**ASSIGNMENT 2 FRONT SHEET**

|  |  |  |  |
| --- | --- | --- | --- |
| **Qualification** | **BTEC Level 5 HND Diploma in Computing** | | |
| **Unit number and title** | Unit 16: Cloud Computing | | |
| **Submission date** |  | **Date Received 1st submission** |  |
| **Re-submission Date** |  | **Date Received 2nd submission** |  |
| **Student Name** | VO NHUT HUY | **Student ID** | GCC18169 |
| **Class** | GCC0701 | **Assessor name** | THAI MINH TUAN |
| **Student declaration**  I certify that the assignment submission is entirely my own work and I fully understand the consequences of plagiarism. I understand that making a false declaration is a form of malpractice. | | | |
|  |  | **Student’s signature** | NHUT HUY |

**Grading grid**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| P5 | P6 | P7 | P8 | M3 | M4 | D2 | D3 |
|  |  |  |  |  |  |  |  |

|  |  |  |
| --- | --- | --- |
| **❒ Summative Feedback: ❒ Resubmission Feedback:** | | |
| **Grade:** | **Assessor Signature:** | **Date:** |
| **Signature & Date:** | | |

**ASSIGNMENT 2 BRIEF**

|  |  |  |  |
| --- | --- | --- | --- |
| **Qualification** | **BTEC Level 5 HND Diploma in Computing** | | |
| **Unit number** | Unit 9: Cloud Computing | | |
| **Assignment title** | Cloud’s implementation and security threats | | |
| **Academic Year** | 2019 – 2020 | | |
| **Unit Tutor** |  | | |
| **Issue date** |  | **Submission date** |  |
| **IV name and date** |  | | |

|  |
| --- |
| **Submission Format:** |
| *Format:* A presentation in Power Point format(about 25 pages)  A security manual(in PDF format)  You must use font *Calibri size 12, set number of the pages and use multiple line spacing at 1.3. Margins must be: left: 1.25 cm; right: 1 cm; top: 1 cm and bottom: 1 cm.* The reference follows Harvard referencing system.  *Submission* Students are compulsory to submit the assignment in due date and in a way requested by the Tutors. The form of submission will be a soft copy posted on <http://cms.greenwich.edu.vn/>  *Note:* The Assignment *must* be your own work, and not copied by or from another student or from  books etc. If you use ideas, quotes or data (such as diagrams) from books, journals or other sources, you must reference your sources, using the Harvard style. Make sure that you know how to reference properly, and that understand the guidelines on plagiarism. *If you do not, you definitely get failed* |
| **Unit Learning Outcomes:** |
| **LO3** Develop Cloud Computing solutions using service provider’s frameworks and open source tools.  **LO4** Analyse the technical challenges for cloud applications and assess their risks |
| **Assignment Brief and Guidance:** |
| **Task 1**  Base on the scenario and architecture design in the first assignment provide the implementation. Because of the time constraint of the assignment, the implementation just provides some demo functions of the scenario. The implementation includes two parts:   * A presentation (about 25 pages)   + which shows which functions are implemented   + How to config, deploy and test the services (Web application, Database Server, Source code management, server logs..) using service provider’s frameworks and open source tools.   + Images for the built functions * The source code for the built application   **Task 2**  The table of contents in your security manual (which should be 500–700 words) should be as follows:   1. Analysis of the most common problems of a cloud computing platform. 2. Possible solutions to these problems. 3. Analysis of the most common security issues in the cloud environment. 4. Discussion on how to overcome these issues. 5. Summary. |

|  |  |  |
| --- | --- | --- |
| Learning Outcomes and Assessment Criteria | | |
| Pass | Merit | Distinction |
| **LO3** Develop Cloud Computing solutions using service provider’s frameworks and open source tools | | **D2** Critically discuss how one can overcome these issues and constraints. |
| **P5**. Implement a cloud platform using open source tools  **P6**. Configure a Cloud Computing platform with a cloud service provider’s framework. | **M3** Discuss the issues and constraints one can face during the development process. |
| **LO4** Analyse the technical challenges for cloud applications and assess their risks | |  |
| **P7** Analyse the most common problems which arise in a Cloud Computing platform and discuss appropriate solutions to these problems.  **P8** Assess the most common security issues in cloud environments. | **M4** Discuss how to overcome these security issues when building a secure cloud platform. | **D3** Critically discuss how an organisation should protect their data when they migrate to a cloud solution. |

Contents

[P5. Implement a cloud platform using open source tools 7](#_Toc50662001)

[P6. Configure a Cloud Computing platform with a cloud service provider’s framework. 17](#_Toc50662002)

[P7 Analyse the most common problems which arise in a Cloud Computing platform and discuss appropriate solutions to these problems. 21](#_Toc50662005)

[1. Security and privacy 21](#_Toc50662006)

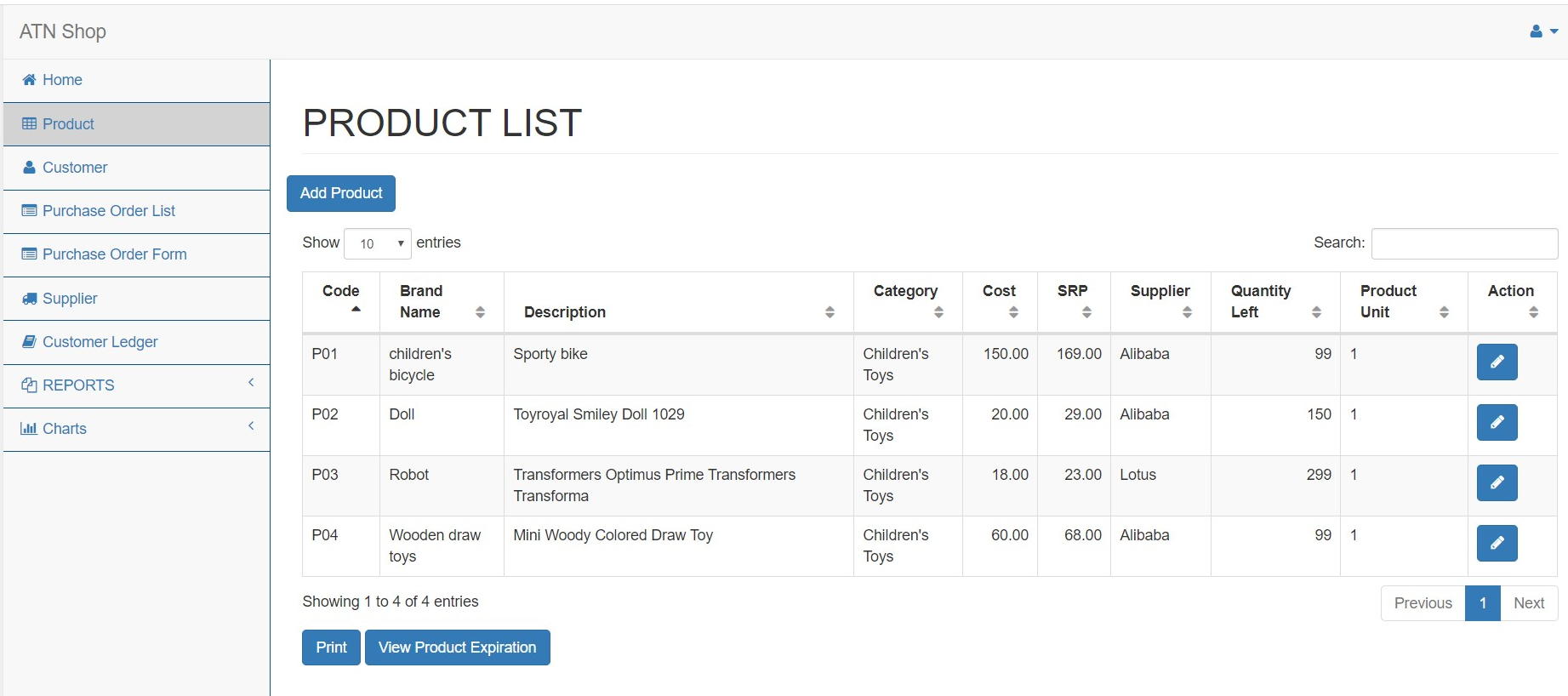
[2. Vulnerability to attack 21](#_Toc50662007)

[3. Limited control and flexibility 22](#_Toc50662008)

[4. Cost concerns 23](#_Toc50662009)

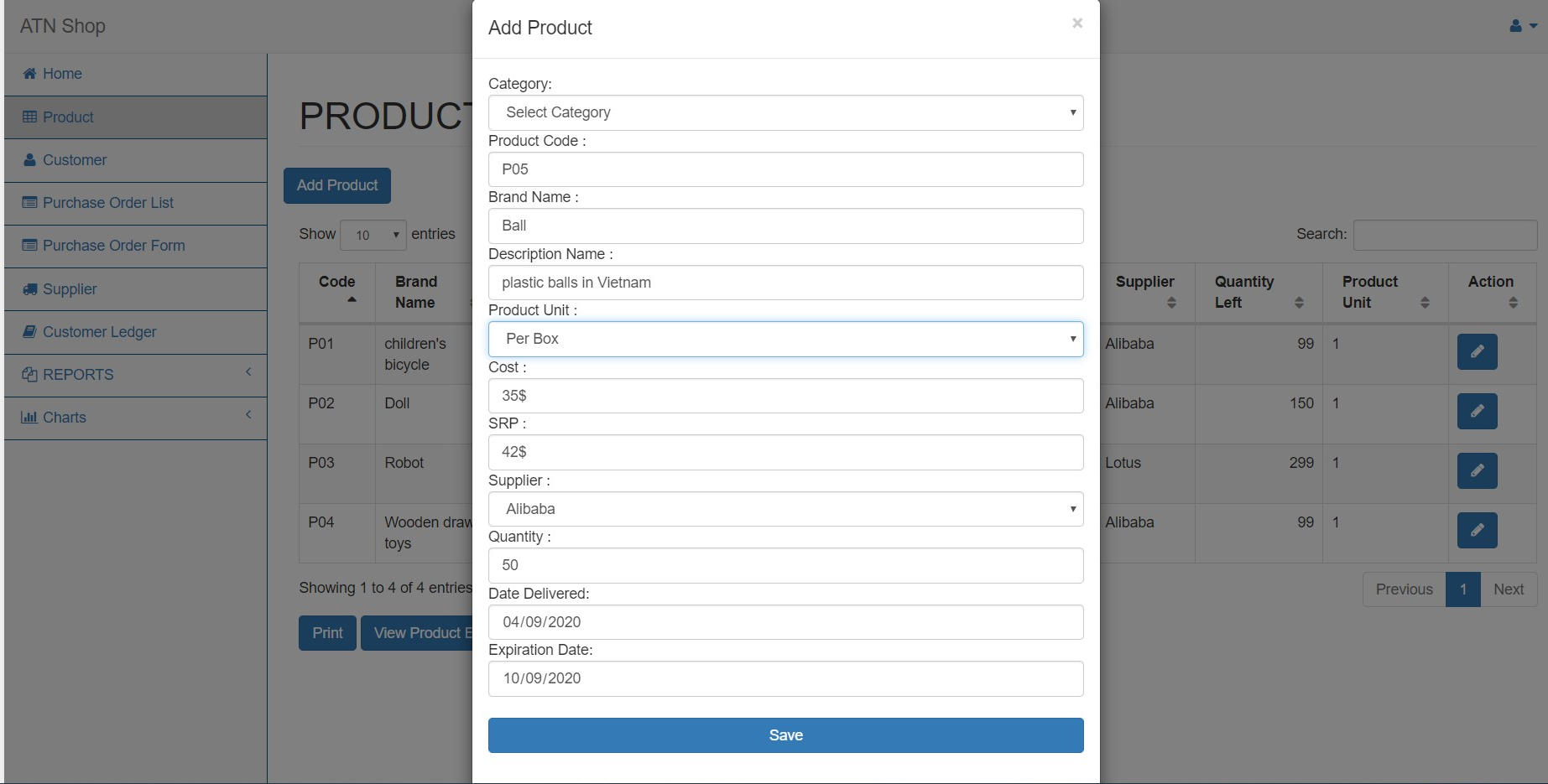
[P8 Assess the most common security issues in cloud environments. 23](#_Toc50662010)

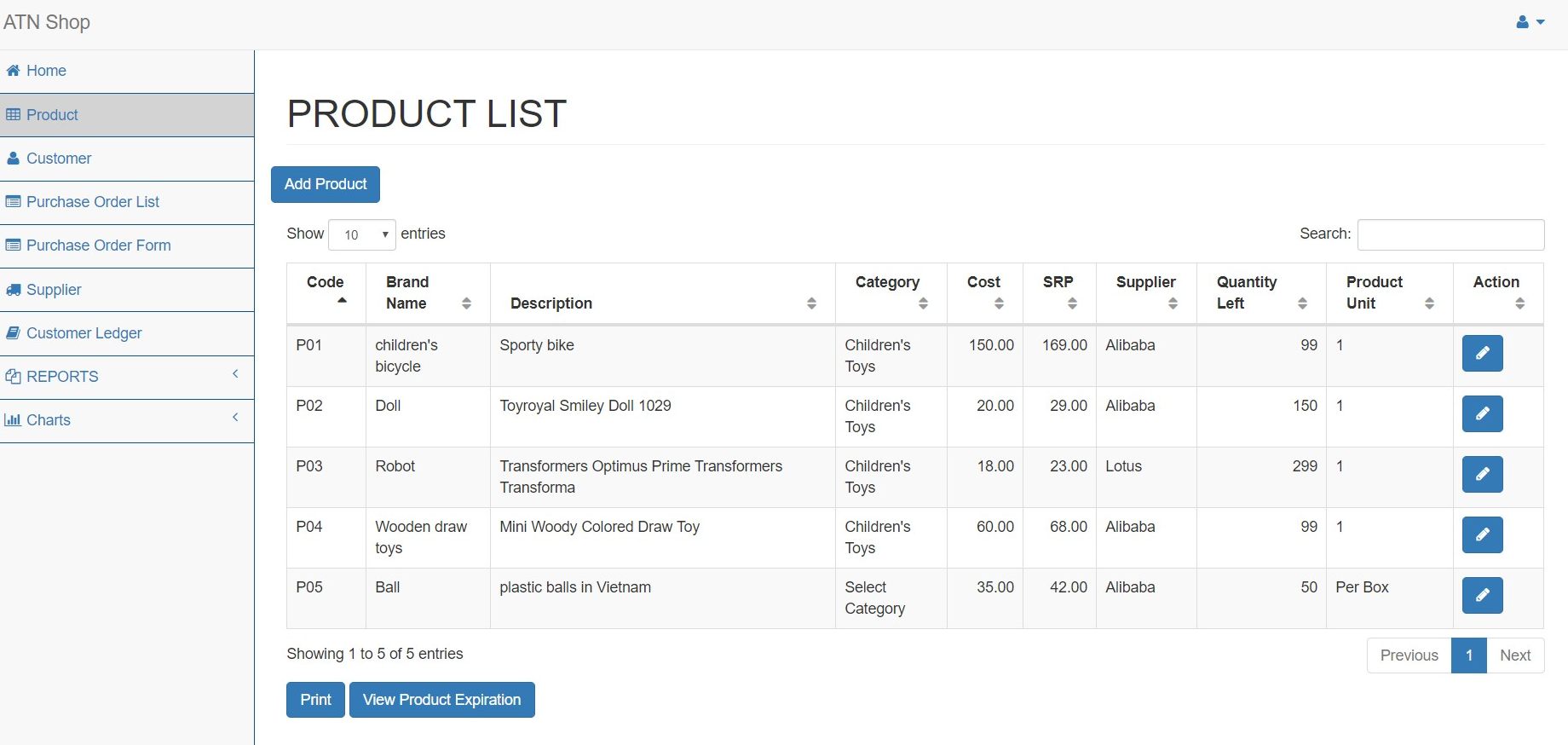
# P5. Implement a cloud platform using open source tools

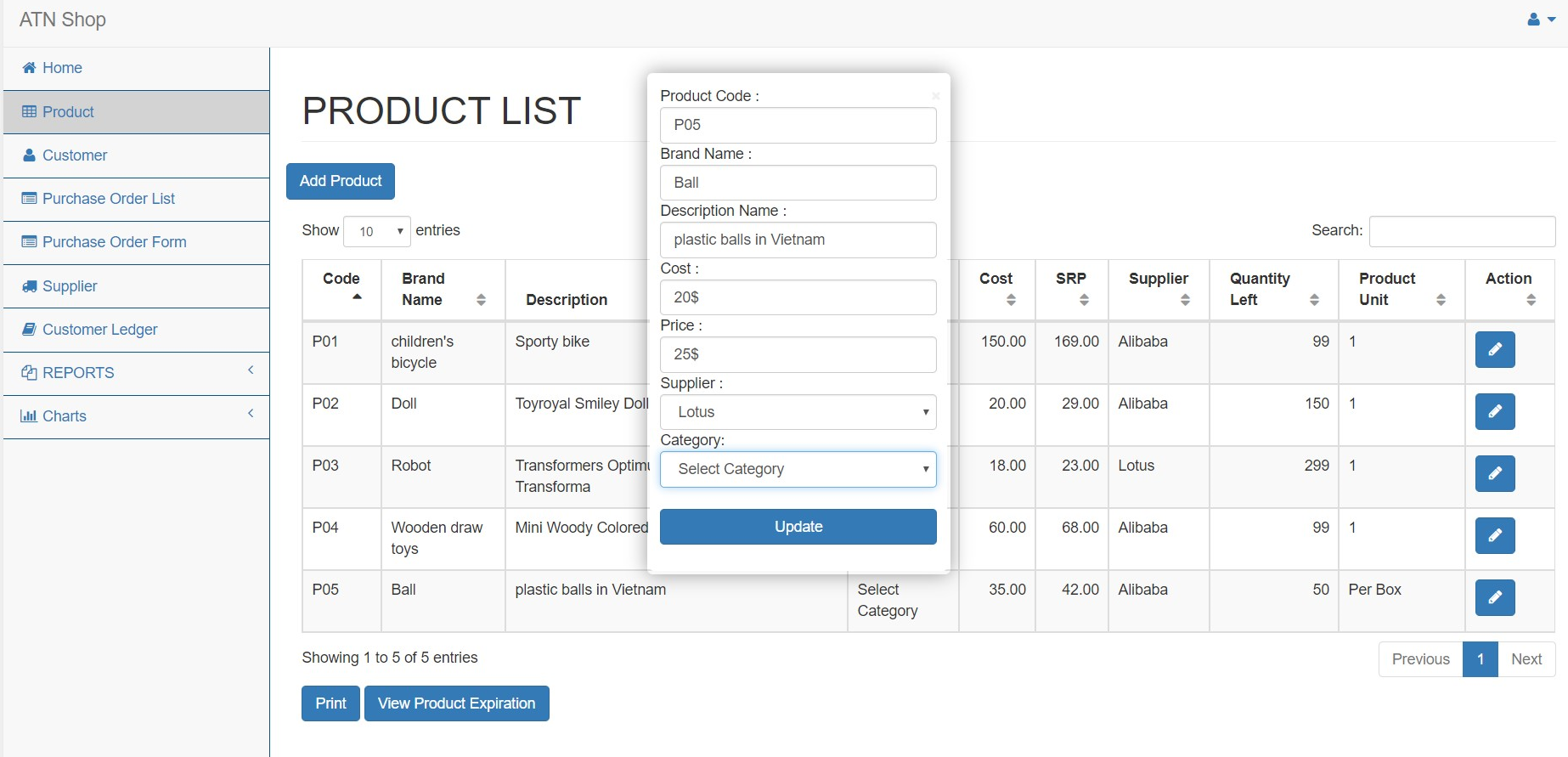


This is the Product List page, we see the display of product information on the page (Code, Brand Name, Description, Category, Cost, SRP, Supplier, Quantity Left, product Unit)

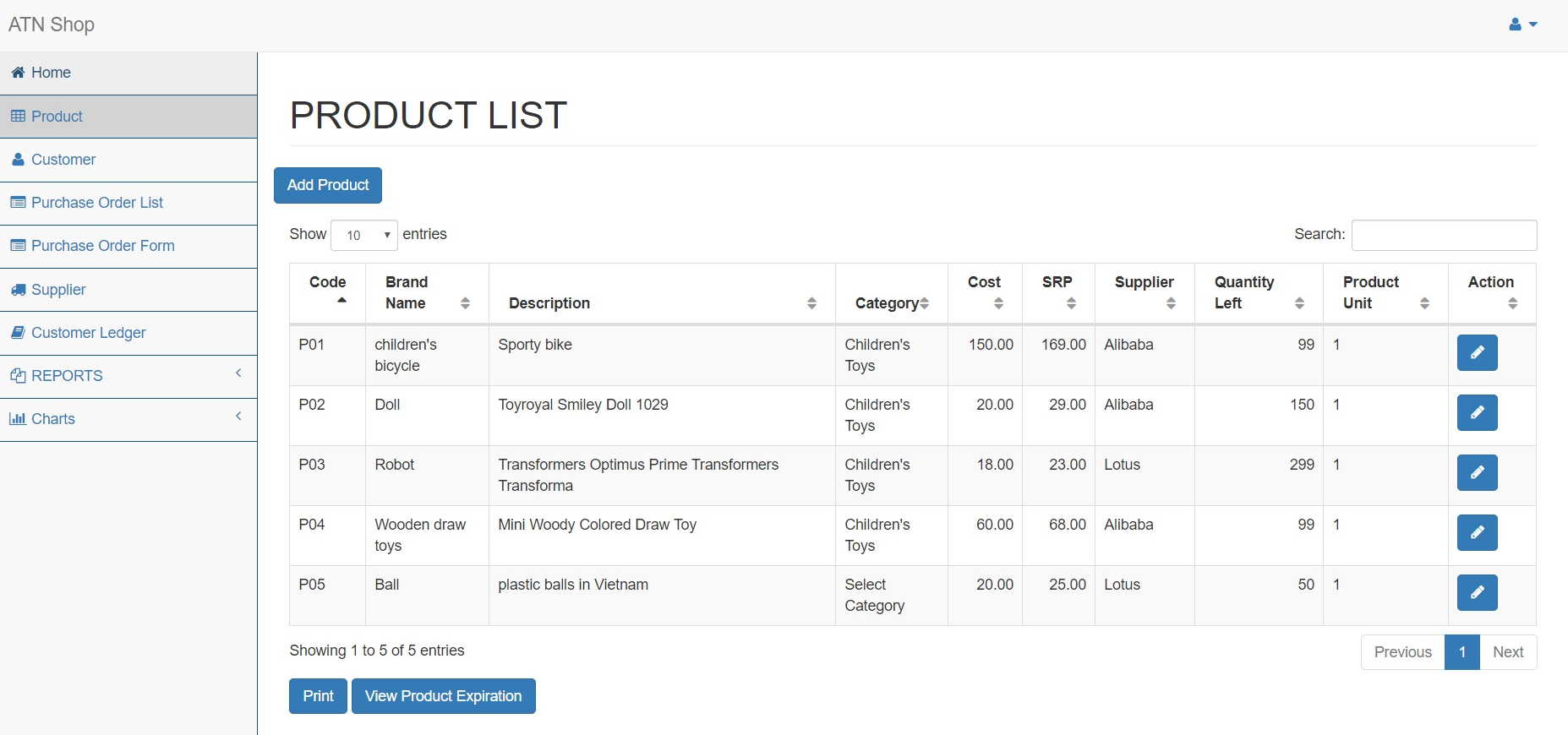
The Add Product section



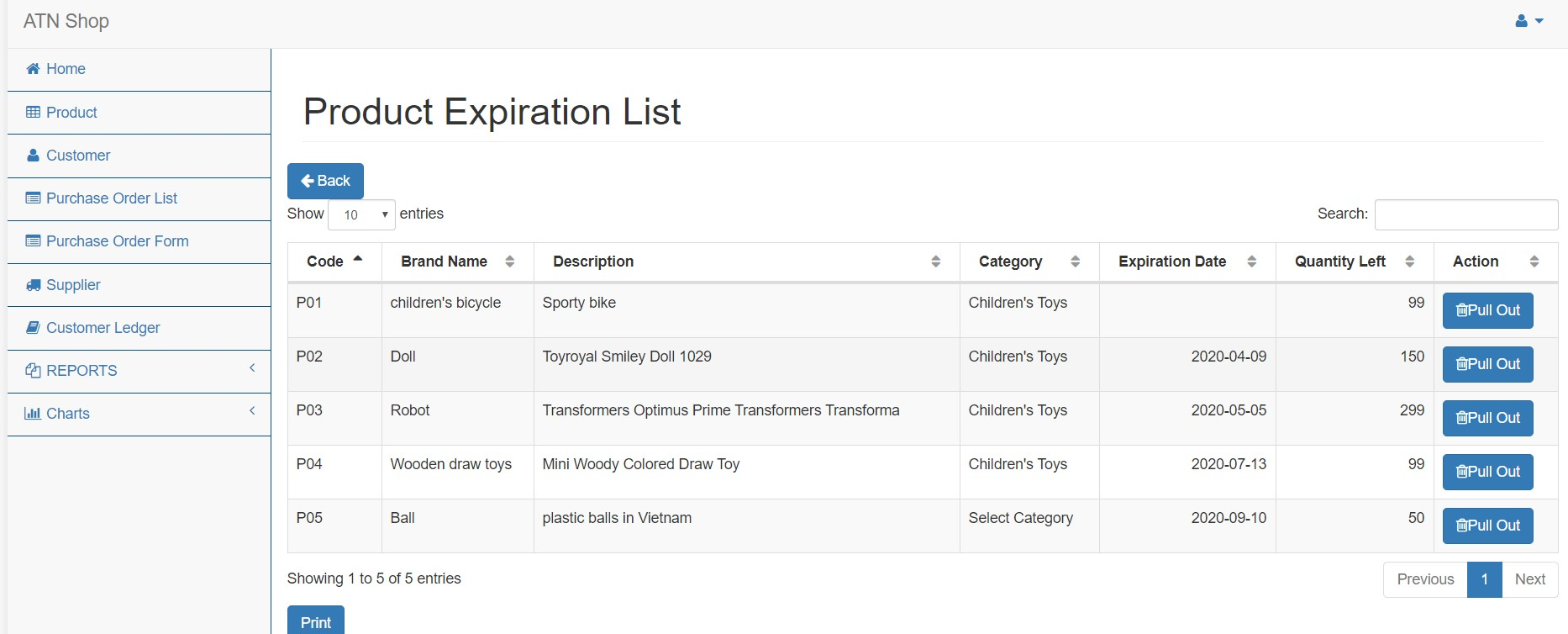
When we enter the complete information when importing goods into the shop from the administrator



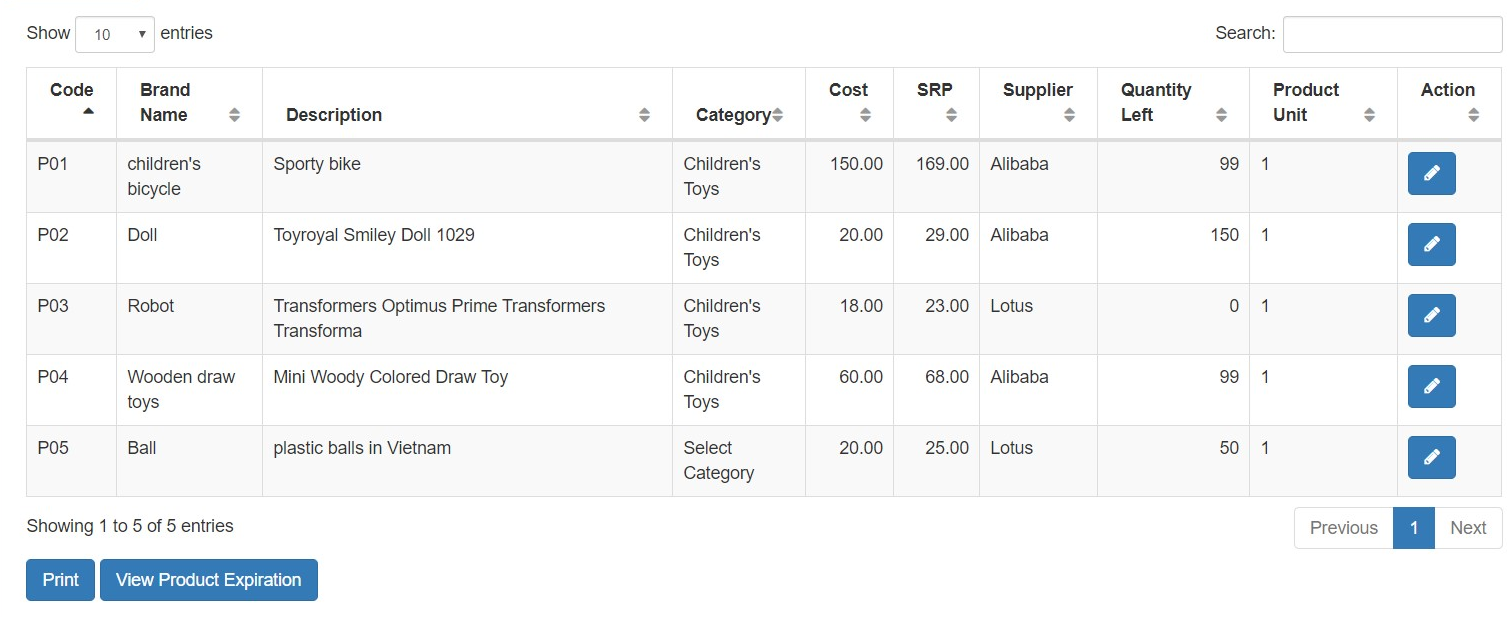
When we want to Edit product information

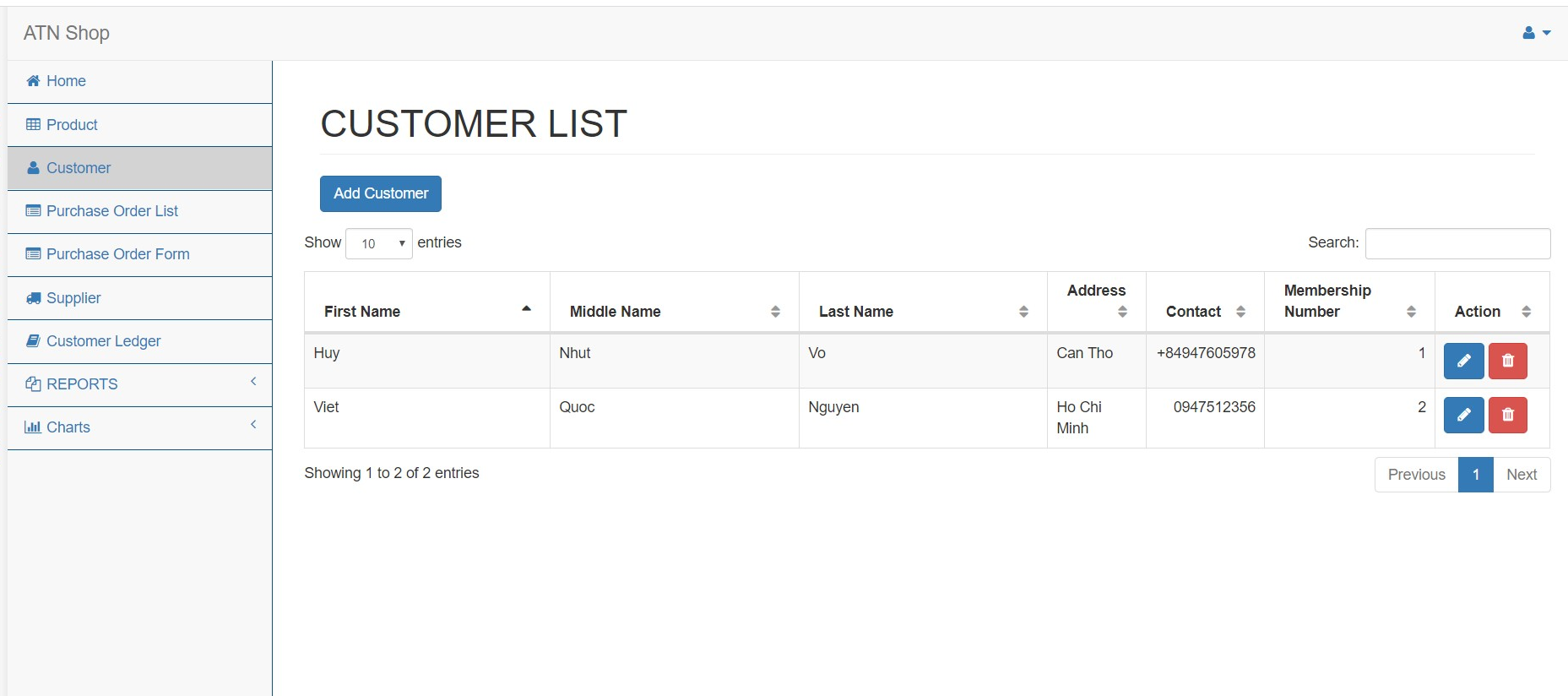
We see the P05 product information has been changed to information

When the administrator wants to delete product information, there is no product in stock for sale

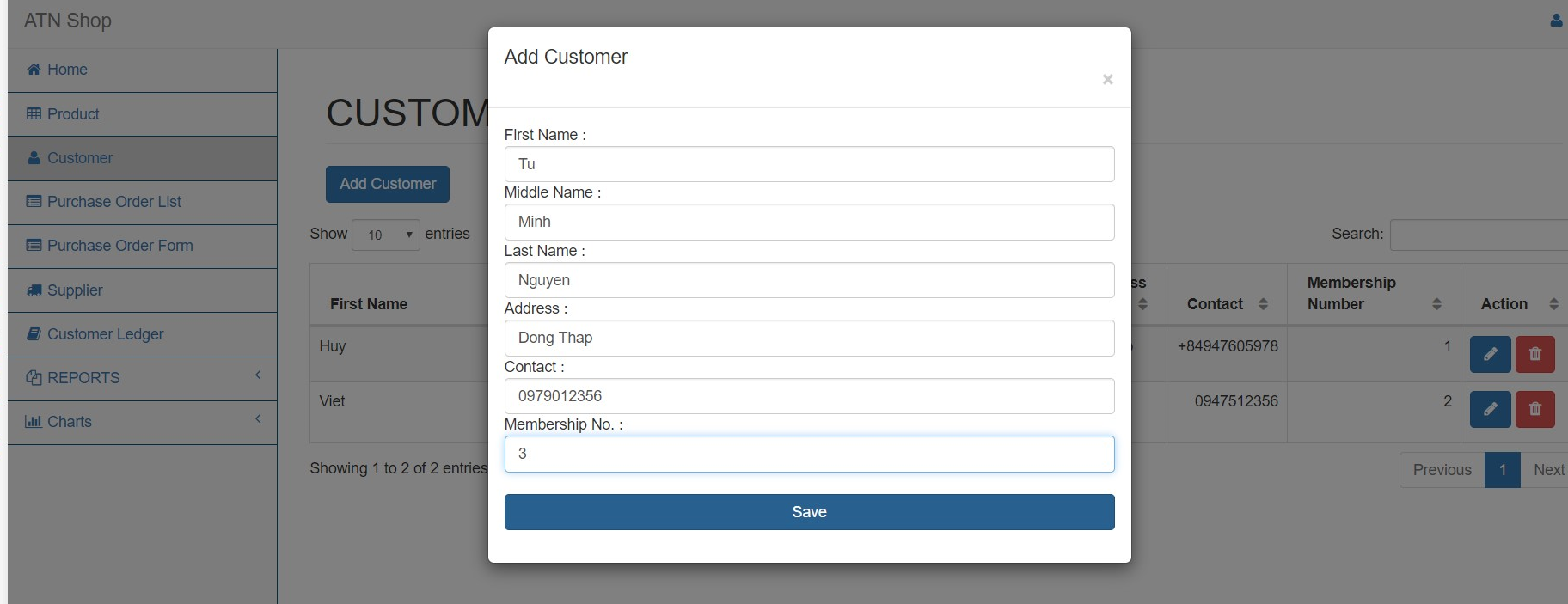


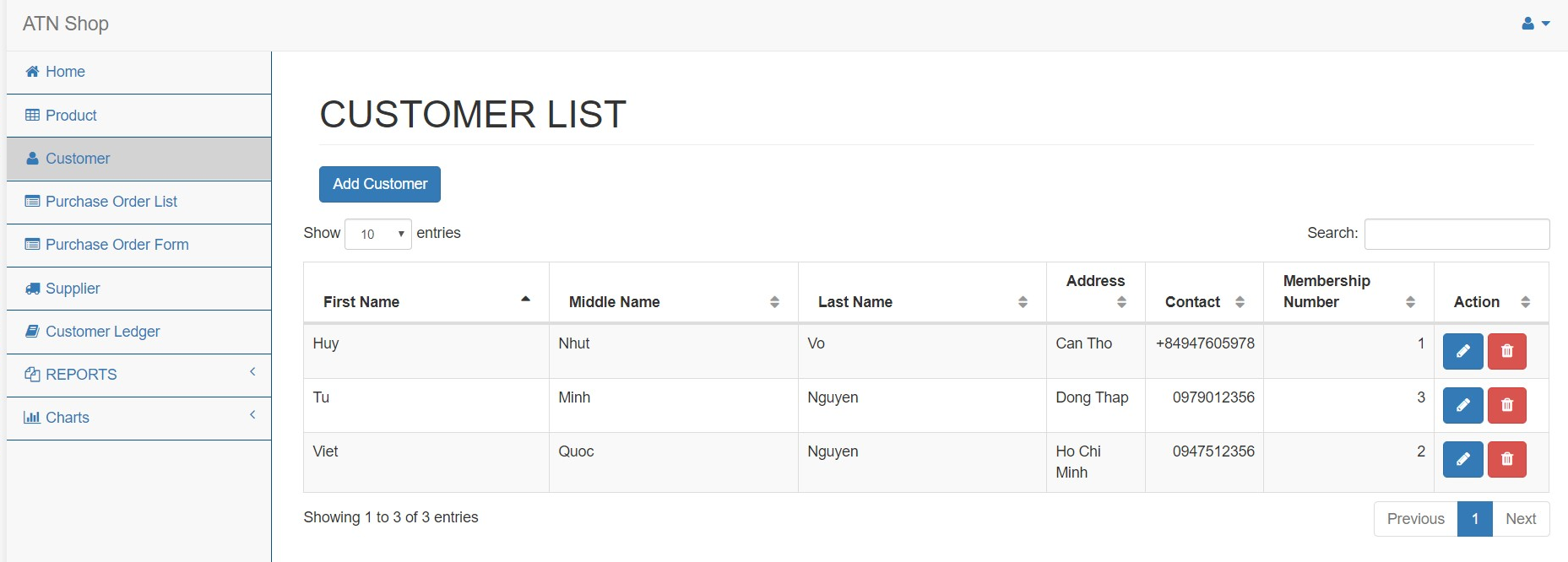
When the shop runs out of P03 products, the administrator can delete it from the list of buyers who want to search



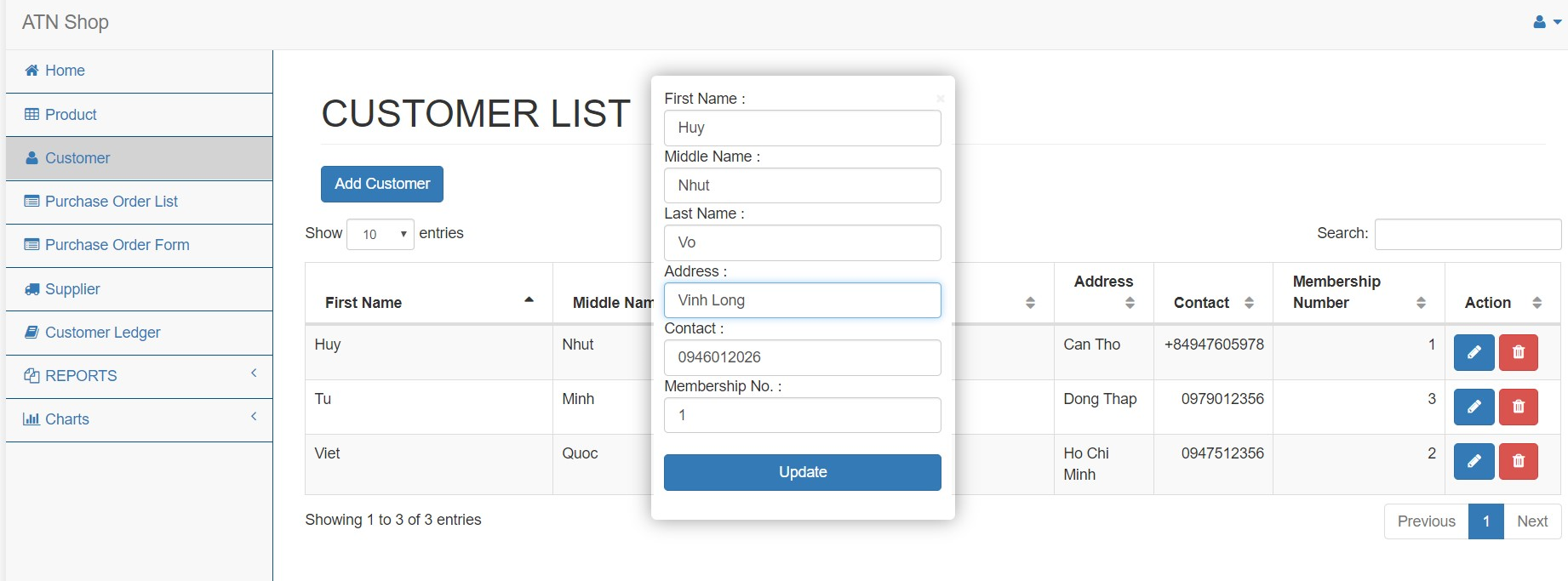
Next is the list of visitors that the administrator can manage

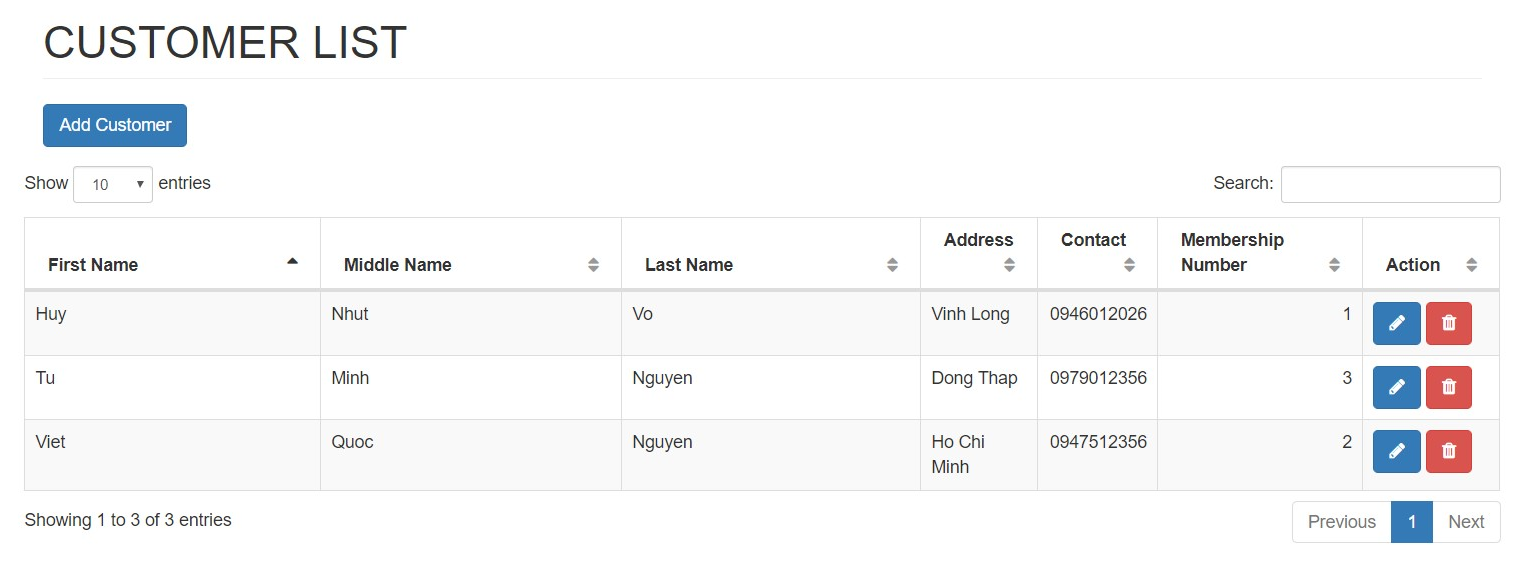
Administrators can add customer information when they have registered to buy goods at the shop



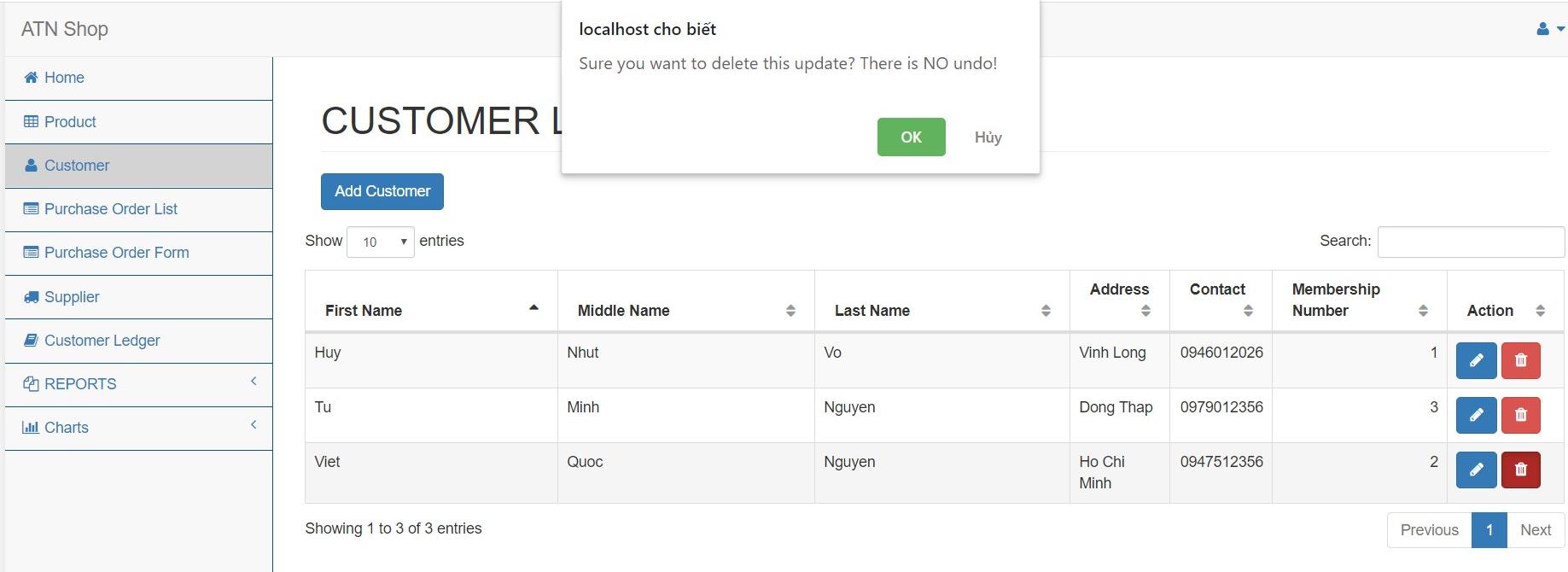


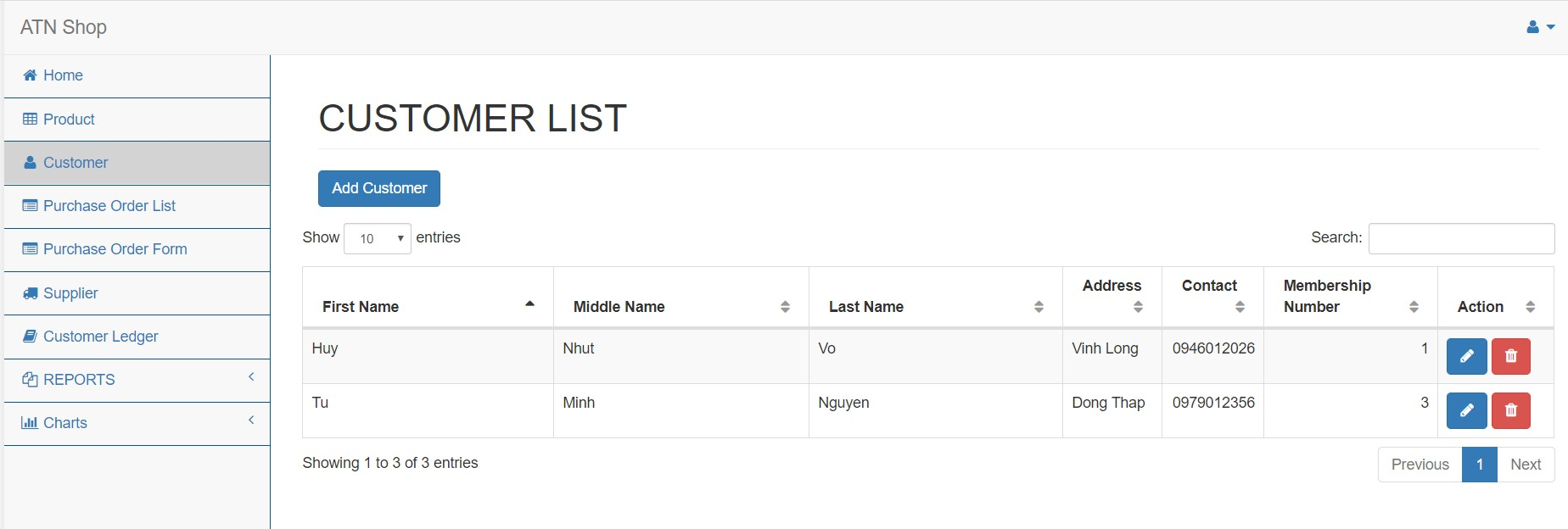
The administrator can also change the user's information when the customer wants to change





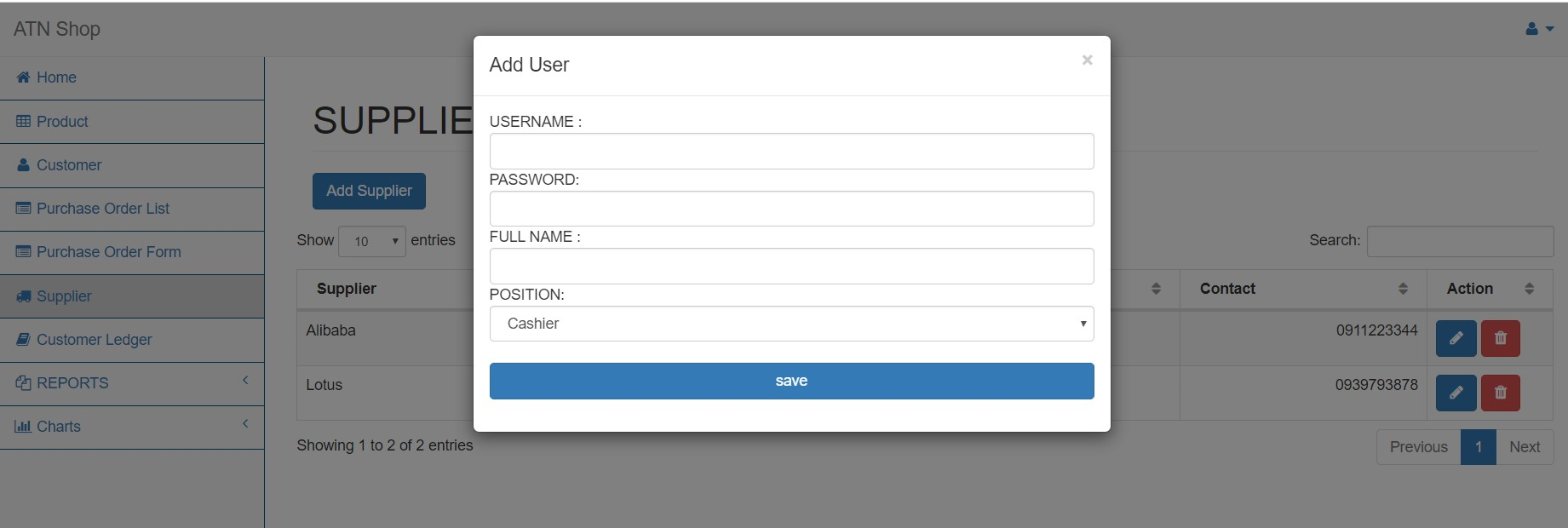
Administrators can also delete customer information when the customer has not bought products from the shop for a long time

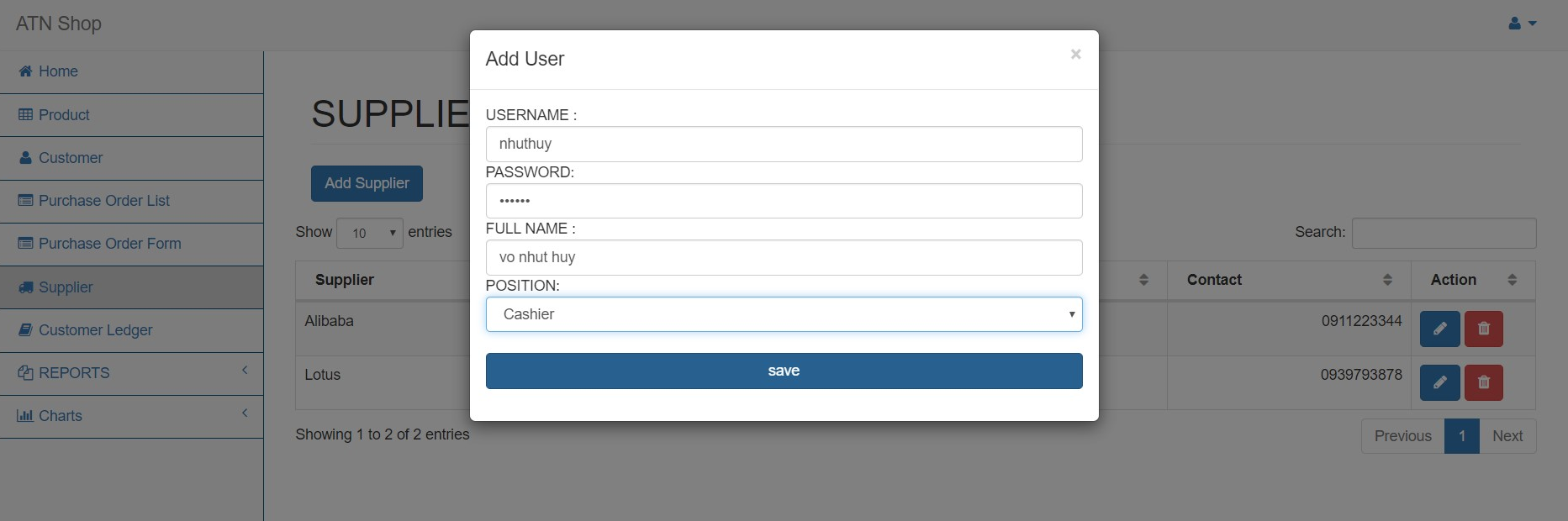


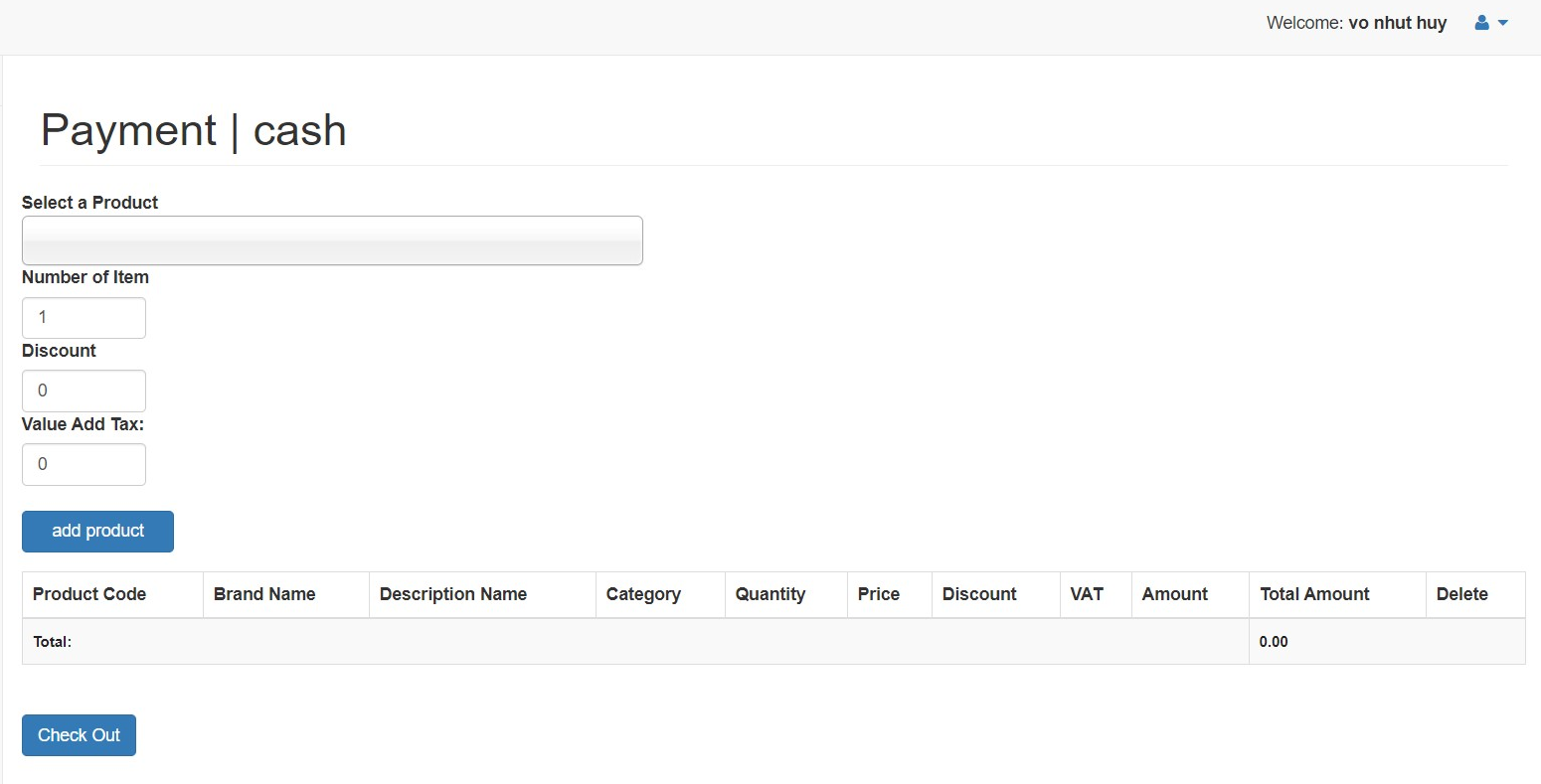


Supplier is managed by an administrator to contact product suppliers for the company and to manage supplier information for the company

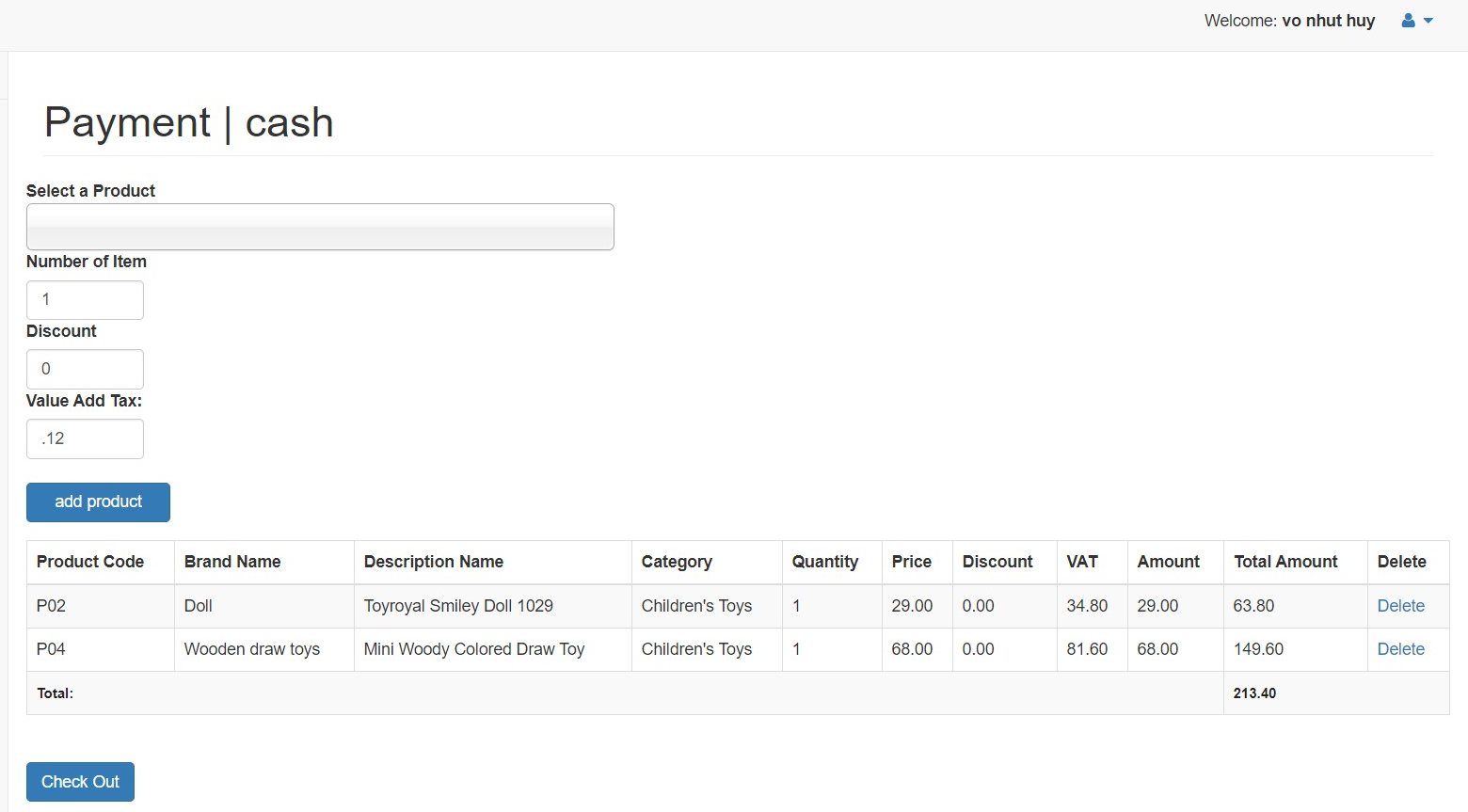


Next is the Cashier section created by the Admin for them

We enter full information for Cashier to create an account



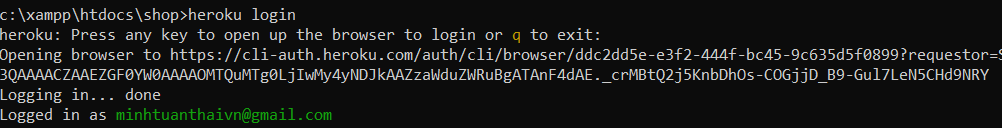
Once logged in to your Cashier account



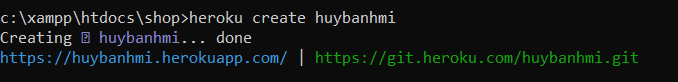
The customer buys the product and has been on the cashier's check out system

**P6. Configure a Cloud Computing platform with a cloud service provider’s framework**.

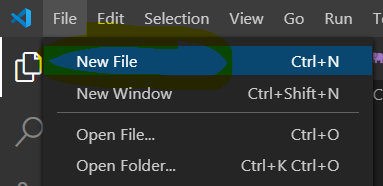
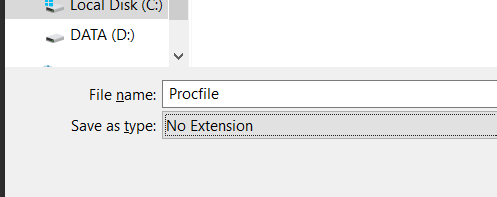
Step 1: heroku login



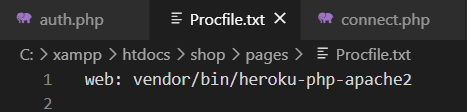
Step 2: heroku create



Step 3: mở visual code ->New file -> Save as -> “Procfile”

● Add this line -> web: vendor/bin/heroku-php-apache2



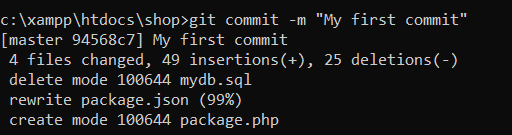
Step 4: ● git init



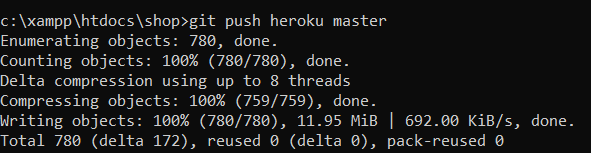
Step 5: ● git add .

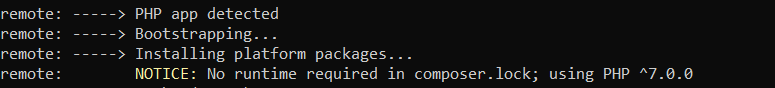


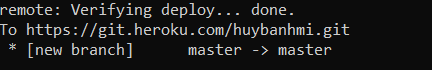
Step 6: git commit -m “My first commit”



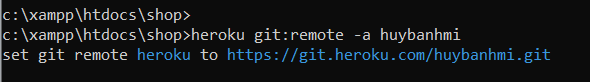
Step 7: git push heroku master



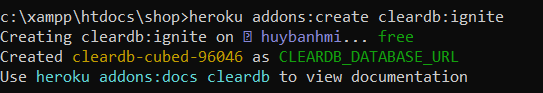




Step 8:• heroku git:remote -a “yourappname”

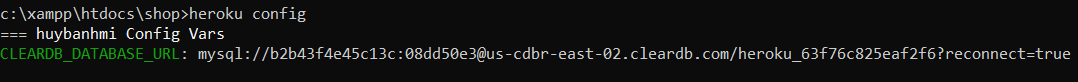


Step 9: heroku addons:create cleardb:ignite



● heroku config

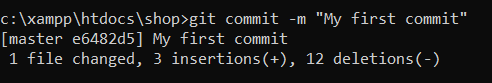
● mysql://username:password@servername/databasename?.....



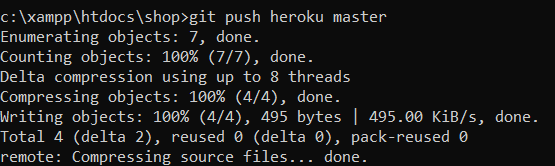
Step 10: git add .



Step 11: git commit -m “My first commit”



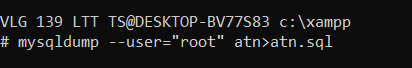
Step 12: git push heroku master



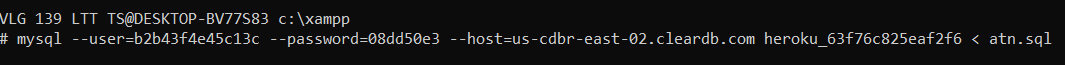
Step 13: Dump database

● Export database

● mysqldump --user=”root” mydb > mydb.sql



● Import database



**P7 Analyse the most common problems which arise in a Cloud Computing platform and discuss appropriate solutions to these problems.**

Cloud computing has benefited many businesses by reducing costs and allowing focus on the core business capabilities of an enterprise, rather than on infrastructure and IT issues. However, cloud computing can have the smallest operational problems:

1. Security and privacy

Any cloud service provider is expected to manage and safeguard the underlying hardware infrastructure of a deployment. However, your responsibilities lie in the realm of user access management, and it’s up to you to carefully weigh all the risk scenarios. Though recent breaches of credit card data and user login credentials are still fresh in the minds of the public, steps have been taken to ensure the safety of data.

* Best practices for minimizing security and privacy risks
* Encryption, encryption, encryption. Turn on encryption wherever you can — easy wins are on object storage such as Amazon, where customer data often resides.
* Implement security at every level of your deployment
* Performs multi-factor authentication for all accounts that access sensitive data or systems.
* Take a risk-based approach to ensure assets are used in the cloud and secure devices.
* Know who is supposed to have access to each resource and service, and limit access to the least privileged level. If an employee cheats and gains access to your implementation, you'll want their impact on the smallest extent possible.

1. Vulnerability to attack

In cloud computing, every component is online, which exposes potential vulnerabilities. Even the best teams suffer severe attacks and security breaches from time to time. Since cloud computing is built as a public service, it’s easy to run before you learn to walk. After all, no one at a cloud vendor checks your administration skills before granting you an account: all it takes to get started is generally a valid credit card

#### Best practices to help you reduce cloud attacks

* Integrate prevention and response strategies into security operations.
* Discover rogue projects with audits
* Make security a core aspect of all IT operations.
* Remove password access from accounts that do not need to log in to services.
* Apply security best practices for any open source software that you are using
* Proactively classify information and apply access control
* Follow security blogs and announcements to be aware of known attacks.
* Again, use encryption whenever and wherever possible.

1. Limited control and flexibility

* Since the cloud infrastructure is entirely owned, managed, and monitored by the service provider, it transfers minimal control over to the customer.
* To varying degrees, cloud users may find they have less control over the function and execution of services within a cloud-hosted infrastructure. A cloud provider’s end-user license agreement and management policies might impose limits on what customers can do with their deployments. Customers retain control of their applications, data, and services, but may not have the same level of control over their backend infrastructure.
* Best practices for maintaining control and flexibility
* Consider using a cloud provider partner to help with implementing, running, and supporting cloud services.
* Understand your responsibilities and the responsibilities of the cloud vendor in the shared responsibility model to reduce the chance of omission or error.
* Make time to understand your cloud service provider’s basic level of support. Will this service level meet your support requirements? Most cloud providers offer additional support tiers over and above the basic support for an additional cost.

1. Cost concerns

* Adopting cloud applications on a small scale that may be viewed as costly for short-term projects. However, in terms of The cost savings, the most important advantage for cloud computing is. However, in terms of The cost savings, the most important advantage for cloud computing is. Cloud services that pay-as-you-go will offer more versatility and lower hardware costs, but the overall price tag could end up being higher than you anticipated. It's a good idea to play with a range of offerings before you are sure of what would work best for you. You might also make use of the cost calculators made available by providers like Amazon Web Services and Google Cloud Platform.
* Best practices to reduce costs
* Try not to over provision your services, but rather look into using auto-scaling services.
* Ensure you have the option to scale DOWN as well as UP.
* Pre-pay and take advantage of reserved instances if you have a known minimum usage.
* Automate the process to start/stop your instances to save money when they are not being used.
* Create alerts to track cloud spending.

# P8 Assess the most common security issues in cloud environments.

* Moving to the cloud is not just a trend, it's becoming a requirement for any organization looking to build better team collaboration, increase productivity, and improve customer experience. But the move to the cloud presents whole new opportunities for human error, attacks, and violations from the mobile workforce. Security issues in the cloud are similar to what you might encounter with on-premises and network computing. However, to prevent and fix cloud security issues, they must be managed in a different way.
* Amazon Web Services (AWS) brings many benefits to your cloud platform, either alone or as a part of a hybrid cloud environment. The flexibility of AWS platforms as services (PaaS) and as services infrastructure (IaaS) makes your organizational network responsive, flexible and easy to use. But they do have safety considerations. Here are some reviews, along with security best practices that keep your AWS environment properly configured and secure

1. Access key

* IAM access keys are not usually rotated. This impairs IAM's ability to secure accounts and groups of users, so the attacker has a longer time on the computer to steal information.
* Best price: Delete or change your access password at least once within 90 days. If you have granted the user the necessary permissions, they can delete their previously accessed private passwords. From there, make sure the old keys are not used to access important services.

2. Exposed root accounts - Root accounts exposed

* Your root account can do great damage when unauthorized parties gain access to them. Administrators often forget to disable native API access.
* Best price: With multi-factor authentication the root account must be protected and used sparingly. Most of the time, even your top admins don't have access to your AWS root account and never share it with users and apps across IAM.

3. Privilege access

* IAM can be deployed with detailed policies and licensing options, to manage all of your accounts and user groups. Sadly, administrators frequently specify unauthorized access to AWS resources. This not only allows users to make changes and have access rights that they should not, but it could do even more harm if a network attacker gets their account.
* Best Practice: Configure your IAM, like any user licensing system, to adhere to the principle of minimum access privileges.

4. Wide IP range for security groups and unrestricted external traffic

* Security groups are like a firewall controlling AWS environment traffic. Unfortunately, administrators often specify a wider than needed range of security group IPs. Cloud Research Team Research. Security groups with unlimited external traffic account for up to 85 per cent of resources. Moreover, there is growing concern that more organizations are failing to adhere to best practices in network security and have misconfiguration or risky configurations. Industry best practices call for restriction of outbound access to prevent data loss in the event of an infringement due to accidental or data outages.
* Best price: Limit the range of IPs you assign to each security group in such a way that everything is on the correct network, but you don't need to leave too much information behind.

5. Vision

* Cloud resources are not sustainable so data tracking and management is difficult. The mean lifespan of a cloud resource is two hours and seven minutes, according to our research. And many businesses have environments with multiple regions and cloud accounts involved. This results in decentralized visibility, and since you can secure what you can see, it makes risk detection difficult.
* Best price: Using a cloud security solution to get a view of the data management volume and resource types (virtual machines, equalizers, security groups, users) on m44574ultiple accounts and the cloud area. Having a vision and understanding of your environment allows you to implement detailed risks reduction policies more.

6. Audit history

* Organizations should monitor user activities to avoid disclosure of accounts information, internal threats and other risks. The core virtualization of the cloud network and the usability of the infrastructure of a third-party provider are huge and sufficiently experienced, as privileged users can change environments as necessary. The downside is that there isn't enough potential for security monitoring.
* To avoid th**i**s risk, user activities must be monitored to identify the account and internal threats.

7. Authentication process

* Stolen or lost information is the leading cause of cloud security issues, according to the Verizon's annual Data Breach Investigation Report. It is not uncommon to find access information to an internet-displayed public cloud environment. Organizations need to guard against theft of accounts.
* In an AWS environment strong password policy and multifactor authentication (MFA) should be enforced. Amazon recommends that you enable MFA on the Dashboard for all accounts with passwords. First, identify which account holds an MFA. Then go into IAM and select all users for the MFA device. Authentication can be done via smartphones and other devices.

REFERENCE

<https://cloudacademy.com/blog/disadvantages-of-cloud-computing/>

<https://www.mcafee.com/enterprise/en-us/security-awareness/cloud/security-issues-in-cloud-computing.html>

<https://renovacloud.com/8-cach-tot-nhat-ve-bao-mat-aws-de-giam-thieu-rui-ro-co-rat-nhieu-loi-ich-ma-ban-ma-amazon-web-services-aws-mang-lai-cho-nen-tang-dam-may-cho-ban-doc-lap-hoac-la-mot-phan-cua-moi-truong-dam-may-lai/>