INCIDENT REPORT: MP-9032-Offensive: Access Secured Documents

Date:12-02-2022

Executive summary:

Using my OWASP Juice Shop application to find a text document that has acquisition information in it.

Results

Application details:

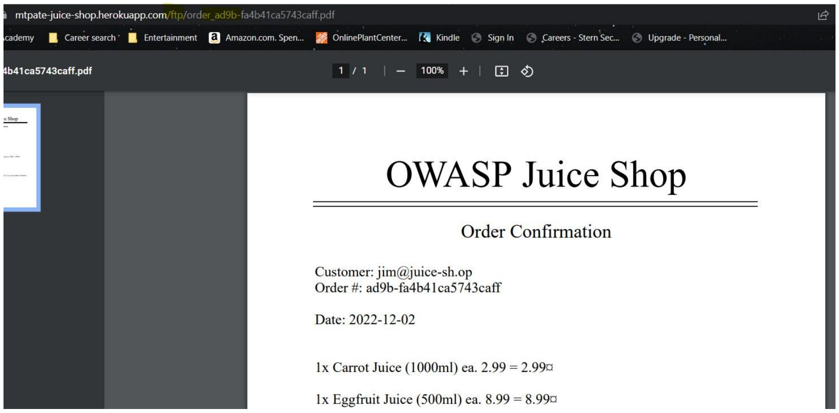
- Application URL: https://mtpate-juice-shop.herokuapp.com/#/

Attack Narrative:

The challenge involves exposing sensitive data by accessing a confidential document. Having done a thorough walkthrough of the application as two different credentialed users (Bender and Jim) and an admin user, I noticed a 'FTP' directory listing while printing an order confirmation. (mtpate-juice-shop.herokuapp.com/ftp/order_ad9b-fa4b41ca5743caff.pdf). I navigated to the /ftp/ directory and found a listing of documents. Along with our order confirmation, there was a document labeled 'acquisitions.md'.

Conclusion:

If you must have an FTP folder, be very, very careful about what you put there. Access controls are important.



OWASP Juice Shop

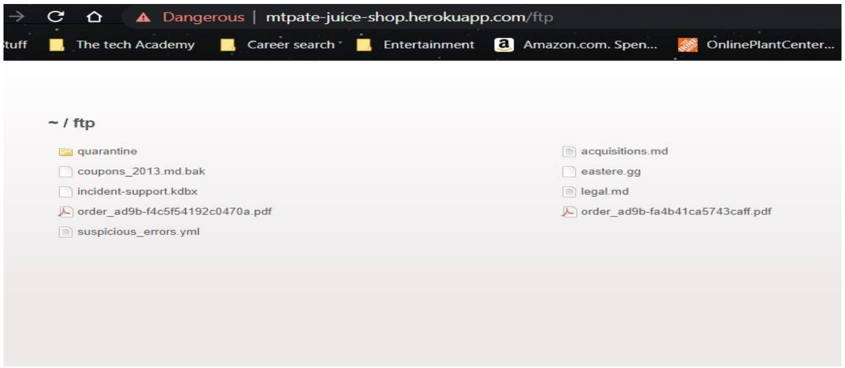
Order Confirmation

Customer: jim@juice-sh.op
Order #: ad9b-fa4b41ca5743caff

Date: 2022-12-02

1x Carrot Juice (1000ml) ea. 2.99 = 2.99¤

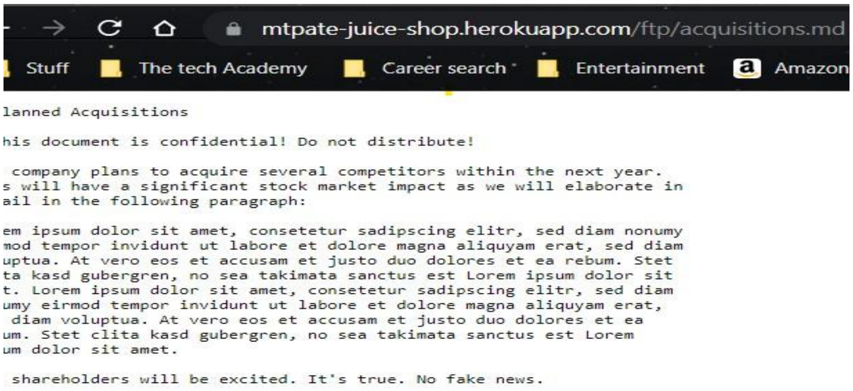
1x Eggfruit Juice (500ml) ea. 8.99 = 8.99¤



~ / ftp

quarantine
coupons_2013.md.bak
incident-support.kdbx
order_ad9b-f4c5f54192c0470a.pdf
suspicious_errors.yml

acquisitions.md
eastere.gg
legal.md
order_ad9b-fa4b41ca5743caff.pdf



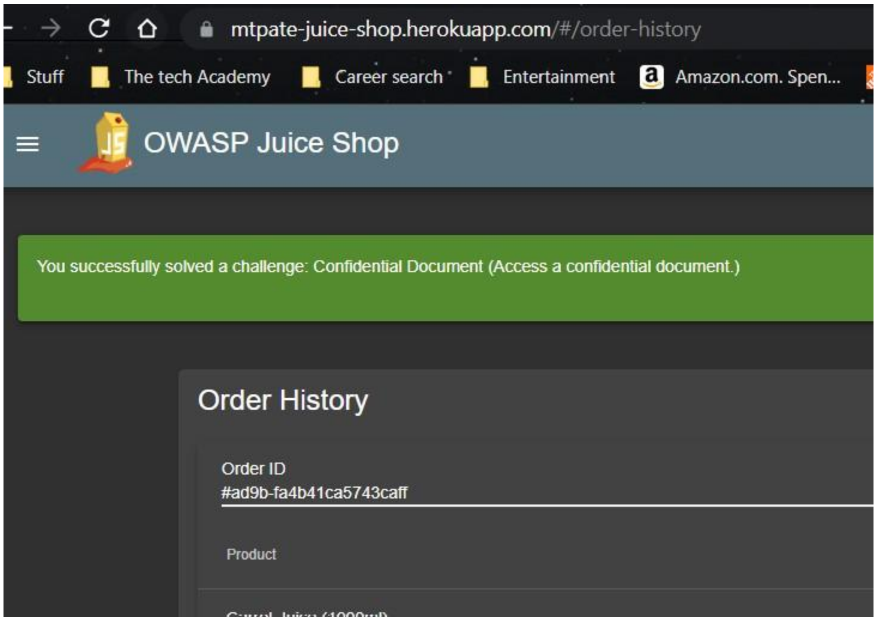
```
lanned Acquisitions

his document is confidential! Do not distribute!

 company plans to acquire several competitors within the next year.
s will have a significant stock market impact as we will elaborate in
ail in the following paragraph:

em ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy
mod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam
uptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet
ta kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit
t. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam
umy eirmod tempor invidunt ut labore et dolore magna aliquyam erat,
 diam voluptua. At vero eos et accusam et justo duo dolores et ea
um. Stet clita kasd gubergren, no sea takimata sanctus est Lorem
um dolor sit amet.

 shareholders will be excited. It's true. No fake news.
```



You successfully solved a challenge: Confidential Document (Access a confidential document.)

Order History

Order ID
#ad9b-fa4b41ca5743caff

Product