

Re: Unfiltered Header Injection in Apache 1.3.34/2.0.57/2.2.1

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2006-05/msg00437.html>

- *From:* "Amit Klein (AKsecurity)" <aksecurity@xxxxxxxxxx>
 - *Date:* Thu, 18 May 2006 21:03:17 +0200
-

On 8 May 2006 at 16:01, Zaninotti, Thiago wrote:

Folks,

During some specific tests with our upcoming Web App Security Scanner tool, we have found that Apache would kindly accept HTML injection through "Expect" header. Originally meant to be a protocol flow control that would give web client the capacity of sending the HTTP headers for server's pre-analysis before submitting the rest of the payload (body), Expect header is not usually used by common user's client-side software (for more details see section 8.2.6 from RFC 2616 – <http://www.ietf.org/rfc/rfc2616.txt>).

Dear Lists,

Thiago Zaninotti (the author of the original message –) and me worked a bit more on some aspects of this phenomena. Here are our results:

In Apache 2.0.x and 2.2.x, the 417 response will be sent by the server only upon connection termination. Such termination can be forced by the client (e.g. closing the browser), or by the server (after the timeout has elapsed, see the Timeout directive in the httpd.conf, typically its value is few minutes). So if you're testing this with Apache, please be patient, the response will take time to appear.

Things to keep in mind:

Regarding XSS

This phenomenon is not XSS per-se. Unless someone can show me how it is possible to force a browser to send the Expect header to the target site (other than via a rogue browser plug-

Re: Unfiltered Header Injection in Apache 1.3.34/2.0.57/2.2.1

in, which seems to me a bigger problem than XSS...). We did verify that the XMLHttpRequest object can send the "Expect" header simply via the setRequestHeader method. Yet there is a bootstrap problem using XHR since it is subject to the same origin policy.

Regarding proxy servers

Proxy servers are not supposed to forward a request with "unexpected" Expect value – see RFC 2616 section 14.20. Indeed, Apache mod_proxy does not forward this request. Yet Squid-2.5.STABLE10 does seem to forward this request (but it probably doesn't cache the response, see below).

Regarding Cacheability

The 417 response is not supposed to be cached. Apache sends the response without any cache-related headers, and thus caching this response is in violation of the RFC (RFC 2616 section 13.4). Indeed, IE 6.0 SP2 and FireFox 1.5.0.2 do not cache this response, even when a META tag is injected to introduce cache-related headers. Still, it's possible that there are cache servers out there that will cache this response.

Combining the above two notes, if there's a proxy cache server that forwards the invalid Expect header, AND caches the response, then this can be used to poison this cache server (e.g. an attacker sending a request to /index.html + Expect header, to the vulnerable Apache server through the proxy server). At the moment we're not aware of a proxy server that behaves this way.

Even without the above vector, this behavior "doesn't feel right", security-wise.

– Thiago and Amit