© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 08 Issue: 02 | January - March 2017
Paper is available at www.jrps.in | Email : info@jrps.in

ENHANCEMENT OF HTTP SERVER SECURITY TO PREVENT ATTACKS ON COMMERCIAL

[1]Sunil , Research Scholar,Department of CSE, Indus Instt. of Engg. & Tech, jind.
[2]Abhishek bhatnagar, A.P., Department of CSE, Indus Instt. of Engg. & Tech, jind

ABSTRACT: HTTP is an application layer protocol designed within framework of Internet Protocol Suite. Its definition presumes an underlying & reliable transport layer protocol,[2] & Transmission Control Protocol is commonly used. However HTTP could be adapted to use unreliable protocols such as User Datagram Protocol, for example within HTTPU & Simple Service Discovery Protocol. There are several threat to HTTP server security. Categories of attack could consist of passive monitoring of data communications exploitation by insiders, close-in attacks, harmful attacks through service provider & active network attacks. Information systems & networks usually offer targets & must be resistant with within order to attack from full range of threat agents, from hackers to nation-states. System must be capable to restrict damage & recovery from occurrence of attacks. The objective of research is to secure HTTP server from external attacks.

ISSN : 2278-6848
03
9 772278 684800
© International Journal for Research Publication and Seminar

[1] Introduction

The **Hypertext Transfer Protocol** (**HTTP**) is an application protocol for distributed, collaborative, hypermedia information systems.[1] HTTP is foundation of data communication for World Wide Web. Hypertext is structured text that uses logical links (hyperlinks) between nodes containing text. HTTP is protocol to exchange or transfer hypertext. Development of HTTP was initiated by Tim Berners-Lee at CERN within 1989. Standards development of HTTP was coordinated by Internet Engineering Task Force (IETF) & World Wide Web Consortium (W3C), culminating within publication of a series of Requests for Comments (RFCs). The first definition of HTTP/1.1, version of HTTP within common use, occurred within RFC 2068 within 1997, although this was obsoleted by RFC 2616 within 1999.

A later version, successor HTTP/2, was standardized within 2015, then supported by major web browsers & already supported by major web servers. HTTP functions as a request–response protocol within client–server computing model. A web browser, for example, may be *client* & an application running on a computer hosting a web site may be *server*. The client submits an HTTP *request* message to server. The server, which provides *resources* such as HTML files & other content, or performs other functions on behalf of client, returns a *response* message to client. The response contains completion status information about request & may also contain requested content within its message body. Web browser is an example of a *user agent*. Other types of user agent consists of indexing software used by search providers voice browsers, mobile apps, & other software that accesses, consumes, or displays web content.HTTP is designed to permit intermediate network elements to improve or enable communications between clients & servers. High-traffic websites often benefit from web cache servers that deliver content on behalf of upstream servers to improve response time. Fielding, Roy T.; Reschke, Julian F. (June 2014). Hypertext Transfer Protocol (HTTP/1.1):