|  |  |
| --- | --- |
| **Lab 7 - Access control vulnerabilities - Privilege escalation** | |
| **Name** | Tran Minh Triet |
| **Student ID** | SE172241 |

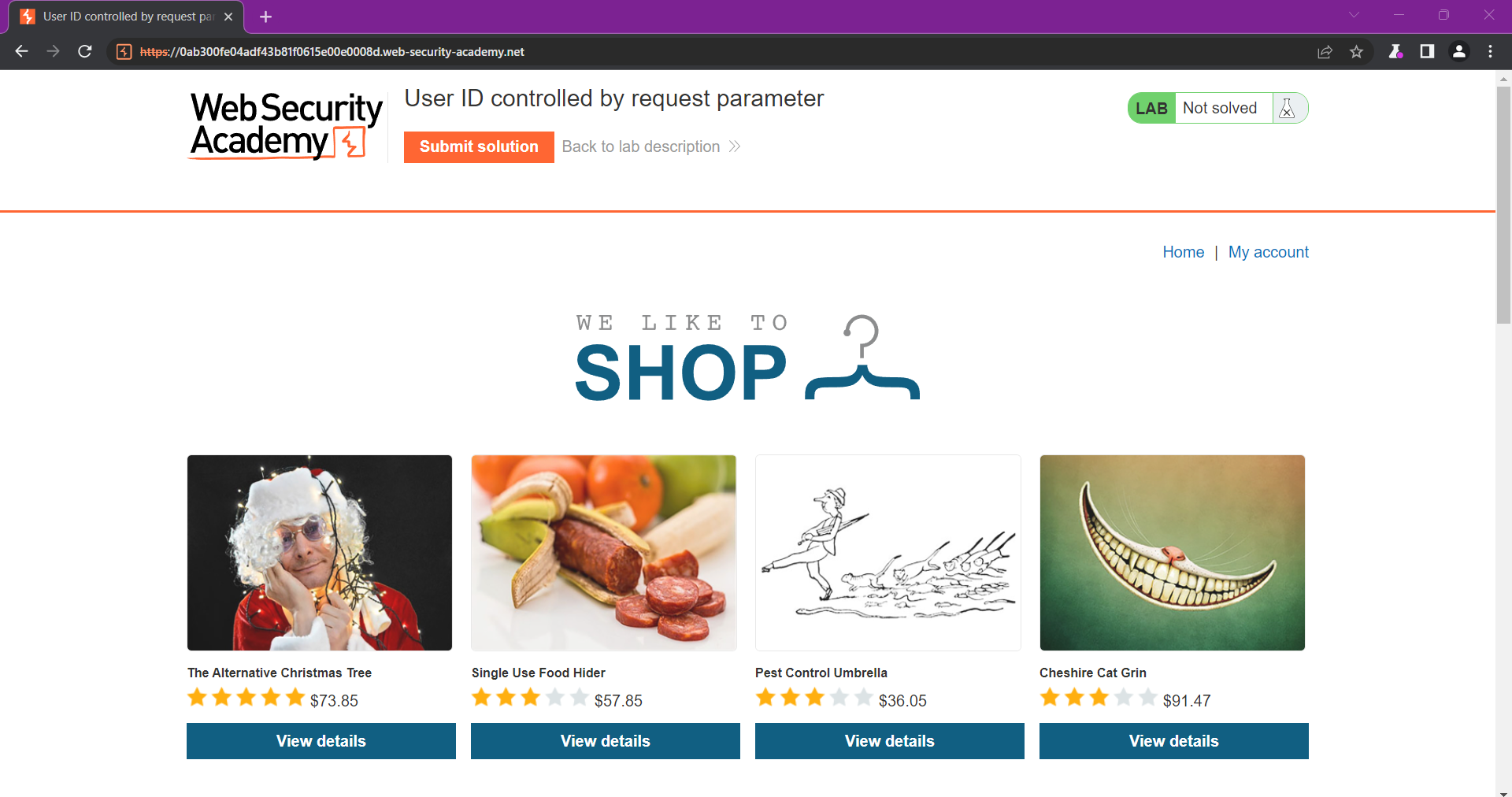
1. In the context of privilege escalation, what is the difference between vertical and horizontal privilege escalation, and can you give an example of each?

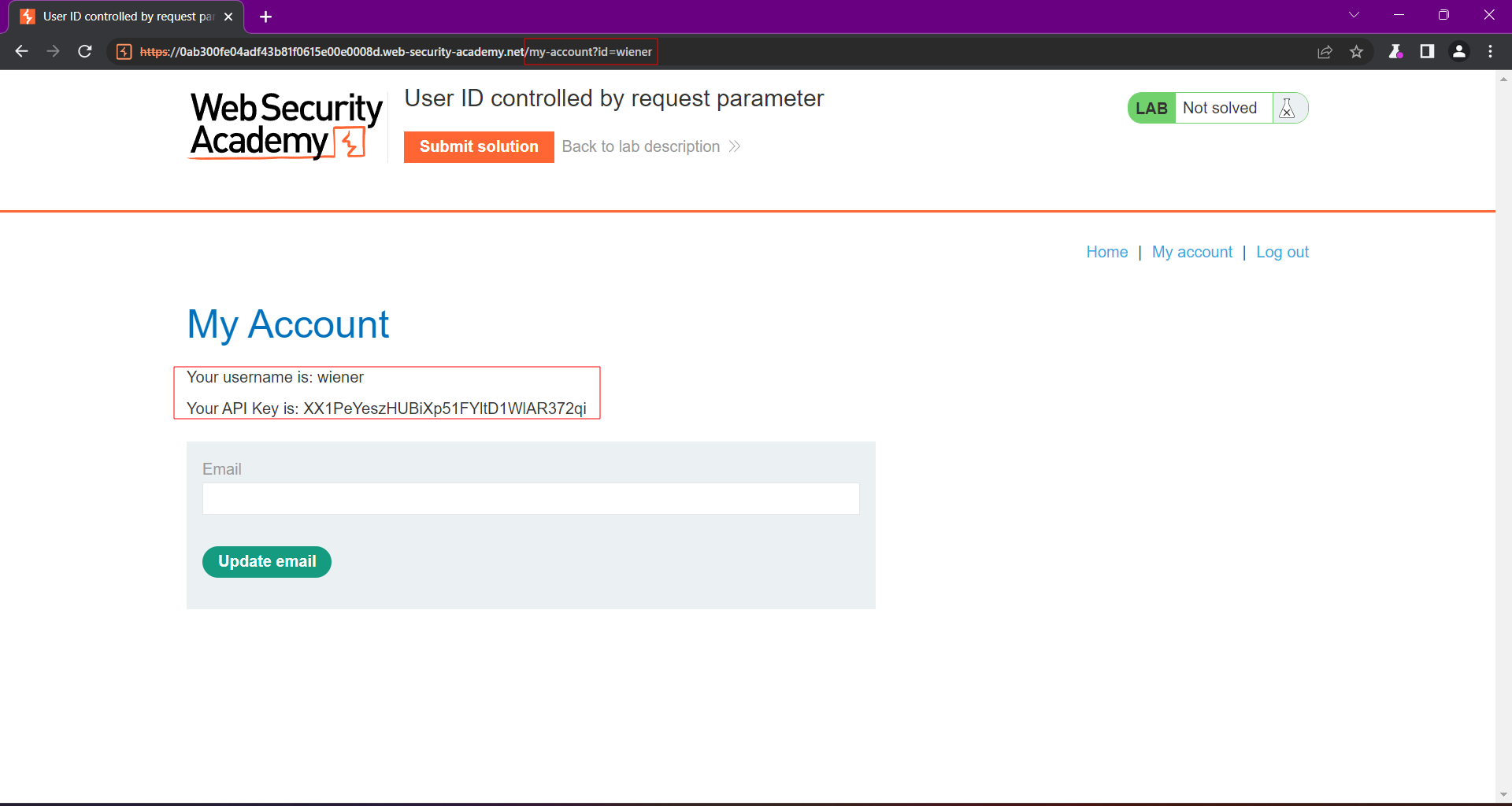
Privilege escalation is a security issue where an attacker gains unauthorized access to higher levels of privilege than originally intended by the system. This could involve elevating user privileges within the same level (horizontal privilege escalation) or acquiring higher-level privileges (vertical privilege escalation). Let's explore the differences between vertical and horizontal privilege escalation along with examples for each.

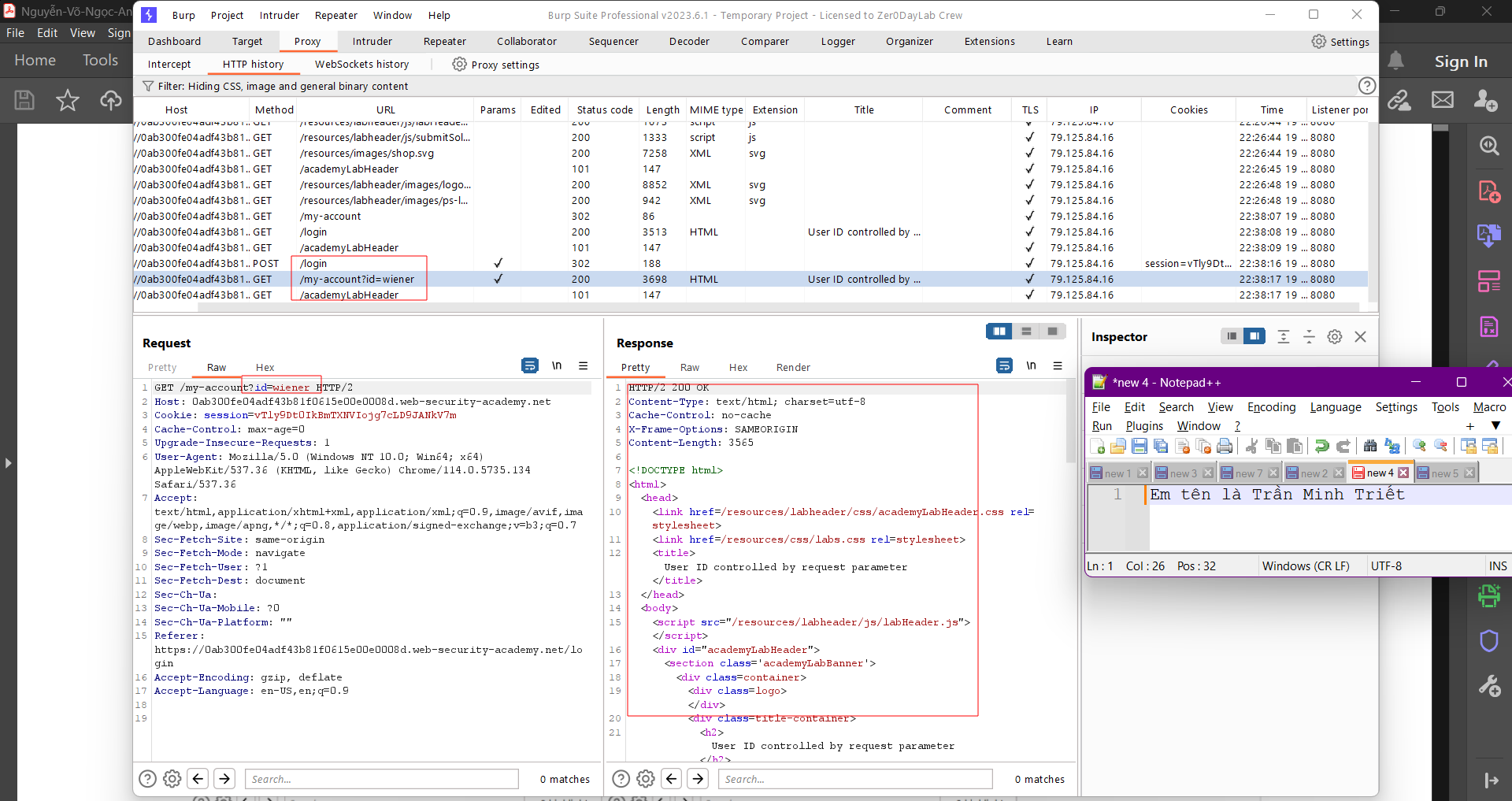
1. What are some effective strategies or practices that can be implemented to prevent privilege escalation vulnerabilities in a system?

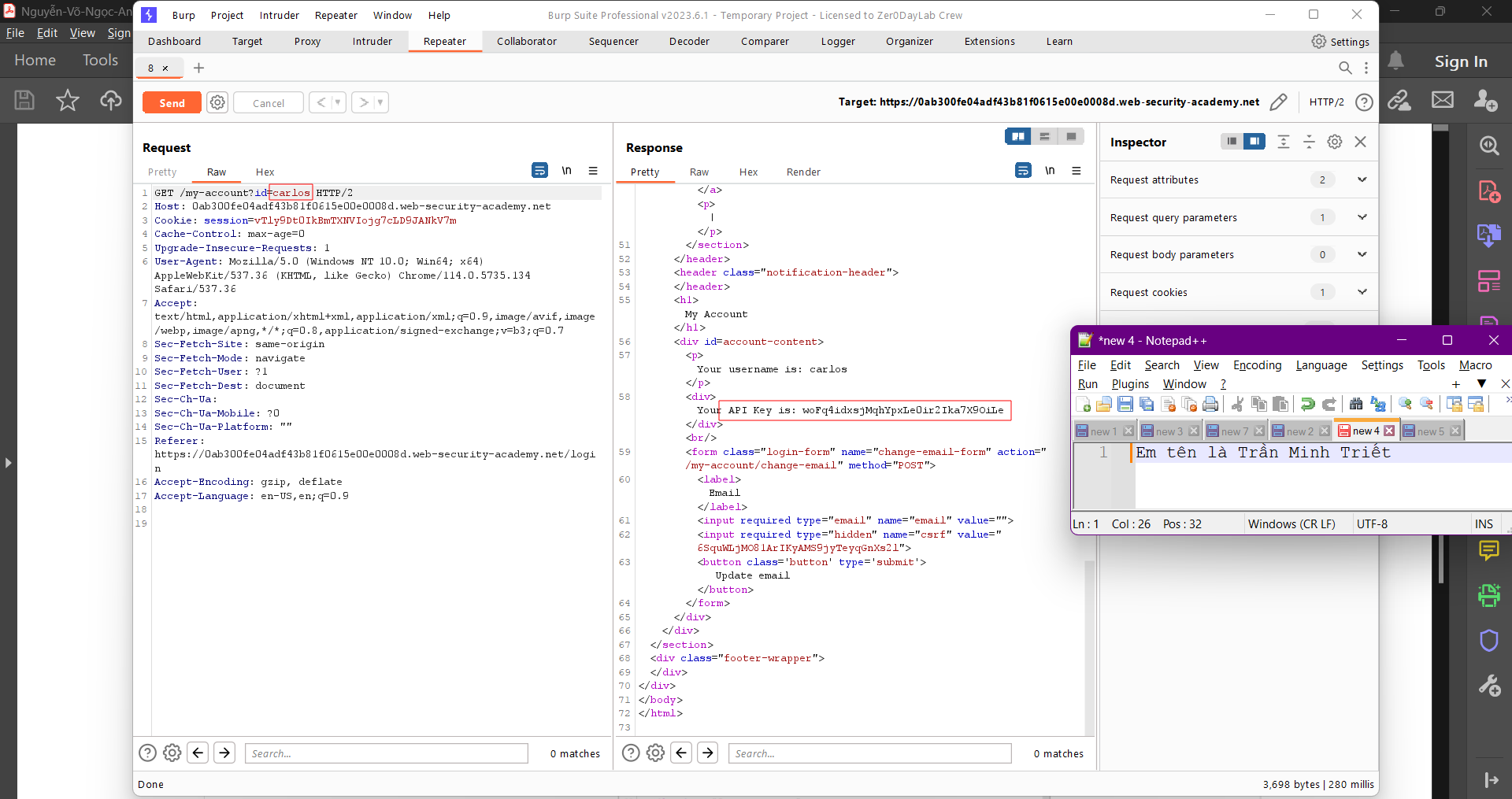
Preventing privilege escalation vulnerabilities in a system is crucial for maintaining the security and integrity of the overall infrastructure. Here are some effective strategies and practices that can be implemented to mitigate the risk of privilege escalation:

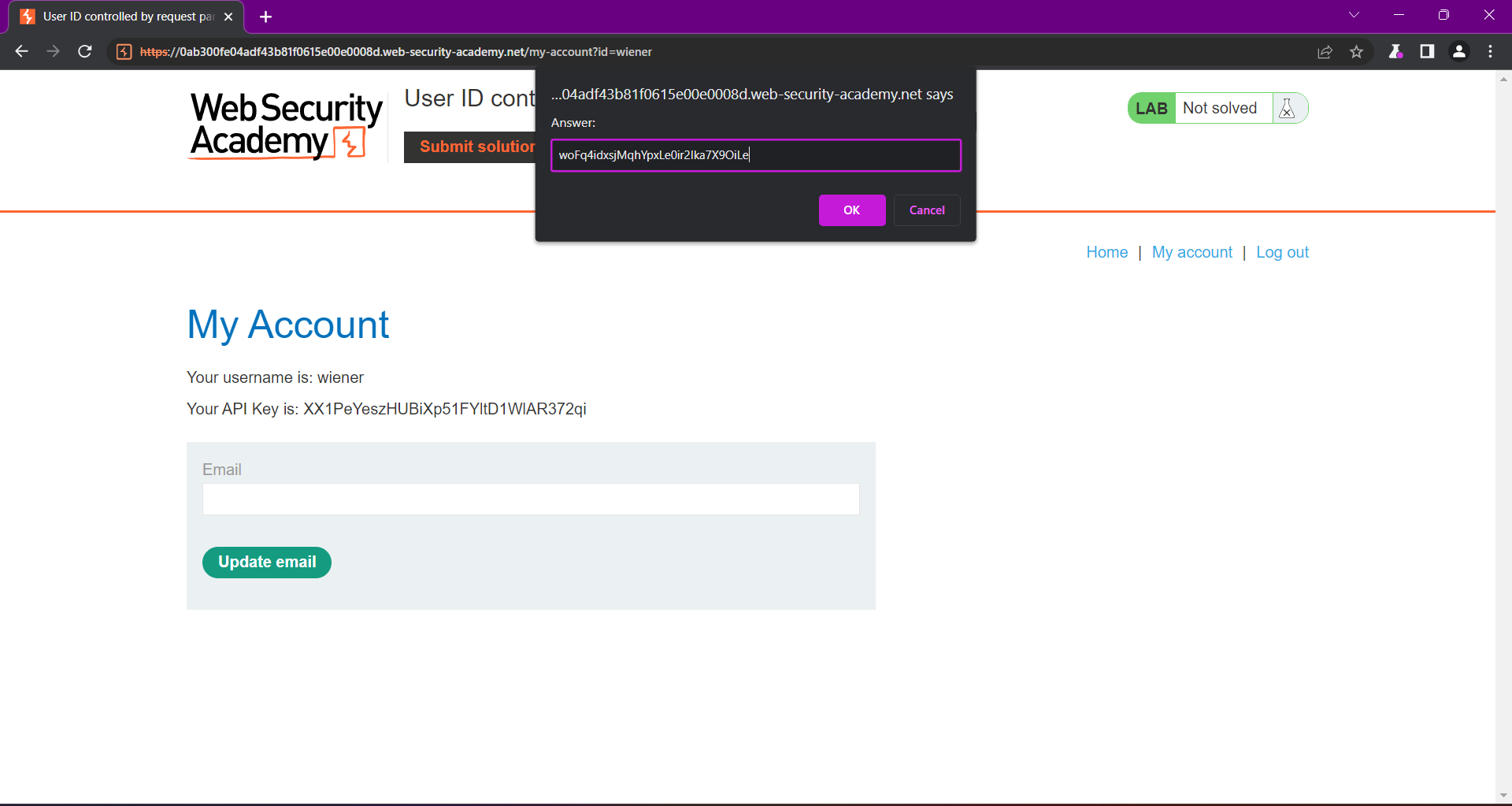
* Patch Management
* Vulnerability Scanning
* Secure Configuration
* Application Hardening
* Network Segmentation
* Strong Authentication
* Log Monitoring
* Incident Response Planning

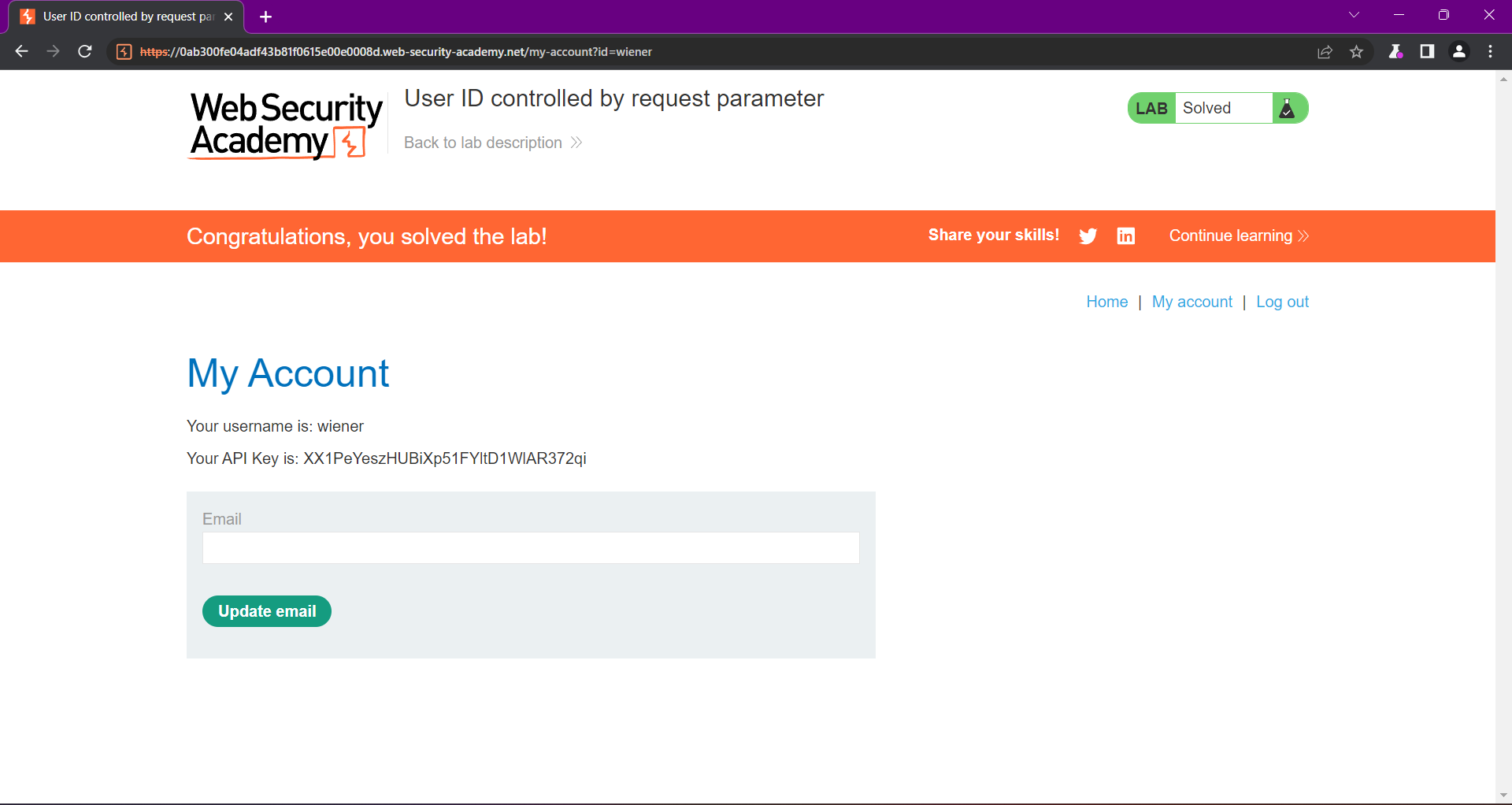
Challenge <[link](https://portswigger.net/web-security/access-control/lab-user-id-controlled-by-request-parameter)>











**---END---**