

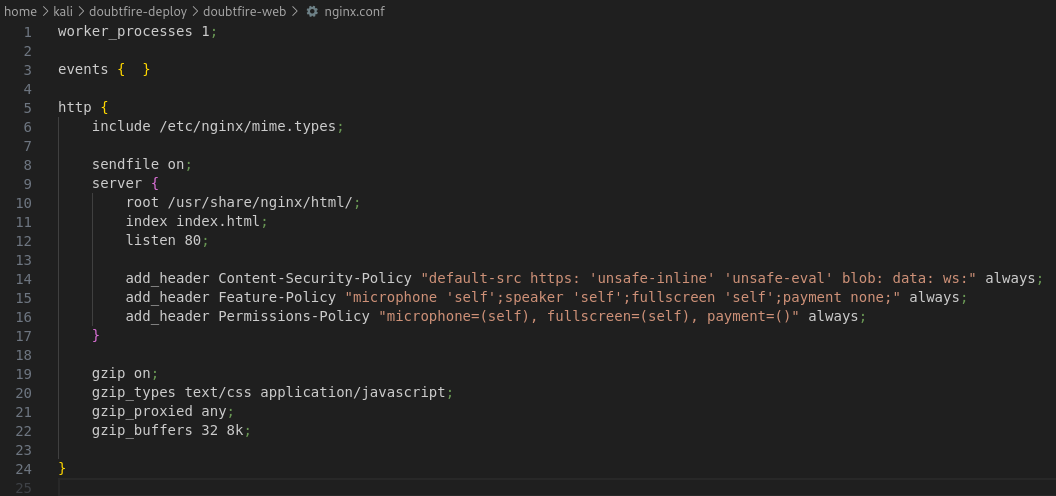
**Finding Name:** Content Security Policy Wildcard Directive

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Team** | **Role** | **Project** | **Quality Assurance** | **Is this a re-tested Finding?** |
| Deakin Carr | SCR | Secure Code Reviewer | Ontrack | Natalia Khobotova | Yes |
|  |  |  |  |  |  |

|  |
| --- |
| **Was this Finding Successful?** |
| Yes |

**Finding Description**

The application’s web server uses a Content Security Policy (CSP) with wildcard directives (default-src https:) that include unsafe sources such as 'unsafe-inline' and 'unsafe-eval'. This configuration allows the execution of inline scripts and evaluation of strings as code, which can lead to Cross-Site Scripting (XSS) attacks and other injection-based vulnerabilities.



**Risk Rating**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **mpact values** | | | | |
| **Very Minor** | **Minor** | **Significant** | **Major** | **Severe** |
| Risk that holds little to no impact. Will not cause damage and regular activity can continue. | Risk that holds minor form of impact, but not significant enough to be of threat. Can cause some damage but not enough to impede regular activity. | Risk that holds enough impact to be somewhat of a threat. Will cause damage that can impede regular activity but will be able to run normally. | Risk that holds major impact to be of threat. Will cause damage that will impede regular activity and will not be able to run normally. | Risk that holds severe impact and is a threat. Will cause critical damage that can cease activity to be run. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Likelihood** | | | | |
| **Rare** | **Unlikely** | **Moderate** | **High** | **Certain** |
| Event may occur and/or if it did, it happens in specific circumstances. | Event could occur occasionally and/or could happen (at some point) | Event may occur and/or happens. | Event occurs at times and/or probably happens a lot. | Event is occurring now and/or happens frequently. |

**Business Impact**

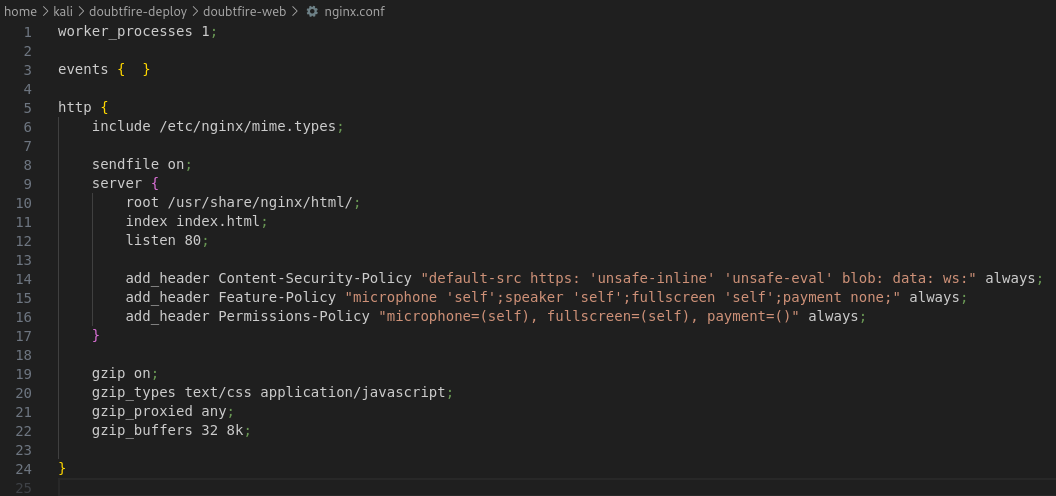
An overly permissive CSP can severely undermine the application's security posture by allowing attackers to execute malicious scripts. This can lead to sensitive data exposure, session hijacking, and persistent attacks affecting all users. The integrity and confidentiality of the application are at risk, potentially harming the organization's reputation and causing financial and legal ramifications.

**Affected Assets**

The main web application, particularly the front-end where the CSP is enforced. This includes all pages served under the domain where the CSP with the wildcard directive is applied.

**Evidence**

The overly permissive configuration can be found at /home/kali/doubtfire-deploy/doubtfire-web/nginx.conf



**Remediation Advice**

* Remove the 'unsafe-inline' and 'unsafe-eval' options from the CSP to prevent the execution of arbitrary inline scripts and code evaluation.
* Define specific source directives for scripts, styles, images, etc., such as script-src 'self'; style-src 'self'; img-src 'self';
* Implement restrictive frame-ancestors and form-action directives, e.g., frame-ancestors 'none'; form-action 'self'; to control where content can be framed from and where forms can submit data.
* Regularly review and update the CSP to adapt to new security practices and requirements.

**References**

O. ELFarsaoui, “How to configure Security Headers in Nginx,” FAUN — Developer Community, Available [How to configure Security Headers in Nginx | by Omar ELFarsaoui | FAUN — Developer Community 🐾](https://faun.pub/how-to-configure-security-headers-in-nginx-aac883201ff2) [Accessed: 10/4/2024]

ChatGPT, “ChatGPT”, OpenAI [Large language model] Available: <https://chat.openai.com> [Accessed: 2/4/2024].

OWASP, "OWASP Zed Attack Proxy (ZAP)," OWASP Foundation, [Online]. Available: <https://www.zaproxy.org/>. [Accessed: 2/4/2024].

**Contact Details**

* Deakin Carr
* Carrde@deakin.edu.au

**Pentest Leader Feedback.**

Hi Deakin, thanks for submitting this finding. Excellent work – great finding! There are no comments from me regarding the vulnerability. However, I noticed that a couple of the reference links are generic and do not provide relevant information about the finding or the remediation process. Please update the reference links to include resources that relate to the vulnerability and/or its resolution.  
  
Updated: Thank you for updating the references. I don’t think any further changes are required. Well done!