### Suricata - Feature #2487

#### Buffers for field/value pairs in http_uri and http_client_body

04/14/2018 06:53 PM - Jason Williams

<table>
<thead>
<tr>
<th>Status:</th>
<th>New</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td>OISF Dev</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td>TBD</td>
</tr>
<tr>
<td>Effort:</td>
<td>medium</td>
</tr>
<tr>
<td>Difficulty:</td>
<td>medium</td>
</tr>
</tbody>
</table>

**Description**

We've found `http_header_names` to be one of our favorite new 4.0 buffers and would like to see if we could carry over this logic to other buffers.

For example, if the string in either the `http_uri` or the `http_client_body` was "field1=value1&field2=value2&field3=value3"

```plaintext
http_uri_(field_name); content:"|0d 0a|field1"; nocase; startswith; content:"field3|0d 0a 0d 0a|"; nocase; endswith;
http_uri_(value_name); content:"|0d 0a|value1"; nocase; startswith; content:"value3|0d 0a 0d 0a|"; nocase; endswith;
```

basically the same for `client_body`

```plaintext
http_client_body_(field_name); content:"|0d 0a|field1"; nocase; startswith; content:"field3|0d 0a 0d 0a|"; nocase; endswith;
http_client_body_(value_name); content:"|0d 0a|value1"; nocase; startswith; content:"value3|0d 0a 0d 0a|"; nocase; endswith;
```

**Related Issues:**

- Related to Feature #1194: Implement `http_args` keyword to match http arguments... New
- Related to Task #4097: Suricon 2020 brainstorm New

**History**

#### #1 - 06/12/2018 05:20 PM - Jason Ish
- Effort set to medium
- Difficulty set to medium

#### #2 - 09/26/2019 03:19 PM - Victor Julien
- Related to Feature #1194: Implement `http_args` keyword to match http arguments - query string or body added

#### #3 - 11/14/2020 02:25 PM - Jeff Lucovsky
- Related to Task #4097: Suricon 2020 brainstorm added