Sri Lanka Institute of Information Technology

IE2062 - Web Security

Final Assignment

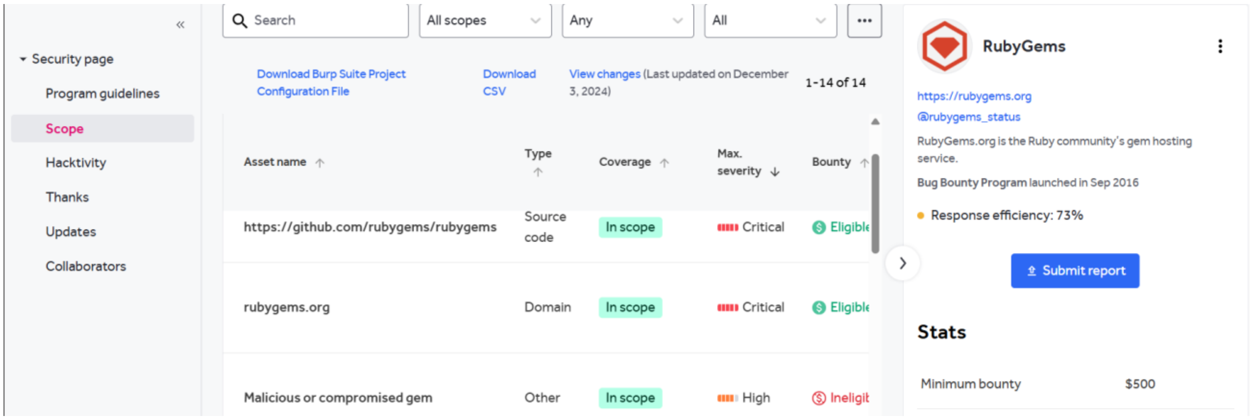
Bug Bounty Report 04

Name: Peiris W.S.S.N

Registration Number: IT23227286

Contents

1. Introduction



RubyGems.org is the Ruby community's gem hosting service.

Bug Bounty Program launched in Sep 2016

Response efficiency: 73%

Asset name ↑	Type ↑	Coverage ↑	Max. severity ↓	Bounty ↑
https://github.com/rubygems/rubygems	Source code	In scope	Critical	Eligible
rubygems.org	Domain	In scope	Critical	Eligible
Malicious or compromised gem	Other	In scope	High	Ineligit

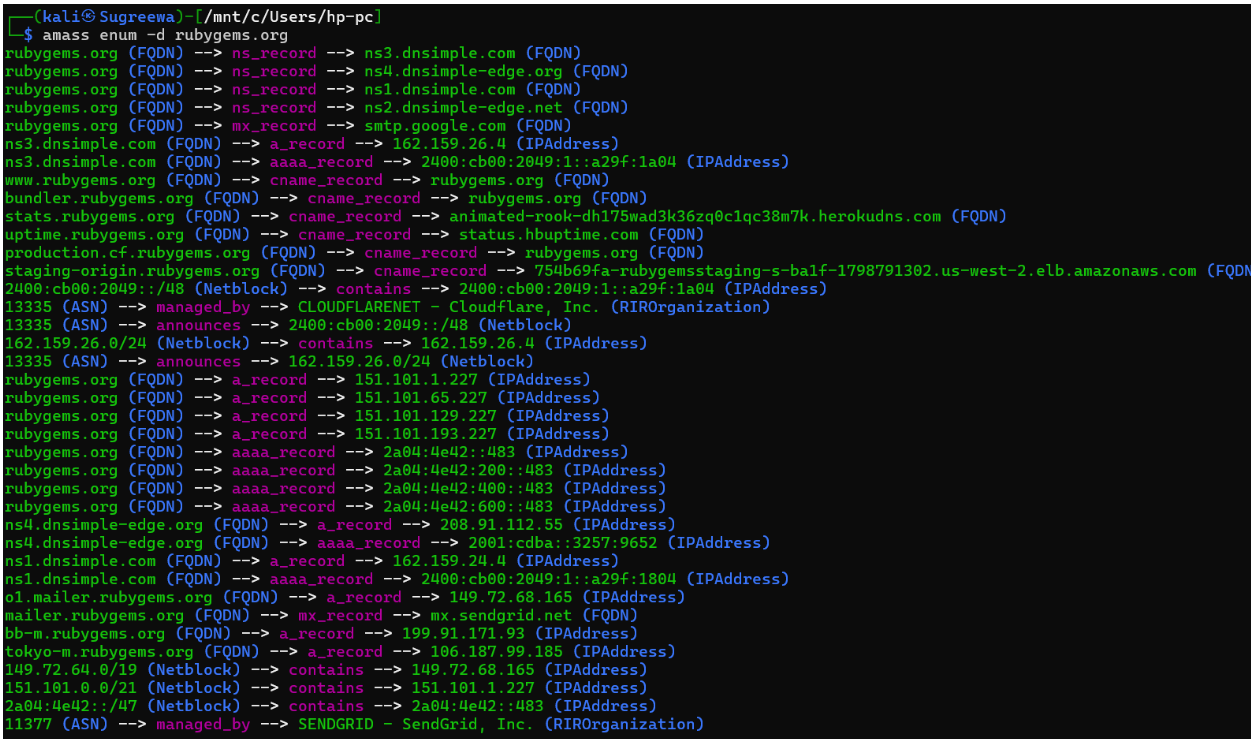
Minimum bounty	$500

Website: https://rubygems.org/

Listed by: RubyGems

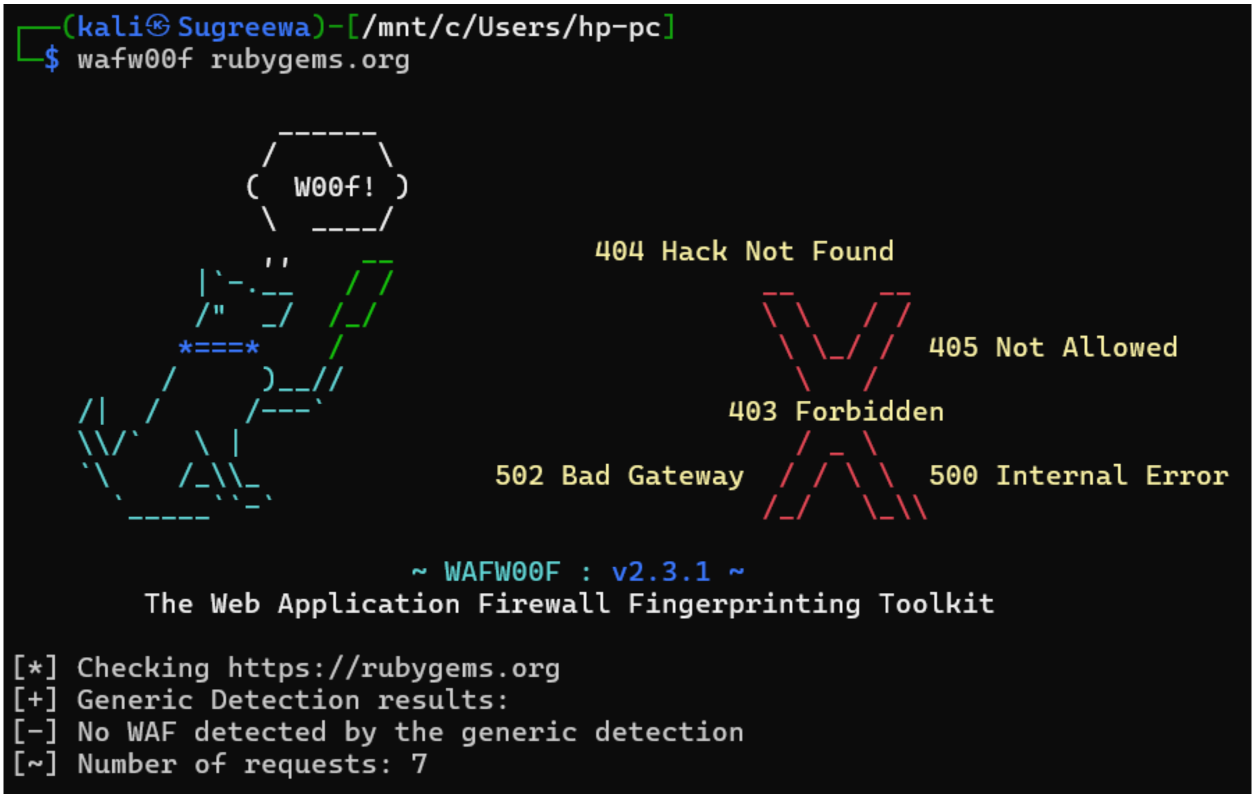
2. Reconnaissance

- **Subdomain enumeration using Amass**



```
┌──(kali㉿Sugreewa)-[/mnt/c/Users/hp-pc]
└─$ amass enum -d rubygems.org
rubygems.org (FQDN) --> ns_record --> ns3.dnsimple.com (FQDN)
rubygems.org (FQDN) --> ns_record --> ns4.dnsimple-edge.org (FQDN)
rubygems.org (FQDN) --> ns_record --> ns1.dnsimple.com (FQDN)
rubygems.org (FQDN) --> ns_record --> ns2.dnsimple-edge.net (FQDN)
rubygems.org (FQDN) --> mx_record --> smtp.google.com (FQDN)
ns3.dnsimple.com (FQDN) --> a_record --> 162.159.26.4 (IPAddress)
ns3.dnsimple.com (FQDN) --> aaaa_record --> 2400:cb00:2049:1::a29f:1a04 (IPAddress)
www.rubygems.org (FQDN) --> cname_record --> rubygems.org (FQDN)
bundler.rubygems.org (FQDN) --> cname_record --> rubygems.org (FQDN)
stats.rubygems.org (FQDN) --> cname_record --> animated-rook-dh175wad3k36zq0c1qc38m7k.herokudns.com (FQDN)
uptime.rubygems.org (FQDN) --> cname_record --> status.hbuptime.com (FQDN)
production.cf.rubygems.org (FQDN) --> cname_record --> rubygems.org (FQDN)
staging-origin.rubygems.org (FQDN) --> cname_record --> 754b69fa-rubygemsstaging-s-ba1f-1798791302.us-west-2.elb.amazonaws.com (FQDN
2400:cb00:2049::/48 (Netblock) --> contains --> 2400:cb00:2049:1::a29f:1a04 (IPAddress)
13335 (ASN) --> managed_by --> CLOUDFLARENET - Cloudflare, Inc. (RIROrganization)
13335 (ASN) --> announces --> 2400:cb00:2049::/48 (Netblock)
162.159.26.0/24 (Netblock) --> contains --> 162.159.26.4 (IPAddress)
13335 (ASN) --> announces --> 162.159.26.0/24 (Netblock)
rubygems.org (FQDN) --> a_record --> 151.101.1.227 (IPAddress)
rubygems.org (FQDN) --> a_record --> 151.101.65.227 (IPAddress)
rubygems.org (FQDN) --> a_record --> 151.101.129.227 (IPAddress)
rubygems.org (FQDN) --> a_record --> 151.101.193.227 (IPAddress)
rubygems.org (FQDN) --> aaaa_record --> 2a04:4e42::483 (IPAddress)
rubygems.org (FQDN) --> aaaa_record --> 2a04:4e42:200::483 (IPAddress)
rubygems.org (FQDN) --> aaaa_record --> 2a04:4e42:400::483 (IPAddress)
rubygems.org (FQDN) --> aaaa_record --> 2a04:4e42:600::483 (IPAddress)
ns4.dnsimple-edge.org (FQDN) --> a_record --> 208.91.112.55 (IPAddress)
ns4.dnsimple-edge.org (FQDN) --> aaaa_record --> 2001:cdba::3257:9652 (IPAddress)
ns1.dnsimple.com (FQDN) --> a_record --> 162.159.24.4 (IPAddress)
ns1.dnsimple.com (FQDN) --> aaaa_record --> 2400:cb00:2049:1::a29f:1804 (IPAddress)
o1.mailer.rubygems.org (FQDN) --> a_record --> 149.72.68.165 (IPAddress)
mailer.rubygems.org (FQDN) --> mx_record --> mx.sendgrid.net (FQDN)
bb-m.rubygems.org (FQDN) --> a_record --> 199.91.171.93 (IPAddress)
tokyo-m.rubygems.org (FQDN) --> a_record --> 106.187.99.185 (IPAddress)
149.72.64.0/19 (Netblock) --> contains --> 149.72.68.165 (IPAddress)
151.101.0.0/21 (Netblock) --> contains --> 151.101.1.227 (IPAddress)
2a04:4e42::/47 (Netblock) --> contains --> 2a04:4e42::483 (IPAddress)
11377 (ASN) --> managed_by --> SENDGRID - SendGrid, Inc. (RIROrganization)
```

- **Firewall Detection**



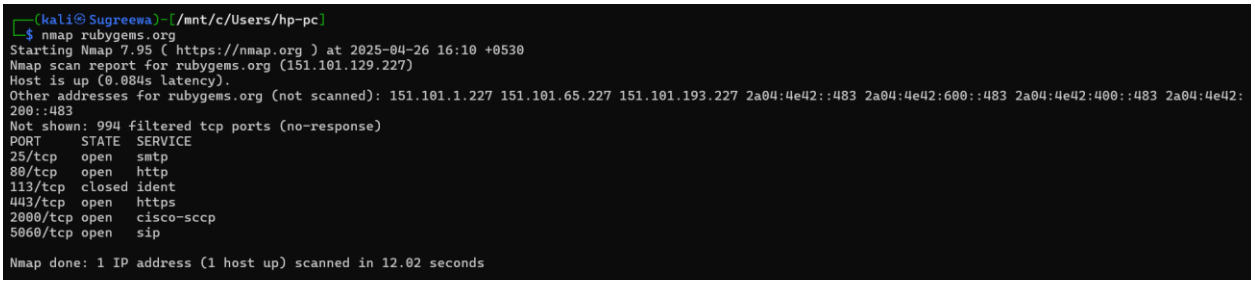
```
┌──(kali㉿Sugreewa)-[/mnt/c/Users/hp-pc]
└─$ wafw00f rubygems.org

                  (  W00f! )
                                        404 Hack Not Found
                                                       405 Not Allowed
                                              403 Forbidden
                                   502 Bad Gateway            500 Internal Error

                    ~ WAFW00F : v2.3.1 ~
        The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://rubygems.org
[+] Generic Detection results:
[-] No WAF detected by the generic detection
[~] Number of requests: 7
```

- **Nmap Scan**

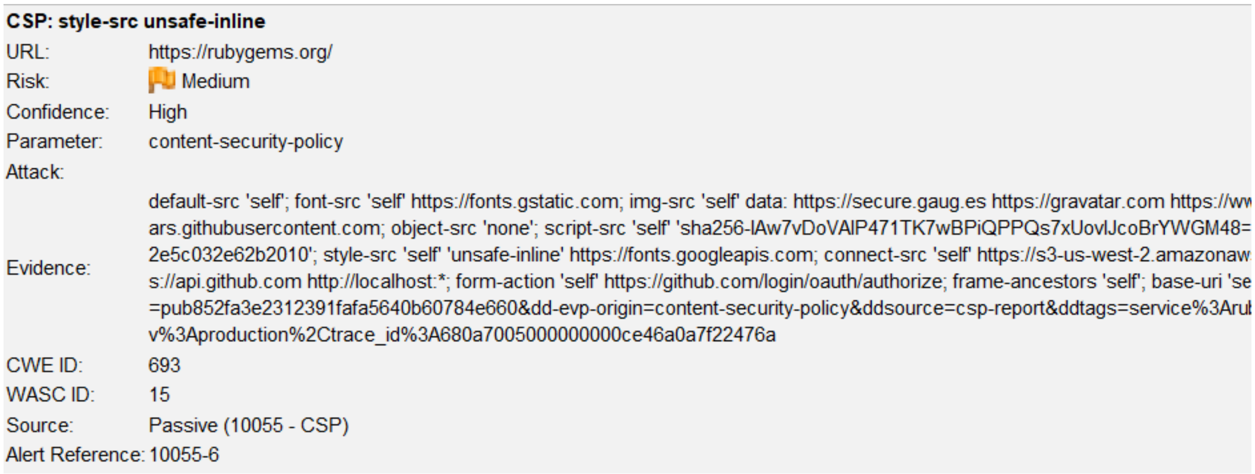


```
┌──(kali㉿Sugreewa)-[/mnt/c/Users/hp-pc]
└─$ nmap rubygems.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-26 16:10 +0530
Nmap scan report for rubygems.org (151.101.129.227)
Host is up (0.084s latency).
Other addresses for rubygems.org (not scanned): 151.101.1.227 151.101.65.227 151.101.193.227 2a04:4e42::483 2a04:4e42:600::483 2a04:4e42:400::483 2a04:4e42:
200::483
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE  SERVICE
25/tcp   open   smtp
80/tcp   open   http
113/tcp  closed ident
443/tcp  open   https
2000/tcp open   cisco-sccp
5060/tcp open   sip

Nmap done: 1 IP address (1 host up) scanned in 12.02 seconds
```

3. Vulnerability

- **CSP: style-src unsafe-inline**



```
CSP: style-src unsafe-inline
URL:             https://rubygems.org/
Risk:            Medium
Confidence:      High
Parameter:       content-security-policy
Attack:
                 default-src 'self'; font-src 'self' https://fonts.gstatic.com; img-src 'self' data: https://secure.gaug.es https://gravatar.com https://ww
                 ars.githubusercontent.com; object-src 'none'; script-src 'self' 'sha256-lAw7vDoVAlP471TK7wBPiQPPQs7xUovlJcoBrYWGM48=
Evidence:        2e5c032e62b2010'; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com; connect-src 'self' https://s3-us-west-2.amazonaw
                 s://api.github.com http://localhost:*; form-action 'self' https://github.com/login/oauth/authorize; frame-ancestors 'self'; base-uri 'se
                 =pub852fa3e2312391fafa5640b60784e660&dd-evp-origin=content-security-policy&ddsource=csp-report&ddtags=service%3Arub
                 v%3Aproduction%2Ctrace_id%3A680a7005000000000ce46a0a7f22476a
CWE ID:          693
WASC ID:         15
Source:          Passive (10055 - CSP)
Alert Reference: 10055-6
```

4. Vulnerability description

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) Cross Site Scripting (XSS), and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files

5. Affected Components

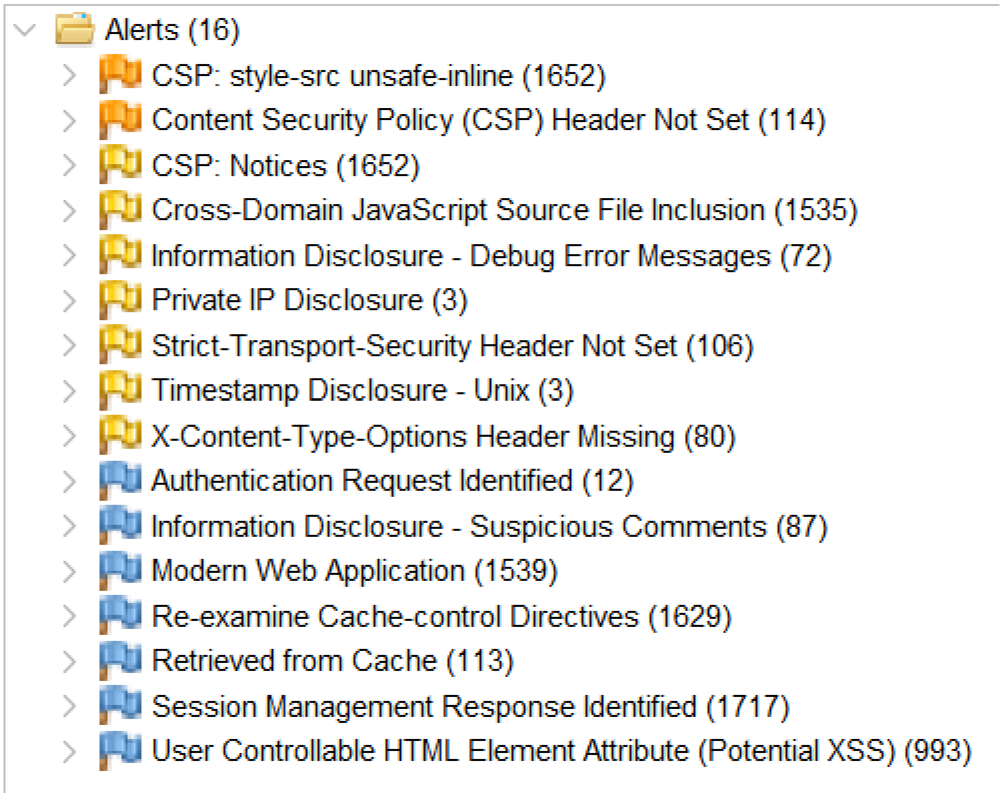
- **Component:** HTTP Response Header → Content-Security-Policy
- **Directive Affected:** style-src
- **Policy:** style-src 'self' 'unsafe-inline' https://fonts.googleapis.com;
- **Impacted Pages:** All responses where this CSP header is set.

6. Impact Assessment

- **Risk Level:** Medium to High (depending on other security controls in place)
- **Potential Impacts:**
  - Allows inline style injection (e.g., via HTML attributes like style="...")
  - May aid in **style-based XSS** or **UI redressing attacks**
  - Reduces defense-in-depth protections against content injection

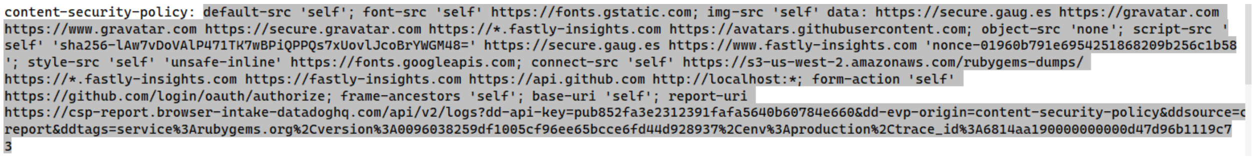
7. Steps to reproduce

- Use ZAP or browser DevTools to inspect the HTTP response headers from the target site.



```
Alerts (16)
    CSP: style-src unsafe-inline (1652)
    Content Security Policy (CSP) Header Not Set (114)
    CSP: Notices (1652)
    Cross-Domain JavaScript Source File Inclusion (1535)
    Information Disclosure - Debug Error Messages (72)
    Private IP Disclosure (3)
    Strict-Transport-Security Header Not Set (106)
    Timestamp Disclosure - Unix (3)
    X-Content-Type-Options Header Missing (80)
    Authentication Request Identified (12)
    Information Disclosure - Suspicious Comments (87)
    Modern Web Application (1539)
    Re-examine Cache-control Directives (1629)
    Retrieved from Cache (113)
    Session Management Response Identified (1717)
    User Controllable HTML Element Attribute (Potential XSS) (993)
```

- Identify the Content-Security-Policy header.



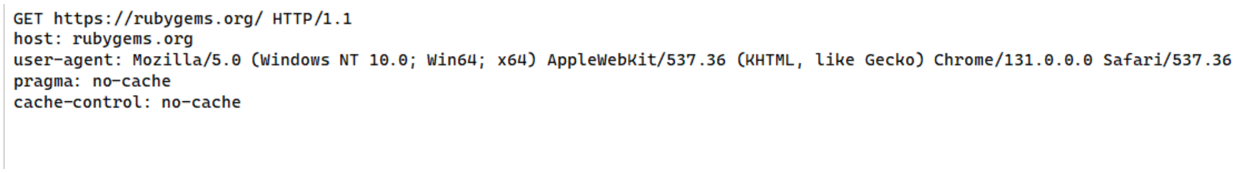
```
content-security-policy: default-src 'self'; font-src 'self' https://fonts.gstatic.com; img-src 'self' data: https://secure.gaug.es https://gravatar.com
https://www.gravatar.com https://secure.gravatar.com https://*.fastly-insights.com https://avatars.githubusercontent.com; object-src 'none'; script-src '
self' 'sha256-lAw7vDoVAlP471TK7wBPiQPPQs7xUovlJcoBrYWGM48=' https://secure.gaug.es https://www.fastly-insights.com 'nonce-01960b791e6954251868209b256c1b58
'; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com; connect-src 'self' https://s3-us-west-2.amazonaws.com/rubygems-dumps/
https://*.fastly-insights.com https://fastly-insights.com https://api.github.com http://localhost:*; form-action 'self'
https://github.com/login/oauth/authorize; frame-ancestors 'self'; base-uri 'self'; report-uri
https://csp-report.browser-intake-datadoghq.com/api/v2/logs?dd-api-key=pub852fa3e2312391fafa5640b60784e660&dd-evp-origin=content-security-policy&ddsource=c
report&ddtags=service%3Arubygems.org%2Cversion%3A0096038259df1005cf96ee65bcce6fd44d928937%2Cenv%3Aproduction%2Ctrace_id%3A6814aa190000000000d47d96b1119c7
3
```

- Confirm that the style-src directive includes 'unsafe-inline'.

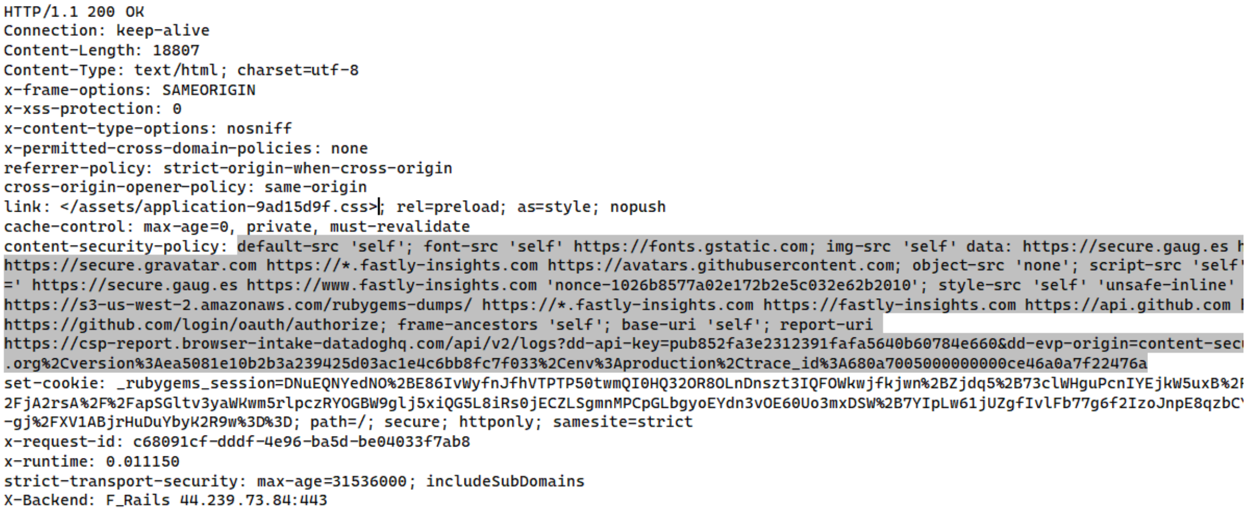
<p style="color: red; font-weight: bold;">This is a test of inline styles.</p>

- Optionally, test whether inline styles are accepted by injecting a simple HTML snippet with a style attribute.

8. Proof of concept



```
GET https://rubygems.org/ HTTP/1.1
host: rubygems.org
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36
pragma: no-cache
cache-control: no-cache
```



```
HTTP/1.1 200 OK
Connection: keep-alive
Content-Length: 18807
Content-Type: text/html; charset=utf-8
x-frame-options: SAMEORIGIN
x-xss-protection: 0
x-content-type-options: nosniff
x-permitted-cross-domain-policies: none
referrer-policy: strict-origin-when-cross-origin
cross-origin-opener-policy: same-origin
link: </assets/application-9ad15d9f.css>; rel=preload; as=style; nopush
cache-control: max-age=0, private, must-revalidate
content-security-policy: default-src 'self'; font-src 'self' https://fonts.gstatic.com; img-src 'self' data: https://secure.gaug.es h
https://secure.gravatar.com https://*.fastly-insights.com https://avatars.githubusercontent.com; object-src 'none'; script-src 'self'
=' https://secure.gaug.es https://www.fastly-insights.com 'nonce-1026b8577a02e172b2e5c032e62b2010'; style-src 'self' 'unsafe-inline'
https://s3-us-west-2.amazonaws.com/rubygems-dumps/ https://*.fastly-insights.com https://fastly-insights.com https://api.github.com h
https://github.com/login/oauth/authorize; frame-ancestors 'self'; base-uri 'self'; report-uri
https://csp-report.browser-intake-datadoghq.com/api/v2/logs?dd-api-key=pub852fa3e2312391fafa5640b60784e660&dd-evp-origin=content-sec
.org%2Cversion%3Aea5081e10b2b3a239425d03ac1e4c6bb8fc7f033%2Cenv%3Aproduction%2Ctrace_id%3A680a7005000000000ce46a0a7f22476a
set-cookie: _rubygems_session=DNuEQNYedNO%2BE86IvWyfnJfhVTPTP50twmQI0HQ32OR8OLnDnszt3IQFOWkwjfkjwn%2BZjdq5%2B73clWHguPcnIYEjkW5uxB%2F
2FjA2rsA%2F%2FapSGltv3yaWKwm5rlpczRYOGBW9glj5xiQG5L8iRs0jECZLSgmnMPCpGLbgyoEYdn3vOE60Uo3mxDSW%2B7YIpLw61jUZgfIvlFb77g6f2IzoJnpE8qzbC
-gj%2FXV1ABjrHuDuYbyK2R9w%3D%3D; path=/; secure; httponly; samesite=strict
x-request-id: c68091cf-dddf-4e96-ba5d-be04033f7ab8
x-runtime: 0.011150
strict-transport-security: max-age=31536000; includeSubDomains
X-Backend: F_Rails 44.239.73.84:443
```

9. Proposed mitigation or fix

Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.