TuneStore 2

By: Mikiyas Solomon
Class: ITIS 4221
Date: October 8, 2022

VULNERABILITY ASSESSMENT AND SYSTEMS ASSURANCE REPORT

TABLE OF CONTENTS

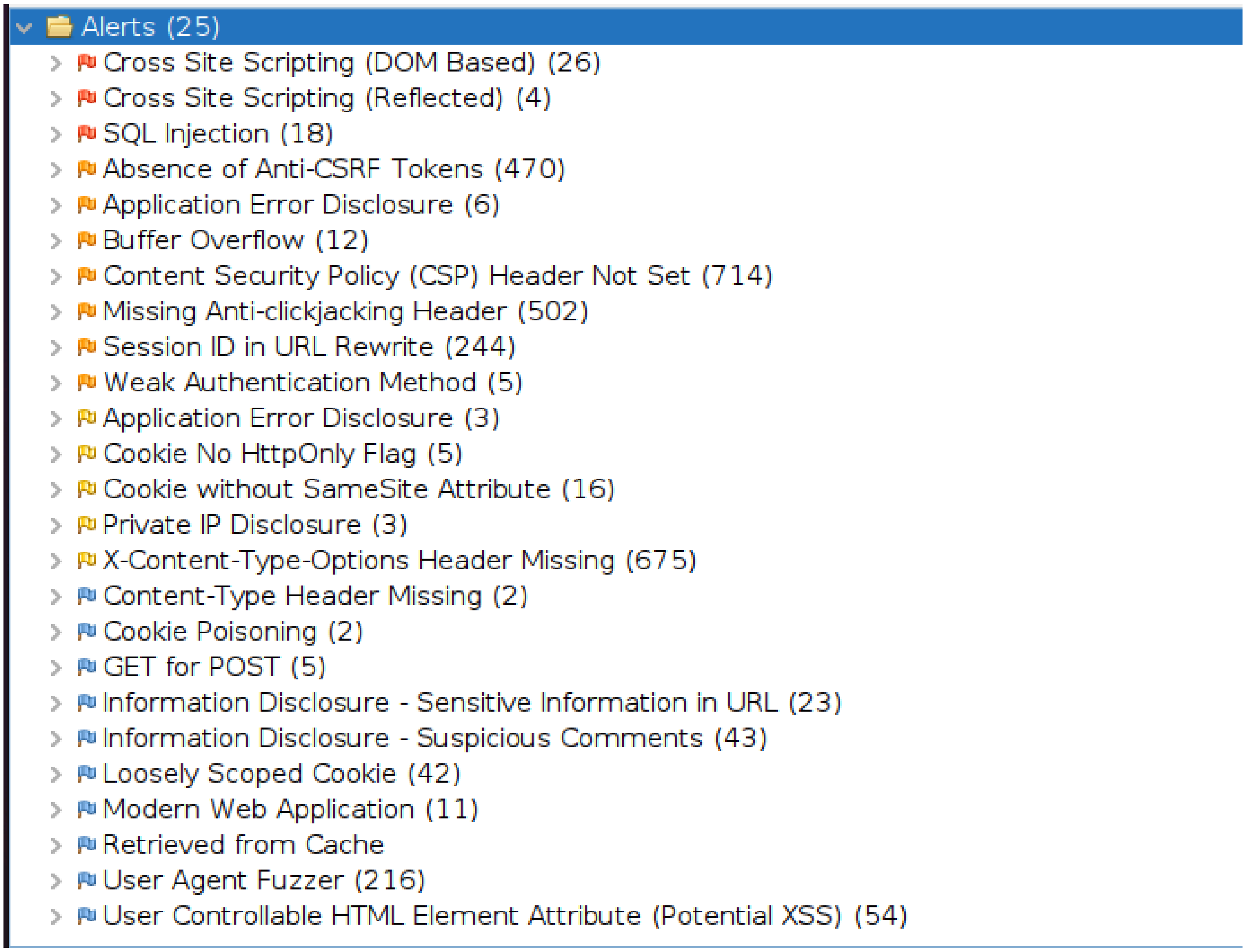
<u>Section</u>

1.0 Purpose

The purpose of this security assessment is to identify Vulnerabilities that ZAP found and determine whether they are false positive or true positive and to identify any vulnerabilities ZAP might have missed.

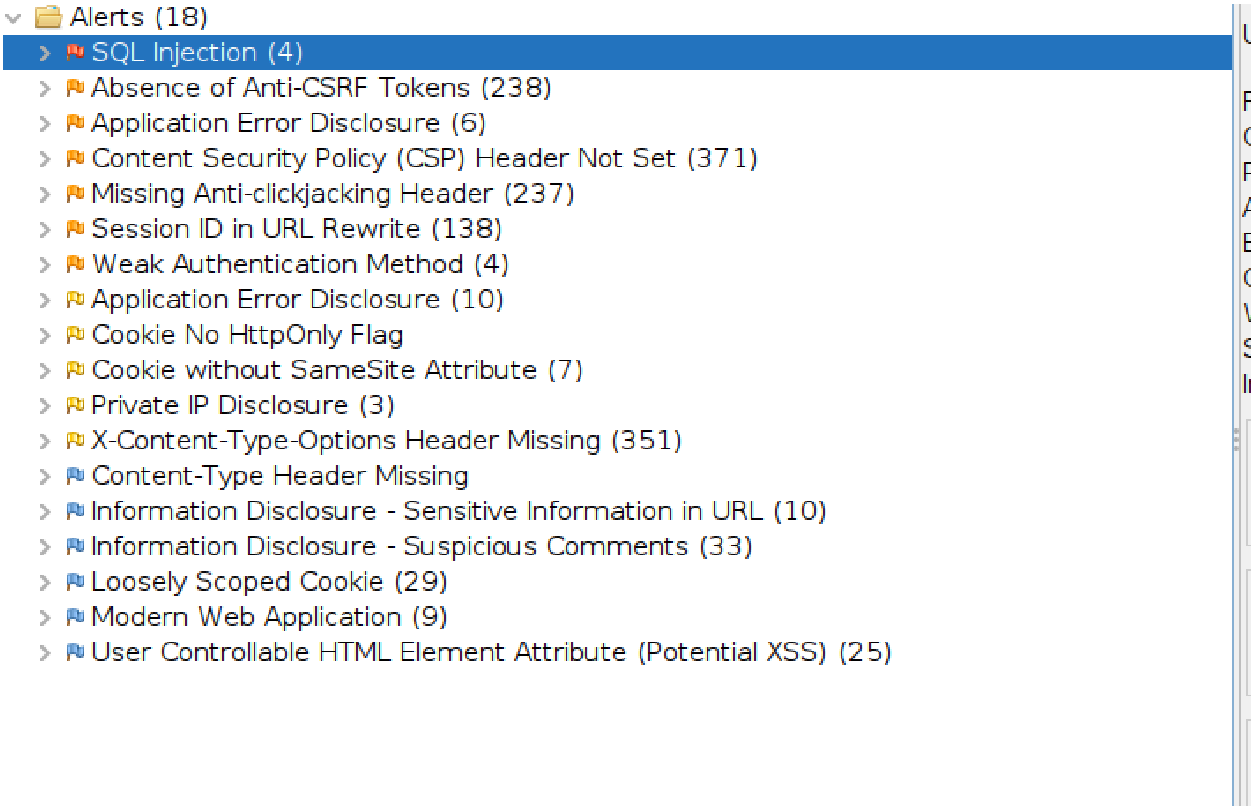
2.0 Zap Analysis

Zed Attack Proxy, short for ZAP is a scanner that is used to scan for vulnerabilities in web applications and by inserting Tunestore's web address I was able to get these results without being logged in:



Alerts (25)
Cross Site Scripting (DOM Based) (26)
Cross Site Scripting (Reflected) (4)
SQL Injection (18)
Absence of Anti-CSRF Tokens (470)
Application Error Disclosure (6)
Buffer Overflow (12)
Content Security Policy (CSP) Header Not Set (714)
Missing Anti-clickjacking Header (502)
Session ID in URL Rewrite (244)
Weak Authentication Method (5)
Application Error Disclosure (3)
Cookie No HttpOnly Flag (5)
Cookie without SameSite Attribute (16)
Private IP Disclosure (3)
X-Content-Type-Options Header Missing (675)
Content-Type Header Missing (2)
Cookie Poisoning (2)
GET for POST (5)
Information Disclosure - Sensitive Information in URL (23)
Information Disclosure - Suspicious Comments (43)
Loosely Scoped Cookie (42)
Modern Web Application (11)
Retrieved from Cache
User Agent Fuzzer (216)
User Controllable HTML Element Attribute (Potential XSS) (54)

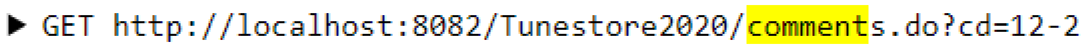
And these results being logged in:



```
Alerts (18)
  SQL Injection (4)
  Absence of Anti-CSRF Tokens (238)
  Application Error Disclosure (6)
  Content Security Policy (CSP) Header Not Set (371)
  Missing Anti-clickjacking Header (237)
  Session ID in URL Rewrite (138)
  Weak Authentication Method (4)
  Application Error Disclosure (10)
  Cookie No HttpOnly Flag
  Cookie without SameSite Attribute (7)
  Private IP Disclosure (3)
  X-Content-Type-Options Header Missing (351)
  Content-Type Header Missing
  Information Disclosure - Sensitive Information in URL (10)
  Information Disclosure - Suspicious Comments (33)
  Loosely Scoped Cookie (29)
  Modern Web Application (9)
  User Controllable HTML Element Attribute (Potential XSS) (25)
```

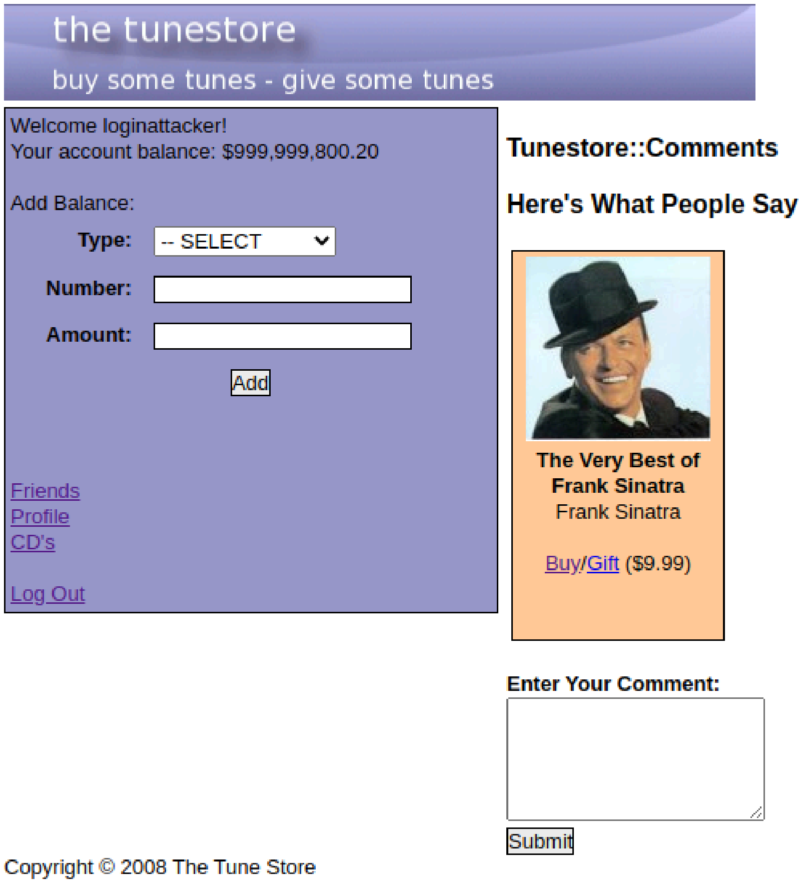
2.1 SQL Injection for comments

A false positive that I noticed was a comment for cd 12-2:



```
▶ GET http://localhost:8082/Tunestore2020/comments.do?cd=12-2
```

Zap used this vulnerability to attempt to allow a user that isn't logged in to comment on a cd but when I logged in as an actual user there was no comment



Welcome loginattacker!
Your account balance: $999,999,800.20

Add Balance:

Type: -- SELECT

Number:

Amount:

Tunestore::Comments

Here's What People Say

The Very Best of Frank Sinatra
Frank Sinatra

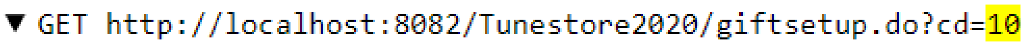
Buy/Gift ($9.99)

Enter Your Comment:

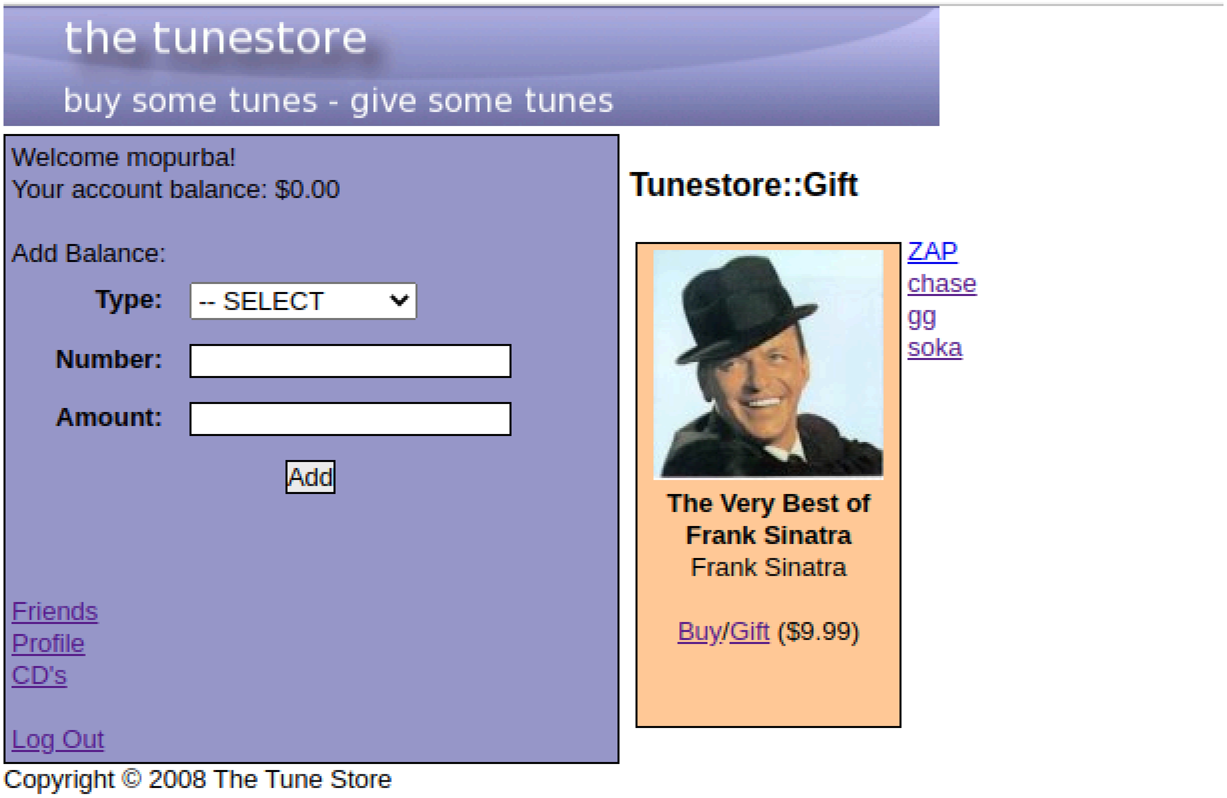
Copyright © 2008 The Tune Store

2.2 SQL Injection for CD gifting

Another false positive was found. A get method was used to attempt to allow someone to gift a cd to any user, however, when I used the attack link it just took me to the cd with no change whatsoever. When choosing a friend to gift it sends them a cd like normal



```
▼ GET http://localhost:8082/Tunestore2020/giftsetup.do?cd=10
```



the tunestore

buy some tunes - give some tunes

Welcome mopurba!
Your account balance: $0.00

Add Balance:

Type: -- SELECT

Number:

Amount:

Tunestore::Gift

The Very Best of Frank Sinatra
Frank Sinatra

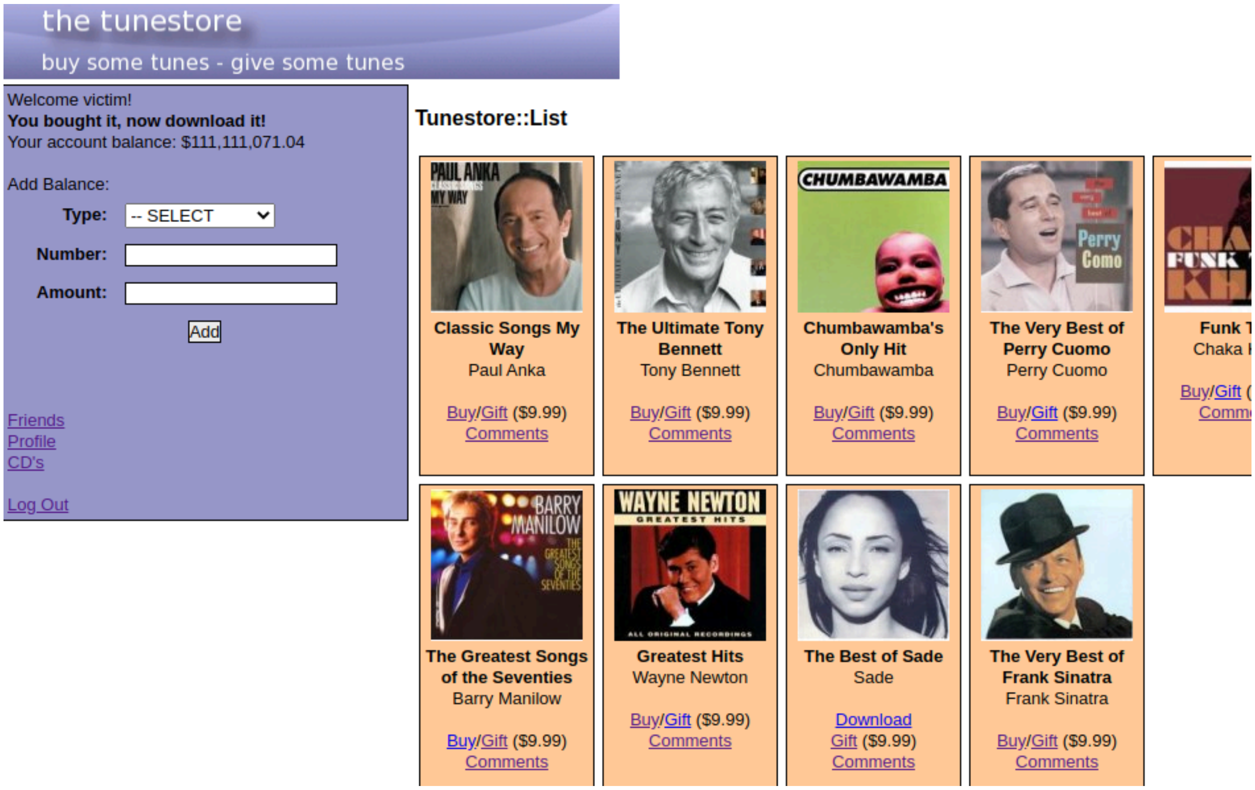
Buy/Gift ($9.99)

Copyright © 2008 The Tune Store

2.3 SQL Injection for CD buying

A true positive was found. A get method was used to attempt to buy a logged-in user a cd. With this attack as long as the victim has money a cd can be purchased.

```
▶ GET http://localhost:8082/Tunestore2020/buy.do?cd=9
```



the tunestore

buy some tunes - give some tunes

Welcome victim!
You bought it, now download it!
Your account balance: $111,111,071.04

Add Balance:

Type:	-- SELECT
Number:	
Amount:	

Add

Friends
Profile
CD's

Log Out

Tunestore::List

Classic Songs My Way
Paul Anka
Buy/Gift ($9.99)
Comments

The Ultimate Tony Bennett
Tony Bennett
Buy/Gift ($9.99)
Comments

Chumbawamba's Only Hit
Chumbawamba
Buy/Gift ($9.99)
Comments

The Very Best of Perry Cuomo
Perry Cuomo
Buy/Gift ($9.99)
Comments

Funk T
Chaka K
Buy/Gift (
Comm

The Greatest Songs of the Seventies
Barry Manilow
Buy/Gift ($9.99)
Comments

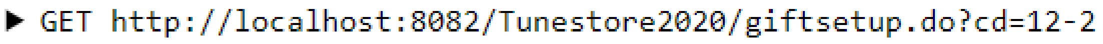
Greatest Hits
Wayne Newton
Buy/Gift ($9.99)
Comments

The Best of Sade
Sade
Download
Gift ($9.99)
Comments

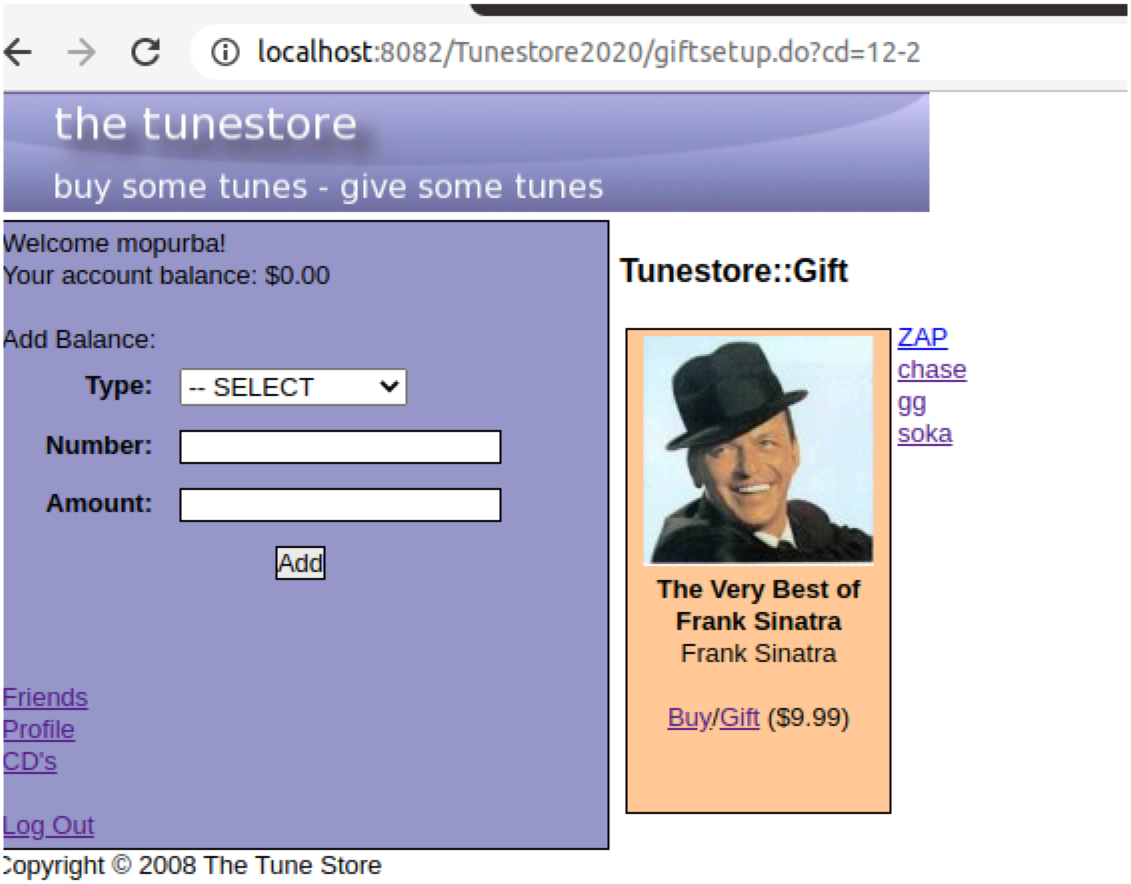
The Very Best of Frank Sinatra
Frank Sinatra
Buy/Gift ($9.99)
Comments

2.4 SQL Injection for CDs

Another false positive that was found was the URL for cd, it was 12-2 but there is no cd that exists so it defaults back to 10



```
▶ GET http://localhost:8082/Tunestore2020/giftsetup.do?cd=12-2
```



localhost:8082/Tunestore2020/giftsetup.do?cd=12-2

the tunestore

buy some tunes - give some tunes

Welcome mopurba!
Your account balance: $0.00

Add Balance:

Type:	-- SELECT
Number:	
Amount:	

Add

Friends
Profile
CD's

Log Out

Copyright © 2008 The Tune Store

Tunestore::Gift

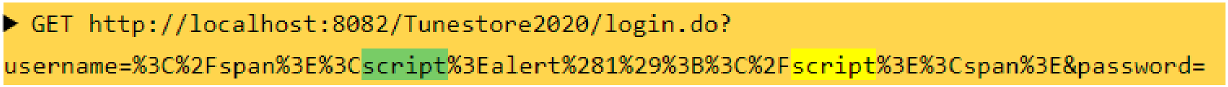
The Very Best of Frank Sinatra
Frank Sinatra

Buy/Gift ($9.99)

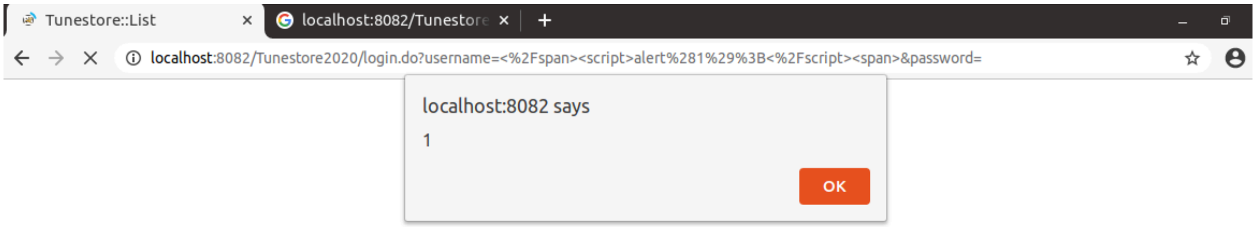
ZAP
chase
gg
soka

2.5 Reflected Alert

A true positive that was found was when zap injected a script into the login of Tunestore and an alert popped up.



```
▶ GET http://localhost:8082/Tunestore2020/login.do?
username=%3C%2Fspan%3E%3Cscript%3Ealert%281%29%3B%3C%2Fscript%3E%3Cspan%3E&password=
```



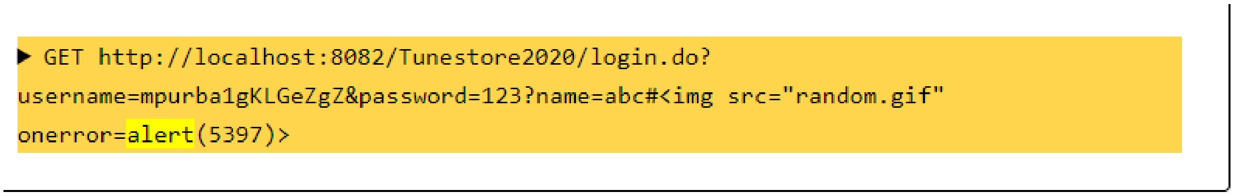
localhost:8082/Tunestore2020/login.do?username=<%2Fspan><script>alert%281%29%3B<%2Fscript><span>&password=

localhost:8082 says

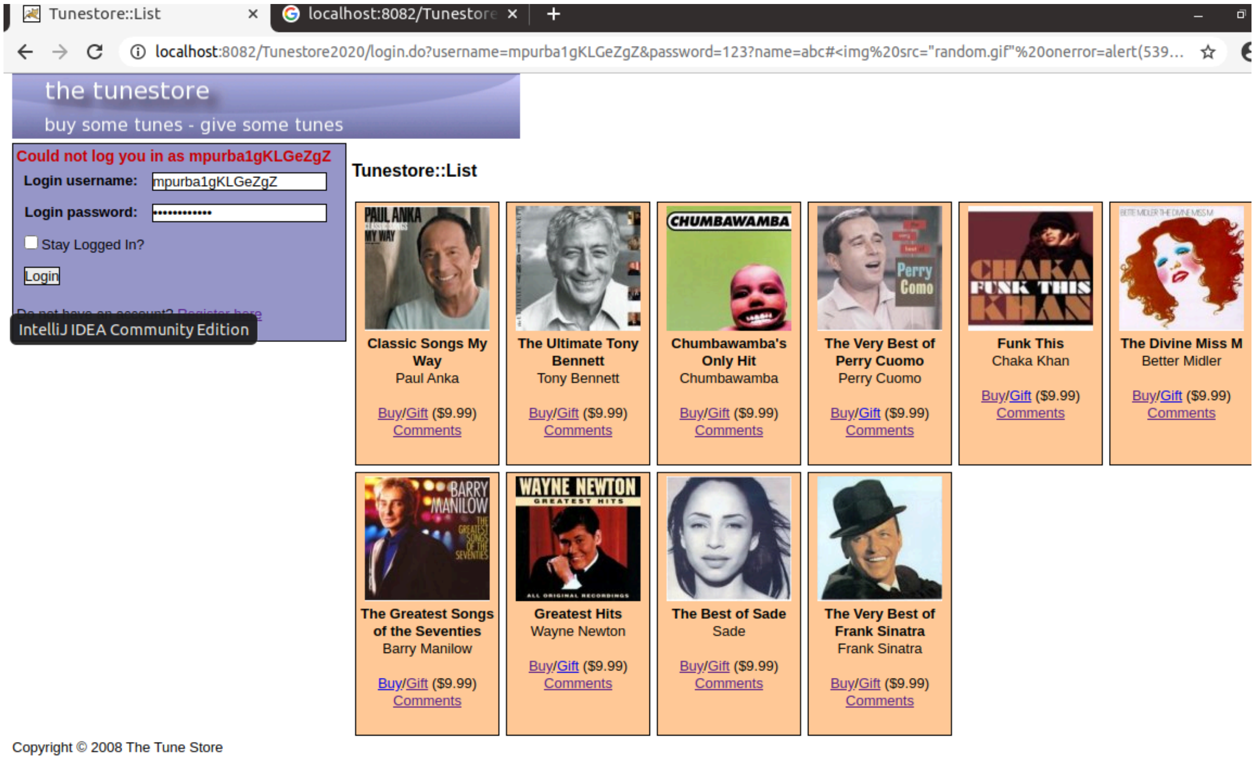
1

2.6 CSS

A False positive was found. ZAP attempted to log in as a user and inject a gif file and an error and alert would pop but the attack failed and nothing happened



```
▶ GET http://localhost:8082/Tunestore2020/login.do?
username=mpurba1gKLGeZgZ&password=123?name=abc#<img src="random.gif"
onerror=alert(5397)>
```


Tunestore::List
localhost:8082/Tunestore
localhost:8082/Tunestore2020/login.do?username=mpurba1gKLGeZgZ&password=123?name=abc#<img%20src="random.gif"%20onerror=alert(539...
the tunestore
buy some tunes - give some tunes
IntelliJ IDEA Community Edition

Could not log you in as mpurba1gKLGeZgZ

Login username: mpurba1gKLGeZgZ

Login password: ••••••••••••

□ Stay Logged In?

Login

Do not have an account? Register here

Tunestore::List

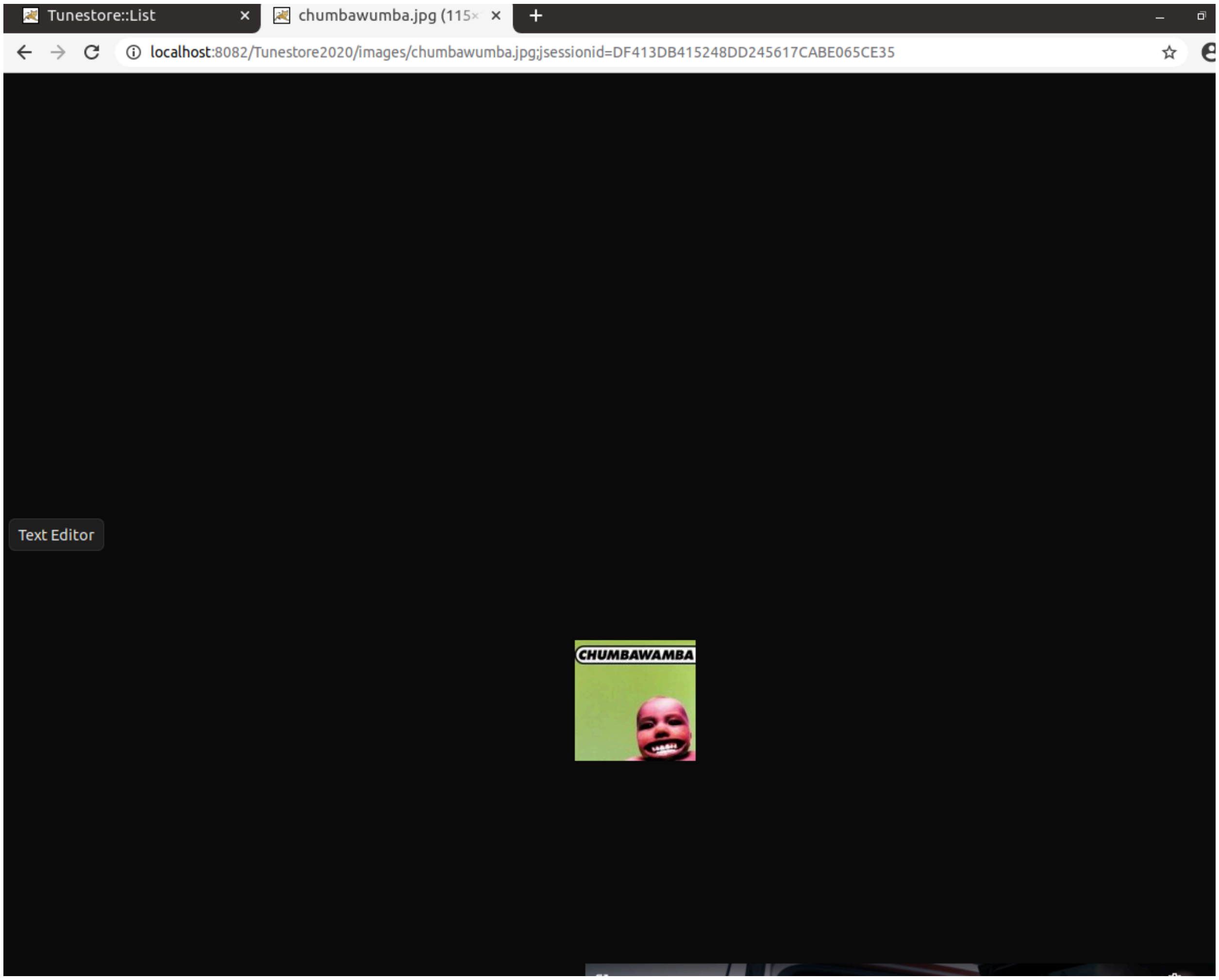
Classic Songs My Way Paul Anka Buy/Gift ($9.99) Comments	**The Ultimate Tony Bennett** Tony Bennett Buy/Gift ($9.99) Comments	**Chumbawamba's Only Hit** Chumbawamba Buy/Gift ($9.99) Comments	**The Very Best of Perry Cuomo** Perry Cuomo Buy/Gift ($9.99) Comments	**Funk This** Chaka Khan Buy/Gift ($9.99) Comments	**The Divine Miss M** Better Midler Buy/Gift ($9.99) Comments
The Greatest Songs of the Seventies Barry Manilow Buy/Gift ($9.99) Comments	**Greatest Hits** Wayne Newton Buy/Gift ($9.99) Comments	**The Best of Sade** Sade Buy/Gift ($9.99) Comments	**The Very Best of Frank Sinatra** Frank Sinatra Buy/Gift ($9.99) Comments		

Copyright © 2008 The Tune Store

2.7 Image

A false positive was found. ZAP copied the image URL of the CD covers and attempted to do an attack but the result was just an image of a CD cover

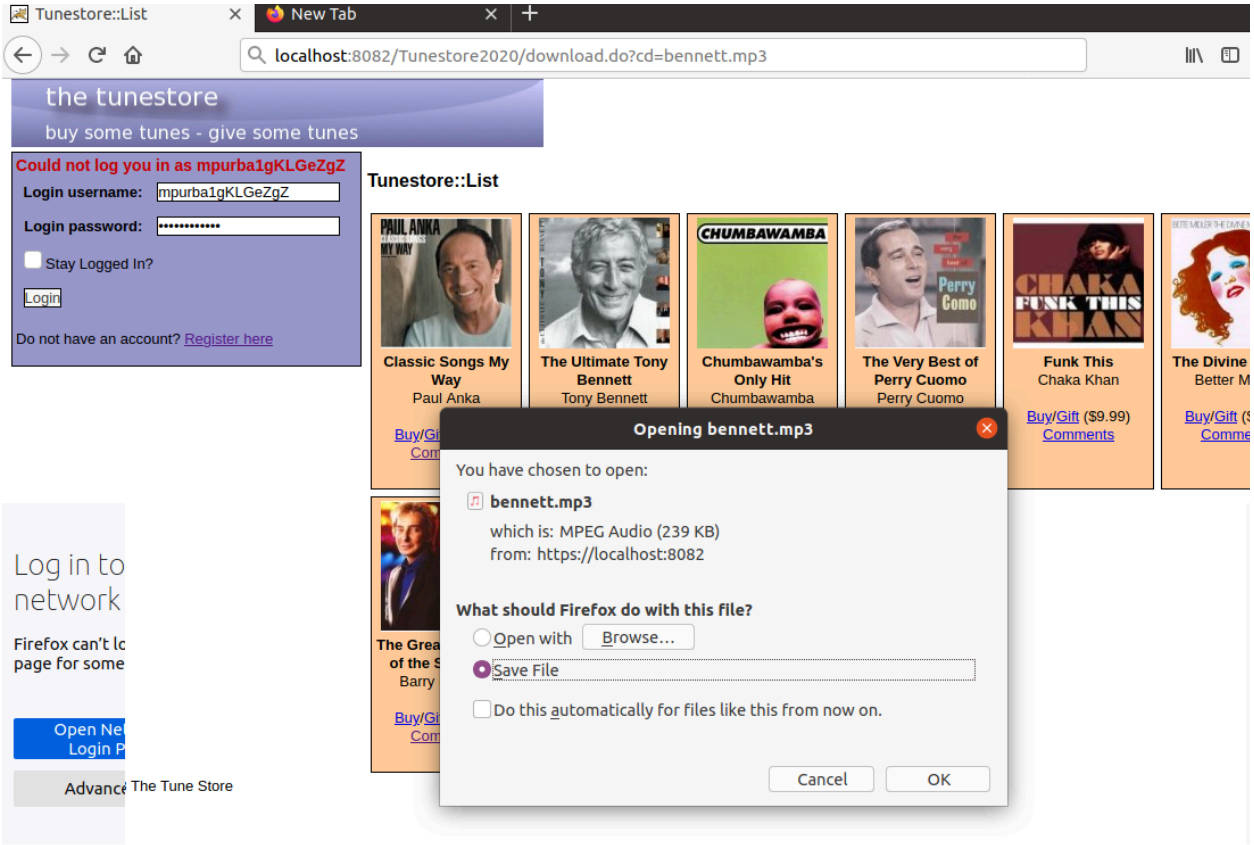
```
▼ GET
http://localhost:8082/Tunestore2020/images/chumbawumba.jpg;jsessionid=DF413DB415248DD
245617CABE065CE35
```



Tunestore::List
chumbawumba.jpg (115×
localhost:8082/Tunestore2020/images/chumbawumba.jpg;jsessionid=DF413DB415248DD245617CABE065CE35
Text Editor
CHUMBAWAMBA

3.0 False negative

A false negative was found. ZAP was not able to find a vulnerability found in URL manipulation. When someone downloads a CD it takes you to a separate link and by manipulating the URL you are able to download any song you want.


Tunestore::List
New Tab
localhost:8082/Tunestore2020/download.do?cd=bennett.mp3
the tunestore
buy some tunes - give some tunes

Could not log you in as mpurba1gKLGeZgZ

Login username: mpurba1gKLGeZgZ

Login password: ••••••••••••

□ Stay Logged In?

Login

Do not have an account? Register here

Tunestore::List

Opening bennett.mp3

You have chosen to open:

bennett.mp3

which is: MPEG Audio (239 KB)
from: https://localhost:8082

What should Firefox do with this file?

○ Open with Browse…

● Save File

□ Do this automatically for files like this from now on.

Cancel OK