118:80/test.php?=%250a
- http://129.105.46.118:80/test.php?=/../../../../../../../../%2A
- http://129.105.46.118:80/test.php?=%2A
- http://129.105.46.118:80/test.php?=/%2A
- http://129.105.46.118:80/test.php?=/
- http://129.105.46.118:80/test.php?=/,%25ENV,/
- http://129.105.46.118:80/test.php?=http://www.spidynamics.com/
- http://129.105.46.118:80/test.php?=%0d%0aInjectedHeader:%20InjectedValue
- http://129.105.46.118:80/test.php?=())[]]{}}

Summary: A potential vulnerability has been discovered within your web application due to the the presence of a fully qualified path name to the root of your system. This most often occurs in context of an error being produced by the web application. Fully qualified server path names allow an attacker to know the file system structure of the web server, which is a baseline for many other types of attacks to be successful. Recommendations include adopting a consistent error handling scheme and mechanism that prevents fully qualified path names from being displayed.

Execution: To verify the issue, click the 'HTTP Response' button on the properties view and search for the keyword '/opt/'.

Fix:

For Development:

Don't display fully qualified pathnames as part of error or informational messages. At the least, fully qualified pathnames can provide an attacker with important information about the architecture of web application.

For Security Operations:

The following recommendations will help to ensure that a potential attacker is not deriving valuable information from any error message that is presented.

- **Uniform Error Codes:** Ensure that you are not inadvertently supplying information to an attacker via the use of inconsistent or "conflicting" error messages. For instance, don't reveal unintended information by utilizing error messages such as Access Denied, which will also let an attacker know that the file he seeks actually exists. Have consistent terminology for files and folders that do exist, do not exist, and which have read access denied.
- **Informational Error Messages:** Ensure that error messages do not reveal too much information. Complete or partial paths, variable and file names, row and column names in tables, and specific database errors should never be revealed to the end user. Remember, an attacker will gather as much information as possible, and then add pieces of seemingly innocuous information together to craft a method of attack.
- **Proper Error Handling:** Utilize generic error pages and error handling logic to inform end users of potential problems. Do not provide system information or other data that could be utilized by an attacker when orchestrating an attack.

For QA:

In reality, simple testing can usually determine how your web application will react to different input errors. More expansive testing must be conducted to cause internal errors to gauge the reaction of the site.

The best course of action for QA associates to take is to ensure that the error handling scheme is consistent. Do you receive a different type of error for a file that does not exist as opposed to a file that does? Are phrases like "Permission Denied" utilized which could reveal the existence of a file to an attacker? It is often a seemingly innocuous piece of information that provides an attacker with the means to discover something else which he can then utilize when conducting an attack.

Attack Request:

```
GET /manual/fr/glossary.html HTTP/1.1
Referer: http://129.105.46.118:80/manual/fr/
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)
Pragma: no-cache
Host: 129.105.46.118
Connection: Keep-Alive
Cookie:
CustomCookie=WebInspect15804ZX5968C937BF2F4C00B8CA168F18502748YF85E;PHPSESSID=0286af493a
cdaf996469d378e8cb3ea1;
```

Attack Response:

```
HTTP/1.1 200 OK
Date: Tue, 28 Aug 2007 09:43:40 GMT
Server: Apache/2.0.54 (Unix) mod_ssl/2.0.54 OpenSSL/0.9.7e DAV/2 PHP/4.3.10
Content-Location: glossary.html.en
Vary: negotiate,accept-language,accept-charset
TCN: choice
Last-Modified: Fri, 04 Feb 2005 22:50:17 GMT
ETag: "1c2c-6649-4e689c40;1c2b-162-f5e7cb00"
Accept-Ranges: bytes
Content-Length: 26185
Connection: close
Content-Type: text/html
Content-Language: en

<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" lang="en" xml:lang="en"><head><!--
      XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
           This file is generated from xml source: DO NOT EDIT
      XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
    -->
<title>Glossary - Apache HTTP Server</title>
<link href="./style/css/manual.css" rel="stylesheet" media="all" type="text/css" title="Main stylesheet" />
<link href="./style/css/manual-loose-100pc.css" rel="alternate stylesheet" media="all" type="text/css"
title="No Sidebar - Default font size" />
<link href="./style/css/manual-print.css" rel="stylesheet" media="print" type="text/css" />
<link href="./images/favicon.ico" rel="shortcut icon" /></head>
<body id="manual-page" class="no-sidebar"><div id="page-header">
<p class="menu"><a href="./mod/">Modules</a> | <a href="./mod/directives.html">Directives</a> | <a
 href="./faq/">FAQ</a> | <a href="./glossary.html">Glossary</a> | <a
href="./sitemap.html">Sitemap</a></p>
<p class="apache">Apache HTTP Server Version 2.0</p>
<img alt="" src="./images/feather.gif" /></div>
<div class="up"><a href="./"><img title="&lt;-" alt="&lt;-" src="./images/left.gif" /></a></div>
<div id="path">
<a href="http://www.apache.org/">Apache</a> &gt; <a href="http://httpd.apache.org/">HTTP
Server</a> &gt; <a href="http://httpd.apache.org/docs-project/">Documentation</a> &gt; <a
href="./">Version 2.0</a></div><div id="pa ... {content removed}
```

Medium **Apache mod_autoindex Directory Contents Disclosure**

File Names:

- http://129.105.46.118:80/icons/?M=A
- http://129.105.46.118:80/icons/small/?M=A
- http://129.105.46.118:80/session1/?M=A
- http://129.105.46.118:80/session2/?M=A
- http://129.105.46.118:80/input/?M=A
- http://129.105.46.118:80/authskip/?M=A
- http://129.105.46.118:80/manual/style/css/?M=A
- http://129.105.46.118:80/manual/style/?M=A
- http://129.105.46.118:80/manual/images/?M=A
- http://129.105.46.118:80/manual/de/images/?M=A
- http://129.105.46.118:80/manual/en/images/?M=A
- http://129.105.46.118:80/manual/es/images/?M=A
- http://129.105.46.118:80/manual/fr/images/?M=A
- http://129.105.46.118:80/manual/ja/images/?M=A
- http://129.105.46.118:80/manual/ko/images/?M=A
- http://129.105.46.118:80/manual/ru/images/?M=A
- http://129.105.46.118:80/manual/de/style/css/?M=A
- http://129.105.46.118:80/manual/de/style/?M=A
- http://129.105.46.118:80/manual/en/style/css/?M=A
- http://129.105.46.118:80/manual/en/style/?M=A
- http://129.105.46.118:80/manual/es/style/css/?M=A
- http://129.105.46.118:80/manual/es/style/?M=A
- http://129.105.46.118:80/manual/fr/style/css/?M=A

- http://129.105.46.118:80/manual/fr/style/?M=A
- http://129.105.46.118:80/manual/ja/style/css/?M=A
- http://129.105.46.118:80/manual/ja/style/?M=A
- http://129.105.46.118:80/manual/ko/style/css/?M=A
- http://129.105.46.118:80/manual/ko/style/?M=A
- http://129.105.46.118:80/manual/ru/style/css/?M=A
- http://129.105.46.118:80/manual/ru/style/?M=A
- http://129.105.46.118:80/manual/style/lang/?M=A
- http://129.105.46.118:80/manual/style/latex/?M=A
- http://129.105.46.118:80/manual/style/xsl/?M=A
- http://129.105.46.118:80/manual/de/style/lang/?M=A
- http://129.105.46.118:80/manual/de/style/latex/?M=A
- http://129.105.46.118:80/manual/de/style/xsl/?M=A
- http://129.105.46.118:80/manual/en/style/lang/?M=A
- http://129.105.46.118:80/manual/en/style/latex/?M=A
- http://129.105.46.118:80/manual/en/style/xsl/?M=A
- http://129.105.46.118:80/manual/es/style/lang/?M=A
- http://129.105.46.118:80/manual/es/style/latex/?M=A
- http://129.105.46.118:80/manual/es/style/xsl/?M=A
- http://129.105.46.118:80/manual/fr/style/lang/?M=A
- http://129.105.46.118:80/manual/fr/style/latex/?M=A
- http://129.105.46.118:80/manual/fr/style/xsl/?M=A
- http://129.105.46.118:80/manual/ja/style/lang/?M=A
- http://129.105.46.118:80/manual/ja/style/latex/?M=A
- http://129.105.46.118:80/manual/ja/style/xsl/?M=A
- http://129.105.46.118:80/manual/ko/style/lang/?M=A
- http://129.105.46.118:80/manual/ko/style/latex/?M=A
- http://129.105.46.118:80/manual/ko/style/xsl/?M=A
- http://129.105.46.118:80/manual/ru/style/lang/?M=A
- http://129.105.46.118:80/manual/ru/style/latex/?M=A
- http://129.105.46.118:80/manual/ru/style/xsl/?M=A
- http://129.105.46.118:80/manual/style/xsl/util/?M=A
- http://129.105.46.118:80/manual/de/style/xsl/util/?M=A
- http://129.105.46.118:80/manual/en/style/xsl/util/?M=A
- http://129.105.46.118:80/manual/es/style/xsl/util/?M=A
- http://129.105.46.118:80/manual/fr/style/xsl/util/?M=A
- http://129.105.46.118:80/manual/ja/style/xsl/util/?M=A
- http://129.105.46.118:80/manual/ko/style/xsl/util/?M=A
- http://129.105.46.118:80/manual/ru/style/xsl/util/?M=A

Summary: A directory contents disclosure vulnerability was found on an Apache web server. When the auto index module (mod_autoindex) is enabled in Apache, as it is in many default configurations, a directory listing can be obtained from the server even if index files exist and Apache directory listings are disabled. This vulnerability is caused by a poor default configuration. Recommendations include removing the mod_autoindex lines from the httpd.conf file or upgrading to a version of Apache that is no longer vulnerable.

Execution: Append a string in the form of "?X=Y" to a request for a directory. This string controls the sorting criteria.

X Values:

D - Directory

M - Modified Date

N - Name

S - Size

Y Values:

A - Ascending

D - Descending

Implication: Directory contents disclosure gives an attacker a complete listing of the files contained in a directory. This may include sensitive files such as back-up copies of source code, include files, configuration files, administration or other "hidden" web applications, databases, and other data files. These files can disclose sensitive information such as customer records to an attacker, or provide detailed information that can lead to the exploitation of other vulnerabilities.

Vulnerable versions: Versions prior to 1.3.22

Fix:

For Security Operations:

Newer versions of Apache HTTP Server are not vulnerable to this issue. Upgrade to a newer version (1.3.22 or later), which is available from the Apache HTTP Server Project Web site.

As a workaround to upgrading, remove the mod_autoindex lines from httpd.conf and restart the Apache server.

For Development:

When building the web application, ensure that up-to-date patches or software upgrades have been installed on the production server.

For QA:

This problem ultimately requires a patch or software upgrade to be installed by Security Operations. If necessary, install the patch or upgrade in your test environment. After verifying that the patch or upgrade has removed the vulnerability, present the results to Security Operations personnel along with a recommendation for installing the patch or upgrade on the production server.

Reference: **Apache**

Apache HTTP Server Project

Auto Index Module Documentation

Module mod_autoindex

SecurityTracker

Apache Web Server May Disclose Directory Contents…

(Apache Issues Fix) Re: Apache Web Server May Disclose Directory Contents…

Attack Request:

```
GET /icons/?M=A HTTP/1.1
Referer: http://129.105.46.118:80/icons/
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)
Pragma: no-cache
Host: 129.105.46.118
Connection: Keep-Alive
Cookie:
CustomCookie=WebInspect15804ZX5968C937BF2F4C00B8CA168F18502748YF85E;PHPSESSID=6ea4a2f4f8
85719ef23b18117ac21c1a;
```

Attack Response:

```
HTTP/1.1 200 OK
Date: Tue, 28 Aug 2007 10:17:53 GMT
Server: Apache/2.0.54 (Unix) mod_ssl/2.0.54 OpenSSL/0.9.7e DAV/2 PHP/4.3.10
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html

1000
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
 <head>
  <title>Index of /icons</title>
 </head>
 <body>
<h1>Index of /icons</h1>
<pre><img src="/icons/blank.gif" alt="Icon "> <a href="?C=N;O=D">Name</a>                    <a
href="?C=M;O=A">Last modified</a>      <a href="?C=S;O=A">Size</a>  <a
href="?C=D;O=A">Description</a><hr><img src="/icons/back.gif" alt="[DIR]"> <a href="/">Parent
Directory</a>                             -
<img src="/icons/image2.gif" alt="[IMG]"> <a href="a.gif">a.gif</a>                 21-Nov-2004 14:35
246
<img src="/icons/image2.gif" alt="[IMG]"> <a href="a.png">a.png</a>                 21-Nov-2004 14:35
293
<img src="/icons/image2.gif" alt="[IMG]"> <a href="alert.black.gif">alert.black.gif</a>
21-Nov-2004 14:35  242
<img src="/icons/image2.gif" alt="[IMG]"> <a href="alert.black.png">alert.black.png</a>
21-Nov-2004 14:35  279
<img src="/icons/image2.gif" alt="[IMG]"> <a href="alert.red.gif">alert.red.gif</a>          21-Nov-2004
14:35  247
<img src="/icons/image2.gif" alt="[IMG]"> <a href="alert.red.png">alert.red.png</a>
21-Nov-2004 14:35  298
<img src="/icons/image2.gif" alt="[IMG]"> <a href="apache_pb.gif">apache_pb.gif</a>
21-Nov-2004 14:35  2.3K
<img src="/icons/image2.gif" alt="[IMG]"> <a href="apache_pb.png">apache_pb.png</a>
21-Nov-2004 14:35  1.4K
<img src="/icons/image2.gif" alt="[IMG]"> <a href="apache_pb2.gif">apache_pb2.gif</a>
21-Nov-2004 14:35  2.4K
<img src="/icons/image2.gif" alt="[IMG]"> <a href="apache_pb2.png">apache_pb2.png</a>
21-Nov-2004 14:35  1.4K
<img src="/icons/image2.gif" alt="[IMG]"> <a href="apache_pb2_ani.gif">apache_pb2_ani.gif</a>
21-Nov-2004 14:35  2.1K
<img src="/icons/image2.gif" alt="[IMG]"> <a href="back.gif">back.gi ... {content removed}
```

Low

Test Application (test.php)

File Names:

- http://129.105.46.118:80/test.php

Summary:

A test script was located on the server. This type of file is usually left by a developer or web master to test a certain function of the web application or web server. Leaving test scripts available on the server is a very unsecure practice. The types of information that can be gleaned from test scripts include fixed authentication session IDs, usernames and passwords, locations or pointers to confidential areas of the web site, and proprietary source code. With this type of information available to attackers, they can either use it to totally breach the security of the site or use it as a stepping stone to retrieve other sensitive data. Recommendations include removing this file from the production server.

Fix:

For Security Operations:

Remove the application from the server. Inform developers and administrators to remove test applications from servers when they are no longer needed. While they are in use, be sure to protect them using HTTP basic authentication.

For Development:

Contact your security or network operations team and request they investigate the issue.

For QA:

Contact your security or network operations team and request they investigate the issue.

Attack Request:

```
GET /test.php HTTP/1.1
Referer: http://129.105.46.118:80/
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)
Pragma: no-cache
Host: 129.105.46.118
Connection: Keep-Alive
Cookie:
CustomCookie=WebInspect15804ZX5968C937BF2F4C00B8CA168F18502748YF85E;PHPSESSID=7a596091d
deaf8f1ce10d359083a3d54;
```

Attack Response:

```
HTTP/1.1 200 OK
Date: Tue, 28 Aug 2007 10:17:39 GMT
Server: Apache/2.0.54 (Unix) mod_ssl/2.0.54 OpenSSL/0.9.7e DAV/2 PHP/4.3.10
X-Powered-By: PHP/4.3.10
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html

1000
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "DTD/xhtml1-transitional.dtd">
<html><head>
<style type="text/css"><!--
body {background-color: #ffffff; color: #000000;}
body, td, th, h1, h2 {font-family: sans-serif;}
pre {margin: 0px; font-family: monospace;}
a:link {color: #000099; text-decoration: none; background-color: #ffffff;}
a:hover {text-decoration: underline;}
table {border-collapse: collapse;}
.center {text-align: center;}
.center table { margin-left: auto; margin-right: auto; text-align: left;}
.center th { text-align: center !important; }
td, th { border: 1px solid #000000; font-size: 75%; vertical-align: baseline;}
h1 {font-size: 150%;}
h2 {font-size: 125%;}
.p {text-align: left;}
.e {background-color: #ccccff; font-weight: bold; color: #000000;}
.h {background-color: #9999cc; font-weight: bold; color: #000000;}
.v {background-color: #cccccc; color: #000000;}
i {color: #666666; background-color: #cccccc;}
img {float: right; border: 0px;}
hr {width: 600px; background-color: #cccccc; border: 0px; height: 1px; color: #000000;}
//--></style>
<title>phpinfo()</title></head>
<body><div class="center">
<table border="0" cellpadding="3" width="600">
<tr class="h"><td>
<a href="http://www.php.net/"><img border="0"
src="/test.php?=PHPE9568F34-D428-11d2-A769-00AA001ACF42" alt="PHP Logo" /></a><h1
class="p">PHP Version 4.3.10</h1>
</td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr><td class="e">System </td><td class="v">Linux slax 2.6.11.8 #1 SMP Sun Jul 10 00:29:57 Local
time zone must be set--see zic  i686 </td></tr>
<tr><td class="e">Build Date </td><td class="v">Jul 10 2005 13:16:35 </td></tr>
<tr><td class="e">Configure Command </td><td class="v"> './configure' '--prefix=/usr/local/php'
'--with-apxs2=/usr/local/apache2/bin/apxs' '-- ... {content removed}
```

Low **Environmental Variables Disclosure**

File Names:

- http://129.105.46.118:80/manual/ru/mod/mod_ssl.html
- http://129.105.46.118:80/manual/ru/mod/mod_rewrite.html
- http://129.105.46.118:80/manual/de/custom-error.html
- http://129.105.46.118:80/manual/mod/mod_rewrite.html.en
- http://129.105.46.118:80/manual/ja/mod/mod_ssl.html
- http://129.105.46.118:80/manual/ko/mod/mod_ssl.html
- http://129.105.46.118:80/manual/ko/mod/mod_rewrite.html
- http://129.105.46.118:80/manual/fr/custom-error.html
- http://129.105.46.118:80/manual/custom-error.html.en
- http://129.105.46.118:80/manual/ko/custom-error.html
- http://129.105.46.118:80/manual/en/custom-error.html
- http://129.105.46.118:80/manual/mod/mod_ssl.html.en
- http://129.105.46.118:80/manual/en/mod/mod_ssl.html
- http://129.105.46.118:80/manual/en/mod/mod_rewrite.html
- http://129.105.46.118:80/manual/es/mod/mod_ssl.html
- http://129.105.46.118:80/manual/es/mod/mod_rewrite.html
- http://129.105.46.118:80/manual/ja/mod/mod_rewrite.html
- http://129.105.46.118:80/manual/de/mod/mod_ssl.html
- http://129.105.46.118:80/manual/de/mod/mod_rewrite.html
- http://129.105.46.118:80/manual/mod/mod_ssl.html
- http://129.105.46.118:80/manual/custom-error.html

- http://129.105.46.118:80/manual/mod/mod_rewrite.html
- http://129.105.46.118:80/manual/ko/custom-error.html.ko.euc-kr
- http://129.105.46.118:80/manual/en/custom-error.html.en
- http://129.105.46.118:80/manual/ru/mod/mod_ssl.html.en
- http://129.105.46.118:80/manual/ru/custom-error.html.en
- http://129.105.46.118:80/manual/fr/mod/mod_ssl.html.en
- http://129.105.46.118:80/manual/fr/mod/mod_rewrite.html.en
- http://129.105.46.118:80/manual/fr/custom-error.html.fr
- http://129.105.46.118:80/manual/ko/mod/mod_ssl.html.en
- http://129.105.46.118:80/manual/ko/mod/mod_rewrite.html.en
- http://129.105.46.118:80/manual/de/custom-error.html.en
- http://129.105.46.118:80/manual/ru/mod/mod_rewrite.html.en
- http://129.105.46.118:80/manual/en/mod/mod_ssl.html.en
- http://129.105.46.118:80/manual/es/mod/mod_ssl.html.en
- http://129.105.46.118:80/manual/es/mod/mod_rewrite.html.en
- http://129.105.46.118:80/manual/ja/mod/mod_ssl.html.en
- http://129.105.46.118:80/manual/ja/mod/mod_rewrite.html.en
- http://129.105.46.118:80/manual/en/mod/mod_rewrite.html.en
- http://129.105.46.118:80/manual/de/mod/mod_ssl.html.en
- http://129.105.46.118:80/manual/de/mod/mod_rewrite.html.en
- http://129.105.46.118:80/manual/ru/custom-error.html
- http://129.105.46.118:80/manual/fr/mod/mod_ssl.html
- http://129.105.46.118:80/manual/fr/mod/mod_rewrite.html
- http://129.105.46.118:80/test.php?=,`@^*$;#
- http://129.105.46.118:80/test.php?=%0aA:B
- http://129.105.46.118:80/test.php?="
- http://129.105.46.118:80/test.php?=%250a
- http://129.105.46.118:80/test.php?=%2500
- http://129.105.46.118:80/test.php?=%00
- http://129.105.46.118:80/test.php?='
- http://129.105.46.118:80/test.php?=())[]]{}}
- http://129.105.46.118:80/test.php?=%0d%0aInjectedHeader:%20InjectedValue
- http://129.105.46.118:80/test.php?=http://www.spidynamics.com/
- http://129.105.46.118:80/test.php?=/,%25ENV,/
- http://129.105.46.118:80/test.php?=/
- http://129.105.46.118:80/test.php?=/%2A
- http://129.105.46.118:80/test.php?=%2A
- http://129.105.46.118:80/test.php?=/../../../../../../../../../%2A

Summary: System Environment variables log files contain information about the nature of your web application, and would allow an attacker to gain insightful information about the web system setup. Recommendations include removing this file from the affected system.

Implication: A fundamental part of any successful attack is reconnaissance and information gathering. The primary danger from exploitation of this vulnerability is that an attacker will be able to utilize the information in launching a more serious attack. It is very simple to check for its existence, and a file most definitely on the short list of things for which a potential attacker would look.

Fix: Remove this file from the system in question. One of the most important aspects of web application security is to restrict access to important files or directories only to those individuals who actually need to access them. Ensure that the private architectural structure of your web application is not exposed to anyone who wishes to view it as even seemingly innocuous directories can provide important information to a potential attacker.

The following recommendations can help to ensure that you are not unintentionally allowing access to either information that could be utilized in conducting an attack or propriety data stored in publicly accessible directories.

- Restrict access to important files or directories only to those who actually need it.
- Ensure that files containing sensitive information are not left publicly accessible or that comments left inside files do not reveal the locations of directories best left confidential.
- Turn off the Automatic Directory Listing feature in your application server package.
- Don't follow standard naming procedures for hidden directories. For example, don't create a hidden directory called "cgi" that contains cgi scripts. Obvious directory names are just that...readily guessed by an attacker.

Remember, the harder you make it for an attacker to access information about your web application, the more likely it is that he will simply find an easier target.

Attack Request:
```
GET /manual/ru/mod/mod_ssl.html HTTP/1.1
Referer: http://129.105.46.118:80/manual/ru/mod/directives.html
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)
Pragma: no-cache
Host: 129.105.46.118
Connection: Keep-Alive
Cookie:
CustomCookie=WebInspect15804ZX5968C937BF2F4C00B8CA168F18502748YF85E;PHPSESSID=0286af493a
cdaf996469d378e8cb3ea1;
```

Attack Response:
```
HTTP/1.1 200 OK
Date: Tue, 28 Aug 2007 09:49:59 GMT
Server: Apache/2.0.54 (Unix) mod_ssl/2.0.54 OpenSSL/0.9.7e DAV/2 PHP/4.3.10
Content-Location: mod_ssl.html.en
Vary: negotiate
```

TCN: choice
Last-Modified: Fri, 04 Feb 2005 22:50:17 GMT
ETag: "1d4a-17869-4e689c40;1d49-56-a64a7c40"
Accept-Ranges: bytes
Content-Length: 96361
Connection: close
Content-Type: text/html
Content-Language: en

<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" lang="en" xml:lang="en"><head><!--
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
This file is generated from xml source: DO NOT EDIT
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
-->
<title>mod_ssl - Apache HTTP Server</title>
<link href="../style/css/manual.css" rel="stylesheet" media="all" type="text/css" title="Main stylesheet" />
<link href="../style/css/manual-loose-100pc.css" rel="alternate stylesheet" media="all" type="text/css"
title="No Sidebar - Default font size" />
<link href="../style/css/manual-print.css" rel="stylesheet" media="print" type="text/css" />
<link href="../images/favicon.ico" rel="shortcut icon" /></head>
<body>

Modules | Directives |
FAQ | Glossary | <a
href="../sitemap.html">Sitemap
Apache HTTP Server Version 2.0

<img title="<-" alt="<-" src="../images/left.gif" />

Apache > HTTP
Server > Documentation > <a
href="../">Version 2.0 > Modules

<div id="pre ... {content removed}

Low **Documentation (README)**

File Names:
- http://129.105.46.118:80/icons/small/README
- http://129.105.46.118:80/icons/README

Summary: A readme file was found. Readme files are usually found within software application installation directories. If a web application was installed directly in a folder or subfolder of the website, a readme file could likely be retrieved by an attacker. The danger in having a readme file available is that it gives away to attackers what type of software you are using as well as recent version information, or a location from where the attacker could download the software itself. Recommendations include removing the file from the production server.

Execution: Parse the Readme file for this type of information:
- Name of the application.
- Most recent version information. Note: The last date indicates what version is on the website.
- A location to download the software.
- The company site that holds the software.

The following items are especially good if the software is not freeware, because you can discover the default installation layout, debug configurations, etc.
- A technical support forum or mailing list.
- References to technical documentation.

Fix:

For Security Operations:

Remove the Readme file from any folder that is accessible via the web. Also, remove any other stray files that may have been left behind from web package installations. Make it a good practice to install the web package in a temp directory located outside of the website, and then copy only the needed files to the web site.

For Development:

Have Security Operations remove this file from the production server.

For QA:

Have Security Operations remove this file from the production server.

Attack Request:
GET /icons/small/README HTTP/1.1
Referer: http://129.105.46.118:80/icons/small/
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)
Pragma: no-cache
Host: 129.105.46.118
Connection: Keep-Alive
Cookie:
CustomCookie=WebInspect15804ZX5968C937BF2F4C00B8CA168F18502748YF85E;PHPSESSID=3e0922905
5471e85751910dd5b91c5ca;

Attack Response:
HTTP/1.1 200 OK
Date: Tue, 28 Aug 2007 09:40:11 GMT
Server: Apache/2.0.54 (Unix) mod_ssl/2.0.54 OpenSSL/0.9.7e DAV/2 PHP/4.3.10

Content-Location: README.txt
Vary: negotiate
TCN: choice
Last-Modified: Sun, 21 Nov 2004 14:35:21 GMT
ETag: "1b75-12c-a64a7c40;eb304600"
Accept-Ranges: bytes
Content-Length: 300
Connection: close
Content-Type: text/plain

These icons are provided as an alternative to the standard Apache icon graphics. All graphics in this directory, with the exception of rainbow.gif, are 16x16 pixels in size, rather than the 20x22 dimension icons which are the normal defaults for Apache and are in the parent directory of this one.

Low **Internal IP Disclosure**

File Names:

- http://129.105.46.118:80/manual/ko/bind.html
- http://129.105.46.118:80/manual/ru/bind.html
- http://129.105.46.118:80/manual/new_features_2_0.html.en
- http://129.105.46.118:80/manual/bind.html.en
- http://129.105.46.118:80/manual/ru/new_features_2_0.html
- http://129.105.46.118:80/manual/ja/bind.html
- http://129.105.46.118:80/manual/fr/bind.html
- http://129.105.46.118:80/manual/ja/new_features_2_0.html
- http://129.105.46.118:80/manual/ko/new_features_2_0.html
- http://129.105.46.118:80/manual/en/mod/mpm_common.html
- http://129.105.46.118:80/manual/en/mod/mod_access.html
- http://129.105.46.118:80/manual/en/mod/mod_ext_filter.html
- http://129.105.46.118:80/manual/en/mod/mod_proxy.html
- http://129.105.46.118:80/manual/es/mod/mod_access.html
- http://129.105.46.118:80/manual/es/mod/mpm_common.html
- http://129.105.46.118:80/manual/de/mod/mod_ext_filter.html
- http://129.105.46.118:80/manual/de/mod/mod_proxy.html
- http://129.105.46.118:80/manual/de/mod/mpm_common.html
- http://129.105.46.118:80/manual/de/mod/mod_access.html
- http://129.105.46.118:80/manual/ja/mod/mod_proxy.html
- http://129.105.46.118:80/manual/ja/mod/mod_ext_filter.html
- http://129.105.46.118:80/manual/ja/mod/mod_access.html
- http://129.105.46.118:80/manual/es/mod/mod_ext_filter.html
- http://129.105.46.118:80/manual/es/mod/mod_proxy.html
- http://129.105.46.118:80/manual/ja/mod/mpm_common.html
- http://129.105.46.118:80/manual/mod/mod_ext_filter.html
- http://129.105.46.118:80/manual/vhosts/examples.html
- http://129.105.46.118:80/manual/ssl/ssl_howto.html
- http://129.105.46.118:80/manual/dns-caveats.html
- http://129.105.46.118:80/manual/ssl/ssl_faq.html
- http://129.105.46.118:80/manual/de/new_features_2_0.html
- http://129.105.46.118:80/manual/mod/mod_proxy.html
- http://129.105.46.118:80/manual/mod/mod_access.html
- http://129.105.46.118:80/manual/new_features_2_0.html
- http://129.105.46.118:80/manual/bind.html
- http://129.105.46.118:80/manual/mod/mpm_common.html
- http://129.105.46.118:80/manual/de/bind.html
- http://129.105.46.118:80/manual/en/new_features_2_0.html
- http://129.105.46.118:80/manual/en/bind.html
- http://129.105.46.118:80/manual/es/bind.html
- http://129.105.46.118:80/manual/es/new_features_2_0.html
- http://129.105.46.118:80/manual/mod/mod_ext_filter.html.en
- http://129.105.46.118:80/manual/de/dns-caveats.html
- http://129.105.46.118:80/manual/en/ssl/ssl_howto.html
- http://129.105.46.118:80/manual/en/dns-caveats.html
- http://129.105.46.118:80/manual/es/vhosts/examples.html
- http://129.105.46.118:80/manual/de/ssl/ssl_faq.html
- http://129.105.46.118:80/manual/en/vhosts/examples.html
- http://129.105.46.118:80/manual/de/ssl/ssl_howto.html
- http://129.105.46.118:80/manual/ja/vhosts/examples.html
- http://129.105.46.118:80/manual/es/ssl/ssl_howto.html
- http://129.105.46.118:80/manual/en/ssl/ssl_faq.html
- http://129.105.46.118:80/manual/es/dns-caveats.html
- http://129.105.46.118:80/manual/ko/dns-caveats.html
- http://129.105.46.118:80/manual/ja/dns-caveats.html
- http://129.105.46.118:80/manual/ko/vhosts/examples.html
- http://129.105.46.118:80/manual/es/ssl/ssl_faq.html
- http://129.105.46.118:80/manual/ko/ssl/ssl_faq.html
- http://129.105.46.118:80/manual/ko/ssl/ssl_howto.html
- http://129.105.46.118:80/manual/ja/ssl/ssl_faq.html
- http://129.105.46.118:80/manual/ja/ssl/ssl_howto.html
- http://129.105.46.118:80/manual/dns-caveats.html.en

- http://129.105.46.118:80/manual/vhosts/examples.html.en
- http://129.105.46.118:80/manual/ko/mod/mod_ext_filter.html
- http://129.105.46.118:80/manual/ko/mod/mod_proxy.html
- http://129.105.46.118:80/manual/ko/mod/mpm_common.html
- http://129.105.46.118:80/manual/ko/mod/mod_access.html
- http://129.105.46.118:80/manual/ru/mod/mpm_common.html
- http://129.105.46.118:80/manual/ru/mod/mod_access.html
- http://129.105.46.118:80/manual/ru/mod/mod_ext_filter.html
- http://129.105.46.118:80/manual/de/vhosts/examples.html
- http://129.105.46.118:80/manual/ru/mod/mod_proxy.html
- http://129.105.46.118:80/manual/mod/mpm_common.html.en
- http://129.105.46.118:80/manual/mod/mod_access.html.en
- http://129.105.46.118:80/manual/mod/mod_proxy.html.en
- http://129.105.46.118:80/manual/fr/vhosts/examples.html
- http://129.105.46.118:80/manual/fr/mod/mod_proxy.html
- http://129.105.46.118:80/manual/fr/mod/mod_ext_filter.html
- http://129.105.46.118:80/manual/fr/mod/mpm_common.html
- http://129.105.46.118:80/manual/fr/mod/mod_access.html
- http://129.105.46.118:80/manual/ssl/ssl_howto.html.en
- http://129.105.46.118:80/manual/fr/dns-caveats.html
- http://129.105.46.118:80/manual/de/new_features_2_0.html.de
- http://129.105.46.118:80/manual/ssl/ssl_faq.html.en
- http://129.105.46.118:80/manual/en/bind.html.en
- http://129.105.46.118:80/manual/de/bind.html.en
- http://129.105.46.118:80/manual/en/new_features_2_0.html.en
- http://129.105.46.118:80/manual/ru/vhosts/examples.html
- http://129.105.46.118:80/manual/ru/new_features_2_0.html.ru.koi8-r
- http://129.105.46.118:80/manual/ru/ssl/ssl_faq.html
- http://129.105.46.118:80/manual/ja/bind.html.ja.euc-jp
- http://129.105.46.118:80/manual/ru/ssl/ssl_howto.html
- http://129.105.46.118:80/manual/ru/dns-caveats.html
- http://129.105.46.118:80/manual/ja/new_features_2_0.html.ja.euc-jp
- http://129.105.46.118:80/manual/ko/new_features_2_0.html.ko.euc-kr
- http://129.105.46.118:80/manual/fr/ssl/ssl_faq.html
- http://129.105.46.118:80/manual/fr/ssl/ssl_howto.html
- http://129.105.46.118:80/manual/fr/bind.html.fr
- http://129.105.46.118:80/manual/en/mod/mpm_common.html.en
- http://129.105.46.118:80/manual/de/mod/mod_proxy.html.en
- http://129.105.46.118:80/manual/en/mod/mod_access.html.en
- http://129.105.46.118:80/manual/ru/bind.html.en
- http://129.105.46.118:80/manual/de/mod/mod_ext_filter.html.en
- http://129.105.46.118:80/manual/en/mod/mod_ext_filter.html.en
- http://129.105.46.118:80/manual/en/mod/mod_proxy.html.en
- http://129.105.46.118:80/manual/es/mod/mod_access.html.en
- http://129.105.46.118:80/manual/de/mod/mpm_common.html.de
- http://129.105.46.118:80/manual/de/mod/mod_access.html.en
- http://129.105.46.118:80/manual/ko/bind.html.ko.euc-kr
- http://129.105.46.118:80/manual/ko/mod/mpm_common.html.en
- http://129.105.46.118:80/manual/ko/mod/mod_access.html.en
- http://129.105.46.118:80/manual/ja/mod/mod_ext_filter.html.en
- http://129.105.46.118:80/manual/ja/mod/mod_proxy.html.en
- http://129.105.46.118:80/manual/ja/mod/mod_access.html.ja.euc-jp
- http://129.105.46.118:80/manual/es/mod/mod_ext_filter.html.en
- http://129.105.46.118:80/manual/es/mod/mod_proxy.html.en
- http://129.105.46.118:80/manual/ja/mod/mpm_common.html.ja.euc-jp
- http://129.105.46.118:80/manual/ru/mod/mod_proxy.html.en
- http://129.105.46.118:80/manual/ru/mod/mod_ext_filter.html.en
- http://129.105.46.118:80/manual/de/vhosts/examples.html.en
- http://129.105.46.118:80/manual/ko/mod/mod_proxy.html.en
- http://129.105.46.118:80/manual/ko/mod/mod_ext_filter.html.ko.euc-kr
- http://129.105.46.118:80/manual/ru/mod/mod_access.html.en
- http://129.105.46.118:80/manual/ru/mod/mpm_common.html.en
- http://129.105.46.118:80/manual/fr/mod/mod_ext_filter.html.en
- http://129.105.46.118:80/manual/fr/mod/mod_proxy.html.en
- http://129.105.46.118:80/manual/ru/vhosts/examples.html.en
- http://129.105.46.118:80/manual/fr/ssl/ssl_faq.html.en
- http://129.105.46.118:80/manual/fr/ssl/ssl_howto.html.en
- http://129.105.46.118:80/manual/fr/vhosts/examples.html.en
- http://129.105.46.118:80/manual/ru/ssl/ssl_faq.html.en
- http://129.105.46.118:80/manual/ru/ssl/ssl_howto.html.en
- http://129.105.46.118:80/manual/ru/dns-caveats.html.en
- http://129.105.46.118:80/manual/de/dns-caveats.html.en
- http://129.105.46.118:80/manual/de/ssl/ssl_howto.html.en
- http://129.105.46.118:80/manual/es/dns-caveats.html.en
- http://129.105.46.118:80/manual/en/ssl/ssl_howto.html.en
- http://129.105.46.118:80/manual/en/dns-caveats.html.en
- http://129.105.46.118:80/manual/es/vhosts/examples.html.en
- http://129.105.46.118:80/manual/de/ssl/ssl_faq.html.en
- http://129.105.46.118:80/manual/en/vhosts/examples.html.en

- http://129.105.46.118:80/manual/ja/vhosts/examples.html.en
- http://129.105.46.118:80/manual/es/ssl/ssl_faq.html.en
- http://129.105.46.118:80/manual/en/ssl/ssl_faq.html.en
- http://129.105.46.118:80/manual/es/ssl/ssl_howto.html.en
- http://129.105.46.118:80/manual/fr/dns-caveats.html.fr
- http://129.105.46.118:80/manual/ja/ssl/ssl_faq.html.en
- http://129.105.46.118:80/manual/ja/ssl/ssl_howto.html.en
- http://129.105.46.118:80/manual/ko/dns-caveats.html.ko.euc-kr
- http://129.105.46.118:80/manual/ja/dns-caveats.html.ja.euc-jp
- http://129.105.46.118:80/manual/ko/vhosts/examples.html.ko.euc-kr
- http://129.105.46.118:80/manual/ko/ssl/ssl_faq.html.en
- http://129.105.46.118:80/manual/ko/ssl/ssl_howto.html.en
- http://129.105.46.118:80/manual/fr/mod/mpm_common.html.en
- http://129.105.46.118:80/manual/fr/mod/mod_access.html.en

Summary: A string matching an internal/reserved IPv4 or IPv6 address range was discovered. This may disclose information about the IP addressing scheme of the internal network and can be valuable to attackers. Internal IPv4/IPv6 ranges are:

10.x.x.x

172.16.x.x through 172.31.x.x

192.168.x.x

fd00::x

If not a part of techical documentation, recommendations include removing the string from the production server.

Fix: This issue can appear for several reasons. The most common is that the application or webserver error message discloses the IP address. This can be solved by determining where to turn off detailed error messages in the application or webserver. Another common reason is due to a comment located in the source of the webpage. This can easily be removed from the source of the page.

Attack Request:

```
GET /manual/ko/bind.html HTTP/1.1
Referer: http://129.105.46.118:80/manual/ko/
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)
Pragma: no-cache
Host: 129.105.46.118
Connection: Keep-Alive
Cookie:
CustomCookie=WebInspect15804ZX5968C937BF2F4C00B8CA168F18502748YF85E;PHPSESSID=0286af493a
cdaf996469d378e8cb3ea1;
```

Attack Response:

```
HTTP/1.1 200 OK
Date: Tue, 28 Aug 2007 09:45:15 GMT
Server: Apache/2.0.54 (Unix) mod_ssl/2.0.54 OpenSSL/0.9.7e DAV/2 PHP/4.3.10
Content-Location: bind.html.ko.euc-kr
Vary: negotiate,accept-language,accept-charset
TCN: choice
Last-Modified: Sun, 27 Feb 2005 11:34:01 GMT
ETag: "1dea-22ee-8a3d9c40;1c58-1a9-8a3d9c40"
Accept-Ranges: bytes
Content-Length: 8942
Connection: close
Content-Type: text/html; charset=euc-kr
Content-Language: ko

<?xml version="1.0" encoding="EUC-KR"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" lang="ko" xml:lang="ko"><head><!--
      XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
           This file is generated from xml source: DO NOT EDIT
      XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
    -->
<title>ÁÖ¼Ò¿Í Æ÷Æ® ÁöÁ¤ (Binding) - Apache HTTP Server</title>
<link href="./style/css/manual.css" rel="stylesheet" media="all" type="text/css" title="Main stylesheet" />
<link href="./style/css/manual-loose-100pc.css" rel="alternate stylesheet" media="all" type="text/css"
title="No Sidebar - Default font size" />
<link href="./style/css/manual-print.css" rel="stylesheet" media="print" type="text/css" />
<link href="./images/favicon.ico" rel="shortcut icon" /></head>
<body id="manual-page"><div id="page-header">
<p class="menu"><a href="./mod/">¸ðµâ</a> | <a href="./mod/directives.html">Áö½Ã¾îµé</a> | <a
href="./faq/">FAQ</a> | <a href="./glossary.html">¿ë¾î</a> | <a
href="./sitemap.html">»çÀÌÆ®¸Ê</a></p>
<p class="apache">Apache HTTP Server Version 2.0</p>
<img alt="" src="./images/feather.gif" /></div>
<div class="up"><a href="./"><img title="&lt;-" alt="&lt;-" src="./images/left.gif" /></a></div>
<div id="path">
<a href="http://www.apache.org/">Apache</a> &gt; <a href="http://httpd.apache.org/">HTTP
Server</a> &gt; <a href="http://httpd.apache.org/docs-project/">Documentation</a> &gt; <a
href="./">Version 2.0</a></div><div i ... {content removed}
```

Low **HTTP TRACE Method Cross-Site Scripting**

File Names: • http://129.105.46.118:80/<script>alert('TRACE');</script>

Summary: The TRACE method is enabled on the webserver. TRACE is a part of the HTTP specification that is intended to be used for debugging and testing purposes. A TRACE request will generate a response containing the text of the original response. Under certain circumstances, an attacker can use the TRACE method's functionality to launch a variant of Cross-Site Scripting attacks against web clients. This can only occur if an attacker can force a web client into executing arbitrary HTTP requests (usually through ActiveX) and the web client also contains weak cross-domain policy enforcement. Recommendations include properly configuring the web server.

Execution: The following HTTP request (sent via a raw HTTP request tool, such as the HTTP Editor in the security toolkit) will demonstrate the TRACE method's functionality. For more detailed information on exploitation of cross-site scripting attacks using the TRACE method, see the information in references.

TRACE /<script>alert('TRACE');</script> HTTP/1.1.

Implication: An attacker could use Cross-Site Scripting attacks to steal cookie information or HTTP basic authentication credentials in some cases.

Fix:

For Developers:

This problem needs to be mitigated in the web server configuration.

For QA:

This problem needs to be mitigated in the web server configuration.

For Security Operations:

For IIS, URLScan can be used to block TRACE requests. For Apache, the TraceEnable directive can be used to disable TRACE requests (older versions of Apache will need to use mod_rewrite, since the TraceEnable directive wasn't added until 1.3.34/2.0.55).

Reference:

CERT Vulnerability Note VU#967593
http://www.kb.cert.org/vuls/id/867593

Researcher Whitepaper
http://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf

URLScan Documentation
http://www.microsoft.com/technet/security/tools/urlscan.mspx

Apache TraceEnable directive
http://httpd.apache.org/docs/1.3/mod/core.html#traceenable

mod_rewrite Documentation
http://httpd.apache.org/docs/mod/mod_rewrite.html

Attack Request:

```
TRACE /<script>alert('TRACE');</script> HTTP/1.1
Referer: http://129.105.46.118:80/
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)
Pragma: no-cache
Host: 129.105.46.118
Connection: Keep-Alive
Cookie: CustomCookie=WebInspect15804ZX5968C937BF2F4C00B8CA168F18502748YF85E
```

Attack Response: [Binary Data]

Low **CGI and Scripting-Related Directories**

File Names: • http://129.105.46.118:80/cgi-bin/

Summary: Directory Enumeration vulnerabilities were discovered within your web application. Risks associated with an attacker discovering a directory on your application server depend upon what type of directory is discovered, and what types of files are contained within it. The primary threat, other than accessing files containing sensitive information, is that an attacker can utilize the information discovered in that directory to perform other types of attacks. Recommendations include restricting access to important directories or files by adopting a "need to know" requirement for both the document and server root, and turning off features such as Automatic Directory Listings that provide information that could be utilized by an attacker when formulating or conducting an attack.

Fix:

For Security Operations:

You should evaluate the production requirements for the found directory. If the directory is not required for production operation, then the directory and its contents should be removed or restricted by a server access control mechanism. More information about implementing access control schemes can be found in the References. Automatic directory indexing should also be disabled, if applicable.

For Development:

This problem will be resolved by the web application server administrator. In general, do not rely on 'hidden' directories within the web root that can contain sensitive resources or web applications. Assume an attacker knows about the existence of all directories and files on your web site, and protect them with proper access controls.

For QA:

This problem will be resolved by the web application server administrator.

Reference:

Implementing Basic Authentication in IIS
http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/abbca505-6f63-4267-aac1-1ea89d861eb4.mspx

Implementing Basic Authentication in Apache
http://httpd.apache.org/docs/howto/auth.html#intro

Attack Request:

```
GET /cgi-bin/ HTTP/1.1
Referer: http://129.105.46.118:80/
```

User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)
Pragma: no-cache
Host: 129.105.46.118
Connection: Keep-Alive
Cookie: CustomCookie=WebInspect15804ZX5968C937BF2F4C00B8CA168F18502748YF85E

Attack Response:

HTTP/1.1 403 Forbidden
Date: Tue, 28 Aug 2007 09:39:34 GMT
Server: Apache/2.0.54 (Unix) mod_ssl/2.0.54 OpenSSL/0.9.7e DAV/2 PHP/4.3.10
Content-Length: 335
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
You don't have permission to access /cgi-bin/
on this server.
<hr>
<address>Apache/2.0.54 (Unix) mod_ssl/2.0.54 OpenSSL/0.9.7e DAV/2 PHP/4.3.10 Server at 129.105.46.118 Port 80</address>
</body></html>

Low

Common Web Site Structure Directories

File Names:

- http://129.105.46.118:80/icons/
- http://129.105.46.118:80/icons/small/

Summary:

Directory Enumeration vulnerabilities were discovered within your web application. Risks associated with an attacker discovering a directory on your application server depend upon what type of directory is discovered, and what types of files are contained within it. The primary threat, other than accessing files containing sensitive information, is that an attacker can utilize the information discovered in that directory to perform other types of attacks. Recommendations include restricting access to important directories or files by adopting a "need to know" requirement for both the document and server root, and turning off features such as Automatic Directory Listings that provide information that could be utilized by an attacker when formulating or conducting an attack.

Fix:

For Security Operations:

You should evaluate the production requirements for the found directory. If the directory is not required for production operation, then the directory and its contents should be removed or restricted by a server access control mechanism. More information about implementing access control schemes can be found in the References. Automatic directory indexing should also be disabled, if applicable.

For Development:

This problem will be resolved by the web application server administrator. In general, do not rely on 'hidden' directories within the web root that can contain sensitive resources or web applications. Assume an attacker knows about the existence of all directories and files on your web site, and protect them with proper access controls.

For QA:

This problem will be resolved by the web application server administrator.

Reference:

Implementing Basic Authentication in IIS

http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/abbca505-6f63-4267-aac1-1ea89d861eb4.mspx

Implementing Basic Authentication in Apache

http://httpd.apache.org/docs/howto/auth.html#intro

Attack Request:

GET /icons/ HTTP/1.1
Referer: http://129.105.46.118:80/
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)
Pragma: no-cache
Host: 129.105.46.118
Connection: Keep-Alive
Cookie: CustomCookie=WebInspect15804ZX5968C937BF2F4C00B8CA168F18502748YF85E

Attack Response:

HTTP/1.1 200 OK
Date: Tue, 28 Aug 2007 09:39:35 GMT
Server: Apache/2.0.54 (Unix) mod_ssl/2.0.54 OpenSSL/0.9.7e DAV/2 PHP/4.3.10
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html

1000
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
 <head>
  <title>Index of /icons</title>
 </head>
 <body>
<h1>Index of /icons</h1>
<pre><img src="/icons/blank.gif" alt="Icon "> Name <a

href="?C=M;O=A">Last modified Size Description<hr><img src="/icons/back.gif" alt="[DIR]"> Parent Directory -
<img src="/icons/image2.gif" alt="[IMG]"> a.gif 21-Nov-2004 14:35 246
<img src="/icons/image2.gif" alt="[IMG]"> a.png 21-Nov-2004 14:35 293
<img src="/icons/image2.gif" alt="[IMG]"> alert.black.gif 21-Nov-2004 14:35 242
<img src="/icons/image2.gif" alt="[IMG]"> alert.black.png 21-Nov-2004 14:35 279
<img src="/icons/image2.gif" alt="[IMG]"> alert.red.gif 21-Nov-2004 14:35 247
<img src="/icons/image2.gif" alt="[IMG]"> alert.red.png 21-Nov-2004 14:35 298
<img src="/icons/image2.gif" alt="[IMG]"> apache_pb.gif 21-Nov-2004 14:35 2.3K
<img src="/icons/image2.gif" alt="[IMG]"> apache_pb.png 21-Nov-2004 14:35 1.4K
<img src="/icons/image2.gif" alt="[IMG]"> apache_pb2.gif 21-Nov-2004 14:35 2.4K
<img src="/icons/image2.gif" alt="[IMG]"> apache_pb2.png 21-Nov-2004 14:35 1.4K
<img src="/icons/image2.gif" alt="[IMG]"> apache_pb2_ani.gif 21-Nov-2004 14:35 2.1K
<img src="/icons/image2.gif" alt="[IMG]"> <a href="back.gif">back.gi ... {content removed}

Low **Database and Datafile Directories**

File Names:
- http://129.105.46.118:80/sql/

Summary: Data-related directories were discovered within your web application during a Directory Enumeration. Risks associated with an attacker discovering a directory on your application server depend upon what type of directory is discovered, and what types of files are contained within it. The primary threat, other than accessing files containing sensitive information, is that an attacker can utilize the information discovered in that directory to perform other types of attacks. Recommendations include restricting access to important directories or files by adopting a "need to know" requirement for both the document and server root, and turning off features such as Automatic Directory Listings that provide information that could be utilized by an attacker when formulating or conducting an attack.

Fix:

For Security Operations:

You should evaluate the production requirements for the found directory. If the directory is not required for production operation, then the directory and its contents should be removed or restricted by a server access control mechanism. More information about implementing access control schemes can be found in the References. Automatic directory indexing should also be disabled, if applicable.

For Development:

This problem will be resolved by the web application server administrator. In general, do not rely on 'hidden' directories within the web root that can contain sensitive resources or web applications. Assume an attacker knows about the existence of all directories and files on your web site, and protect them with proper access controls.

For QA:

This problem will be resolved by the web application server administrator.

Reference:

Implementing Basic Authentication in IIS

http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/abbca505-6f63-4267-aac1-1ea89d861eb4.mspx

Implementing Basic Authentication in Apache

http://httpd.apache.org/docs/howto/auth.html#intro

Attack Request:

GET /sql/ HTTP/1.1
Referer: http://129.105.46.118:80/
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)
Pragma: no-cache
Host: 129.105.46.118
Connection: Keep-Alive
Cookie: CustomCookie=WebInspect15804ZX5968C937BF2F4C00B8CA168F18502748YF85E

Attack Response:

HTTP/1.1 200 OK
Date: Tue, 28 Aug 2007 09:39:36 GMT
Server: Apache/2.0.54 (Unix) mod_ssl/2.0.54 OpenSSL/0.9.7e DAV/2 PHP/4.3.10
X-Powered-By: PHP/4.3.10
Content-Length: 561
Connection: close
Content-Type: text/html

<HTML>
<HEAD>
<TITLE>SQL Injection Exercise</TITLE>
<STYLE type="text/css">
BODY
{
font-family: arial;

```
}
</STYLE>
</HEAD>
<BODY>
<h2>SANS Web Application Security Workshop - SQL injection exercise </h2>
  <form name="queryform" method="POST" action="">
  Please enter a search string <BR><BR>
  <table>
  <tr>
   <td>Query String: </td><td><input type="text" name="search"></td>
  </tr>
  </table>
  <BR>
  <input type="checkbox" name="showquery">Show Query<br><br>
  <input type="submit" name="Submit" value="Submit">
  </form>
 </BODY>
</HTML>
```

Low **Documentation Directories**

File Names:
- http://129.105.46.118:80/manual/

Summary: Directory Enumeration vulnerabilities were discovered within your web application. Risks associated with an attacker discovering a directory on your application server depend upon what type of directory is discovered, and what types of files are contained within it. The primary threat, other than accessing files containing sensitive information, is that an attacker can utilize the information discovered in that directory to perform other types of attacks. Recommendations include restricting access to important directories or files by adopting a "need to know" requirement for both the document and server root, and turning off features such as Automatic Directory Listings that provide information that could be utilized by an attacker when formulating or conducting an attack.

Fix:

For Security Operations:

You should evaluate the production requirements for the found directory. If the directory is not required for production operation, then the directory and its contents should be removed or restricted by a server access control mechanism. More information about implementing access control schemes can be found in the References. Automatic directory indexing should also be disabled, if applicable.

For Development:

This problem will be resolved by the web application server administrator. In general, do not rely on 'hidden' directories within the web root that can contain sensitive resources or web applications. Assume an attacker knows about the existence of all directories and files on your web site, and protect them with proper access controls.

For QA:

This problem will be resolved by the web application server administrator.

Reference:

Implementing Basic Authentication in IIS

http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/abbca505-6f63-4267-aac1-1ea89d861eb4.mspx

Implementing Basic Authentication in Apache

http://httpd.apache.org/docs/howto/auth.html#intro

Attack Request:

```
GET /manual/ HTTP/1.1
Referer: http://129.105.46.118:80/
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)
Pragma: no-cache
Host: 129.105.46.118
Connection: Keep-Alive
Cookie: CustomCookie=WebInspect15804ZX5968C937BF2F4C00B8CA168F18502748YF85E
```

Attack Response:

```
HTTP/1.1 200 OK
Date: Tue, 28 Aug 2007 09:39:37 GMT
Server: Apache/2.0.54 (Unix) mod_ssl/2.0.54 OpenSSL/0.9.7e DAV/2 PHP/4.3.10
Content-Location: index.html.en
Vary: negotiate,accept-language,accept-charset
TCN: choice
Last-Modified: Sun, 20 Feb 2005 11:09:12 GMT
ETag: "1c1d-1d0a-6099a600;1c1c-25b-6099a600"
Accept-Ranges: bytes
Content-Length: 7434
Connection: close
Content-Type: text/html
Content-Language: en

<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" lang="en" xml:lang="en"><head><!--
      XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
           This file is generated from xml source: DO NOT EDIT
      XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

-->
<title>Apache HTTP Server Version 2.0 Documentation - Apache HTTP Server</title>
<link href="./style/css/manual.css" rel="stylesheet" media="all" type="text/css" title="Main stylesheet" />
<link href="./style/css/manual-loose-100pc.css" rel="alternate stylesheet" media="all" type="text/css" title="No Sidebar - Default font size" />
<link href="./style/css/manual-print.css" rel="stylesheet" media="print" type="text/css" />
<link href="./images/favicon.ico" rel="shortcut icon" /></head>
<body id="index-page">

Modules | Directives | FAQ | Glossary | Sitemap
Apache HTTP Server Version 2.0

<img title="<-" alt="<-" src="./images/left.gif" />

Apache > HTTP Server > Documentation</d ... {content removed}

Low **Unix-Related Directories**

File Names:
- http://129.105.46.118:80/~nobody/

Summary:
Unix-related directories were discovered within your web application during a Directory Enumeration scan. Risks associated with an attacker discovering a directory on your application server depend upon what type of directory is discovered, and what types of files are contained within it. The primary threat, other than accessing files containing sensitive information, is that an attacker can utilize the information discovered in that directory to perform other types of attacks. Recommendations include restricting access to important directories or files by adopting a "need to know" requirement for both the document and server root, and turning off features such as Automatic Directory Listings that provide information that could be utilized by an attacker when formulating or conducting an attack.

Fix:

For Security Operations:

You should evaluate the production requirements for the found directory. If the directory is not required for production operation, then the directory and its contents should be removed or restricted by a server access control mechanism. More information about implementing access control schemes can be found in the References. Automatic directory indexing should also be disabled, if applicable.

For Development:

This problem will be resolved by the web application server administrator. In general, do not rely on 'hidden' directories within the web root that can contain sensitive resources or web applications. Assume an attacker knows about the existence of all directories and files on your web site, and protect them with proper access controls.

For QA:

This problem will be resolved by the web application server administrator.

Reference:

Implementing Basic Authentication in IIS

http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/abbca505-6f63-4267-aac1-1ea89d861eb4.mspx

Implementing Basic Authentication in Apache

http://httpd.apache.org/docs/howto/auth.html#intro

Attack Request:

```
GET /~nobody/ HTTP/1.1
Referer: http://129.105.46.118:80/
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)
Pragma: no-cache
Host: 129.105.46.118
Connection: Keep-Alive
Cookie: CustomCookie=WebInspect15804ZX5968C937BF2F4C00B8CA168F18502748YF85E
```

Attack Response:

```
HTTP/1.1 403 Forbidden
Date: Tue, 28 Aug 2007 09:39:43 GMT
Server: Apache/2.0.54 (Unix) mod_ssl/2.0.54 OpenSSL/0.9.7e DAV/2 PHP/4.3.10
Content-Length: 454
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access /~nobody/
on this server.</p>
<p>Additionally, a 403 Forbidden
error was encountered while trying to use an ErrorDocument to handle the request.</p>
<hr>
<address>Apache/2.0.54 (Unix) mod_ssl/2.0.54 OpenSSL/0.9.7e DAV/2 PHP/4.3.10 Server at
129.105.46.118 Port 80</address>
</body></html>
```

Low **Web Application Common Directories**

File Names:
- http://129.105.46.118:80/forms/

Summary: Directory Enumeration vulnerabilities were discovered within your web application. Risks associated with an attacker discovering a directory on your application server depend upon what type of directory is discovered, and what types of files are contained within it. The primary threat, other than accessing files containing sensitive information, is that an attacker can utilize the information discovered in that directory to perform other types of attacks. Recommendations include restricting access to important directories or files by adopting a "need to know" requirement for both the document and server root, and turning off features such as Automatic Directory Listings that provide information that could be utilized by an attacker when formulating or conducting an attack.

Fix:

For Security Operations:

You should evaluate the production requirements for the found directory. If the directory is not required for production operation, then the directory and its contents should be removed or restricted by a server access control mechanism. More information about implementing access control schemes can be found in the References. Automatic directory indexing should also be disabled, if applicable.

For Development:

This problem will be resolved by the web application server administrator. In general, do not rely on 'hidden' directories within the web root that can contain sensitive resources or web applications. Assume an attacker knows about the existence of all directories and files on your web site, and protect them with proper access controls.

For QA:

This problem will be resolved by the web application server administrator.

Reference:

Implementing Basic Authentication in IIS

http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/abbca505-6f63-4267-aac1-1ea89d861eb4.mspx

Implementing Basic Authentication in Apache

http://httpd.apache.org/docs/howto/auth.html#intro

Attack Request:

```
GET /forms/ HTTP/1.1
Referer: http://129.105.46.118:80/
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)
Pragma: no-cache
Host: 129.105.46.118
Connection: Keep-Alive
Cookie: CustomCookie=WebInspect15804ZX5968C937BF2F4C00B8CA168F18502748YF85E
```

Attack Response:

```
HTTP/1.1 200 OK
Date: Tue, 28 Aug 2007 09:39:26 GMT
Server: Apache/2.0.54 (Unix) mod_ssl/2.0.54 OpenSSL/0.9.7e DAV/2 PHP/4.3.10
X-Powered-By: PHP/4.3.10
Content-Length: 505
Connection: close
Content-Type: text/html

<html>
<META HTTP-EQUIV="CACHE-CONTROL" CONTENT="NO-CACHE">
<h1>Login</h1>

<form name="form" method="post" action="/forms/index.php">
   <p><label for="txtUsername">Username:</label>
   <br /><input type="text" title="Enter your Username" name="txtUsername" /></p>

   <p><label for="txtpassword">Password:</label>
   <br /><input type="password" title="Enter your password" name="txtPassword" /></p>

   <p><input type="submit" name="Submit" value="Login" /></p>

</form>
</html>
```

Best Practice

Potential filename found in comments

File Names:
- http://129.105.46.118:80/manual/style/xsl/common.xsl
- http://129.105.46.118:80/manual/ru/style/xsl/common.xsl
- http://129.105.46.118:80/manual/ru/style/xsl/directiveindex.xsl
- http://129.105.46.118:80/manual/ru/style/xsl/faq.xsl
- http://129.105.46.118:80/manual/ru/style/xsl/indexpage.xsl
- http://129.105.46.118:80/manual/ru/style/xsl/manualpage.xsl
- http://129.105.46.118:80/manual/ru/style/xsl/moduleindex.xsl
- http://129.105.46.118:80/manual/ru/style/xsl/quickreference.xsl
- http://129.105.46.118:80/manual/ru/style/xsl/sitemap.xsl
- http://129.105.46.118:80/manual/ru/style/xsl/synopsis.xsl
- http://129.105.46.118:80/manual/ko/style/xsl/common.xsl
- http://129.105.46.118:80/manual/ko/style/xsl/directiveindex.xsl
- http://129.105.46.118:80/manual/ko/style/xsl/faq.xsl
- http://129.105.46.118:80/manual/ko/style/xsl/indexpage.xsl
- http://129.105.46.118:80/manual/ko/style/xsl/manualpage.xsl
- http://129.105.46.118:80/manual/ko/style/xsl/moduleindex.xsl
- http://129.105.46.118:80/manual/ko/style/xsl/quickreference.xsl

- http://129.105.46.118:80/manual/ko/style/xsl/sitemap.xsl
- http://129.105.46.118:80/manual/ko/style/xsl/synopsis.xsl
- http://129.105.46.118:80/manual/ja/style/xsl/common.xsl
- http://129.105.46.118:80/manual/ja/style/xsl/directiveindex.xsl
- http://129.105.46.118:80/manual/ja/style/xsl/faq.xsl
- http://129.105.46.118:80/manual/ja/style/xsl/indexpage.xsl
- http://129.105.46.118:80/manual/ja/style/xsl/manualpage.xsl
- http://129.105.46.118:80/manual/ja/style/xsl/moduleindex.xsl
- http://129.105.46.118:80/manual/ja/style/xsl/quickreference.xsl
- http://129.105.46.118:80/manual/ja/style/xsl/sitemap.xsl
- http://129.105.46.118:80/manual/ja/style/xsl/synopsis.xsl
- http://129.105.46.118:80/manual/fr/style/xsl/common.xsl
- http://129.105.46.118:80/manual/fr/style/xsl/directiveindex.xsl
- http://129.105.46.118:80/manual/fr/style/xsl/faq.xsl
- http://129.105.46.118:80/manual/fr/style/xsl/indexpage.xsl
- http://129.105.46.118:80/manual/fr/style/xsl/manualpage.xsl
- http://129.105.46.118:80/manual/fr/style/xsl/moduleindex.xsl
- http://129.105.46.118:80/manual/fr/style/xsl/quickreference.xsl
- http://129.105.46.118:80/manual/fr/style/xsl/sitemap.xsl
- http://129.105.46.118:80/manual/fr/style/xsl/synopsis.xsl
- http://129.105.46.118:80/manual/es/style/xsl/common.xsl
- http://129.105.46.118:80/manual/es/style/xsl/directiveindex.xsl
- http://129.105.46.118:80/manual/es/style/xsl/faq.xsl
- http://129.105.46.118:80/manual/es/style/xsl/indexpage.xsl
- http://129.105.46.118:80/manual/es/style/xsl/manualpage.xsl
- http://129.105.46.118:80/manual/es/style/xsl/moduleindex.xsl
- http://129.105.46.118:80/manual/es/style/xsl/quickreference.xsl
- http://129.105.46.118:80/manual/es/style/xsl/sitemap.xsl
- http://129.105.46.118:80/manual/es/style/xsl/synopsis.xsl
- http://129.105.46.118:80/manual/en/style/xsl/common.xsl
- http://129.105.46.118:80/manual/en/style/xsl/directiveindex.xsl
- http://129.105.46.118:80/manual/en/style/xsl/faq.xsl
- http://129.105.46.118:80/manual/en/style/xsl/indexpage.xsl
- http://129.105.46.118:80/manual/en/style/xsl/manualpage.xsl
- http://129.105.46.118:80/manual/en/style/xsl/moduleindex.xsl
- http://129.105.46.118:80/manual/en/style/xsl/quickreference.xsl
- http://129.105.46.118:80/manual/en/style/xsl/sitemap.xsl
- http://129.105.46.118:80/manual/en/style/xsl/synopsis.xsl
- http://129.105.46.118:80/manual/de/style/xsl/common.xsl
- http://129.105.46.118:80/manual/de/style/xsl/directiveindex.xsl
- http://129.105.46.118:80/manual/de/style/xsl/faq.xsl
- http://129.105.46.118:80/manual/de/style/xsl/indexpage.xsl
- http://129.105.46.118:80/manual/de/style/xsl/manualpage.xsl
- http://129.105.46.118:80/manual/de/style/xsl/moduleindex.xsl
- http://129.105.46.118:80/manual/de/style/xsl/quickreference.xsl
- http://129.105.46.118:80/manual/de/style/xsl/sitemap.xsl
- http://129.105.46.118:80/manual/de/style/xsl/synopsis.xsl
- http://129.105.46.118:80/manual/style/xsl/directiveindex.xsl
- http://129.105.46.118:80/manual/style/xsl/faq.xsl
- http://129.105.46.118:80/manual/style/xsl/indexpage.xsl
- http://129.105.46.118:80/manual/style/xsl/manualpage.xsl
- http://129.105.46.118:80/manual/style/xsl/moduleindex.xsl
- http://129.105.46.118:80/manual/style/xsl/quickreference.xsl
- http://129.105.46.118:80/manual/style/xsl/sitemap.xsl
- http://129.105.46.118:80/manual/style/xsl/synopsis.xsl

Summary: A URL or filename was found in the comments of the file.

Attack Request:
```
GET /manual/style/xsl/common.xsl HTTP/1.1
Referer: http://129.105.46.118:80/manual/style/manual.de.xsl
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)
Pragma: no-cache
Host: 129.105.46.118
Connection: Keep-Alive
Cookie:
CustomCookie=WebInspect15804ZX5968C937BF2F4C00B8CA168F18502748YF85E;PHPSESSID=0286af493a
cdaf996469d378e8cb3ea1;
```

Attack Response:
```
HTTP/1.1 200 OK
Date: Tue, 28 Aug 2007 10:07:14 GMT
Server: Apache/2.0.54 (Unix) mod_ssl/2.0.54 OpenSSL/0.9.7e DAV/2 PHP/4.3.10
Last-Modified: Sat, 19 Feb 2005 14:36:22 GMT
ETag: "1eb0-a14d-27a50580"
Accept-Ranges: bytes
Content-Length: 41293
Connection: close
Content-Type: application/xml

<?xml version="1.0"?>
```

```
<!--
 Copyright 2002-2005 The Apache Software Foundation or its licensors, as
 applicable.

 Licensed under the Apache License, Version 2.0 (the "License");
 you may not use this file except in compliance with the License.
 You may obtain a copy of the License at

     http://www.apache.org/licenses/LICENSE-2.0

 Unless required by applicable law or agreed to in writing, software
 distributed under the License is distributed on an "AS IS" BASIS,
 WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
 See the License for the specific language governing permissions and
 limitations under the License.
-->

<!DOCTYPE xsl:stylesheet [
   <!ENTITY nbsp SYSTEM "util/nbsp.xml">
   <!ENTITY lf SYSTEM "util/lf.xml">
]>
<xsl:stylesheet version="1.0"
           xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
              xmlns="http://www.w3.org/1999/xhtml">

<!--                                                    -->
<!-- Please, don't hard-code output strings! Use the language          -->
<!-- files and the translation "stuff"...                              -->
<!--                                                    -->

<!-- Injected variables:                                          -->
<!--   $is-chm         - (boolean) target is for CHM generation or not   -->
<!--   $is-zip         - (boolean) target is for ZIP generation or not   -->
<!--   $message        - (node-set) localized common text snippets       -->
<!--   $doclang        - (string) document language                      -->
<!--   $output-encoding - (string) MIME charset name of the output       -->
<!--                   encoding                ... {content removed}
```

Best Practice **Privacy Policy Not Present**

File Names:
- http://129.105.46.118:80/privacy.html
- http://129.105.46.118:80/privacy.htm

Summary: WebInspect has failed to find a Privacy Policy available within your web application. This check is associated with WebInspect's compliance policies. Many legislative initiatives require that organizations place a publicly accessible document within their web application that defines their information privacy policy. As a general rule, these information privacy policies must detail what information an organization collects, the purpose for collecting it, potential avenues of disclosure, and any methods of addressing potential grievances. Recommendations include adding an accessible and comprehensive privacy policy to your web application, and providing a link to that resource on every page that requests information from users.

Descriptions:

Any standard web application privacy policy should include the following components:
- A description of the intended purpose for collecting the data.
- A description of the use of the data.
- Methods for limiting the use and disclosure of the information.
- A list of the types of third parties to whom the information might be disclosed.
- Contact information for inquires and complaints.

Attack Request:

```
GET /privacy.html HTTP/1.1
Referer: http://129.105.46.118:80/
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)
Pragma: no-cache
Host: 129.105.46.118
Connection: Keep-Alive
Cookie: CustomCookie=WebInspect15804ZX5968C937BF2F4C00B8CA168F18502748YF85E
```

Attack Response:

```
HTTP/1.1 404 Not Found
Date: Tue, 28 Aug 2007 09:39:49 GMT
Server: Apache/2.0.54 (Unix) mod_ssl/2.0.54 OpenSSL/0.9.7e DAV/2 PHP/4.3.10
Content-Length: 335
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL /privacy.html was not found on this server.</p>
<hr>
<address>Apache/2.0.54 (Unix) mod_ssl/2.0.54 OpenSSL/0.9.7e DAV/2 PHP/4.3.10 Server at
```

129.105.46.118 Port 80</address>
</body></html>