

The background features abstract, overlapping geometric shapes in various shades of blue, ranging from light sky blue to deep navy blue. These shapes are primarily located on the left and right sides of the frame, creating a modern, dynamic feel. The central area is a plain, light grayish-white.

RPG

この問題に取り組む前に

- ▶ この演習もスロットとガチャ同様デベロッパーツールを使用します。

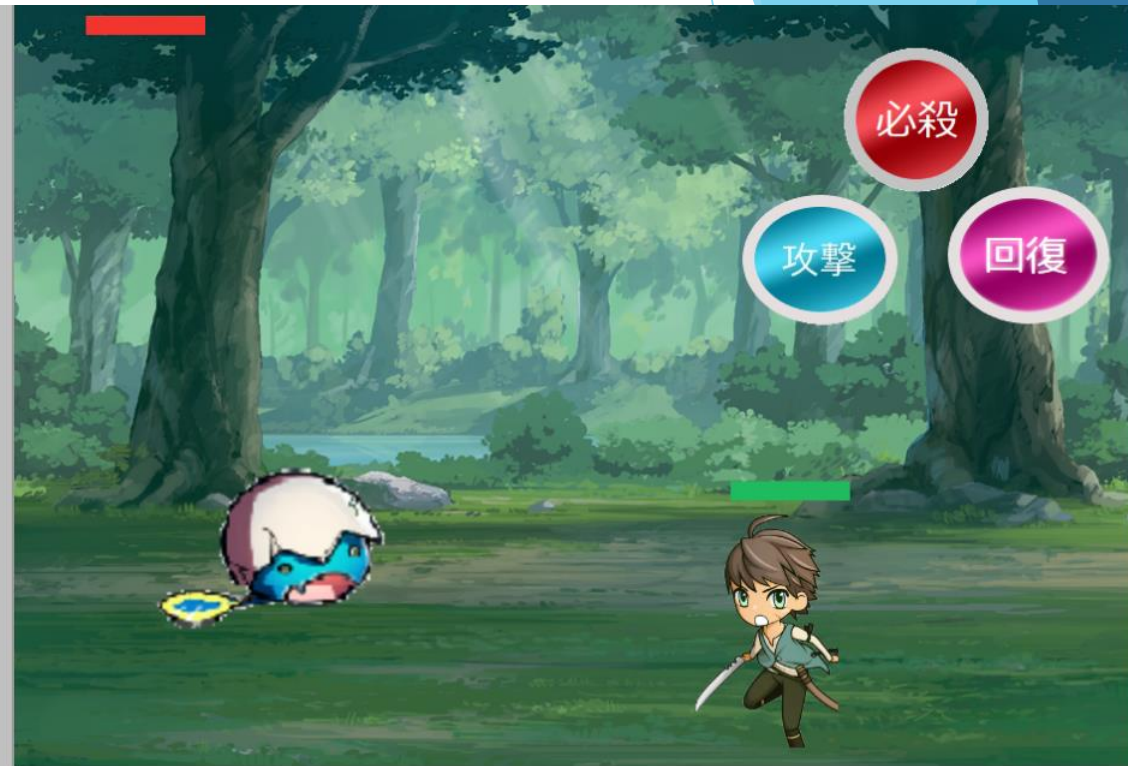
使用方法はスロット問題資料をご覧ください。

RPGの目的

- ▶ この問題はFLAG 1 = ○○とFLAG 2 = ○○の○○がわかれば問題クリアとなります。
- ▶ デベロッパーツールの使い方の復習

RPGの仕様

演習問題に行くと
チュートリアルが始まります。

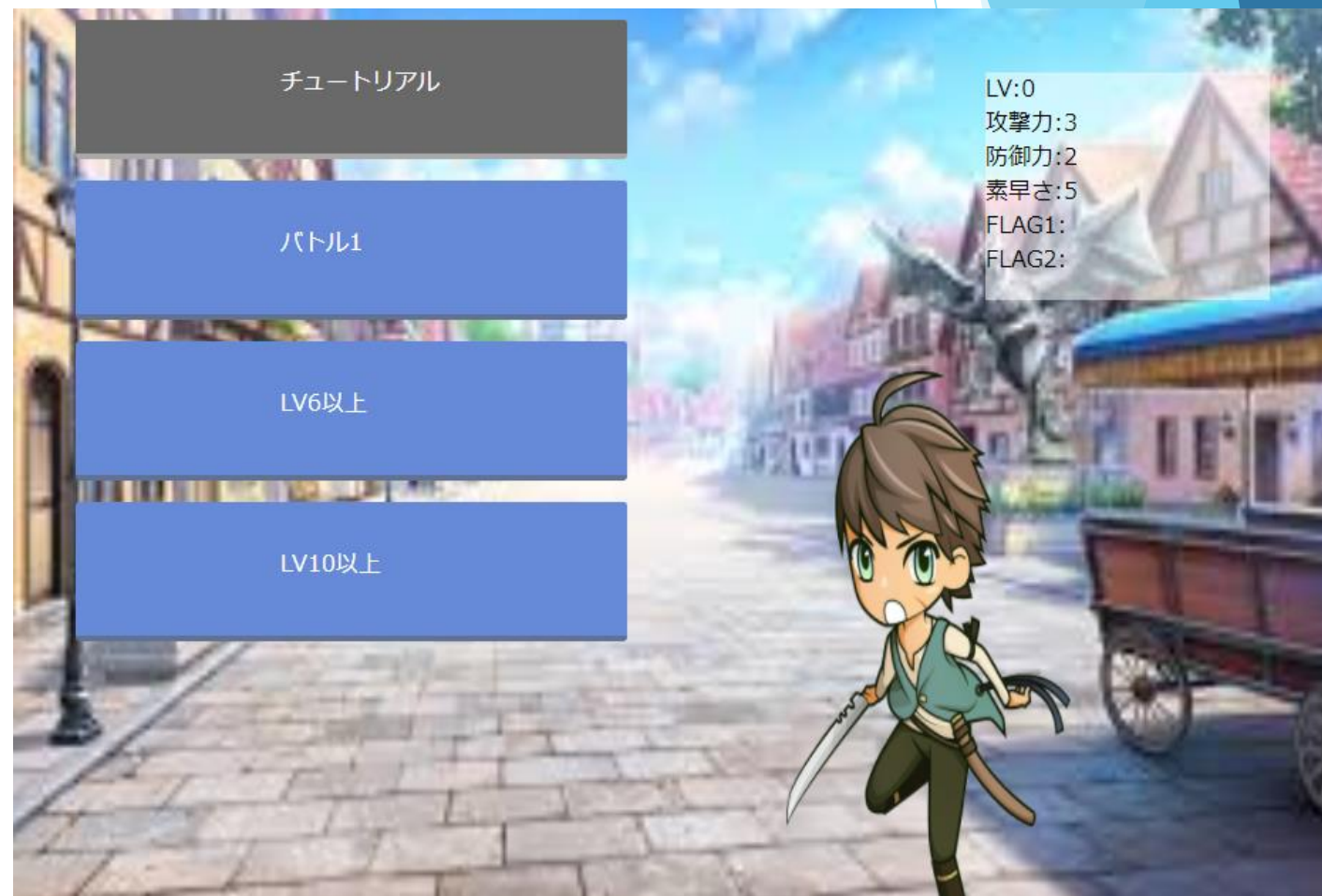


戦闘画面の説明



RPGの仕様

チュートリアル終了後
ステージ選択画面に行
きます。



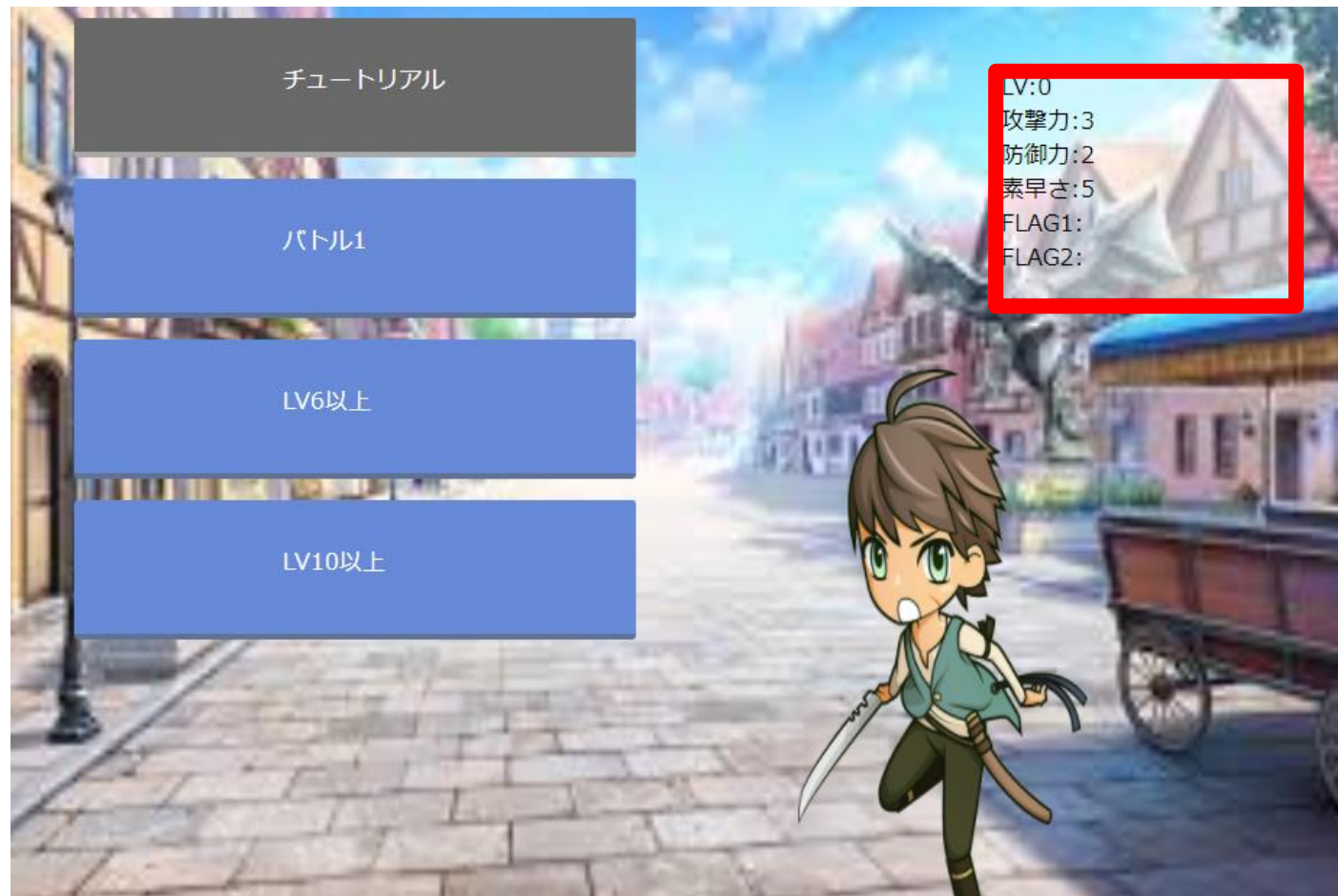
RPGの仕様



レベルUP ↑ ↑

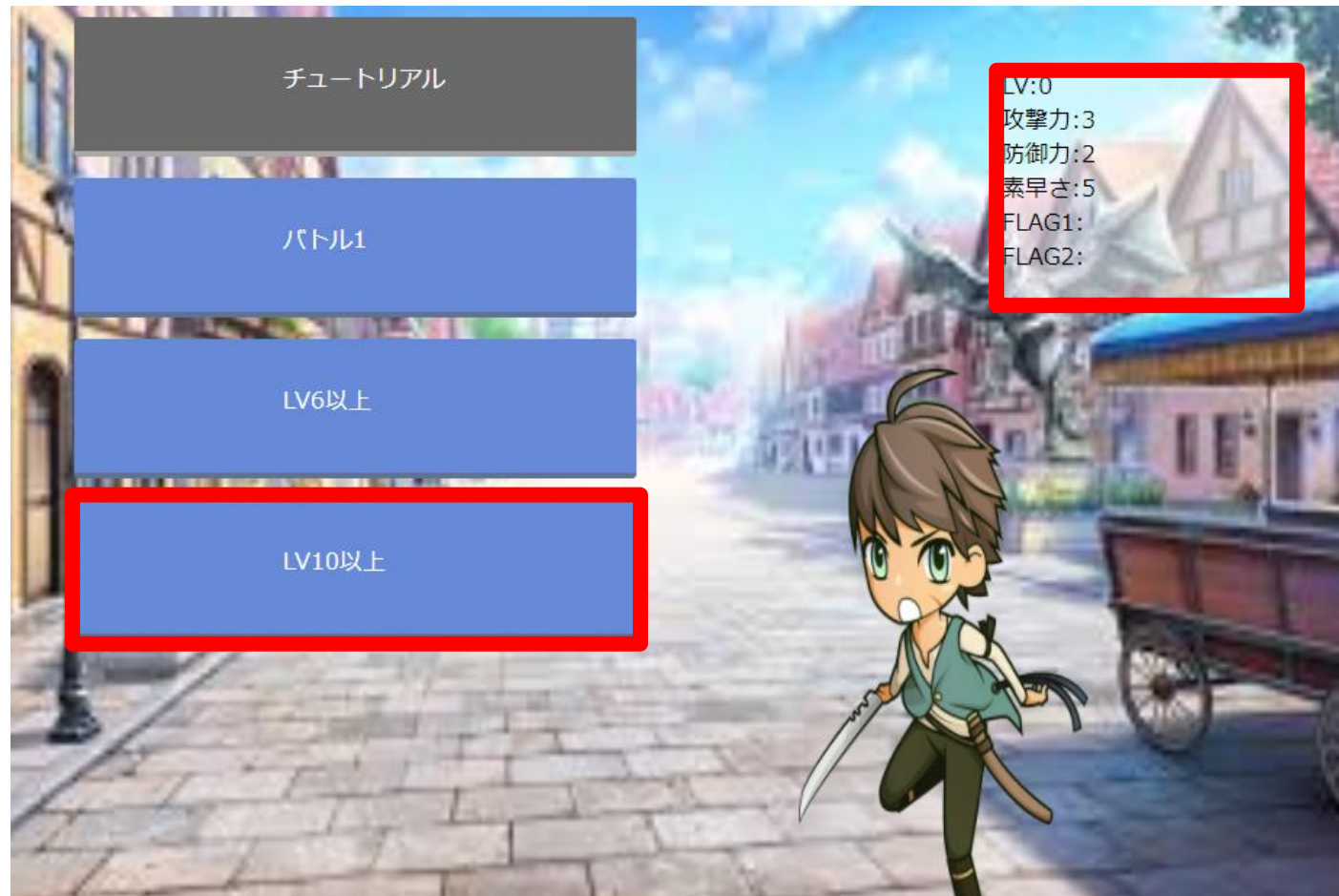
敵を何回か倒すとレベルが上がってきます

FLAG 1 を表示させよう



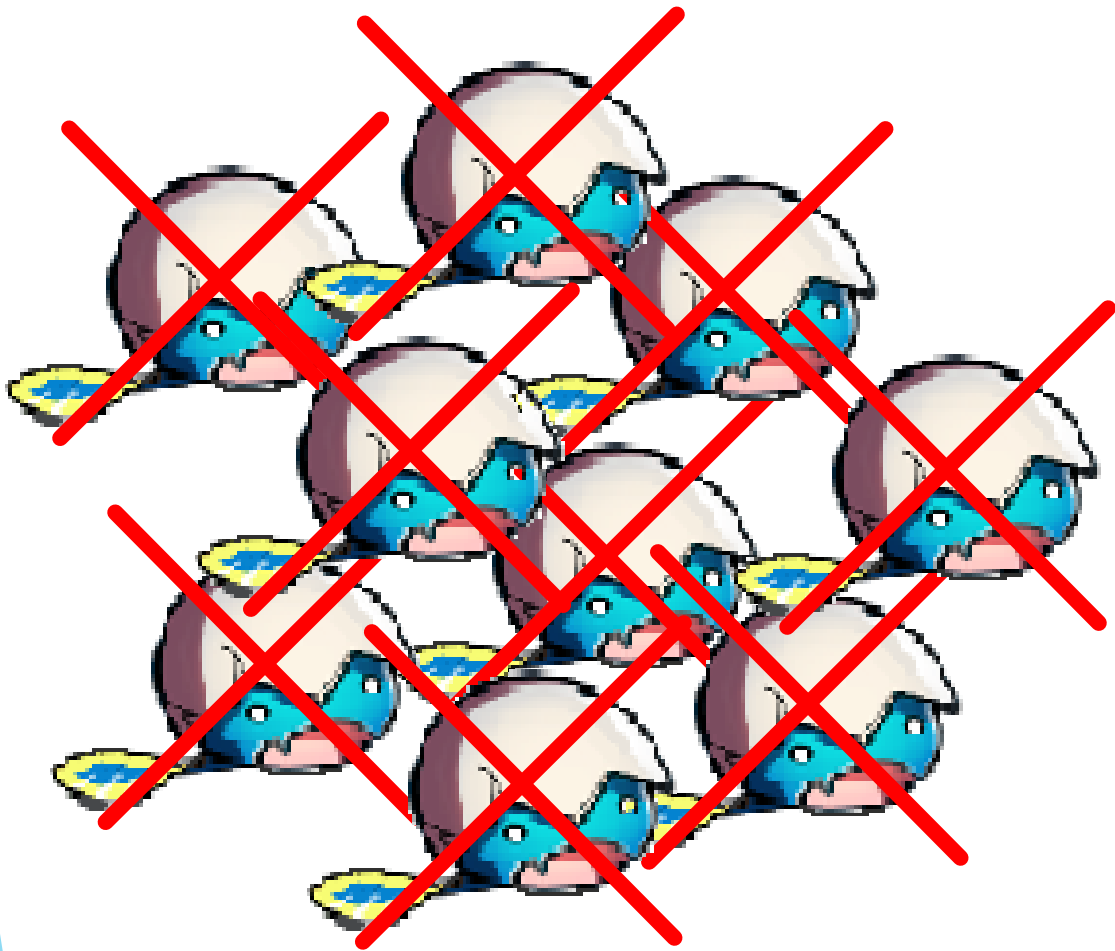
FLAG1はLV10以上になると表示されます。

FLAG 1 を表示させよう



LV10で入れる場所にFLAGがあるのではないかと推測します。

FLAG 1 を表示させよう



レベルUP ↑ ↑

レベルUP ↑ ↑

レベルUP ↑ ↑

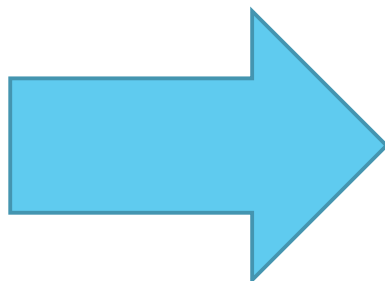
レベルUP ↑ ↑



RPG経験者ならわかると思いますが、真面目にレベルを上げるのは時間がかかり面倒くさいですね...

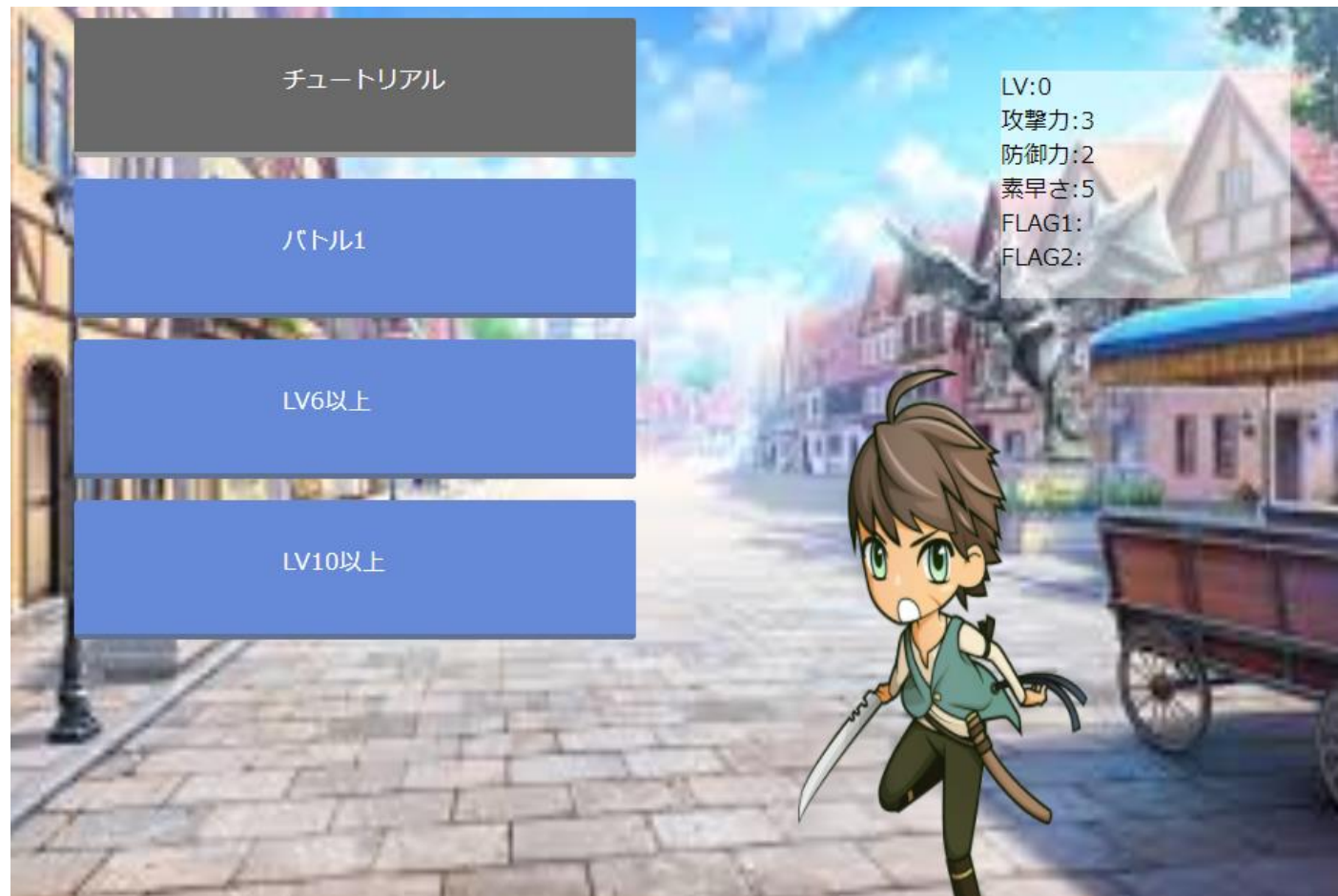
FLAG 1 を表示させよう

LV1



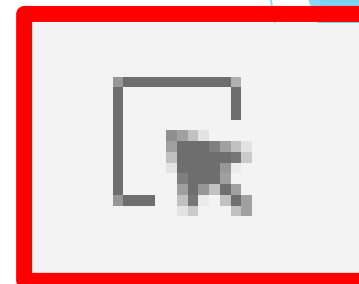
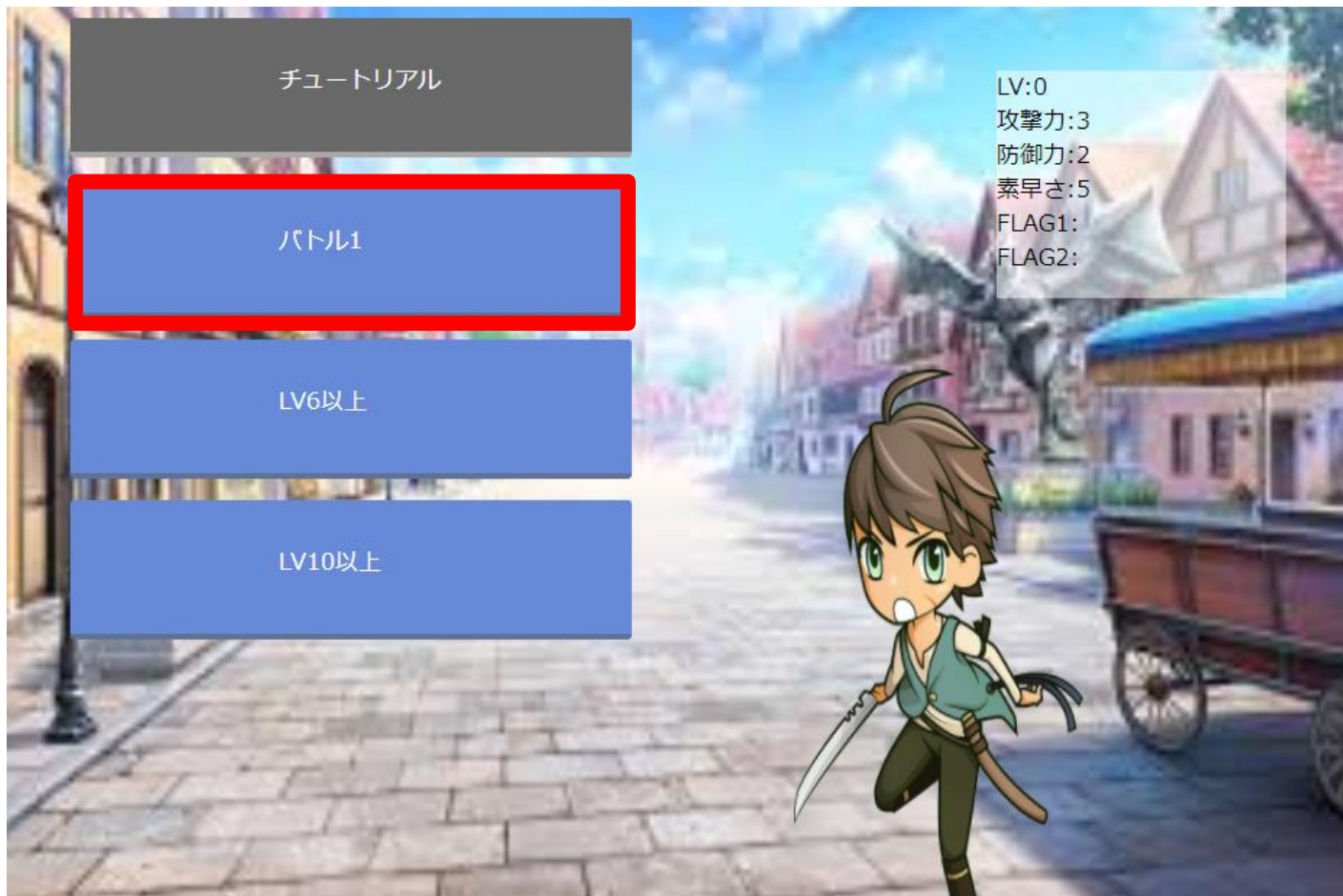
LV10でなくてもLV10のステージに入れるように書き換えてみます。

FLAG 1 を表示させよう



ステージ選択画面でデベロッパーツールを使います

FLAG 1 を表示させよう



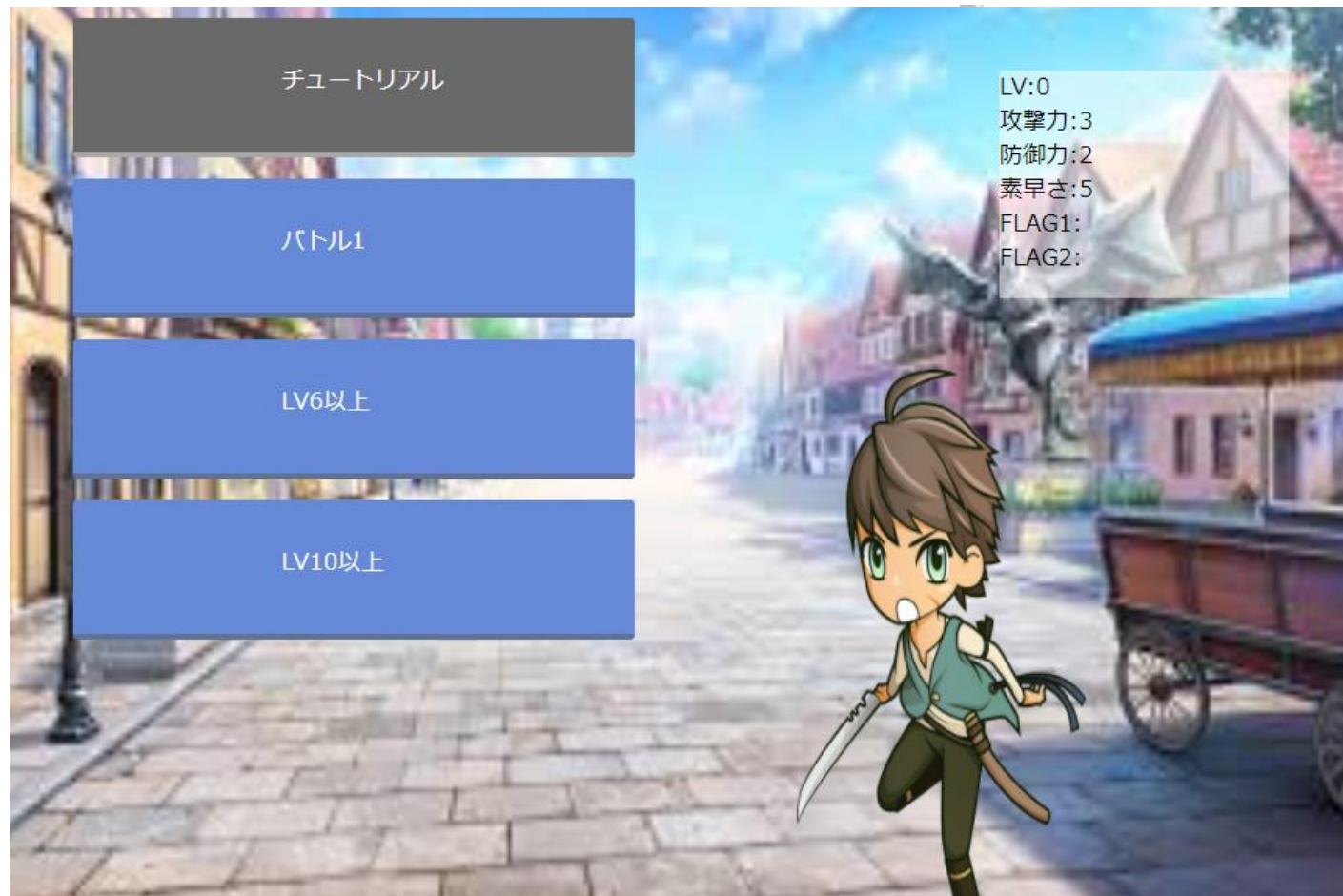
デベロッパー起動したら右のアイコンをクリックし、バトル1をクリックしてください。

FLAG 1 を表示させよう

```
▼<body oncontextmenu="return false" bgcolor="black">
  ▼<ul>
    ▼<li>
      <a href="#" class="square_btn2">チュートリアル</a>
    </li>
    ▼<li>
      *** <a href="game2.php" class="square_btn"> バトル1</a> == $0
    </li>
    ▼<li>
      <a id="lv3" href="#" class="square_btn"> LV6以上</a>
    </li>
    ▼<li>
      <a id="lv4" href="#" class="square_btn"> LV10以上</a>
    </li>
    ▶<div class="box">...</div>
    
  </ul>
</body>
</html>
```

すると、バトル1の部分が水色で表示されます。

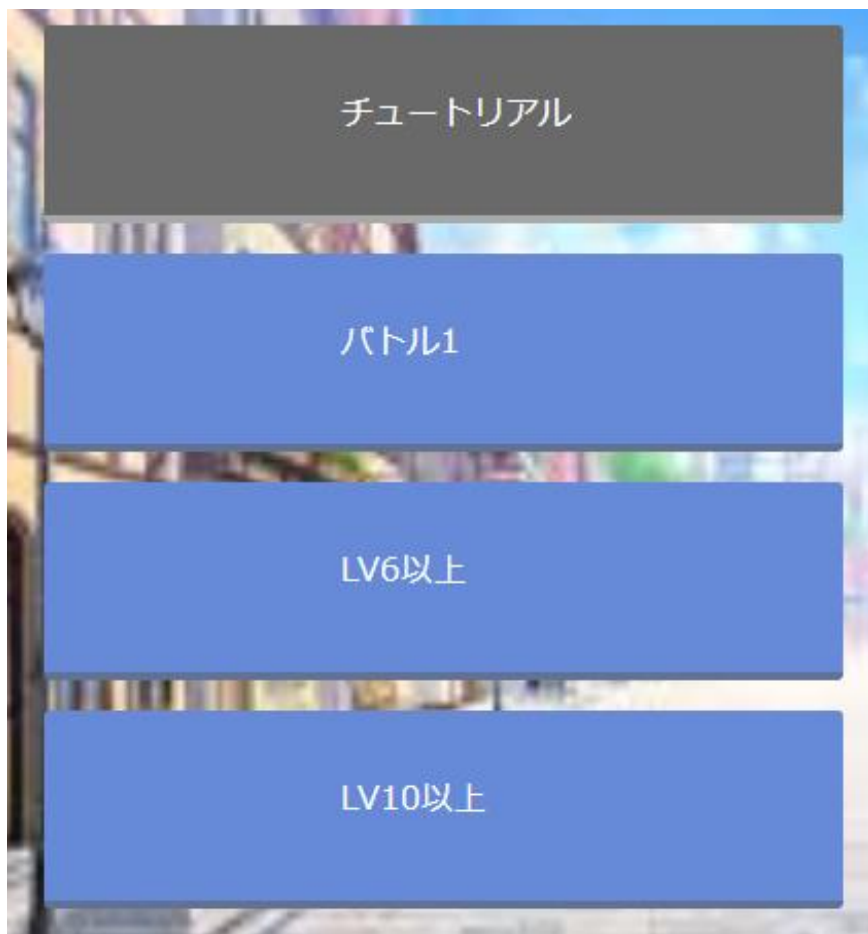
FLAG 1 を表示させよう



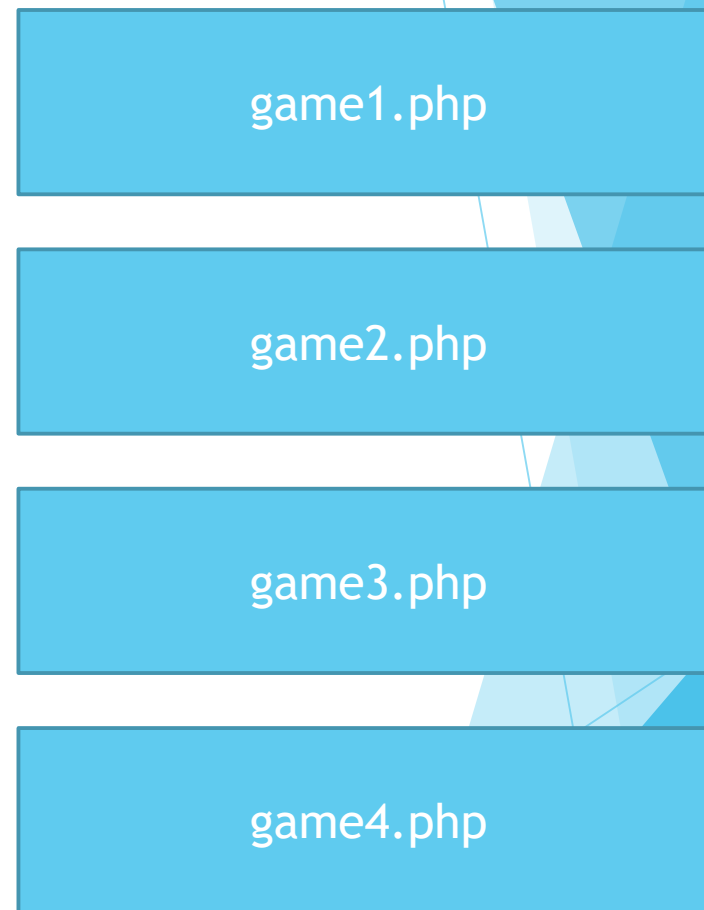
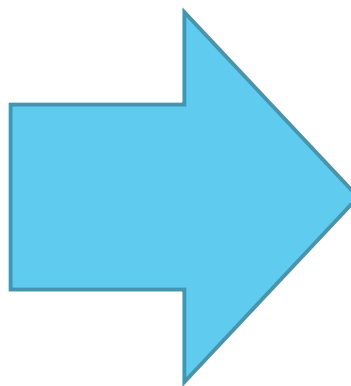
```
oncontextmenu="return false" bgcolor="black">  
>  
li>  
  <a href="#" class="square_btn2">チュートリアル</a>  
/li>  
li>  
  <a href="game2.php" class="square_btn">バトル1</a> == $0  
/li>  
li>  
  <a id="lv3" href="#" class="square_btn"> LV6以上</a>  
/li>  
li>  
  <a id="lv4" href="#" class="square_btn"> LV10以上</a>  
/li>  
div class="box">...</div>  
img class="soutai" src="play2.png" alt="写真" width="200"  
height="400">  
l>  
y>  
>
```

見比べてみると、バトル1をクリックすると
game2.phpに行くよと書いてあります

FLAG 1 を表示させよう



これを考えると...



game2.phpをgame4.phpに書き換えれば入ることができそうですね

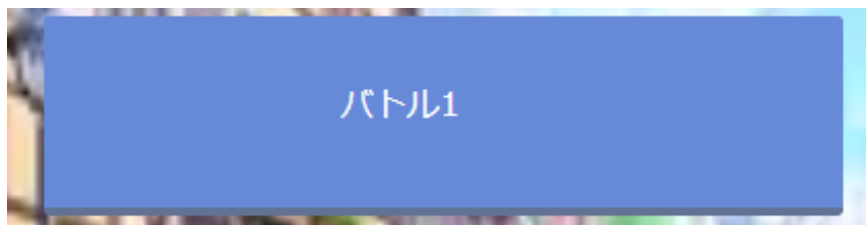
FLAG 1 を表示させよう

```
▼<body oncontextmenu="return false" bgcolor="black">
  ▼<ul>
    ▼<li>
      <a href="#" class="square_btn2">チュートリアル</a>
    </li>
    ▼<li>
      <a href="game2.php" class="square_btn">バトル1</a> == $0
    </li>
    ▼<li>
      <a id="lv3" href="#" class="square_btn">LV6以上</a>
    </li>
    ▼<li>
      <a id="lv4" href="#" class="square_btn">LV10以上</a>
    </li>
    ▶<div class="box">...</div>
    
  </ul>
</body>
</html>
```

```
▼<body oncontextmenu="return false" bgcolor="black">
  ▼<ul>
    ▼<li>
      <a href="#" class="square_btn2">チュートリアル</a>
    </li>
    ▼<li>
      <a href="game4.php" class="square_btn">バトル1</a> == $0
    </li>
    ▼<li>
      <a id="lv3" href="#" class="square_btn">LV6以上</a>
    </li>
    ▼<li>
      <a id="lv4" href="#" class="square_btn">LV10以上</a>
    </li>
    ▶<div class="box">...</div>
    
  </ul>
</body>
</html>
```

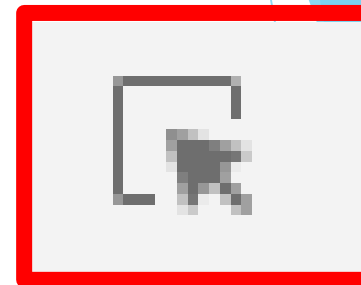
先ほど水色になった部分のhrefと書かれているところをダブルクリックすると書き換えが可能になるのでgame2.phpをgame4.phpに書き換えてください。

FLAG 1 を表示させよう



書き換えた後バトル1をクリックし、右の画面が出てくれば書き換え成功です。

FLAG 1 を表示させよう



最後に、デベロッパーツールを使ってアイコンをクリックし、このバトル画面をクリックします。

FLAG 1 を表示させよう

```
<!DOCTYPE html>
<html>
  <head>...</head>
  <body>
    <div id="enchant-stage" style="position: absolute; font-size:
    12px; text-size-adjust: none; -webkit-tap-highlight-color:
    rgba(0, 0, 0, 0); width: 934px; height: 636px;">
      <div style="position: absolute; overflow: hidden; transform-
      origin: 0px 0px; width: 940px; height: 640px; transform:
      scale(0.99375); background-color: white;" == $0
        <canvas width="940" height="640" style="position: absolute;
        top: 0px; left: 0px;">
        </div>
      </div>
    </div>
    <!--<form action = ghgfl.php method = "POST">
    <input type="hidden" name="ghg" value="win">
    <input type="submit" style="position: absolute; left: 400px;
    top: 300px" value="Brute force">
    </form> -->
  </body>
</html>
```

すると、先ほどと同じように水色になります。

FLAG 1 を表示させよう

```
<!DOCTYPE html>
▼<html>
  ▶<head>...</head>
  ▼<body>
    ▼<div id="enchant-stage" style="position: absolute; font-size:
      12px; text-size-adjust: none; -webkit-tap-highlight-color:
      rgba(0, 0, 0, 0); width: 934px; height: 636px;">
      ▼<div style="position: absolute; overflow: hidden; transform-
        origin: 0px 0px; width: 940px; height: 640px; transform:
        scale(0.99375); background-color: white;"> == $0
        <canvas width="940" height="640" style="position: absolute;
          top: 0px; left: 0px;">
        </div>
      </div>
      <!--<form action = ghgfl.php method = "POST">
      <input type="hidden" name="ghg" value="win">
      <input type="submit" style="position: absolute; left: 400px;
      top: 300px" value="Brute force">
      </form> -->
    </body>
  </html>
```

```
<!DOCTYPE html>
▼<html>
  ▼<head>
    <meta charset="UTF-8">
    <meta http-equiv="x-ua-compatible" content="IE=Edge">
    <meta name="viewport" content="width=device-width, user-
      scalable=no">
    <meta name="apple-mobile-web-app-capable" content="yes">
    <script type="text/javascript" src="jQuery.main.js"></script>
    <script type="text/javascript" src="enchant.js"></script>
    <script type="text/javascript" src="ui.enchant.js"></script>
    <script type="text/javascript" src="final_battle.js"></script>
    <style type="text/css">
      body {
        margin: 0;
        padding: 0;
      }
    </style>
    <!-- FLAG{LV OVER10} -->
  </head>
```

水色になったところのすぐ上に<head>...</head>と書かれた場所の▶のアイコンを押すとFLAG1が表示されます

FLAG2を表示させよう



FLAG2は先ほどのこのキャラクターを倒すことができればFLAG2が手に入ります。

FLAG2を表示させよう



LOSE

しかし、このキャラは最強です。
たとえ、LV10000000でも絶対勝てません！

FLAG2を表示させよう

では、どうしたらいいか...？

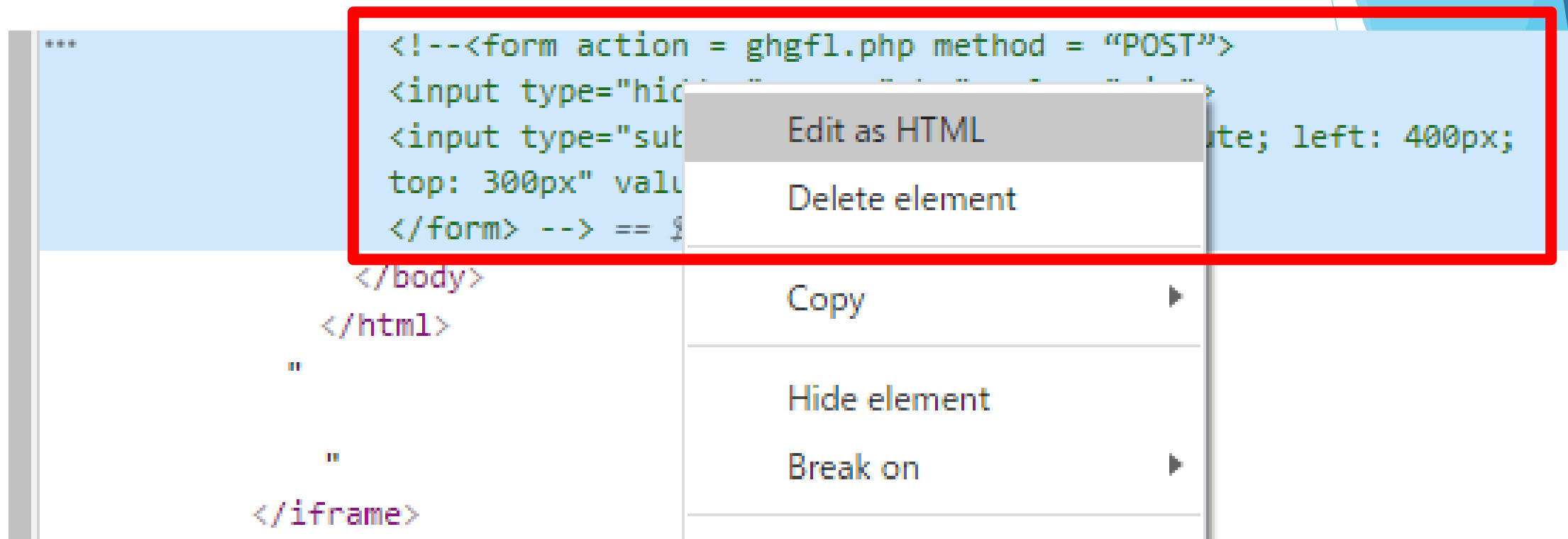


FLAG2を表示させよう

```
<!DOCTYPE html>
<html>
  <head>...</head>
  <body>
    <div id="enchant-stage" style="position: absolute; font-size:
    12px; text-size-adjust: none; -webkit-tap-highlight-color:
    rgba(0, 0, 0, 0); width: 934px; height: 636px;">
      <div style="position: absolute; overflow: hidden; transform-
      origin: 0px 0px; width: 940px; height: 640px; transform:
      scale(0.99375); background-color: white;"> == $0
        <canvas width="940" height="640" style="position: absolute;
        top: 0px; left: 0px;">
      </div>
    </div>
    <!--<form action = ghgfl.php method = "POST">
    <input type="hidden" name="ghg" value="win">
    <input type="submit" style="position: absolute; left: 400px;
    top: 300px" value="Brute force">
    </form> -->
  </body>
</html>
```

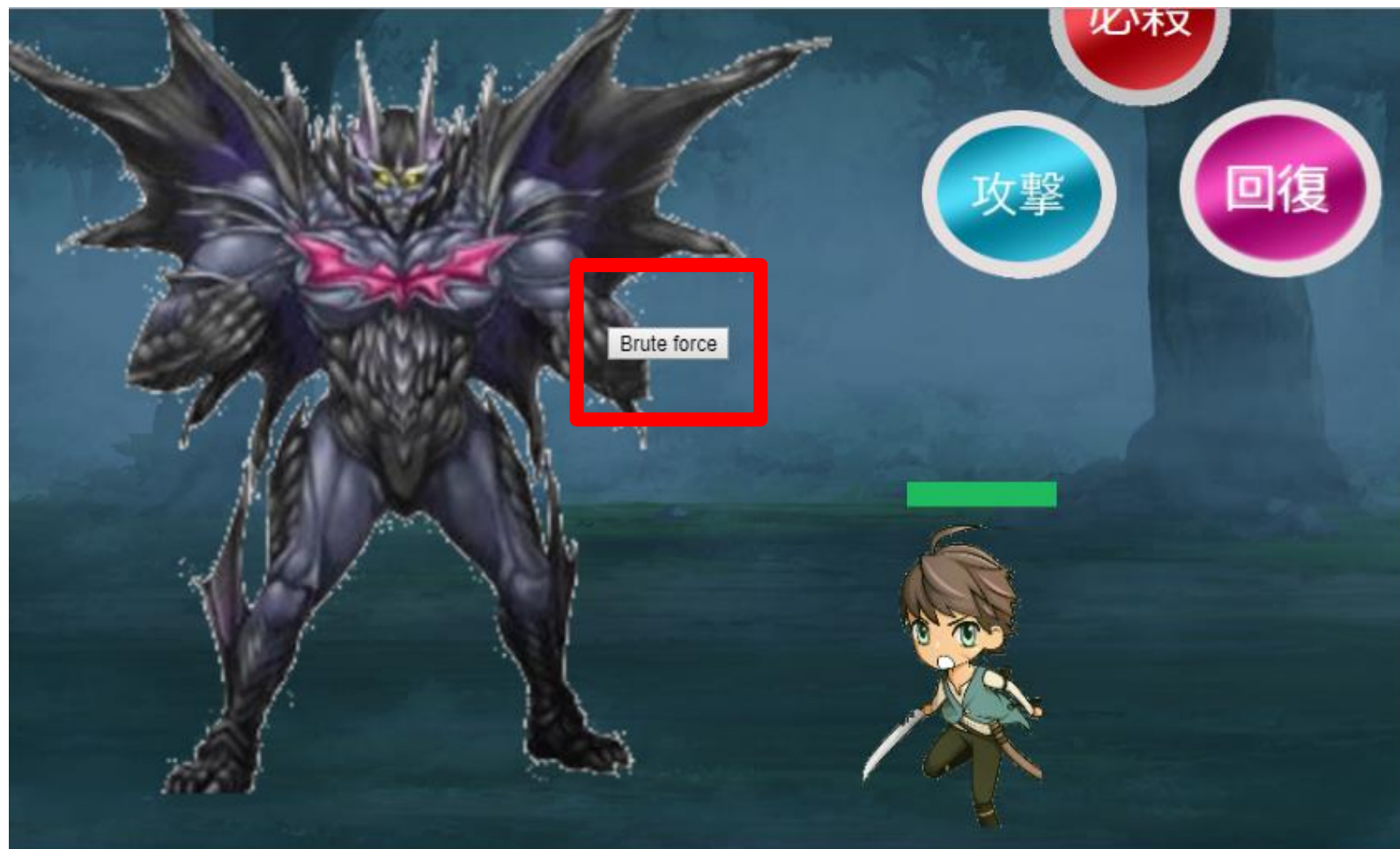
先ほどバトル画面をデベロッパーツールでクリックしたときに水色になったところの下に黄緑で書かれているところがあったと思います

FLAG2を表示させよう



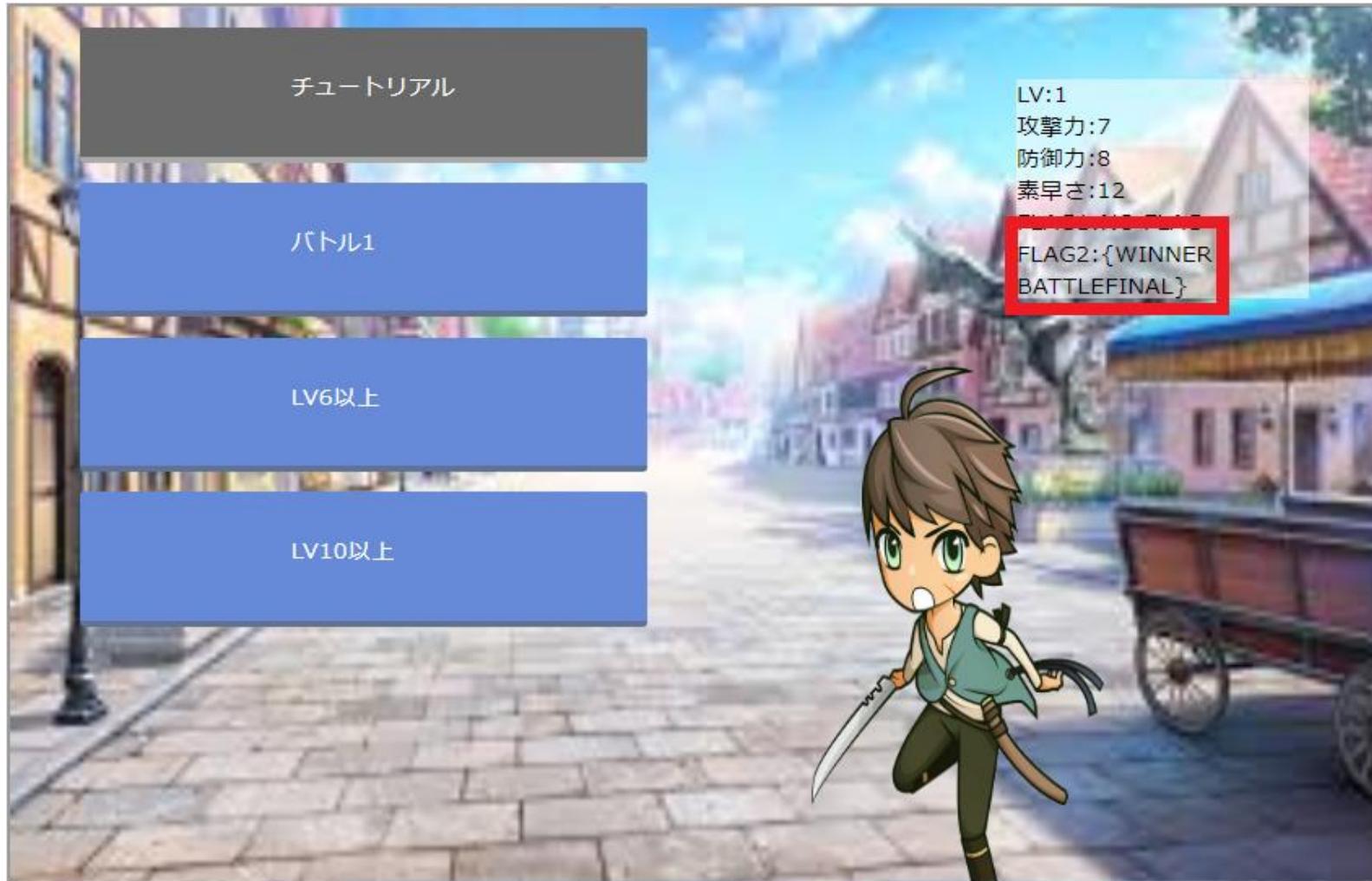
実はこれが隠しボタンで戦わずして勝つことができます
この部分を右クリックし、「Edit as HTML」を押して
＜！－－と－－＞を消してみよう。

FLAG2を表示させよう



すると、ボタンが現れます！ 押してみると...

FLAG2を表示させよう



FLAG2が手に入ります

別解（発展）

別解（発展）の目的

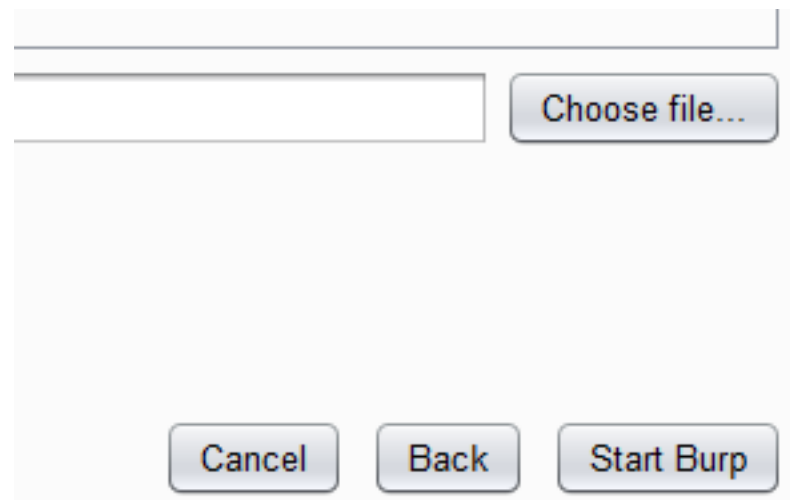
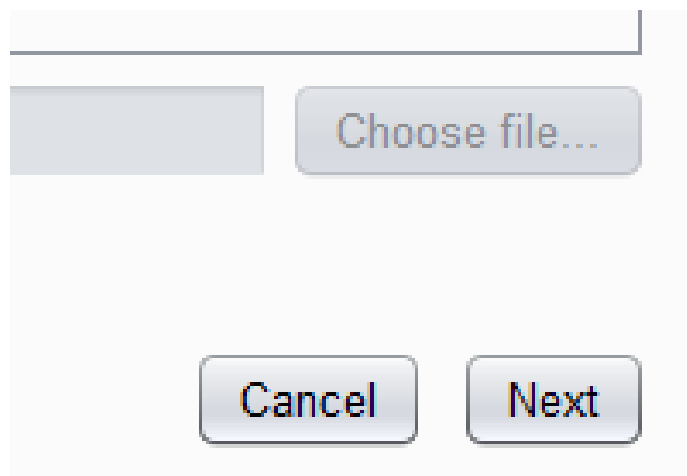
- ▶ この問題を通して、各処理に通信が送られていることを学びます。
- ▶ ツールを使うことによって通信を止めて、**内容を書き換えることと一度の通信で大量の通信内容を送ることができる**ことを理解します。
- ▶ ※発展問題はBrup suiteを使わないと解けません！

Brup suiteのダウンロードは下記から
お願い致します。

↓ここからダウンロード↓

<https://portswigger.net/burp/communitydownload>

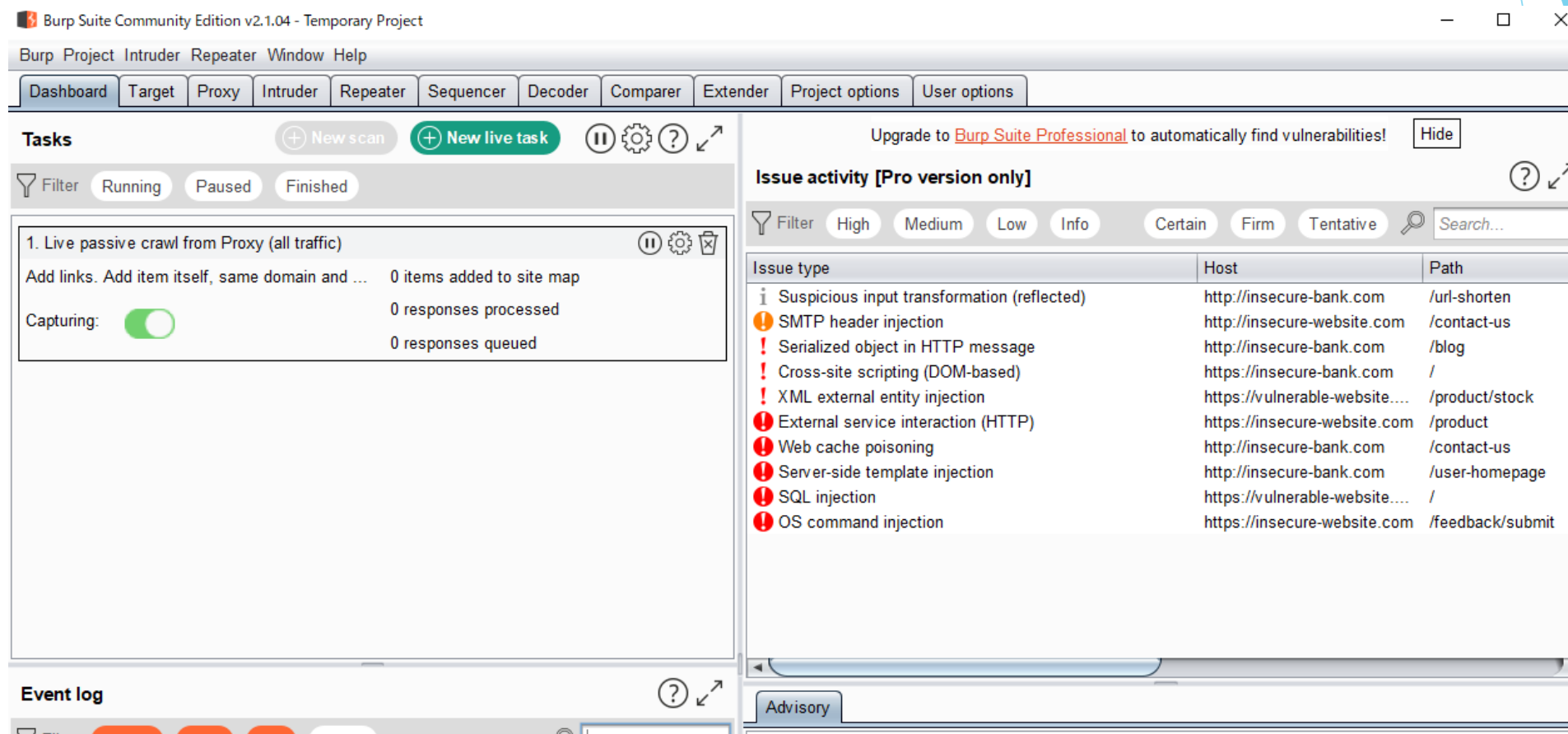
Brupの使い方（今回使う機能の説明）



Brupを開いたら画面右下にある「Next」を押してください

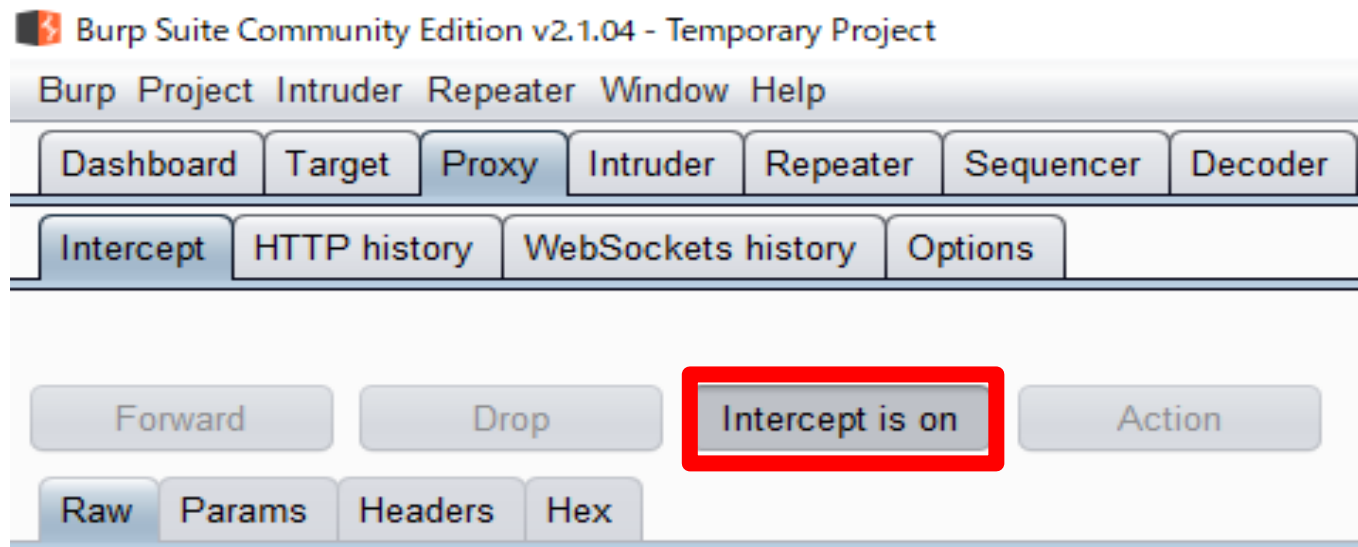
その次に、画面右下にある「Start Burp」を押してください

Brupの使い方（今回使う機能の説明）



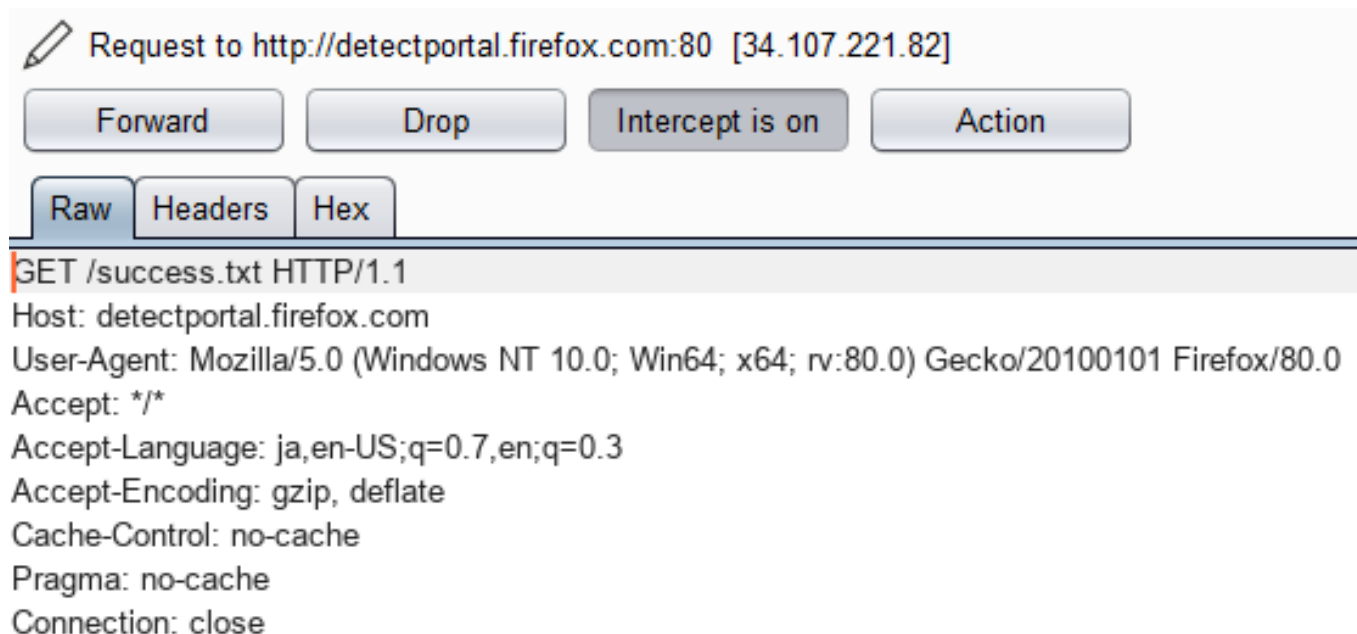
すると、Brupが起動します。

Proxyの説明



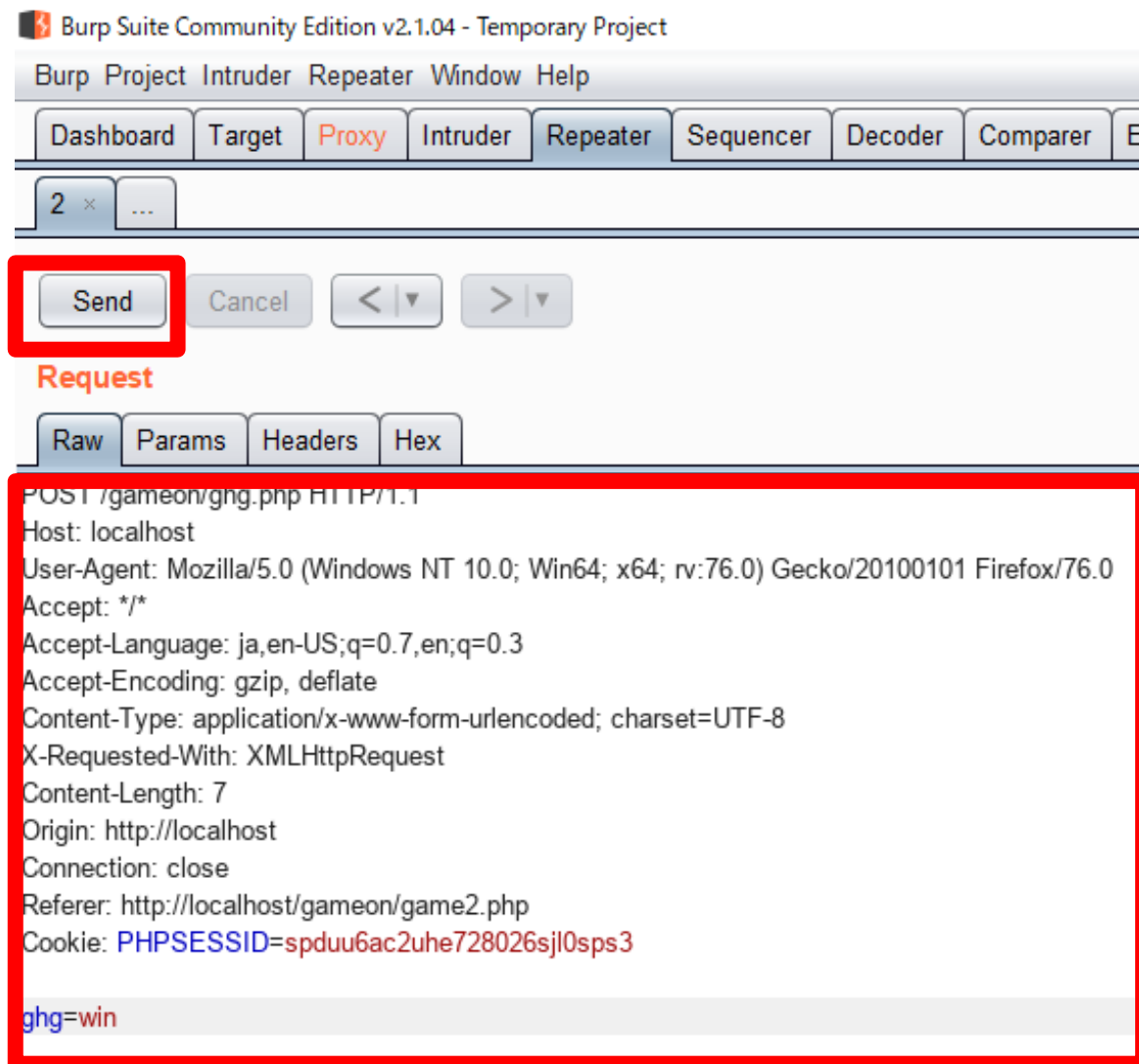
「intercept is on/off」は意図的に通信を止めることができる機能です

Proxyの説明



通信を止めると通信の内容が表示される

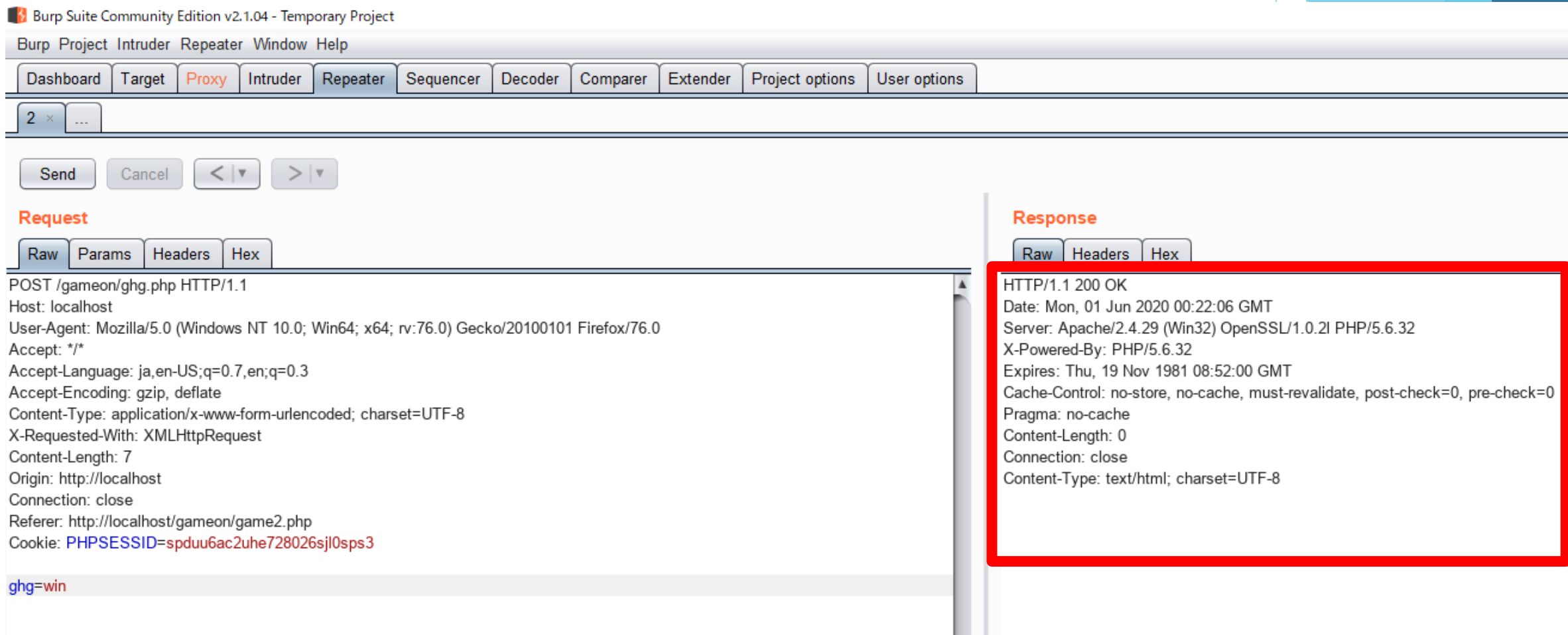
Repeaterの説明



1. 先ほどの通信内容をコピーします。

2. 「Send」を押すことで内容が送られる。

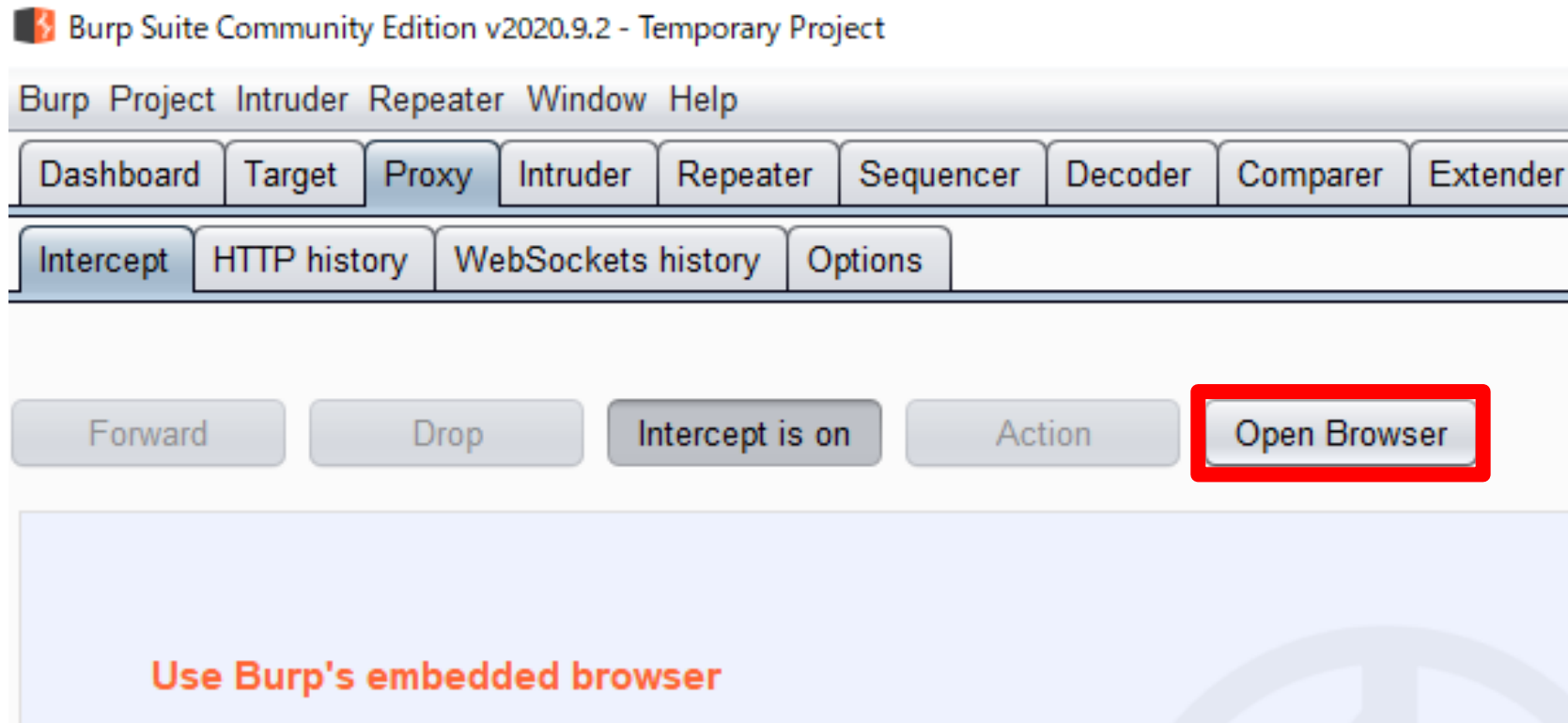
Repeaterの説明



内容が送られると右側にこのような画面が表示されます

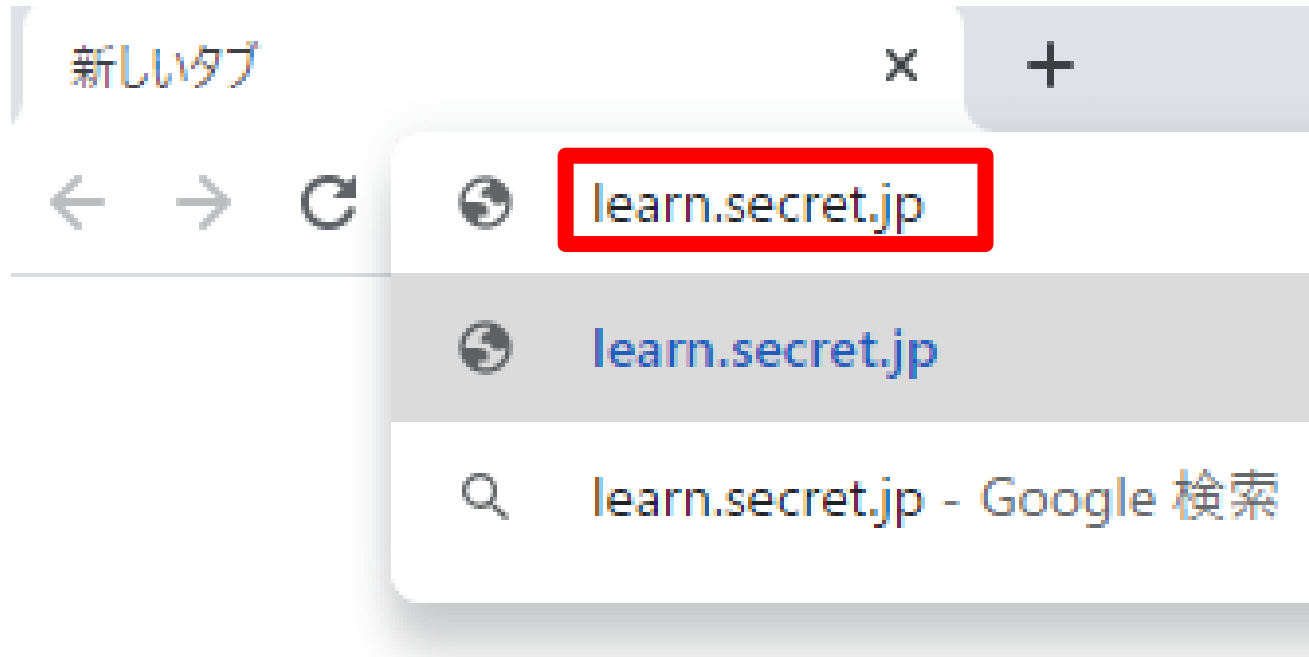
それでは問題解説に移ります

その前に . . .



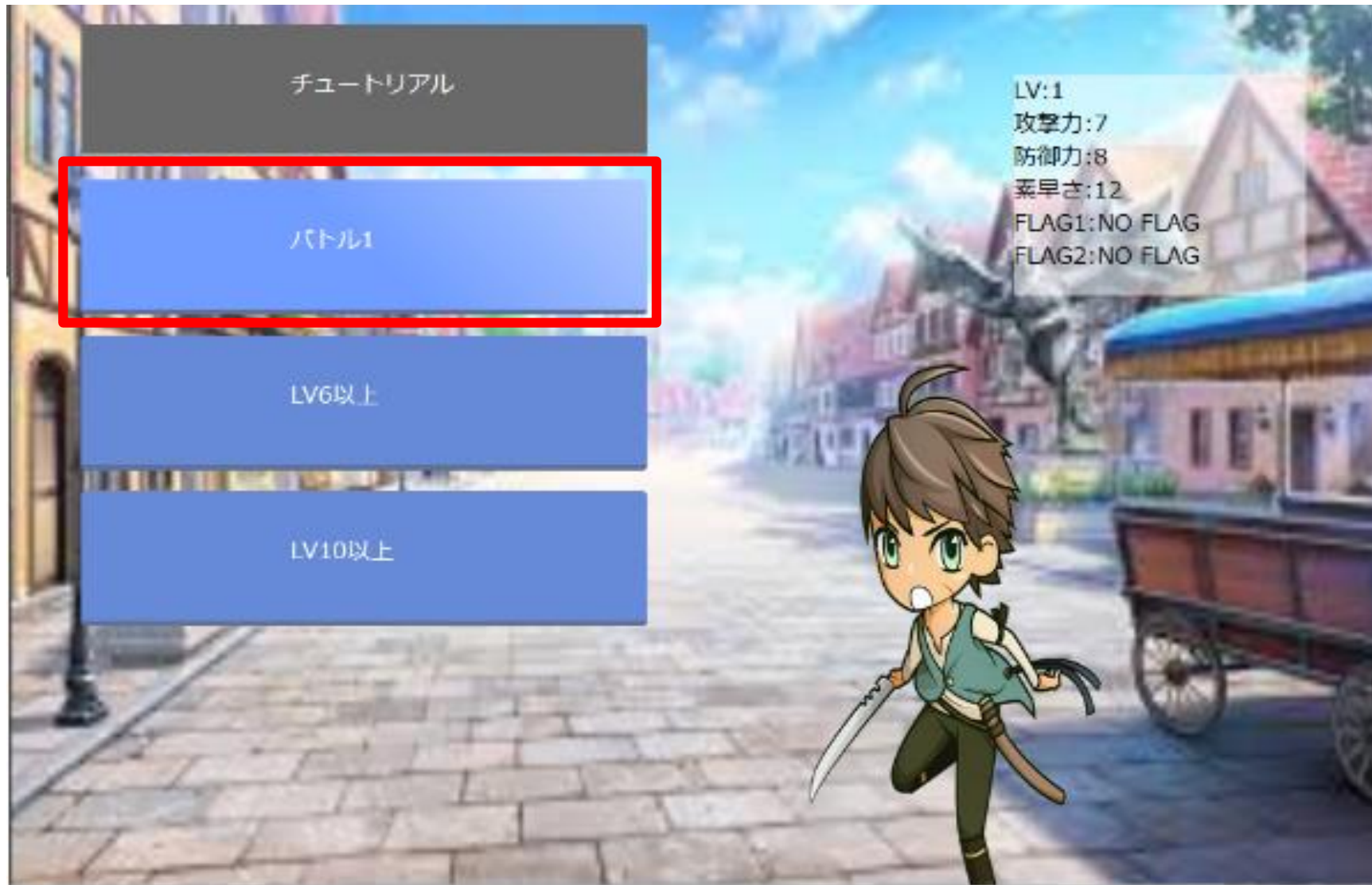
「Open Browser」を押すとchromeが起動します。起動したらRPGのチュートリアルまで進めてください。

その前に . . .

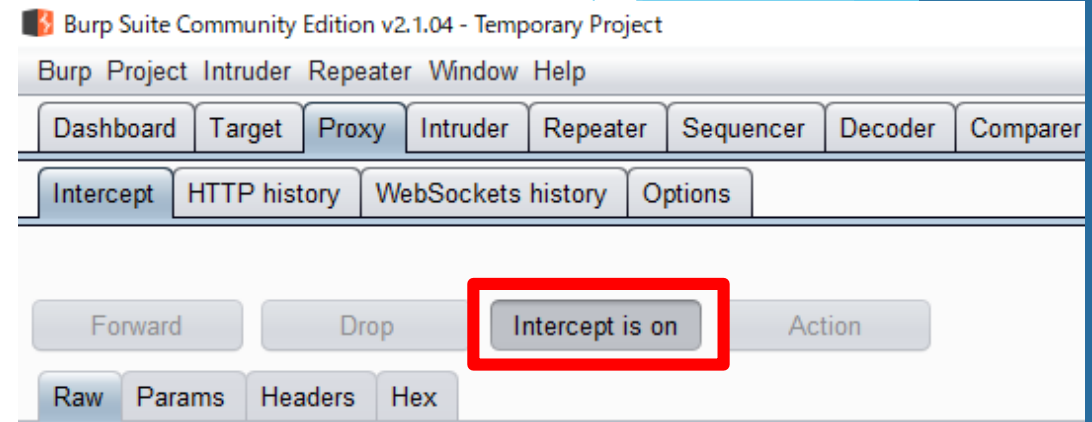


起動したら「learn.secret.jp」と検索し、RPGをチュートリアルまで進めてください。

LV10にしよう！（FLAG1）



LV10にしよう！（FLAG1）



Intercept is offと書いてあるのを押して、**OFFをON**に切り替えよう！

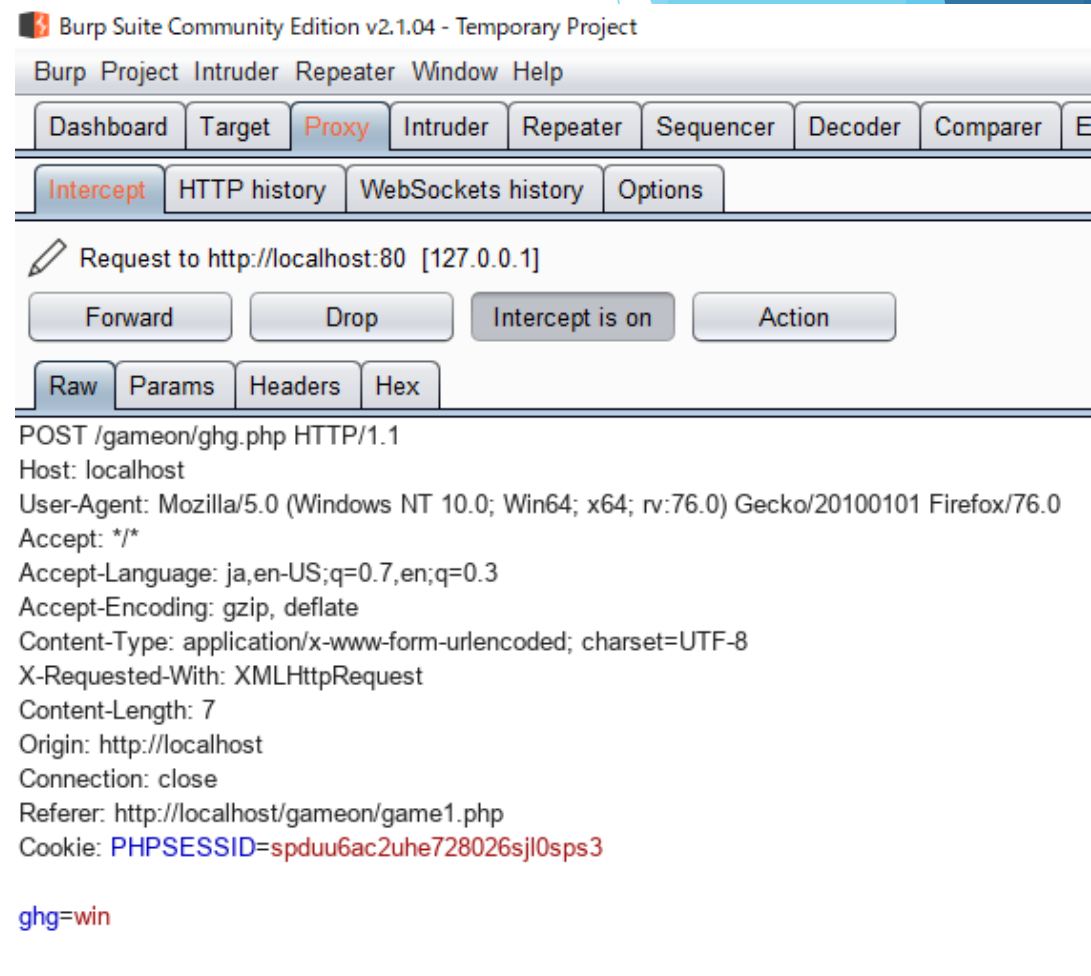
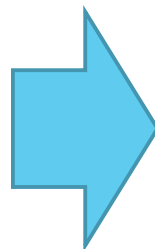
この手順が終わったら敵を倒そう！

LV10にしよう！ (FLAG1)



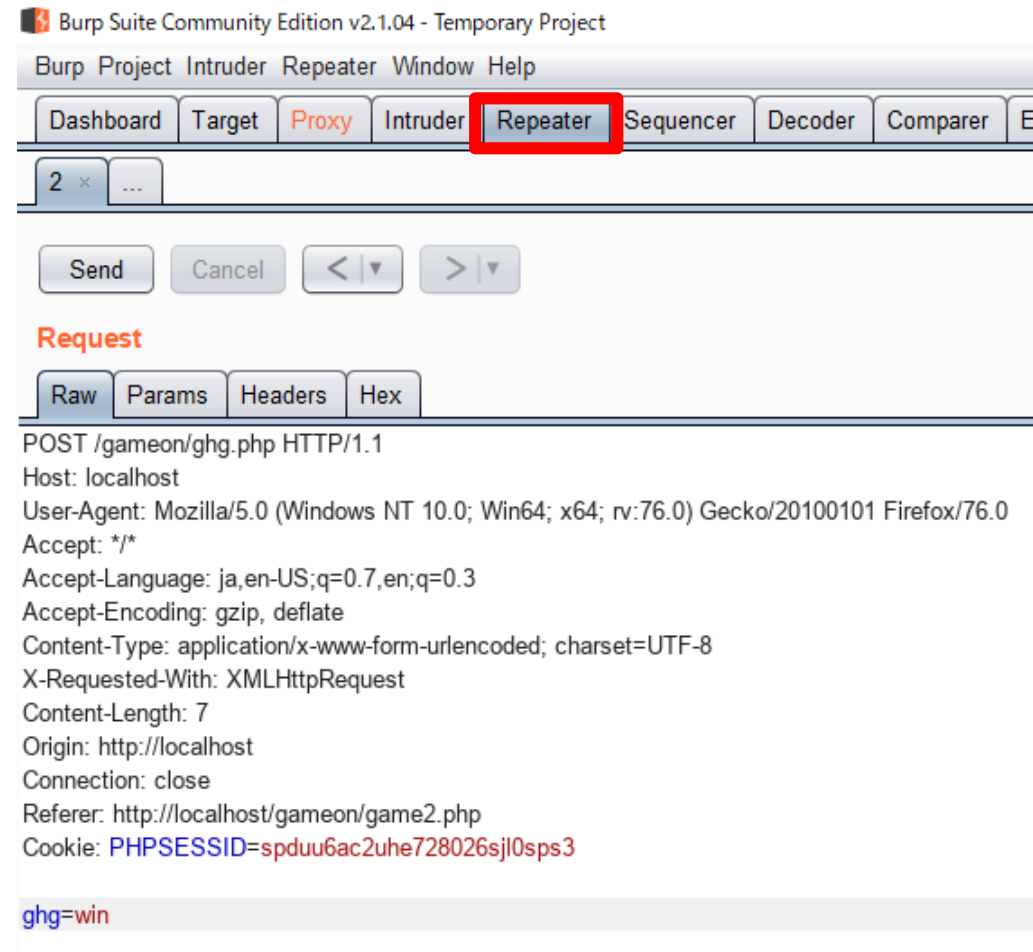
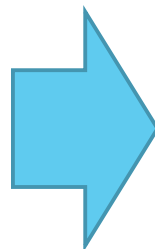
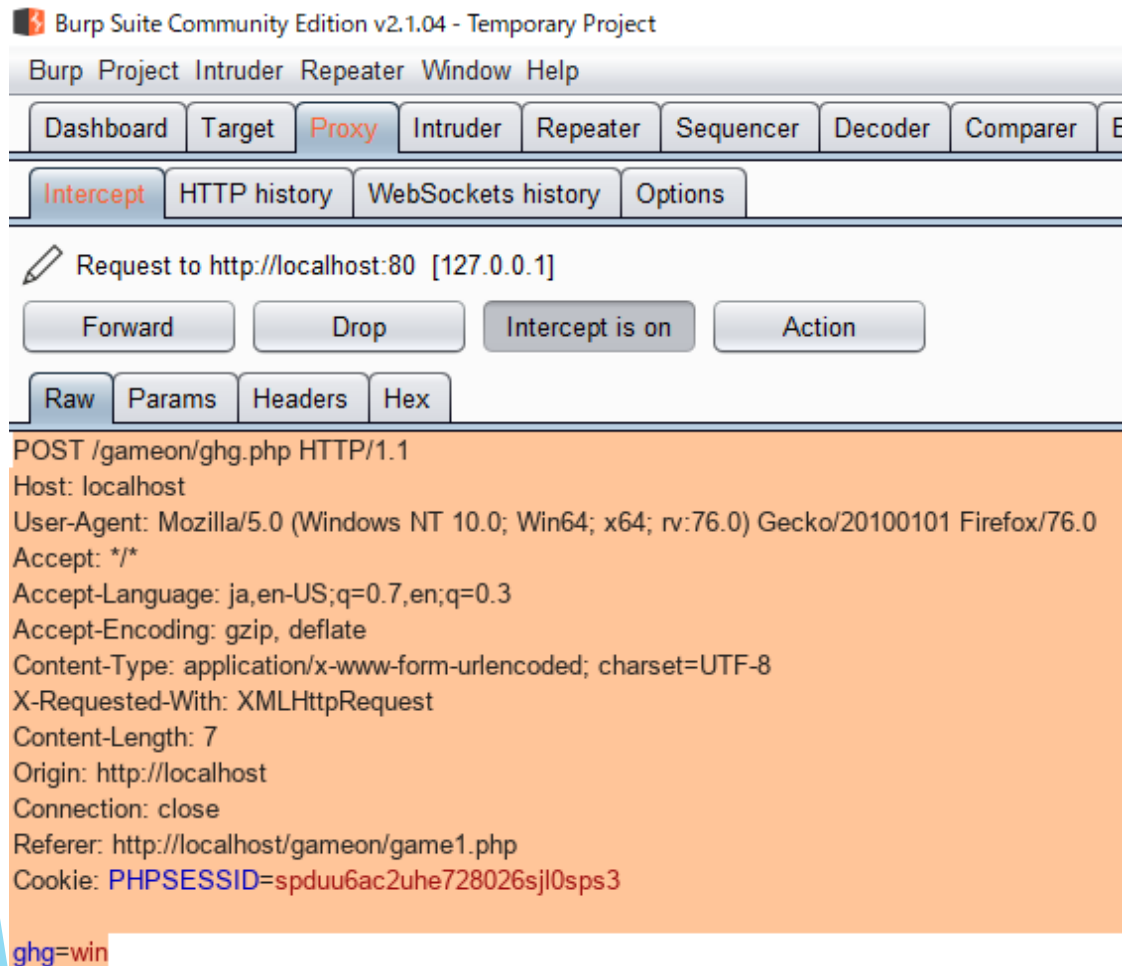
WIN

この画面でクリックしても
動かず止まる！
(通信が止まる。)



なんか入ってる！
これは敵を倒した証拠！

LV10にしよう！ (FLAG1)



この内容を **C t r l + C** でコピーしよう！

C t r l + V で内容を貼り付ける！

LV10にしよう！ (FLAG1)

Burp Suite Community Edition v2.1.04 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

2 × ...

Send Cancel < >

Request

Raw Params Headers Hex

POST /gameon/ghg.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:76.0) Gecko/20100101 Firefox/76.0
Accept: */*
Accept-Language: ja,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 7
Origin: http://localhost
Connection: close
Referer: http://localhost/gameon/game2.php
Cookie: PHPSESSID=spduu6ac2uhe728026sjl0sps3

ghg=win

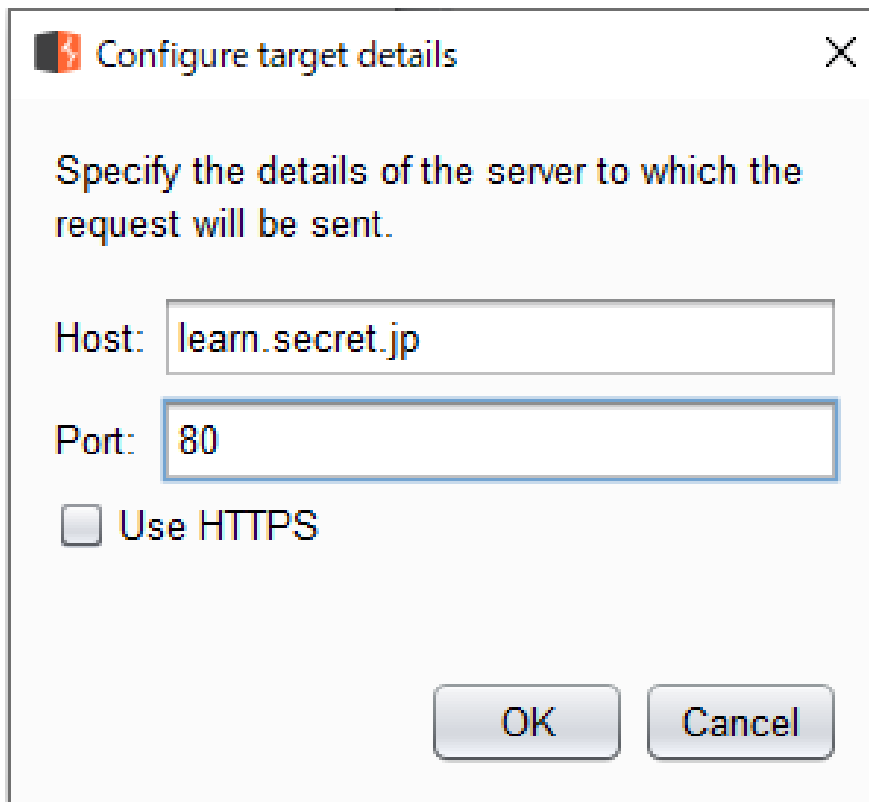
Response

Raw Headers Hex

HTTP/1.1 200 OK
Date: Mon, 01 Jun 2020 00:22:06 GMT
Server: Apache/2.4.29 (Win32) OpenSSL/1.0.2l PHP/5.6.32
X-Powered-By: PHP/5.6.32
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8

Sandを押すと押した数だけ経験値がもらえる！

LV10にしよう！ (FLAG1)



Configure target details

Specify the details of the server to which the request will be sent.

Host: learn.secret.jp

Port: 80

☐ Use HTTPS

OK Cancel

× Sandを押したときこの画面が出てきたら・・・

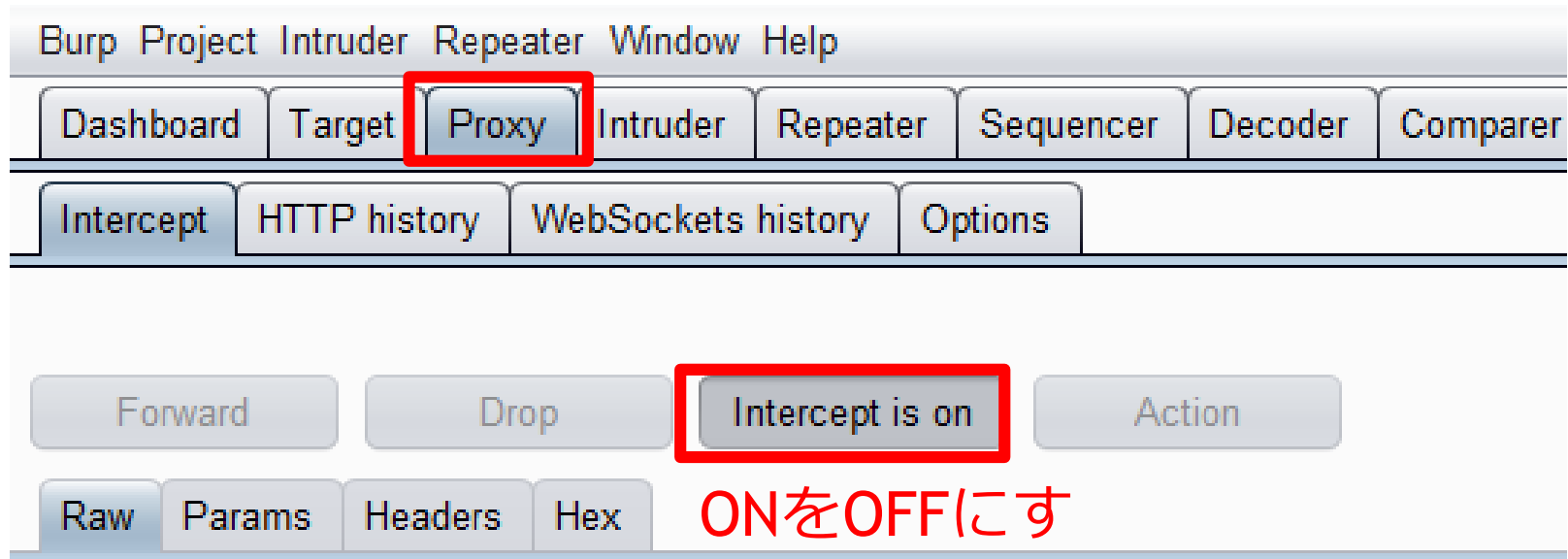
Host:learn.secret.jp

Port:80

と入力してOKを押そう！

LV10にしよう！（FLAG1）

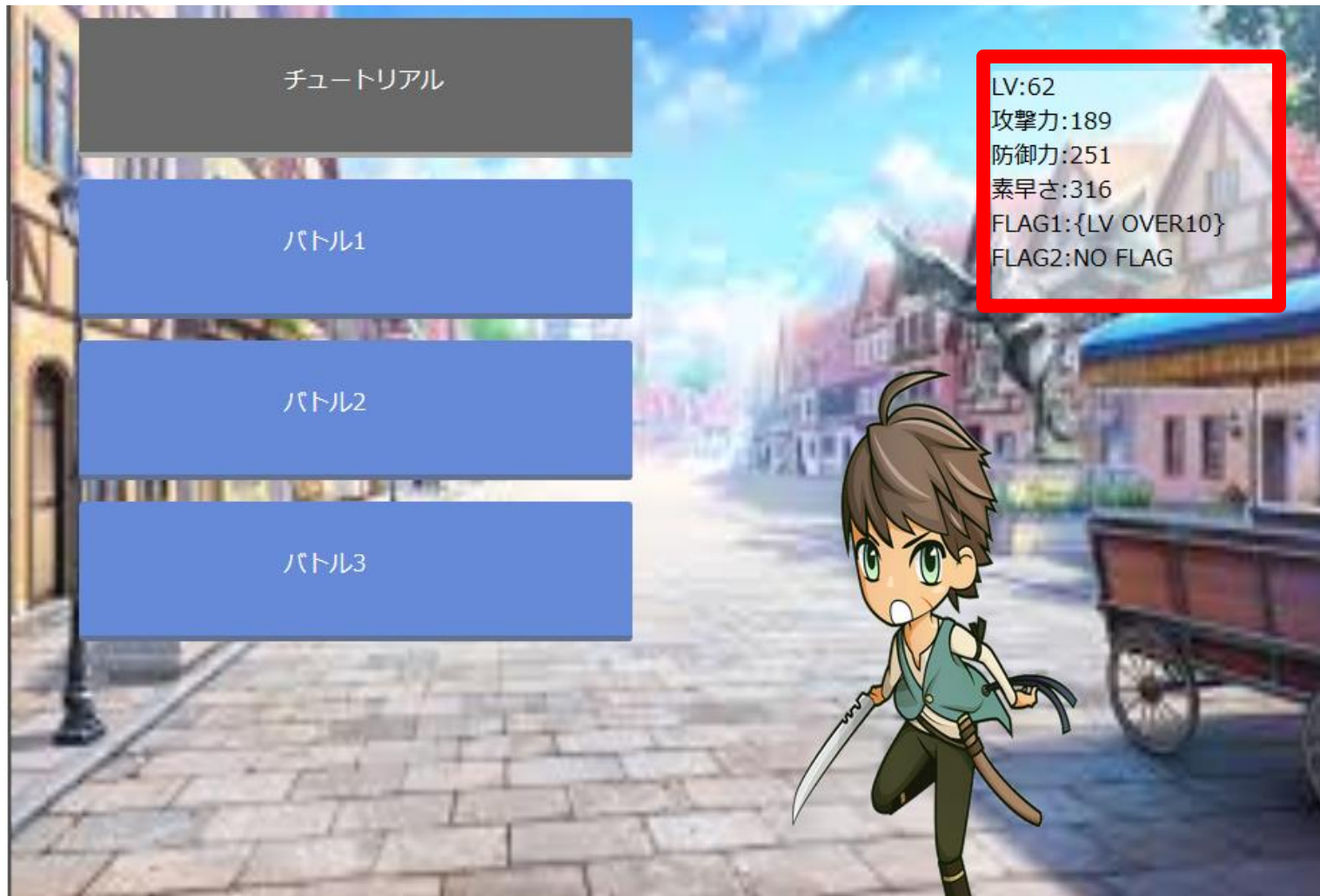
Burp Suite Community Edition v2.1.04 - Temporary Project



ONをOFFにする！

通信が始まる！

LV10にしよう！（FLAG1）



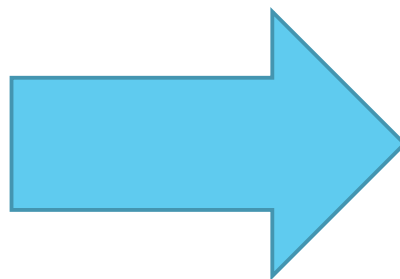
レベルが上がってFLAG1にLV10達成のメッセージが出てくる！

何が起こったのか（説明）

Before



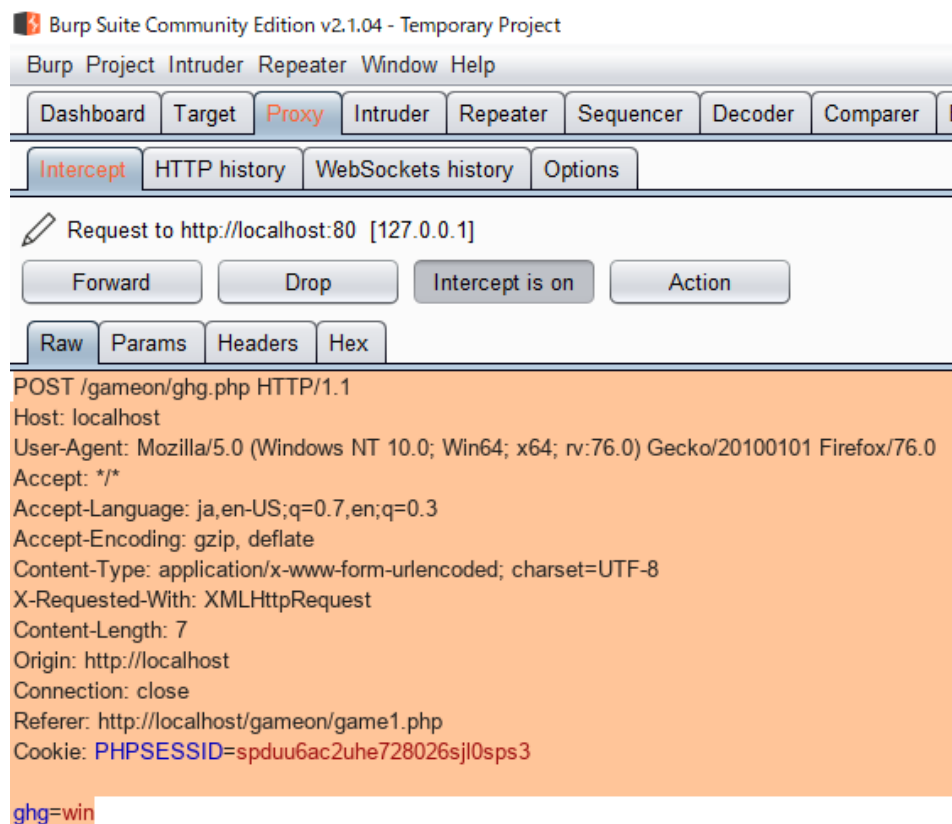
一回の戦いで



After



何が起こったのか（説明）



= 敵を一回倒した処理

何が起こったのか（説明）

Burp Suite Community Edition v2.1.04 - Temporary Project

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

2 x ...

Send Cancel < >

Request

Raw Params Headers Hex

POST /gameon/ghg.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:76.0) Gecko/20100101 Firefox/76.0
Accept: */*
Accept-Language: ja,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 7
Origin: http://localhost
Connection: close
Referer: http://localhost/gameon/game2.php
Cookie: PHPSESSID=spduu6ac2uhe728026sjl0sps3

ghg=win

Response

Raw Headers Hex

HTTP/1.1 200 OK
Date: Mon, 01 Jun 2020 00:22:06 GMT
Server: Apache/2.4.29 (Win32) OpenSSL/1.0.2l PHP/5.6.32
X-Powered-By: PHP/5.6.32
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8

クリックすると敵が倒されていた！（押す度に経験値がもらえていた！）

簡単に言うと・・・

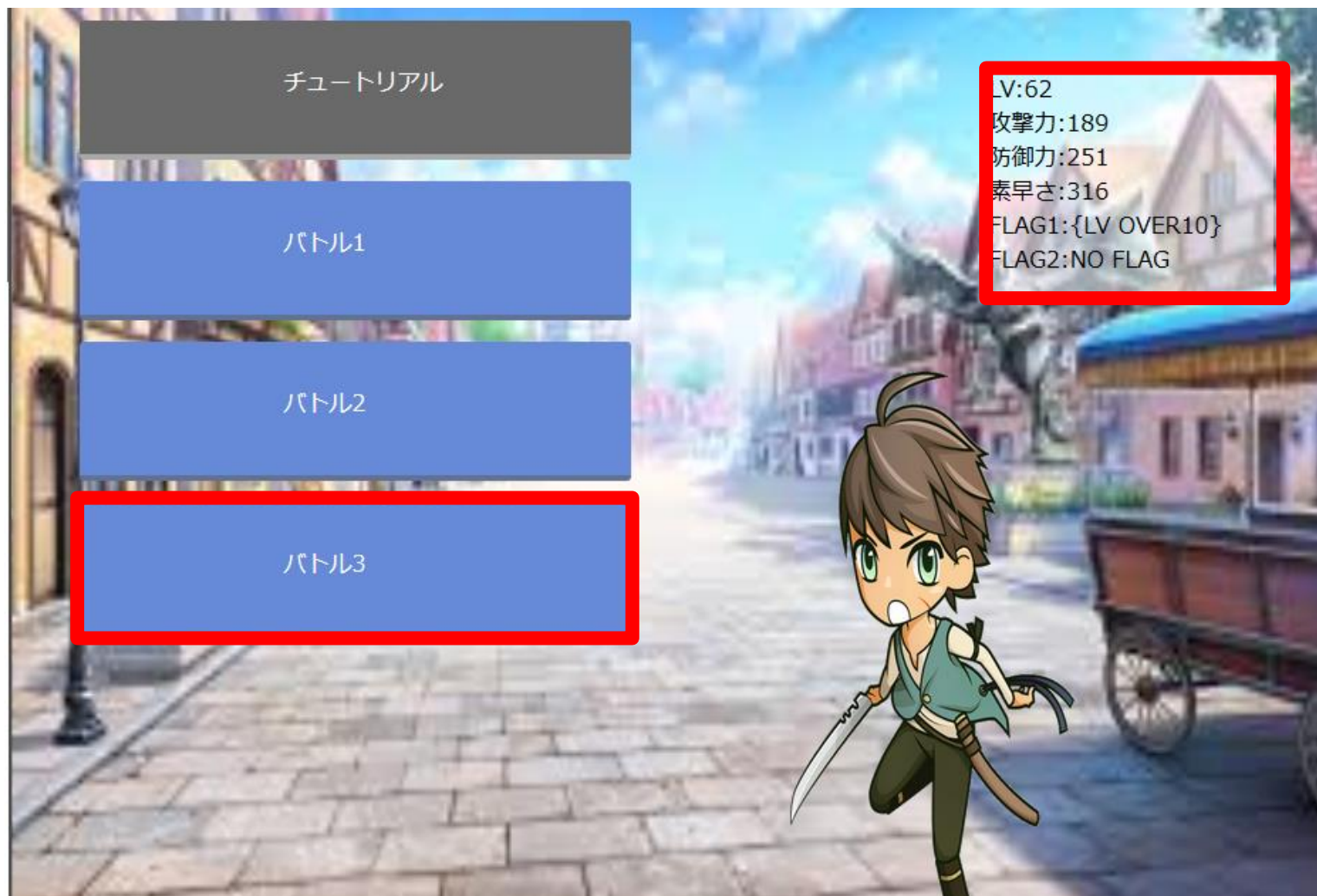


SANTENDO Scratch（経験値）

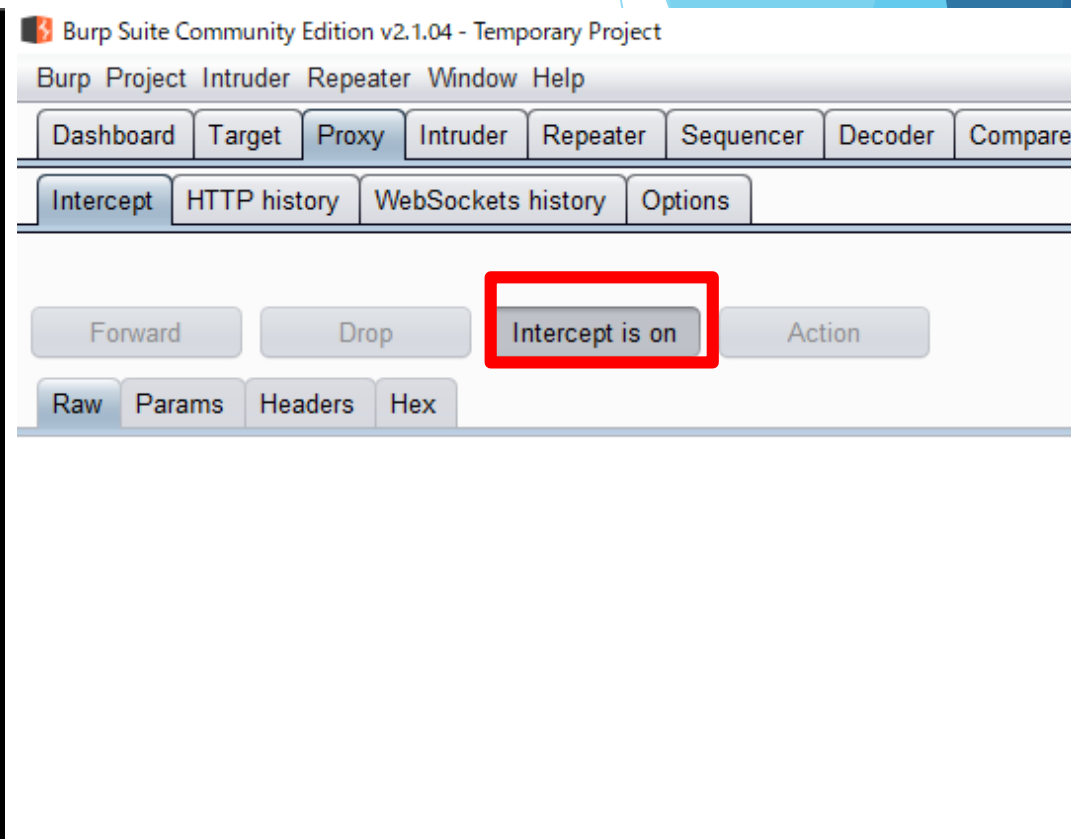
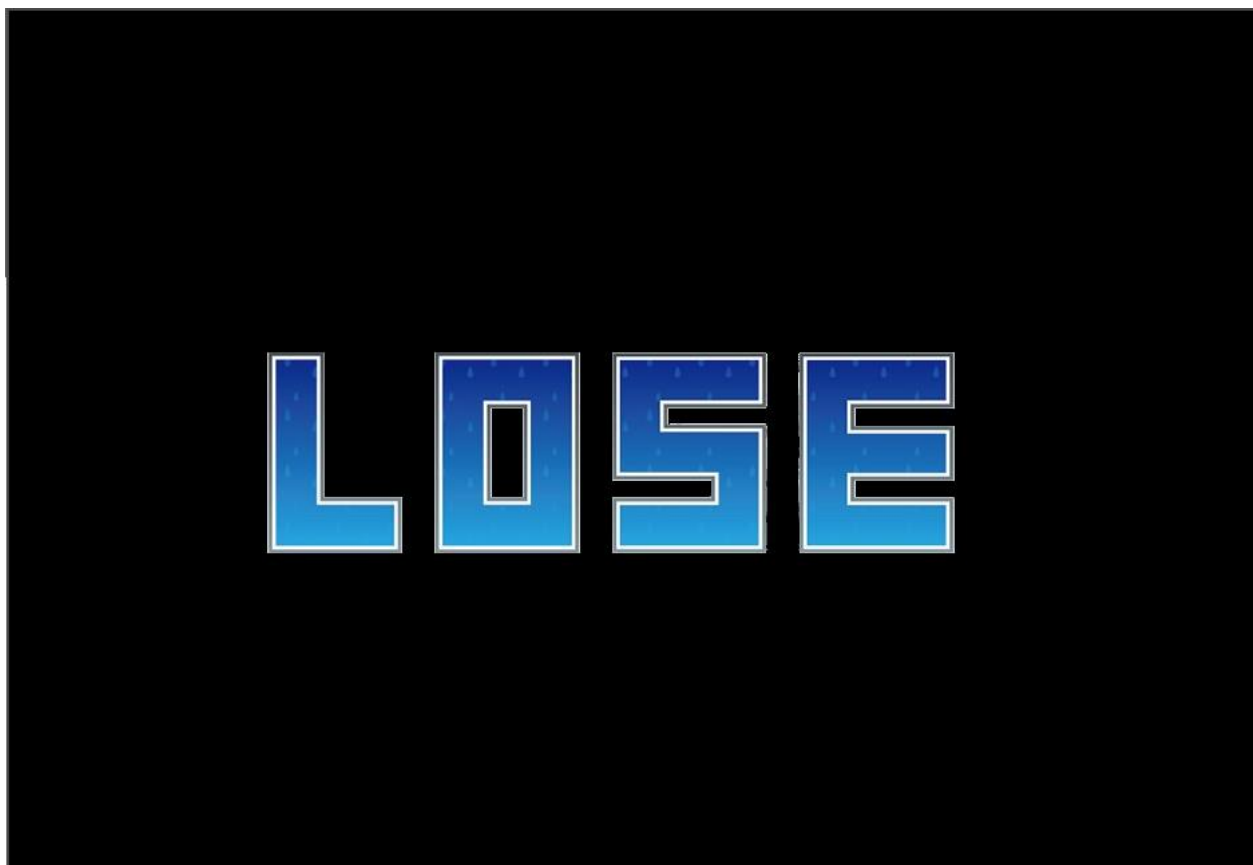
× クリックした回数 =



最終ボスを倒そう！（FLAG2）



最終ボスを倒そう！（FLAG2）



最終ボスとの戦いで負けてしまったときLOSEと出てきたときにintercept is off から onにします。

最終ボスを倒そう！（FLAG2）

```
Raw Params Headers Hex
Pretty Raw \n Actions ▼
1 POST /gameon/ghgfl.php HTTP/1.1
2 Host: learn.secret.jp
3 Content-Length: 8
4 Accept: */*
5 X-Requested-With: XMLHttpRequest
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win6
  like Gecko) Chrome/85.0.4183.121 Safari/537.36
7 Content-Type: application/x-www-form-urlencoded
8 Origin: http://learn.secret.jp
9 Referer: http://learn.secret.jp/gameon/game4.p
10 Accept-Encoding: gzip, deflate
11 Accept-Language: ja,en-US;q=0.9,en;q=0.8
12 Cookie: PHPSESSID=2c6ffn3jukorprvjmgcf7s7t6u
13 Connection: close
14
15 ghg=lose
```

すると、負けてしまったときの通信が送られてきます。

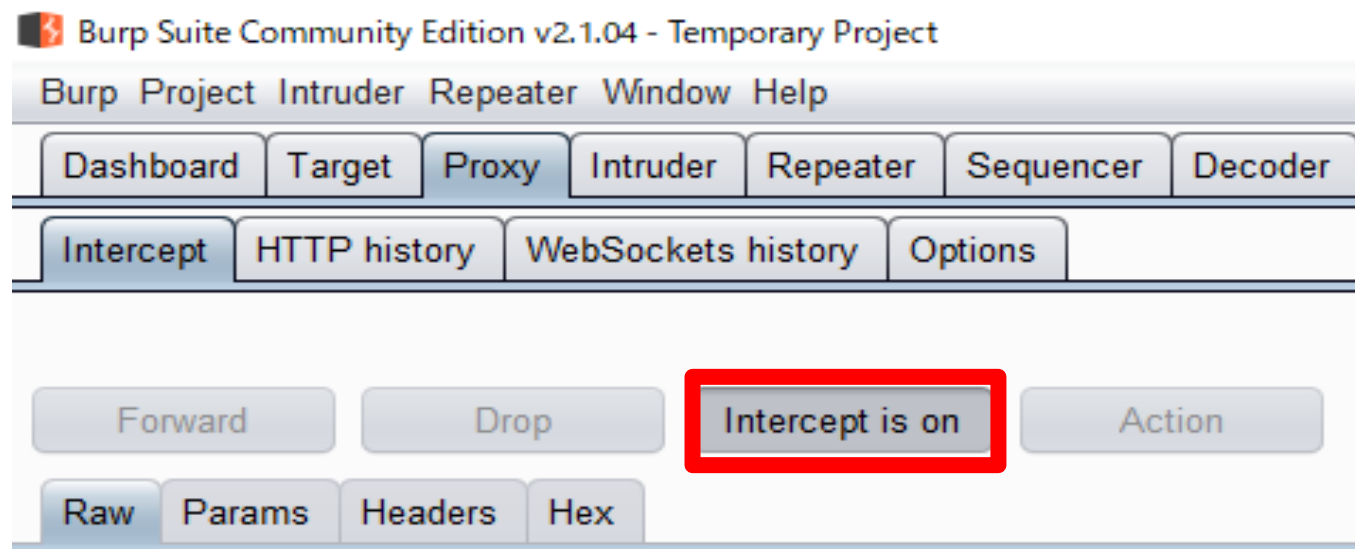
最終ボスを倒そう！（FLAG2）

```
Raw Params Headers Hex
Pretty Raw \n Actions v
1 POST /gameon/ghgfl.php HTTP/1.1
2 Host: learn.secret.jp
3 Content-Length: 8
4 Accept: */*
5 X-Requested-With: XMLHttpRequest
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win6
  like Gecko) Chrome/85.0.4183.121 Safari/537.36
7 Content-Type: application/x-www-form-urlencoded
8 Origin: http://learn.secret.jp
9 Referer: http://learn.secret.jp/gameon/game4.p
10 Accept-Encoding: gzip, deflate
11 Accept-Language: ja,en-US;q=0.9,en;q=0.8
12 Cookie: PHPSESSID=2c6ffn3jukorprvjmgcf7s7t6u
13 Connection: close
14
15 ghg=lose
```

```
Raw Params Headers Hex
Pretty Raw \n Actions v
1 POST /gameon/ghgfl.php HTTP/1.1
2 Host: learn.secret.jp
3 Content-Length: 8
4 Accept: */*
5 X-Requested-With: XMLHttpRequest
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win6
  like Gecko) Chrome/85.0.4183.121 Safari/537.36
7 Content-Type: application/x-www-form-urlencoded
8 Origin: http://learn.secret.jp
9 Referer: http://learn.secret.jp/gameon/game4.p
10 Accept-Encoding: gzip, deflate
11 Accept-Language: ja,en-US;q=0.9,en;q=0.8
12 Cookie: PHPSESSID=2c6ffn3jukorprvjmgcf7s7t6u
13 Connection: close
14
15 ghg=win
```

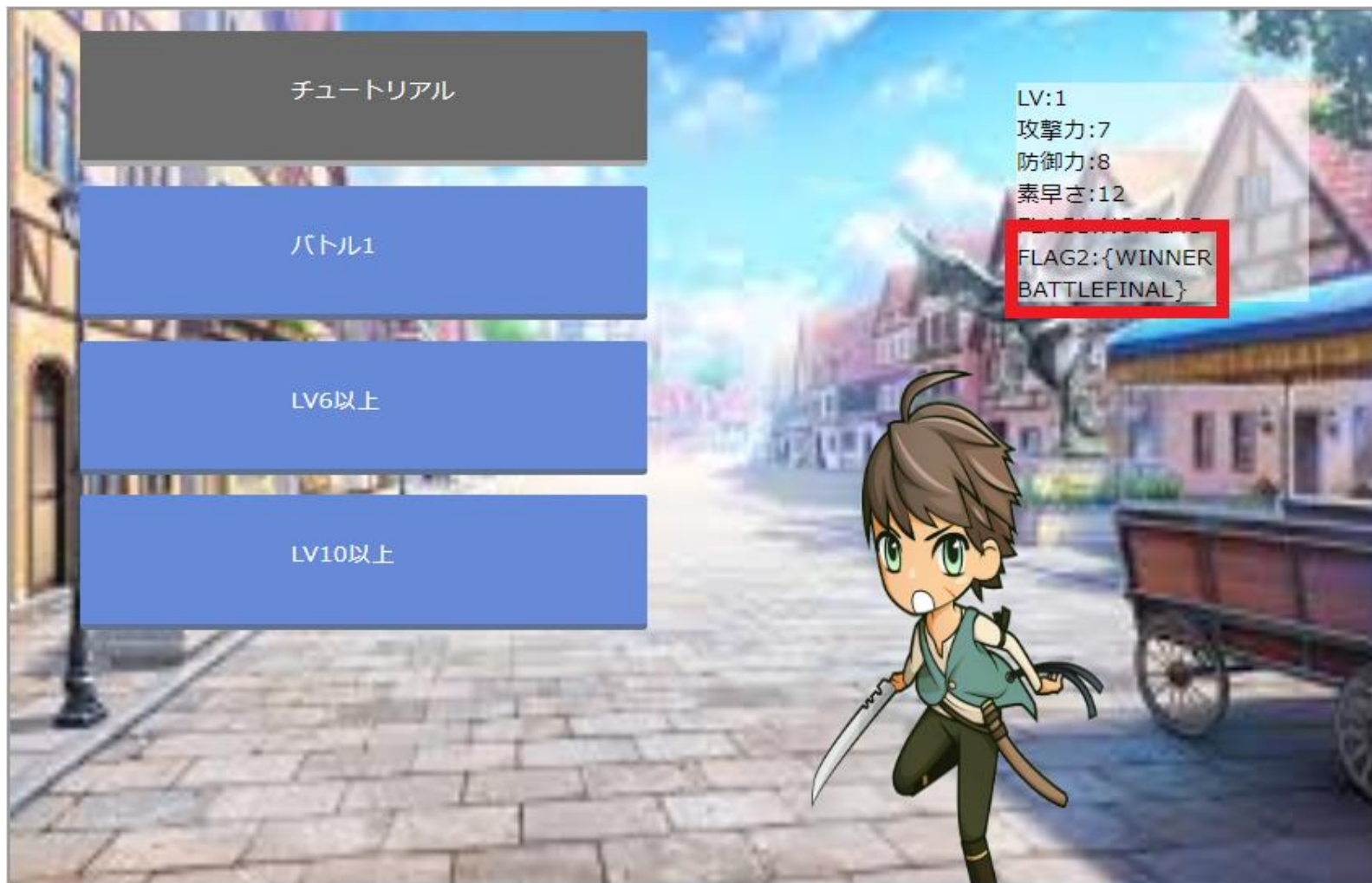
どうしても勝ちたいので一番下のloseをwinに書き換えてしまいましょう。

最終ボスを倒そう！（FLAG2）



書き換えたらintercept is on から off にします。

最終ボスを倒そう！（FLAG2）



すると、FLAG2が手に入ります