**Sri Lanka Institute of Information Technology**

**IE2062 - Web Security**

**Final Assignment**

**Bug Bounty Report 03**

**Name:** Peiris W.S.S.N

**Registration Number:** IT23227286

Contents

[**1.** **Introduction** 3](#_Toc197095111)

[**2.** **Reconnaissance** 3](#_Toc197095112)

[**3.** **Vulnerability** 5](#_Toc197095113)

[**4.** **Vulnerability description** 5](#_Toc197095114)

[**5.** **Affected Components** 6](#_Toc197095115)

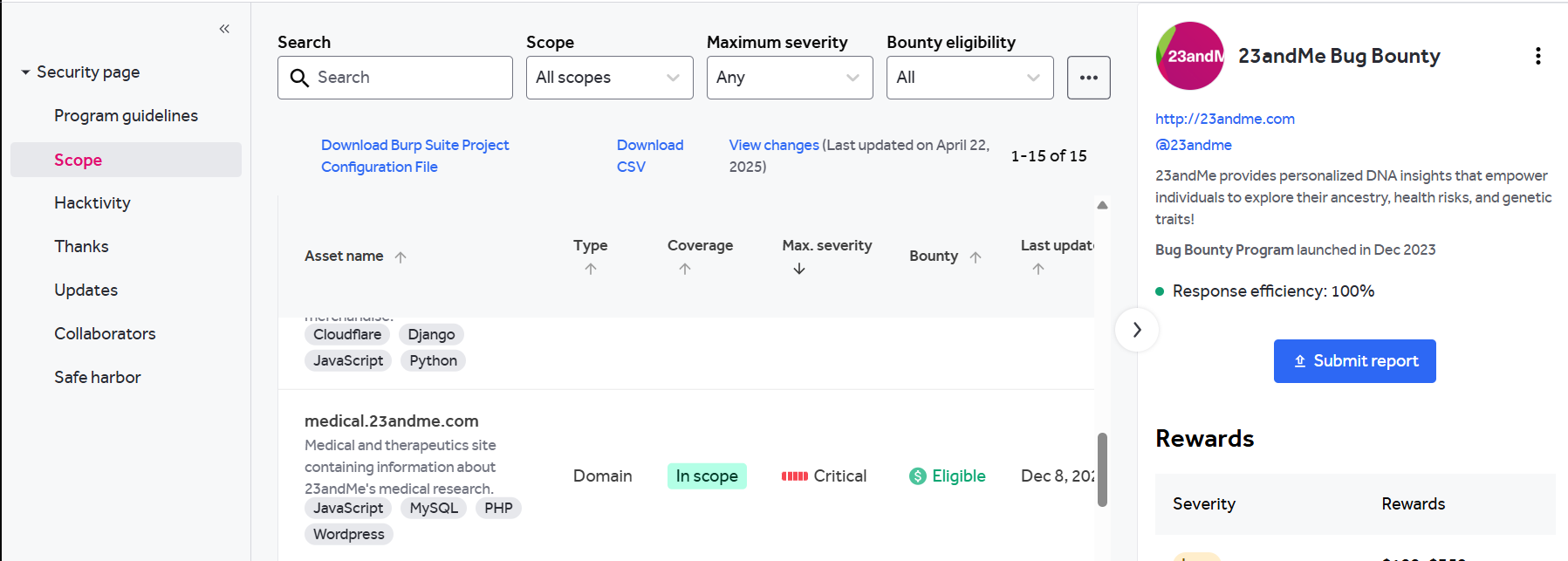
[**6.** **Impact Assessment** 6](#_Toc197095116)

[**7.** **Steps to reproduce** 7](#_Toc197095117)

[**8.** **Proof of concept** 8](#_Toc197095118)

[**9.** **Proposed mitigation or fix** 8](#_Toc197095119)

# **Introduction**

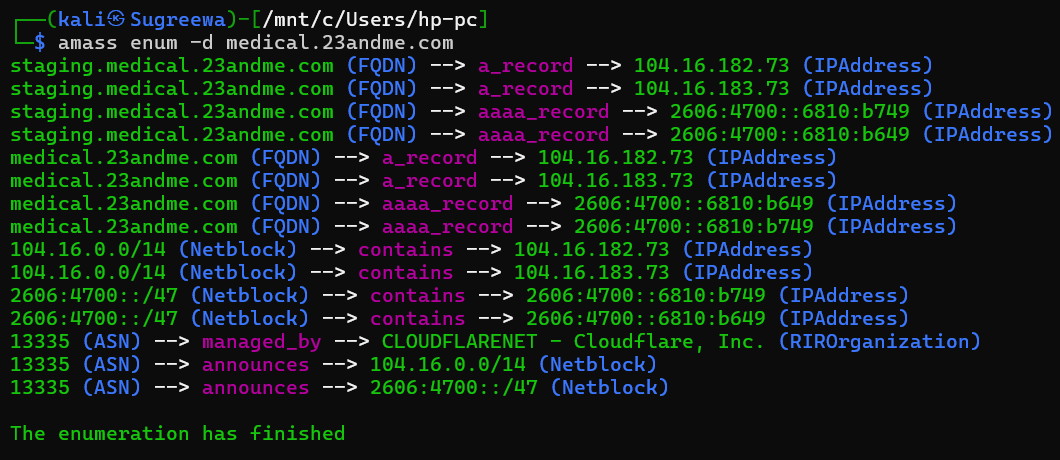


**Website:** <https://medical.23andme.com/>

**Listed by:** 23andMe Bug Bounty

# **Reconnaissance**

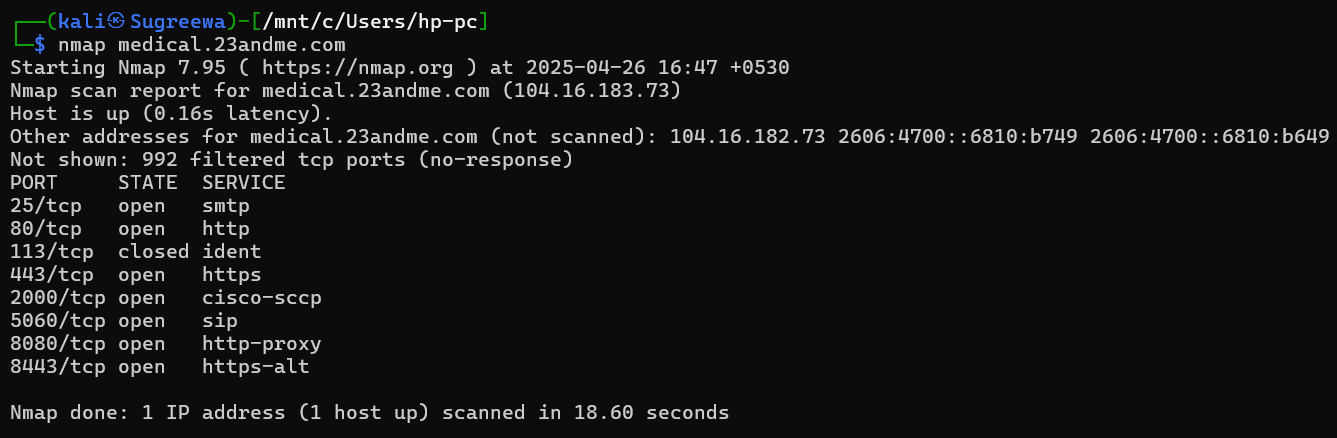
* **Subdomain enumeration using Amass**

****

* **Firewall Detection**

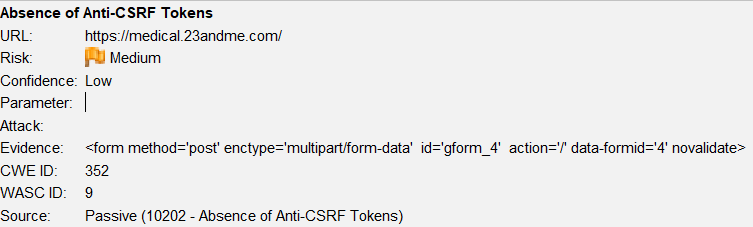
****

* **Nmap Scan**



# **Vulnerability**

* **Absence of Anti-CSRF Tokens**

****

# **Vulnerability description**

No Anti-CSRF tokens were found in a HTML submission form.

A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf.

* CSRF attacks are effective in a number of situations, including:
* The victim has an active session on the target site.
* The victim is authenticated via HTTP auth on the target site.
* The victim is on the same local network as the target site.

CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.

1. **Affected Components**

* **Form ID:** gform\_4
* **Form Method:** POST
* **Endpoint:** /
* **Content Type:** multipart/form-data
* **Missing Security Elements:** No known anti-CSRF token detected (e.g., csrf\_token, \_csrf, CSRFToken, etc.)
* **Form Fields Involved:** gform\_field\_values, gform\_submit, gform\_submit\_button\_4, input\_4\_1, state\_4, etc.

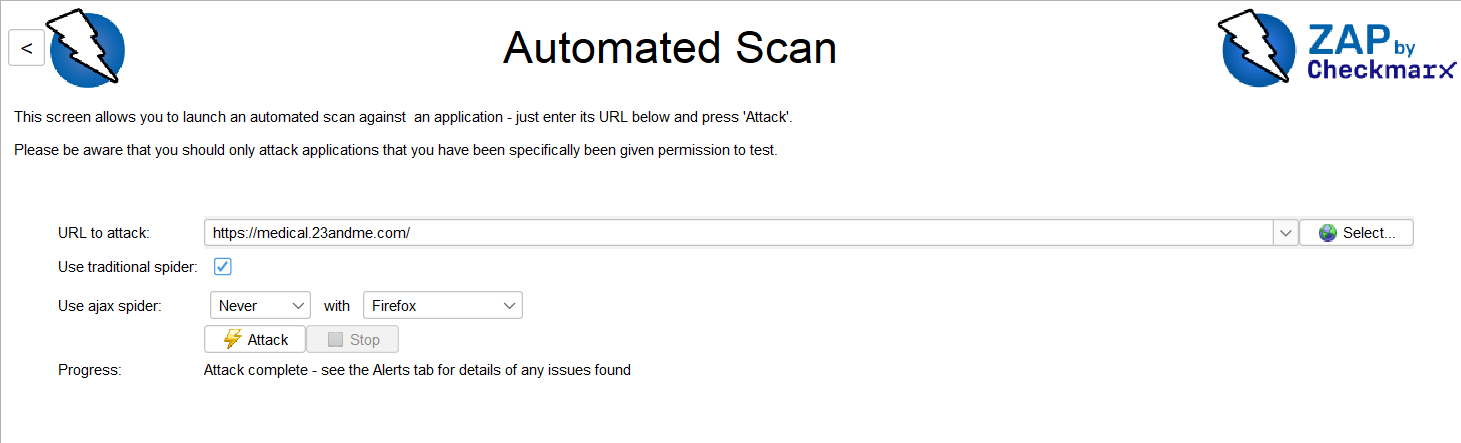
# **Impact Assessment**

**Risk Level:** Medium

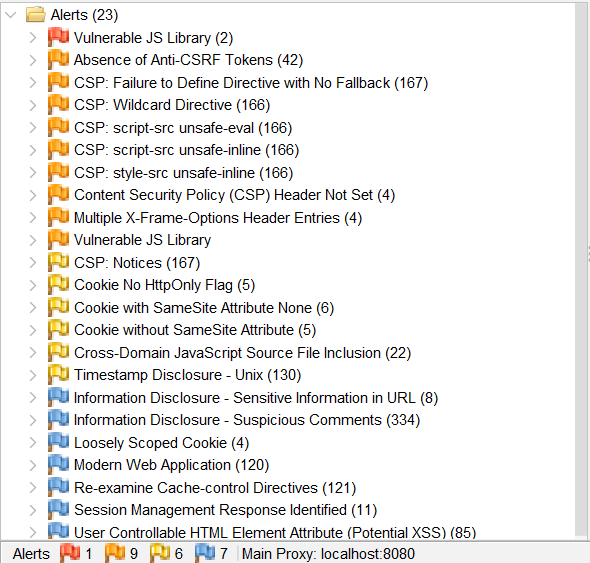
**Impacts:**

* Unauthorized transactions or actions (e.g., form submissions, state changes)
* Data leakage or manipulation
* Account hijacking (if combined with XSS)
* Potential for privilege escalation and session abuse

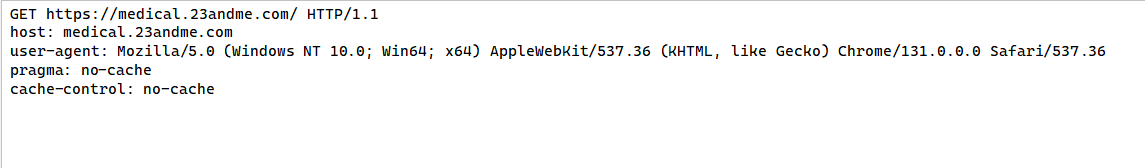
# **Steps to reproduce**

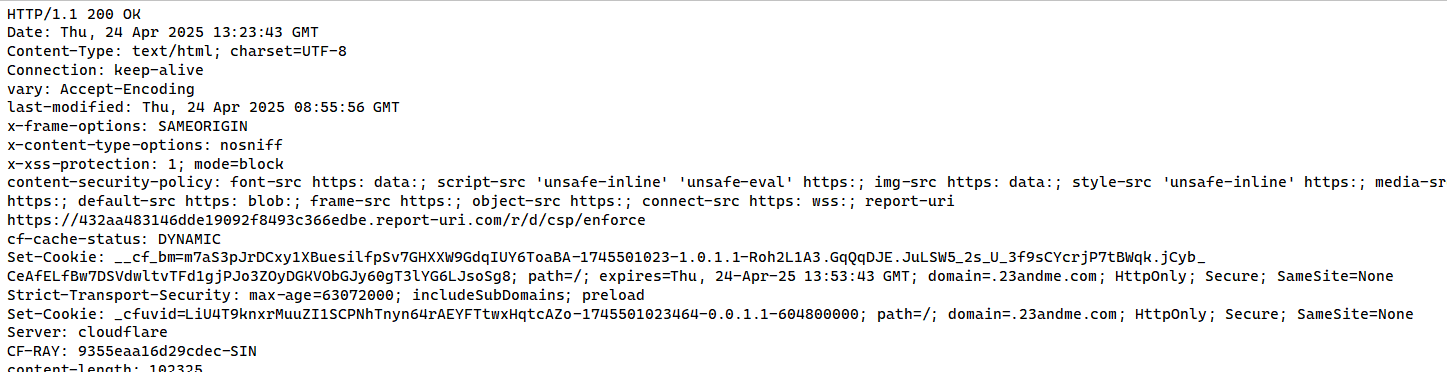


Perform a scan with Zap’s automated scan and go to the alerts tab.



# **Proof of concept**





# **Proposed mitigation or fix**

**Phase: Architecture and Design**

Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid. For example, use anti-CSRF packages such as the OWASP CSRFGuard.

**Phase: Implementation**

Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script.

**Phase: Architecture and Design**

Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable (CWE-330). Note that this can be bypassed using XSS. Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to perform that operation. Note that this can be bypassed using XSS.

Use the ESAPI Session Management control. This control includes a component for CSRF. Do not use the GET method for any request that triggers a state change.

**Phase: Implementation**

Check the HTTP Referer header to see if the request originated from an expected page. This could break legitimate functionality, because users or proxies may have disabled sending the Referer for privacy reasons.