Sri Lanka Institute of Information Technology

Web Security - IE2062

Bug Bounty Report 8

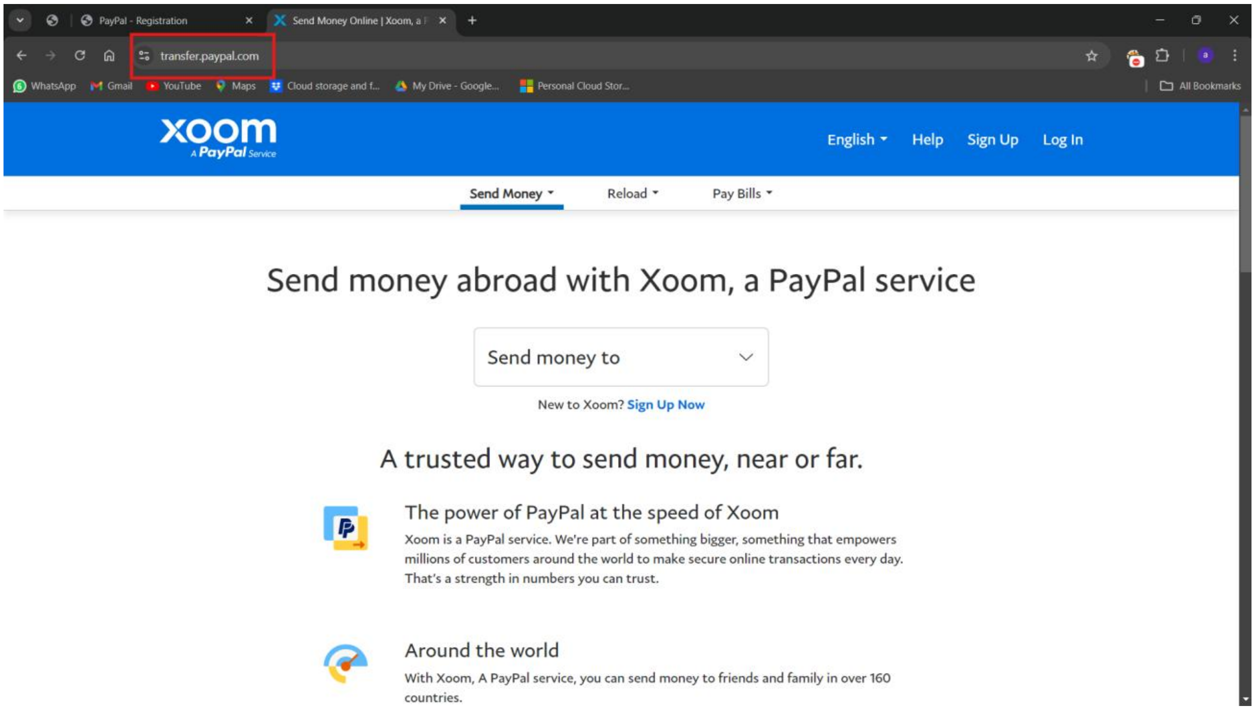
PERERA A.P.J

IT22280992

Group Y2S2.CS

Table of Contents

1. **TARGET:** https://transfer.paypal.com



Send money abroad with Xoom, a PayPal service

Send money to

New to Xoom? Sign Up Now

A trusted way to send money, near or far.

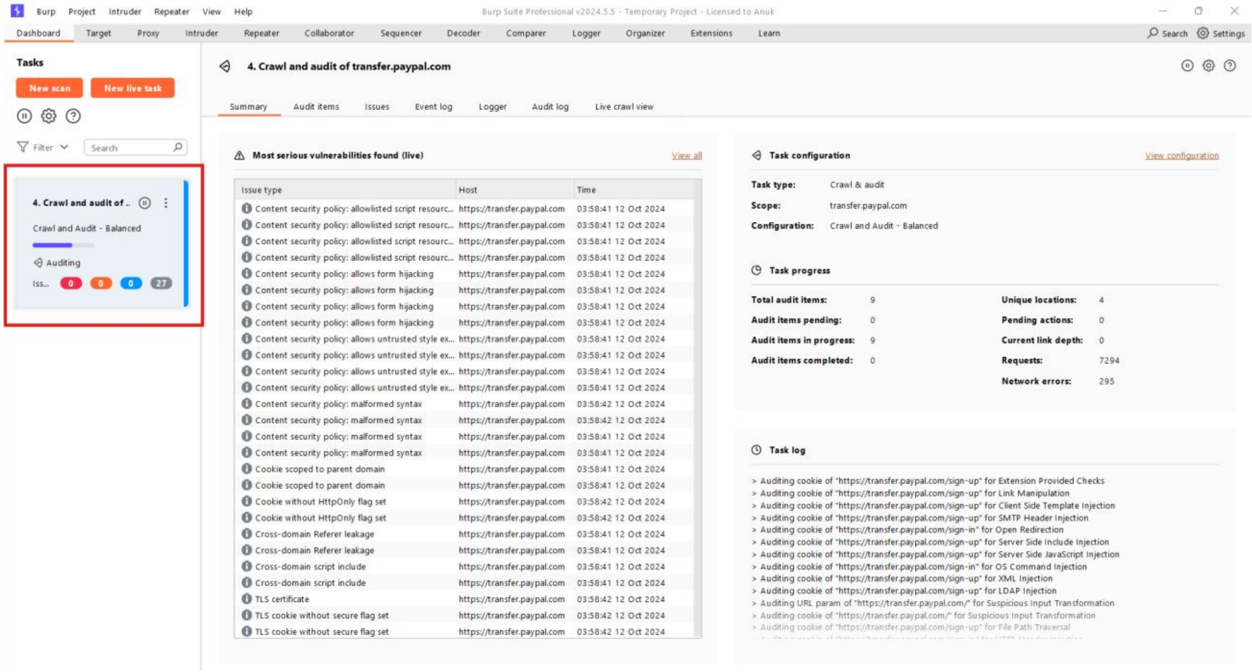
The power of PayPal at the speed of Xoom

Xoom is a PayPal service. We're part of something bigger, something that empowers millions of customers around the world to make secure online transactions every day. That's a strength in numbers you can trust.

Around the world

With Xoom, A PayPal service, you can send money to friends and family in over 160 countries.

- Using burpsuite scan found vulnerability.


Burp Project Intruder Repeater View Help
Burp Suite Professional v2024.5.5 - Temporary Project - Licensed to Anuk
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Search Settings
Tasks
New scan
New live task
Filter
Search
4. Crawl and audit of ..
Crawl and Audit - Balanced
Auditing
Iss...
0
0
0
27
Summary Audit items Issues Event log Logger Audit log Live crawl view
View all
View configuration

4. Crawl and audit of transfer.paypal.com

Most serious vulnerabilities found (live)

Issue type	Host	Time
Content security policy: allowlisted script resourc...	https://transfer.paypal.com	03:58:41 12 Oct 2024
Content security policy: allowlisted script resourc...	https://transfer.paypal.com	03:58:41 12 Oct 2024
Content security policy: allowlisted script resourc...	https://transfer.paypal.com	03:58:41 12 Oct 2024
Content security policy: allowlisted script resourc...	https://transfer.paypal.com	03:58:41 12 Oct 2024
Content security policy: allows form hijacking	https://transfer.paypal.com	03:58:41 12 Oct 2024
Content security policy: allows form hijacking	https://transfer.paypal.com	03:58:41 12 Oct 2024
Content security policy: allows form hijacking	https://transfer.paypal.com	03:58:41 12 Oct 2024
Content security policy: allows form hijacking	https://transfer.paypal.com	03:58:41 12 Oct 2024
Content security policy: allows untrusted style ex...	https://transfer.paypal.com	03:58:41 12 Oct 2024
Content security policy: allows untrusted style ex...	https://transfer.paypal.com	03:58:41 12 Oct 2024
Content security policy: allows untrusted style ex...	https://transfer.paypal.com	03:58:41 12 Oct 2024
Content security policy: allows untrusted style ex...	https://transfer.paypal.com	03:58:41 12 Oct 2024
Content security policy: malformed syntax	https://transfer.paypal.com	03:58:42 12 Oct 2024
Content security policy: malformed syntax	https://transfer.paypal.com	03:58:42 12 Oct 2024
Content security policy: malformed syntax	https://transfer.paypal.com	03:58:41 12 Oct 2024
Content security policy: malformed syntax	https://transfer.paypal.com	03:58:41 12 Oct 2024
Cookie scoped to parent domain	https://transfer.paypal.com	03:58:41 12 Oct 2024
Cookie scoped to parent domain	https://transfer.paypal.com	03:58:41 12 Oct 2024
Cookie without HttpOnly flag set	https://transfer.paypal.com	03:58:42 12 Oct 2024
Cookie without HttpOnly flag set	https://transfer.paypal.com	03:58:42 12 Oct 2024
Cross-domain Referer leakage	https://transfer.paypal.com	03:58:41 12 Oct 2024
Cross-domain Referer leakage	https://transfer.paypal.com	03:58:41 12 Oct 2024
Cross-domain script include	https://transfer.paypal.com	03:58:41 12 Oct 2024
Cross-domain script include	https://transfer.paypal.com	03:58:41 12 Oct 2024
TLS certificate	https://transfer.paypal.com	03:58:42 12 Oct 2024
TLS cookie without secure flag set	https://transfer.paypal.com	03:58:42 12 Oct 2024
TLS cookie without secure flag set	https://transfer.paypal.com	03:58:42 12 Oct 2024

Task configuration

Task type: Crawl & audit
Scope: transfer.paypal.com
Configuration: Crawl and Audit - Balanced

Task progress

Total audit items:	9	**Unique locations:**	4
Audit items pending:	0	**Pending actions:**	0
Audit items in progress:	9	**Current link depth:**	0
Audit items completed:	0	**Requests:**	7294
		Network errors:	295

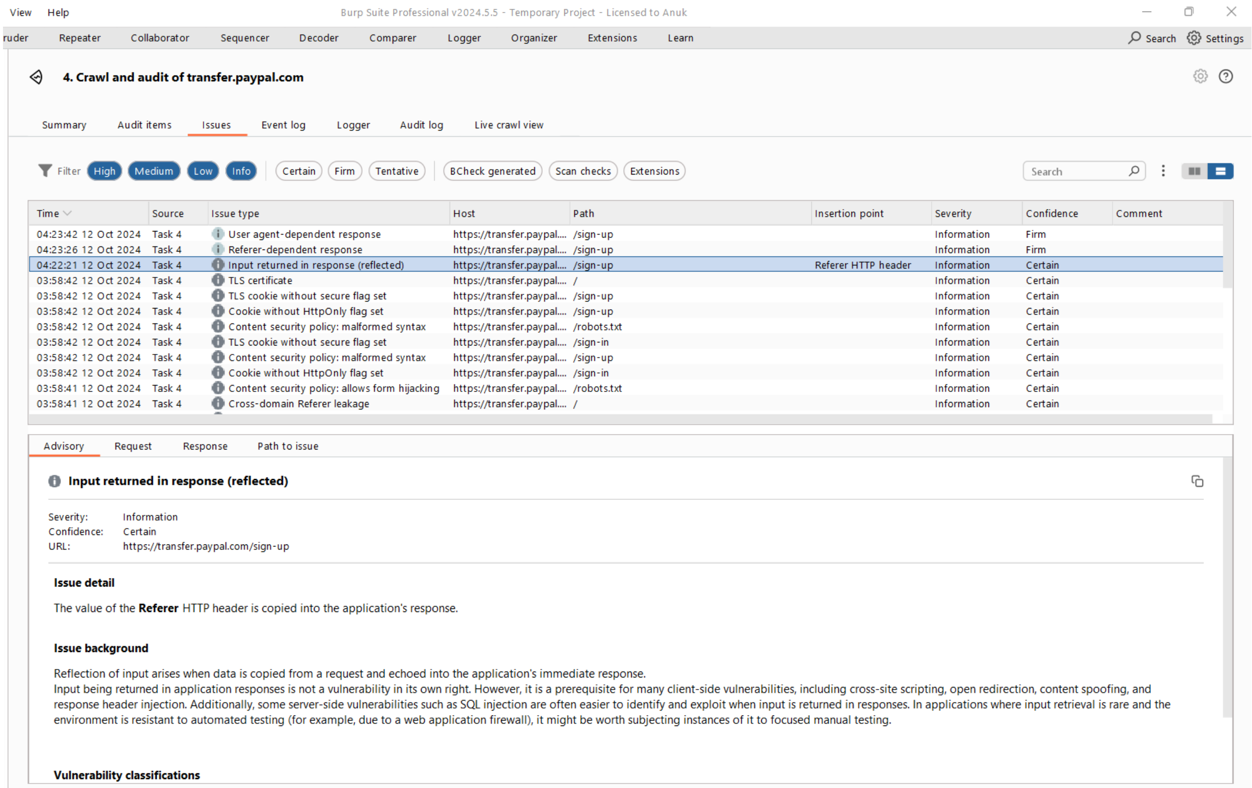
Task log

```
> Auditing cookie of "https://transfer.paypal.com/sign-up" for Extension Provided Checks
> Auditing cookie of "https://transfer.paypal.com/sign-up" for Link Manipulation
> Auditing cookie of "https://transfer.paypal.com/sign-up" for Client Side Template Injection
> Auditing cookie of "https://transfer.paypal.com/sign-up" for SMTP Header Injection
> Auditing cookie of "https://transfer.paypal.com/sign-in" for Open Redirection
> Auditing cookie of "https://transfer.paypal.com/sign-up" for Server Side Include Injection
> Auditing cookie of "https://transfer.paypal.com/sign-up" for Server Side JavaScript Injection
> Auditing cookie of "https://transfer.paypal.com/sign-in" for OS Command Injection
> Auditing cookie of "https://transfer.paypal.com/sign-up" for XML Injection
> Auditing cookie of "https://transfer.paypal.com/sign-up" for LDAP Injection
> Auditing URL param of "https://transfer.paypal.com/" for Suspicious Input Transformation
> Auditing cookie of "https://transfer.paypal.com/" for Suspicious Input Transformation
> Auditing cookie of "https://transfer.paypal.com/sign-up" for File Path Traversal
> Auditing cookie of "https://transfer.paypal.com/sign-in" for HTTP Header Injection
```

2. Vulnerability

2.1 Vulnerability title

- Input returned in response (Reflected Cross-Site Scripting (XSS)).



4. Crawl and audit of transfer.paypal.com

Time	Source	Issue type	Host	Path	Insertion point	Severity	Confidence	Comment
04:23:42 12 Oct 2024	Task 4	User agent-dependent response	https://transfer.paypal....	/sign-up		Information	Firm	
04:23:26 12 Oct 2024	Task 4	Referer-dependent response	https://transfer.paypal....	/sign-up		Information	Firm	
04:22:21 12 Oct 2024	Task 4	Input returned in response (reflected)	https://transfer.paypal....	/sign-up	Referer HTTP header	Information	Certain	
03:58:42 12 Oct 2024	Task 4	TLS certificate	https://transfer.paypal....	/		Information	Certain	
03:58:42 12 Oct 2024	Task 4	TLS cookie without secure flag set	https://transfer.paypal....	/sign-up		Information	Certain	
03:58:42 12 Oct 2024	Task 4	Cookie without HttpOnly flag set	https://transfer.paypal....	/sign-up		Information	Certain	
03:58:42 12 Oct 2024	Task 4	Content security policy: malformed syntax	https://transfer.paypal....	/robots.txt		Information	Certain	
03:58:42 12 Oct 2024	Task 4	TLS cookie without secure flag set	https://transfer.paypal....	/sign-in		Information	Certain	
03:58:42 12 Oct 2024	Task 4	Content security policy: malformed syntax	https://transfer.paypal....	/sign-up		Information	Certain	
03:58:42 12 Oct 2024	Task 4	Cookie without HttpOnly flag set	https://transfer.paypal....	/sign-in		Information	Certain	
03:58:41 12 Oct 2024	Task 4	Content security policy: allows form hijacking	https://transfer.paypal....	/robots.txt		Information	Certain	
03:58:41 12 Oct 2024	Task 4	Cross-domain Referer leakage	https://transfer.paypal....	/		Information	Certain	

Input returned in response (reflected)

Severity: Information
Confidence: Certain
URL: https://transfer.paypal.com/sign-up

Issue detail

The value of the **Referer** HTTP header is copied into the application's response.

Issue background

Reflection of input arises when data is copied from a request and echoed into the application's immediate response.
Input being returned in application responses is not a vulnerability in its own right. However, it is a prerequisite for many client-side vulnerabilities, including cross-site scripting, open redirection, content spoofing, and response header injection. Additionally, some server-side vulnerabilities such as SQL injection are often easier to identify and exploit when input is returned in responses. In applications where input retrieval is rare and the environment is resistant to automated testing (for example, due to a web application firewall), it might be worth subjecting instances of it to focused manual testing.

Vulnerability classifications

2.2 Vulnerability description

- One of the design weakening issues, which is popularly termed as reflected cross site scripting (xss) attacks, arises when an application reflects any user input back in its response without sanitizing or encoding the data properly. This threat allows a hacker to plant and execute rogue scripts within webpages while the latter page which may be linked to the former does not require any changes to be made. Consequently, attackers can perform data exfiltration (for example sucking out session cookies), identity theft or even phishing scams. Though reflected xss attacks tend to be less permanent or lasting since it only concerns individuals who 'consume' the attackers decoratively designed input, it is still a danger to the security of persons. In order to reduce the effect of raising and exploiting this vulnerability, careful validation and encoding of all user inputs should be done, besides other securing measures such as Content Security Policies (CSP) which involve more active efforts to harden the application against XSS vulnerabilities.

2.3 Affected components

The Reflected Cross-Site Scripting (XSS) vulnerability can affect several key components of a web application, primarily those involved in processing, handling, or rendering user-supplied data. The main affected components include:

1. User Input Fields:

   - Any form field, search box, or URL parameter that takes input from users. This includes fields for login, registration, search, and comments, as well as any other places where data is directly taken from users.

2. Dynamic Content Rendering:

   - Web pages or components that render user input dynamically in HTML, JavaScript, or other client-side content without proper encoding or sanitization.

3. URL Parameters:

   - Query strings and URL parameters used for navigation or passing data between pages. If these are reflected in the response without filtering, they become prime targets for XSS attacks.

4. Error Messages and Notifications:

   - Pages that display error messages based on user input, such as login errors or invalid search queries. If these responses contain unsanitized user input, they can inadvertently execute malicious code.

5. JavaScript Libraries and Frameworks:

   - Components that process or manipulate user input using JavaScript. Vulnerabilities can occur if these libraries or frameworks do not handle input securely or if they improperly trust user data.

6. Search Functionality:

   - Search features that reflect the query string or parameters back to the user. Attackers may inject scripts in search queries that are reflected on the results page, enabling malicious code execution.

7. Third-Party Integrations:

   - Any third-party widgets or APIs that accept and return user data, such as social media plugins, comment systems, and external analytics. If not securely implemented, they can introduce or propagate XSS vulnerabilities.

8. Headers and Metadata:

   - Application headers, such as Location or Referer, that might reflect user data, especially if they are displayed back to the user on error pages or redirects.

2.4 Impact assessment

The Impact Assessment for a Reflected Cross-Site Scripting (XSS) Vulnerability outlines the potential consequences of a successful attack exploiting this vulnerability. The severity of the impact depends on the nature of the application, the data it handles, and the permissions granted to the affected user. Here are the primary impacts:

1. Data Theft:

   - Attackers can steal sensitive information, such as session cookies, authentication tokens, or personal data stored in the browser. This enables unauthorized access to user accounts and potentially other systems.

2. Session Hijacking:

   - By capturing session cookies, attackers can impersonate users and access their accounts. This could lead to identity theft, unauthorized financial transactions, or manipulation of user profiles.

3. Account Compromise:

   - In applications with high privileges, such as administrative accounts, the attacker can exploit XSS to take control of the entire application or backend systems, leading to extensive damage.

4. Phishing Attacks:

   - XSS allows attackers to inject deceptive content, such as fake login forms, onto the application. This can trick users into entering their credentials, which the attacker then captures for use in other malicious activities.

5. Malware Distribution:

   - Malicious scripts injected through XSS can redirect users to download malware, ransomware, or other harmful software, compromising user devices and potentially spreading across networks.

6. Reputation Damage:

- Successful XSS attacks can lead to customer distrust and reputational damage, especially if the site is perceived as insecure. This can impact user retention, sales, and overall business credibility.

7. Compliance Violations:

- Data exposure due to XSS can result in breaches of data protection laws, such as GDPR, HIPAA, or PCI-DSS. This could lead to legal penalties, fines, and additional scrutiny from regulatory authorities.

8. Operational Disruption:

- Addressing XSS attacks can cause significant operational disruption, as developers and security teams work to remediate the issue, recover from data loss, and restore user trust. This may also involve incident response activities, forensic analysis, and security audits.

2.5 Steps to reproduce

To reproduce a Reflected Cross-Site Scripting (XSS) Vulnerability, you can follow these steps in a controlled environment. This example demonstrates how to exploit a URL parameter vulnerability, which is commonly found in search or input forms. Ensure you have permission to test the application and use only for ethical and authorized purposes.

Steps to Reproduce

1. Identify a Potentially Vulnerable Page:
   - Look for pages that take user input and reflect it directly in the page response. Common pages include search, error, and query parameter pages, where inputs are often displayed back to the user.
   - Example: A search page at http://example.com/search?q=

2. Inject a Basic Script:
   - Test if the page reflects your input by entering a simple HTML or JavaScript snippet. Try injecting a script into the URL parameter:
   - Replace q with the name of the input parameter used on the page if different.

3. Analyze the Response:
   - When the page loads, observe if the JavaScript code is executed. If an alert box pops up with the message "XSS," this indicates that the input was reflected and executed as a script, confirming an XSS vulnerability.

4. Try Other Payloads for Testing:
   - To further confirm the vulnerability, you can experiment with other script payloads to check the extent of the execution capability. For example:
   - This example uses an image tag with an onerror event, which will trigger if the image fails to load, executing the alert function.

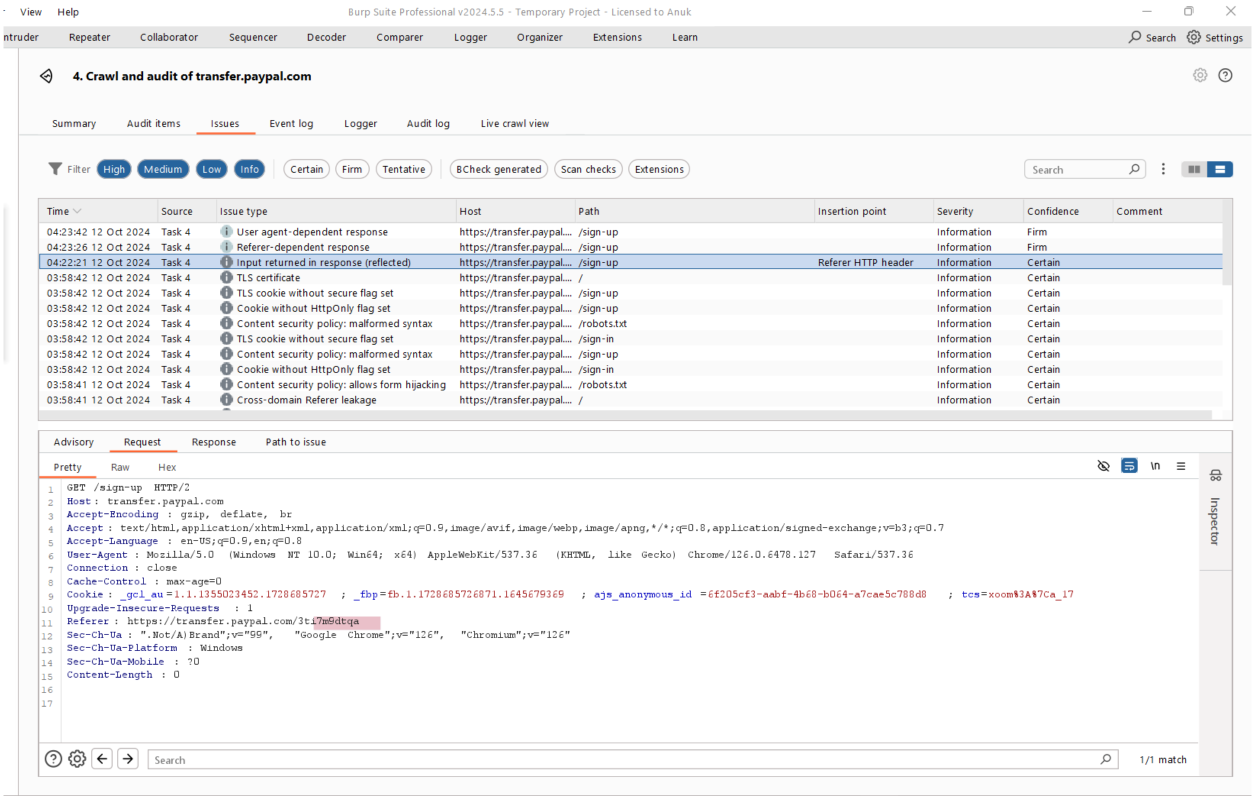
5. Document Findings:

   - Record the steps taken, the payloads used, and the application’s response for further analysis. Document any potential risks associated with this vulnerability, such as data theft or session hijacking.

6. Report and Remediate:

   - If testing in a real environment, responsibly report the vulnerability to the application owner or security team. Provide information on how to reproduce the issue and suggest remediation steps, such as input sanitization and output encoding.

2.6 Proof of concept

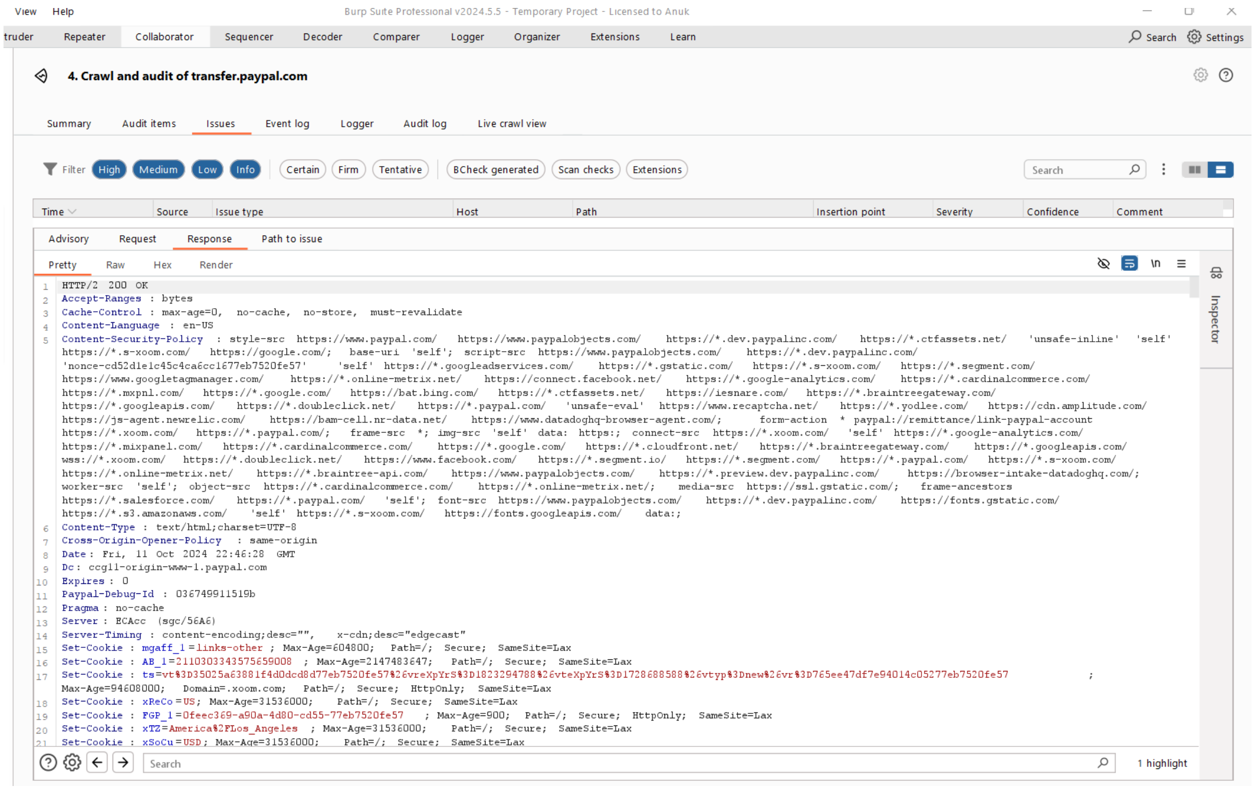


4. Crawl and audit of transfer.paypal.com

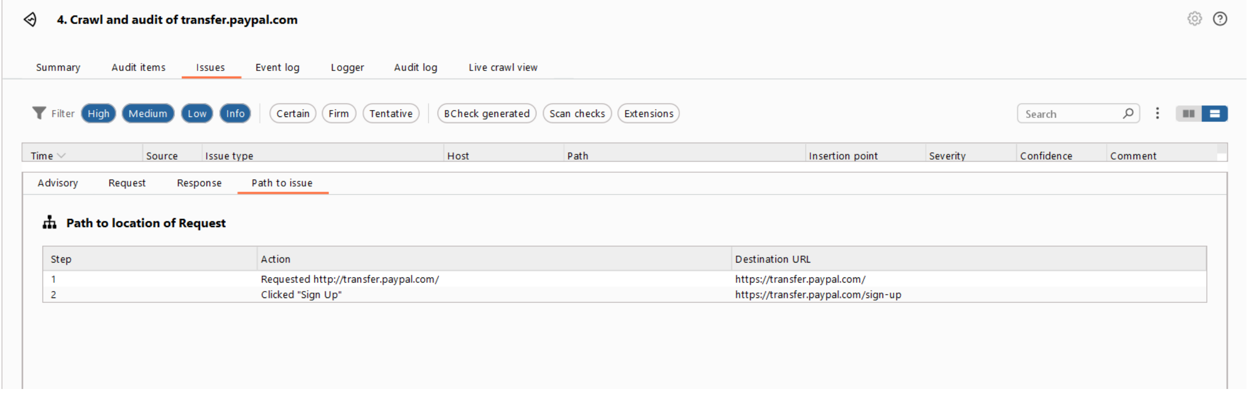
Time	Source	Issue type	Host	Path	Insertion point	Severity	Confidence	Comment
04:23:42 12 Oct 2024	Task 4	User agent-dependent response	https://transfer.paypal....	/sign-up		Information	Firm	
04:23:26 12 Oct 2024	Task 4	Referer-dependent response	https://transfer.paypal....	/sign-up		Information	Firm	
04:22:21 12 Oct 2024	Task 4	Input returned in response (reflected)	https://transfer.paypal....	/sign-up	Referer HTTP header	Information	Certain	
03:58:42 12 Oct 2024	Task 4	TLS certificate	https://transfer.paypal....	/		Information	Certain	
03:58:42 12 Oct 2024	Task 4	TLS cookie without secure flag set	https://transfer.paypal....	/sign-up		Information	Certain	
03:58:42 12 Oct 2024	Task 4	Cookie without HttpOnly flag set	https://transfer.paypal....	/sign-up		Information	Certain	
03:58:42 12 Oct 2024	Task 4	Content security policy: malformed syntax	https://transfer.paypal....	/robots.txt		Information	Certain	
03:58:42 12 Oct 2024	Task 4	TLS cookie without secure flag set	https://transfer.paypal....	/sign-in		Information	Certain	
03:58:42 12 Oct 2024	Task 4	Content security policy: malformed syntax	https://transfer.paypal....	/sign-up		Information	Certain	
03:58:42 12 Oct 2024	Task 4	Cookie without HttpOnly flag set	https://transfer.paypal....	/sign-in		Information	Certain	
03:58:41 12 Oct 2024	Task 4	Content security policy: allows form hijacking	https://transfer.paypal....	/robots.txt		Information	Certain	
03:58:41 12 Oct 2024	Task 4	Cross-domain Referer leakage	https://transfer.paypal....	/		Information	Certain	

```
GET /sign-up  HTTP/2
Host : transfer.paypal.com
Accept-Encoding : gzip, deflate, br
Accept : text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language : en-US;q=0.9,en;q=0.8
User-Agent : Mozilla/5.0  (Windows  NT 10.0;  Win64;  x64)  AppleWebKit/537.36   (KHTML,  like  Gecko)  Chrome/126.0.6478.127   Safari/537.36
Connection : close
Cache-Control : max-age=0
Cookie : _gcl_au=1.1.1355023452.1728685727  ; _fbp=fb.1.1728685726871.1645679369   ; ajs_anonymous_id =6f205cf3-aabf-4b68-b064-a7cae5c788d8   ; tcs=xoom%3A%7Ca_17
Upgrade-Insecure-Requests  : 1
Referer : https://transfer.paypal.com/3ti7m9dtqa
Sec-Ch-Ua : ".Not/A)Brand";v="99",   "Google  Chrome";v="126",   "Chromium";v="126"
Sec-Ch-Ua-Platform  : Windows
Sec-Ch-Ua-Mobile  : ?0
Content-Length  : 0


```

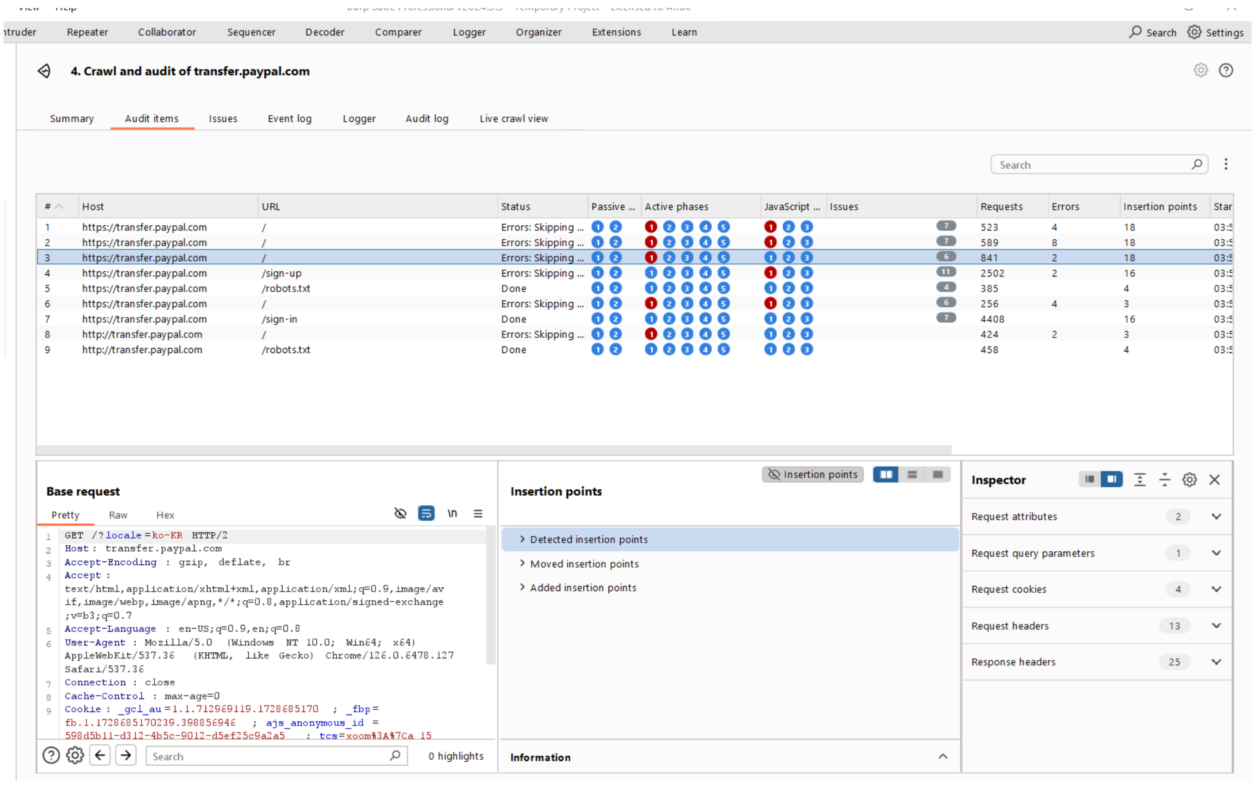


```
HTTP/2  200  OK
Accept-Ranges : bytes
Cache-Control : max-age=0,  no-cache,  no-store,  must-revalidate
Content-Language  : en-US
Content-Security-Policy  : style-src  https://www.paypal.com/   https://www.paypalobjects.com/   https://*.dev.paypalinc.com/   https://*.ctfassets.net/   'unsafe-inline'  'self'
https://*.s-xoom.com/   https://google.com/;   base-uri  'self';  script-src  https://www.paypalobjects.com/    https://*.dev.paypalinc.com/
'nonce-cd52d1e1c45c4ca6cc1677eb7520fe57'     'self'  https://*.googleadservices.com/    https://*.gstatic.com/   https://*.s-xoom.com/   https://*.segment.com/
https://www.googletagmanager.com/    https://*.online-metrix.net/    https://connect.facebook.net/    https://*.google-analytics.com/    https://*.cardinalcommerce.com/
https://*.mxpnl.com/   https://*.google.com/   https://bat.bing.com/   https://*.ctfassets.net/   https://iesnare.com/   https://*.braintreegateway.com/
https://*.googleapis.com/   https://*.doubleclick.net/   https://*.paypal.com/   'unsafe-eval'  https://www.recaptcha.net/   https://*.yodlee.com/   https://cdn.amplitude.com/
https://js-agent.newrelic.com/    https://bam-cell.nr-data.net/    https://www.datadoghq-browser-agent.com/;      form-action  *  paypal://remittance/link-paypal-account
https://*.xoom.com/   https://*.paypal.com/;   frame-src  *;  img-src  'self'  data:  https:;  connect-src  https://*.xoom.com/   'self'  https://*.google-analytics.com/
https://*.mixpanel.com/   https://*.cardinalcommerce.com/    https://*.google.com/   https://*.cloudfront.net/   https://*.braintreegateway.com/    https://*.googleapis.com/
wss://*.xoom.com/   https://*.doubleclick.net/   https://www.facebook.com/   https://*.segment.io/   https://*.segment.com/   https://*.paypal.com/   https://*.s-xoom.com/
https://*.online-metrix.net/    https://*.braintree-api.com/    https://www.paypalobjects.com/    https://*.preview.dev.paypalinc.com/     https://browser-intake-datadoghq.com/;
worker-src  'self';  object-src  https://*.cardinalcommerce.com/    https://*.online-metrix.net/;    media-src  https://ssl.gstatic.com/;    frame-ancestors
https://*.salesforce.com/   https://*.paypal.com/   'self';  font-src  https://www.paypalobjects.com/    https://*.dev.paypalinc.com/    https://fonts.gstatic.com/
https://*.s3.amazonaws.com/    'self'  https://*.s-xoom.com/    https://fonts.googleapis.com/    data:;
Content-Type : text/html;charset=UTF-8
Cross-Origin-Opener-Policy  : same-origin
Date : Fri,  11  Oct  2024  22:46:28  GMT
Dc : ccg11-origin-www-1.paypal.com
Expires : 0
Paypal-Debug-Id  : 036749911519b
Pragma : no-cache
Server : ECAcc  (sgc/56A6)
Server-Timing : content-encoding;desc="",    x-cdn;desc="edgecast"
Set-Cookie : mgaff_1 =links-other ; Max-Age=604800;   Path=/;  Secure;  SameSite=Lax
Set-Cookie : AB_1=211030334357565900 8  ; Max-Age=2147483647;   Path=/;  Secure;  SameSite=Lax
Set-Cookie : ts=vt%3D35025a63881f4d0dcd8d77eb7520fe57%26vreXpYrS%3D1823294788%26vteXpYrS%3D1728688588%26vtyp%3Dnew%26vr%3D765ee47df7e94014c05277eb7520fe57          ;
Max-Age=94608000;   Domain=.xoom.com;   Path=/;  Secure;  HttpOnly;  SameSite=Lax
Set-Cookie : xReCo =US; Max-Age=31536000;    Path=/;  Secure;  SameSite=Lax
Set-Cookie : FGP_1 =0feec369-a90a-4d80-cd55-77eb7520fe57    ; Max-Age=900;   Path=/;  Secure;  HttpOnly;  SameSite=Lax
Set-Cookie : xTZ=America%2FLos_Angeles  ; Max-Age=31536000;    Path=/;  Secure;  SameSite=Lax
Set-Cookie : xSoCu =USD; Max-Age=31536000;    Path=/;  Secure;  SameSite=Lax
```



Path to location of Request

Step	Action	Destination URL
1	Requested http://transfer.paypal.com/	https://transfer.paypal.com/
2	Clicked "Sign Up"	https://transfer.paypal.com/sign-up



#	Host	URL	Status	Passive ...	Active phases	JavaScript ...	Issues	Requests	Errors	Insertion points	Star
1	https://transfer.paypal.com	/	Errors: Skipping ...	1 2	1 2 3 4 5	1 2 3	7	523	4	18	03:5
2	https://transfer.paypal.com	/	Errors: Skipping ...	1 2	1 2 3 4 5	1 2 3	7	589	8	18	03:5
3	https://transfer.paypal.com	/	Errors: Skipping ...	1 2	1 2 3 4 5	1 2 3	6	841	2	18	03:5
4	https://transfer.paypal.com	/sign-up	Errors: Skipping ...	1 2	1 2 3 4 5	1 2 3	11	2502	2	16	03:5
5	https://transfer.paypal.com	/robots.txt	Done	1 2	1 2 3 4 5	1 2 3	4	385		4	03:5
6	https://transfer.paypal.com	/	Errors: Skipping ...	1 2	1 2 3 4 5	1 2 3	6	256	4	3	03:5
7	https://transfer.paypal.com	/sign-in	Done	1 2	1 2 3 4 5	1 2 3	7	4408		16	03:5
8	http://transfer.paypal.com	/	Errors: Skipping ...	1 2	1 2 3 4 5	1 2 3		424	2	3	03:5
9	http://transfer.paypal.com	/robots.txt	Done	1 2	1 2 3 4 5	1 2 3		458		4	03:5

Base request

```
GET /?locale=ko-KR HTTP/2
Host: transfer.paypal.com
Accept-Encoding : gzip, deflate, br
Accept :
text/html,application/xhtml+xml,application/xml;q=0.9,image/av
if,image/webp,image/apng,*/*;q=0.8,application/signed-exchange
;v=b3;q=0.7
Accept-Language : en-US;q=0.9,en;q=0.8
User-Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127
Safari/537.36
Connection : close
Cache-Control : max-age=0
Cookie : _gcl_au=1.1.712969119.1728685170 ; _fbp=
fb.1.1728685170239.398856946 ; ajs_anonymous_id =
598d5b11-d312-4b5c-9012-d5ef25c9a2a5 ; tcs=xoom%3A%7Ca 15
```

Inspector	
Request attributes	2
Request query parameters	1
Request cookies	4
Request headers	13
Response headers	25

2.7 <u>Proposed mitigation or fix</u>

- Input validation.
- Output Encoding.
- Use HTTP-only and secure Cookies.
- Implement a Control Security Policy.
- Avoid unsafe-inline Script and Styles.
- Sanitize HTML.
- Use Framework-Specific XSS Protection.
- Educate Content Regular Security Testing and Developers.