Suricata - Bug #418
Stray backslashes should be escaped in PrintRawUriFp()
03/02/2012 02:32 PM - Will Metcalf

<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>Anoop Saldanha</td>
</tr>
<tr>
<td>Category</td>
<td></td>
</tr>
<tr>
<td>Target version</td>
<td>1.3beta2</td>
</tr>
<tr>
<td>Affected Versions</td>
<td></td>
</tr>
<tr>
<td>Difficulty</td>
<td></td>
</tr>
<tr>
<td>Label</td>
<td></td>
</tr>
</tbody>
</table>

Description
To avoid confusion with actual escaped characters this function should escape stray backslashes.

Example:
```
nc www.openinfosecfoundation.org 80
GET /foo/\x80 HTTP/1.0

HTTP/1.1 404 Not Found
Date: Fri, 02 Mar 2012 19:41:33 GMT
Server: 
Content-Length: 206
Connection: close
Content-Type: text/html; charset=iso-8859-1

In Suricata this request will look like this in the http.log.
03/02/2012-14:24:34.652663 <hostname unknown> [**] /foo/\x80 [**] <useragent unknown> [**] <no referer> [**] GET [**] HTTP/1.0 [**] 404 [**] 206 bytes [**]...

Similar request in an Apache log..
127.0.0.1 -- [01/Feb/2012:09:23:52 -0600] "GET /foo/\x80 HTTP/1.0" 404 484 "-" "-"
```

History

#1 - 04/25/2012 05:31 AM - Victor Julien
- Description updated
- Status changed from New to Assigned
- Assignee changed from Victor Julien to Anoop Saldanha
- Estimated time set to 2.00 h

Anoop can you look into this as part of the buffer api work?

#2 - 05/04/2012 11:07 AM - Anoop Saldanha
- File 0001-bug-418-update-http-log-to-escape-backslashes.patch added

patch attached.

#3 - 05/16/2012 04:51 AM - Victor Julien
- Status changed from Assigned to Closed
- % Done changed from 0 to 100

Applied, thanks Anoop!

Files