## Suricata - Bug #1442

### HTTP URL parser

04/07/2015 08:44 AM - Lucky b56

<table>
<thead>
<tr>
<th>Status:</th>
<th>Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td></td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td></td>
</tr>
<tr>
<td>Affected Versions:</td>
<td></td>
</tr>
<tr>
<td>Difficulty:</td>
<td></td>
</tr>
<tr>
<td>Effort:</td>
<td></td>
</tr>
<tr>
<td>Label:</td>
<td></td>
</tr>
</tbody>
</table>

#### Description

Wrong parsing by HTTP parser. The URL I have is: GET /kk/?error=The operation completed successfully&code=0 HTTP/1.0
It takes space as url and http protocol separation. The decoded structure is:

```
"http": {
  "hostname": "installs.ws",
  "url": "/kk/?error=The",
  "http_user_agent": "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 6.1; WOW64; SV1; Acoo Browser; Avant Browser; Avant Browser; SlimBrowser)",
  "http_content_type": "text/html",
  "connection": "keep-alive",
  "content_length": "568",
  "content_type": "text/html; charset=ISO-8859-1",
  "date": "Wed, 04 Mar 2015 15:05:39 GMT",
  "server": "nginx/1.5.13",
  "http_refer": "vi74mm4d.info",
  "http_method": "GET",
  "protocol": "operation completed successfully&code=0 HTTP/1.0",
  "status": "200",
  "length": 568,
  "tx_id": 0
}
```

I'm using 2.1beta3

#### History

**#1 - 04/07/2015 11:27 AM - Victor Julien**

I think suri/libhtp may be correct here, as the HTTP rfc's don't allow spaces in the URI. Can you confirm the server parses the uri correctly?

**#2 - 04/07/2015 08:48 PM - Lucky b56**

Yes. It's a malware trying to communicate with their custom HTTP server I believe.

**#3 - 04/07/2015 11:39 PM - Anoop Saldanha**

Lucky b56 wrote:

Yes. It's a malware trying to communicate with their custom HTTP server I believe.

It's more like custom server, rather than custom HTTP server. It's just that the protocol is very similar to HTTP.

**#4 - 04/08/2015 05:53 AM - Victor Julien**

Are you able to share a pcap either in the ticket or privately?

**#5 - 04/08/2015 06:04 AM - Lucky b56**

Unfortunately I don't have a pcap. You can close this issue now.

**#6 - 04/28/2015 03:28 AM - Victor Julien**

- Status changed from New to Closed