

ASSIGNMENT 2

Qualification	BTEC Level 5 HND Diploma in Computing		
Unit number and title	Unit 16: Cloud Computing		
Submission date	8/04/2023	Date Received 1st submission	12/04/2023
Re-submission Date		Date Received 2nd submission	
Student Name	Tran Hoang Anh	Student ID	BH00173
Class	IT0501	Assessor name	Le Van Thuan
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	

Grading grid

P5	P6	P7	P8	M3	M4	D2	D3

⚙ **Summative Feedback:**

⚙ **Resubmission Feedback:**

Grade:

Assessor Signature:

Date:

Signature & Date:

Contents

I.Introduction	5
II.Body	5
P5 Configure a Cloud Computing platform with a cloud service provider's framework.	5
P6 Implement a cloud platform using open source tools.	7
1.Home Page	8
4. Demo.....	14
4.1. Demo Register	14
4.2. Demo Login	15
4.3.Demo Add to cart from customer	16
5.Demo create product from admin	20
P7 Analyse the most common problems which arise in a Cloud Computing platform and discuss appropriate solutions to these problems.	24
P8 Assess the most common security issues in cloud environments.	27
3. Insider threats	33
4. Misconfiguration.....	35
III.Conclusion	42
IV.Reference	42

Figures

Figure 1:Homepage 1	9
Figure 2:Homepage 2	9
Figure 3:Product.....	10
Figure 4:Cart.....	11
Figure 5:Category	12
Figure 6:Login and Register.....	13

Figure 7:Demo Register.....	15
Figure 8:Demo Login 1	16
Figure 9:Demo Login 2	16
Figure 10: Info of Product	17
Figure 11:Demo Cart 1	18
Figure 12:Demo Cart 2	19
Figure 13:Demo create product.....	20
Figure 14:Product when added.....	21
Figure 15: Action include: edit and delete.....	21
Figure 16: Edit Product	22
Figure 17: Delete product (Here will appear a alert ' Do you want to delete ?').....	23
Figure 18: The common data breaches	28
Figure 19:Top data breaches	29
Figure 20: SQL injection attack	40

I.Introduction

In the scientific world, cloud computing has received a lot of attention. Cloud computing is a methodology for provides on-demand network access to a shared pool of programmatic computing resources that can be deployed and released quickly and with little administrative effort. I'm a company employee of ATN, will design a cloud computing solution in this assignment 2, I will explain it more clearly as well as have instructions and demo steps.

II.Body

P5 Configure a Cloud Computing platform with a cloud service provider's framework.

As mentioned in exercise 1 about designing a model to be able to put the website of ATN company on the system. I used the public cloud system. Besides, I will use PaaS and IaaS service delivery platforms to combine. This will be optimized by me and presented according to the diagram below.

1. Amazon Web Services (IaaS)

Amazon Web Services (AWS) can help your business thrive. AWS is the world's most comprehensive and broadly adopted cloud platform. Offering over 175 fully-featured cloud services from data centers around the globe, organizations from large enterprises and governmental agencies to fast-growing startups, have easy access to IT services like processing, networking, storage, security and more. AWS helps them lower costs, become more agile and innovate faster to scale and grow.

AWS is commonly used for:

- Storing large amounts of data
- Processing large datasets
- Handling peak loads for e-commerce websites

- Hosting static websites
- Hosting dynamic applications or websites with web, application and database tiers
- And so much more

Some additional benefits of AWS, beyond what's listed above, include:

- Better security options
- Increased productivity through automation
- New revenue streams through differentiated solutions
- Higher availability leading to improved user satisfaction
- Rapid experimentation and transformation in response to business changes and needs
- Faster innovation and time to market
- Reduced costs with better performance
- Open standards eliminate getting locked into one vendor

Below are the steps to implement and use AWS that I apply in this project. Follow my steps below:

- Step 1: Register AWS
- Step 2: Active account and Login
- Step 3: Create Instance (EC2)
- Step 4: Set up system and open port
- Step 5: Connect with VMWare (XShell)

P6 Implement a cloud platform using open source tools.

Below I will perform the operations and functions of the website to check if the website is really running or not.

The functions I will perform include:

- Registration
- Log in
- Product
- Category
- Cart

Link github: https://github.com/HoangAnh3723/toy_shop.git

1.Home Page

[Login](#) | [Contact](#)

TOY STORE ONLINE

Cart (0)

[HOME PAGE](#)
[CATEGORY](#)
[CART](#)
[CONTACT](#)

12-12


DEAL DAY

SẴN NGAY

FREESHIP - GÓI QUÀ MIỄN PHÍ*


TỪ 1 - 15/12/2021

* FREESHIP CHO ĐƠN HÀNG TỪ 200K
* KÈM CHỈ CHỖ CÓ QUÀ TẶNG BƯỚC BẮT HÀNG ĐỂ ĐƯỢC CÓ QUÀ MIỄN PHÍ




MUA NGAY

Sale Toys




Disney Encanto Dolores Mirabel Fashion Doll 11 Inches

229\$ ~~209\$~~




LEGO Pirates Imperial Flagship (10210) (Discontinued by manufacturer)

36.234\$ ~~31.000\$~~



Melissa & Doug Mine to Love Jenna 12-Inch Soft Body Baby Doll

551\$ ~~499\$~~



NERF Ultra Strike Motorized Blaster

436\$ ~~404\$~~

Figure 1:Homepage 1

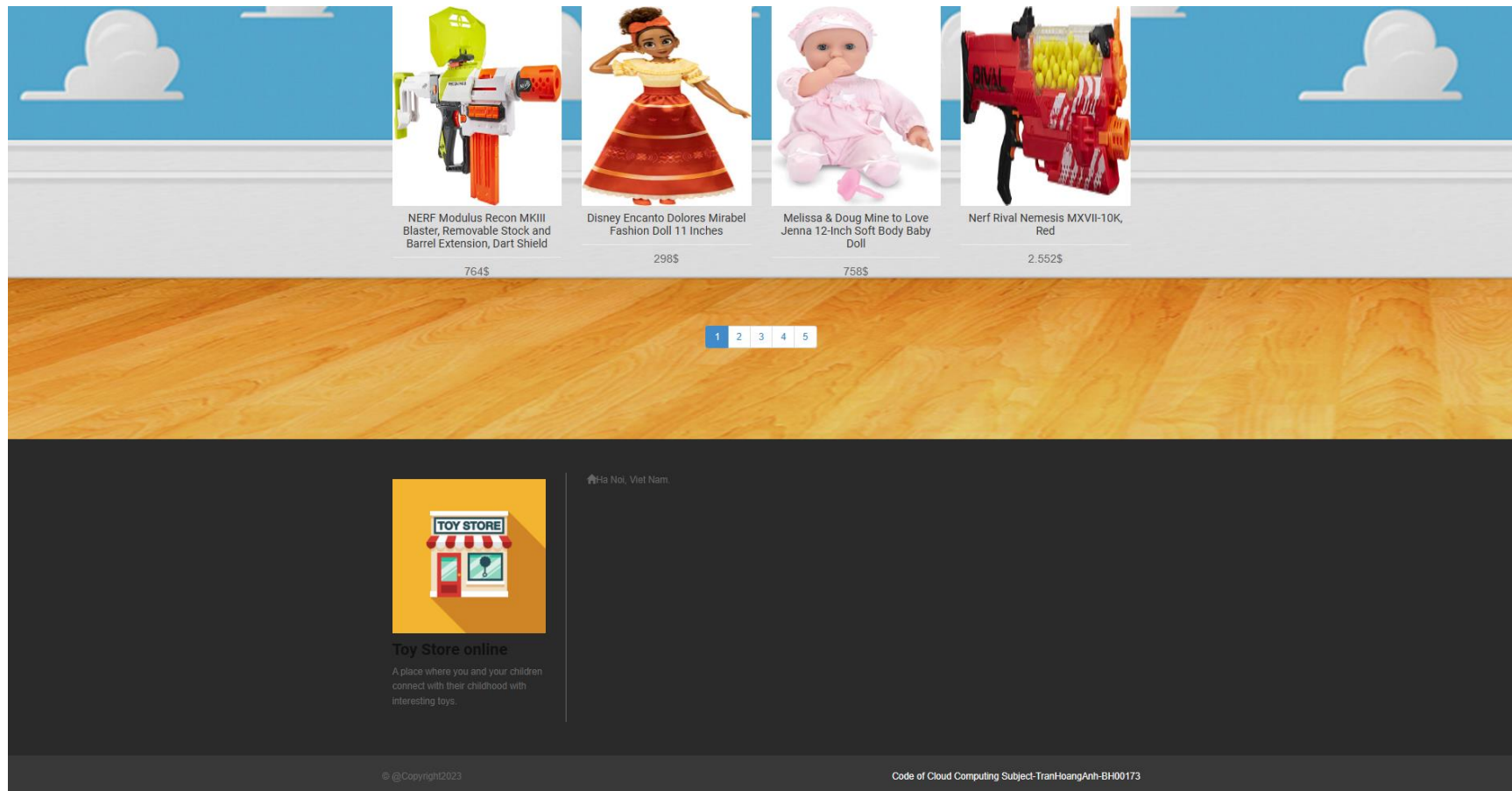


Figure 2:Homepage 2

2.Product

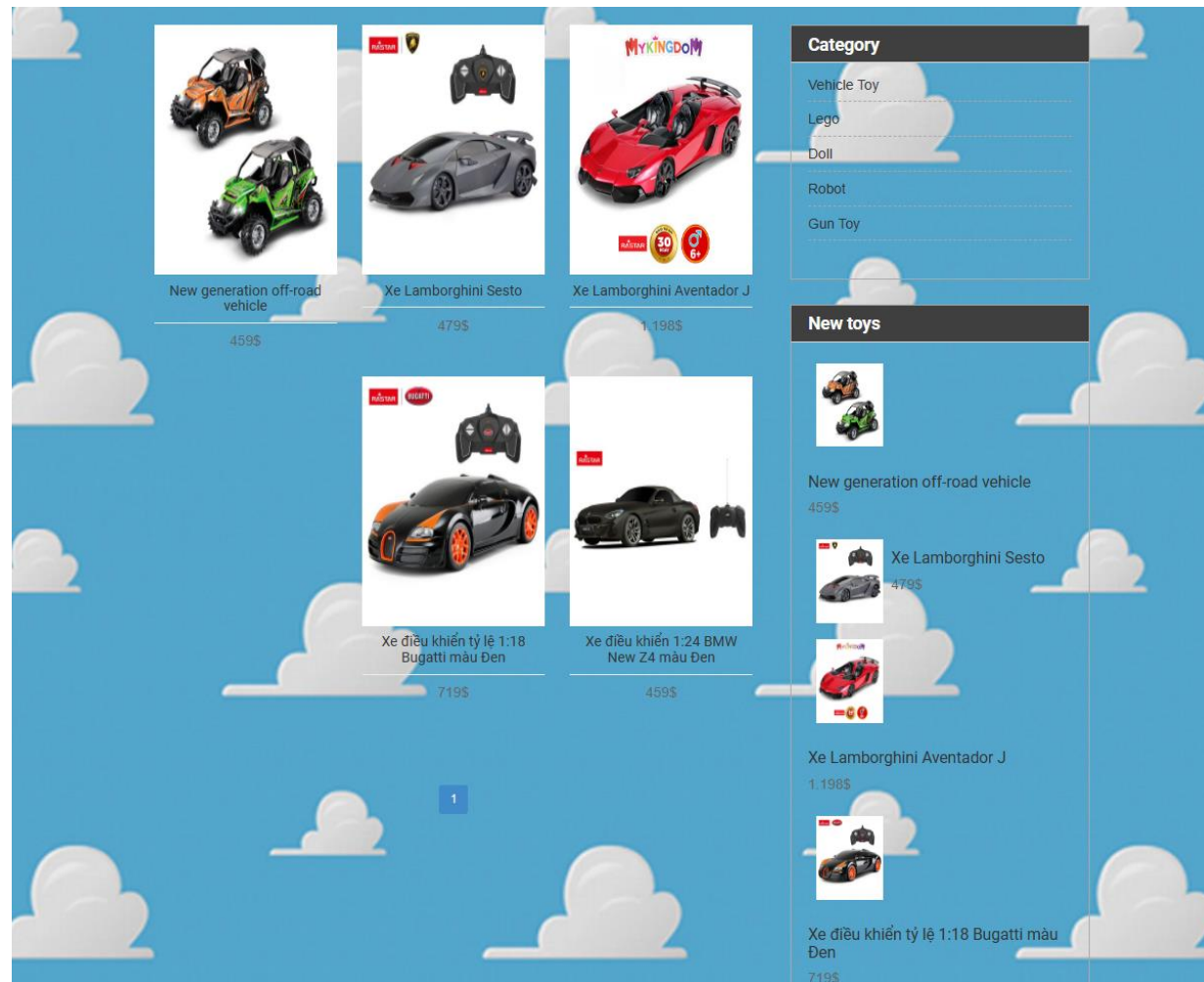


Figure 3:Product

3.Cart

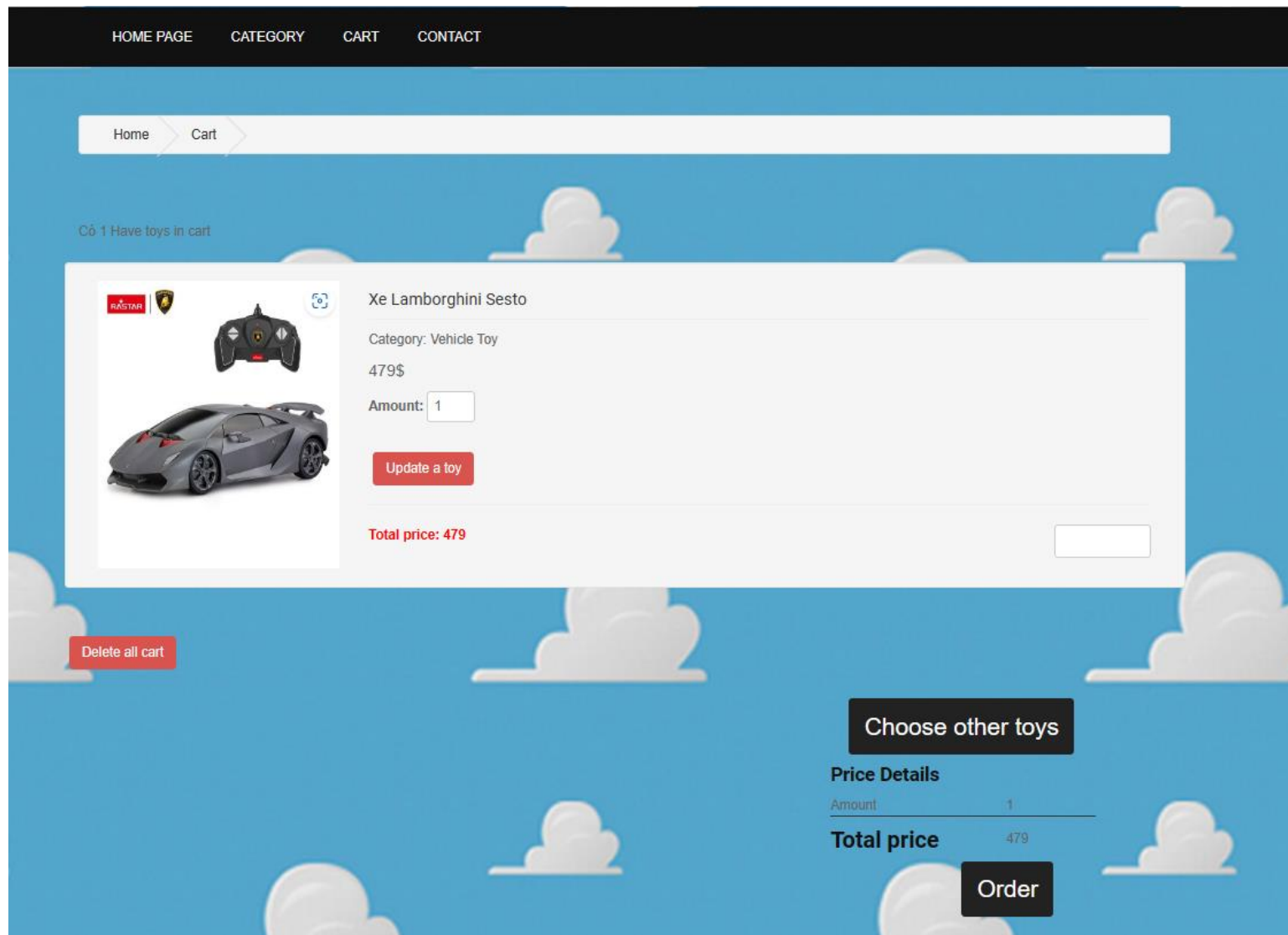


Figure 4:Cart

4.Category

[HOME PAGE](#)
[CATEGORY](#)
[CART](#)
[CONTACT](#)

Home Page


VEHICLE TOY

LEGO

DOLL


ROBOT

GUN TOY




Trạm Cảnh Sát

6.399\$




LEGO Star Wars Millennium Falcon 7965

8.947\$




Ulanlan Military Vehicle Building Blocks Sets with 6 Mini Soldiers

562\$



LEGO Icons Chevrolet Camaro Z28 10304

3.908\$



LEGO Pirates Imperial Flagship (10210) (Discontinued by manufacturer)

37.953\$

Category

Vehicle Toy


LEGO

Doll

Robot


Gun Toy

New toys




New generation off-road vehicle

459\$



Xe Lamborghini Sesto

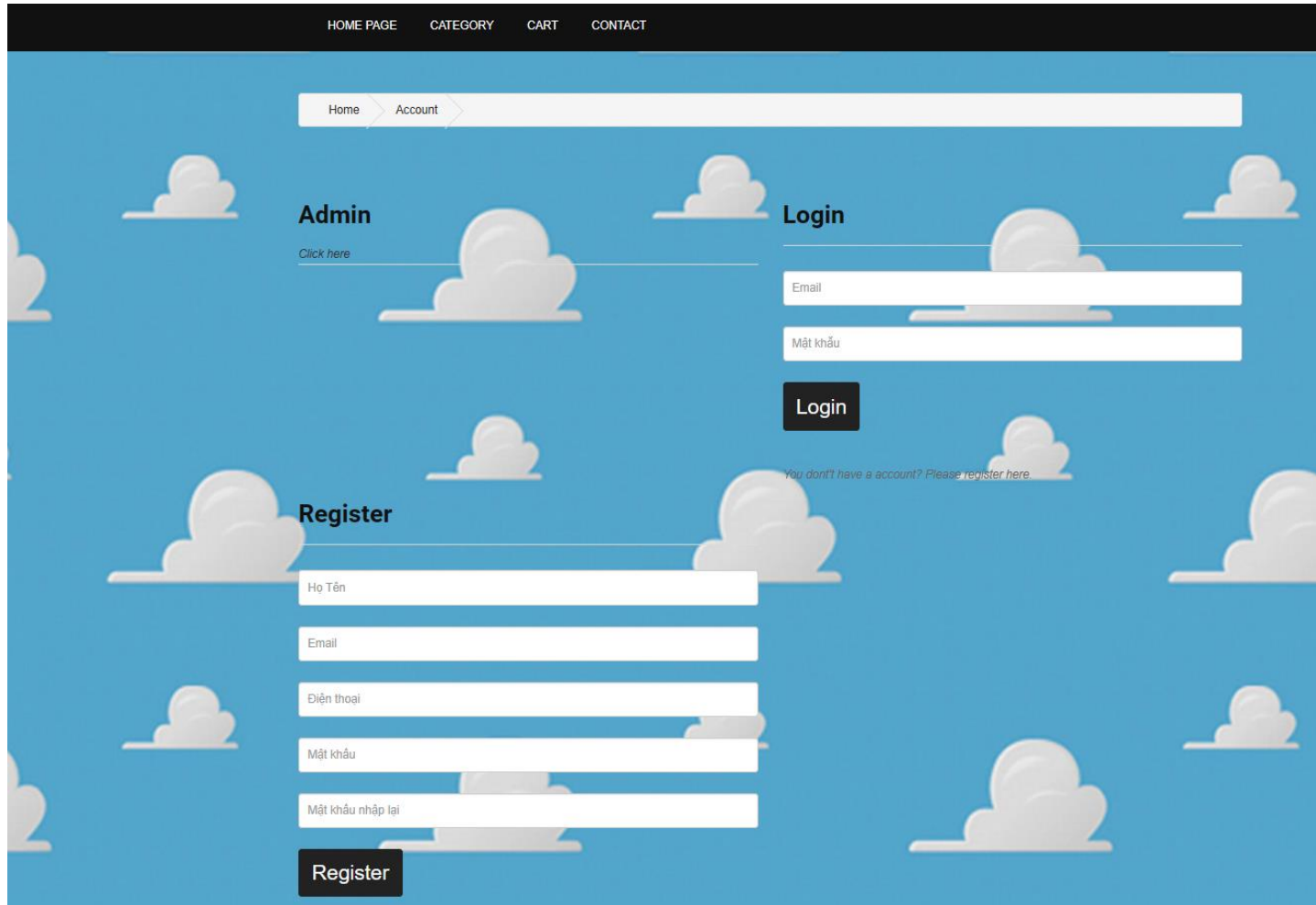
479\$



Xe Lamborghini Aventador J

Figure 5:Category

5.Log in and Register



HOME PAGE CATEGORY CART CONTACT

Home > Account >

Admin
[Click here](#)

Login

Email

Mật khẩu

Login

[You don't have a account? Please register here.](#)

Register

Họ Tên

Email

Điện thoại

Mật khẩu

Mật khẩu nhập lại

Register

Figure 6:Login and Register

4. Demo

4.1. Demo Register

I will create an account with the following information:

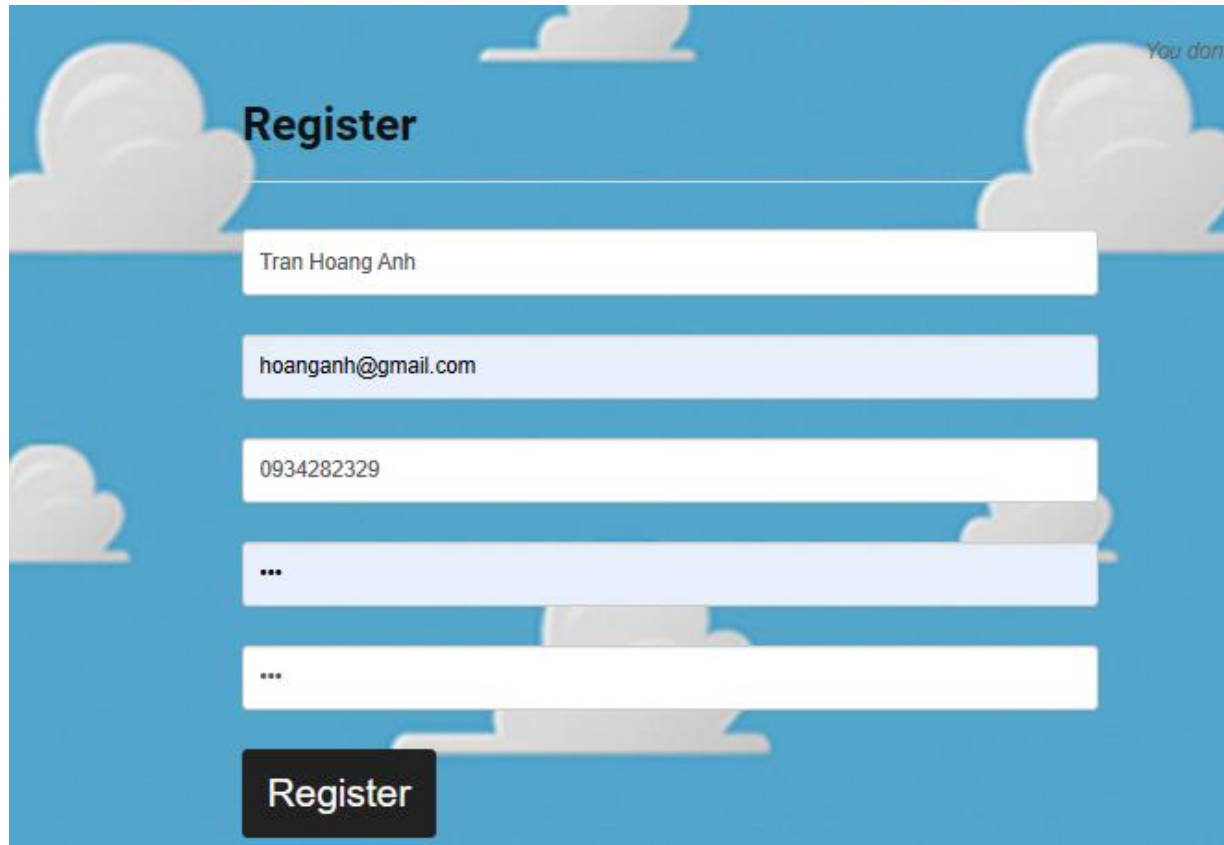
Fullname: Tran Hoang Anh

Email: hoanganh@gmail.com

Phone:0934282329

Password:123

Re-password:123

The image shows a registration form titled "Register" on a blue background with white clouds. The form has five input fields: a name field containing "Tran Hoang Anh", an email field containing "hoanganh@gmail.com", a phone number field containing "0934282329", and two password fields, each containing three dots "..." to indicate masked text. A black "Register" button is at the bottom left of the form area. In the top right corner of the form area, the text "You don't?" is visible.

Register

Tran Hoang Anh

hoanganh@gmail.com

0934282329

...

...

Register

You don't?

Figure 7: Demo Register

4.2. Demo Login

I will login the account information I just created with email:hoanganh@gmail.com and password 123

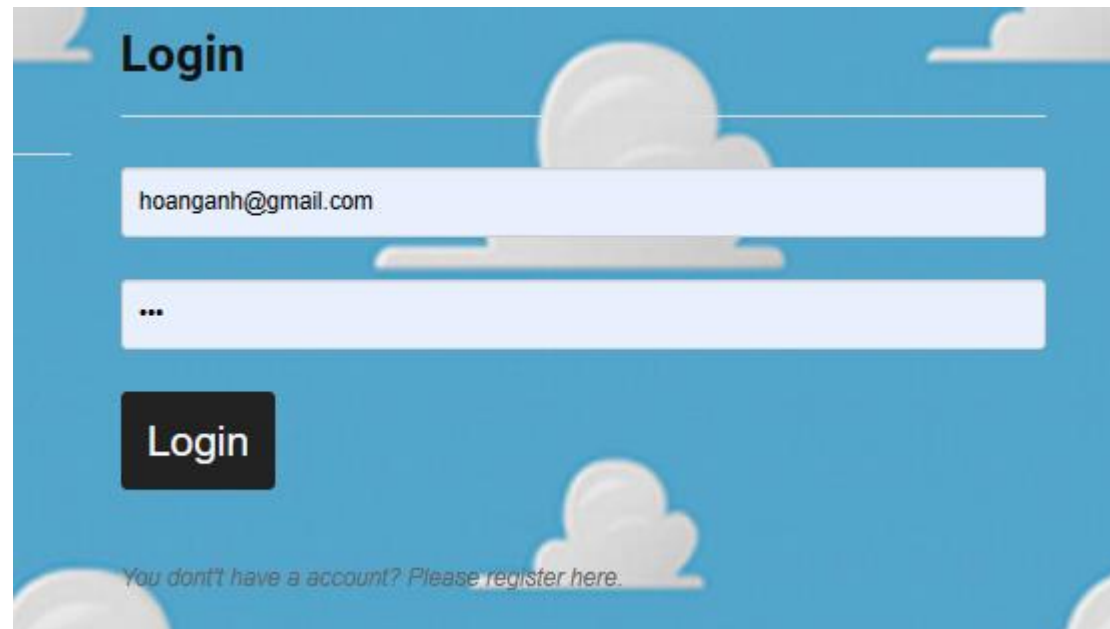


Figure 8:Demo Login 1

And this is the result:

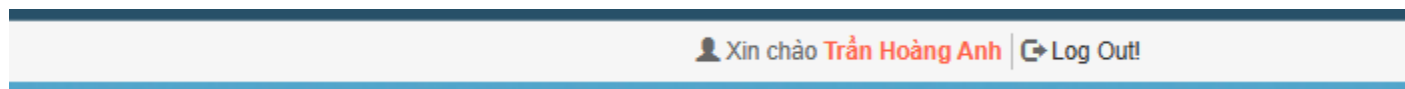



Figure 9:Demo Login 2

4.3.Demo Add to cart from customer

Choose random product, here I'll choose product "New generation off-road vehicle":

[Home page](#)
[Toy](#)
[New generation off-road vehicle](#)



New generation off-road vehicle

Trademark: VECTO

Category: Vehicle Toy


344\$ - 459\$

[add to cart](#)
[BUY NOW!!!](#)

Category


- Vehicle Toy
- Lego
- Doll
- Robot
- Gun Toy

New toys




New generation off-road vehicle

459\$



Xe Lamborghini Sesto

479\$



Xe Lamborghini Aventador J

1.198\$

Toy infor

Đồ Chơi VECTO Xe Vượt Địa Hình Thế Hệ Mới (Xanh Lá) VT1918/GR

Là phiên bản nâng cấp của các mẫu xe vượt địa hình điều khiển từ xa trước đây. Xe vượt địa hình thế hệ mới được cải tiến cả từ bên ngoài lẫn bên trong, tạo nên một phiên bản hoàn hảo mà bé trai nào cũng muốn sở hữu cho mình một chiếc.

- Vẻ ngoài độc đáo với các đường nét được cắt dọc thân xe một cách mạnh mẽ, kết hợp cùng phong cách phối màu theo trường phái hiện đại tạo nên một vẻ ngoại quan độc nhất, mà khó có dòng xe nào trên thị trường sở hữu được.
- Chưa dừng lại ở đó, với hệ thống công nghệ tân tiến bên trong giúp xe di chuyển vô cùng mượt mà khi bé điều khiển. Chắc chắn giúp bé dễ dàng chinh phục mọi địa hình trên đường đua.

Bộ sản phẩm Xe vượt địa hình thế hệ mới bao gồm:

- 1 x Xe điều khiển (sử dụng pin sạc/ có đi kèm)
- 1 x Remote điều khiển (Sử dụng pin tiểu/ không đi kèm)
- 1 x Cáp sạc USB

VECTO - THẾ GIỚI ĐỒ CHƠI BÉ TRAI CỰC ĐỈNH

VECTO là thương hiệu đồ chơi dành riêng cho các bé trai, với các dòng đồ chơi trải dài từ đồ chơi mô hình cho đến các đồ chơi điều khiển từ xa. Với mong muốn giúp các bé trai có một sự phát triển toàn diện từ trí não đến thể chất, Vecto đã phát triển đa dạng các loại đồ chơi để đem đến cho bé nhiều lựa chọn nhất có thể, có thể kể đến như:

Figure 10: Info of Product

It'll show all information about product (Trademark, category, price, info). Then we can click to button" Add to cart":

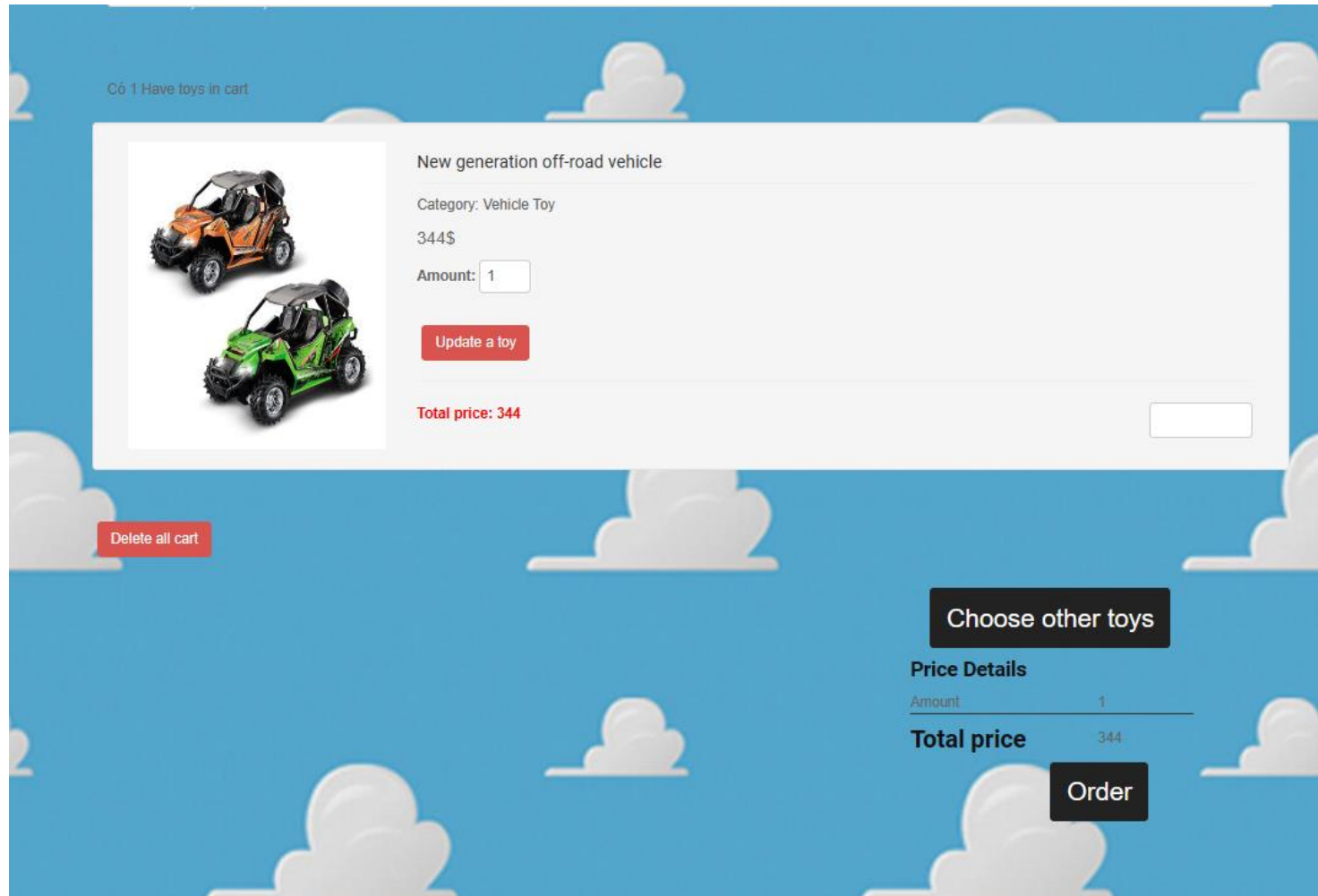


Figure 11: Demo Cart 1

At the cart, it'll show informations about:

- Update toy: can increase amount of product and it'll edit total price.
- Delete all cart: delete all added products

- Choose other toys: Go to Homepage
- Order: It'll display about info of customer, Item info, image of product and can choose payment and service.

[Home page](#)
[Confirm a order](#)



Customer info

Tên customer : Trần Hoàng Anh

Điện thoại: 0934282329

Email: hoanganh@gmail.com

Enter a address to delivery

04/12/2023  Payment: Pay card 


Item info

Toy	Amount	Price
New generation off-road vehicle	1	344\$
Total Price:		344\$

service

Choose service

Toy (1)



New generation off-road vehicle

Category: Vehicle Toy

344\$

Số lượng : 1

Order

Figure 12: Demo Cart 2

5.Demo create product from admin

Toy Store online

Account

Admin

Online

Admin page

Management

List

Thêm Toy

Thêm Toy

Tên

NERF Modulus Recon MKIII Blaster, Removable Stock and Barrel Extension, Dart Shield

Hình ảnh

Choose File 01_244.jpg

Thương hiệu

DGH

Category

Vehicle Toy

Ngày

03/31/2023

Giá

459

Khuyến mãi

Có khuyến mãi

Giá khuyến mãi

321

Mô tả

X Copy Paste Undo Redo Bold Italic Text Color Background Color Bulleted List Numbered List Link Unlink Full Screen Source Code MS HTML

B I S T A # = : * ~ ` " ' & # % ^ _ { } [\ | ; , . / ? ! @ \$ % ^ & * () - + = < > < > Kiểu Bình thư ... ?

goood

body p

Cancel

Create

Code of Cloud Computing Subject-TranHoangAnh-BH00173

Copyright © 2023

Figure 13: Demo create product

After press all info of product, it'll like below:

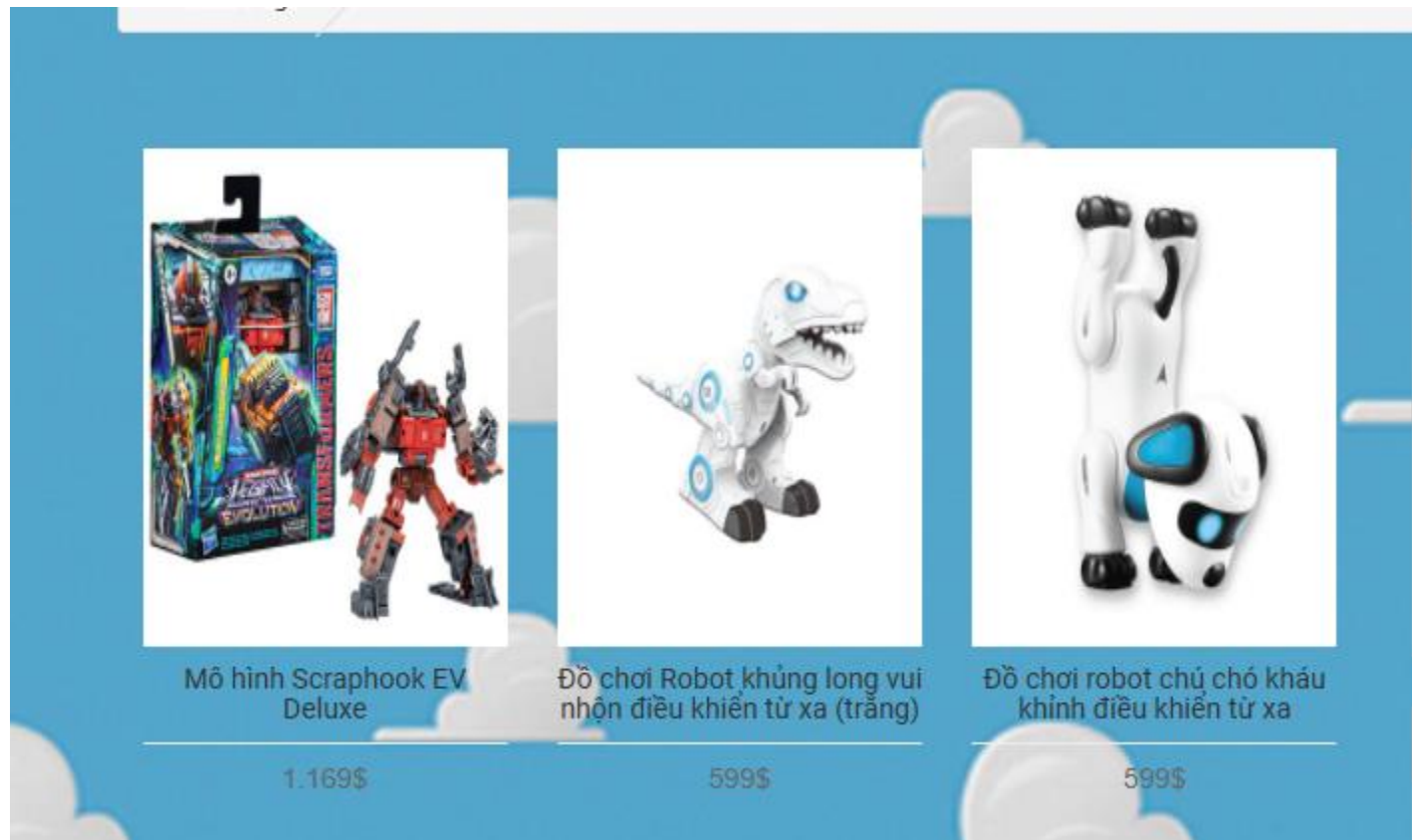


Figure 14:Product when added

Addition, I also can edit, delete products.




Name	Price	Image	Landmark	Category	Action
Disney Encanto Dolores Mirabel Fashion Doll 11 Inches	298		Jakks Pacific Inc.	Doll	 

Figure 15: Action include: edit and delete

Figure 16: Edit Product

Toy Store online

Admin

Online

























Admin page

Management

List

Manage Toy

Show 10 entries

Name	Price	Image	Landmark	Category	Action
Disney Encanto Dolores Mirabel Fashion Doll 11 Inches	298		Jakks Pacific Inc.	Doll	 
LEGO Icons Chevrolet Camaro Z28 10304	3.908		LEGO	Lego	 
LEGO Pirates Imperial Flagship (10210) (Discontinued by manufacturer)	37.953		Lego	Lego	 
LEGO Star Wars Millennium Falcon 7965	8.947		LEGO Star Wars	Lego	 
Melissa & Doug Mine to Love Jenna 12-Inch Soft Body Baby Doll	758		Melissa & Doug	Doll	 
Mô hình Scraphook EV Deluxe	1.169		TRANSFORMERS	Robot	 
NERF Modulus Recon MKIII Blaster, Removable Stock and Barrel Extension, Dart Shield	764		Hasbro	Gun Toy	 
Nerf Rival Nemesis MXVII-10K, Red	2.552		Hasbro	Gun Toy	 

localhost:8000 says

Do you actually want to delete ?

OK

Cancel

Account

Search:

localhost:8000/Admin/xaosp.php?id=237

Figure 17: Delete product (Here will appear a alert ' Do you want to delete ?')

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

Cloud computing is a general term for anything that involves delivering hosted services over the internet. These services are divided into three main categories or types of cloud computing: infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS).

A cloud can be private or public. A public cloud sells services to anyone on the internet. A private cloud is a proprietary network or a data center that supplies hosted services to a limited number of people, with certain access and permissions settings. Private or public, the goal of cloud computing is to provide easy, scalable access to computing resources and IT services.

Cloud infrastructure involves the hardware and software components required for proper implementation of a cloud computing model. Cloud computing can also be thought of as utility computing or on-demand computing.

The name cloud computing was inspired by the cloud symbol that's often used to represent the internet in flowcharts and diagrams.

It's evident that cloud computing is a trend that's only going to get bigger. We forecasted the relevance and deployment of the cloud in organizations like Alibaba, Amazon, Google, and Microsoft in our business intelligence trends piece.

There are several common problems that can arise when using a cloud computing platform, some of which include:

- **Data Security and Privacy**

Data security is a major concern when switching to cloud computing. User or organizational data stored in the cloud is critical and private. Even if the cloud service provider assures data integrity, it is your responsibility to carry out user authentication and authorization, identity management, data encryption, and access control. Security issues on the cloud include identity theft, data breaches, malware infections, and a lot more which eventually decrease the trust amongst the users of your applications. This can in turn lead to potential loss in revenue alongside reputation and stature. Also, dealing with cloud computing requires sending and receiving huge amounts of data at high speed, and therefore is susceptible to data leaks.

- **Solution:** Implement strong encryption techniques to secure sensitive data. Additionally, access controls and authentication mechanisms should be put in place to ensure that only authorized personnel can access the data. Regular audits and vulnerability assessments can also help identify and address any security gaps.

- **Cost Management**

Even as almost all cloud service providers have a “Pay As You Go” model, which reduces the overall cost of the resources being used, there are times when there are huge costs incurred to the enterprise using cloud computing. When there is under optimization of the resources, let’s say that the servers are not being used to their full potential, add up to the hidden costs. If there is a degraded application performance or sudden spikes or overages in the usage, it adds up to the overall cost. Unused resources are one of the other main reasons why the costs go up. If you turn on the services or an instance of cloud and forget to turn it off during the weekend or when there is no current use of it, it will increase the cost without even using the resources.

- **Solution:** implement strong encryption techniques to secure sensitive data. Additionally, access controls and authentication mechanisms should be put in place to ensure that only authorized personnel can access the data. Regular audits and vulnerability assessments can also help identify and address any security gaps.
- **Multi-Cloud Environments**

Due to an increase in the options available to the companies, enterprises not only use a single cloud but depend on multiple cloud service providers. Most of these companies use hybrid cloud tactics and close to 84% are dependent on multiple clouds. This often ends up being hindered and difficult to manage for the infrastructure team. The process most of the time ends up being highly complex for the IT team due to the differences between multiple cloud providers.

- **Solution:** implement strong encryption techniques to secure sensitive data. Additionally, access controls and authentication mechanisms should be put in place to ensure that only authorized personnel can access the data. Regular audits and vulnerability assessments can also help identify and address any security gaps.
- **Performance Challenges**

Performance is an important factor while considering cloud-based solutions. If the performance of the cloud is not satisfactory, it can drive away users and decrease profits. Even a little latency while loading an app or a web page can result in a huge drop in the percentage of users. This latency can be a product of inefficient load balancing, which means that the server cannot efficiently split the incoming traffic so as to provide the best user experience. Challenges also arise in the case of fault tolerance, which means the operations continue as required even when one or more of the components fail.

- **Solution:** implement strong encryption techniques to secure sensitive data. Additionally, access controls and authentication mechanisms should be put in place to ensure that only authorized personnel can access the data. Regular audits and vulnerability assessments can also help identify and address any security gaps.
- **Interoperability and Flexibility**

When an organization uses a specific cloud service provider and wants to switch to another cloud-based solution, it often turns up to be a tedious procedure since applications written for one cloud with the application stack are required to be re-written for the other cloud. There is a lack of flexibility from switching from one cloud to another due to the complexities involved. Handling data movement, setting up the security from scratch and network also add up to the issues encountered when changing cloud solutions, thereby reducing flexibility.

- **Solution:** implement strong encryption techniques to secure sensitive data. Additionally, access controls and authentication mechanisms should be put in place to ensure that only authorized personnel can access the data. Regular audits and vulnerability assessments can also help identify and address any security gaps.
- **High Dependence on Network**

Since cloud computing deals with provisioning resources in real-time, it deals with enormous amounts of data transfer to and from the servers. This is only made possible due to the availability of the high-speed network. Although these data and resources are exchanged over the network, this can prove to be highly vulnerable in case of limited bandwidth or cases when there is a sudden outage. Even when the enterprises can cut their hardware costs, they need to ensure that the internet bandwidth is high as well there are zero network outages, or else it can result in a potential business loss. It is therefore a major challenge for smaller enterprises that have to maintain network bandwidth that comes with a high cost.

- **Solution:** implement strong encryption techniques to secure sensitive data. Additionally, access controls and authentication mechanisms should be put in place to ensure that only authorized personnel can access the data. Regular audits and vulnerability assessments can also help identify and address any security gaps.
- **Lack of Knowledge and Expertise**

Due to the complex nature and the high demand for research working with the cloud often ends up being a highly tedious task. It requires immense knowledge and wide expertise on the subject. Although there are a lot of professionals in the field they need to constantly update themselves. Cloud computing is a highly paid job due to the extensive gap between demand and supply. There are a lot of vacancies but very few talented cloud engineers, developers, and professionals. Therefore, there is a need for upskilling so these professionals can actively understand, manage and develop cloud-based applications with minimum issues and maximum reliability.

- **Solution:** invest in training and development programs to equip staff with the necessary skills and knowledge. Additionally, working with experienced cloud service providers can help leverage their expertise and best practices.

P8 Assess the most common security issues in cloud environments.

Cloud security is the protection of data stored online via cloud computing platforms from theft, leakage, and deletion. Methods of providing cloud security include firewalls, penetration testing, obfuscation, tokenization, virtual private networks (VPN), and avoiding public internet connections. Cloud security is a form of cybersecurity.

Key takeaways:

- Cloud security refers broadly to measures undertaken to protect digital assets and data stored online via cloud services providers.
- Cloud computing is the delivery of different services through the Internet, including data storage, servers, databases, networking, and software.
- Measures to protect this data include two-factor authorization (2FA), the use of VPNs, security tokens, data encryption, and firewall services, among others.

Cloud computing is the delivery of different services through the Internet. These resources include tools and applications like data storage, servers, databases, networking, and software. Rather than keeping files on a proprietary hard drive or local storage device, cloud-based storage makes it possible to save them to a remote database. As long as an electronic device has access to the web, it has access to the data and the software programs to run it. Cloud computing is a popular option for people and businesses for a number of reasons including cost savings, increased productivity, speed and efficiency, performance, and security.

Cloud security is essential for the many users who are concerned about the safety of the data they store in the cloud. They believe their data is safer on their own local servers where they feel they have more control over the data. But data stored in the cloud may be more secure because cloud service providers have superior security measures, and their employees are security experts. On-premise data can be more vulnerable to security breaches, depending on the type of attack. Social engineering and malware can make any data storage system vulnerable, but on-site data may be more vulnerable since its guardians are less experienced in detecting security threats.

The security issues:

1.Data breaches

A data breach is an incident where information is stolen or taken from a system without the knowledge or authorization of the system's owner. A small company or large organization may suffer a data breach. Stolen data may involve sensitive, proprietary, or confidential information such as credit card numbers, customer data, trade secrets, or matters of national security.

The effects brought on by a data breach can come in the form of damage to the target company's reputation due to a perceived 'betrayal of trust.' Victims and their customers may also suffer financial losses should related records be part of the information stolen.

Based on the number of data breach incidents recorded between January 2005 and April 2015, personally identifiable information (PII) was the most stolen record type while financial data came in second.



Figure 18: The common data breaches

Most data breaches are attributed to hacking or malware attacks. Other frequently observed breach methods include the following:

- **Insider leak:** A trusted individual or person of authority with access privileges steals data.
- **Payment card fraud:** Payment card data is stolen using physical skimming devices.
- **Loss or theft:** Portable drives, laptops, office computers, files, and other physical properties are lost or stolen.
- **Unintended disclosure:** Through mistakes or negligence, sensitive data is exposed.
- **Unknown:** In a small number of cases, the actual breach method is unknown or undisclosed.

Date	Organization	Industry	Number of Records Stolen
Between 2013 and 2014	Yahoo	Email service provider	3,000,000,000
October 2016	Adult Friend Finder	Adult website	412,200,000
May 2016	MySpace	Social media website	360,000,000
Between 2007 and February 2013	Experian	Credit bureau	200,000,000
2012	LinkedIn	Social media website	165,000,000
February 2018	Under Armour/MyFitnessPal	Fitness mobile app	150,000,000
Between May and July 2017	Equifax	Information solutions company	145,500,000
May 2014	eBay	Online auction website	145,000,000
March 2008	Heartland Payment Systems	Credit and debit processor	134,000,000
December 2013	Target	Retailer	110,000,000
17-19 April 2011 (discovery date)	Sony PlayStation Network	Electronics firm	102,000,000

Figure 19: Top data breaches

2. Malware and viruses

2.1. Malware

Malware is a catch-all term for any type of malicious software, regardless of how it works, its intent, or how it's distributed. A virus is a specific type of malware that self-replicates by inserting its code into other programs. Computer viruses have been prominent since almost the beginning of the commercial internet: The first one was created in 1982 for the Apple II, and other versions quickly followed.

Malware can infect networks and devices and is designed to harm those devices, networks and/or their users in some way.

Depending on the type of malware and its goal, this harm may present itself differently to the user or endpoint. In some cases, the effect malware has is relatively mild and benign, and in others, it can be disastrous.

Type of Malware:

- **Worms**

A worm is a standalone program that can self-replicate and spread over a network. Unlike a virus, a worm spreads by exploiting a vulnerability in the infected system or through email as an attachment masquerading as a legitimate file. A graduate student created the first worm (the Morris worm) in 1988 as an intellectual exercise. Unfortunately, it replicated itself quickly and soon spread across the internet.

- **Ransomware.**

As the name implies, ransomware demands that users pay a ransom—usually in bitcoin or other cryptocurrency—to regain access to their computer. The most recent category of malware is ransomware, which garnered headlines in 2016 and 2017 when ransomware infections encrypted the computer systems of major organizations and thousands of individual users around the globe.

- **Scareware.**

Many desktop users have encountered scareware, which attempts to frighten the victim into buying unnecessary software or providing their financial data. Scareware pops up on a user's desktop with flashing images or loud alarms, announcing that the computer has been infected. It usually urges the victim to quickly enter their credit card data and download a fake antivirus program.

- **Adware and spyware.**

Adware pushes unwanted advertisements at users and spyware secretly collects information about the user. Spyware may record the websites the user visits, information about the user's computer system and vulnerabilities for a future attack, or the user's keystrokes. Spyware that records keystrokes is called a keylogger. Keyloggers steal credit card numbers, passwords, account numbers, and other sensitive data simply by logging what the user types.

- **Fileless malware.**

Unlike traditional malware, fileless malware does not download code onto a computer, so there is no malware signature for a virus scanner to detect. Instead, fileless malware operates in the computer's memory and may evade detection by hiding in a trusted utility, productivity tool, or security application.

2.2. Virus

Viruses spread by attaching themselves to legitimate files and programs, and are distributed through infected websites, flash drives, and emails. A victim activates a virus by opening the infected application or file. Once activated, a virus may delete or encrypt files, modify applications, or disable system functions.

Computer viruses can be spread via email, with some even capable of hijacking email software to spread themselves. Others may attach to legitimate software, within software packs, or infect code, and other viruses can be downloaded from compromised application stores and infected code repositories. A key feature of any computer virus is it requires a victim to execute its code or payload, which means the host application should be running.

Types of Computer Viruses

There are several types of computer viruses that can infect devices. This section will cover computer virus protections and how to get rid of computer viruses.

- **Resident Virus**

Viruses propagate themselves by infecting applications on a host computer. A resident virus achieves this by infecting applications as they are opened by a user. A non-resident virus is capable of infecting executable files when programs are not running.

- **Multipartite Virus**

A multipartite virus uses multiple methods to infect and spread across computers. It will typically remain in the computer's memory to infect the hard disk, then spread through and infect more drives by altering the content of applications. This results in performance lag and application memory running low.

Multipartite viruses can be avoided by not opening attachments from untrusted sources and by installing trusted antivirus software. It can also be prevented by cleaning the boot sector and the computer's entire disk.

- **Direct Action**

A direct action virus accesses a computer's main memory and infects all programs, files, and folders located in the autoexec.bat path, before deleting itself. This virus typically alters the performance of a system but is capable of destroying all data on the computer's hard disk and any USB device attached to it. Direct action viruses can be avoided through the use of antivirus scanners. They are easy to detect, as is restoring infected files.

- **Browser Hijacker**

A browser hijacker manually changes the settings of web browsers, such as replacing the homepage, editing the new tab page, and changing the default search engine. Technically, it is not a virus because it cannot infect files but can be hugely damaging to computer users, who often will not be able to restore their homepage or search engine. It can also contain adware that causes unwanted pop-ups and advertisements.

Browser hijackers typically attach to free software and malicious applications from unverified websites or app stores, so only use trusted software and reliable antivirus software.

- **Overwrite Virus**

Overwrite viruses are extremely dangerous. They can delete data and replace it with their own file content or code. Once files get infected, they cannot be replaced, and the virus can affect Windows, DOS, Linux, and Apple systems. The only way this virus can be removed is by deleting all of the files it has infected, which could be devastating. The best way to protect against the overwrite virus is to use a trusted antivirus solution and keep it updated.

- **Web Scripting Virus**

A web scripting virus attacks web browser security, enabling a hacker to inject web-pages with malicious code, or client-side scripting. This allows cyber criminals to attack major websites, such as social networking sites, email providers, and any site that enables user input or reviews. Attackers can use the virus to send spam, commit fraudulent activity, and damage server files.

Protecting against web scripting is reliant on deploying real-time web browser protection software, using cookie security, disabling scripts, and using malicious software removal tools.

- **File Infector**

A file infector is one of the most common computer viruses. It overwrites files when they are opened and can quickly spread across systems and networks. It largely affects files with .exe or .com extensions. The best way to avoid file infector viruses is to only download official software and deploy an antivirus solution

- **Network Virus**

Network viruses are extremely dangerous because they can completely cripple entire computer networks. They are often difficult to discover, as the virus could be hidden within any computer on an infected network. These viruses can easily replicate and spread by using the internet to transfer to devices connected to the network. Trusted, robust antivirus solutions and advanced firewalls are crucial to protecting against network viruses.

- **Boot Sector Virus**

A boot sector virus targets a computer's master boot record (MBR). The virus injects its code into a hard disk's partition table, then moves into the main memory when a computer restarts. The presence of the virus is signified by boot-up problems, poor system performance, and the hard disk becoming unable to locate. Most modern computers come with boot sector safeguards that restrict the potential of this type of virus.

3. Insider threats

An insider is any person who has or had authorized access to or knowledge of an organization's resources, including personnel, facilities, information, equipment, networks, and systems.

Insider threat is the potential for an insider to use their authorized access or understanding of an organization to harm that organization.

This harm can include malicious, complacent, or unintentional acts that negatively affect the integrity, confidentiality, and availability of the organization, its data, personnel, or facilities. External stakeholders and customers of the Cybersecurity and Infrastructure Security Agency (CISA) may find this generic definition better suited and adaptable for their organization's use.

CISA defines insider threat as the threat that an insider will use their authorized access, wittingly or unwittingly, to do harm to the department's mission, resources, personnel, facilities, information, equipment, networks, or systems. This threat can manifest as damage to the department through the following insider behaviors:

- Espionage
- Terrorism
- Unauthorized disclosure of information
- Corruption, including participation in transnational organized crime
- Sabotage
- Workplace violence
- Intentional or unintentional loss or degradation of departmental resources or capabilities

Types of Insider Threats:

➤ **Unintentional Threat**

Negligence – An insider of this type exposes an organization to a threat through carelessness. Negligent insiders are generally familiar with security and/or IT policies but choose to ignore them, creating risk for the organization. Examples include allowing someone to “piggyback” through a secure entrance point, misplacing or losing a portable storage device containing sensitive information, and ignoring messages to install new updates and security patches.

Accidental – An insider of this type mistakenly causes an unintended risk to an organization. Examples include mistyping an email address and accidentally sending a sensitive business document to a competitor, unknowingly or inadvertently clicking on a hyperlink, opening an attachment in a phishing email that contains a virus, or improperly disposing of sensitive documents.

➤ **Intentional Threats**

The intentional insider is often synonymously referenced as a “malicious insider.” Intentional threats are actions taken to harm an organization for personal benefit or to act on a personal grievance. For example, many insiders are motivated to “get even” due to a

perceived lack of recognition (e.g., promotion, bonuses, desirable travel) or termination. Their actions can include leaking sensitive information, harassing associates, sabotaging equipment, perpetrating violence, or stealing proprietary data or intellectual property in the false hope of advancing their careers.

➤ **Other Threats**

Collusive Threats – A subset of malicious insider threats is referred to as collusive threats, where one or more insiders collaborate with an external threat actor to compromise an organization. These incidents frequently involve cybercriminals recruiting an insider or several insiders to enable fraud, intellectual property theft, espionage, or a combination of the three.

Third-Party Threats – Additionally, third-party threats are typically contractors or vendors who are not formal members of an organization, but who have been granted some level of access to facilities, systems, networks, or people to complete their work. These threats may be direct or indirect threats.

4. Misconfiguration

Cloud misconfiguration refers to any glitches, gaps, or errors that could expose your environment to risk during cloud adoption. These cyber threats come in the form of security breaches, external hackers, ransomware, malware, or insider threats that use vulnerabilities to access your network.

The NSA considers cloud misconfiguration a leading vulnerability in a cloud environment. While these risks are often less sophisticated, the issues' prevalence is generally through the roof.

Misconfiguration is a cloud computing problem because multi-cloud environments can be quite complicated, and it can be tough to detect and manually remediate mistakes. According to a Gartner survey, these issues cause 80% of all data security breaches, and until 2025, up to 99% of cloud environment failures will be attributed to human errors.

Some common Cloud Misconfigurations and solute them

- **Unrestricted Inbound Ports**

All ports open to the internet can be potentially problematic. Cloud services mostly use high-number UDP or TCP ports to prevent exposure risks, but determined hackers can still sniff them out. Obfuscation can be helpful, but it's insufficient by itself.

When migrating to a multi-cloud environment, make sure you know the full range of open ports and then restrict or lock down those that aren't strictly necessary.

- **Unrestricted Outbound Ports**

These ports create opportunities for security events like data exfiltration, lateral movement, and internal network scans once there's a system compromise. Granting outbound access to RDP or SSH is a common cloud misconfiguration. Application servers seldom have to SSH to other network servers, so it's unnecessary to use open outbound ports for SSH.

Make sure you limit the outbound port access and use the least privilege principle to restrict outbound communications.

- **"Secrets" Management**

This configuration issue can be damaging to your organization. Securing secrets like API keys, passwords, encryption keys, and admin credentials is essential. But most companies openly avail these through compromised servers, poorly configured cloud buckets, HTML code, and GitHub repositories. This is as risky as leaving your home's deadbolt key taped to your front door.

You can beat this by maintaining an inventory of all your company secrets in the cloud and regularly evaluating how they're secured. Otherwise, threat actors could easily breach your systems, access your data, and overrun your cloud resources to effect irreversible damage.

You may also use secret management solutions and services like Hashicorp Vault, AWS Secrets Manager, Azure Key Vault, and AWS Parameter Store.

- **Disabled Monitoring and Logging**

Surprisingly, most organizations fail to configure, enable, or review the telemetry data and logs offered by public clouds, which can be sophisticated. It would help to have someone responsible for regular reviews and flagging security-related incidents.

This valuable tip isn't only limited to IaaS public clouds. You'll also get the same information from storage-as-a-service vendors, which you must also review regularly. A maintenance alert or update bulletin could leave your organization with profound security implications, but it won't help if there's no one paying attention.

- **ICMP Left Open**

The ICMP (Internet Control Message Protocol) reports network device errors, but it's a common target for threat actors. This happens because while the protocol can display if your server is responsive and online, cybercriminals can also use it to pinpoint an attack.

Furthermore, it's also an attack vector for denial-of-service (DDoS) and many types of malware. A ping flood or ping sweep can overwhelm your servers with ICMP messages. While it's a dated attack strategy, it's still effective. So make sure your cloud configuration blocks ICMP.

- **Insecure Automated Backups**

Insider threats to your cloud environment are an ever-present cybersecurity risk. According to McAfee, about 92% of business organizations have workers' credentials being sold on the darknet. One section where insider threats can be particularly damaging is when you fail to secure automated cloud data backup properly.

You may have protected your master data, but poorly configured backups will inadvertently remain vulnerable and exposed to insider threats.

When migrating to the cloud, ensure your backups are encrypted whether at rest or in transit. Also, verify the permissions to restrict access to the backups.

- **Storage Access**

Most cloud users believe that "authenticated users" only cover those already authenticated within the relevant apps or organizations regarding storage buckets. Unfortunately, this isn't the case.

"Authenticated users" refers to any person with AWS authentication, essentially any AWS client. Due to this misunderstanding, alongside the resulting control settings misconfiguration, you may have your storage objects wholly exposed to public access. Be especially cautious when setting storage object access to grant it to only the people within your organization.

- **Lack of Validation**

This cloud configuration error is a meta-issue: most organizations don't create and implement systems for identifying misconfigurations whenever they occur. Whether an outside auditor or internal resource, you need someone to verify that permissions and services are correctly configured and deployed.

Create a schedule that ensures validation occurs like clockwork because mistakes are inevitable as the cloud environment evolves. You also need a rigorous process of auditing cloud configurations periodically. Otherwise, you may leave a security loophole that cybercriminals can exploit.

- **Unlimited Access to Non-HTTPS/HTTP Ports**

Web servers are made to host web services and websites to the internet, alongside other services like RDP or SSH for databases or management. However, you must block these from accessing every part of the internet.

Improperly configured ports can open your cloud infrastructure up to malicious actors looking to brute force or exploit the authentication. When opening these ports to the web, ensure you limit them to accept traffic from specific addresses, such as your office.

- **Overly Permissive Access to Virtual Machines, Containers, and Hosts**

Would you connect a virtual or physical server in your data center directly to the internet without protecting it using a firewall or filter? You likely wouldn't, but people do exactly this in their cloud infrastructures all the time.

Some of the most common examples include:

- Enabling legacy protocols and ports like FTP on cloud hosts
- Legacy protocols and ports like rexec, rsh, and telnet in physical servers that have been made virtual and moved to the cloud
- Exposing etcd (port 2379) for Kubernetes clusters to the public internet

You can avoid this cloud configuration mistake by securing important ports and disabling (or at the very least locking down) legacy, insecure protocols in your cloud environment the same way you would treat your on-premise data center.

- **Enabling Too Many Cloud Access Permissions**

A major benefit of cloud computing is its ease of scalability. However, this simplicity of expansion is not without its downsides. As cloud environments grow larger and more complex, administrators rapidly lose oversight of system controls.

Lack of visibility makes it harder for admins to review permissions and restrict access. They may also find it easier to enable default permission settings for all users to avoid dealing with an influx of access requests.

Unnecessary permissions greatly increase the risk of insider threats, which could result in cloud leaks and data breaches.

Organizations should seek to adopt the emerging Secure Access Service Edge (SASE) architecture, which enables more efficient cloud security, including the use of Cloud Access Service Brokers (CASBs) and Cloud Security Posture Management (CSPM) solutions to manage user permissions in multi-cloud environments.

- **Subdomain Hijacking (AKA Dangling DNS)**

A common cause of this type of cyberattack is when an organization deletes a subdomain from its virtual host (e.g. AWS, Azure, Github, etc.) but forgets to delete the its associated records from the Domain Name System (DNS).

Once the attacker discovers the unused subdomain, they can re-register it via the hosting platform and route users to their own malicious web pages.

Such hijacking could result in malware injections or phishing attacks to unsuspecting users and can cause severe reputational damage to the original subdomain owner.

To avoid subdomain hijacking, organizations should always remember to delete DNS records for all domains and subdomains that are no longer in use.

- **Misconfigurations Specific to Your Cloud Provider(s)**

While misconfigurations like open ports and overly permissive access are applicable to all cloud providers, many misconfigurations exist that are more specific to the service(s) you're using. For example, default public access settings for S3 buckets is a well-known AWS flaw.

5. The SQL injection attack

SQL injections target SQL servers in the cloud infrastructure that run vulnerable database applications. Thus, the cyber attacker exploits the vulnerabilities of the web servers, and from there, injects a malicious code in order to circumvent the login credentials and gain unauthorised access to the backend databases.

If this is successful, the cyber attacker can then further manipulate the contents of the SQL server databases; retrieve confidential data; remotely execute system commands; or even take control of the web server for further criminal activities. The SQL injection attacks can also be launched by a botnet.

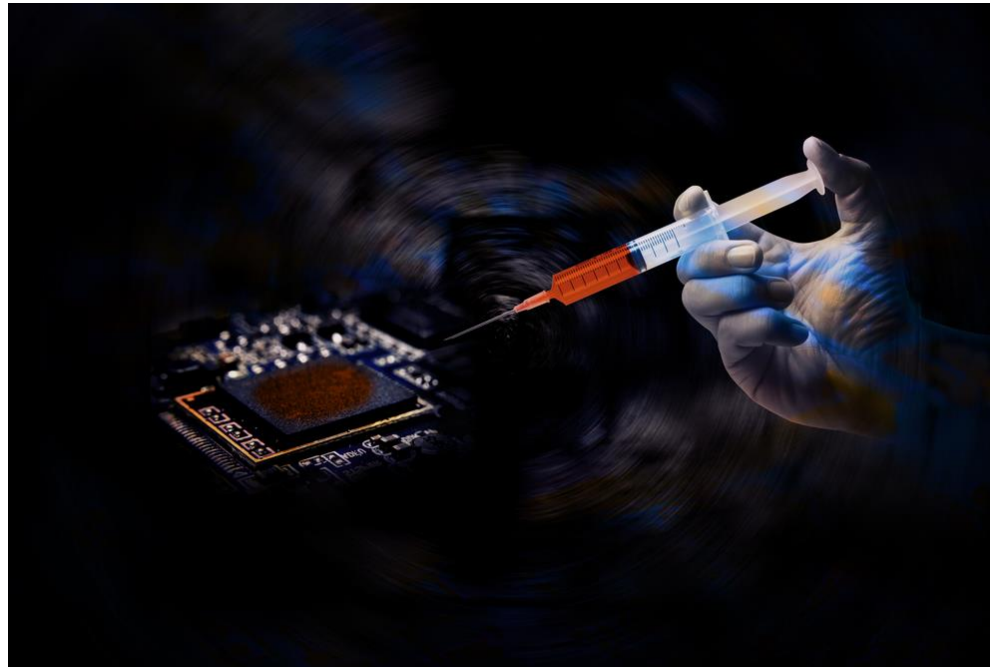


Figure 20: SQL injection attack

For example, the Asprox botnet used a thousand bots that were equipped with an SQL injection kit to fire an SQL injection attack (SOURCE: 1). The bots first sent encoded SQL queries containing the exploit payload to Google for searching web servers that ran the ASP.net framework.

Then, the bots started executed a SQL injection attack against the web sites returned from those queries. In the end, over 6 million URLs belonging to 153,000 different web sites that were hosted on various cloud infrastructures were impacted the Asprox botnet

5.1. Cross Site Scripting (XSS)

With this, the cyber attacker injects malicious scripts, such as JavaScript, VBScript, ActiveX, HTML, and Flash, into a vulnerable dynamic web page in order to execute these various scripts on the victim's web browser. Afterwards, the cyber attacker could then steal the session cookie used for authorisation for the purposes of accessing the victim's account or tricking the victim into clicking a malicious link.

For example, cyber researchers recently in Germany have successfully demonstrated an XSS attack against the Amazon AWS Cloud Computing Platform. The vulnerability in the Amazon store allowed the team to hijack an AWS session and gain successful access to all of the customer data (this included authentication data, tokens, and plain text passwords).

5.2. The wrapping attack

Wrapping attacks make use of the Extensible Markup Language (XML) signature wrapping (or XML rewriting) to exploit a weakness when web servers validate signed requests. This type of cyber attack is accomplished during the translation of Simple Object Access Protocol (SOAP) messages between a legitimate user and the web server.

The cyber attacker embeds a bogus element (the wrapper) into the message structure, moves the original message body under the wrapper, and replaces the content of the message with malicious code. From here, it is then sent to then to the server hosted on the cloud computing infrastructure

By using the XML signature wrapping technique, the cyber researchers also demonstrated an account hijacking attack that exploited a vulnerability in the Amazon AWS (SOURCE: 4). By altering authorised digitally signed SOAP messages, the cyber researchers were then able to obtain unauthorised access to a customer's account. They could also delete and create new images on the customer's EC2 instance, and also perform other administrative tasks.

III. Conclusion

In this assignment 2, I have detailed the specifics as well as presented how to put a website on Heroku and AWS systems, the systems I have set up and instructions on how to do this. to configure. In part II.4 I also demoed the functions and checked for errors and results. With the following sections, I have analyzed and given my personal views on security in cloud computing. In this assignment, I really hope I can get the corresponding score. The entire content in the article is presented by me based on my personal views with the sections.

IV. Reference

<https://www.linkedin.com/pulse/cloud-malware-injection-attacks-christian-otteman?trk=pulse-article>

<https://www.webopedia.com/definitions/misconfiguration/>

<https://www.cisa.gov/defining-insider-threats#:~:text=The%20Cybersecurity%20and%20Infrastructure%20Security,equipment%2C%20networks%2C%20or%20systems.>

<https://www.trellix.com/en-us/security-awareness/ransomware/malware-vs-viruses.html#:~:text=Malware%20is%20a%20catch%2Dall,its%20code%20into%20other%20programs.>

<http://www.laptopusa.net/cach-tang-mo-rong-dung-luong-o-dia-he-thong-tren-windows-10-8-7>

<https://www.techtarget.com/searchsecurity/definition/malware>

<https://www.crowdstrike.com/cybersecurity-101/malware/malware-vs-virus/>

<https://www.trendmicro.com/vinfo/us/security/definition/data-breach>

<https://www.kaspersky.com/resource-center/definitions/what-is-cloud-security>

<https://www.crowdstrike.com/cybersecurity-101/cloud-security/cloud-security-risks-threats-challenges/>

<https://www.geeksforgeeks.org/7-most-common-cloud-computing-challenges/>

<https://www.techtarget.com/searchcloudcomputing/definition/cloud-computing>