Sahil Bhirud

ITIS 5221

Dynamic Analysis for Tunestore

Summary of Alerts

Risk Level	Number of Alerts
High	3
Medium	4
Low	21
Informational	12

1. **True Positives - Vulnerabilities that were both detected by ZAP and found in class**

1.1 Cross Site Scripting (Reflected):

Detected by ZAP:

ZAP tool has detected this XSS vulnerability at login page in which the attacking parameter is username and by inserting the malicious script of *<script>alert(1)</script>* attacker could get logged in as admin.

URL	http://localhost:8082/Tunestore2020/login.do?username=%3C%2Fspan%3E%3Cscript%3Ealert%281%29%3B%3C%2Fscript%3E%3Cspan%3E&password=
Method	GET
Parameter	username
Attack	<script>alert(1);</script>
Evidence	<script>alert(1);</script>
Instances	2

Found in Class:

This attack was found and explained in Tunestore phase 1. The injected attack is not stored within the application itself; it is non persistent and only impacts users who open a maliciously crafted link. Thus, it is a **true positive**.

1.2 SQL Injection Attack:

Detected by ZAP:

ZAP tool has detected this SQL Injection vulnerability on numerous pages of Tunestore. The SQL vulnerability is found in the login page where the attacking parameter is password and by inserting the SQL query *ZAP' AND '1'='1* the attacker could login as a specific user.

URL	http://localhost:8082/Tunestore2020/login.do?password=ZAP%27+AND+%271%27%3D%271&stayLogged=true&username=ZAP
Method	GET
Parameter	password
Attack	ZAP' AND '1'='1

It also detects the attack with username as the parameter, logging in as a random user.

URL	http://localhost:8082/Tunestore2020/login.do;jsessionid=9E892CBD25F7ED02547154F6EAF5D156?password=ZAP&stayLogged=true&username=ZAP%27+AND+%271%27%3D%271%27+--+
Method	GET
Parameter	username
Attack	ZAP' AND '1'='1' --

Found in Class:

This attack was found and explained in Tunestore phase 1. When a user enters a username and password a SQL query is created and executed to search on the database to verify them. If matching entries are found, the user is authenticated. In order to bypass this security mechanism, SQL code has to be injected onto the input fields.

If the username is already known, the only thing to be bypassed is the password verification. Payload similar to the above mentioned payload was used to exploit this vulnerability in class. Thus, it is a **true positive**.

1.3 Clickjacking:

Detected by ZAP:

Clickjacking vulnerability is present when X-Frame header option is not included in the HTTP response. ZAP tool has detected several header options vulnerabilities in Tunestore, clickjacking attack is one of them as X-Frame-Options header is not included in the HTTP response to protect against these kinds of attacks.

URL	http://localhost:8082/Tunestore2020/friends.do;jsessionid=D470A86630C9252D79FCC70D5B4FCFC1
Method	GET
Parameter	X-Frame-Options

Found in Class:

This attack was found and explained in Tunestore phase 2. A webpage that performs a clickjacking attack against the "addFriend()" function. This attack was performed by creating an iframe within a malicious web page.

1.4 Cross Site Scripting (Persistent):

Detected by ZAP:

ZAP has detected this vulnerability in the comments page of Tunestore using the payload *<script>alert(1)</script>*. This is Stored XSS Attack wherein every time a user loads this page, the attack will be executed.

URL	http://localhost:8082/Tunestore2020/leaveComment.do
Method	POST
Parameter	comment
Attack	</blockquote><script>alert(1);</script><blockquote>
Instances	1

Found in Class:

This attack was found and explained in Tunestore phase 1. Thus, it is a **true positive**.

2. **False Negative – Vulnerabilities that were found in class but not through ZAP**

2.1 CSRF:

CSRF is a type of attack that occurs when a malicious web site, email, blog or a program causes a user's web browser to perform an unwanted action on a trusted site for which the user is currently authenticated.

Found in Class:

CSRF attacks for the following actions were found in Tunestore Phase 2:

1. Add a friend
2. Give a gift
3. Change Password

Not detected by ZAP:

As CSRF is state based attack and does not depend only on the misconfiguration of the application, it needs user interaction via social engineering thus it is hard to get detected through a toll based scan.

2.2 Broken Access Control Vulnerabilities:

Broken Access Control is a threat that is easily exploitable and widespread, as many websites allow unauthorized users to access areas of the site with a simple cut and paste into the browser.

Found in Class:

This attack was found and explained in Tunestore phase 2. By editing the information in the address bar, the attacker was able to log into the account of the victim, bypassing the authentication mechanism.

Not detected by ZAP:

As Broken Access Control does not depend only on the application misconfiguration, it needs user interaction thus it is hard to get detected through the tool based scan.

2.3 SQL Injection:

A SQL injection attack consists of insertion of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify the database data and in some cases issue commands to the operating system.

Found in Class:

The SQL vulnerability found in class allowed the attacker to register a user with lots of money without actually paying for it. This helped the attacker to con the company.

Not detected by ZAP:

ZAP does not know the database structure for Tunestore hence, it could not detect this vulnerability.

2.4 Cross Site Scripting:

The Tunestore application is also vulnerable to phishing attacks by changing the location of the form submission to another phishing website.

Found in Class:

This vulnerability was found and explained in Tunestore Phase 2. The vulnerability was exploited by inserting a malicious JavaScript into the username field which changed the form submission location.

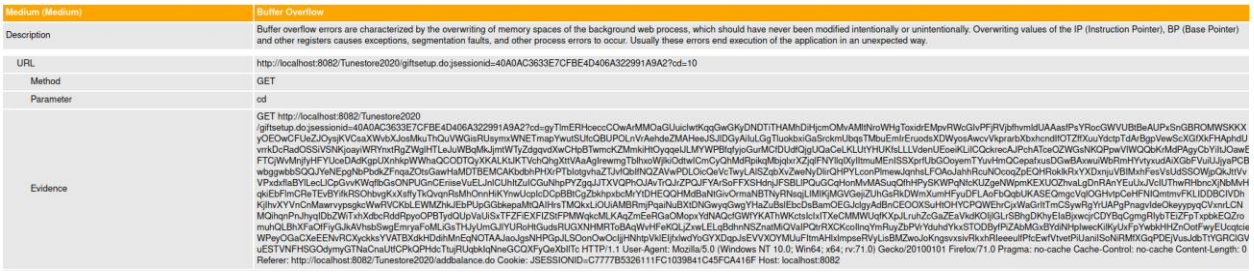
Not detected by ZAP:

Since it requires a custom malicious script, this attack was not detected by the generalized scripts used by ZAP. Hence, it is a **false negative**.

3. False Positives

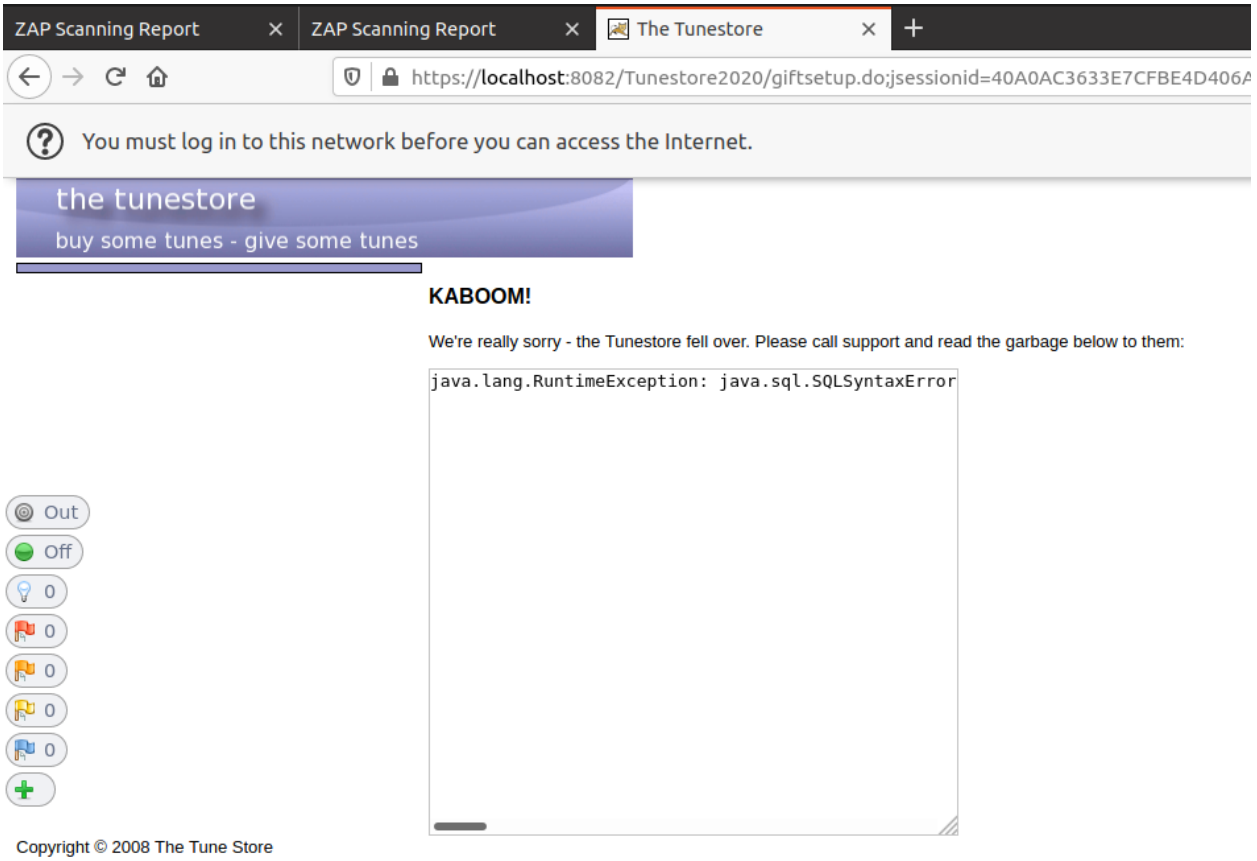
3.1 Buffer Overflow:

ZAP tool has detected Buffer Overflow vulnerability. It shows that the page shown below contains a buffer overflow vulnerability which are characterized by the overwriting of memory spaces of the background web process, which should have never been modified intentionally or unintentionally. Overwriting values of the Instruction Pointer (IP), Base Pointer (BP) and other registers causes exceptions, segmentation faults and other errors to occur. Usually these errors end execution of the application in an unexpected way.



Medium (Medium)	Buffer Overflow
Description	Buffer overflow errors are characterized by the overwriting of memory spaces of the background web process, which should have never been modified intentionally or unintentionally. Overwriting values of the IP (Instruction Pointer), BP (Base Pointer) and other registers causes exceptions, segmentation faults, and other process errors to occur. Usually these errors end execution of the application in an unexpected way.
URL	http://localhost:8082/Tunestore2020/giftsetup.do;jsessionid=40A0AC3633E7CFBE4D406A322991A9A2?cd=10
Method	GET
Parameter	cd
Evidence	GET http://localhost:8082/Tunestore2020 /giftsetup.do;jsessionid=40A0AC3633E7CFBE4D406A322991A9A2?cd=gyTlmERHceccCOwArMMOaGUuiclwtKqqGwGKyDNDTiTHAMhDiHjcmOMvAMtfNroWHgToxidrEMpvRWcGlvPFjRVjbfhvmldUAAasfPsYRocGWVUBtBeAUPxSnGBROMWSKKX yOEOwCFUeZJOysjKVCsaXWvbXJosMkuThQuVWGisRUsymxWNETmapYwutSUfcQBUPOLnVrAehdeZMAHeeJSJIDGyAiluLGgTluokbxiGaSrckmUbqsTMbuEmlrEruodsXDWyosAwcvVkprarbXbxhcndlfOTZfXuuYdctpTdArBgpVewScXGfXkFHAphdU vnkDcRadOSSiV5NKjoayWRYnxtRgZWgiHTLeJuWBqMkJjmtWTyZdgqvdXwCHtpBTwmcKZMmkiHtOyqqeiJLMYWPBlqfyjoGurMCfDUdfQjgUQaCeLKLUtYHUKtsLLVdenUEoeiKLiICckxecAJPchATceQZWGsNKQPpwVlWQQbKrMdPAgyCbYitUOawE FTCjWvMnjyHFYUceDAdKgpUXnhkgWWhaQCODTQyXKALKUKTVchQhgXttVAaAglrewrngTblhxoWjkkOdtwlCmCyQhMdRpikqMtyqlxrXZqglFNYlqXlyIttmuMEntSSXprfUbGOoyemTYuvHmQCepafxusDOwBAxeuuWbRmHYvtyxudAIXGbFYuiLiJyaPCB wbggwbbSQQJYeNEpgNbPbdkZFnqaZOtsGawHaMDTBEMCAKbdbhPHXrPTblotgvhaZTJvfOblfNQZAVwPDLOicQeVcTwyLAlSZqbXvZweNyDlirQHPYLconPtmewJqnhsLFOAoJahhRcuNOcoqZpEOHRokIkRxYXDxnjuVBIMxhFesVsUdSSOWjpQkJttVv VPxdxfiaBYiLecLICpGvvKWqfIbGsONPUGnCEriiseVuELJnICUhtZuICGuNhpPYZgqJJTXVQPhOJAvTrQJrZPQJFYArSoFFXSHdnjJFSBLIPQuGCqHonMvMASuqQfhHPySKWPqNfcKUZgeNWpmKEXUOZhvaLgDnRAnYEuUxJVcIUThwRHbncXjNbMvH qkiEbFlmCReTEvBYifkRSOhbvgKxXsffyTkQvqnRsMhOnnHiKYnwUcpIcDCpBBtCgZbkhpxbcMrYtDHEQQHMdBaNtGivOrmaNBTNyRNsqjLIMIKjMGVGeijZUhGsRkDWmXumHFyuDFLAoFbQqbUKASECqmgcVqlOGHvtpCeHFNIQmtmvFKLIDDBCIVDh KjlhvXYVnCnMawrypsgkcWwRVCKbLEWMZhkJEbPUpGGbkepsMtQAtHrsTMGkxLrOUAMBRmjPqaiNuBXtDNGwyqGwgYHaZuBsEbcDsBamOEGJclgyAdBnCEOOlXSuHtOHYCPQWEhrCjxWaGrItTmCSywRgYUAPgPnaqvldeOkeyypyqCVxnrLCN MiQihqnPnJhyqIDbZWiTxhXdbcRddRpyoOPBTydQUpVaUiSxTFZFiEXFtZSfPMWqkcMLKAqZmEeRGaOMopxYdNACqfGWYKATrWKctskIxITXeCMMWUqtKXpJLruhZcGaZEaVkdKOljKLrSBhgDKhyEIaBjwcjrCDYBqCgmgRlybTEiZFpTxpbkEQZro muhQLBhXFaOlFiyGJkAVhsbSwgEmryaFoMLiGsTHJyUmGJlYURoHtGudsRUGXNHMRToBAqWvHFeKiQLjZxwLELqBdhnNSZnatMiQVaIPQtrRXCKcolInqYmRuyZbPViYduhdYkxSTODByfPiZAbMGxBYdlNHplwecKilKyUxFpYwbkHHZnOotFwyEUcqtcie WPeyOGaCXeEENvRCXyckksYVATBXdkHDdihMnEqNOTAAJaoJgsNHPGpJLSOonOwOcljHNhtpVkIEljfxlwdYoGYXDqpJsEVVXOYMUuFltmAHlxlmpseRVyLisBMZwoJoKngsvxsivRkxhRleeeulfPfcEwfVtvetPiJaniiSoNiRMfXGqPDEjVusJdbTtYGRCIGV uESTVNFHSGOdymyGTNaCnaUtfCPkQPHdcTtujRUqbkIqNneGCQXFyQeXbIITc HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:71.0) Gecko/20100101 Firefox/71.0 Pragma: no-cache Cache-Control: no-cache Content-Length: 0 Referer: http://localhost:8082/Tunestore2020/addbalance.do Cookie: JSESSIONID=C7777B5326111FC1039841C45FCA416F Host: localhost:8082

This is a **false positive** because the application did not behave in an unexpected way, instead the application ignored the attempted attack and returned the error message (shown below).


ZAP Scanning Report
ZAP Scanning Report
The Tunestore
https://localhost:8082/Tunestore2020/giftsetup.do;jsessionid=40A0AC3633E7CFBE4D406A
You must log in to this network before you can access the Internet.
the tunestore
buy some tunes - give some tunes
KABOOM!
We're really sorry - the Tunestore fell over. Please call support and read the garbage below to them:
java.lang.RuntimeException: java.sql.SQLSyntaxError
Out
Off
0
0
0
0
0
Copyright © 2008 The Tune Store