

**Finding Name:** Unencrypted Communications.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Team** | **Role** | **Project** | **Quality Assurance** | **Is this a re-tested Finding?** |
| Mohammad Nouri | PT | Junior Team Member | Ontrack | Nabiha Masood and Oliver Power |  |
|  |  |  |  |  |  |

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

**Finding Description**

Information leakage via port 3306

The information leakage, displaying Maria DB (database) versions on an open port (port 3306), poses a potential security risk. Attackers can exploit this information in reconnaissance activities to identify known vulnerabilities associated with the disclosed software versions. This could facilitate unauthorized access, data breaches, or other malicious actions.

**Risk Rating**  
Impact: Minor  
Likelihood: Moderate

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Impact 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**

The foremost impact is the security risk posed by exposing sensitive information. Attackers could exploit this information to identify known vulnerabilities associated with specific versions of Ruby and Rails. This could potentially lead to unauthorized access, data breaches, or other malicious activities, putting both the company's data and its users' information at risk.

If a vulnerability is found and exploited, it could lead to significant reputation damage for the company. Users will lose trust in the company's ability to protect their data, resulting in decreased confidence in the application and potentially leading to loss of business and negative publicity.

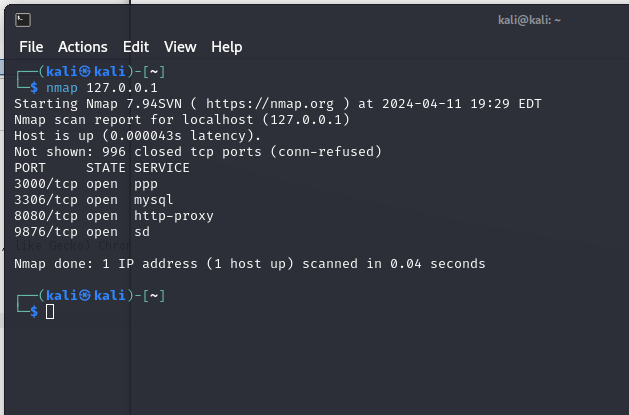
**Affected Assets**

The backend of the web application is affected.

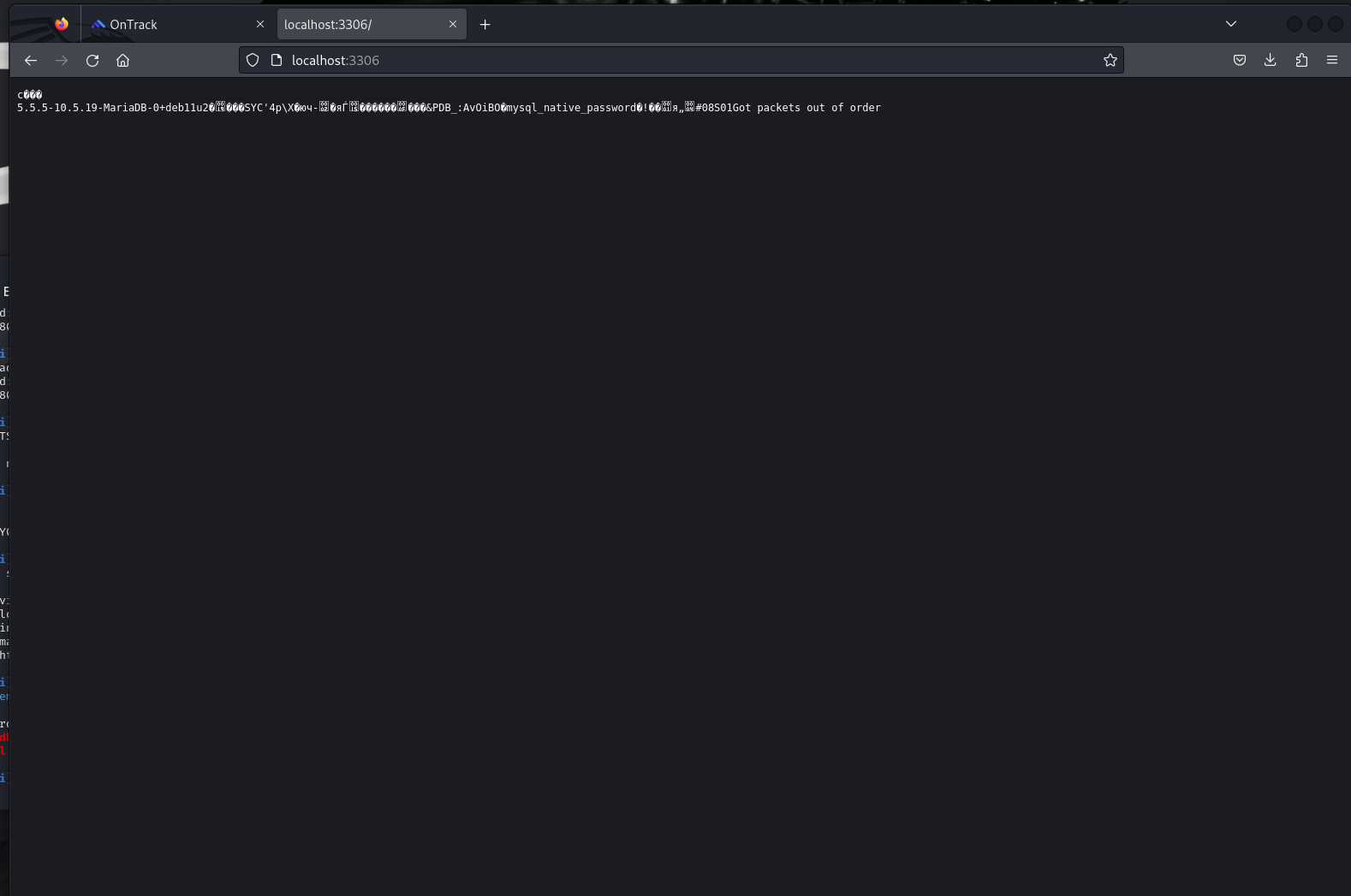
**Evidence**

Once the application is setup and running via vscode.

I ran an Nmap scan to check for open ports:



After the scan I visited <http://localhost:3306> and the following page loaded with the information:



**Remediation Advice**

Implement Access Controls: Restrict access to sensitive information by implementing access controls. This can involve configuring firewalls, web server settings, or application-level access controls to limit access to the port displaying version information. Only trusted IP addresses or authorized users should be allowed to access this information.

**References**

**Contact Details**

MOHAMMAD NOURI mnouri@deakin.edu.au

**Pentest Leader Feedback.**

The lead will provide feedback to enact on.