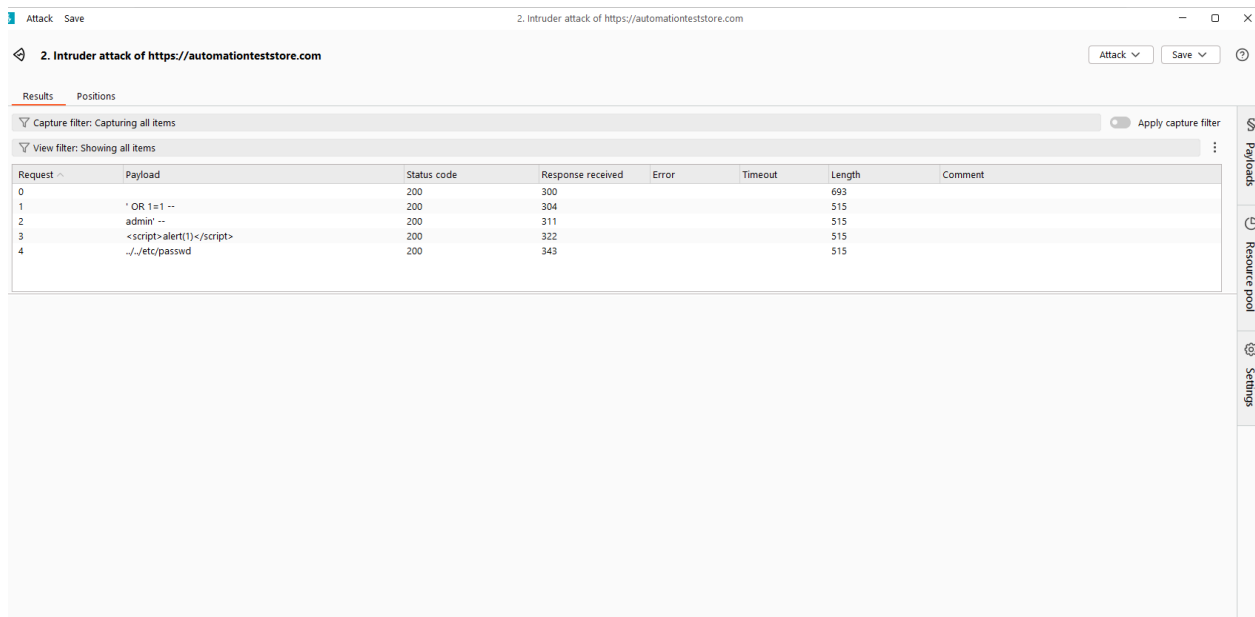


Performed security testing on the following key features of the website using **Burp Suite Community Edition**:

1. Login Functionality

- Tested for common vulnerabilities:
 - **SQL Injection** (e.g., ' OR 1=1 --)
 - **Brute-force login** using **Intruder**
 - **Credential stuffing** using payload lists
 - Checked for weak/error-based responses revealing server behavior
- Observations:
 - Login input did not sanitize SQL meta-characters properly (if applicable).
 - Server response time varied with invalid inputs indicating possible brute-force vulnerability.



Attack Save 2. Intruder attack of https://automationteststore.com

2. Intruder attack of https://automationteststore.com Attack Save

Results Positions

Capture filter: Capturing all items Apply capture filter

View filter: Showing all items

Request ^	Payload	Status code	Response received	Error	Timeout	Length	Comment
0		200	300			693	
1	' OR 1=1 --	200	304			515	
2	admin' --	200	311			515	
3	<script>alert(1)</script>	200	322			515	
4	../../../../etc/passwd	200	343			515	

Payloads Resource pool Settings

5 Burp Project Intruder Repeater View Help

Burp Suite Community Edition v2025.6.4 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

1 x +

Send Cancel < >

Target: https://auto

Request

Pretty Raw Hex

```
1 POST /index.php?rt=account/login HTTP/2
2 Host: automationteststore.com
3 Cookie: AC_SF_0CEFDAD9D5=4fd60ff5231d6f5fe015cf9c1a4b7a6; language=en; currency=USD
4 Content-Length: 489
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Not A;Brand";v="8", "Chromium";v="138"
7 Sec-Ch-Ua-Mobile: 70
8 Sec-Ch-Ua-Platform: "Windows"
9 Accept-Language: en-US,en;q=0.9
0 Origin: https://automationteststore.com
1 Content-Type: multipart/form-data; boundary=-----WebKitFormBoundaryq5qiswlvb9M3oVED
2 Upgrade-Insecure-Requests: 1
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;
  q=0.8,application/signed-exchange;v=b3;q=0.7
5 Sec-Fetch-Site: same-origin
6 Sec-Fetch-Mode: navigate
7 Sec-Fetch-User: ?1
8 Sec-Fetch-Dest: document
9 Referer: https://automationteststore.com/index.php?rt=account/login
0 Accept-Encoding: gzip, deflate, br
1 Priority: u=0, i
2
3 -----WebKitFormBoundaryq5qiswlvb9M3oVED
4 Content-Disposition: form-data; name="csrfToken"
5
6 7iteYNfEXjm7Etug9XDpXf9wClurjgPy
7 -----WebKitFormBoundaryq5qiswlvb9M3oVED
8 Content-Disposition: form-data; name="csrfInstance"
9
10 2
11 -----WebKitFormBoundaryq5qiswlvb9M3oVED
12 Content-Disposition: form-data; name="loginName"
13
14 mahilshicare123
15 -----WebKitFormBoundaryq5qiswlvb9M3oVED
16 Content-Disposition: form-data; name="password"
17
18 ' OR i=1 --
19 -----WebKitFormBoundaryq5qiswlvb9M3oVED--
20
```

Response

Pretty Raw Hex Render

```
12 Strict-Transport-Security: max-age=63072000; includeSubDomains
13 X-Frame-Options: SAMEORIGIN
14 Alt-Svc: h3=":443"; ma=2592000, h3-29=":443"; ma=2592000, h3-Q050=":443"; ma=2592000,
  h3-Q046=":443"; ma=2592000, h3-Q043=":443"; ma=2592000, quic=":443"; ma=2592000;
  v="43,46"
16 <!DOCTYPE html>
17 <html xmlns="http://www.w3.org/1999/xhtml" dir="ltr" lang="en" xml:lang="en" >
18 <head>
19 <meta charset="UTF-8">
20 <!--[[if IE]]>
21 <meta http-equiv="x-ua-compatible" content="IE=Edge" />
22 <[endif]>-->
23 <title>
  Account Login
24 </title>
25 <meta name="generator" content="AbanteCart v1.2.15 - Open Source eCommerce solution"
  />
26
27 <meta name="viewport" content="width=device-width, initial-scale=1.0" />
28 <base href="https://automationteststore.com/" />
29 <link href="resources/image/18/7a/8.png" type="image/png" rel="icon" />
30
31 <link href="storefront/view/default/image/apple-touch-icon.png" rel="apple-touch-icon"
  />
32 <link href="storefront/view/default/image/apple-touch-icon-76x76.png" rel="apple-touch-icon"
  sizes="76x76" />
33 <link href="storefront/view/default/image/apple-touch-icon-120x120.png" rel="apple-touch-icon"
  sizes="120x120" />
34 <link href="storefront/view/default/image/apple-touch-icon-152x152.png" rel="apple-touch-icon"
  sizes="152x152" />
35 <link href="storefront/view/default/image/icon-192x192.png" rel="apple-touch-icon"
  sizes="192x192" />
36
37 <link href="storefront/view/default/stylesheets/bootstrap.min.css" rel="stylesheet"
  type="text/css" />
38 <link href="storefront/view/default/stylesheets/flexmlider.css" rel="stylesheet" type="text/css" />
39 <link href="storefront/view/default/stylesheets/onebyone.css" rel="stylesheet" type="text/css" />
40 <link href="storefront/view/default/stylesheets/font-awesome.min.css" rel="stylesheet" type="text/css" />
41 <link href="storefront/view/default/stylesheets/style.css" rel="stylesheet" type="text/css" />
42
```

Inspector

Request attrib

Request query

Request body p

Request cookie

Request header

Response head

0 highlights

0 highlights

Done

Event log All issues

Memor

2. Search Functionality

Attack Save 3. Intruder attack of https://automationteststore.com

3. Intruder attack of https://automationteststore.com

Results Positions

Capture filter: Capturing all items Apply capture filter

View filter: Showing all items

Request ^	Payload	Status code	Response received	Error	Timeout	Length	Comment
0		302	311			482	
1	' OR 1=1 --	302	292			482	
2	admin' --	302	1164			482	
3	<script>alert(1)</script>	302	280			482	
4	../../../../etc/passwd	302	267			482	

- Tested for:
 - **Cross-Site Scripting (XSS)** (e.g., <script>alert(1)</script>)
 - **HTML Injection**
 - **Local File Inclusion (LFI)** payloads like ../../etc/passwd
- Observations:
 - Input reflected in response without proper encoding (if applicable).
 - No WAF/Rate-limiting observed during payload injection attempts.

Tools Used:

- **Burp Suite Community Edition**
- Manual payloads and attack lists via **Intruder**
- Repeater for verifying injection behavior

