WEB APPLICATION SECURITY TESTING REPORT

1. **Executive Summary**:

A comprehensive Web application security test was done using labs tests from portswigger software for learning. GinandJuice shop website was used to test my web security scanners for any SQL injection flaws and portswigger's JWT authentication via algorithm confusion was used to exploit some authentication flaws. I used the Burp suite tool to aid in executing these tests.

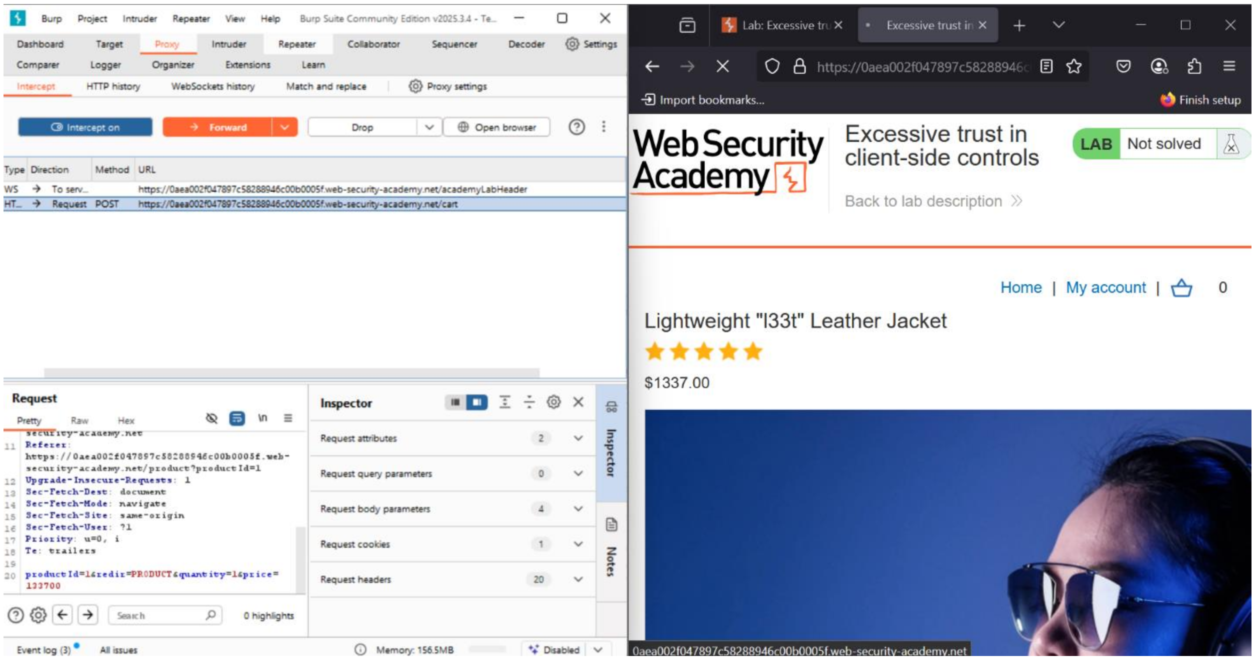
2. **Introduction:**

- **Objective:** Conduct web security testing to identify vulnerabilities like SQL injection, XSS and authentication flaws.
- **Testing Approach:**
  - Gray-box testing
  - Authentication token obtain and replace
  - Burp suite

3. **Scope:**

The tests included user authentication flow, session tokens, client and server requests, proxy setup and e-commerce application.

4. **Methodology:**
   - **SQL Injection:** A proxy was setup between burp suite and the clients web browser to ensure that all web traffic requests can be intercepted. When a client sends a request to order a juice from GinandJuice shop online the request is intercepted and the price of the juice can be changed before payment is made. Below are some pictures to show the test that was run.



Type	Direction	Method	URL
WS	→ To serv...		https://0aea002f047897c58288946c00b0005f.web-security-academy.net/academyLabHeader
HT...	→ Request	POST	https://0aea002f047897c58288946c00b0005f.web-security-academy.net/cart

Request

Pretty Raw Hex

```
security-academy.net
Referer:
https://0aea002f047897c58288946c00b0005f.web-security-academy.net/product?productId=1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers

productId=1&redir=PRODUCT&quantity=1&price=133700
```

0 highlights

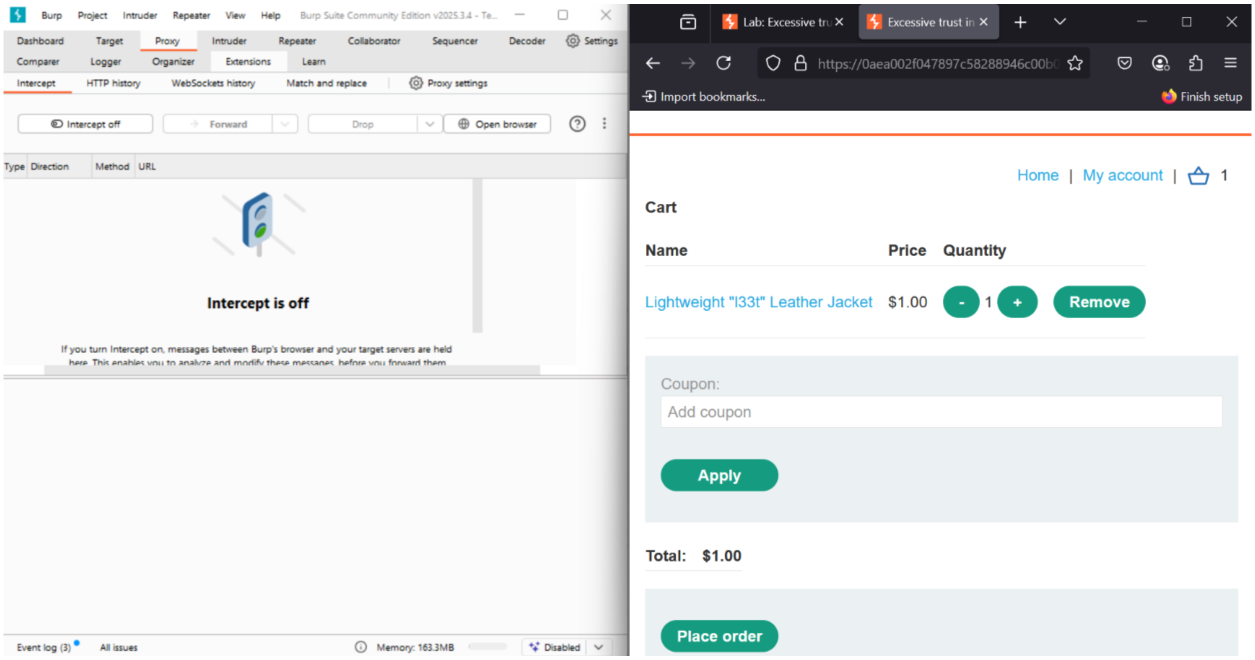
Inspector

Request attributes	2
Request query parameters	0
Request body parameters	4
Request cookies	1
Request headers	20

Lightweight "l33t" Leather Jacket

$1337.00

0aea002f047897c58288946c00b0005f.web-security-academy.net



Intercept is off

If you turn Intercept on, messages between Burp's browser and your target servers are held here. This enables you to analyze and modify these messages, before you forward them.

Cart

Name	Price	Quantity	
Lightweight "l33t" Leather Jacket	$1.00	- 1 +	Remove

Coupon:

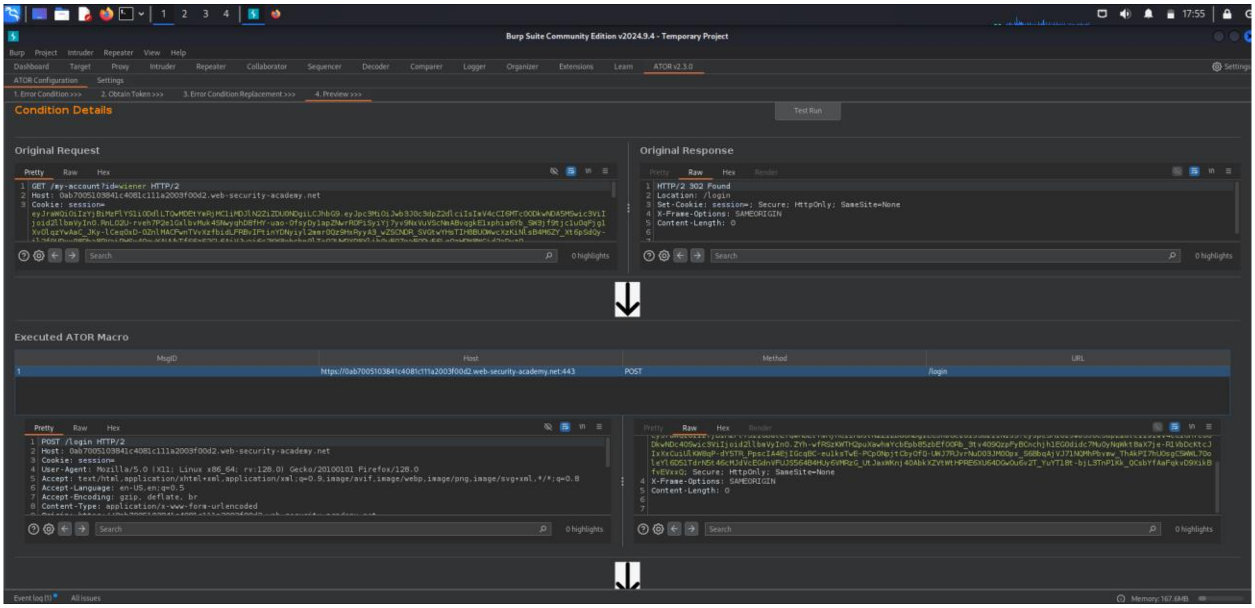
Add coupon

Apply

Total: $1.00

Place order

- **Authentication flaws:** Here the user authentication flow is used here. A user would try to sign in to a site and a session token is assigned to that request. After we copy the web address link and log out. We then try to log back in using the web address link copied but are sent back to the sign in page, this is where burp suites extension, Authentication Token Obtain and Replace (ATOR) comes in. We would send the 2 requests for logging in to our repeater, the failed request and successful request. We then Forward the requests to our ATOR extension to perform modifications. With ATOR we can highlight the session cookies to ensure that when we call the failed request it picks the successful request session cookie and redirect to that page to ensure a successful login. After ATOR does the modification, we would be able to sign in directly with the request that failed at first. Below are some pictures to show the test that was run.


Burp Suite Community Edition v2024.9.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn ATOR v2.3.0
ATOR Configuration Settings
1. Error Condition >>> 2. Obtain Token >>> 3. Error Condition Replacement >>> 4. Preview >>>
Test Run
Pretty Raw Hex Render
Search
0 highlights
Event log (1) All issues
Memory: 167.6MB
17:55

Condition Details

Original Request

```
GET /my-account?id=wiener HTTP/2
Host: 0ab7005103841c4081c111a2003f00d2.web-security-academy.net
Cookie: session=
eyJraWQiOiIzYjBiMzFlYS1iODdlLTQwMDEtYmRjMC1iMDJlN2ZiZDU0NDgiLCJhbGciOiJSUzI1NiJ9.eyJpc3MiOiJwb3J0c3dpZ2dlciIsImV4cCI6MTc0ODkwNDA5MSwic3ViI
joid2llbmVyIn0.RnLO2U-rveh7P2elGxlbvMuk4SNwyqhD8fHY-uao-0fsyDy1apZNwrROFiSyiYj7yv9NxVuVScNmABvqgkElxphia6Yb_SM3jf9tjcluOqFjgl
XvOlqzYwAaC_JKy-lCeqOxD-0ZnlMACFwnTVvXzfbidLFRBvIFtinYDNyiyl2mmr0Qz9HxRyyA9_wZSCNDR_SVGtwYHsTIHBBUOWwcXzKiNlsB4M6ZY_Xt6pSdQy-
```

Original Response

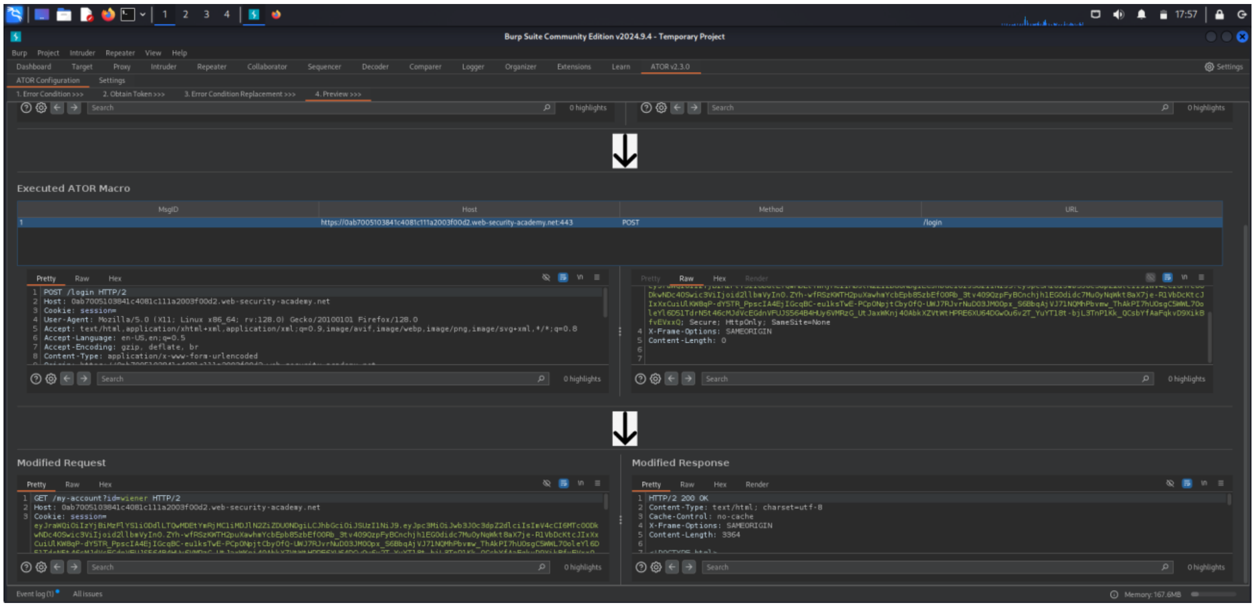
```
HTTP/2 302 Found
Location: /login
Set-Cookie: session=; Secure; HttpOnly; SameSite=None
X-Frame-Options: SAMEORIGIN
Content-Length: 0
```

Executed ATOR Macro

MsgID	Host	Method	URL
1	https://0ab7005103841c4081c111a2003f00d2.web-security-academy.net:443	POST	/login

```
POST /login HTTP/2
Host: 0ab7005103841c4081c111a2003f00d2.web-security-academy.net
Cookie: session=
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
```

```
DkwNDc40Swic3ViIjoid2llbmVyIn0.ZYh-wfRSzKWTH2puXawhmYcbEpb85zbEf0ORb_3tv409QzpFyBCnchjhlEGOdidc7MuOyNqWktBaX7je-RlVbDcKtcJ
IxXxCuiUlKWBqP-dY5TR_PpscIA4EjIGcqBC-eulksTwE-PCpONpjtCbyOfQ-UWJ7RJvrNuD03JMO0px_S6BbqAjVJ71NQMhPbvmw_ThAkPI7hUOsgCSWWL7Oo
leYl6D51TdrN5t46cMJdVcEGdnVFUJS564B4HUy6VMRzG_UtJaxWKnj40AbkXZVtWtHPRE6XU64DGwOu6v2T_YuYT18t-bjL3TnPlKk_QCsbYfAaFqkvD9XikB
fvEVxxQ; Secure; HttpOnly; SameSite=None
X-Frame-Options: SAMEORIGIN
Content-Length: 0
```


Burp Suite Community Edition v2024.9.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn ATOR v2.3.0
ATOR Configuration Settings
1. Error Condition >>> 2. Obtain Token >>> 3. Error Condition Replacement >>> 4. Preview >>>
Pretty Raw Hex Render
Search
0 highlights
Event log (1) All issues
Memory: 167.6MB
17:57

Executed ATOR Macro

MsgID	Host	Method	URL
1	https://0ab7005103841c4081c111a2003f00d2.web-security-academy.net:443	POST	/login

```
POST /login HTTP/2
Host: 0ab7005103841c4081c111a2003f00d2.web-security-academy.net
Cookie: session=
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
```

```
DkwNDc40Swic3ViIjoid2llbmVyIn0.ZYh-wfRSzKWTH2puXawhmYcbEpb85zbEf0ORb_3tv409QzpFyBCnchjhlEGOdidc7MuOyNqWktBaX7je-RlVbDcKtcJ
IxXxCuiUlKWBqP-dY5TR_PpscIA4EjIGcqBC-eulksTwE-PCpONpjtCbyOfQ-UWJ7RJvrNuD03JMO0px_S6BbqAjVJ71NQMhPbvmw_ThAkPI7hUOsgCSWWL7Oo
leYl6D51TdrN5t46cMJdVcEGdnVFUJS564B4HUy6VMRzG_UtJaxWKnj40AbkXZVtWtHPRE6XU64DGwOu6v2T_YuYT18t-bjL3TnPlKk_QCsbYfAaFqkvD9XikB
fvEVxxQ; Secure; HttpOnly; SameSite=None
X-Frame-Options: SAMEORIGIN
Content-Length: 0
```

Modified Request

```
GET /my-account?id=wiener HTTP/2
Host: 0ab7005103841c4081c111a2003f00d2.web-security-academy.net
Cookie: session=
eyJraWQiOiIzYjBiMzFlYS1iODdlLTQwMDEtYmRjMC1iMDJlN2ZiZDU0NDgiLCJhbGciOiJSUzI1NiJ9.eyJpc3MiOiJwb3J0c3dpZ2dlciIsImV4cCI6MTc0ODk
wNDc40Swic3ViIjoid2llbmVyIn0.ZYh-wfRSzKWTH2puXawhmYcbEpb85zbEf0ORb_3tv409QzpFyBCnchjhlEGOdidc7MuOyNqWkt8aX7je-RlVbDcKtcJIxXx
CuiUlKWBqP-dY5TR_PpscIA4EjIGcqBC-eulksTwE-PCpONpjtCbyOfQ-UWJ7RJvrNuD03JMO0px_S6BbqAjVJ71NQMhPbvmw_ThAkPI7hUOsgCSWWL7OoleYl6D
```

Modified Response

```
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
Cache-Control: no-cache
X-Frame-Options: SAMEORIGIN
Content-Length: 3364
```

5. **Identified Vulnerabilities:**
   - Cross Site Scripting
   - Security misconfiguration
   - SQL injection
   - Authentication bypass by algorithm confusion

6. **Mitigation Strategies:**
   - Cross Site Scripting:
     - Filter input on arrival.
     - Encode data on output.
     - Use appropriate response headers.
   - Security misconfiguration:
     - Adopt repeatable hardening processes.
     - Perform regular updates.
     - Continuous monitoring.
   - SQL injection:
     - Input validation
     - Parametrized queries including prepared statements
   - Authentication bypass by algorithm confusion:
     - Clearly define JSON web token configuration.
     - Secure the use of the JKU parameter.

7. **Conclusion:**

   These mitigation strategies listed when followed would help prevent the vulnerabilities stated earlier in the report and ensure systems are more secure and free from threats, vulnerabilities and attack.