

**Finding Name:** Unencrypted Communications.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Team** | **Role** | **Project** | **Quality Assurance** | **Is this a re-tested Finding?** |
| Mohnish Sharma | PT | Senior Team Member | Ontrack |  |  |
|  |  |  |  |  |  |

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

**Finding Description**

Brute Force Authentication.

**Risk Rating**  
Impact: Severe  
Likelihood: Severe

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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. |

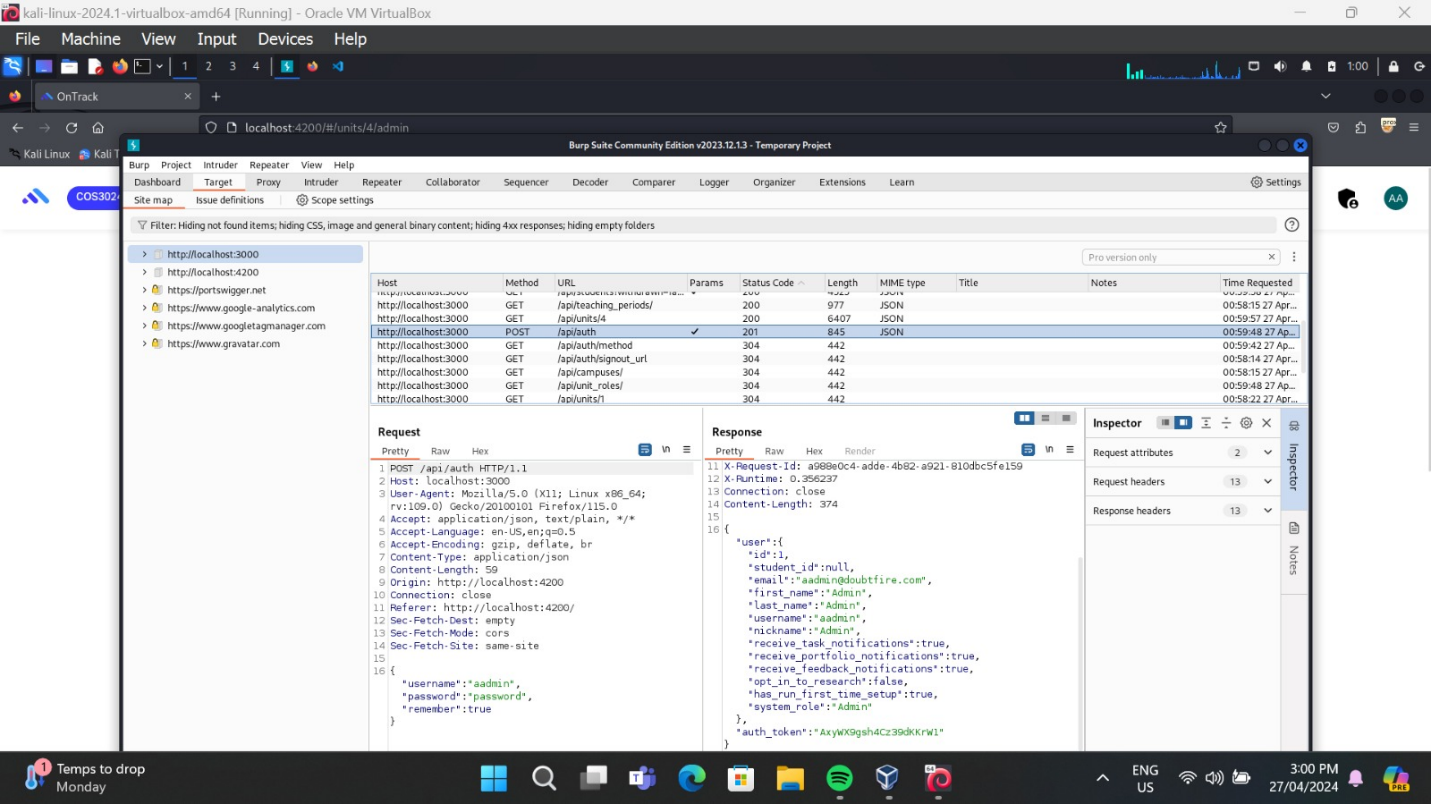
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Likelihood** | | | | |
| **Rare** | **Unlikely** | **Moderate** | **High** | **Certain** |
| Event may occur and/or if it did, it happens in specific circumstances. | Event could occur occasionally and/or could happen (at some point) | Event may occur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

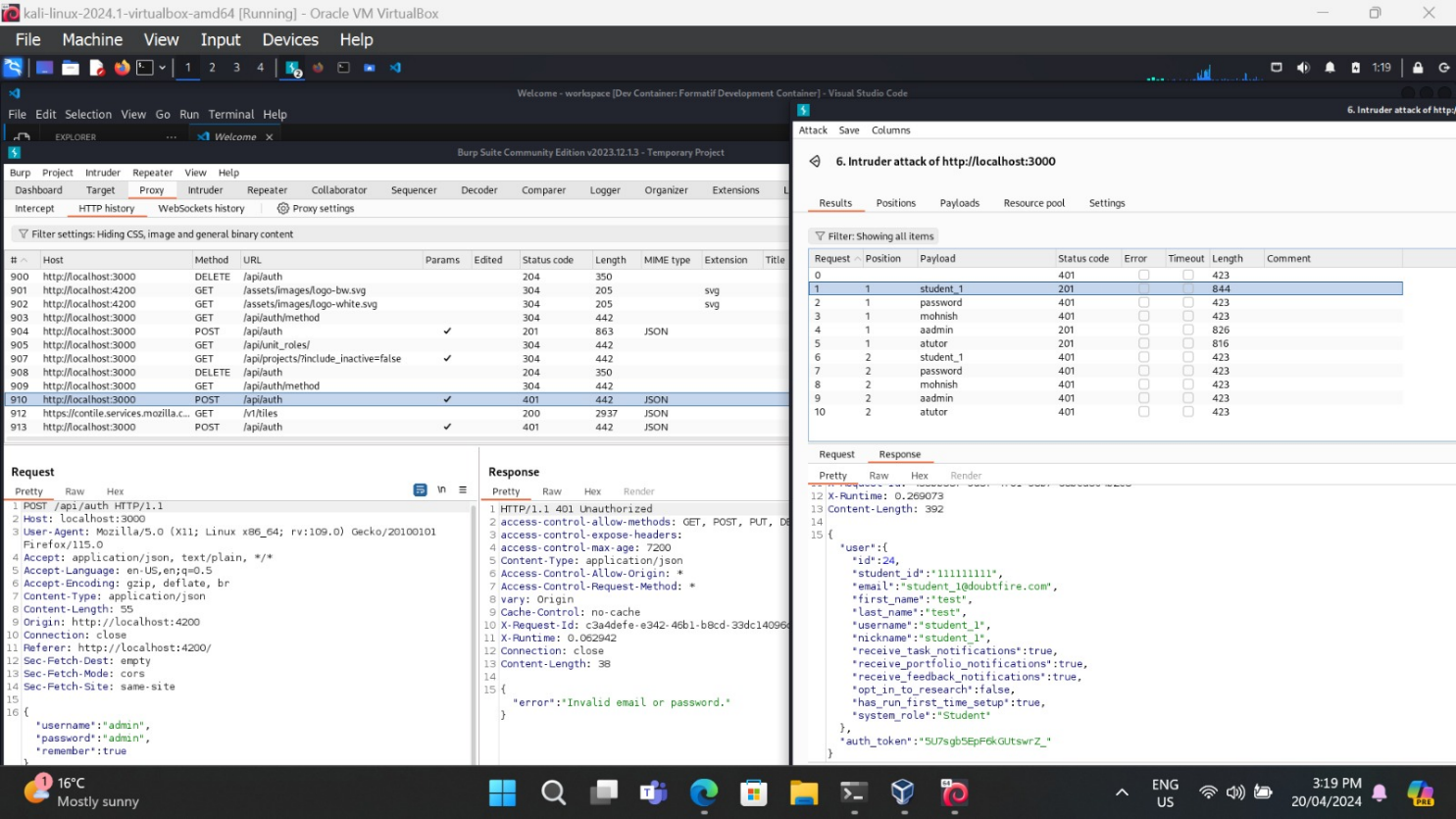
**Business Impact:**

* **Data Breach: Successful brute force attacks can lead to unauthorized access to sensitive data stored within the system, including user accounts, personal information, financial data, and proprietary information.**
* **Financial Loss: Data breaches resulting from brute force attacks can incur significant financial losses due to regulatory fines, legal fees, compensation to affected parties, and damage to the organization's reputation, which may lead to customer churn and loss of revenue.**
* **Reputation Damage: A successful brute force attack can tarnish the organization's reputation, eroding trust among customers, partners, and stakeholders. This can have long-term consequences on brand image and market competitiveness.**
* **Operational Disruption: Dealing with the aftermath of a brute force attack, such as restoring compromised accounts, investigating the incident, and implementing additional security measures, can disrupt normal business operations and divert resources from other critical tasks.**
* **Regulatory Compliance Violations: Depending on the industry and location, data breaches resulting from brute force attacks may lead to non-compliance with data protection regulations (e.g., GDPR, HIPAA, PCI DSS), resulting in legal penalties, fines, and reputational damage.**

**Affected Assets:**

* **User Accounts: Brute force attacks primarily target user accounts, including employee accounts, customer accounts, and administrative accounts, which may contain sensitive information and access privileges.**
* **Authentication Systems: The vulnerability affects the authentication systems, including login pages, authentication APIs, and associated mechanisms used to verify user credentials.**
* **Data Stores: Brute force attacks may compromise data stored within the system, such as databases, file servers, and cloud storage, where sensitive information is stored.**
* **Application Functionality: Successful brute force attacks may enable unauthorized access to application functionalities, such as administrative controls, financial transactions, and sensitive operations.**
* **System Resources: Brute force attacks consume system resources, including CPU, memory, and network bandwidth, potentially impacting the performance and availability of the system for legitimate users.**

**Evidence**

****

**Remediation Advice**

* **Account Lockout Policies: Temporarily lock accounts after multiple failed login attempts.**
* **Strong Password Policies: Require complex passwords to thwart guessing.**
* **Multi-Factor Authentication (MFA): Add extra layers of security beyond passwords.**
* **Rate Limiting: Restrict the number of login attempts per time period.**
* **Monitor and Alert: Watch for unusual login patterns and alert admins.**
* **CAPTCHA or Challenge-Response: Differentiate between humans and bots.**
* **User Education: Teach users about password security and phishing risks.**
* **Regular Updates: Keep authentication systems patched and current.**
* **Security Testing: Regularly test and audit authentication mechanisms.**

**References**

[**https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5\_overly\_permissive\_cors\_policy**](https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy)

**Contact Details**

Name: Mohnish Sharma

**Pentest Leader Feedback.**

The lead will provide feedback to enact on.