

pfSense - Bug #10765

Ampersands in ldap_extended_query are escaped twice

07/15/2020 11:04 AM - Louis Sautier

Status:	New	Start date:	07/15/2020
Priority:	Normal	Due date:	
Assignee:		% Done:	0%
Category:	Authentication	Estimated time:	0.00 hour
Target version:		Affected Architecture:	All
Affected Version:	2.4.4		

Description

Hello,
I recently ran into an issue with an LDAP server whose Query field contained an ampersand.

The field is set to

```
memberOf=CN=Some Group,OU=One & Two,DC=blah,DC=local
```

That results in

```
<ldap_extended_query><![CDATA[memberOf=CN=Some Group,OU=One & Two,DC=blah,DC=local]]>
</ldap_extended_query>
```

in config.xml.

Re-writing the XML config with Python shows that & is escaped twice (once because of CDATA, once because of the HTML entities):

```
#!/usr/bin/env python3
import xml.etree.ElementTree as ET

xml = "
<ldap_extended_query><![CDATA[memberOf=CN=Some Group,OU=One & Two,DC=blah,DC=local]]></ldap_ex
tended_query>"
tree = ET.fromstring(xml)
print(ET.tostring(tree, encoding="unicode"))
```

Running the script results in

```
<ldap_extended_query>memberOf=CN=Some Group,OU=One && Two,DC=blah,DC=local
</ldap_extended_query>
```

Both syntaxes should be equivalent. However, when the configuration is reloaded, the query (as shown in the WEB UI) becomes

```
memberOf=CN=Some Group,OU=One & Two,DC=blah,DC=local
```

and is now invalid.

History

#1 - 09/02/2020 05:20 AM - Louis Sautier

Hello, I am surprised that this issue hasn't been assigned to anybody in 2 months. Is there anything I can do to give it more visibility? I can provide more info if required, just let me know.

The reason this is problematic is that every time I use [this pfsense ansible module](#), I break my LDAP config because it rewrites the whole XML file.

#2 - 09/02/2020 07:55 AM - Jim Pingle

- *Category set to Authentication*

That is an unsupported add-on, and a rare use case. You are welcome to submit a PR with a fix, but it's not something we would rush to direct resources to fix.