# pfSense - Bug #8143

## XSS in status_filter_reload.php

11/28/2017 03:01 PM - Anonymous

| | | | |
|---|---|---|---|
| **Status:** | Resolved | **Start date:** | 11/28/2017 |
| **Priority:** | Very High | **Due date:** | |
| **Assignee:** | Jim Pingle | **% Done:** | 100% |
| **Category:** | Web Interface | **Estimated time:** | 0.00 hour |
| **Target version:** | 2.4.2-p1 | | |
| **Plus Target Version:** | | **Affected Version:** | All |
| **Release Notes:** | Default | **Affected Architecture:** | All |

**Description**

I am not sure the procedure for pushing fixes like this. If I push it to gitlab will it be public? I wouldn't want to expose a security flaw until its fixed. If you type this in the URL with a pfsense box you will find it pretty easily. "status_filter_reload.php?user=</script><script>alert(1)</script>" The fix is pretty simple in status_filter_reload.php on line 169 if you change

```
if ("<?=$_REQUEST['user']?>" != "true")
```

to

```
if ("<?=htmlspecialchars($_REQUEST['user'])?>" != "true")
```

It works fine.

### Associated revisions

**Revision 82b1d76f - 11/28/2017 03:28 PM - Stephen Jones**

Fixed #8143 Remove any html special characters for request variable

**Revision fea5a8af - 11/28/2017 03:30 PM - Stephen Jones**

Fixed #8143 Remove any html special characters for request variable

**Revision 11b3b8e6 - 11/28/2017 03:39 PM - Stephen Jones**

Fixed #8143 Remove any html special characters for request variable

**Revision 36ca9be2 - 11/28/2017 03:41 PM - Stephen Jones**

Fixed #8143 Remove any html special characters for request variable

### History

**#1 - 11/28/2017 03:17 PM - Jim Pingle**

*- Category set to Web Interface*

*- Priority changed from Normal to Very High*

*- Affected Architecture All added*

*- Affected Architecture deleted ()*

Usually we will push a fix to master and cherry pick it to the latest development and release branches, which right now would be: RELENG_2_4_2, RELENG_2_3, and RELENG_2_3_5. This bug report will remain private until whatever release(es) we put out next, at which time we'll draft an SA for it. Having the fix be public isn't a problem for cases like this.

#### #2 - 11/28/2017 03:40 PM - Anonymous

*- Status changed from New to Feedback*

*- % Done changed from 0 to 100*

Applied in changeset 82b1d76f934d793fe681c9c80da1a8e32cefc1f5.

#### #3 - 12/01/2017 03:36 PM - Jim Pingle

*- Status changed from Feedback to Resolved*

*- Target version set to 2.4.2-p1*

*- Affected Version set to All*

This looks good in current snapshots.

#### #4 - 12/14/2017 11:09 AM - Jim Pingle

*- Private changed from Yes to No*