

Sri Lanka Institute of Information Technology



**Missing Secure,HttpOnly,SameSite Flags on
Cookies - Report 10**

IT23187214

Web Security - IE2062

Vulnerability Title:

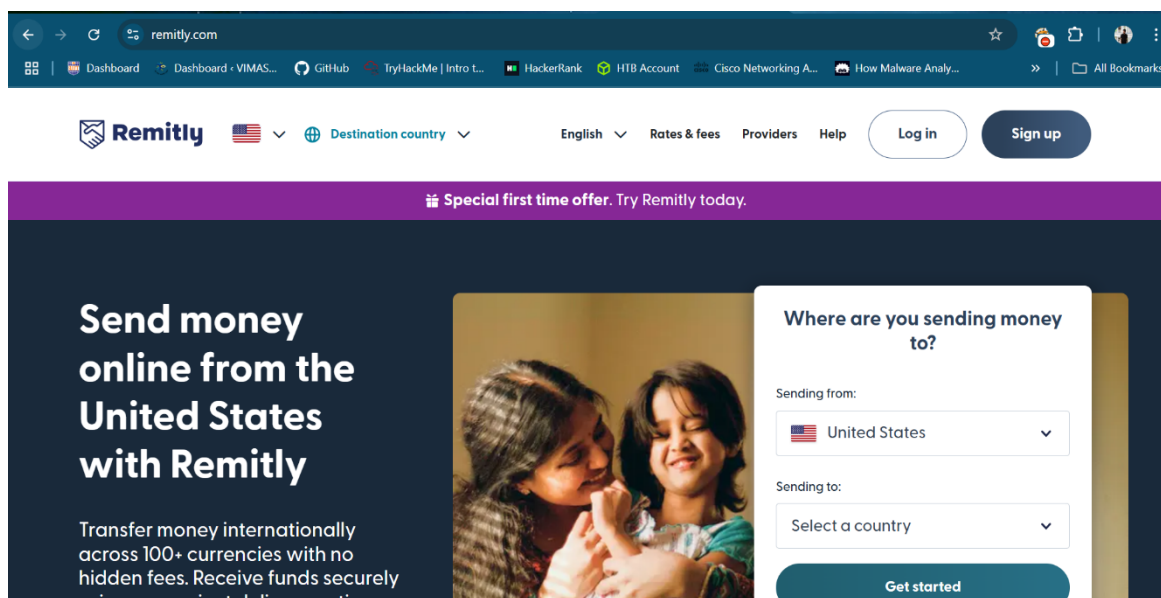
Missing Secure, HttpOnly, SameSite Flags on Cookies

Vulnerability Description:

I found this program on the hackerone Bug hunting website. The website hosted at <https://www.remitly.com>. Session cookies are critical for maintaining authenticated sessions between a user's browser and a web server. If cookies lack the **Secure**, **HttpOnly**, or **SameSite** attributes, they are exposed to multiple security risks:

- **Without Secure:** Cookies can be transmitted over unencrypted HTTP connections, making them vulnerable to interception via Man-in-the-Middle (MITM) attacks.
- **Without HttpOnly:** Cookies can be accessed via JavaScript, increasing the risk of theft through Cross-Site Scripting (XSS) attacks.
- **Without SameSite:** Cookies may be sent in cross-site requests, allowing Cross-Site Request Forgery (CSRF) attacks.

Proper configuration of these cookie attributes is essential to protect user sessions from interception and exploitation.



Affected Components:

- **URL:** <https://www.remitly.com>
- **Cookies Affected:**
 - cookie_consent
 - de_id
 - de_hash
 - pm_sub
 - _policy
 - gr
 - ci_csrf_input
 - HTTP Methods Observed: GET, OPTIONS

Impact Assessment:

- **Risk Level:** Medium

Failure to set Secure, HttpOnly, and SameSite flags can allow attackers to:

- Steal session cookies via JavaScript (if XSS vulnerabilities exist)
- Hijack user sessions through network sniffing on insecure connections
- Launch CSRF attacks to perform unauthorized actions on behalf of the user

If a malicious actor obtains a session cookie, they could impersonate the user and gain unauthorized access to their account or sensitive operations.

Steps to Reproduce:

1. Nikto Scan Results

- Ran Nikto with tuning options to identify web vulnerabilities.
- Discovered multiple cookies set without Secure and HttpOnly flags.

```
(bhr@desktop-2ftqhat) ~/Desktop
$ nikto -h https://www.remitley.com -tuning x 6
- Nikto v2.5.0

+ Multiple IPs found: 52.52.124.58, 54.177.174.82
+ Target IP: 52.52.124.58
+ Target Hostname: www.remitley.com
+ Target Port: 443

+ SSL Info: Subject: /CN=www.remitley.com
Ciphers: TLS_AES_128_GCM_SHA256
Issuer: /C=US/O=Amazon/CN=Amazon RSA 2048 M03
+ Start Time: 2025-04-26 10:50:39 (GMT-5)

+ Server: istio-envoy
+ /: Uncommon header 'origin-agent-cluster' found, with contents: ?1.
+ /: Uncommon header 'x-envoy-upstream-service-time' found, with contents: 126.
+ /: Cookie cookie_consent created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie cookie_consent created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie de_id created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie de_hash created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie ; Max-Age created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie ; Max-Age created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie pm_sub created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie msub_policy created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie ; Path created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: .ilyqs00v: Retrieved access-control-allow-origin header: https://www.remitley.com/.
+ /: .ilyqs00v: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.nets
parker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /: .ilyqs00v: Cookie gr created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ All CGI directories 'found', use '-C none' to test none
+ : Server banner changed from 'istio-envoy' to 'awselb/2.0'.
+ /robots.txt: contains 65 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ /: The Content-Encoding header is set to 'deflate' which may mean that the server is vulnerable to the BREACH attack. See: http://breachattack.com/
+ /: [B][B] /nikto-test-wuZL4Xn.html: Cookie ci_csrf_input created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /nikto-test-wuZL4Xn.html: Cookie ci_csrf_input created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ OPTIONS: Allowed HTTP Methods: GET, HEAD
+ 2063 requests: 0 error(s) and 20 item(s) reported on remote host
+ End Time: 2025-04-26 11:20:36 (GMT-5) (1797 seconds)
```

2. Manual XSS Validation Using JavaScript

- Injected and executed:

alert(document.cookie);
- Verified that cookies like cookie_consent and gr were accessible via JavaScript



3. Header Inspection via Curl

- Inspected response headers:

```
curl -I https://www.remitly.com | grep -i set-cookie
```

- Confirmed that cookies were missing Secure, HttpOnly, and SameSite flags in response.

```
(bhr@desktop-2ftqhat)-[~] desktop
$ curl -I http://www.remitly.com | grep -i set-cookie
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total     Spent    Left     Speed
0 100 100    0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
* Target IP: 53.52.124.56
```

4. Strict-Transport-Security (HSTS) Check

- Verified that HSTS is set:

```
strict-transport-security: max-age=31536000
```

- HTTPS is enforced, but cookies still need Secure/HttpOnly/SameSite individually for full protection.

```
(bhr@desktop-2ftqhat)-[~] fly.com
$ curl -I https://www.remitly.com | grep -i strict-transport-security
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total     Spent    Left     Speed
0 100 100    0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
* SSL-Session: Subject: CN=DigiCert SHA2 Extended Validation Code Signing CA
strict-transport-security: max-age=15552000; includeSubDomains NO3
strict-transport-security: max-age=31536000; includeSubDomains NO3
```

Proof of Concept (PoC):

1. Captured Cookies without Security Flags:

Set-Cookie: cookie_consent=value; path=/;

Set-Cookie: de_id=value; path=/;

Set-Cookie: gr=value; path=/;

2. Manual JavaScript Execution:

```
alert(document.cookie);
```

3. Observed Behavior:

- Cookies were readable via JavaScript, confirming that **HttpOnly** flag is missing.
- Cookies could theoretically be stolen if an XSS vulnerability existed.
- Secure flag missing on some cookies allows possible interception under certain conditions if not properly encrypted.

Proposed Mitigation or Fix:

To address the missing cookie security attributes:

1. Set the Secure Flag:

Ensure that all cookies are set with the Secure attribute, so they are transmitted only over HTTPS:

Set-Cookie: cookie_name=value; Secure

2. Set the HttpOnly Flag:

Prevent client-side scripts from accessing cookies by adding HttpOnly:

Set-Cookie: cookie_name=value; HttpOnly

3. Set the SameSite Attribute:

Mitigate CSRF attacks by using SameSite=Lax or SameSite=Strict:

Set-Cookie: cookie_name=value; SameSite=Lax

4. Conduct Regular Security Reviews:

Regularly audit cookie settings in all web applications to ensure security best practices are applied across environments.

5. Update Application Configuration:

Ensure that the server-side cookie setting mechanisms (application code, web server config) apply these attributes by default.

6. Apply Secure Defaults:

Frameworks or load balancers should enforce Secure and HttpOnly settings wherever possible.

7. Use environment-based secrets handling systems such as Vault, AWS Secrets Manager, or .env files outside of the building process.

Conclusion:

A few cookies set by <https://www.remitly.com> are missing important security attributes (Secure, HttpOnly, and SameSite). Manual testing confirmed that cookies were accessible via client-side scripts, exposing users to elevated risks like session hijacking and CSRF. Although HTTPS (HSTS) is enforced, cookies must be individually secured to prevent client-side exploitation.