

# Vulnerability Report

-BY VEENA TAPALE

## Contents :

1. Executive Summary
2. Scan Results
3. Our Findings
4. Risk Assessment
  - Critical Severity Vulnerability

## 1. Executive Summary

A vulnerability scan detects and classifies system weaknesses in computers, networks and communications equipment and predicts the effectiveness of countermeasures.

Here we gather the data of the website, such as version of the website, cross site scripting etc.

Also to check vulnerabilities on the website.

Website :-

<http://zero.webappsecurity.com/>

## 2. Scan Results

We found vulnerabilities by doing default scan. The total number requests are **20834** out of which **1** was failed request.

## 3. Our Findings

Now the scan is over and we have found the issues with the website and that is almost around 47 issues. Further we will be classifying them.

## 4. Risk Assessment

The 47 issues were found to us and they were of following types

- |                |      |
|----------------|------|
| 1. Critical    | - 4  |
| 2. Important   | - 8  |
| 3. Medium      | - 10 |
| 4. Low         | - 19 |
| 5. Information | - 6  |

---

Total	- 47
-------	------

## Critical Severity Vulnerability

We found 2 critical vulnerabilities on website.

1. Out-of-date Version (Apache)
2. Out-of-date Version (OpenSSL)
3. Out-of-date Version (Tomcat)

### 1. Out-of-date Version (Apache)

**Identified Version :-** 2.2.6

**Latest Version :-** 2.4.48

#### **Impact :-**

Impact of this, is since it is older version, hence it is out of date version.

Therefore, it can be attacked by hackers/attackers i.e. it is vulnerable to attacks. Also, as this is banking website therefore there is chance that it will allow any other attacker to steal our user's passwords and may be sometimes credentials like credit card and debit card details.

#### **Remedy/Solution :-**

We must have to do our software up to date so that it will become more secure than previous version and there will be less possibility of vulnerable attacks.

## **Apache HTTP Server Resource Management Errors Vulnerability :-**

Stack consumption vulnerability in the fnmatch implementation in apr\_fnmatch.c in the Apache Portable Runtime (APR) library before 1.4.3 and the Apache HTTP Server before 2.2.18, and in fnmatch.c in libc in NetBSD 5.1, OpenBSD 4.8, FreeBSD, Apple Mac OS X 10.6, Oracle Solaris 10, and Android, allows context- dependent attackers to cause a denial of service (CPU and memory consumption) via \*? sequences in the first argument, as demonstrated by attacks against mod\_autoindex in httpd.

## **Apache HTTP Server Insufficient Information Vulnerability :-**

modules/arch/win32/mod\_isapi.c in mod\_isapi in the Apache HTTP Server 2.0.37 through 2.0.63, 2.2.0 through 2.2.14, and 2.3.x before 2.3.7, when running on Windows, does not ensure that request processing is complete before calling isapi\_unload for an ISAPI .dll module, which allows remote attackers to execute arbitrary code via unspecified vectors related to a crafted request, a reset packet, and "orphaned callback pointers."

## **Apache HTTP Server Other Vulnerability :-**

The ap\_proxy\_ajp\_request function in mod\_proxy\_ajp.c in mod\_proxy\_ajp in the Apache HTTP Server 2.2.x before 2.2.15 does not properly handle certain situations in which a client sends no request body, which allows remote attackers to cause a denial of service (backend server outage) via a crafted request, related to use of a 500 error code instead of the appropriate 400 error code.

## **Apache HTTP Server Resource Management Errors Vulnerability**

**:-**

The mod\_proxy\_ajp module in the Apache HTTP Server before 2.2.21, when used with mod\_proxy\_balancer in certain configurations, allows remote attackers to cause a denial of service (temporary "error state" in the backend server) via a malformed HTTP request.

**Apache HTTP Server Improper Input Validation Vulnerability :-** The mod\_proxy module in the Apache HTTP Server 1.3.x through 1.3.42, 2.0.x through 2.0.64, and 2.2.x through 2.2.21 does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers via a malformed URI containing an initial @ (at sign) character.

## **Apache HTTP Server Resource Management Errors Vulnerability**

**:-**

The mod\_proxy\_ajp module in the Apache HTTP Server before 2.2.21, when used with mod\_proxy\_balancer in certain configurations, allows remote attackers to cause a denial of service (temporary "error state" in the backend server) via a malformed HTTP request.

## **Apache HTTP Server Resource Management Errors Vulnerability**

**:-**

The byterange filter in the Apache HTTP Server 1.3.x, 2.0.x through 2.0.64, and 2.2.x through 2.2.19 allows remote attackers to cause a denial of service (memory and CPU consumption) via a Range header that expresses multiple overlapping ranges, as exploited in the wild in August 2011, a different vulnerability than [CVE-2007-0086](#).

## **Apache HTTP Server Resource Management Errors Vulnerability**

**:-**

The mod\_deflate module in Apache httpd 2.2.11 and earlier compresses large files until completion even after the associated network connection is closed, which allows remote attackers to cause a denial of service (CPU consumption).

## **Apache HTTP Server Resource Management Errors Vulnerability**

**:-**

The mod\_deflate module in Apache httpd 2.2.11 and earlier compresses large files until completion even after the associated network connection is closed, which allows remote attackers to cause a denial of service (CPU consumption).

## **Apache HTTP Server Numeric Errors Vulnerability :-**

The `stream_reqbody_cl` function in `mod_proxy_http.c` in the `mod_proxy` module in the Apache HTTP Server before 2.3.3, when a reverse proxy is configured, does not properly handle an amount of streamed data that exceeds the Content-Length value, which allows remote attackers to cause a denial of service (CPU consumption) via crafted requests.

## **Apache HTTP Server Configuration Vulnerability :-**

The Apache HTTP Server 2.2.11 and earlier 2.2 versions does not properly handle `Options=IncludesNOEXEC` in the `AllowOverride` directive, which allows local users to gain privileges by configuring (1) `Options Includes`, (2) `Options +Includes`, or (3) `Options +IncludesNOEXEC` in a `.htaccess` file, and then inserting an `exec` element in a `.shtml` file.

## **Apache HTTP Server Numeric Errors Vulnerability :-**

The `stream_reqbody_cl` function in `mod_proxy_http.c` in the `mod_proxy` module in the Apache HTTP Server before 2.3.3, when a reverse proxy is configured, does not properly handle an amount of streamed data that exceeds the Content-Length value, which allows remote attackers to cause a denial of service (CPU consumption) via crafted requests.



## **Apache HTTP Server Other Vulnerability :-**

The Solaris pollset feature in the Event Port backend in poll/unix/port.c in the Apache Portable Runtime (APR) library before 1.3.9, as used in the Apache HTTP Server before 2.2.14 and other products, does not properly handle errors, which allows remote attackers to cause a denial of service (daemon hang) via unspecified HTTP requests, related to the prefork and event MPMs.

## **Apache HTTP Server Cryptographic Issues Vulnerability :-**

The TLS protocol, and the SSL protocol 3.0 and possibly earlier, as used in Microsoft Internet Information Services (IIS) 7.0, mod\_ssl in the Apache HTTP Server 2.2.14 and earlier, OpenSSL before 0.9.8l, GnuTLS 2.8.5 and earlier, Mozilla Network Security Services (NSS) 3.12.4 and earlier, multiple Cisco products, and other products, does not properly associate renegotiation handshakes with an existing connection, which allows man-in-the-middle attackers to insert data into HTTPS sessions, and possibly other types of sessions protected by TLS or SSL, by sending an unauthenticated request that is processed retroactively by a server in a post-renegotiation context, related to a "plaintext injection" attack, aka the "Project Mogul" issue.

## **Apache HTTP Server Other Vulnerability :-**

The mod\_proxy\_ftp module in the Apache HTTP Server allows remote attackers to bypass intended access restrictions and send arbitrary commands to an FTP server via vectors related to the embedding of these commands in the Authorization HTTP header, as demonstrated by a certain module in VulnDisco Pack Professional 8.11.

## **Apache HTTP Server Other Vulnerability :-**

The Solaris pollset feature in the Event Port backend in poll/unix/port.c in the Apache Portable Runtime (APR) library before 1.3.9, as used in the Apache HTTP Server before 2.2.14 and other products, does not properly handle errors, which allows remote attackers to cause a denial of service (daemon hang) via unspecified HTTP requests, related to the prefork and event MPMs.

## **Apache HTTP Server Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability :-**

Multiple cross-site scripting (XSS) vulnerabilities in the balancer\_handler function in the manager interface in mod\_proxy\_balancer.c in the mod\_proxy\_balancer module in the Apache HTTP Server 2.2.x before 2.2.24-dev and 2.4.x before 2.4.4 allow remote attackers to inject arbitrary web script or HTML via a crafted string.

## **Apache HTTP Server Cryptographic Issues Vulnerability :-**

mod\_rewrite.c in the mod\_rewrite module in the Apache HTTP Server 2.2.x before 2.2.25 writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to execute arbitrary commands via an HTTP request containing an escape sequence for a terminal emulator.

## **Apache HTTP Server Permissions, Privileges, and Access Controls Vulnerability :-**

mod\_dav.c in the Apache HTTP Server before 2.2.25 does not properly determine whether DAV is enabled for a URI, which allows remote attackers to cause a denial of service (segmentation fault) via a MERGE request in which the URI is configured for handling by the mod\_dav\_svn module, but a certain href attribute in XML data refers to a non-DAV URI.

## **Apache HTTP Server Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability :-**

Multiple cross-site scripting (XSS) vulnerabilities in the Apache HTTP Server 2.2.x before 2.2.24-dev and 2.4.x before 2.4.4 allow remote attackers to inject arbitrary web script or HTML via vectors involving hostnames and URIs in the (1) mod\_imagemap, (2) mod\_info, (3) mod\_ldap, (4) mod\_proxy\_ftp, and (5) mod\_status modules.

## **Apache HTTP Server Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability :-**

Multiple cross-site scripting (XSS) vulnerabilities in the `make_variant_list` function in `mod_negotiation.c` in the `mod_negotiation` module in the Apache HTTP Server

2.4.x before 2.4.3, when the MultiViews option is enabled, allow remote attackers to inject arbitrary web script or HTML via a crafted filename that is not properly handled during construction of a variant list.

## **Apache HTTP Server Permissions, Privileges, and Access Controls Vulnerability :-**

`envvars` (aka `envvars-std`) in the Apache HTTP Server before 2.4.2 places a zero-length directory name in the `LD_LIBRARY_PATH`, which allows local users to gain privileges via a Trojan horse DSO in the current working directory during execution of `apachectl`.

## **Apache HTTP Server Permissions, Privileges, and Access Controls Vulnerability :-**

`mod_dav.c` in the Apache HTTP Server before 2.2.25 does not properly determine whether DAV is enabled for a URI, which allows remote attackers to cause a denial of service (segmentation fault) via a MERGE request in which the URI is configured for handling by the `mod_dav_svn` module, but a certain href attribute in XML data refers to a non-DAV URI.

**Apache HTTP Server Improper Input Validation Vulnerability :-** The `dav_xml_get_cdata` function in `main/util.c` in the `mod_dav` module in the Apache HTTP Server before 2.4.8 does not properly remove whitespace characters from CDATA sections, which allows remote attackers to cause a denial of service (daemon crash) via a crafted DAV WRITE request.

**Apache HTTP Server Improper Input Validation Vulnerability :-** The `dav_xml_get_cdata` function in `main/util.c` in the `mod_dav` module in the Apache HTTP Server before 2.4.8 does not properly remove whitespace characters from CDATA sections, which allows remote attackers to cause a denial of service (daemon crash) via a crafted DAV WRITE request.

**Apache HTTP Server Insufficient Information Vulnerability :-** `mod_session_dbd.c` in the `mod_session_dbd` module in the Apache HTTP Server before 2.4.5 proceeds with save operations for a session without considering the dirty flag and the requirement for a new session ID, which has unspecified impact and remote attack vectors.

**Apache HTTP Server Insufficient Information Vulnerability :-** `mod_session_dbd.c` in the `mod_session_dbd` module in the Apache HTTP Server before 2.4.5 proceeds with save operations for a session without considering the dirty flag and the requirement for a new session ID, which has unspecified impact and remote attack vectors.

**Apache HTTP Server Improper Input Validation Vulnerability :-** The mod\_proxy module in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x before 2.2.18, when the Revision 1179239 patch is in place, does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers by using the HTTP/0.9 protocol with a malformed URI containing an initial @ (at sign) character. NOTE: this vulnerability exists because of an incomplete fix for [CVE-2011-3368](#).

**Apache HTTP Server Improper Input Validation Vulnerability :-** The mod\_proxy module in the Apache HTTP Server 1.3.x through 1.3.42, 2.0.x through 2.0.64, and 2.2.x through 2.2.21, when the Revision 1179239 patch is in place, does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers via a malformed URI containing an @ (at sign) character and a : (colon) character in invalid positions. NOTE: this vulnerability exists because of an incomplete fix for [CVE-2011-3368](#).

### **Apache HTTP Server Numeric Errors Vulnerability :-**

Integer overflow in the ap\_pregsub function in server/util.c in the Apache HTTPServer 2.0.x through 2.0.64 and 2.2.x through 2.2.21, when the mod\_setenvif module is enabled, allows local users to gain privileges via a .htaccess file with a crafted SetEnvIf directive, in conjunction with a crafted HTTP request header, leading to a heap-based buffer overflow.

## **Apache HTTP Server Improper Input Validation Vulnerability :-**

The `ap_pregsub` function in `server/util.c` in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x through 2.2.21, when the `mod_setenvif` module is enabled, does not restrict the size of values of environment variables, which allows local users to cause a denial of service (memory consumption or NULL pointer dereference) via a `.htaccess` file with a crafted `SetEnvIf` directive, in conjunction with a crafted `HTTPrequest` header, related to (1) the `"len += "` statement and (2) the `apr_pcalloc` function call, a different vulnerability than [CVE-2011-3607](#).

## **Apache HTTP Server Resource Management Errors Vulnerability**

**:-**

The Apache HTTP Server 1.x and 2.x allows remote attackers to cause a denial of service (daemon outage) via partial HTTP requests, as demonstrated by Slowloris, related to the lack of the `mod_reqtimeout` module in versions before 2.2.15.

## **Apache HTTP Server Permissions, Privileges, and Access Controls Vulnerability :-**

`protocol.c` in the Apache HTTP Server 2.2.x through 2.2.21 does not properly restrict header information during construction of Bad Request (aka 400) error documents, which allows remote attackers to obtain the values of HTTPOnly cookies via vectors involving a (1) long or (2) malformed header in conjunction with crafted web script.

## **Apache HTTP Server Permissions, Privileges, and Access Controls Vulnerability :-**

envvars (aka envvars-std) in the Apache HTTP Server before 2.4.2 places a zero-length directory name in the LD\_LIBRARY\_PATH, which allows local users to gain privileges via a Trojan horse DSO in the current working directory during execution of apachectl.

## **Apache HTTP Server Resource Management Errors Vulnerability**

**:-**

scoreboard.c in the Apache HTTP Server 2.2.21 and earlier might allow local users to cause a denial of service (daemon crash during shutdown) or possibly have unspecified other impact by modifying a certain type field within a scoreboard shared memory segment, leading to an invalid call to the free function.

## **Apache HTTP Server Resource Management Errors Vulnerability**

**:-**

The Apache HTTP Server 1.x and 2.x allows remote attackers to cause a denial of service (daemon outage) via partial HTTP requests, as demonstrated by Slowloris, related to the lack of the mod\_reqtimeout module in versions before 2.2.15.



## **Apache HTTP Server Resource Management Errors Vulnerability**

**:-**

scoreboard.c in the Apache HTTP Server 2.2.21 and earlier might allow local users to cause a denial of service (daemon crash during shutdown) or possibly have unspecified other impact by modifying a certain type field within a scoreboard shared memory segment, leading to an invalid call to the free function.

## **Apache HTTP Server Configuration Vulnerability :-**

The Apache HTTP Server 2.2.11 and earlier 2.2 versions does not properly handle Options=IncludesNOEXEC in the AllowOverride directive, which allows local users to gain privileges by configuring (1) Options Includes, (2) Options +Includes, or (3) Options +IncludesNOEXEC in a .htaccess file, and then inserting an exec element in a .shtml file.

## **Apache HTTP Server Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability :-**

Cross-site scripting (XSS) vulnerability in mod\_status in the Apache HTTP Server 2.2.0 through 2.2.6, 2.0.35 through 2.0.61, and 1.3.2 through 1.3.39, when the server-status page is enabled, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

## **Apache HTTP Server Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability :-**

Cross-site scripting (XSS) vulnerability in balancer-manager in mod\_proxy\_balancer in the Apache HTTP Server 2.2.0 through 2.2.6 allows remote attackers to inject arbitrary web script or HTML via the (1) ss, (2) wr, or (3) rr parameters, or (4) the URL.

## **Apache HTTP Server Resource Management Errors Vulnerability**

**:-**

Unspecified vulnerability in mod\_proxy\_balancer for Apache HTTP Server 2.2.x before 2.2.7-dev, when running on Windows, allows remote attackers to trigger memory corruption via a long URL. NOTE: the vendor could not reproduce this issue.

## **Apache HTTP Server Cross-Site Request Forgery (CSRF) Vulnerability :-**

Cross-site request forgery (CSRF) vulnerability in the balancer-manager in mod\_proxy\_balancer for Apache HTTP Server 2.2.x allows remote attackers to gain privileges via unspecified vectors.

## **Apache HTTP Server Improper Control of Generation of Code('Code Injection') Vulnerability :-**

CRLF injection vulnerability in the mod\_negotiation module in the Apache HTTP Server 2.2.6 and earlier in the 2.2.x series, 2.0.61 and earlier in the 2.0.x series, and 1.3.39 and earlier in the 1.3.x series allows remote authenticated users to inject arbitrary HTTP headers and conduct HTTP response splitting attacks by uploading a file with a multi-line name containing HTTP header sequences and a file extension, which leads to injection within a (1) "406 Not Acceptable" or (2) "300 Multiple Choices" HTTP response when the extension is omitted in a request for the file.

## **Apache HTTP Server Exposure of Sensitive Information to an Unauthorized Actor Vulnerability :-**

Apache HTTP Server, when running on Linux with a document root on a Windows share mounted using smbfs, allows remote attackers to obtain unprocessed content such as source files for .php programs via a trailing "\" (backslash), which is not handled by the intended AddType directive.

## **Apache HTTP Server Resource Management Errors Vulnerability :-**

The balancer\_handler function in mod\_proxy\_balancer in the Apache HTTP Server 2.2.0 through 2.2.6, when a threaded Multi-Processing Module is used, allows remote authenticated users to cause a denial of service (child process crash) via an invalid bb variable.

## **Apache HTTP Server Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability :-**

Cross-site scripting (XSS) vulnerability in the (1) mod\_imap module in the Apache HTTP Server 1.3.0 through 1.3.39 and 2.0.35 through 2.0.61 and the (2) mod\_imagemap module in the Apache HTTP Server 2.2.0 through 2.2.6 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

## **Apache HTTP Server Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability :-**

Cross-site scripting (XSS) vulnerability in proxy\_ftp.c in the mod\_proxy\_ftp module in Apache 2.0.63 and earlier, and mod\_proxy\_ftp.c in the mod\_proxy\_ftp module in Apache 2.2.9 and earlier 2.2 versions, allows remote attackers to inject arbitrary web script or HTML via a wildcard in the last directory component in the pathname in an FTP URI.

## **Apache HTTP Server Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability :-**

Cross-site scripting (XSS) vulnerability in the mod\_negotiation module in the Apache HTTP Server 2.2.6 and earlier in the 2.2.x series, 2.0.61 and earlier in the 2.0.x series, and 1.3.39 and earlier in the 1.3.x series allows remote authenticated users to inject arbitrary web script or HTML by uploading a file with a name containing XSS sequences and a file extension, which leads to injection within a (1) "406 Not Acceptable" or (2) "300 Multiple Choices" HTTP response when the extension is omitted in a request for the file.

## **Apache HTTP Server DEPRECATED: Code Vulnerability :-**

The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in `modules/http/http_filters.c`.

**Apache HTTP Server Improper Input Validation Vulnerability :-** The `lua_websocket_read` function in `lua_request.c` in the `mod_lua` module in the Apache HTTP Server through 2.4.12 allows remote attackers to cause a denial of service (child-process crash) by sending a crafted WebSocket Ping frame after a Lua script has called the `wsupgrade` function.

## **Apache HTTP Server Resource Management Errors Vulnerability**

**:-**

The `deflate_in_filter` function in `mod_deflate.c` in the `mod_deflate` module in the Apache HTTP Server before 2.4.10, when request body decompression is enabled, allows remote attackers to cause a denial of service (resource consumption) via crafted request data that decompresses to a much larger size.

**Apache HTTP Server Improper Input Validation Vulnerability :-** The `log_cookie` function in `mod_log_config.c` in the `mod_log_config` module in the Apache HTTP Server before 2.4.8 allows remote attackers to cause a denial of service (segmentation fault and daemon crash) via a crafted cookie that is not properly handled during truncation.

**Apache HTTP Server Improper Input Validation Vulnerability :-** The log\_cookie function in mod\_log\_config.c in the mod\_log\_config module in the Apache HTTP Server before 2.4.8 allows remote attackers to cause a denial of service (segmentation fault and daemon crash) via a crafted cookie that is not properly handled during truncation.

## **Apache HTTP Server Resource Management Errors Vulnerability**

**:-**

The mod\_cgid module in the Apache HTTP Server before 2.4.10 does not have a timeout mechanism, which allows remote attackers to cause a denial of service (process hang) via a request to a CGI script that does not read from its stdin file descriptor.

## **Apache HTTP Server Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') Vulnerability :-**

Race condition in the mod\_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status\_handler function in modules/generators/mod\_status.c and the lua\_ap\_scoreboard\_worker function in modules/lua/lua\_request.c.

## **Apache HTTP Server Resource Management Errors Vulnerability**

**:-**

The mod\_cgid module in the Apache HTTP Server before 2.4.10 does not have a timeout mechanism, which allows remote attackers to cause a denial of service (process hang) via a request to a CGI script that does not read from its stdin file descriptor.

## **Apache HTTP Server Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability :-**

In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod\_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.

## **Apache HTTP Server Improper Input Validation Vulnerability :-**

In Apache httpd before 2.2.34 and 2.4.x before 2.4.27, the value placeholder in [Proxy-]Authorization headers of type 'Digest' was not initialized or reset before or between successive key=value assignments by mod\_auth\_digest. Providing an initial key with no '=' assignment could reflect the stale value of uninitialized pool memory used by the prior request, leading to leakage of potentially confidential information, and a segfault in other cases resulting in denial of service.

## **Apache HTTP Server Improper Access Control Vulnerability :-**

The Apache HTTP Server through 2.4.23 follows RFC 3875 section 4.1.18 and therefore does not protect applications from the presence of untrusted client data in the HTTP\_PROXY environment variable, which might allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted Proxy header in an HTTP request, aka an "httpoxy" issue. NOTE: the vendor states "This mitigation has been assigned the identifier CVE-2016-5387"; in other words, this is not a CVE ID for a vulnerability.

**Apache HTTP Server Improper Authentication Vulnerability :-** In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent replay attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.



## **Apache HTTP Server Out-of-bounds Read Vulnerability :-**

A specially crafted HTTP request header could have crashed the Apache HTTP Server prior to version 2.4.30 due to an out of bound read while preparing data to be cached in shared memory. It could be used as a Denial of Service attack against users of mod\_cache\_socache. The vulnerability is considered as low risk since mod\_cache\_socache is not widely used, mod\_cache\_disk is not concerned by this vulnerability.

## **Apache HTTP Server Improper Neutralization of CRLF Sequences ('CRLF Injection') Vulnerability :-**

Possible CRLF injection allowing HTTP response splitting attacks for sites which use mod\_userdir. This issue was mitigated by changes made in 2.4.25 and 2.2.32 which prohibit CR or LF injection into the "Location" or other outbound header key or value. Fixed in Apache HTTP Server 2.4.25 (Affected 2.4.1-2.4.23). Fixed in Apache HTTP Server 2.2.32 (Affected 2.2.0-2.2.31).

## **Apache HTTP Server Uncontrolled Resource Consumption Vulnerability :-**

In Apache HTTP server versions 2.4.37 and prior, by sending request bodies in a slow loris way to plain resources, the h2 stream for that request unnecessarily occupied a server thread cleaning up that incoming data. This affects only HTTP/2(mod\_http2) connections.

## **Apache HTTP Server Improper Input Validation Vulnerability :-**

Apache HTTP Server mod\_cluster before version httpd 2.4.23 is vulnerable to an Improper Input Validation in the protocol parsing logic in the load balancer resulting in a Segmentation Fault in the serving httpd process.

## **Apache HTTP Server Use After Free Vulnerability :-**

Apache httpd allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed. This affects the Apache HTTP Server through 2.2.34 and 2.4.x through 2.4.27. The attacker sends an unauthenticated OPTIONSHTTP request when attempting to read secret data. This is a use-after-free issue and thus secret data is not always sent, and the specific data depends on many factors including configuration. Exploitation with .htaccess can be blocked with apatch to the ap\_limit\_section function in server/core.c.

## **Apache HTTP Server NULL Pointer Dereference Vulnerability :-**

When an HTTP/2 stream was destroyed after being handled, the Apache HTTP Server prior to version 2.4.30 could have written a NULL pointer potentially to already freed memory. The memory pools maintained by the server make this vulnerability hard to trigger in usual configurations, the reporter and the team could not reproduce it outside debug builds, so it is classified as low risk.

## **Apache HTTP Server Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability :-**

A specially crafted request could have crashed the Apache HTTP Server prior to version 2.4.30, due to an out of bound access after a size limit is reached by reading the HTTP header. This vulnerability is considered very hard if not impossible to trigger in non-debug mode (both log and build level), so it is classified as low risk for common server usage.