mtrudel / **bandit** Public

Code | Issues 1 | Pull requests 1 | Actions | Security and quality 5 | Ins

Commit `f2ca636`

mtrudel authored 6 hours ago · ✕ 23 / 27 · Verified

```
Merge commit from fork
```

main · 1.11.0

1 parent 21612c7 commit f2ca636

2 files changed +25 -3

Top

Filter files…

- lib/bandit
  - headers.ex
- test/bandit/http1
  - protocol_test.exs

Search within code

lib/bandit/headers.ex

```
@@ -49,9 +49,11 @@ defmodule Bandit.Headers do
49 49    @spec get_content_length(Plug.Conn.headers()) ::
50 50            {:ok, nil | non_neg_integer()} | {:error, String.t()}
51 51    def get_content_length(headers) do
52       -    case get_header(headers, "content-length") do
53       -      nil -> {:ok, nil}
54       -      value -> parse_content_length(value)
    52   +    # We need to special case this because we don't accept multiple content-
         length headers
```

```
      53 +     case Enum.filter(headers, &(elem(&1, 0) == "content-length")) do
      54 +       [] -> {:ok, nil}
      55 +       [{"content-length", value}] -> parse_content_length(value)
      56 +       _ -> {:error, "invalid content-length header (RFC9112§6.3)"}
55    57         end
56    58       end
57    59
```

test/bandit/http1/protocol_test.exs

```
@@ -828,6 +828,26 @@ defmodule HTTP1ProtocolTest do
828   828         send_resp(conn, 200, "OK")
829   829       end
830   830
      831 +     # Error case for content-length as defined in https://www.rfc-editor.org/rfc/rfc9112.html#section-6.3-2.5
      832 +     @tag :capture_log
      833 +     test "rejects a request with multiple separate content length headers, even if identical",
      834 +          context do
      835 +       # Use a smaller body size to avoid raciness in reading the response
      836 +       response =
      837 +         Req.post!(context.req,
      838 +           url: "/expect_body_with_multiple_content_length",
      839 +           headers: [{"content-length", "8000"}, {"content-length", "8000"}],
      840 +           body: String.duplicate("a", 8_000)
      841 +         )
      842 +
      843 +       assert response.status == 400
      844 +
      845 +       assert_receive {:log, %{level: :error, msg: {:string, msg}}}, 500
      846 +
      847 +       assert msg ==
      848 +                "** (Bandit.HTTPError) Content length unknown error: \"invalid content-length header (RFC9112§6.3)\""
      849 +     end
      850 +
831   851       # Error case for content-length as defined in https://www.rfc-editor.org/rfc/rfc9112.html#section-6.3-2.5
832   852       @tag :capture_log
```

```
833  853        test "rejects a request with non-matching multiple content lengths",
                context do
```

Comments 0

Please sign in to comment.