**Suricata - Feature #1194**

**Implement http_args keyword to match http arguments - query string or body**

05/21/2014 06:27 AM - Anoop Saldanha

<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>Community Ticket</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>low</td>
</tr>
</tbody>
</table>

**Description**

We can use a http_args keyword that would match on the "name = value" pairs of http arguments from the query string or from the body.

**Related issues:**

Related to Feature #2487: Buffers for field/value pairs in http_uri and http...

**History**

#1 - 05/25/2014 10:35 PM - Anoop Saldanha

The idea is to make this a sticky buffer. Does that sound fine? Currently all the http keywords are modifiers. Would that be an issue with regard to consistency on how other http keywords behave?

#2 - 05/26/2014 03:49 AM - Victor Julien

Can you give some rule examples?

#3 - 05/26/2014 07:43 AM - Anoop Saldanha

```
alert tcp any any -> any any (http_args; content:"argument"; sid:1;)
alert tcp any any -> any any (http_args; content:"argument"; pcre:"/argument1"; sid:1;)
```

Similarly, other content keywords can be used.

To use other modifier keywords or sticky buffer, one would have to use pkt_data.

```
alert tcp any any -> any any (http:args; content:"argument"; pcre:"/argument1";
pkt_data; content:"uri"; http_uri; sid:1;)
```

#4 - 09/08/2016 03:28 PM - Andreas Herz

- Assignee changed from Anoop Saldanha to OISF Dev

#5 - 08/09/2018 10:28 AM - Victor Julien

- Assignee changed from OISF Dev to Anonymous
- Priority changed from Low to Normal
- Effort set to medium
- Difficulty set to low

#6 - 02/23/2019 10:14 PM - Andreas Herz

- Assignee set to Community Ticket

#7 - 09/26/2019 03:19 PM - Victor Julien

- Related to Feature #2487: Buffers for field/value pairs in http_uri and http_client_body added