
HOYT LLC
http://hoytllc.com
Strategic Consulting

Hoyt LLC Audit Report

Device report for 208.64.163.11

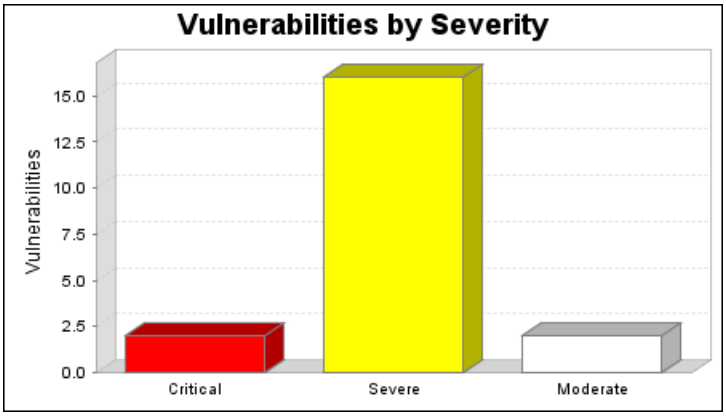
Audited on July 22 2010

1. Executive Summary

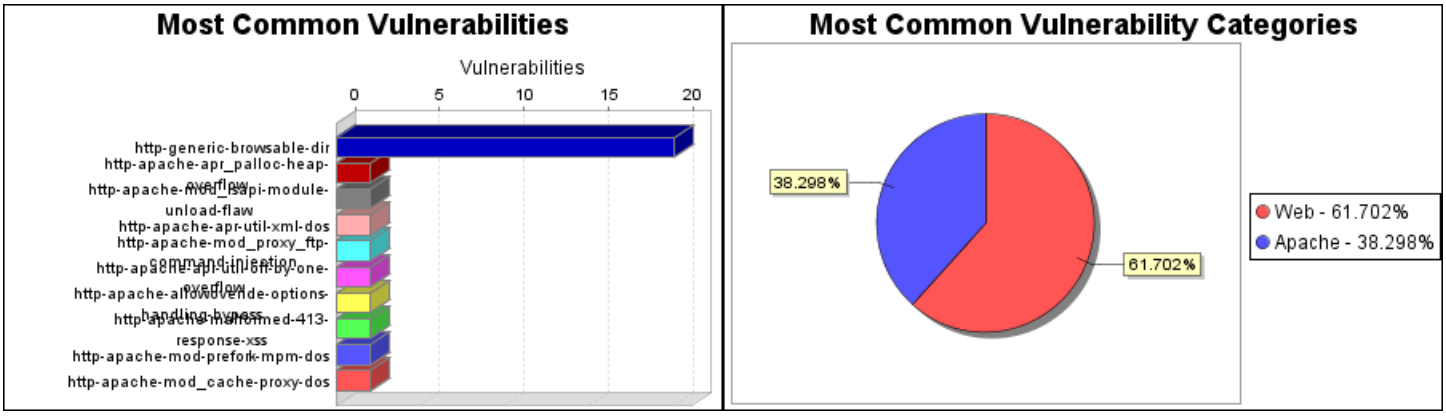
This report represents a security audit performed by Hoyt LLC. It contains confidential information about the state of your network. Access to this information by unauthorized personnel may allow them to compromise your network.

Site Name	Start Time	End Time	Total Time	Status
www.harborexpress.com	July 22, 2010 08:52, EDT	July 22, 2010 09:15, EDT	23 minutes	Success

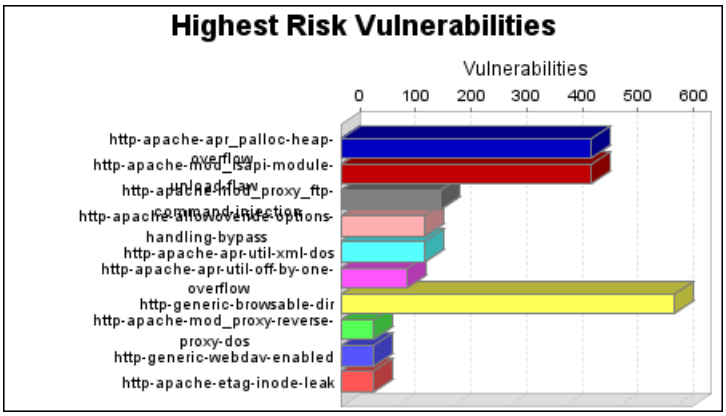
The audit was performed on one system which was found to be active and was scanned.



There were 20 vulnerabilities found during this scan. Of these, 2 were critical vulnerabilities. Critical vulnerabilities require immediate attention. They are relatively easy for attackers to exploit and may provide them with full control of the affected systems. 16 vulnerabilities were severe. Severe vulnerabilities are often harder to exploit and may not provide the same access to affected systems. There were 2 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.



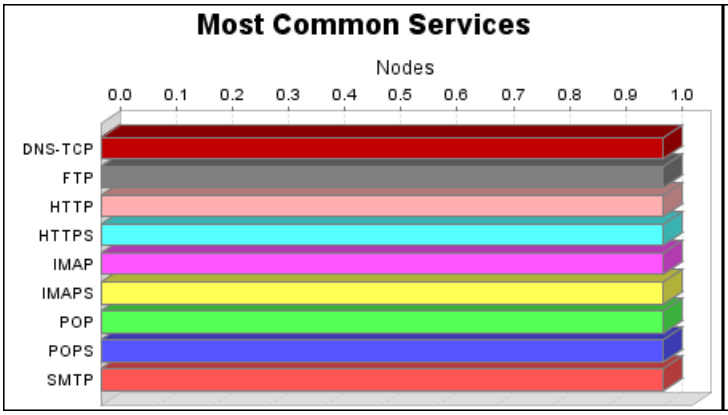
There were 20 occurrences of the http-generic-browsable-dir vulnerability, making it the most common vulnerability. There were 58 vulnerabilities in the Web category, making it the most common vulnerability category.



The http-apache-apr_palloc-heap-overflow and http-apache-mod_isapi-module-unload-flaw vulnerabilities pose the highest risk to the organization with a risk score of 450. 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 9 services found to be running during this scan.



The DNS-TCP, FTP, HTTP, HTTPS, IMAP, IMAPS, POP, POPS and SMTP services were found on 1 systems, making them the most common services. The HTTPS service was found to have the most vulnerabilities during this scan with 32 vulnerabilities.

2. Discovered Systems

Node	Operating System	Risk	Aliases
208.64.163.11	CentOS Linux	3.63	•ftp.digitalimaginginc.com •www.harborexpress.com

3. Discovered and Potential Vulnerabilities

3.1. Critical Vulnerabilities

3.1.1. Apache APR apr_palloc Heap Overflow (http-apache-apr_palloc-heap-overflow)

Description:

A flaw in apr_palloc() in the bundled copy of APR could cause heap overflows in programs that try to apr_palloc() a user controlled size. The Apache HTTP Server itself does not pass unsanitized user-provided sizes to this function, so it could only be triggered through some other application which uses apr_palloc() in a vulnerable way.

Affected Nodes:

Affected Nodes:	Additional Information:
208.64.163.11:80 (ftp.digitalimaginginc.com)	Running vulnerable HTTP service: Apache 2.2.3.
208.64.163.11:443 (ftp.digitalimaginginc.com)	Running vulnerable HTTPS service: Apache 2.2.3.

References:

Source	Reference
BID	35949
CVE	CVE-2009-2412
SECUNIA	36138
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

Apache >= 2.1 and < 2.3

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.13.tar.bz2

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.

3.1.2. Apache mod_isapi Module Unload Flaw (http-apache-mod_isapi-module-unload-flaw)

Description:

A flaw was found with within mod_isapi which would attempt to unload the ISAPI dll when it encountered various error states. This could leave the callbacks in an undefined state and result in a segfault. On Windows platforms using mod_isapi, a remote attacker could send a malicious request to trigger this issue, and as win32 MPM runs only one process, this would result in a denial of service, and potentially allow arbitrary code execution.

Affected Nodes:

Affected Nodes:	Additional Information:
208.64.163.11:80 (ftp.digitalimaginginc.com)	Running vulnerable HTTP service: Apache 2.2.3.
208.64.163.11:443 (ftp.digitalimaginginc.com)	Running vulnerable HTTPS service: Apache 2.2.3.

References:

Source	Reference
BID	38494
CVE	CVE-2010-0425
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

Apache >= 2.1 and < 2.3

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.15.tar.bz2

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.

3.2. Severe Vulnerabilities

3.2.1. Apache APR-util XML Denial of Service (http-apache-apr-util-xml-dos)

Description:

A denial of service flaw was found in the bundled copy of the APR-util library Extensible Markup Language (XML) parser. A remote attacker could create a specially-crafted XML document that would cause excessive memory consumption when processed by the XML decoding engine.

Affected Nodes:

Affected Nodes:	Additional Information:
208.64.163.11:80 (ftp.digitalimaginginc.com)	Running vulnerable HTTP service: Apache 2.2.3.
208.64.163.11:443 (ftp.digitalimaginginc.com)	Running vulnerable HTTPS service: Apache 2.2.3.

References:

Source	Reference
BID	35253
CVE	CVE-2009-1955
SECUNIA	35284
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

Apache >= 2.1 and < 2.3

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.bz2

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.

3.2.2. Apache mod_prixy_ftp FTP Command Injection (http-apache-mod_proxy_ftp-command-injection)

Description:

A flaw was found in the mod_proxy_ftp module. In a reverse proxy configuration, a remote attacker could use this flaw to bypass intended access restrictions by creating a carefully-crafted HTTP Authorization header, allowing the attacker to send arbitrary commands to the FTP server.

Affected Nodes:

Affected Nodes:	Additional Information:
208.64.163.11:80 (ftp.digitalimaginginc.com)	Running vulnerable HTTP service: Apache 2.2.3.
208.64.163.11:443 (ftp.digitalimaginginc.com)	Running vulnerable HTTPS service: Apache 2.2.3.

References:

Source	Reference
BID	36254
CVE	CVE-2007-6422
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

Apache >= 2.1 and < 2.3

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.14.tar.bz2

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.

3.2.3. Apache APR-util Off-by-one Overflow (http-apache-apr-util-off-by-one-overflow)

Description:

An off-by-one overflow flaw was found in the way the bundled copy of the APR-util library processed a variable list of arguments. An attacker could provide a specially-crafted string as input for the formatted output conversion routine, which could, on big-endian platforms, potentially lead to the disclosure of sensitive information or a denial of service.

Affected Nodes:

Affected Nodes:	Additional Information:
208.64.163.11:80 (ftp.digitalimaginginc.com)	Running vulnerable HTTP service: Apache 2.2.3.
208.64.163.11:443 (ftp.digitalimaginginc.com)	Running vulnerable HTTPS service: Apache 2.2.3.

References:

Source	Reference
BID	35251
CVE	CVE-2009-1956
SECUNIA	35284
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

Apache >= 2.1 and < 2.3

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.bz2

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.

3.2.4. Apache AllowOverride Options handling bypass (http-apache-allowoveride-options-handling-bypass)

Description:

A flaw was found in the handling of the "Options" and "AllowOverride" directives. In configurations using the "AllowOverride" directive with certain "Options=" arguments, local users were not restricted from executing commands from a Server-Side-Include script as intended.

Affected Nodes:

Affected Nodes:	Additional Information:
208.64.163.11:80 (ftp.digitalimaginginc.com)	Running vulnerable HTTP service: Apache 2.2.3.
208.64.163.11:443 (ftp.digitalimaginginc.com)	Running vulnerable HTTPS service: Apache 2.2.3.

References:

Source	Reference
BID	35115
CVE	CVE-2009-1195
SECUNIA	35261
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

Apache >= 2.1 and < 2.3

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.bz2

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.

3.2.5. Apache HTTP Method 413 Error Response Cross-Site Scripting Vulnerability (http-apache-malformed-413-response-xss)

Description:

Certain versions of the Apache web server do no properly sanitize the request method in 413 error response page returned when a malformed request with a huge value for Content-Length is sent to the server. This lack of escaping results in a cross-site scripting vulnerablity on the server.

This vulnerability is only exploitable if a flawed HTTP client can be forced to send an HTTP request with an invalid method name.

Affected Nodes:

Affected Nodes:	Additional Information:
208.64.163.11:80 (ftp.digitalimaginginc.com)	Running vulnerable HTTP service: Apache 2.2.3. http://www.harborexpress.com/ 3: <title>413 Request Entity Too Large</title> 4: </head><body> 5: Request Entity Too Large 6: The requested resource /index.shtml 7: does not allow request data with <SCRIPT>NXSSTEST</SCRIPT> requests
208.64.163.11:443 (ftp.digitalimaginginc.com)	Running vulnerable HTTPS service: Apache 2.2.3. https://www.harborexpress.com/ 3: <title>413 Request Entity Too Large</title> 4: </head><body> 5: Request Entity Too Large 6: The requested resource /index.html 7: does not allow request data with <SCRIPT>NXSSTEST</SCRIPT> requests

References:

Source	Reference
BID	26663
CVE	CVE-2007-6203
URL	http://procheckup.com/Vulnerability_PR07-37.php
SECUNIA	27906
URL	http://svn.apache.org/viewvc?view=rev&revision=604425
URL	http://svn.apache.org/viewvc?view=rev&revision=602473
URL	http://svn.apache.org/viewvc?view=rev&revision=600645

Vulnerability Solution:

•Apache >= 2.0 and < 2.1

Upgrade to Apache version 2.0.62

Apache 2.0.62 was never released because of quality problems found in the pre-release tarballs. Upgrade to Apache 2.0.63 instead.

•Apache >= 2.1 and < 2.3

Upgrade to Apache version 2.2.7

Apache 2.2.7 was never released because of quality problems found in the pre-release tarballs. Upgrade to Apache 2.2.8 instead.

3.2.6. Apache Signals Sent to Arbitrary Processes Denial of Service (http-apache-mod-prefork-mpm-dos)

Description:

Some versions of the Apache HTTP server do not verify that a process is an Apache child process before sending it signals. A local attacker with the ability to run scripts on the HTTP server could manipulate the scoreboard (worker_score and process_score arrays) to reference an arbitrary process ID and cause arbitrary processes to be terminated which could lead to a denial of service.

Affected Nodes:

Affected Nodes:	Additional Information:
208.64.163.11:80 (ftp.digitalimaginginc.com)	Running vulnerable HTTP service: Apache 2.2.3.
208.64.163.11:443 (ftp.digitalimaginginc.com)	Running vulnerable HTTPS service: Apache 2.2.3.

References:

Source	Reference
BID	24215
CVE	CVE-2007-3304
SECUNIA	26273
URL	http://httpd.apache.org/security/vulnerabilities_13.html
URL	http://httpd.apache.org/security/vulnerabilities_20.html
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

•Apache >= 1.0 and < 2.0

Upgrade to Apache version 1.3.39

Download and apply the upgrade from: http://www.apache.org/dist/httpd/apache_1.3.39.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 >= 2.0 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.

3.2.7. Apache mod_cache Proxy Denial of Service (http-apache-mod_cache-proxy-dos)

Description:

Some versions of Apache httpd ship a mod_cache module that may crash due to a buffer over-read when parsing maliciously crafted cache-control headers such as s-maxage, max-age, min-fresh, or max-stale. This could lead to a denial of service if using a threaded Multi-Processing Module.

Affected Nodes:

Affected Nodes:	Additional Information:
208.64.163.11:80 (ftp.digitalimaginginc.com)	Running vulnerable HTTP service: Apache 2.2.3.
208.64.163.11:443 (ftp.digitalimaginginc.com)	Running vulnerable HTTPS service: Apache 2.2.3.

References:

Source	Reference
BID	24649
CVE	CVE-2007-1863
SECUNIA	26273
URL	http://httpd.apache.org/security/vulnerabilities_20.html

Source	Reference
URL	http://httpd.apache.org/security/vulnerabilities_22.html

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.

3.2.8. Apache mod_proxy Reverse Proxy Denial of Service (http-apache-mod_proxy-reverse-proxy-dos)

Description:

A denial of service flaw was found in the mod_proxy module when it was used as a reverse proxy. A remote attacker could use this flaw to force a proxy process to consume large amounts of CPU time.

Affected Nodes:

Affected Nodes:	Additional Information:
208.64.163.11:80 (ftp.digitalimaginginc.com)	Running vulnerable HTTP service: Apache 2.2.3.
208.64.163.11:443 (ftp.digitalimaginginc.com)	Running vulnerable HTTPS service: Apache 2.2.3.

References:

Source	Reference
BID	35565
CVE	CVE-2009-1890
SECUNIA	35691
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

Apache >= 2.1 and < 2.3

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.bz2

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.

3.2.9. Apache mod_proxy_ajp Denial of Service (http-apache-mod_proxy_ajp-dos)

Description:

mod_proxy_ajp would return the wrong status code if it encountered an error, causing a backend server to be put into an error state until the retry timeout expired. A remote attacker could send malicious requests to trigger this issue, resulting in denial of service.

Affected Nodes:

Affected Nodes:	Additional Information:
208.64.163.11:80 (ftp.digitalimaginginc.com)	Running vulnerable HTTP service: Apache 2.2.3.
208.64.163.11:443 (ftp.digitalimaginginc.com)	Running vulnerable HTTPS service: Apache 2.2.3.

References:

Source	Reference
BID	38491
CVE	CVE-2010-0408
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

Apache >= 2.1 and < 2.3

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.15.tar.bz2

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.

3.2.10. Apache mod_proxy_ftp Denial of Service (http-apache-mod_proxy_ftp-dos)

Description:

A NULL pointer dereference flaw was found in the mod_proxy_ftp module. A malicious FTP server to which requests are being proxied could use this flaw to crash an httpd child process via a malformed reply to the EPSV or PASV commands, resulting in a limited denial of service.

Affected Nodes:

Affected Nodes:	Additional Information:
208.64.163.11:80 (ftp.digitalimaginginc.com)	Running vulnerable HTTP service: Apache 2.2.3.
208.64.163.11:443 (ftp.digitalimaginginc.com)	Running vulnerable HTTPS service: Apache 2.2.3.

References:

Source	Reference
BID	36260
CVE	CVE-2009-3094
SECUNIA	36549
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

Apache >= 2.1 and < 2.3

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.14.tar.bz2

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.

3.2.11. 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:
208.64.163.11:80 (ftp.digitalimaginginc.com)	http://www.harborexpress.com/icons/small/ 5: </head> 6: <body> 7: Index of /icons/small 8: <table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a ... 9: ...IR]"></td><td>Parent Directory</td><td> ...
208.64.163.11:80 (ftp.digitalimaginginc.com)	http://www.harborexpress.com/icons/ 5: </head> 6: <body> 7: Index of /icons 8: <table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a ... 9: ...IR]"></td><td>Parent Directory</td><td> </td><...
208.64.163.11:80 (ftp.digitalimaginginc.com)	http://www.harborexpress.com/icons/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 5: </head> 6: <body> 7: Index of /icons 8: <table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a ... 9: ...IR]"></td><td>Parent Directory</td><td> </td><...
208.64.163.11:80 (ftp.digitalimaginginc.com)	http://www.harborexpress.com/icons/small/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 5: </head> 6: <body> 7: Index of /icons/small 8: <table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a ... 9: ...IR]"></td><td>Parent Directory</td><td> ...
208.64.163.11:80 (ftp.digitalimaginginc.com)	http://www.harborexpress.com/manual/de/images/ 5: </head> 6: <body> 7: Index of /manual/de/images 8: <table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a ... 9: ...IR]"></td><td>Parent Directory</td><td>&n...

Affected Nodes:	Additional Information:
208.64.163.11:80 (ftp.digitalimaginginc.com)	http://www.harborexpress.com/manual/images/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 5: </head> 6: <body> 7: Index of /manual/images 8: <table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a ... 9: ...IR]"></td><td>Parent Directory</td><td> ...
208.64.163.11:80 (ftp.digitalimaginginc.com)	http://www.harborexpress.com/manual/images/ 5: </head> 6: <body> 7: Index of /manual/images 8: <table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a ... 9: ...IR]"></td><td>Parent Directory</td><td> ...
208.64.163.11:443 (ftp.digitalimaginginc.com)	https://www.harborexpress.com/manual/images/ 5: </head> 6: <body> 7: Index of /manual/images 8: <table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a ... 9: ...IR]"></td><td>Parent Directory</td><td> ...
208.64.163.11:443 (ftp.digitalimaginginc.com)	https://www.harborexpress.com/manual/images/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 5: </head> 6: <body> 7: Index of /manual/images 8: <table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a ... 9: ...IR]"></td><td>Parent Directory</td><td> ...
208.64.163.11:443 (ftp.digitalimaginginc.com)	https://www.harborexpress.com/manual/de/style/css/ 5: </head> 6: <body> 7: Index of /manual/de/style/css 8: <table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a ... 9: ...IR]"></td><td>Parent Directory</td>...
208.64.163.11:443	https://www.harborexpress.com/icons/small/?P=+ADw-script+AD4-alert(42)+ADw-

Affected Nodes:	Additional Information:
(ftp.digitalimaginginc.com)	/script+AD4- 5: </head> 6: <body> 7: Index of /icons/small 8: <table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a ... 9: ...IR]"></td><td>Parent Directory</td><td> ...
208.64.163.11:443 (ftp.digitalimaginginc.com)	https://www.harborexpress.com/icons/small/ 5: </head> 6: <body> 7: Index of /icons/small 8: <table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a ... 9: ...IR]"></td><td>Parent Directory</td><td> ...
208.64.163.11:443 (ftp.digitalimaginginc.com)	https://www.harborexpress.com/manual/de/style/xsl/util/ 5: </head> 6: <body> 7: Index of /manual/de/style/xsl/util 8: <table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a ... 9: ...IR]"></td><td>Parent Directory
208.64.163.11:443 (ftp.digitalimaginginc.com)	https://www.harborexpress.com/icons/?P=+ADw-script+AD4-alert(42)+ADw-/script+AD4- 5: </head> 6: <body> 7: Index of /icons 8: <table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a ... 9: ...IR]"></td><td>Parent Directory</td><td> </td><...
208.64.163.11:443 (ftp.digitalimaginginc.com)	https://www.harborexpress.com/icons/ 5: </head> 6: <body> 7: Index of /icons 8: <table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a ... 9: ...IR]"></td><td>Parent Directory</td><td> </td><...
208.64.163.11:443 (ftp.digitalimaginginc.com)	https://www.harborexpress.com/manual/de/style/lang/ 5: </head> 6: <body>

Affected Nodes:	Additional Information:
	7: Index of /manual/de/style/lang 8: <table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a ... 9: ...IR]"></td><td>Parent Directory</td>...
208.64.163.11:443 (ftp.digitalimaginginc.com)	https://www.harborexpress.com/manual/de/images/ 5: </head> 6: <body> 7: Index of /manual/de/images 8: <table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a ... 9: ...IR]"></td><td>Parent Directory</td><td>&n...
208.64.163.11:443 (ftp.digitalimaginginc.com)	https://www.harborexpress.com/manual/de/style/ 5: </head> 6: <body> 7: Index of /manual/de/style 8: <table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a ... 9: ...IR]"></td><td>Parent Directory</td><td>&n...
208.64.163.11:443 (ftp.digitalimaginginc.com)	https://www.harborexpress.com/manual/de/style/xsl/ 5: </head> 6: <body> 7: Index of /manual/de/style/xsl 8: <table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a ... 9: ...IR]"></td><td>Parent Directory</td>...
208.64.163.11:443 (ftp.digitalimaginginc.com)	https://www.harborexpress.com/manual/de/style/latex/ 5: </head> 6: <body> 7: Index of /manual/de/style/latex 8: <table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a ... 9: ...IR]"></td><td>Parent Directory</td>...

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.

3.2.12. Apache APR-util Heap Underwrite (http-apache-apr-util-heap-underwrite)

Description:

A heap-based underwrite flaw was found in the way the bundled copy of the APR-util library created compiled forms of particular search patterns. An attacker could formulate a specially-crafted search keyword, that would overwrite arbitrary heap memory locations when processed by the pattern preparation engine.

Affected Nodes:

Affected Nodes:	Additional Information:

Affected Nodes:	Additional Information:
208.64.163.11:80 (ftp.digitalimaginginc.com)	Running vulnerable HTTP service: Apache 2.2.3.
208.64.163.11:443 (ftp.digitalimaginginc.com)	Running vulnerable HTTPS service: Apache 2.2.3.

References:

Source	Reference
BID	35221
CVE	CVE-2009-0023
SECUNIA	35284
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

Apache >= 2.1 and < 2.3

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.bz2

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.

3.2.13. Apache mod_deflate Denial of Service (http-apache-mod_deflate-dos)

Description:

A denial of service flaw was found in the mod_deflate module. This module continued to compress large files until compression was complete, even if the network connection that requested the content was closed before compression completed. This would cause mod_deflate to consume large amounts of CPU if mod_deflate was enabled for a large file.

Affected Nodes:

Affected Nodes:	Additional Information:
208.64.163.11:80 (ftp.digitalimaginginc.com)	Running vulnerable HTTP service: Apache 2.2.3.
208.64.163.11:443 (ftp.digitalimaginginc.com)	Running vulnerable HTTPS service: Apache 2.2.3.

References:

Source	Reference

Source	Reference
BID	35623
CVE	CVE-2009-1891
SECUNIA	35781
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

Apache >= 2.1 and < 2.3
Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.bz2
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.

3.2.14. Apache mod_imap/mod_imagemap Cross-Site Scripting Vulnerability in imagemap File Menus (http-apache-mod_imap-mod_imagemap-menu-xss)

Description:

Versions of Apache httpd older than 1.3.40, 2.0.62 and 2.2.7 ship with a mod_imap/mod_imagemap module that is vulnerable to a cross-site scripting vulnerability.

Exploiting the vulnerability requires that mod_imap (Apache 1.3/2.0) or mod_imagemap (Apache 2.2) is enabled and that at least one imagemap file is accessible on the web server. Such files usually bear the .map extension. The XSS vulnerability can be triggered by sending a specially crafted GET request to obtain the HTML menu associated to an imagemap file, example:

```
GET /foo.map/<script>alert(42)</script> HTTP/1.1
Host: bar
```

Affected Nodes:

Affected Nodes:	Additional Information:
208.64.163.11:80 (ftp.digitalimaginginc.com)	Running vulnerable HTTP service: Apache 2.2.3.
208.64.163.11:443 (ftp.digitalimaginginc.com)	Running vulnerable HTTPS service: Apache 2.2.3.

References:

Source	Reference

Source	Reference
BID	26838
CVE	CVE-2007-5000
SECUNIA	28073
SECUNIA	28081
SECUNIA	28046
URL	http://httpd.apache.org/security/vulnerabilities_13.html
URL	http://httpd.apache.org/security/vulnerabilities_20.html
URL	http://httpd.apache.org/security/vulnerabilities_22.html
URL	http://svn.apache.org/viewvc?view=rev&revision=603282
URL	http://svn.apache.org/viewvc?view=rev&revision=603597
URL	http://svn.apache.org/viewvc?view=rev&revision=603619
URL	http://svn.apache.org/viewvc?view=rev&revision=603711

Vulnerability Solution:

•Apache >= 1.0 and < 2.0

Upgrade to Apache version 1.3.41

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/apache_1.3.41.tar.bz2

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 >= 2.0 and < 2.1

Upgrade to Apache version 2.0.63

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.0.63.tar.bz2

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 2.2.8

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.8.tar.bz2

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.

3.2.15. Apache mod_proxy Date Parsing Buffer Over-read Denial of Service (http-apache-mod_proxy-date-parsing-dos)

Description:

Some versions of Apache httpd ship a mod_proxy module that may crash due to a buffer over-read when parsing maliciously crafted date headers such as Date, Expires, or Last-Modified. This could lead to a denial of service if using a threaded Multi-Processing Module.

On sites where mod_proxy acts as a reverse proxy, a remote attacker could send a carefully crafted HTTP request that would cause the Apache child process handling that request to crash.

On sites where mod_proxy acts as a regular (forward) proxy, a malicious remote server could cause a similar crash by sending a carefully crafted HTTP reply. For this to happen, a remote attacker would have to entice a user behind the vulnerable proxy to visit a malicious site.

Affected Nodes:

Affected Nodes:	Additional Information:
208.64.163.11:80 (ftp.digitalimaginginc.com)	Running vulnerable HTTP service: Apache 2.2.3.
208.64.163.11:443 (ftp.digitalimaginginc.com)	Running vulnerable HTTPS service: Apache 2.2.3.

References:

Source	Reference
BID	25489
CVE	CVE-2007-3847
SECUNIA	26636
URL	http://httpd.apache.org/security/vulnerabilities_20.html
URL	http://httpd.apache.org/security/vulnerabilities_22.html
URL	http://svn.apache.org/viewvc?view=rev&revision=561616
URL	http://svn.apache.org/viewvc?view=rev&revision=563329
URL	http://svn.apache.org/viewvc?view=rev&revision=563198

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.

3.2.16. Apache Request Header Information Disclosure (http-apache-request-header-info-disclosure)

Description:

A flaw in the core subrequest process code was fixed, to always provide a shallow copy of the headers_in array to the subrequest, instead of a pointer to the parent request's array as it had for requests without request bodies. This meant all modules such as mod_headers which may manipulate the input headers for a subrequest would poison the parent request in two ways, one by modifying the parent request, which might not be intended, and second by leaving pointers to modified header fields in memory allocated to the subrequest scope, which could be freed before the main request processing was finished, resulting in a segfault or in revealing data from another request on threaded servers, such as the worker or winnt MPMs.

Affected Nodes:

Affected Nodes:	Additional Information:
208.64.163.11:80 (ftp.digitalimaginginc.com)	Running vulnerable HTTP service: Apache 2.2.3.
208.64.163.11:443 (ftp.digitalimaginginc.com)	Running vulnerable HTTPS service: Apache 2.2.3.

References:

Source	Reference
BID	38494
CVE	CVE-2010-0434
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

Apache >= 2.1 and < 2.3

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.15.tar.bz2

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:
208.64.163.11:80 (ftp.digitalimaginginc.com)	Running vulnerable HTTP service: Apache 2.2.3. http://www.harborexpress.com/login.htm 1: "2d20649-3c3-fa9d3b00"
208.64.163.11:443 (ftp.digitalimaginginc.com)	Running vulnerable HTTPS service: Apache 2.2.3. https://www.harborexpress.com/ 1: "2ae02f4-dc3-af2239c0"

References:

Source	Reference
BID	6939
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. WebDAV Extensions are Enabled (http-generic-webdav-enabled)

Description:

WebDAV is a set of extensions to the HTTP protocol that allows users to collaboratively edit and manage files on remote web servers. Many web servers enable WebDAV extensions by default, even when they are not needed. Because of its added complexity, it is considered good practice to disable WebDAV if it is not currently in use.

Affected Nodes:

Affected Nodes:	Additional Information:
208.64.163.11:80 (ftp.digitalimaginginc.com)	Running vulnerable HTTP service: Apache 2.2.3.
208.64.163.11:443 (ftp.digitalimaginginc.com)	Running vulnerable HTTPS service: Apache 2.2.3.

References:

Source	Reference
URL	http://www.nextgenss.com/papers/iisrconfig.pdf

Vulnerability Solution:

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

Disable WebDAV for IIS

For Microsoft IIS, follow Microsoft's instructions to disable WebDAV for the entire server.

•Apache

Disable WebDAV for Apache

Make sure the mod_dav module is disabled, or ensure that authentication is required on directories where DAV is required.

•Apache Tomcat, Tomcat, Tomcat Web Server

Disable WebDAV for Apache Tomcat

Disable the WebDAV Servlet for all web applications found on the web server. This can be done by removing the servlet definition for WebDAV (the org.apache.catalina.servlets.WebdavServlet class) and remove all servlet mappings referring to the WebDAV servlet.

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

Disable WebDAV for iPlanet/Sun ONE

Disable WebDAV on the web server. This can be done by disabling WebDAV for the server instance and for all virtual servers.

To disable WebDAV for the server instance, enter the Server Manager and uncheck the "Enable WebDAV Globally" checkbox then click the "OK" button.

To disable WebDAV for each virtual server, enter the Class Manager and uncheck the "Enable WebDAV Globally" checkbox next to each server instance then click the "OK" button.

4. Discovered Services

4.1. DNS-TCP

DNS, the Domain Name System, provides naming services on the Internet. DNS is primarily used to convert names, such as www.rapid7.com to their corresponding IP address for use by network programs, such as a browser. This service is used primarily for zone transfers between DNS servers. It can, however, be used for standard DNS queries as well.

4.1.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
208.64.163.11 (ftp.digitalimaginginc.com)	tcp	53	0	•BIND 9.3.4-P1

4.2. 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.

4.2.1. 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.

4.2.2. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
208.64.163.11 (ftp.digitalimaginginc.com)	tcp	21	0	•ProFTPD 1.3.1 •ftp.banner: 220 ProFTPD 1.3.1 Server (ProFTPD) [208.64.163.11]

4.3. 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.

4.3.1. 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.

4.3.2. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
208.64.163.11 (ftp.digitalimaginginc.com)	tcp	80	7	•Apache 2.2.3 •WebDAV: •http.banner: Apache/2.2.3 (CentOS) •http.banner.server: Apache/2.2.3 (CentOS) •verbs-1: GET •verbs-2: HEAD •verbs-3: OPTIONS •verbs-4: POST •verbs-count: 4

4.4. HTTPS

HTTPS, the HyperText Transfer Protocol over TLS/SSL, is used to exchange multimedia content on the World Wide Web using encrypted (TLS/SSL) connections. Once the TLS/SSL connection is established, the standard HTTP protocol is used. The multimedia files commonly used with HTTP include text, sound, images and video.

4.4.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
208.64.163.11 (ftp.digitalimaginginc.com)	tcp	443	7	•Apache 2.2.3 •WebDAV: •http.banner: Apache/2.2.3 (CentOS) •http.banner.server: Apache/2.2.3 (CentOS) •https.cert.issuer.dn: CN=UTN-USERFirst-Hardware, OU=http://www.usertrust.com, O=The USERTRUST Network, L=Salt Lake City, ST=UT, C=US •https.cert.key.alg.name: RSA •https.cert.not.valid.after: Fri, 17 Sep 2010 19:59:59 EDT •https.cert.not.valid.before: Mon, 17 Sep 2007 20:00:00 EDT •https.cert.selfsigned: false •https.cert.serial.number: 232322238194487829358448688631416712672 •https.cert.sig.alg.name: SHA1withRSA •https.cert.subject.dn: CN=apollo.techevolution.com, OU=Comodo InstantSSL, OU=Hosted by Techevolution,

Device	Protocol	Port	Vulnerabilities	Additional Information
				O=Techevolution, STREET=85 Exchange Street L12, L=Lynn, ST=MA, OID.2.5.4.17=01901, C=US •https.cert.validchain: true •tls: true •tls.version.ssl20: true •verbs-1: GET •verbs-2: HEAD •verbs-3: OPTIONS •verbs-4: POST •verbs-count: 4
208.64.163.11 (ftp.digitalimaginginc.com)	tcp	8443	0	•sw-cp-server 1.0.0 •http.banner: sw-cp-server/1.0.0 •http.banner.server: sw-cp-server/1.0.0 •https.cert.issuer.dn: CN=UTN-USERFirst-Hardware, OU=http://www.usertrust.com, O=The USERTRUST Network, L=Salt Lake City, ST=UT, C=US •https.cert.key.alg.name: RSA •https.cert.not.valid.after: Fri, 17 Sep 2010 19:59:59 EDT •https.cert.not.valid.before: Mon, 17 Sep 2007 20:00:00 EDT •https.cert.selfsigned: false •https.cert.serial.number: 232322238194487829358448688631416712672 •https.cert.sig.alg.name: SHA1withRSA •https.cert.subject.dn: CN=apollo.techevolution.com, OU=Comodo InstantSSL, OU=Hosted by Techevolution, O=Techevolution, STREET=85 Exchange Street L12, L=Lynn, ST=MA, OID.2.5.4.17=01901, C=US •https.cert.validchain: true •tls: true

4.5. IMAP

IMAP, the Interactive Mail Access Protocol or Internet Message Access Protocol, is used to access and manipulate electronic mail (e-mail). IMAP servers can contain several folders, aka mailboxes, containing messages (e-mails) for users.

4.5.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
208.64.163.11	tcp	143	0	•imap.banner: * OK [CAPABILITY IMAP4rev1 UIDPLUS

Device	Protocol	Port	Vulnerabilities	Additional Information
(ftp.digitalimaginginc.com)				CHILDREN NAMESPACE THREAD=ORDEREDSUBJECT THREAD=REFERENCES SORT QUOTA IDLE ACL ACL2=UNION STARTTLS] Courier-IMAP ready. Copyright 1998-2004 Double Precision, Inc. See COPYING for distribution information.

4.6. IMAPS

IMAPS, the Internet Message Access Protocol over TLS/SSL, is used to access and manipulate electronic mail (e-mail) using encrypted (TLS/SSL) connections. Once the TLS/SSL connection is established, the standard IMAP protocol is used. IMAP servers can contain several folders, aka mailboxes, containing messages (e-mails) for users.

4.6.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
208.64.163.11 (ftp.digitalimaginginc.com)	tcp	993	0	

4.7. POP

The Post Office Protocol allows workstations to retrieve e-mail dynamically from a mailbox server.

4.7.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
208.64.163.11 (ftp.digitalimaginginc.com)	tcp	110	0	•pop.banner: +OK Hello there. <9295.1279803281@localhost.localdomain>

4.8. POPS

The Post Office Protocol allows workstations to retrieve e-mail dynamically from a mailbox server. POPS simply adds SSL support to POP3.

4.8.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
208.64.163.11 (ftp.digitalimaginginc.com)	tcp	995	0	

4.9. SMTP

SMTP, the Simple Mail Transfer Protocol, is the Internet standard way to send e-mail messages between hosts. Clients typically submit outgoing e-mail to their SMTP server, which then forwards the message on through other SMTP servers until it reaches its final

destination.

4.9.1. General Security Issues

Installed by default

By default, most UNIX workstations come installed with the sendmail (or equivalent) SMTP server to handle mail for the local host (e.g. the output of some cron jobs is sent to the root account via email). Check your workstations to see if sendmail is running, by telnetting to port 25/tcp. If sendmail is running, you will see something like this: $ telnet mybox 25 Trying 192.168.0.1... Connected to mybox. Escape character is '^]'. 220 mybox. ESMTP Sendmail 8.12.2/8.12.2; Thu, 9 May 2002 03:16:26 -0700 (PDT) If sendmail is running and you don't need it, then disable it via /etc/rc.conf or your operating system's equivalent startup configuration file. If you do need SMTP for the localhost, make sure that the server is only listening on the loopback interface (127.0.0.1) and is not reachable by other hosts. Also be sure to check port 587/tcp, which some versions of sendmail use for outgoing mail submissions.

Promiscuous relay

Perhaps the most common security issue with SMTP servers is servers which act as a "promiscuous relay", or "open relay". This describes servers which accept and relay mail from anywhere to anywhere. This setup allows unauthenticated 3rd parties (spammers) to use your mail server to send their spam to unwitting recipients. Promiscuous relay checks are performed on all discovered SMTP servers. See "smtp-general-openrelay" for more information on this vulnerability and how to fix it.

4.9.2. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
208.64.163.11 (ftp.digitalimaginginc.com)	tcp	25	0	•qmail •advertise-esmtp: 1 •advertised-esmtp-extension-count: 5 •advertises-esmtp: TRUE •smtp.banner: 220 apollo.techevolution.com ESMTP •smtp.cert.issuer.dn: CN=UTN-USERFirst-Hardware, OU=http://www.usertrust.com, O=The USERTRUST Network, L=Salt Lake City, ST=UT, C=US •smtp.cert.key.alg.name: RSA •smtp.cert.not.valid.after: Fri, 17 Sep 2010 19:59:59 EDT •smtp.cert.not.valid.before: Mon, 17 Sep 2007 20:00:00 EDT •smtp.cert.selfsigned: false •smtp.cert.serial.number: 232322238194487829358448688631416712672 •smtp.cert.sig.alg.name: SHA1withRSA •smtp.cert.subject.dn: CN=apollo.techevolution.com, OU=Comodo InstantSSL, OU=Hosted by Techevolution, O=Techevolution, STREET=85 Exchange Street L12, L=Lynn, ST=MA, OID.2.5.4.17=01901, C=US

Device	Protocol	Port	Vulnerabilities	Additional Information
				•smtp.cert.validchain: true •supported-auth-method-count: 3 •supported-auth-method:1: LOGIN •supported-auth-method:2: CRAM-MD5 •supported-auth-method:3: PLAIN •supports-8bitmime: TRUE •supports-auth: TRUE •supports-auth=login: TRUE •supports-debug: FALSE •supports-expand: FALSE •supports-pipelining: TRUE •supports-starttls: TRUE •supports-turn: FALSE •supports-verify: FALSE
208.64.163.11 (ftp.digitalimaginginc.com)	tcp	587	0	•qmail •advertise-esmtp: 1 •advertised-esmtp-extension-count: 5 •advertises-esmtp: TRUE •smtp.banner: 220 apollo.techevolution.com ESMTP •smtp.cert.issuer.dn: CN=UTN-USERFirst-Hardware, OU=http://www.usertrust.com, O=The USERTRUST Network, L=Salt Lake City, ST=UT, C=US •smtp.cert.key.alg.name: RSA •smtp.cert.not.valid.after: Fri, 17 Sep 2010 19:59:59 EDT •smtp.cert.not.valid.before: Mon, 17 Sep 2007 20:00:00 EDT •smtp.cert.selfsigned: false •smtp.cert.serial.number: 232322238194487829358448688631416712672 •smtp.cert.sig.alg.name: SHA1withRSA •smtp.cert.subject.dn: CN=apollo.techevolution.com, OU=Comodo InstantSSL, OU=Hosted by Techevolution, O=Techevolution, STREET=85 Exchange Street L12, L=Lynn, ST=MA, OID.2.5.4.17=01901, C=US •smtp.cert.validchain: true •supported-auth-method-count: 3 •supported-auth-method:1: LOGIN •supported-auth-method:2: CRAM-MD5

Device	Protocol	Port	Vulnerabilities	Additional Information
				•supported-auth-method:3: PLAIN •supports-8bitmime: TRUE •supports-auth: TRUE •supports-auth=login: TRUE •supports-debug: FALSE •supports-expand: FALSE •supports-pipelining: TRUE •supports-starttls: TRUE •supports-turn: FALSE •supports-verify: FALSE

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://208.64.163.11:80

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)

- _private
- cgi-bin
- css
- error
- img
- usage

Successful (200)

- common
- icons
- images
- manual
  - howto
  - images
  - misc
  - mod
  - programs
  - vhosts

9.1.2. Guessed URLs

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

Access Error (403)

- _private
  - ?P=+ADw-script+AD4-alert(42)+ADw-
    - script+AD4-
    - script+AD4-
    - script+AD4-
    - script+AD4-
    - script+AD4-
- cgi-bin

- css
- error
- img

Error (400)

- never
  - found
    - %0
      - cgi-bin
- usr
  - local
    - apache
      - vhosts
        - %0
        - %1
          - %2
            - %3
              - %4
                - cgi-bin
                - docs
        - %2.0.%3.0
        - %3+
          - %2.-1
            - %2.-2
              - %2.-3
                - %2
          - %2.1
            - %2.2
              - %2.3
                - %2
                - %2.4+
- your
  - docroot
    - %{REQUEST_FILENAME}

Redirect (301)

- icons
  - small
- images

- manual
- manual
  - images

Successful (200)

- ?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-
- about
  - _vti_cnf
    - index.html
  - index.shtml
- charters
  - index.shtml
- common
  - index.shtml
- commuters
  - index.shtml
- cruisendine

- css
  - style.css
- employment
  - index.shtml
- harborislands
  - index.shtml
- icons
  - README
  - small
    - README
- images
  - index.shtml
- index.shtml
- index.shtml
- manual
  - de
    - developer
      - index.html
    - faq
      - index.html
    - howto
      - index.html
      - index.html
    - images
    - index.html
    - misc
      - index.html
    - mod
      - index.html
    - platform
      - index.html
    - programs
      - index.html
  - index.html

9.1.3. Linked URLs

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

Redirect (301)

- about

- charters
- commuters
- cruisendine
- employment
- harborislands
- whalewatch

Successful (200)

- about
- charters
  - islandboats.shtml
  - offseason.shtml
  - salemferry.shtml
  - testimonials.shtml
  - voyager.shtml
- common
  - WTA_Privacy_Policy.pdf
  - WTA_Terms_of_Use.pdf
- commuters
  - Boston%20Fares_spring.shtml
  - Boston%20Fares_winter.shtml
  - Directions.shtml
  - Logan%20Fares_spring.shtml
  - Logan%20Fares_winter.shtml
  - T_Hull-Boston.shtml
  - T_Logan-Quincy.shtml
  - T_Quincy-Boston.shtml
  - boats.shtml
- cruisendine
  - bluescruise.shtml
  - cruisendine.shtml
  - cruisenplay2009.pdf
  - fireworks.shtml
- employment
- global.css
- harborislands
  - tours.shtml
- icons
  - small

- manual
  - bind.html
  - caching.html
  - configuring.html
  - content-negotiation.html
  - de
    - bind.html
    - caching.html
    - configuring.html
    - content-negotiation.html
    - custom-error.html
    - developer
      - API.html
      - debugging.html
      - documenting.html
      - filters.html
      - hooks.html
      - modules.html
      - request.html
      - thread_safety.html
    - dns-caveats.html
    - dso.html
    - env.html
    - faq
      - all_in_one.html
      - background.html
      - error.html
      - support.html
    - filter.html
    - glossary.html
    - handler.html
    - howto
      - access.html
      - auth.html
      - cgi.html
      - htaccess.html
      - public_html.html
      - ssi.html
    - install.html

- invoking.html
- license.html
- logs.html
- misc
  - perf-tuning.html
  - relevant_standards.html
  - rewriteguide.html
  - security_tips.html
  - perf-tuning.html
  - rewriteguide.html
  - security_tips.html
- mod
  - beos.html
  - core.html
  - directive-dict.html
  - directives.html
  - event.html
  - mod_actions.html
  - mod_alias.html
  - mod_asis.html
  - mod_auth_basic.html
  - mod_auth_digest.html
  - mod_authn_alias.html
  - mod_authn_anon.html
  - mod_authn_dbd.html
  - mod_authn_dbm.html
  - mod_authn_default.html
  - mod_authn_file.html
  - mod_authnz_ldap.html
  - mod_authz_dbm.html
  - mod_authz_default.html
  - mod_authz_groupfile.html
  - mod_authz_host.html
  - mod_authz_owner.html
  - mod_authz_user.html
  - mod_autoindex.html
  - mod_cache.html
  - mod_cern_meta.html
  - mod_cgi.html

- mod_cgid.html
- mod_charset_lite.html
- mod_dav.html
- mod_dav_fs.html
- mod_dav_lock.html
- mod_dbd.html
- mod_deflate.html
- mod_dir.html
- mod_disk_cache.html
- mod_dumpio.html
- mod_echo.html
- mod_env.html
- mod_example.html
- mod_expires.html
- mod_ext_filter.html
- mod_file_cache.html
- mod_filter.html
- mod_headers.html
- mod_ident.html
- mod_imagemap.html
- mod_include.html
- mod_info.html
- mod_isapi.html
- mod_ldap.html
- mod_log_config.html
- mod_log_forensic.html
- mod_logio.html
- mod_mem_cache.html
- mod_mime.html
- mod_mime_magic.html
- mod_negotiation.html
- mod_nw_ssl.html
- mod_proxy.html
- mod_proxy_ajp.html
- mod_proxy_balancer.html
- mod_proxy_connect.html
- mod_proxy_ftp.html
- mod_proxy_http.html
- mod_rewrite.html

- mod_setenvif.html
- mod_so.html
- mod_speling.html
- mod_ssl.html
- mod_status.html
- mod_suexec.html
- mod_unique_id.html
- mod_userdir.html
- mod_usertrack.html
- mod_version.html
- mod_vhost_alias.html
- module-dict.html
- mpm_common.html
- mpm_netware.html
- mpm_winnt.html
- mpmt_os2.html
- prefork.html
- quickreference.html
- worker.html
- core.html
- directive-dict.html
- directives.html
- mod_cache.html
- mod_dir.html
- mod_disk_cache.html
- mod_expires.html
- mod_file_cache.html
- mod_mem_cache.html
- mod_mime.html
- mod_negotiation.html
- mod_proxy.html
- mod_rewrite.html
- mod_so.html
- mod_userdir.html
- module-dict.html
- mpm_common.html
- quickreference.html
- mpm.html
- new_features_2_0.html

- new_features_2_2.html
- platform
  - ebcdic.html
  - netware.html
  - win_compiling.html
  - windows.html
  - ebcdic.html
  - netware.html
  - windows.html
- programs
  - ab.html
  - apachectl.html
  - apxs.html
  - configure.html
  - dbmmanage.html
  - htcacheclean.html
  - htdbm.html
  - htdigest.html
  - htpasswd.html
  - httpd.html
  - httxt2dbm.html
  - logresolve.html
  - other.html
  - rotatelogs.html
  - suexec.html
  - configure.html
  - htcacheclean.html
- rewrite
  - rewrite_guide.html
  - rewrite_guide_advanced.html
- sections.html
- server-wide.html
- sitemap.html
- ssl
  - ssl_compat.html
- stopping.html
- style
  - css
    - manual-loose-100pc.css

- manual-print.css
- manual.css
- manual-loose-100pc.css
- manual-print.css
- manual.css
- suexec.html
- upgrading.html
- urlmapping.html
- vhosts
- details.html
- fd-limits.html
- mass.html
- name-based.html
- developer
- dns-caveats.html
- dso.html
- en
- bind.html
- caching.html
- configuring.html
- content-negotiation.html
- howto
- access.html
- auth.html
- cgi.html
- htaccess.html
- public_html.html
- ssi.html
- env.html
- faq
- filter.html
- fr
- bind.html
- glossary.html
- handler.html
- install.html
- invoking.html
- ja
- bind.html

- configuring.html
- content-negotiation.html
- howto
- ko
- bind.html
- configuring.html
- content-negotiation.html
- howto
- license.html
- logs.html
- mpm.html
- new_features_2_0.html
- new_features_2_2.html
- sections.html
- server-wide.html
- sitemap.html
- ssl
- stopping.html
- suexec.html
- upgrading.html
- urlmapping.html

9.2. https://208.64.163.11:443

9.2.1. 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
- css
- error
- img
- usage

Successful (200)

- icons
- manual
- howto
- images
- misc

- mod
- programs
- vhosts

9.2.2. Guessed URLs

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

Access Error (403)

- cgi-bin
  - ?P=+ADw-script+AD4-alert(42)+ADw-
    - script+AD4-
    - script+AD4-
    - script+AD4-
    - script+AD4-
    - script+AD4-
    - script+AD4-
- css
- error
- img
  - common
  - common
  - glyph
  - glyph

Error (400)

- never
  - found
    - %0
      - cgi-bin
        - $1
      - cgi-bin
      - docs
      - docs
      - cgi-bin
      - docs
- usr
  - local
    - apache
      - vhosts
        - %0

- %1
  - %2
    - %3
      - %4
        - cgi-bin
        - docs
      - docs
    - %2.0.%3.0
    - %3+
      - %2.-1
        - %2.-2
          - %2.-3
            - %2
        - %2.1
          - %2.2
            - %2.3
              - %2
              - %2.4+
- var
  - logs
    - errorlog.%Y-%m-%d-%H_%M_%S
- www
  - commercial
  - homepages
  - hosts
    - ${lowercase:%{SERVER_NAME}}
      - docs
        - $1
- your
  - docroot
    - %{REQUEST_FILENAME}

Redirect (301)

- icons
  - small
- manual
- manual
  - images

Successful (200)

- ?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-
- css
  - style.css
- icons
  - README
  - small
    - README
- index.html
- index.html
- manual
  - de
    - developer
      - index.html
      - index.html
      - index.html
    - faq
      - index.html
    - howto
      - index.html

- index.html
- images
- index.html
- misc
- index.html
- mod
- index.html
- platform
- index.html
- programs
- index.html
- rewrite
- ssl
- index.html
- style
- css
- vhosts
- index.html
- en
- index.html
- index.html

9.2.3. Linked URLs

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

Successful (200)

- css
- winxp.blue.css
- winxp.blue.css
- manual-chm.css
- manual-loose-100pc.css
- manual-print.css
- manual-zip-100pc.css
- manual-zip.css
- manual.css
- manual-loose-100pc.css
- manual-print.css
- manual.css
- manual-loose-100pc.css
- manual-print.css

- manual.css
- icons
  - small
- manual
  - bind.html
  - caching.html
  - configuring.html
  - content-negotiation.html
  - de
    - bind.html
    - caching.html
    - configuring.html
    - content-negotiation.html
    - custom-error.html
    - developer
      - API.html
      - debugging.html
      - documenting.html
      - filters.html
      - hooks.html
      - modules.html
      - request.html
      - thread_safety.html
    - dns-caveats.html
    - dso.html
    - env.html
    - faq
      - all_in_one.html
      - background.html
      - error.html
      - support.html
    - filter.html
    - glossary.html
    - handler.html
    - howto
      - access.html
      - auth.html
      - cgi.html
      - htaccess.html

- public_html.html
- ssi.html
- install.html
- invoking.html
- license.html
- logs.html
- misc
- perf-tuning.html
- relevant_standards.html
- rewriteguide.html
- security_tips.html
- mod
- beos.html
- core.html
- directive-dict.html
- directives.html
- event.html
- mod_actions.html
- mod_alias.html
- mod_asis.html
- mod_auth_basic.html
- mod_auth_digest.html
- mod_authn_alias.html
- mod_authn_anon.html
- mod_authn_dbd.html
- mod_authn_dbm.html
- mod_authn_default.html
- mod_authn_file.html
- mod_authnz_ldap.html
- mod_authz_dbm.html
- mod_authz_default.html
- mod_authz_groupfile.html
- mod_authz_host.html
- mod_authz_owner.html
- mod_authz_user.html
- mod_autoindex.html
- mod_cache.html
- mod_cern_meta.html
- mod_cgi.html

- mod_cgid.html
- mod_charset_lite.html
- mod_dav.html
- mod_dav_fs.html
- mod_dav_lock.html
- mod_dbd.html
- mod_deflate.html
- mod_dir.html
- mod_disk_cache.html
- mod_dumpio.html
- mod_echo.html
- mod_env.html
- mod_example.html
- mod_expires.html
- mod_ext_filter.html
- mod_file_cache.html
- mod_filter.html
- mod_headers.html
- mod_ident.html
- mod_imagemap.html
- mod_include.html
- mod_info.html
- mod_isapi.html
- mod_ldap.html
- mod_log_config.html
- mod_log_forensic.html
- mod_logio.html
- mod_mem_cache.html
- mod_mime.html
- mod_mime_magic.html
- mod_negotiation.html
- mod_nw_ssl.html
- mod_proxy.html
- mod_proxy_ajp.html
- mod_proxy_balancer.html
- mod_proxy_connect.html
- mod_proxy_ftp.html
- mod_proxy_http.html
- mod_rewrite.html

- mod_setenvif.html
- mod_so.html
- mod_speling.html
- mod_ssl.html
- mod_status.html
- mod_suexec.html
- mod_unique_id.html
- mod_userdir.html
- mod_usertrack.html
- mod_version.html
- mod_vhost_alias.html
- module-dict.html
- mpm_common.html
- mpm_netware.html
- mpm_winnt.html
- mpmt_os2.html
- prefork.html
- quickreference.html
- worker.html
- mpm.html
- new_features_2_0.html
- new_features_2_2.html
- platform
  - ebcdic.html
  - netware.html
  - perf-hp.html
  - win_compiling.html
  - windows.html
  - ebcdic.html
  - netware.html
  - windows.html
  - ebcdic.html
  - netware.html
  - windows.html
- programs
  - ab.html
  - apachectl.html
  - apxs.html
  - configure.html

- dbmmanage.html
- htcacheclean.html
- htdbm.html
- htdigest.html
- htpasswd.html
- httpd.html
- httxt2dbm.html
- logresolve.html
- other.html
- rotatelogs.html
- suexec.html
- rewrite
  - index.html
  - rewrite_guide.html
  - rewrite_guide_advanced.html
  - rewrite_intro.html
  - rewrite_tech.html
- sections.html
- server-wide.html
- sitemap.html
- ssl
  - ssl_compat.html
  - ssl_faq.html
  - ssl_howto.html
  - ssl_intro.html
- stopping.html
- style
  - build.properties
  - lang
  - latex
    - atbeginend.sty
  - xsl
    - util
- suexec.html
- upgrading.html
- urlmapping.html
- vhosts
  - details.html
  - examples.html

- fd-limits.html
- ip-based.html
- mass.html
- name-based.html
- developer
- API.html
- debugging.html
- documenting.html
- filters.html
- hooks.html
- modules.html
- request.html
- thread_safety.html
- dns-caveats.html
- dso.html
- en
- bind.html
- caching.html
- configuring.html
- content-negotiation.html
- developer
- API.html
- debugging.html
- documenting.html
- filters.html
- hooks.html
- modules.html
- request.html
- thread_safety.html
- modules.html
- dns-caveats.html
- dso.html
- env.html
- faq
- all_in_one.html
- background.html
- error.html
- support.html
- filter.html

- glossary.html
- handler.html
- howto
  - auth.html
  - cgi.html
  - htaccess.html
  - public_html.html
  - ssi.html
  - access.html
  - auth.html
  - cgi.html
  - htaccess.html
  - public_html.html
  - ssi.html
- install.html
- invoking.html
- license.html
- logs.html
- misc
  - perf-tuning.html
  - rewriteguide.html
  - security_tips.html
  - perf-tuning.html
  - rewriteguide.html
  - security_tips.html
- mod
  - core.html
  - directive-dict.html
  - directives.html
  - mod_alias.html
  - mod_asis.html
  - mod_authz_host.html
  - mod_autoindex.html
  - mod_cache.html
  - mod_cgi.html
  - mod_deflate.html
  - mod_dir.html
  - mod_disk_cache.html
  - mod_env.html

- mod_expires.html
- mod_ext_filter.html
- mod_file_cache.html
- mod_headers.html
- mod_include.html
- mod_log_config.html
- mod_mem_cache.html
- mod_mime.html
- mod_mime_magic.html
- mod_negotiation.html
- mod_proxy.html
- mod_rewrite.html
- mod_setenvif.html
- mod_so.html
- mod_unique_id.html
- mod_vhost_alias.html
- module-dict.html
- mpm_common.html
- quickreference.html
- core.html
- directive-dict.html
- directives.html
- mod_alias.html
- mod_asis.html
- mod_autoindex.html
- mod_cache.html
- mod_cgi.html
- mod_dir.html
- mod_disk_cache.html
- mod_env.html
- mod_expires.html
- mod_file_cache.html
- mod_include.html
- mod_mem_cache.html
- mod_mime.html
- mod_mime_magic.html
- mod_negotiation.html
- mod_proxy.html
- mod_rewrite.html

- mod_so.html
- mod_userdir.html
- mod_vhost_alias.html
- module-dict.html
- mpm_common.html
- quickreference.html
- mpm.html
- new_features_2_0.html
- new_features_2_2.html
- programs
  - apxs.html
  - configure.html
  - htcacheclean.html
  - httpd.html
  - suexec.html
  - apxs.html
  - configure.html
  - htcacheclean.html
  - httpd.html
- sections.html
- server-wide.html
- sitemap.html
- ssl
- stopping.html
- suexec.html
- upgrading.html
- urlmapping.html
- vhosts
  - details.html
  - name-based.html
  - details.html
  - name-based.html
- env.html
- faq
- filter.html
- fr
  - bind.html
- glossary.html
- handler.html

- install.html
- invoking.html
- ja
  - bind.html
  - configuring.html
  - content-negotiation.html
  - dns-caveats.html
  - dso.html
  - howto
- ko
  - bind.html
  - configuring.html
  - content-negotiation.html
  - dns-caveats.html
  - dso.html
  - howto
- license.html
- logs.html
- mpm.html
- new_features_2_0.html
- new_features_2_2.html
- sections.html
- server-wide.html
- sitemap.html
- ssl
- stopping.html
- suexec.html
- upgrading.html
- urlmapping.html

9.3. https://208.64.163.11:8443

9.3.1. Common Default URLs

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

Successful (200)

- login.php3
- plesk

9.3.2. Guessed URLs

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

Successful (200)

- ?P=+ADw-script+AD4-alert(42)+ADw-
  - script+AD4-
  - script+AD4-
- get_password.php
  - <script>xss<
    - script>
    - script>
    - script>
    - script>
    - script>
    - script>
    - script>
    - script>
    - script>
    - script>
    - script>
    - script>
    - script>
    - script>
    - script>
    - script>
    - script>
    - script>
    - script>
    - script>
    - script>
    - script>
    - script>
    - script>
    - script>
    - script>
    - script>
    - script>
    - script>
    - script>
    - script>
    - script>

- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>

- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>

- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>

- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- script>
- help.php
- help.php?context=
- index.php
- index.php
- javascript
  - chk.js.php
  - main.IeIE7.fixes.js?plesk_version=psa-9.2.2-92090714.19
- locales
  - en-US
    - help
      - 39588.htm
      - 47132.htm
      - 58818.htm
      - 59204.htm
      - 59205.htm
      - 59206.htm
      - 59207.htm
      - 59208.htm
      - 59209.htm
      - 59210.htm
      - 59211.htm
      - 59212.htm
      - 59214.htm

- 59215.htm
- 59216.htm
- 59217.htm
- 59218.htm
- 59219.htm
- 59220.htm
- 59221.htm
- 59223.htm
- 59224.htm
- 59225.htm
- 59226.htm
- 59246.htm
- 59247.htm
- 59248.htm
- 59249.htm
- 59250.htm
- 59251.htm
- 59252.htm
- 59253.htm
- 59254.htm
- 59255.htm
- 59256.htm
- 59257.htm
- 59258.htm
- 59259.htm
- 59260.htm
- 59261.htm
- 59262.htm
- 59263.htm
- 59264.htm
- 59265.htm
- 59266.htm
- 59267.htm
- 59268.htm
- 59269.htm
- 59270.htm
- 59271.htm
- 59272.htm
- 59273.htm

- 59274.htm
- 59275.htm
- 59282.htm
- 59312.htm
- 59313.htm
- 59314.htm
- 59315.htm
- 59316.htm
- 59317.htm
- 59318.htm
- 59319.htm
- 59325.htm
- 59326.htm
- 59327.htm
- 59331.htm
- 59335.htm
- 59349.htm
- 59352.htm
- 59359.htm
- 59360.htm
- 59371.htm
- 59375.htm
- 59376.htm
- 59377.htm
- 59402.htm
- 59404.htm
- 59405.htm
- 59406.htm
- 59407.htm
- 59408.htm
- 59421.htm
- 59424.htm
- 59425.htm
- 59426.htm
- 59443.htm
- 59444.htm
- 59446.htm
- 59450.htm
- 59464.htm

- 59471.htm
- 59472.htm
- 59473.htm
- 59475.htm
- 59476.htm
- 59480.htm
- 60174.htm
- 60179.htm
- 60188.htm
- 60203.htm
- 60204.htm
- 60205.htm
- 60210.htm
- 60285.htm
- 60286.htm
- 60287.htm
- 60305.htm
- 60330.htm
- 60331.htm
- 60421.htm
- 60422.htm
- 60795.htm
- 60927.htm
- 61056.htm
- 61064.htm
- 61069.htm
- 61078.htm
- 61091.htm
- 61092.htm
- 61093.htm
- 61094.htm
- 61095.htm
- 61098.htm
- 61099.htm
- 61865.htm
- 62121.htm
- 63016.htm
- 63017.htm
- dhtml_search.htm

- navigation.htm
- tab_toc.htm
- title.htm
- toc.htm
- toc5880510.htm
- toc58805104.htm
- toc58805109.htm
- toc58805110.htm
- toc58805116.htm
- toc58805129.htm
- toc58805269.htm
- toc58805272.htm
- toc58805273.htm
- toc58805276.htm
- toc58805284.htm
- toc58805287.htm
- toc58805291.htm
- toc58805295.htm
- toc58805296.htm
- toc58805303.htm
- toc58805308.htm
- toc58805312.htm
- toc58805316.htm
- toc58805319.htm
- toc58805320.htm
- toc58805327.htm
- toc588055.htm
- toc5880551.htm
- toc588059.htm

- login.php3
- login_up.php3
- plesk
  - %3f.jsp
  - .svn
    - entries
  - ADw-script AD4-alert(42) ADw-
    - script AD4-
  - CVS
    - Entries

- Root
- DEADJOE
- README
- README.TXT
- Trace.axd
- WEB-INF
- WS_FTP.LOG
- Web.sitemap
- _vti_bin
- _vti_bot
- _vti_cnf
- _vti_log
- _vti_pvt
- _vti_script
- _vti_shm
- _vti_txt
- adojavas.inc
- adovbs.inc
- default.asp
- default.aspx
- default.htm
- default.html
- default.jsp
- default.php
- default.shtml
- default.wml
- index.asp
- index.aspx
- index.bak
- index.cfm
- index.cgi
- index.chtml
- index.htm
- index.html
- index.jsp
- index.old
- index.php
- index.php3
- index.shtml

- index.swf
- readme.txt
- servlet
- sitemap.xml
- web-inf
- web.config
- wp-login.php
- skins
  - aqua
    - css
      - ie.css
- top.php3

9.3.3. Linked URLs

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

Successful (200)

- get_password.php
- javascript
  - chk.js.php
  - chk.js.php
    - <script>xss<
      - url
      - dhtml_search.htm
      - stylesheet.css
      - tab_search.htm
      - 39585.htm
      - 59204.htm
      - 59215.htm
      - 59218.htm
      - 59223.htm
      - 59246.htm
      - 59249.htm
      - 59256.htm
      - 59268.htm
      - 59269.htm
      - 59409.htm
      - 59443.htm
      - 59471.htm
      - 60210.htm

- stylesheet.css
- tab_toc.htm
- toc58805109.htm
- toc5880514.htm
- toc58805272.htm
- toc58805276.htm
- toc58805295.htm
- toc58805303.htm
- toc58805308.htm
- toc58805312.htm
- toc58805316.htm
- toc58805319.htm
- toc588055.htm
- toc5880551.htm
- toc588059.htm
- tab_toc.htm
- 39585.htm
- 59204.htm
- 59215.htm
- 59218.htm
- 59223.htm
- 59246.htm
- 59249.htm
- 59256.htm
- 59268.htm
- 59269.htm
- 59271.htm
- 59272.htm
- 59312.htm
- 59375.htm
- 59409.htm
- 59443.htm
- 59471.htm
- 60210.htm
- stylesheet.css
- tab_toc.htm
- toc.htm
- toc58805110.htm
- toc58805116.htm

- toc58805129.htm
- toc5880514.htm
- toc58805269.htm
- toc58805272.htm
- toc58805276.htm
- toc58805295.htm
- toc58805303.htm
- toc58805308.htm
- toc58805312.htm
- toc58805316.htm
- toc58805319.htm
- toc588055.htm
- toc5880551.htm
- toc588059.htm
- 39585.htm
- 59204.htm
- 59215.htm
- 59218.htm
- 59223.htm
- 59246.htm
- 59249.htm
- 59256.htm
- 59268.htm
- 59269.htm
- 59270.htm
- 59409.htm
- 59443.htm
- 59471.htm
- 60210.htm
- stylesheet.css
- tab_toc.htm
- toc.htm
- toc58805109.htm
- toc5880514.htm
- toc58805273.htm
- toc58805276.htm
- toc58805295.htm
- toc58805303.htm
- toc58805308.htm

- toc58805312.htm
- toc58805316.htm
- toc58805319.htm
- toc588055.htm
- toc5880551.htm
- toc588059.htm
- 39585.htm
- 59204.htm
- 59215.htm
- 59218.htm
- 59223.htm
- 59246.htm
- 59249.htm
- 59256.htm
- 59257.htm
- 59258.htm
- 59259.htm
- 59263.htm
- 59264.htm
- 59265.htm
- 59266.htm
- 59267.htm
- 59268.htm
- 59269.htm
- 59409.htm
- 59443.htm
- 59471.htm
- 60210.htm
- 61091.htm
- 61092.htm
- stylesheet.css
- tab_toc.htm
- toc.htm
- toc58805109.htm
- toc5880514.htm
- toc58805272.htm
- toc58805284.htm
- toc58805287.htm
- toc58805291.htm

- toc58805295.htm
- toc58805303.htm
- toc58805308.htm
- toc58805312.htm
- toc58805316.htm
- toc58805319.htm
- toc588055.htm
- toc5880551.htm
- toc588059.htm
- 39585.htm
- 59204.htm
- 59215.htm
- 59218.htm
- 59223.htm
- 59246.htm
- 59249.htm
- 59250.htm
- 59251.htm
- 59252.htm
- 59256.htm
- 59268.htm
- 59269.htm
- 59409.htm
- 59443.htm
- 59471.htm
- 60210.htm
- 60927.htm
- stylesheet.css
- tab_toc.htm
- toc.htm
- toc58805109.htm
- toc5880514.htm
- toc58805272.htm
- toc58805276.htm
- toc58805296.htm
- toc58805303.htm
- toc58805308.htm
- toc58805312.htm
- toc58805316.htm

- toc58805319.htm
- toc588055.htm
- toc5880551.htm
- toc588059.htm
- 39585.htm
- 59204.htm
- 59215.htm
- 59218.htm
- 59223.htm
- 59246.htm
- 59247.htm
- 59248.htm
- 59249.htm
- 59256.htm
- 59268.htm
- 59269.htm
- 59409.htm
- 59443.htm
- 59471.htm
- 60210.htm
- 60421.htm
- stylesheet.css
- tab_toc.htm
- toc.htm
- toc58805109.htm
- toc5880514.htm
- toc58805272.htm
- toc58805276.htm
- toc58805295.htm
- toc58805308.htm
- toc58805312.htm
- toc58805316.htm
- toc58805319.htm
- toc588055.htm
- toc5880551.htm
- toc588059.htm
- 39585.htm
- 59204.htm
- 59215.htm

- 59218.htm
- 59223.htm
- 59224.htm
- 59225.htm
- 59226.htm
- 59246.htm
- 59249.htm
- 59256.htm
- 59268.htm
- 59269.htm
- 59409.htm
- 59443.htm
- 59471.htm
- 60210.htm
- stylesheet.css
- tab_toc.htm
- toc.htm
- toc58805109.htm
- toc5880514.htm
- toc58805272.htm
- toc58805276.htm
- toc58805295.htm
- toc58805303.htm
- toc58805312.htm
- toc58805316.htm
- toc58805319.htm
- toc588055.htm
- toc5880551.htm
- toc588059.htm
- 39585.htm
- 59204.htm
- 59215.htm
- 59218.htm
- 59219.htm
- 59220.htm
- 59221.htm
- 59223.htm
- 59246.htm
- 59249.htm

- 59256.htm
- 59268.htm
- 59269.htm
- 59409.htm
- 59443.htm
- 59471.htm
- 60210.htm
- stylesheet.css
- tab_toc.htm
- toc.htm
- toc58805109.htm
- toc5880514.htm
- toc58805272.htm
- toc58805276.htm
- toc58805295.htm
- toc58805303.htm
- toc58805308.htm
- toc58805316.htm
- toc58805319.htm
- toc588055.htm
- toc5880551.htm
- toc588059.htm
- 39585.htm
- 59204.htm
- 59215.htm
- 59216.htm
- 59217.htm
- 59218.htm
- 59223.htm
- 59246.htm
- 59249.htm
- 59256.htm
- 59268.htm
- 59269.htm
- 59409.htm
- 59443.htm
- 59471.htm
- 60210.htm
- stylesheet.css

- tab_toc.htm
- toc.htm
- toc58805109.htm
- toc5880514.htm
- toc58805272.htm
- toc58805276.htm
- toc58805295.htm
- toc58805303.htm
- toc58805308.htm
- toc58805312.htm
- toc58805319.htm
- toc588055.htm
- toc5880551.htm
- toc588059.htm
- 39585.htm
- 59204.htm
- 59205.htm
- 59208.htm
- 59209.htm
- 59210.htm
- 59211.htm
- 59215.htm
- 59218.htm
- 59223.htm
- 59246.htm
- 59249.htm
- 59256.htm
- 59268.htm
- 59269.htm
- 59409.htm
- 59443.htm
- 59471.htm
- 60210.htm
- stylesheet.css
- tab_toc.htm
- toc.htm
- toc58805109.htm
- toc5880514.htm
- toc58805272.htm

- toc58805276.htm
- toc58805295.htm
- toc58805303.htm
- toc58805308.htm
- toc58805312.htm
- toc58805316.htm
- toc58805320.htm
- toc58805327.htm
- toc588055.htm
- toc5880551.htm
- toc588059.htm
- tab_toc.htm
- tab_toc.htm
- common.js?plesk_version=psa-9.2.2-92090714.19
- frameset.js?plesk_version=psa-9.2.2-92090714.19
- main.js?plesk_version=psa-9.2.2-92090714.19
- tooltip.js?plesk_version=psa-9.2.2-92090714.19
- widget.js?plesk_version=psa-9.2.2-92090714.19
- locales
  - en-US
    - help
      - 39585.htm
      - 39588.htm
      - 47132.htm
      - 58818.htm
      - 58819.htm
      - 58820.htm
      - 58821.htm
      - 58822.htm
      - 58823.htm
      - 59204.htm
      - 59205.htm
      - 59206.htm
      - 59207.htm
      - 59208.htm
      - 59209.htm
      - 59210.htm
      - 59211.htm
      - 59212.htm

- 59214.htm
- 59215.htm
- 59216.htm
- 59217.htm
- 59218.htm
- 59219.htm
- 59220.htm
- 59221.htm
- 59223.htm
- 59224.htm
- 59225.htm
- 59226.htm
- 59246.htm
- 59247.htm
- 59248.htm
- 59249.htm
- 59250.htm
- 59251.htm
- 59252.htm
- 59253.htm
- 59254.htm
- 59255.htm
- 59256.htm
- 59257.htm
- 59258.htm
- 59259.htm
- 59260.htm
- 59261.htm
- 59262.htm
- 59263.htm
- 59264.htm
- 59265.htm
- 59266.htm
- 59267.htm
- 59268.htm
- 59269.htm
- 59270.htm
- 59271.htm
- 59272.htm

- 59273.htm
- 59274.htm
- 59275.htm
- 59276.htm
- 59277.htm
- 59281.htm
- 59282.htm
- 59283.htm
- 59286.htm
- 59287.htm
- 59288.htm
- 59289.htm
- 59290.htm
- 59291.htm
- 59295.htm
- 59297.htm
- 59298.htm
- 59299.htm
- 59300.htm
- 59303.htm
- 59310.htm
- 59311.htm
- 59312.htm
- 59313.htm
- 59314.htm
- 59315.htm
- 59316.htm
- 59317.htm
- 59318.htm
- 59319.htm
- 59321.htm
- 59322.htm
- 59323.htm
- 59324.htm
- 59325.htm
- 59326.htm
- 59327.htm
- 59328.htm
- 59329.htm

- 59330.htm
- 59331.htm
- 59332.htm
- 59333.htm
- 59334.htm
- 59335.htm
- 59336.htm
- 59337.htm
- 59338.htm
- 59342.htm
- 59349.htm
- 59350.htm
- 59351.htm
- 59352.htm
- 59353.htm
- 59355.htm
- 59356.htm
- 59357.htm
- 59358.htm
- 59359.htm
- 59360.htm
- 59361.htm
- 59362.htm
- 59364.htm
- 59365.htm
- 59366.htm
- 59369.htm
- 59371.htm
- 59374.htm
- 59375.htm
- 59376.htm
- 59377.htm
- 59378.htm
- 59402.htm
- 59403.htm
- 59404.htm
- 59405.htm
- 59406.htm
- 59407.htm

- 59408.htm
- 59409.htm
- 59410.htm
- 59411.htm
- 59415.htm
- 59416.htm
- 59417.htm
- 59418.htm
- 59420.htm
- 59421.htm
- 59422.htm
- 59423.htm
- 59424.htm
- 59425.htm
- 59426.htm
- 59427.htm
- 59430.htm
- 59440.htm
- 59443.htm
- 59444.htm
- 59446.htm
- 59447.htm
- 59450.htm
- 59451.htm
- 59452.htm
- 59453.htm
- 59455.htm
- 59457.htm
- 59464.htm
- 59465.htm
- 59466.htm
- 59467.htm
- 59468.htm
- 59469.htm
- 59470.htm
- 59471.htm
- 59472.htm
- 59473.htm
- 59475.htm

- 59476.htm
- 59480.htm
- 59481.htm
- 59482.htm
- 59483.htm
- 60174.htm
- 60175.htm
- 60176.htm
- 60177.htm
- 60178.htm
- 60179.htm
- 60181.htm
- 60182.htm
- 60187.htm
- 60188.htm
- 60189.htm
- 60190.htm
- 60191.htm
- 60192.htm
- 60195.htm
- 60201.htm
- 60202.htm
- 60203.htm
- 60204.htm
- 60205.htm
- 60206.htm
- 60210.htm
- 60279.htm
- 60280.htm
- 60285.htm
- 60286.htm
- 60287.htm
- 60304.htm
- 60305.htm
- 60306.htm
- 60307.htm
- 60317.htm
- 60320.htm
- 60321.htm

- 60322.htm
- 60323.htm
- 60324.htm
- 60326.htm
- 60327.htm
- 60328.htm
- 60329.htm
- 60330.htm
- 60331.htm
- 60421.htm
- 60422.htm
- 60795.htm
- 60927.htm
- 61056.htm
- 61058.htm
- 61059.htm
- 61060.htm
- 61062.htm
- 61063.htm
- 61064.htm
- 61067.htm
- 61068.htm
- 61069.htm
- 61070.htm
- 61071.htm
- 61072.htm
- 61073.htm
- 61074.htm
- 61078.htm
- 61091.htm
- 61092.htm
- 61093.htm
- 61094.htm
- 61095.htm
- 61098.htm
- 61099.htm
- 61865.htm
- 62121.htm
- 62127.htm

- 63016.htm
- 63017.htm
- dhtml_search.js
- highlight.js
- locate.js
- navigation.htm
- prettify.css
- stylesheet.css
- tab_search.htm
- tab_toc.htm
- tab_toc.htm
- title.htm
- toc.htm
- toc.htm
- toc5880510.htm
- toc5880510.htm
- toc58805100.htm
- toc58805104.htm
- toc58805109.htm
- toc58805109.htm
- toc58805110.htm
- toc58805116.htm
- toc58805117.htm
- toc58805120.htm
- toc58805129.htm
- toc58805131.htm
- toc58805133.htm
- toc5880514.htm
- toc58805147.htm
- toc5880515.htm
- toc58805154.htm
- toc58805160.htm
- toc58805164.htm
- toc58805168.htm
- toc58805172.htm
- toc58805175.htm
- toc58805197.htm
- toc5880520.htm
- toc58805201.htm

- toc5880580.htm
- toc588059.htm
- toc588059.htm
- login_up.php3
- skins
  - aqua
    - css
      - general.css
      - main
        - apps-control.css
        - buttons.css
        - custom.css
        - desktop.css
        - double-list-control.css
        - layout.css
        - tabs.css
      - misc.css
      - top
        - custom.css
        - layout.css
- top.php3