

Price Manipulation



TABLE OF CONTENTS

01

Attack overview

Basic overview

02

Intro. to Parameter Tampering

Basic Definition

03

Exploitation

Exploiting our vulnerable WebApp

04

How to prevent this ?

Intro to MAC

05

Recap and Q/A

Fast Recap and Answering Questions

01

Price
Manipulation



What is Price Manipulation Attack ?

- Through a high level definition, price manipulation attack is an attack that is performed against the web applications that offer any paid service, and in this attack, the attacker works on changing the actual price that should be paid, to his desired amount of money.



TABLE OF CONTENTS

01

Attack overview

Basic overview

02

Intro. to Parameter Tampering

Basic Definition

03

Exploitation

Exploiting our vulnerable WebApp

04

How to prevent this ?

Intro to MAC

05

Recap and Q/A

Fast Recap and Answering Questions

02

Intro to Parameter Tampering



What is Parameter Tampering?

- **Parameter Tampering** is based on the manipulation of parameters exchanged between client and server in order to modify the application data, such as user credentials, permissions, price and quantity of products, etc....



TABLE OF CONTENTS

01

Attack overview

Basic overview

02

Intro. to Parameter Tampering

Basic Definition

03

Exploitation

Exploiting our vulnerable WebApp

04

How to prevent this ?

Intro to MAC

05

Recap and Q/A

Fast Recap and Answering Questions

03

Exploitation



Let's Hack our vulnerable website :

- First we need to know the behavior of the application when we legitimately try to buy an item.
- We will notice that the developer tries to send the item's price data with the request performed when we attempt to buy the item.
- Now lets try to buy another one and modify the price parameter to make the item very cheap.
- Now lets see the response for our purchase.
- And **CONGRATS!!** We have bought the item with a very cheap price !

TABLE OF CONTENTS

01

Attack overview

Basic overview

02

Intro. to Parameter Tampering

Basic Definition

03

Exploitation

Exploiting our vulnerable WebApp

04

Prevention

Intro to MAC

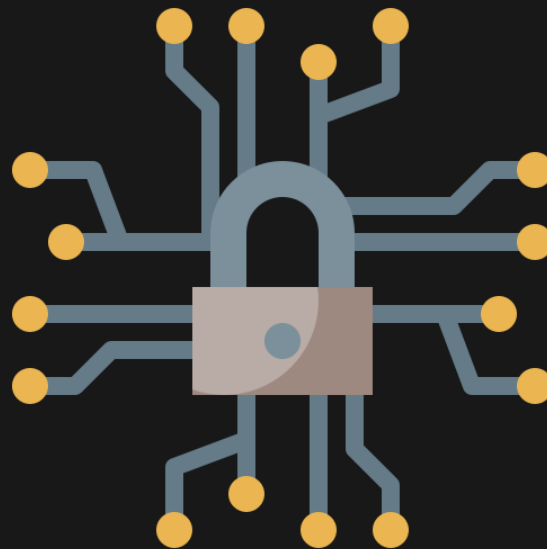
05

Recap and Q/A

Fast Recap and Answering Questions

04

Prevention



Message Authentication Code MAC

Message Authentication Code (MAC):

- In cryptography, a message authentication code is a short piece of information used for authenticating a message, In other words, To confirm that the message come from the stated sender and has not been changed.
- The MAC value protects a message's data integrity, as well as the authenticity, by allowing verifiers to detect any modification in message content.

Message Authentication Code MAC


How does MAC work?

- When sending parameters :

ID	Title	Price	Quantity
3	iphone	\$1099	1

Secret_Password

a7822!*afSb4



Shared with the
website and the
payment
gateway

MAC = Hash(3iphone\$10991a7822!*afSb4) = f5s4afaf4hj6fbsda7f9sh7asf461aa

Message Authentication Code MAC

- Parameters that the user will be redirected to the payment gateway with :

ID = 3

Title = iphone

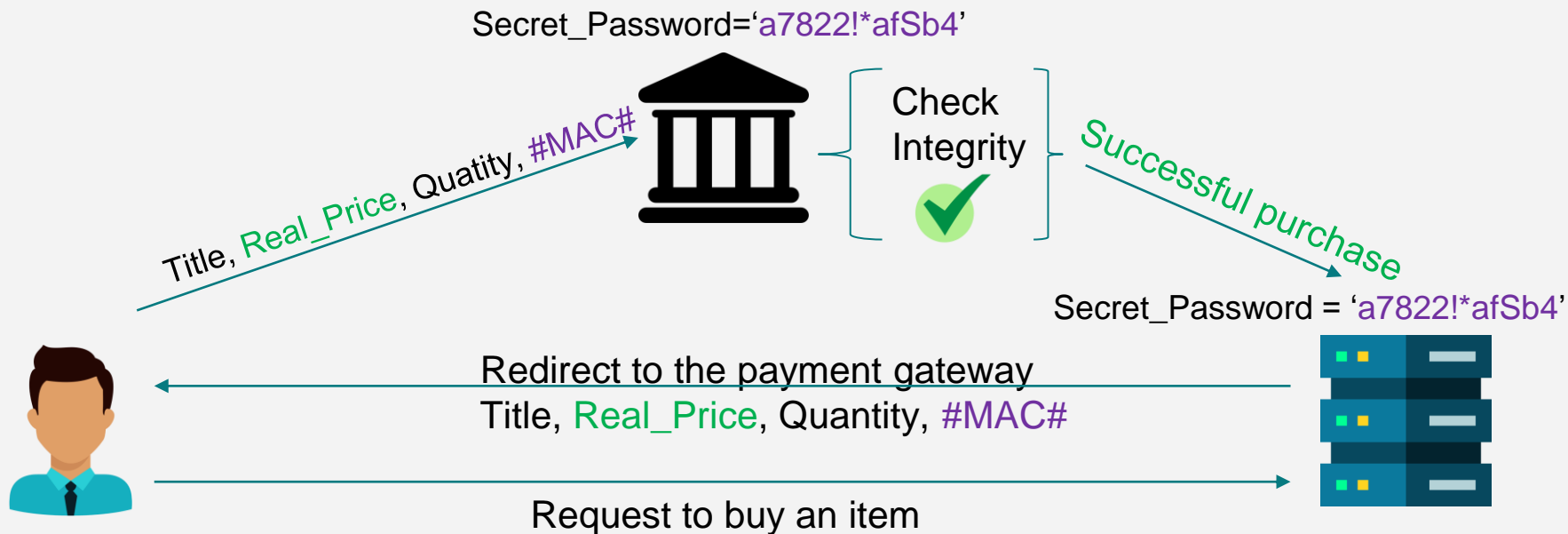
Price = \$1099

Quantity = 1

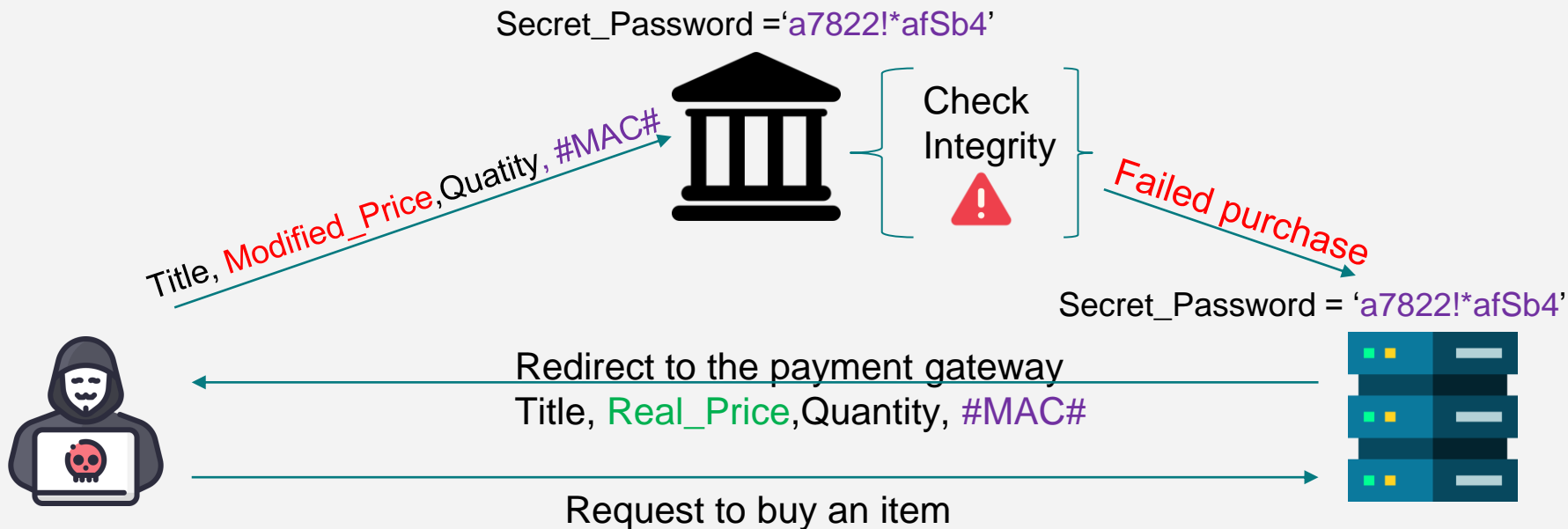
MAC = f5s4afaf4hj6fbsda7f9sh7asf461aa

- Now if any manipulation was applied on the parameters,
The generated MAC by the payment gateway will be totally different from this one,
So the transaction will be **rejected !**

How MAC works?



How MAC works?





Thank You

Presented by Saleh Adel

RESOURCES

https://owasp.org/www-community/attacks/Web_Parameter_Tampering

https://en.wikipedia.org/wiki/Message_authentication_code

