
HOYT LLC
http://hoytllc.com
Strategic Consulting

Hoyt LLC Audit Report

Site report for www.sailinganarchy.com

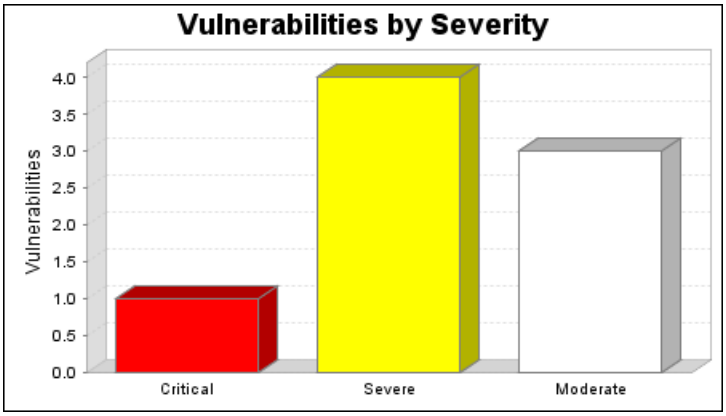
Audited on July 20 2010

1. Executive Summary

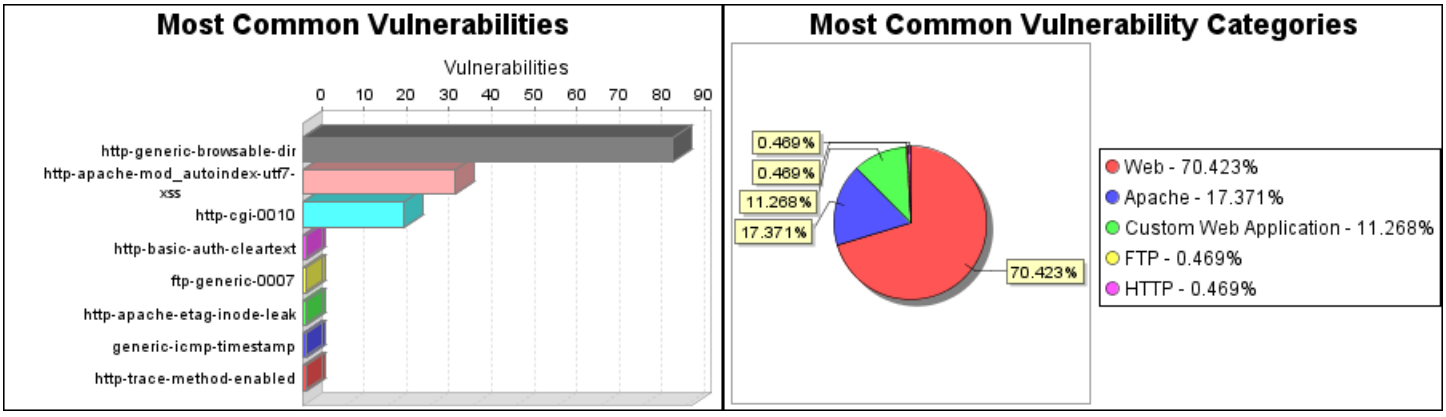
This report represents a security audit performed by Hoyt LLC. It contains confidential information about the state of your network. Access to this information by unauthorized personnel may allow them to compromise your network.

Site Name	Start Time	End Time	Total Time	Status
www.sailinganarchy.com	July 20, 2010 14:32, EDT	July 20, 2010 15:05, EDT	32 minutes	Success

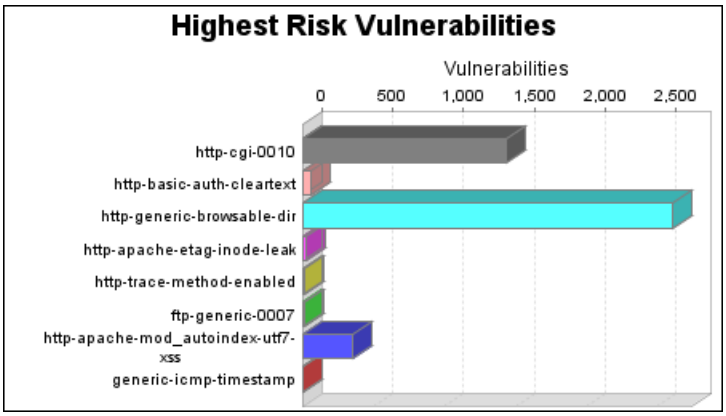
The audit was performed on one system which was found to be active and was scanned.



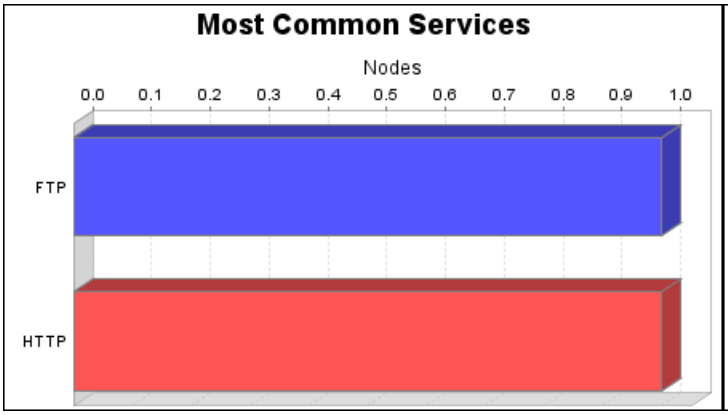
There were 8 vulnerabilities found during this scan. One critical vulnerability was found. Critical vulnerabilities require immediate attention. They are relatively easy for attackers to exploit and may provide them with full control of the affected systems. 4 vulnerabilities were severe. Severe vulnerabilities are often harder to exploit and may not provide the same access to affected systems. There were 3 moderate vulnerabilities discovered. These often provide information to attackers that may assist them in mounting subsequent attacks on your network. These should also be fixed in a timely manner, but are not as urgent as the other vulnerabilities.



There were 87 occurrences of the http-generic-browsable-dir vulnerability, making it the most common vulnerability. There were 150 vulnerabilities in the Web category, making it the most common vulnerability category.



The http-cgi-0010 vulnerability poses the highest risk to the organization with a risk score of 1,440. Vulnerability risk scores are calculated by looking at the likelihood of attack and impact, based upon CVSS metrics. The impact and likelihood are then multiplied by the number of instances of the vulnerability to come up with the final risk score.
One operating system was identified during this scan.
There were 2 services found to be running during this scan.



The FTP and HTTP services were found on 1 systems, making them the most common services. The HTTP service was found to have the most vulnerabilities during this scan with 150 vulnerabilities.

2. Discovered Systems

Node	Operating System	Risk	Aliases
216.9.43.114	Cisco IOS 15.0)	1.78	•www.sailinganarchy.com

3. Discovered and Potential Vulnerabilities

3.1. Critical Vulnerabilities

3.1.1. HTTP Basic Authentication Enabled (http-basic-auth-cleartext)

Description:

The HTTP Basic Authentication scheme is not considered to be a secure method of user authentication (unless used in conjunction with some external secure system such as TLS/SSL), as the user name and password are passed over the network as cleartext.

Affected Nodes:

Affected Nodes:	Additional Information:
216.9.43.114:80 (www.sailinganarchy.com)	Running vulnerable HTTP service. http://www.sailinganarchy.com/stats/ `1: Basic realm="sailinganarchy.com authentication"`

References:

Source	Reference
URL	http://tools.ietf.org/html/rfc2617

Vulnerability Solution:

•Use Basic Authentication over TLS/SSL (HTTPS)

Enable HTTPS on the Web server. The TLS/SSL protocol will protect cleartext Basic Authentication credentials.

•Use Digest Authentication

Replace Basic Authentication with the alternative Digest Authentication scheme. By modern cryptographic standards Digest Authentication is weak. But for a large range of purposes it is valuable as a replacement for Basic Authentication. It remedies some, but not all, weaknesses of Basic Authentication. See RFC 2617, section 4. Security Considerations for more information.

3.2. Severe Vulnerabilities

3.2.1. FTP server does not support AUTH command (ftp-generic-0007)

Description:

FTP clients send credentials (user ID and password) in clear text to the FTP server by default. This allows malicious users to intercept the credentials if they can eavesdrop on the connection.

Newer FTP servers support the AUTH command, which provides enhanced authentication options such as TLS, Kerberos, GSSAPI, etc. This should be used to prevent eavesdropping on FTP connections.

Affected Nodes:

Affected Nodes:	Additional Information:
216.9.43.114:21 (www.sailinganarchy.com)	Server supports none of the following AUTH mechanisms: TLS TLS-C KERBEROS_V4 GSSAPI SSL

References:

None

Vulnerability Solution:

Upgrade/migrate to a FTP server that supports the AUTH command.

3.2.2. Cross Site Scripting Vulnerability (http-cgi-0010)

Description:

The web application is vulnerable to cross-site scripting (XSS). Cross-site scripting vulnerabilities allow malicious attackers to take advantage of web server scripts to inject JavaScript or HTML code that is executed on the client-side browser. This is often caused by server-side scripts written in languages such as PHP, ASP, .NET, Perl or Java that do not adequately filter data sent along with page requests. This malicious code will appear to come from your web application when it runs in the browser of an unsuspecting user.

An exploit script can be made to:

•access other sites inside another client's private intranet.

•steal another client's cookie(s).

•modify another client's cookie(s).

•steal another client's submitted form data.

•modify another client's submitted form data (before it reaches the server).

•submit a form to your application on the user's behalf which modifies passwords or other application data

The two most common methods of attack are:

•Clicking on a URL link sent in an e-mail

•Clicking on a URL link while visiting a website

In both scenarios, the URL will generally link to the trusted site, but will contain additional data that is used to trigger the XSS attack.

Note that SSL connectivity does not protect against this issue.

Affected Nodes:

Affected Nodes:	**Additional Information:**
216.9.43.114:80 (www.sailinganarchy.com)	Running vulnerable HTTP service. http://www.sailinganarchy.com/php/ask.php/<script>xss</script> 21: <font face="Arial, Helvetica, sans-serif" size="3" color... 22: is where you get to ask questions that you've always want... 23: in the sport but didn't know who to ask. Pick the profess... 24: question, and we'll find the answer. 25: ..."/php/ask.php/<script>xss</script>">
216.9.43.114:80 (www.sailinganarchy.com)	Injected into the "from_addr" form parameter on http://www.sailinganarchy.com/php/ask.php: 34: <tr> 35: <td width="145" align="right" valign="top" nowrap class... 36: Email:<font color="#003399" size="2" face="Arial, Hel... 37: <td width="495" align="left" valign="top"><input name="... 38: value = "<script>nxpxsstest">
216.9.43.114:80 (www.sailinganarchy.com)	Injected into the "from_name" form parameter on http://www.sailinganarchy.com/php/ask.php : 27: <tr> 28: <td width="145" align="right" valign="top" nowrap class... 29: Name:<font color="#003399" size="2" face="Arial, Helv... 30: <td width="495" align="left" valign="top"><input name="... 31: value = "<script>nxpxsstest">
216.9.43.114:80 (www.sailinganarchy.com)	Injected into the "question1" form parameter on http://www.sailinganarchy.com/php/ask.php: 45: <select name="profession"><option value="">Pick One</... 46: </tr> 47: <tr>

Affected Nodes:	Additional Information:
	48: <td width="145" align="right" valign="top" nowrap class... 49: ...="qQuestion1"><script>nxpxsstest</textarea></td>
216.9.43.114:80 (www.sailinganarchy.com)	Injected into the "question2" form parameter on http://www.sailinganarchy.com/php/ask.php: 50: </tr> 51: <tr> 52: <td width="145" align="right" valign="top" nowrap class... 53: 2:</td> 54: ...d="question2"><script>nxpxsstest</textarea></td>
216.9.43.114:80 (www.sailinganarchy.com)	Injected into the "question3" form parameter on http://www.sailinganarchy.com/php/ask.php: 55: </tr> 56: <tr> 57: <td width="145" align="right" valign="top" nowrap class... 58: 3:</td> 59: ...d="question3"><script>nxpxsstest</textarea></td>
216.9.43.114:80 (www.sailinganarchy.com)	Running vulnerable HTTP service. http://www.sailinganarchy.com/search.php/<script>xss</script> 81: 82: 83: 84: 85: ...="/search.php/<script>xss</script>" target="_self" method="post" na...
216.9.43.114:80 (www.sailinganarchy.com)	Running vulnerable HTTP service. http://www.sailinganarchy.com/z_search.php/<script>xss</script> 212: 213: 214: 215: 216: .../z_search.php/<script>xss</script>" target="_self" method="post" na...
216.9.43.114:80 (www.sailinganarchy.com)	Injected into the "a" URL parameter in http://www.sailinganarchy.com/a_link.php?a=http://www.sailinganarchy.com/article.php?get=5908 by changing the URL to http://www.sailinganarchy.com/a_link.php?a=http://www.sailinganarchy.com/a=<script>nxpxsstestrticle.php?get=5908 9: 10: <font face="Arial, Helvetica, sans-serif">Copy the link <...

Affected Nodes:	Additional Information:
	11: 12: <p> 13: ...anarchy.com/a=<script>nxpxsstestrticle.php?get=5908" />
216.9.43.114:80 (www.sailinganarchy.com)	Running vulnerable HTTP service. http://www.sailinganarchy.com/article_submission.php/<script>xss</script> 16: Submit your Article to the Editor</str... 17: <table width="900" align="center" cellpadding="5" cellspacing="5"> 18: <tr> 19: <td> 20: ...ubmission.php/<script>xss</script>">
216.9.43.114:80 (www.sailinganarchy.com)	Injected into the "from_addr" form parameter on http://www.sailinganarchy.com/contact_editor.php: 33: </tr> 34: <tr> 35: <td width="150" align="right" valign="top" nowrap class="bold_s... 36: email:</td> 37: ...255" value = "<script>nxpxsstest">
216.9.43.114:80 (www.sailinganarchy.com)	Injected into the "from_addr" form parameter on http://www.sailinganarchy.com/article_submission.php: 28: </tr> 29: <tr> 30: <td align="right" valign="top" nowrap class="bold_standard_text... 31: email:</td> 32: ...255" value = "<script>nxpxsstest">
216.9.43.114:80 (www.sailinganarchy.com)	Injected into the "from_name" form parameter on http://www.sailinganarchy.com/article_submission.php: 22: <tr> 23: <td width="140" align="right" valign="top" nowrap class="bol... 24: <td align="left" valign="top"> 25: <input name="from_name" type="text" id="from_name" size="7... 26: value="<script>nxpxsstest">
216.9.43.114:80 (www.sailinganarchy.com)	Injected into the "title" form parameter on http://www.sailinganarchy.com/article_submission.php: 35: <tr> 36: <td align="right" valign="top" nowrap class="bold_standard_text...

Affected Nodes:	Additional Information:
	37: </td> 38: <td align="left" valign="top"> 39: ...255" value = "<script>nxpxsstest">
216.9.43.114:80 (www.sailinganarchy.com)	Injected into the "cname" form parameter on http://www.sailinganarchy.com/cgi-bin/sachat/bluechat.cgi: 3: </head> 4: <frameset cols="150,*"> 5: <frameset rows="150,*"> 6: <frame name="logo" scrolling="no" noresize src="bc_logo.cgi"> 7: ...nds.cgi?cname=<script>nxpxsstest">
216.9.43.114:80 (www.sailinganarchy.com)	Injected into the "cname" form parameter on http://www.sailinganarchy.com/cgi-bin/sachat/bluechat.cgi: 3: </head> 4: <frameset cols="150,*"> 5: <frameset rows="150,*"> 6: <frame name="logo" scrolling="no" noresize src="bc_logo.cgi"> 7: ...nds.cgi?cname=<script>nxpxsstest">
216.9.43.114:80 (www.sailinganarchy.com)	Running vulnerable HTTP service. http://www.sailinganarchy.com/contact_admin.php/<script>xss</script> 22: If you have a question about... 23: Please Click Here 24: 25: 26: ...act_admin.php/<script>xss</script>">
216.9.43.114:80 (www.sailinganarchy.com)	Injected into the "comments" form parameter on http://www.sailinganarchy.com/contact_admin.php: 51: you want to start a 52: new paragraph 53: make 54: sure to hit enter twice </td> 55: ...id="comments"><script>nxpxsstest</textarea></td>
216.9.43.114:80 (www.sailinganarchy.com)	Injected into the "from_addr" form parameter on http://www.sailinganarchy.com/contact_admin.php: 34: </tr> 35: <tr> 36: <td width="150" align="right" valign="top" nowrap class="bold_s... 37: email:</td> 38: ...255" value = "<script>nxpxsstest">

Affected Nodes:	Additional Information:
216.9.43.114:80 (www.sailinganarchy.com)	Injected into the "from_name" form parameter on http://www.sailinganarchy.com/contact_admin.php: 28: <tr> 29: <td align="right" valign="top" nowrap class="bold_standard_t... 30: <td align="left" valign="top"> 31: <input name="from_name" type="text" id="from_name" size="5... 32: value="<script>nxpxsstest">
216.9.43.114:80 (www.sailinganarchy.com)	Running vulnerable HTTP service. http://www.sailinganarchy.com/contact_editor.php/<script>xss</script> 21: To submit an article please use <a ... 22: For Technical Issues <a href="/contact_admin.php">Contact the ... 23: 24: 25: ...ct_editor.php/<script>xss</script>">
216.9.43.114:80 (www.sailinganarchy.com)	Injected into the "comments" form parameter on http://www.sailinganarchy.com/contact_editor.php: 50: you want to start a 51: new paragraph 52: make 53: sure to hit enter twice </td> 54: ...id="comments"><script>nxpxsstest</textarea></td>
216.9.43.114:80 (www.sailinganarchy.com)	Injected into the "comments" form parameter on http://www.sailinganarchy.com/article_submission.php: 57: 58: 59: 60: </td> 61: ...id="comments"><script>nxpxsstest</textarea>
216.9.43.114:80 (www.sailinganarchy.com)	Injected into the "from_name" form parameter on http://www.sailinganarchy.com/contact_editor.php: 27: <tr> 28: <td align="right" valign="top" nowrap class="bold_standard_t... 29: <td align="left" valign="top"> 30: <input name="from_name" type="text" id="from_name" size="5... 31: value="<script>nxpxsstest">

References:

Source	Reference
CERT	CA-2000-02
URL	http://en.wikipedia.org/wiki/Cross_site_scripting

Vulnerability Solution:

Audit the affected url and other similar dynamic pages or scripts that could be relaying untrusted malicious data from the user input. In general, the following practices should be followed while developing dynamic web content:

•Explicitly set the character set encoding for each page generated by the web server

•Identify special characters

•Encode dynamic output elements

•Filter specific characters in dynamic elements

•Examine cookies

For more information on the above practices, read the following CERT advisory: CERT Advisory CA-2000-02

•For ASP.NET applications, the validateRequest attribute can be added to the page or the web.config. For example:

```
<%@ Page ... validateRequest="true" %>

OR

<system.web>
 <pages validateRequest="true" />
</system.web>
```

In addition, all dynamic content should be HTML encoded using HTTPUtility.HTMLEncode.

•For PHP applications, input data should be validated using functions such as strip_tags and utf8_decode. Dynamic content should be HTML encoded using htmlentities.

•For Perl applications, input data should be validated whenever possible using regular expressions. Dynamic content should be HTML encoded using HTML::Entities::encode or Apache::Util::html_encode (when using mod_perl).

3.2.3. Browsable web directory (http-generic-browsable-dir)

Description:

A web directory was found to be browsable, which means that anyone can see the contents of the directory. These directories can be found:

•via page spidering (following hyperlinks), or
•as part of a parent path (checking each directory along the path and searching for "Directory Listing" or similar strings), or
•by brute forcing a list of common directories.

Browsable directories could allow an attacker to view "hidden" files in the web root, including CGI scripts, data files, or backup pages.

Affected Nodes:

Affected Nodes:	**Additional Information:**
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/cst_composites/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/cst_composites</title> 5: </head> 6: <body> 7: Index of /ADs/cst_composites 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/devoti/ 4: <title>Index of /ADs/devoti</title> 5: </head> 6: <body> 7: Index of /ADs/devoti 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/devoti/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/devoti</title> 5: </head> 6: <body> 7: Index of /ADs/devoti 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/dimension/ 4: <title>Index of /ADs/dimension</title> 5: </head> 6: <body> 7: Index of /ADs/dimension 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/dimension/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/dimension</title>

Affected Nodes:	Additional Information:
	5: </head> 6: <body> 7: Index of /ADs/dimension 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/dimension/_notes/ 4: <title>Index of /ADs/dimension/_notes</title> 5: </head> 6: <body> 7: Index of /ADs/dimension/_notes 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/dimension/_notes/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/dimension/_notes</title> 5: </head> 6: <body> 7: Index of /ADs/dimension/_notes 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/dirtydog/ 4: <title>Index of /ADs/dirtydog</title> 5: </head> 6: <body> 7: Index of /ADs/dirtydog 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/dirtydog/_notes/ 4: <title>Index of /ADs/dirtydog/_notes</title> 5: </head> 6: <body> 7: Index of /ADs/dirtydog/_notes 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/dirtydog/glasses/ 4: <title>Index of /ADs/dirtydog/glasses</title> 5: </head> 6: <body> 7: Index of /ADs/dirtydog/glasses 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80	http://www.sailinganarchy.com/ADs/edson_marine/

Affected Nodes:	Additional Information:
(www.sailinganarchy.com)	4: <title>Index of /ADs/edson_marine</title> 5: </head> 6: <body> 7: Index of /ADs/edson_marine 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/edson_marine/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/edson_marine</title> 5: </head> 6: <body> 7: Index of /ADs/edson_marine 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/euro_marine/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/euro_marine</title> 5: </head> 6: <body> 7: Index of /ADs/euro_marine 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/euro_marine/ 4: <title>Index of /ADs/euro_marine</title> 5: </head> 6: <body> 7: Index of /ADs/euro_marine 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/evolution_sails/ 4: <title>Index of /ADs/evolution_sails</title> 5: </head> 6: <body> 7: Index of /ADs/evolution_sails 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/farr/ 4: <title>Index of /ADs/farr</title> 5: </head> 6: <body> 7: Index of /ADs/farr 8: ... alt="[DIR]"> Parent Directory ...

Affected Nodes:	Additional Information:
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/farr/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/farr</title> 5: </head> 6: <body> 7: Index of /ADs/farr 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/farr/_notes/ 4: <title>Index of /ADs/farr/_notes</title> 5: </head> 6: <body> 7: Index of /ADs/farr/_notes 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/farr/_notes/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/farr/_notes</title> 5: </head> 6: <body> 7: Index of /ADs/farr/_notes 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/farrier/ 4: <title>Index of /ADs/farrier</title> 5: </head> 6: <body> 7: Index of /ADs/farrier 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/farrier/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/farrier</title> 5: </head> 6: <body> 7: Index of /ADs/farrier 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/finn/ 4: <title>Index of /ADs/finn</title> 5: </head> 6: <body> 7: Index of /ADs/finn 8: ... alt="[DIR]"> Parent Directory ...

Affected Nodes:	Additional Information:
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/finn/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/finn</title> 5: </head> 6: <body> 7: Index of /ADs/finn 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/flexfold/ 4: <title>Index of /ADs/flexfold</title> 5: </head> 6: <body> 7: Index of /ADs/flexfold 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/flexfold/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/flexfold</title> 5: </head> 6: <body> 7: Index of /ADs/flexfold 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/flyingtiger/ 4: <title>Index of /ADs/flyingtiger</title> 5: </head> 6: <body> 7: Index of /ADs/flyingtiger 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/flyingtiger/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/flyingtiger</title> 5: </head> 6: <body> 7: Index of /ADs/flyingtiger 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/flyingtiger/_notes/ 4: <title>Index of /ADs/flyingtiger/_notes</title> 5: </head> 6: <body> 7: Index of /ADs/flyingtiger/_notes 8: ... alt="[DIR]"> Parent Directory ...

Affected Nodes:	Additional Information:
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/flyingtiger/_notes/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/flyingtiger/_notes</title> 5: </head> 6: <body> 7: Index of /ADs/flyingtiger/_notes 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/goetz/ 4: <title>Index of /ADs/goetz</title> 5: </head> 6: <body> 7: Index of /ADs/goetz 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/gunboat/ 4: <title>Index of /ADs/gunboat</title> 5: </head> 6: <body> 7: Index of /ADs/gunboat 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/gunboat/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/gunboat</title> 5: </head> 6: <body> 7: Index of /ADs/gunboat 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/halifax_saint_pierre/ 4: <title>Index of /ADs/halifax_saint_pierre</title> 5: </head> 6: <body> 7: Index of /ADs/halifax_saint_pierre 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/halifax_saint_pierre/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/halifax_saint_pierre</title> 5: </head>

Affected Nodes:	Additional Information:
	6: <body> 7: Index of /ADs/halifax_saint_pierre 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/heineken/ 4: <title>Index of /ADs/heineken</title> 5: </head> 6: <body> 7: Index of /ADs/heineken 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/isailfast/ 4: <title>Index of /ADs/isailfast</title> 5: </head> 6: <body> 7: Index of /ADs/isailfast 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/isailfast/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/isailfast</title> 5: </head> 6: <body> 7: Index of /ADs/isailfast 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/isailfast/_notes/ 4: <title>Index of /ADs/isailfast/_notes</title> 5: </head> 6: <body> 7: Index of /ADs/isailfast/_notes 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/isailfast/_notes/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/isailfast/_notes</title> 5: </head> 6: <body> 7: Index of /ADs/isailfast/_notes 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80	http://www.sailinganarchy.com/ADs/jk3yachtsales/

Affected Nodes:	Additional Information:
(www.sailinganarchy.com)	4: <title>Index of /ADs/jk3yachtsales</title> 5: </head> 6: <body> 7: Index of /ADs/jk3yachtsales 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/jk3yachtsales/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/jk3yachtsales</title> 5: </head> 6: <body> 7: Index of /ADs/jk3yachtsales 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/kinsale/ 4: <title>Index of /ADs/kinsale</title> 5: </head> 6: <body> 7: Index of /ADs/kinsale 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/landing_school/ 4: <title>Index of /ADs/landing_school</title> 5: </head> 6: <body> 7: Index of /ADs/landing_school 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/landing_school/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/landing_school</title> 5: </head> 6: <body> 7: Index of /ADs/landing_school 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/len_bose/ 4: <title>Index of /ADs/len_bose</title> 5: </head> 6: <body> 7: Index of /ADs/len_bose 8: ... alt="[DIR]"> Parent Directory ...

Affected Nodes:	Additional Information:
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/lewmar/ 4: <title>Index of /ADs/lewmar</title> 5: </head> 6: <body> 7: Index of /ADs/lewmar 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/lewmar/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/lewmar</title> 5: </head> 6: <body> 7: Index of /ADs/lewmar 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/liveskipper/ 4: <title>Index of /ADs/liveskipper</title> 5: </head> 6: <body> 7: Index of /ADs/liveskipper 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/marten/ 4: <title>Index of /ADs/marten</title> 5: </head> 6: <body> 7: Index of /ADs/marten 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/Philsfoils/ 4: <title>Index of /ADs/Philsfoils</title> 5: </head> 6: <body> 7: Index of /ADs/Philsfoils 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/Philsfoils/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/Philsfoils</title> 5: </head> 6: <body> 7: Index of /ADs/Philsfoils 8: ... alt="[DIR]"> Parent Directory ...

Affected Nodes:	Additional Information:
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/S_40/ 4: <title>Index of /ADs/S_40</title> 5: </head> 6: <body> 7: Index of /ADs/S_40 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/S_40/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/S_40</title> 5: </head> 6: <body> 7: Index of /ADs/S_40 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/S_40/_notes/ 4: <title>Index of /ADs/S_40/_notes</title> 5: </head> 6: <body> 7: Index of /ADs/S_40/_notes 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/S_40/_notes/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/S_40/_notes</title> 5: </head> 6: <body> 7: Index of /ADs/S_40/_notes 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/UK/ 4: <title>Index of /ADs/UK</title> 5: </head> 6: <body> 7: Index of /ADs/UK 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/UK/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/UK</title> 5: </head> 6: <body> 7: Index of /ADs/UK

Affected Nodes:	Additional Information:
	8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/icons/ 4: <title>Index of /icons</title> 5: </head> 6: <body> 7: Index of /icons 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/java/ 4: <title>Index of /java</title> 5: </head> 6: <body> 7: Index of /java 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/Logs/ 4: <title>Index of /Logs</title> 5: </head> 6: <body> 7: Index of /Logs 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/temp/ 4: <title>Index of /temp</title> 5: </head> 6: <body> 7: Index of /temp 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/len_bose/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/len_bose</title> 5: </head> 6: <body> 7: Index of /ADs/len_bose 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/2006/ 4: <title>Index of /2006</title> 5: </head> 6: <body>

Affected Nodes:	Additional Information:
	7: Index of /2006 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/2006/podcasts/ 4: <title>Index of /2006/podcasts</title> 5: </head> 6: <body> 7: Index of /2006/podcasts 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/aeroyacht/ 4: <title>Index of /ADs/aeroyacht</title> 5: </head> 6: <body> 7: Index of /ADs/aeroyacht 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/aeroyacht/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/aeroyacht</title> 5: </head> 6: <body> 7: Index of /ADs/aeroyacht 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/akilaria/ 4: <title>Index of /ADs/akilaria</title> 5: </head> 6: <body> 7: Index of /ADs/akilaria 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/akilaria/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/akilaria</title> 5: </head> 6: <body> 7: Index of /ADs/akilaria 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/archambault/ 4: <title>Index of /ADs/archambault</title>

Affected Nodes:	Additional Information:
	5: </head> 6: <body> 7: Index of /ADs/archambault 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/archambault/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/archambault</title> 5: </head> 6: <body> 7: Index of /ADs/archambault 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/atlas/ 4: <title>Index of /ADs/atlas</title> 5: </head> 6: <body> 7: Index of /ADs/atlas 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/atlas/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/atlas</title> 5: </head> 6: <body> 7: Index of /ADs/atlas 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/bahia_corinthianyc/ 4: <title>Index of /ADs/bahia_corinthianyc</title> 5: </head> 6: <body> 7: Index of /ADs/bahia_corinthianyc 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/bahia_corinthianyc/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/bahia_corinthianyc</title> 5: </head> 6: <body> 7: Index of /ADs/bahia_corinthianyc 8: ... alt="[DIR]"> Parent Directory ...

Affected Nodes:	Additional Information:
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/barcelona_worlds/ 4: <title>Index of /ADs/barcelona_worlds</title> 5: </head> 6: <body> 7: Index of /ADs/barcelona_worlds 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/barcelona_worlds/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/barcelona_worlds</title> 5: </head> 6: <body> 7: Index of /ADs/barcelona_worlds 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/breton_yachts/ 4: <title>Index of /ADs/breton_yachts</title> 5: </head> 6: <body> 7: Index of /ADs/breton_yachts 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/breton_yachts/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/breton_yachts</title> 5: </head> 6: <body> 7: Index of /ADs/breton_yachts 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/camet/ 4: <title>Index of /ADs/camet</title> 5: </head> 6: <body> 7: Index of /ADs/camet 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/camet/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/camet</title> 5: </head> 6: <body> 7: Index of /ADs/camet 8: ... alt="[DIR]"> Parent Directory ...

Affected Nodes:	Additional Information:
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/catch_the_wind/ 4: <title>Index of /ADs/catch_the_wind</title> 5: </head> 6: <body> 7: Index of /ADs/catch_the_wind 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/catch_the_wind/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/catch_the_wind</title> 5: </head> 6: <body> 7: Index of /ADs/catch_the_wind 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/chandlery/ 4: <title>Index of /ADs/chandlery</title> 5: </head> 6: <body> 7: Index of /ADs/chandlery 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/chandlery/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/chandlery</title> 5: </head> 6: <body> 7: Index of /ADs/chandlery 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/csi/ 4: <title>Index of /ADs/csi</title> 5: </head> 6: <body> 7: Index of /ADs/csi 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/csi/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/csi</title> 5: </head> 6: <body>

Affected Nodes:	Additional Information:
	7: Index of /ADs/csi 8: ... alt="[DIR]"> Parent Directory ...
216.9.43.114:80 (www.sailinganarchy.com)	http://www.sailinganarchy.com/ADs/cst_composites/ 4: <title>Index of /ADs/cst_composites</title> 5: </head> 6: <body> 7: Index of /ADs/cst_composites 8: ... alt="[DIR]"> Parent Directory ...

References:

None

Vulnerability Solution:

•Apache

Disable web directory browsing for all directories and subdirectories

In your httpd.conf file, disable the "Indexes" option for the appropriate <Directory> tag by removing it from the Options line.

In addition, you should always make sure that proper permissions are set on all files and directories within the web root (including CGI scripts and backup files). Do not copy files in the web root unless you want these files to be available over the web. Periodically go through your web directories and clean out any unused, obsolete, or unknown files and directories.

•IIS, PWS, Microsoft-IIS, Internet Information Server, Internet Information Services, Microsoft-PWS

Disable web directory browsing for all directories and subdirectories

In the Internet Information Services control panel or MMC, choose the appropriate virtual directory entry and select Properties. Uncheck the 'Allow Directory Browsing' option.

In addition, you should always make sure that proper permissions are set on all files and directories within the web root (including CGI scripts and backup files). Do not copy files in the web root unless you want these files to be available over the web. Periodically go through your web directories and clean out any unused, obsolete, or unknown files and directories.

•Java System Web Server, iPlanet

Disable web directory indexing for all directories and subdirectories

The iPlanet web server indexes directories by searching the directory for an index file (by default index.html or home.html). If an index file is not found, the Document Preferences settings are checked to see what the Directory Indexing setting contains. This should be set to None to disable directory indexing.

For older versions of iPlanet that do not support the Directory Indexing setting, create a file called index.html or home.html in each directory. This page will then be served instead of a directory listing.

•Apache Tomcat, Tomcat, Tomcat Web Server, Apache Coyote, Apache-Coyote

Disable web directory browsing for all directories and subdirectories

Edit Tomcat's web.xml file. In the "default" servlet, change the "listings" parameter from "true" to "false". Restart the server.

In addition, you should always make sure that proper permissions are set on all files and directories within the web root (including CGI scripts and backup files). Do not copy files in the web root unless you want these files to be available over the web. Periodically go through your web directories and clean out any unused, obsolete, or unknown files and directories.

3.2.4. Apache mod_autoindex UTF-7 Cross-Site Scripting Vulnerability (http-apache-mod_autoindex-utf7-xss)

Description:

Some versions of Apache httpd ship a mod_autoindex module that does not define a charset in the Content-type header. This allows remote attackers to inject arbitrary web script or HTML, via the 'P' parameter using the UTF-7 charset, in flawed browsers that do not derive the response charset as required by RFC 2616. Such browsers include Microsoft Internet Explorer, which attempts to perform automatic charset detection.

Affected Nodes:

Affected Nodes:	Additional Information:
216.9.43.114:80 (www.sailinganarchy.com)	Running vulnerable HTTP service: Apache. http://www.sailinganarchy.com/ADs/aeroyacht/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/aeroyacht</title> 5: </head> 6: <body> 7: Index of /ADs/aeroyacht 8: ...f="?C=N;O=D;P=+ADw-script+AD4-alert(42)+ADw-/script+AD4-">Name ...
216.9.43.114:80 (www.sailinganarchy.com)	Running vulnerable HTTP service: Apache. http://www.sailinganarchy.com/ADs/akilaria/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/akilaria</title> 5: </head> 6: <body> 7: Index of /ADs/akilaria 8: ...f="?C=N;O=D;P=+ADw-script+AD4-alert(42)+ADw-/script+AD4-">Name ...
216.9.43.114:80 (www.sailinganarchy.com)	Running vulnerable HTTP service: Apache. http://www.sailinganarchy.com/ADs/archambault/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/archambault</title> 5: </head> 6: <body> 7: Index of /ADs/archambault 8: ...f="?C=N;O=D;P=+ADw-script+AD4-alert(42)+ADw-/script+AD4-">Name ...

Affected Nodes:	Additional Information:
216.9.43.114:80 (www.sailinganarchy.com)	Running vulnerable HTTP service: Apache. http://www.sailinganarchy.com/ADs/atlas/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/atlas</title> 5: </head> 6: <body> 7: Index of /ADs/atlas 8: ...f="?C=N;O=D;P=+ADw-script+AD4-alert(42)+ADw-/script+AD4-">Name ...
216.9.43.114:80 (www.sailinganarchy.com)	Running vulnerable HTTP service: Apache. http://www.sailinganarchy.com/ADs/bahia_corinthianyc/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/bahia_corinthianyc</title> 5: </head> 6: <body> 7: Index of /ADs/bahia_corinthianyc 8: ...f="?C=N;O=D;P=+ADw-script+AD4-alert(42)+ADw-/script+AD4-">Name ...
216.9.43.114:80 (www.sailinganarchy.com)	Running vulnerable HTTP service: Apache. http://www.sailinganarchy.com/ADs/barcelona_worlds/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/barcelona_worlds</title> 5: </head> 6: <body> 7: Index of /ADs/barcelona_worlds 8: ...f="?C=N;O=D;P=+ADw-script+AD4-alert(42)+ADw-/script+AD4-">Name ...
216.9.43.114:80 (www.sailinganarchy.com)	Running vulnerable HTTP service: Apache. http://www.sailinganarchy.com/ADs/breton_yachts/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/breton_yachts</title> 5: </head> 6: <body> 7: Index of /ADs/breton_yachts 8: ...f="?C=N;O=D;P=+ADw-script+AD4-alert(42)+ADw-/script+AD4-">Name ...
216.9.43.114:80 (www.sailinganarchy.com)	Running vulnerable HTTP service: Apache. http://www.sailinganarchy.com/ADs/camet/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/camet</title> 5: </head> 6: <body> 7: Index of /ADs/camet 8: ...f="?C=N;O=D;P=+ADw-script+AD4-alert(42)+ADw-/script+AD4-">Name ...

Affected Nodes:	Additional Information:
216.9.43.114:80 (www.sailinganarchy.com)	Running vulnerable HTTP service: Apache. http://www.sailinganarchy.com/ADs/catch_the_wind/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/catch_the_wind</title> 5: </head> 6: <body> 7: Index of /ADs/catch_the_wind 8: ...f="?C=N;O=D;P=+ADw-script+AD4-alert(42)+ADw-/script+AD4-">Name ...
216.9.43.114:80 (www.sailinganarchy.com)	Running vulnerable HTTP service: Apache. http://www.sailinganarchy.com/ADs/chandlery/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/chandlery</title> 5: </head> 6: <body> 7: Index of /ADs/chandlery 8: ...f="?C=N;O=D;P=+ADw-script+AD4-alert(42)+ADw-/script+AD4-">Name ...
216.9.43.114:80 (www.sailinganarchy.com)	Running vulnerable HTTP service: Apache. http://www.sailinganarchy.com/ADs/csi/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/csi</title> 5: </head> 6: <body> 7: Index of /ADs/csi 8: ...f="?C=N;O=D;P=+ADw-script+AD4-alert(42)+ADw-/script+AD4-">Name ...
216.9.43.114:80 (www.sailinganarchy.com)	Running vulnerable HTTP service: Apache. http://www.sailinganarchy.com/ADs/cst_composites/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/cst_composites</title> 5: </head> 6: <body> 7: Index of /ADs/cst_composites 8: ...f="?C=N;O=D;P=+ADw-script+AD4-alert(42)+ADw-/script+AD4-">Name ...
216.9.43.114:80 (www.sailinganarchy.com)	Running vulnerable HTTP service: Apache. http://www.sailinganarchy.com/ADs/devoti/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/devoti</title> 5: </head> 6: <body> 7: Index of /ADs/devoti 8: ...f="?C=N;O=D;P=+ADw-script+AD4-alert(42)+ADw-/script+AD4-">Name ...

Affected Nodes:	Additional Information:
216.9.43.114:80 (www.sailinganarchy.com)	Running vulnerable HTTP service: Apache. http://www.sailinganarchy.com/ADs/dimension/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/dimension</title> 5: </head> 6: <body> 7: Index of /ADs/dimension 8: ...f="?C=N;O=D;P=+ADw-script+AD4-alert(42)+ADw-/script+AD4-">Name ...
216.9.43.114:80 (www.sailinganarchy.com)	Running vulnerable HTTP service: Apache. http://www.sailinganarchy.com/ADs/dimension/_notes/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/dimension/_notes</title> 5: </head> 6: <body> 7: Index of /ADs/dimension/_notes 8: ...f="?C=N;O=D;P=+ADw-script+AD4-alert(42)+ADw-/script+AD4-">Name ...
216.9.43.114:80 (www.sailinganarchy.com)	Running vulnerable HTTP service: Apache. http://www.sailinganarchy.com/ADs/edson_marine/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/edson_marine</title> 5: </head> 6: <body> 7: Index of /ADs/edson_marine 8: ...f="?C=N;O=D;P=+ADw-script+AD4-alert(42)+ADw-/script+AD4-">Name ...
216.9.43.114:80 (www.sailinganarchy.com)	Running vulnerable HTTP service: Apache. http://www.sailinganarchy.com/ADs/euro_marine/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/euro_marine</title> 5: </head> 6: <body> 7: Index of /ADs/euro_marine 8: ...f="?C=N;O=D;P=+ADw-script+AD4-alert(42)+ADw-/script+AD4-">Name ...
216.9.43.114:80 (www.sailinganarchy.com)	Running vulnerable HTTP service: Apache. http://www.sailinganarchy.com/ADs/farr/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/farr</title> 5: </head> 6: <body> 7: Index of /ADs/farr

Affected Nodes:	Additional Information:
	8: ...f="?C=N;O=D;P=+ADw-script+AD4-alert(42)+ADw-/script+AD4-">Name ...
216.9.43.114:80 (www.sailinganarchy.com)	Running vulnerable HTTP service: Apache. http://www.sailinganarchy.com/ADs/farr/_notes/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/farr/_notes</title> 5: </head> 6: <body> 7: Index of /ADs/farr/_notes 8: ...f="?C=N;O=D;P=+ADw-script+AD4-alert(42)+ADw-/script+AD4-">Name ...
216.9.43.114:80 (www.sailinganarchy.com)	Running vulnerable HTTP service: Apache. http://www.sailinganarchy.com/ADs/farrier/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/farrier</title> 5: </head> 6: <body> 7: Index of /ADs/farrier 8: ...f="?C=N;O=D;P=+ADw-script+AD4-alert(42)+ADw-/script+AD4-">Name ...
216.9.43.114:80 (www.sailinganarchy.com)	Running vulnerable HTTP service: Apache. http://www.sailinganarchy.com/ADs/finn/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/finn</title> 5: </head> 6: <body> 7: Index of /ADs/finn 8: ...f="?C=N;O=D;P=+ADw-script+AD4-alert(42)+ADw-/script+AD4-">Name ...
216.9.43.114:80 (www.sailinganarchy.com)	Running vulnerable HTTP service: Apache. http://www.sailinganarchy.com/ADs/flexfold/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/flexfold</title> 5: </head> 6: <body> 7: Index of /ADs/flexfold 8: ...f="?C=N;O=D;P=+ADw-script+AD4-alert(42)+ADw-/script+AD4-">Name ...
216.9.43.114:80 (www.sailinganarchy.com)	Running vulnerable HTTP service: Apache. http://www.sailinganarchy.com/ADs/flyingtiger/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/flyingtiger</title> 5: </head> 6: <body> 7: Index of /ADs/flyingtiger

Affected Nodes:	Additional Information:
	8: ...f="?C=N;O=D;P=+ADw-script+AD4-alert(42)+ADw-/script+AD4-">Name ...
216.9.43.114:80 (www.sailinganarchy.com)	Running vulnerable HTTP service: Apache. http://www.sailinganarchy.com/ADs/flyingtiger/_notes/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/flyingtiger/_notes</title> 5: </head> 6: <body> 7: Index of /ADs/flyingtiger/_notes 8: ...f="?C=N;O=D;P=+ADw-script+AD4-alert(42)+ADw-/script+AD4-">Name ...
216.9.43.114:80 (www.sailinganarchy.com)	Running vulnerable HTTP service: Apache. http://www.sailinganarchy.com/ADs/gunboat/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/gunboat</title> 5: </head> 6: <body> 7: Index of /ADs/gunboat 8: ...f="?C=N;O=D;P=+ADw-script+AD4-alert(42)+ADw-/script+AD4-">Name ...
216.9.43.114:80 (www.sailinganarchy.com)	Running vulnerable HTTP service: Apache. http://www.sailinganarchy.com/ADs/halifax_saint_pierre/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/halifax_saint_pierre</title> 5: </head> 6: <body> 7: Index of /ADs/halifax_saint_pierre 8: ...f="?C=N;O=D;P=+ADw-script+AD4-alert(42)+ADw-/script+AD4-">Name ...
216.9.43.114:80 (www.sailinganarchy.com)	Running vulnerable HTTP service: Apache. http://www.sailinganarchy.com/ADs/isailfast/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/isailfast</title> 5: </head> 6: <body> 7: Index of /ADs/isailfast 8: ...f="?C=N;O=D;P=+ADw-script+AD4-alert(42)+ADw-/script+AD4-">Name ...
216.9.43.114:80 (www.sailinganarchy.com)	Running vulnerable HTTP service: Apache. http://www.sailinganarchy.com/ADs/isailfast/_notes/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/isailfast/_notes</title> 5: </head>

Affected Nodes:	Additional Information:
	6: <body> 7: Index of /ADs/isailfast/_notes 8: ...f="?C=N;O=D;P=+ADw-script+AD4-alert(42)+ADw-/script+AD4-">Name ...
216.9.43.114:80 (www.sailinganarchy.com)	Running vulnerable HTTP service: Apache. http://www.sailinganarchy.com/ADs/jk3yachtsales/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/jk3yachtsales</title> 5: </head> 6: <body> 7: Index of /ADs/jk3yachtsales 8: ...f="?C=N;O=D;P=+ADw-script+AD4-alert(42)+ADw-/script+AD4-">Name ...
216.9.43.114:80 (www.sailinganarchy.com)	Running vulnerable HTTP service: Apache. http://www.sailinganarchy.com/ADs/landing_school/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/landing_school</title> 5: </head> 6: <body> 7: Index of /ADs/landing_school 8: ...f="?C=N;O=D;P=+ADw-script+AD4-alert(42)+ADw-/script+AD4-">Name ...
216.9.43.114:80 (www.sailinganarchy.com)	Running vulnerable HTTP service: Apache. http://www.sailinganarchy.com/ADs/len_bose/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/len_bose</title> 5: </head> 6: <body> 7: Index of /ADs/len_bose 8: ...f="?C=N;O=D;P=+ADw-script+AD4-alert(42)+ADw-/script+AD4-">Name ...
216.9.43.114:80 (www.sailinganarchy.com)	Running vulnerable HTTP service: Apache. http://www.sailinganarchy.com/ADs/lewmar/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/lewmar</title> 5: </head> 6: <body> 7: Index of /ADs/lewmar 8: ...f="?C=N;O=D;P=+ADw-script+AD4-alert(42)+ADw-/script+AD4-">Name ...
216.9.43.114:80 (www.sailinganarchy.com)	Running vulnerable HTTP service: Apache. http://www.sailinganarchy.com/ADs/Philsfoils/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4-

Affected Nodes:	Additional Information:
	4: <title>Index of /ADs/Philsfoils</title> 5: </head> 6: <body> 7: Index of /ADs/Philsfoils 8: ...f="?C=N;O=D;P=+ADw-script+AD4-alert(42)+ADw-/script+AD4-">Name ...
216.9.43.114:80 (www.sailinganarchy.com)	Running vulnerable HTTP service: Apache. http://www.sailinganarchy.com/ADs/S_40/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/S_40</title> 5: </head> 6: <body> 7: Index of /ADs/S_40 8: ...f="?C=N;O=D;P=+ADw-script+AD4-alert(42)+ADw-/script+AD4-">Name ...
216.9.43.114:80 (www.sailinganarchy.com)	Running vulnerable HTTP service: Apache. http://www.sailinganarchy.com/ADs/S_40/_notes/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/S_40/_notes</title> 5: </head> 6: <body> 7: Index of /ADs/S_40/_notes 8: ...f="?C=N;O=D;P=+ADw-script+AD4-alert(42)+ADw-/script+AD4-">Name ...
216.9.43.114:80 (www.sailinganarchy.com)	Running vulnerable HTTP service: Apache. http://www.sailinganarchy.com/ADs/UK/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 4: <title>Index of /ADs/UK</title> 5: </head> 6: <body> 7: Index of /ADs/UK 8: ...f="?C=N;O=D;P=+ADw-script+AD4-alert(42)+ADw-/script+AD4-">Name ...

References:

Source	Reference
BID	25653
CVE	CVE-2007-4465
URL	http://securityreason.com/achievement_securityalert/46
URL	http://svn.apache.org/viewvc?view=rev&revision=570532
URL	http://svn.apache.org/viewvc?view=rev&revision=570962
URL	http://svn.apache.org/viewvc?view=rev&revision=570961

Source	Reference
URL	http://archive.apache.org/dist/httpd/CHANGES_2.2.6
URL	http://archive.apache.org/dist/httpd/CHANGES_2.0.61

Vulnerability Solution:

•Apache >= 2.0 and < 2.1

Upgrade to Apache version 2.0.61

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.0.61.tar.gz

Many platforms and distributions provide pre-built binary packages for Apache. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

•Apache >= 2.1 and < 2.3

Upgrade to Apache version 2.2.6

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.6.tar.gz

Many platforms and distributions provide pre-built binary packages for Apache. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.3. Moderate Vulnerabilities

3.3.1. Apache ETag Inode Information Leakage (http-apache-etag-inode-leak)

Description:

Certain versions of Apache use the requested file's inode number to construct the 'ETag' response header. While not a vulnerability in and of itself, this information makes certain NFS attacks much simpler to execute.

Affected Nodes:

Affected Nodes:	Additional Information:
216.9.43.114:80 (www.sailinganarchy.com)	Running vulnerable HTTP service: Apache. http://www.sailinganarchy.com/ `1: "21dc9f-324-3c33d000"`

References:

Source	Reference
BID	6939

Source	Reference
XF	apache-mime-information-disclosure(11438)

Vulnerability Solution:

•Disable inode-based ETag generation in the Apache config

You can remove inode information from the ETag header by adding the following directive to your Apache config:

```
FileETag MTime Size
```

•OpenBSD

Apply OpenBSD 3.2 errata #8 for Apache inode and pid leak

Download and apply the patch from: http://www.openbsd.org/errata32.html#httpd

The OpenBSD team has released a patch for the Apache inode and pid leak problem. This patch can be applied cleanly to 3.2 stable and rebuilt. Restart httpd for the changes to take effect. OpenBSD 3.3 will ship with the patched httpd by default. The patch can be applied to earlier 3.x versions of OpenBSD, but it may require editing of the source code.

3.3.2. ICMP timestamp response (generic-icmp-timestamp)

Description:

The remote host responded to an ICMP timestamp request. The ICMP timestamp response contains the remote host's date and time. This information could theoretically be used against some systems to exploit weak time-based random number generators in other services.

In addition, the versions of some operating systems can be accurately fingerprinted by analyzing their responses to invalid ICMP timestamp requests.

Affected Nodes:

Affected Nodes:	Additional Information:
216.9.43.114 (www.sailinganarchy.com)	Remote system time: 14:33:55.429 EDT

References:

Source	Reference
XF	icmp-timestamp(322)
CVE	CVE-1999-0524

Vulnerability Solution:

•HP-UX

Disable ICMP timestamp responses on HP/UX

Execute the following command:

ndd -set /dev/ip ip_respond_to_timestamp_broadcast 0

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•Cisco IOS

Disable ICMP timestamp responses on Cisco IOS

Use ACLs to block ICMP types 13 and 14. For example:

```
deny icmp any any 13
deny icmp any any 14
```

Note that it is generally preferable to use ACLs that block everything by default and then selectively allow certain types of traffic in. For example, block everything and then only allow ICMP unreachable, ICMP echo reply, ICMP time exceeded, and ICMP source quench:

```
permit icmp any any unreachable
permit icmp any any echo-reply
permit icmp any any time-exceeded
permit icmp any any source-quench
```

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•SGI Irix

Disable ICMP timestamp responses on SGI Irix

IRIX does not offer a way to disable ICMP timestamp responses. Therefore, you should block ICMP on the affected host using ipfilterd, and/or block it at any external firewalls.

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•Linux

Disable ICMP timestamp responses on Linux

Linux offers neither a sysctl nor a /proc/sys/net/ipv4 interface to disable ICMP timestamp responses. Therefore, you should block ICMP on the affected host using iptables, and/or block it at the firewall. For example:

```
ipchains -A input -p icmp --icmp-type timestamp-request -j DROP
ipchains -A output -p icmp --icmp-type timestamp-reply -j DROP
```

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•Microsoft Windows NT, Microsoft Windows NT Workstation, Microsoft Windows NT Server, Microsoft Windows NT Advanced Server, Microsoft Windows NT Server, Enterprise Edition, Microsoft Windows NT Server, Terminal Server Edition

Disable ICMP timestamp responses on Windows NT 4

Windows NT 4 does not provide a way to block ICMP packets. Therefore, you should block them at the firewall.

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•OpenBSD

Disable ICMP timestamp responses on OpenBSD

Set the "net.inet.icmp.tstamprepl" sysctl variable to 0.

```
sysctl -w net.inet.icmp.tstamprepl=0
```

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•Cisco PIX

Disable ICMP timestamp responses on Cisco PIX

A properly configured PIX firewall should never respond to ICMP packets on its external interface. In PIX Software versions 4.1(6) until 5.2.1, ICMP traffic to the PIX's internal interface is permitted; the PIX cannot be configured to NOT respond. Beginning in PIX Software version 5.2.1, ICMP is still permitted on the internal interface by default, but ICMP responses from its internal interfaces can be disabled with the icmp command, as follows, where <inside> is the name of the internal interface:

```
icmp deny any 13 <inside>
icmp deny any 14 <inside>
```

Don't forget to save the configuration when you are finished.

See Cisco's support document Handling ICMP Pings with the PIX Firewall for more information.

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•Sun Solaris

Disable ICMP timestamp responses on Solaris

Execute the following commands:

```
/usr/sbin/ndd -set /dev/ip ip_respond_to_timestamp 0
/usr/sbin/ndd -set /dev/ip ip_respond_to_timestamp_broadcast 0
```

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•Microsoft Windows 2000, Microsoft Windows 2000 Professional, Microsoft Windows 2000 Server, Microsoft Windows 2000 Advanced Server, Microsoft Windows 2000 Datacenter Server

Disable ICMP timestamp responses on Windows 2000

Use the IPSec filter feature to define an apply an IP filter list that blocks ICMP types 13 and 14. Note that the standard TCP/IP blocking capability under the "Networking and Dialup Connections" control panel is NOT capable of blocking ICMP (only TCP and UDP). The IPSec filter features, while they may seem strictly related to the IPSec standards, will allow you to selectively block these ICMP packets. See http://support.microsoft.com/kb/313190 for more information.

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•Microsoft Windows XP, Microsoft Windows XP Home, Microsoft Windows XP Professional, Microsoft Windows Server 2003, Microsoft Windows Server 2003, Standard Edition, Microsoft Windows Server 2003, Enterprise Edition, Microsoft Windows Server 2003,

Datacenter Edition, Microsoft Windows Server 2003, Web Edition, Microsoft Windows Small Business Server 2003

Disable ICMP timestamp responses on Windows XP/2K3

ICMP timestamp responses can be disabled by deselecting the "allow incoming timestamp request" option in the ICMP configuration panel of Windows Firewall.

1. Go to the Network Connections control panel.
2. Right click on the network adapter and select "properties", or select the internet adapter and select File->Properties.
3. Select the "Advanced" tab.
4. In the Windows Firewall box, select "Settings".
5. Select the "General" tab.
6. Enable the firewall by selecting the "on (recommended)" option.
7. Select the "Advanced" tab.
8. In the ICMP box, select "Settings".
9. Deselect (uncheck) the "Allow incoming timestamp request" option.
10. Select "OK" to exit the ICMP Settings dialog and save the settings.
11. Select "OK" to exit the Windows Firewall dialog and save the settings.
12. Select "OK" to exit the internet adapter dialog.

For more information, see: http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/hnw_understanding_firewall.mspx?mfr=true

•Microsoft Windows Vista, Microsoft Windows Vista Home, Basic Edition, Microsoft Windows Vista Home, Basic N Edition, Microsoft Windows Vista Home, Premium Edition, Microsoft Windows Vista Ultimate Edition, Microsoft Windows Vista Enterprise Edition, Microsoft Windows Vista Business Edition, Microsoft Windows Vista Business N Edition, Microsoft Windows Vista Starter Edition, Microsoft Windows Server 2008, Microsoft Windows Server 2008 Standard Edition, Microsoft Windows Server 2008 Enterprise Edition, Microsoft Windows Server 2008 Datacenter Edition, Microsoft Windows Server 2008 HPC Edition, Microsoft Windows Server 2008 Web Edition, Microsoft Windows Server 2008 Storage Edition, Microsoft Windows Small Business Server 2008, Microsoft Windows Essential Business Server 2008

Disable ICMP timestamp responses on Windows Vista/2008

ICMP timestamp responses can be disabled via the netsh command line utility.

1. Go to the Windows Control Panel.
2. Select "Windows Firewall".
3. In the Windows Firewall box, select "Change Settings".
4. Enable the firewall by selecting the "on (recommended)" option.
5. Open a Command Prompt.
6. Enter "netsh firewall set icmpsetting 13 disable"

For more information, see: http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/hnw_understanding_firewall.mspx?mfr=true

•Disable ICMP timestamp responses

Disable ICMP timestamp replies for the device. If the device does not support this level of configuration, the easiest and most effective

solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

3.3.3. HTTP TRACE Method Enabled (http-trace-method-enabled)

Description:

The HTTP TRACE method is normally used to return the full HTTP request back to the requesting client for proxy-debugging purposes. An attacker can create a webpage using XMLHTTP, ActiveX, or XMLDOM to cause a client to issue a TRACE request and capture the client's cookies. This effectively results in a Cross-Site Scripting attack.

Affected Nodes:

Affected Nodes:	Additional Information:

216.9.43.114:80 (www.sailinganarchy.com)	Running vulnerable HTTP service.
	http://www.sailinganarchy.com/
	`1: TRACE / HTTP/1.1`
	`2: Host: www.sailinganarchy.com`
	`3: Cookie:` vulnerable=yes

References:

Source	Reference
OSVDB	877
SUN	50603
URL	http://www.kb.cert.org/vuls/id/867593
BID	9561
URL	http://www.apacheweek.com/issues/03-01-24#news

Vulnerability Solution:

•Apache

Disable HTTP TRACE Method for Apache

Newer versions of Apache (1.3.34 and 2.0.55 and later) provide a configuration directive called TraceEnable. To deny TRACE requests, add the following line to the server configuration:

```
TraceEnable off
```

For older versions of the Apache webserver, use the mod_rewrite module to deny the TRACE requests:

```
RewriteEngine On
RewriteCond %{REQUEST_METHOD} ^TRACE
```

```
RewriteRule .* - [F]
```

•IIS, PWS, Microsoft-IIS, Internet Information Server, Internet Information Services, Microsoft-PWS

Disable HTTP TRACE Method for Microsoft IIS

For Microsoft Internet Information Services (IIS), you may use the URLScan tool, freely available at http://www.microsoft.com/technet/security/tools/urlscan.mspx

•Java System Web Server, SunONE WebServer, Sun-ONE-Web-Server, iPlanet

Disable HTTP TRACE Method for SunONE/iPlanet

•For Sun ONE/iPlanet Web Server v6.0 SP2 and later, add the following configuration to the top of the default object in the 'obj.conf' file:

```
<Client method="TRACE">
  AuthTrans fn="set-variable"
     remove-headers="transfer-encoding"
     set-headers="content-length: -1"
     error="501"
</Client>
```

You must then restart the server for the changes to take effect.

•For Sun ONE/iPlanet Web Server prior to v6.0 SP2, follow the instructions provided the 'Relief/Workaround' section of Sun's official advisory: http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F50603

•Lotus Domino

Disable HTTP TRACE Method for Domino

Follow IBM's instructions for disabling HTTP methods on the Domino server by adding the following line to the server's NOTES.INI file:

```
HTTPDisableMethods=TRACE
```

After saving NOTES.INI, restart the Notes web server by issuing the console command "tell http restart".

4. Discovered Services

4.1. FTP

FTP, the File Transfer Protocol, is used to transfer files between systems. On the Internet, it is often used on web pages to download files from a web site using a browser. FTP uses two connections, one for control connections used to authenticate, navigate the FTP server and initiate file transfers. The other connection is used to transfer data, such as files or directory listings.

4.1.1. General Security Issues

Cleartext authentication

The original FTP specification only provided means for authentication with cleartext user ids and passwords. Though FTP has added support for more secure mechanisms such as Kerberos, cleartext authentication is still the primary mechanism. If a malicious user is in a position to monitor FTP traffic, user ids and passwords can be stolen.

4.1.2. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
216.9.43.114 (www.sailinganarchy.com)	tcp	21	1	•ftp.banner: 220 ftp.sailinganarchy.com FTP server ready.

4.2. HTTP

HTTP, the HyperText Transfer Protocol, is used to exchange multimedia content on the World Wide Web. The multimedia files commonly used with HTTP include text, sound, images and video.

4.2.1. General Security Issues

Simple authentication scheme

Many HTTP servers use BASIC as their primary mechanism for user authentication. This is a very simple scheme that uses base 64 to encode the cleartext user id and password. If a malicious user is in a position to monitor HTTP traffic, user ids and passwords can be stolen by decoding the base 64 authentication data. To secure the authentication process, use HTTPS (HTTP over TLS/SSL) connections to transmit the authentication data.

4.2.2. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
216.9.43.114 (www.sailinganarchy.com)	tcp	80	5	•Apache •http.banner: Apache •http.banner.server: Apache •verbs-1: GET •verbs-2: HEAD

Device	Protocol	Port	Vulnerabilities	Additional Information
				•verbs-3: OPTIONS •verbs-4: POST •verbs-5: TRACE •verbs-count: 5

5. Discovered Users and Groups

No user or group information was discovered during the scan.

6. Discovered Databases

No database information was discovered during the scan.

7. Discovered Files and Directories

No file or directory information was discovered during the scan.

8. Policy Evaluations

No policy evaluations were performed.

9. Spidered Web Sites

9.1. http://216.9.43.114:80

9.1.1. Common Default URLs

The following URLs were guessed. They are often included with default web server or web server add-on installations.

Access Error (403)

- cgi-bin
- error

Requires Authentication (401)

- stats

Successful (200)

- Logs
- archives
- css
- icons
- images
- includes
- java
- php
- temp

9.1.2. Guessed URLs

The following URLs were guessed using various tricks based on the discovered web site content.

Access Error (403)

- cgi-bin
  - sachat

Redirect (301)

- ADs
  - Philsfoils
  - S_40
  - S_40
    - _notes
  - UK

- aeroyacht
- akilaria
- archambault
- atlas
- bahia_corinthianyc
- barcelona_worlds
- breton_yachts
- camet
- catch_the_wind
- chandlery
- csi
- cst_composites
- devoti
- dimension
- dimension
  - _notes
- edson_marine
- euro_marine
- farr
- farr
  - _notes
- farrier
- finn
- flexfold
- flyingtiger
- flyingtiger
  - _notes
- gunboat
- halifax_saint_pierre
- isailfast
- isailfast
  - _notes
- jk3yachtsales
- landing_school
- len_bose
- lewmar
- liveskipper

Redirect (302)

- forums
  - %23index.php%23
  - index.CGI
  - index.FCGI
  - index.PHP
  - index.PHP3
  - index.PHP4
  - index.PHP5
  - index.PHTML
  - index.PL
  - index.PY
  - index.RB
  - index.SH
  - index.SHTML
  - index.php.
  - index.php.bak
  - index.php.old
  - index.php.tmp
  - index.php
    - <script>xss<
      - script>
  - index.php~

Successful (200)

- 2006
  - podcasts
- ?P=+ADw-script+AD4-alert(42)+ADw-
  - script+AD4-
  - script+AD4-
  - script+AD4-
  - script+AD4-
  - script+AD4-
  - script+AD4-
  - script+AD4-
  - script+AD4-
  - script+AD4-
  - script+AD4-
  - script+AD4-
  - script+AD4-

- script+AD4-
- script+AD4-
- script+AD4-
- script+AD4-
- script+AD4-
- script+AD4-
- script+AD4-
- script+AD4-
- script+AD4-
- script+AD4-
- script+AD4-
- script+AD4-
- script+AD4-
- script+AD4-
- script+AD4-
- script+AD4-
- script+AD4-
- script+AD4-
- script+AD4-
- script+AD4-
- script+AD4-
- script+AD4-
- script+AD4-
- script+AD4-
- script+AD4-
- ADs
- Philsfoils
- S_40
  - _notes
- UK
- aeroyacht
- akilaria
- archambault
- atlas
- bahia_corinthianyc
- barcelona_worlds
- breton_yachts
- camet

- catch_the_wind
- chandlery
- csi
- cst_composites
- devoti
- dimension
- dirtydog
- edson_marine
- euro_marine
- evolution_sails
- farr
- farrier
- finn
- flexfold
- flyingtiger
- goetz
- gunboat
- halifax_saint_pierre
- heineken
- index.htm
- isailfast
- jk3yachtsales
- kinsale
- landing_school
- len_bose
- lewmar
- liveskipper
- marten

- a_link.php
  - <script>xss<
    - script>
    - script>
    - script>
    - script>
    - script>
    - script>
    - script>
    - script>
    - script>

- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- about.htm
- advertise.htm
- archives.htm
- article.php
- article_submission.php
- article_submission.php
- ask
  - 2005_ask.php
  - 2006_ask.php
  - ask.php
  - ask.php
- calendar
  - index.php
  - index.php
  - race_calendar.php
- cgi-bin
  - sachat
    - bluechat.cgi
- cil
  - ac_live.php
- classified.htm
- contact_admin.php
- contact_admin.php
- contact_editor.php
- contact_editor.php
- eanarchy
  - eanarchy_subscribe.htm
- editor
  - audio_video.php
  - audio_video.php

- pimpin.php
- index.htm
- index.html
- index_page1.php
- index_page2.php
- index_page2.php
- jcal
  - calendar.html?id=
- otwa
  - 33rd_ac_raceday.php
- php
- purchase
  - buy.htm
- search.php
- search.php
- terms.htm
- z_search.php

9.1.3. Linked URLs

The following URLs were found as links in the content of other web pages.

Redirect (301)

- news
- otwa
- sayc

Redirect (302)

- forums
- forums
  - index.php?showtopic=44697

Successful (200)

- ADs
  - S_40
    - _notes
      - s40_1.jpg.mno
  - dimension
    - _notes
      - dimension_index.gif.mno
  - dirtydog
    - _notes

- dd_125x1501.swf
- glasses
- farr
- _notes
- index_far30worlds.jpg.mno
- farr_ad.swf
- flyingtiger
- _notes
- ft_logo_125.gif.mno
- otw_2009kwrw_ft.gif.mno
- hullreservationagreementmay17.pdf
- gunboat
- gunboat_forum.swf
- isailfast
- _notes
- index_isailfast.gif.mno
- nauticexpo
- nauticexpo.htm
- a_link.php?a=http:
- www.sailinganarchy.com
- article.php?get=5908
- article.php?get=5908
- ask
- 2005_ask.php
- 2006_ask.php
- ask.htm
- calendar
- race_calendar.php
- cil
- ac_live.php
- css
- SA_CSS.css
- page_layout.css
- z_page_layout.css
- editor
- 2005
- pimpin_2005.htm
- csys_2005_aerostructures.pdf
- 2006
- pimpin_2006.htm

- antrim%2040.htm
- back%20the%20shield.htm
- mk2hfplan.pdf
- pimpin.php
- fringe
  - 2007
    - 2007_D-P_NewsFinal.pdf
    - BrigBrochWebFull-1.pdf
    - Chieftain%20FYS%20Listing.pdf
    - rocket%20refuel.htm
  - 2010
    - 2010%20SA%20sportboat%20regatta.htm
- index_page1.php
- java
  - ad_rotation.js
  - new_window.js
- jcal
  - calendar3.js
- php
  - ask.php
  - functions_js.js
- sa_menu.js
- sayc
- search_tips.htm
- z_search.php