|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **#** | **CVE ID** | **CWE ID** | **# of Exploits** | **Vulnerability Type(s)** | **Publish Date** | **Update Date** | **Score** | **Gained Access Level** | **Access** | **Complexity** | **Authentication** | **Conf.** | **Integ.** | **Avail.** |
| 1 | [CVE-2011-4317](https://www.cvedetails.com/cve/CVE-2011-4317/) | [20](https://www.cvedetails.com/cwe-details/20/cwe.html) |  |  | 2011-11-30 | 2021-06-06 | **4.3** | None | Remote | Medium | Not required | None | Partial | None |
| 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. | | | | | | | | | | | | | | |
| 2 | [CVE-2011-3368](https://www.cvedetails.com/cve/CVE-2011-3368/) | [20](https://www.cvedetails.com/cwe-details/20/cwe.html) | **1** |  | 2011-10-05 | 2021-06-06 | **5.0** | None | Remote | Low | Not required | Partial | None | None |  |  |  |  |  |
| 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. | | | | | | | | | | | | | | |
| 3 | [CVE-2010-0010](https://www.cvedetails.com/cve/CVE-2010-0010/) | [189](https://www.cvedetails.com/cwe-details/189/cwe.html) | **1** | DoS Exec Code Overflow | 2010-02-02 | 2021-06-06 | **6.8** | None | Remote | Medium | Not required | Partial | Partial | Partial |  |  |  |  |  |
| Integer overflow in the ap\_proxy\_send\_fb function in proxy/proxy\_util.c in mod\_proxy in the Apache HTTP Server before 1.3.42 on 64-bit platforms allows remote origin servers to cause a denial of service (daemon crash) or possibly execute arbitrary code via a large chunk size that triggers a heap-based buffer overflow. | | | | | | | | | | | | | | |
| 4 | [CVE-2007-6750](https://www.cvedetails.com/cve/CVE-2007-6750/) | [399](https://www.cvedetails.com/cwe-details/399/cwe.html) |  | DoS | 2011-12-27 | 2018-01-10 | **5.0** | None | Remote | Low | Not required | None | None | Partial |  |  |  |  |  |
| 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. | | | | | | | | | | | | | | |
| 5 | [CVE-2007-6388](https://www.cvedetails.com/cve/CVE-2007-6388/) | [79](https://www.cvedetails.com/cwe-details/79/cwe.html) |  | XSS | 2008-01-08 | 2021-06-06 | **4.3** | None | Remote | Medium | Not required | None | Partial | None |  |  |  |  |  |
| 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. | | | | | | | | | | | | | | |
| 6 | [CVE-2005-3352](https://www.cvedetails.com/cve/CVE-2005-3352/) |  |  | XSS | 2005-12-13 | 2021-06-06 | **4.3** | None | Remote | Medium | Not required | None | Partial | None |  |  |  |  |  |
| Cross-site scripting (XSS) vulnerability in the mod\_imap module of Apache httpd before 1.3.35-dev and Apache httpd 2.0.x before 2.0.56-dev allows remote attackers to inject arbitrary web script or HTML via the Referer when using image maps. | | | | | | | | | | | | | | |
| 7 | [CVE-2004-1082](https://www.cvedetails.com/cve/CVE-2004-1082/) |  |  |  | 2004-02-03 | 2018-10-30 | **7.5** | None | Remote | Low | Not required | Partial | Partial | Partial |  |  |  |  |  |
| mod\_digest\_apple for Apache 1.3.31 and 1.3.32 on Mac OS X Server does not properly verify the nonce of a client response, which allows remote attackers to replay credentials. | | | | | | | | | | | | | | |
| 8 | [CVE-2004-0940](https://www.cvedetails.com/cve/CVE-2004-0940/) | [119](https://www.cvedetails.com/cwe-details/119/cwe.html) |  | Exec Code Overflow XSS | 2005-02-09 | 2021-06-06 | **6.9** | None | Local | Medium | Not required | Complete | Complete | Complete |  |  |  |  |  |
| Buffer overflow in the get\_tag function in mod\_include for Apache 1.3.x to 1.3.32 allows local users who can create SSI documents to execute arbitrary code as the apache user via SSI (XSSI) documents that trigger a length calculation error. | | | | | | | | | | | | | | |
| 9 | [CVE-2004-0492](https://www.cvedetails.com/cve/CVE-2004-0492/) |  |  | DoS Exec Code Overflow | 2004-08-06 | 2021-06-06 | **10.0** | None | Remote | Low | Not required | Complete | Complete | Complete |  |  |  |  |  |
| Heap-based buffer overflow in proxy\_util.c for mod\_proxy in Apache 1.3.25 to 1.3.31 allows remote attackers to cause a denial of service (process crash) and possibly execute arbitrary code via a negative Content-Length HTTP header field, which causes a large amount of data to be copied. | | | | | | | | | | | | | | |
| 10 | [CVE-2004-0263](https://www.cvedetails.com/cve/CVE-2004-0263/) |  |  | +Info | 2004-11-23 | 2017-10-10 | **5.0** | None | Remote | Low | Not required | Partial | None | None |  |  |  |  |  |
| PHP 4.3.4 and earlier in Apache 1.x and 2.x (mod\_php) can leak global variables between virtual hosts that are handled by the same Apache child process but have different settings, which could allow remote attackers to obtain sensitive information. | | | | | | | | | | | | | | |
| 11 | [CVE-2003-0993](https://www.cvedetails.com/cve/CVE-2003-0993/) |  |  | Bypass | 2004-03-29 | 2021-06-06 | **7.5** | None | Remote | Low | Not required | Partial | Partial | Partial |  |  |  |  |  |
| mod\_access in Apache 1.3 before 1.3.30, when running big-endian 64-bit platforms, does not properly parse Allow/Deny rules using IP addresses without a netmask, which could allow remote attackers to bypass intended access restrictions. | | | | | | | | | | | | | | |