Asset IP Address	Vulnerability Title	Vulnerability CVSS Score	nerability Severity L	Severity
10.20.20.18	TCP timestamp response	0	1	LOW
10.20.20.18	SSH Weak Message Authentication Code Algorithms	4	4	MEDIUM
10.20.20.18	HTTP OPTIONS Method Enabled	2.6	3	LOW
10.20.20.18	Apache HTTPD: DoS for HTTP/2 connections by continuous SETTINGS (CVE-2018-11763)	4.3	4	MEDIUM
10.20.20.18	Apache HTTPD: Limited cross-site scripting in mod_proxy error page (CVE-2019-10092)	4.3	4	MEDIUM
10.20.20.18	Apache HTTPD: Possible out of bound access after failure in reading the HTTP request (CVE-2018-1301)	4.3	4	MEDIUM
10.20.20.18	Apache HTTPD: Possible write of after free on HTTP/2 stream shutdown (CVE-2018-1302)	4.3	4	MEDIUM
10.20.20.18	Apache HTTPD: Push Diary Crash on Specifically Crafted HTTP/2 Header (CVE-2020-11993)	4.3	4	MEDIUM
10.20.20.18	Apache HTTPD: Tampering of mod_session data for CGI applications (CVE-2018-1283)	3.5	4	MEDIUM
10.20.20.18	Click Jacking	4.3	4	MEDIUM
10.20.20.18	Apache HTTPD: Apache httpd URL normalization inconsistincy (CVE-2019-0220)	5	5	MEDIUM
10.20.20.18	Apache HTTPD: Denial of service in mod_lua r:parsebody (CVE-2022-29404)	5	5	MEDIUM
10.20.20.18	Apache HTTPD: DoS for HTTP/2 connections by crafted requests (CVE-2018-1333)	5	5	MEDIUM
10.20.20.18	Apache HTTPD: DoS for HTTP/2 connections via slow request bodies (CVE-2018-17189)	5	5	MEDIUM
10.20.20.18	Apache HTTPD: Information Disclosure in mod_lua with websockets (CVE-2022-30556)	5	5	MEDIUM
10.20.20.18	Apache HTTPD: NULL pointer dereference in httpd core (CVE-2021-34798)	5	5	MEDIUM
10.20.20.18	Apache HTTPD: Out of bound write in mod_authnz_ldap when using too small Accept-Language values (CVE-2017-15710)	5	5	MEDIUM
10.20.20.18	Apache HTTPD: Possible out of bound read in mod_cache_socache (CVE-2018-1303)	5	5	MEDIUM
10.20.20.18	Apache HTTPD: Push Diary Crash on Specifically Crafted HTTP/2 Header (CVE-2020-9490)	5	5	MEDIUM
10.20.20.18	Apache HTTPD: Request splitting via HTTP/2 method injection and mod_proxy (CVE-2021-33193)	5	5	MEDIUM
10.20.20.18	Apache HTTPD: mod_http2, memory corruption on early pushes (CVE-2019-10081)	5	5	MEDIUM
10.20.20.18	Apache HTTPD: mod_http2, read-after-free on a string compare (CVE-2019-0196)	5	5	MEDIUM
10.20.20.18	Apache HTTPD: mod_lua Use of uninitialized value of in r:parsebody (CVE-2022-22719)	5	5	MEDIUM
10.20.20.18	Apache HTTPD: mod_proxy_ajp: Possible request smuggling (CVE-2022-26377)	5	5	MEDIUM
10.20.20.18	Apache HTTPD: mod_proxy_ftp use of uninitialized value (CVE-2020-1934)	5	5	MEDIUM
10.20.20.18	Apache HTTPD: mod_proxy_wstunnel tunneling of non Upgraded connections (CVE-2019-17567)	5	5	MEDIUM
10.20.20.18	Apache HTTPD: mod_session NULL pointer dereference (CVE-2021-26690)	5	5	MEDIUM
10.20.20.18	Apache HTTPD: mod_session_cookie does not respect expiry time (CVE-2018-17199)	5	5	MEDIUM
10.20.20.18	Apache HTTPD: read beyond bounds in mod_isapi (CVE-2022-28330)	5	5	MEDIUM
10.20.20.18	Apache HTTPD: read beyond bounds via ap_rwrite() (CVE-2022-28614)	5	5	MEDIUM
10.20.20.18	Apache HTTPD: Possible NULL dereference or SSRF in forward proxy configurations in Apache HTTP Server 2.4.51 and earlier (CVE-2021-44224)	6.4	6	MEDIUM
10.20.20.18	Apache HTTPD: Read beyond bounds in ap_strcmp_match() (CVE-2022-28615)	6.4	6	MEDIUM
10.20.20.18	Apache HTTPD: core: Possible buffer overflow with very large or unlimited LimitXMLRequestBody (CVE-2022-22721)	5.8	6	MEDIUM
10.20.20.18	Apache HTTPD: mod_auth_digest access control bypass (CVE-2019-0217)	6	6	MEDIUM
10.20.20.18	Apache HTTPD: mod_http2, read-after-free in h2 connection shutdown (CVE-2019-10082)	6.4	6	MEDIUM
10.20.20.18	Apache HTTPD: mod_rewrite CWE-601 open redirect (CVE-2020-1927)	5.8	6	MEDIUM
10.20.20.18	Apache HTTPD: mod_rewrite potential open redirect (CVE-2019-10098)	5.8	6	MEDIUM
10.20.20.18	Apache HTTPD: <FilesMatch> bypass with a trailing newline in the file name (CVE-2017-15715)	6.8	7	HIGH
10.20.20.18	Apache HTTPD: Apache HTTP Server privilege escalation from modules' scripts (CVE-2019-0211)	7.2	7	HIGH
10.20.20.18	Apache HTTPD: Weak Digest auth nonce generation in mod_auth_digest (CVE-2018-1312)	6.8	7	HIGH
10.20.20.18	Apache HTTPD: mod_auth_digest possible stack overflow by one nul byte (CVE-2020-35452)	6.8	7	HIGH
10.20.20.18	Apache HTTPD: mod_proxy SSRF (CVE-2021-40438)	6.8	7	HIGH
10.20.20.18	Apache HTTPD: HTTP request smuggling vulnerability in Apache HTTP Server 2.4.52 and earlier (CVE-2022-22720)	7.5	8	HIGH
10.20.20.18	Apache HTTPD: Possible buffer overflow when parsing multipart content in mod_lua of Apache HTTP Server 2.4.51 and earlier (CVE-2021-44790)	7.5	8	HIGH
10.20.20.18	Apache HTTPD: ap_escape_quotes buffer overflow (CVE-2021-39275)	7.5	8	HIGH
10.20.20.18	Apache HTTPD: mod_http2, DoS attack by exhausting h2 workers. (CVE-2019-9517)	7.8	8	HIGH
10.20.20.18	Apache HTTPD: mod_proxy X-Forwarded-For dropped by hop-by-hop mechanism (CVE-2022-31813)	7.5	8	HIGH
10.20.20.18	Apache HTTPD: mod_sed: Read/write beyond bounds (CVE-2022-23943)	7.5	8	HIGH
10.20.20.18	Apache HTTPD: mod_session response handling heap overflow (CVE-2021-26691)	7.5	8	