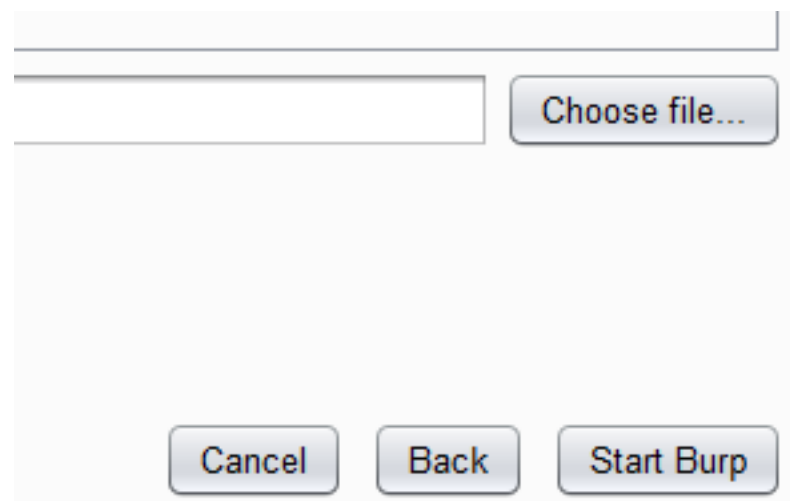
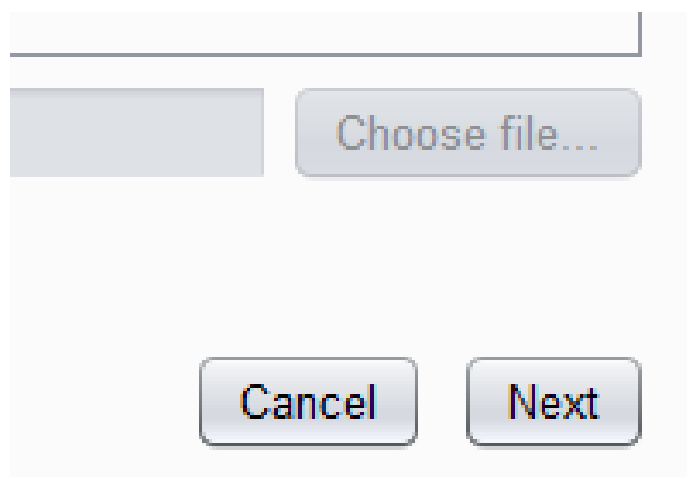


※この問題は
Burp suiteを使わないと解けません！

↓ここからダウンロード↓

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

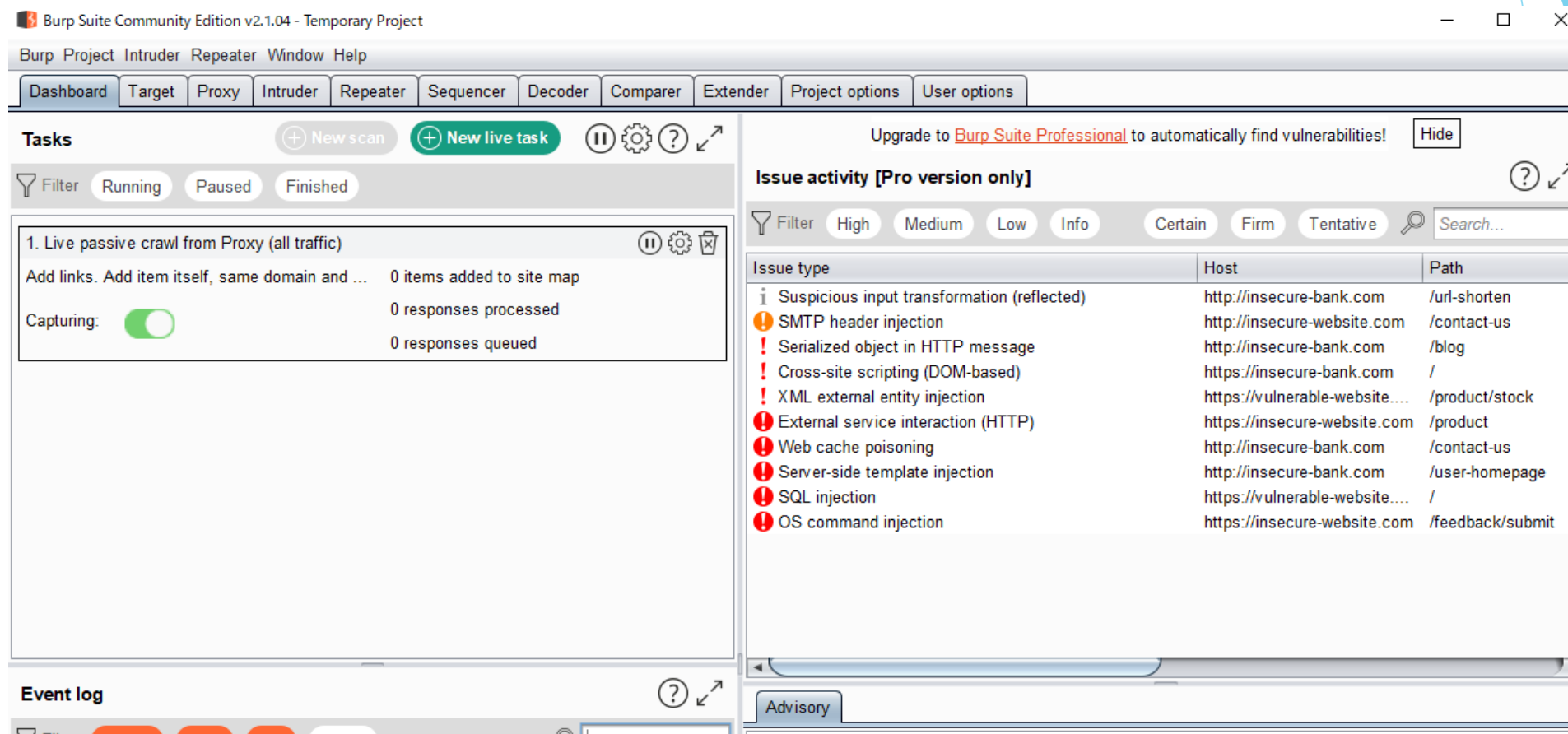
Brupの使い方（今回使う機能の説明）



Brupを開いたら画面右下にある「Next」を押してください

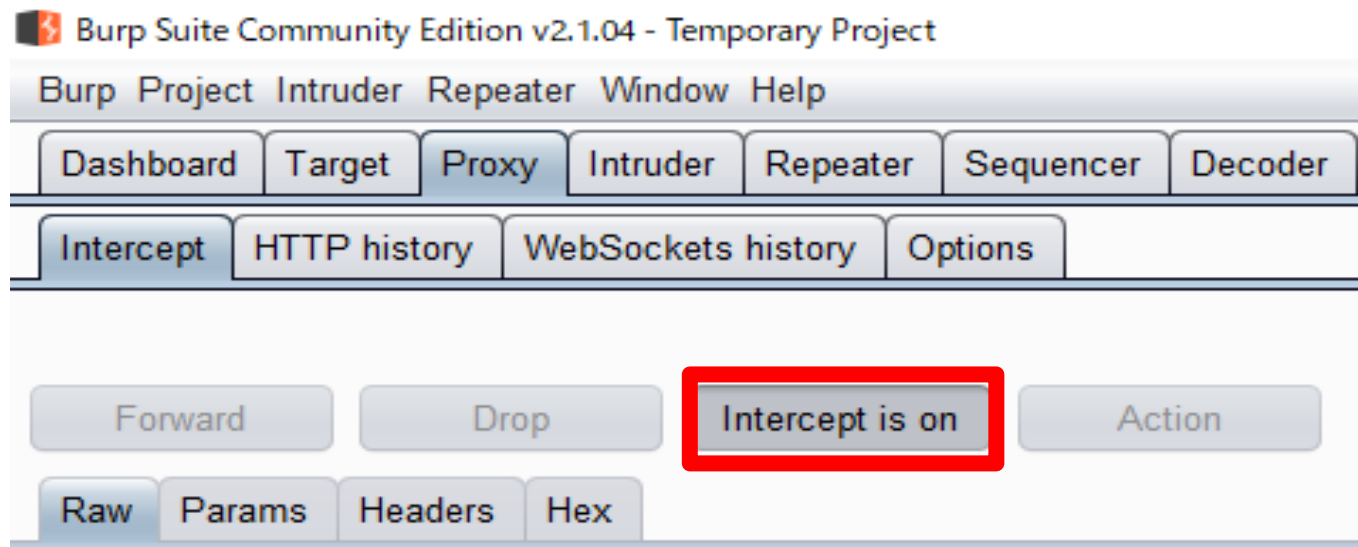
その次に、画面右下にある「Start Burp」を押してください

Brupの使い方（今回使う機能の説明）



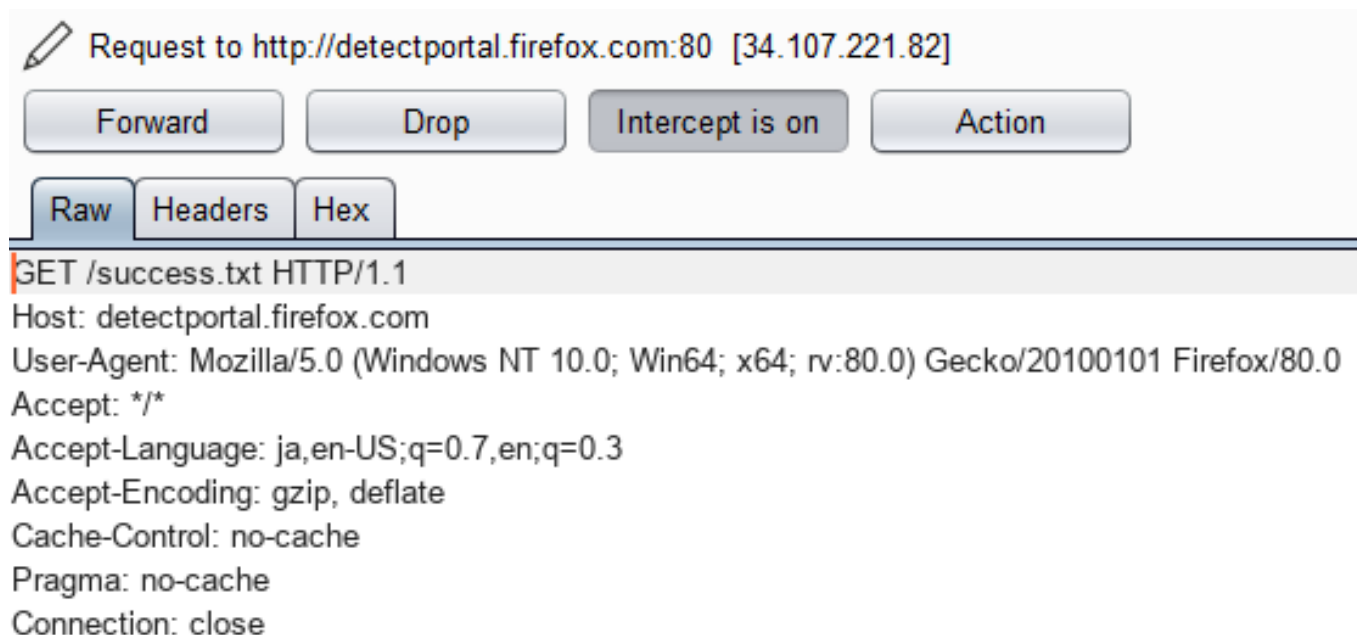
すると、Brupが起動します。

Proxyの説明



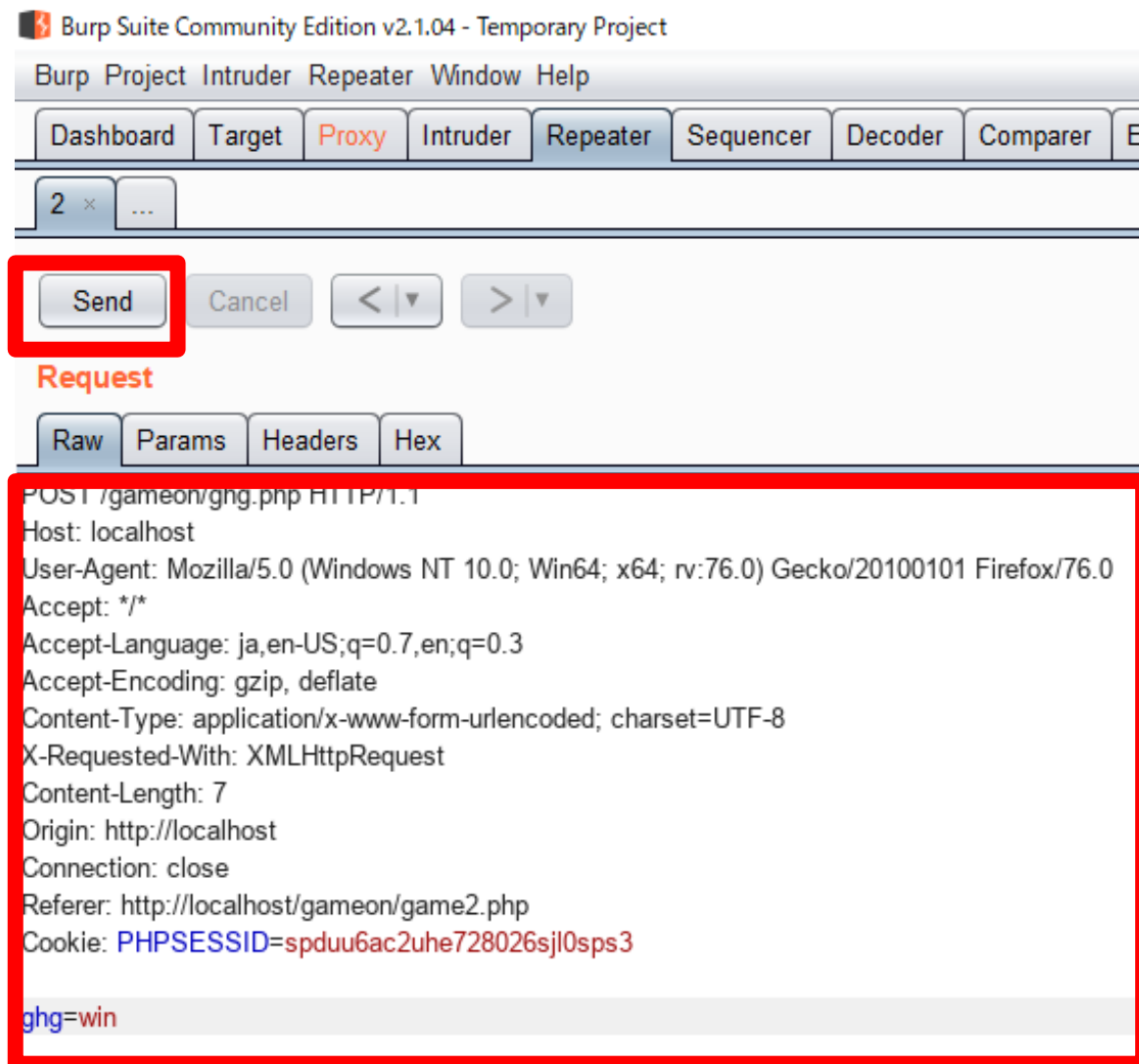
「intercept is on/off」は意図的に通信を止めることができる機能です

Proxyの説明



通信を止めると通信の内容が表示される

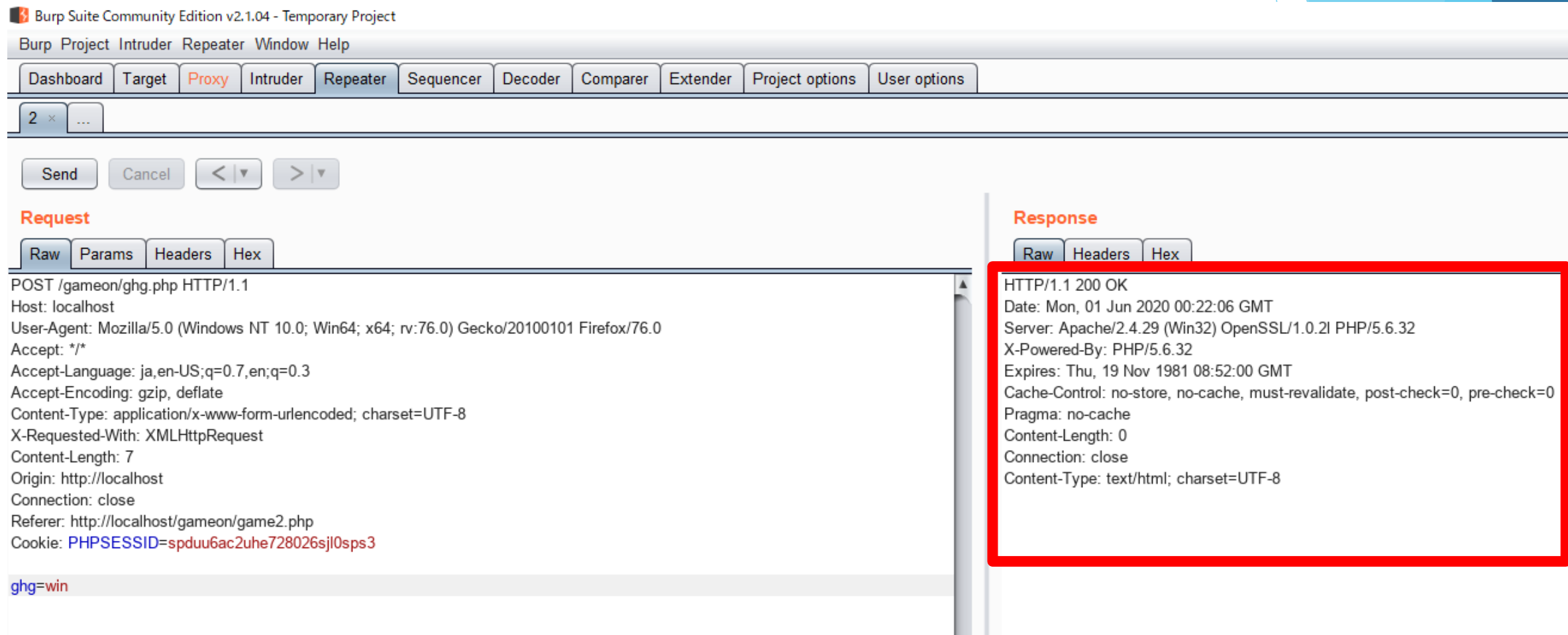
Repeaterの説明



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。

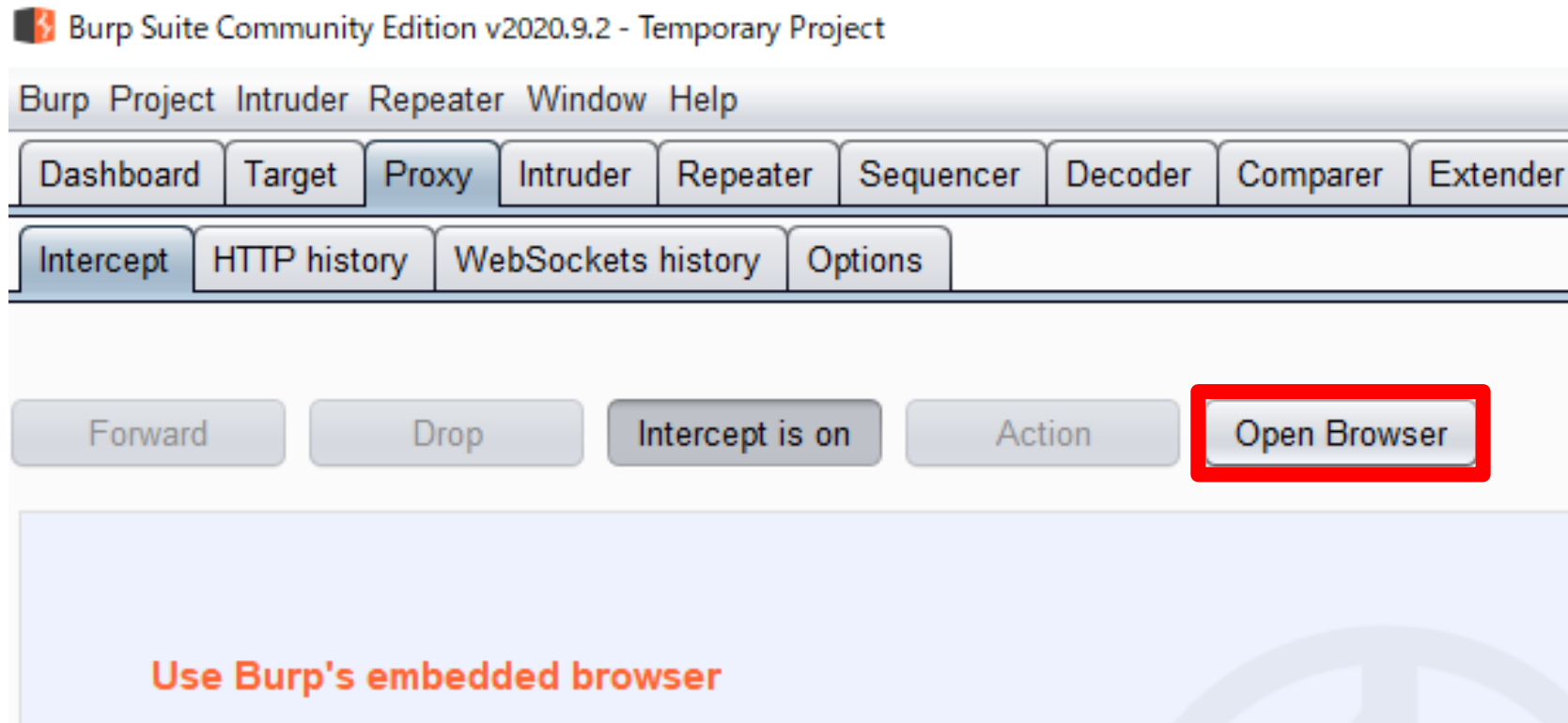
Repeaterの説明



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

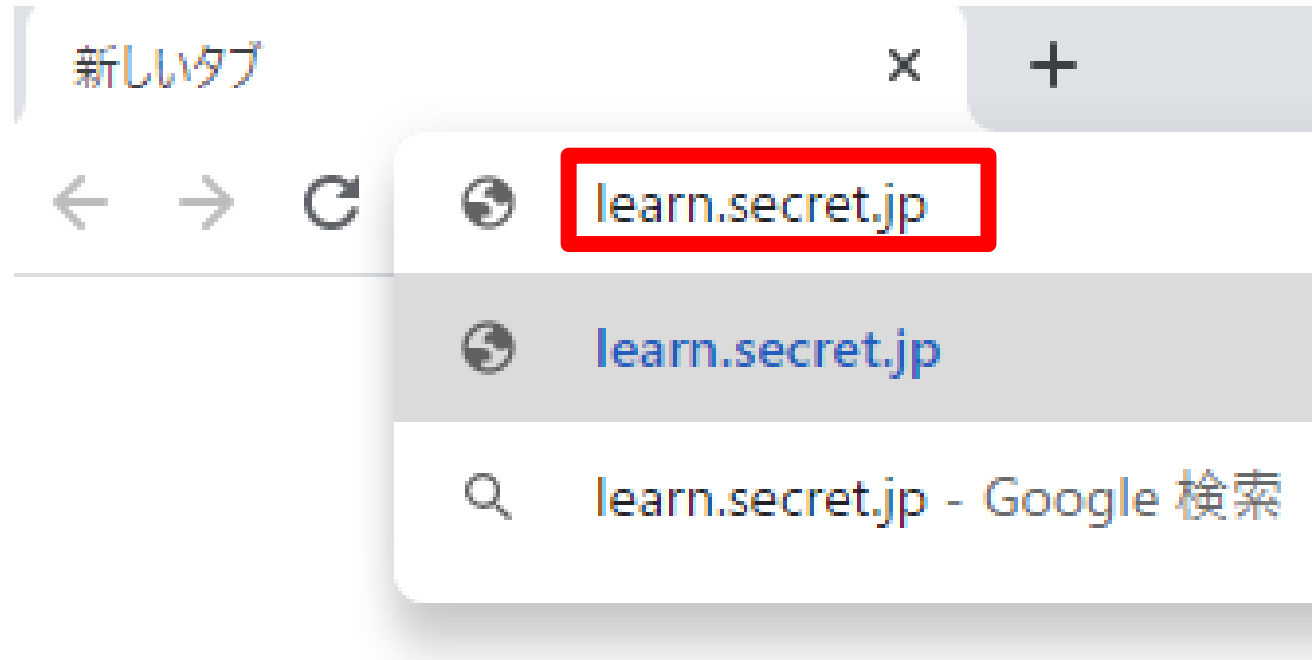
それでは問題解説に移ります

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 . . .

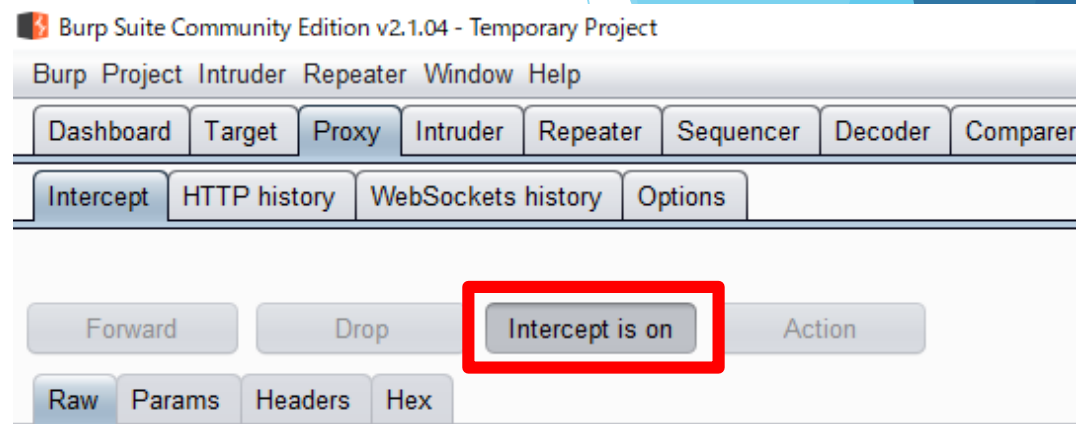
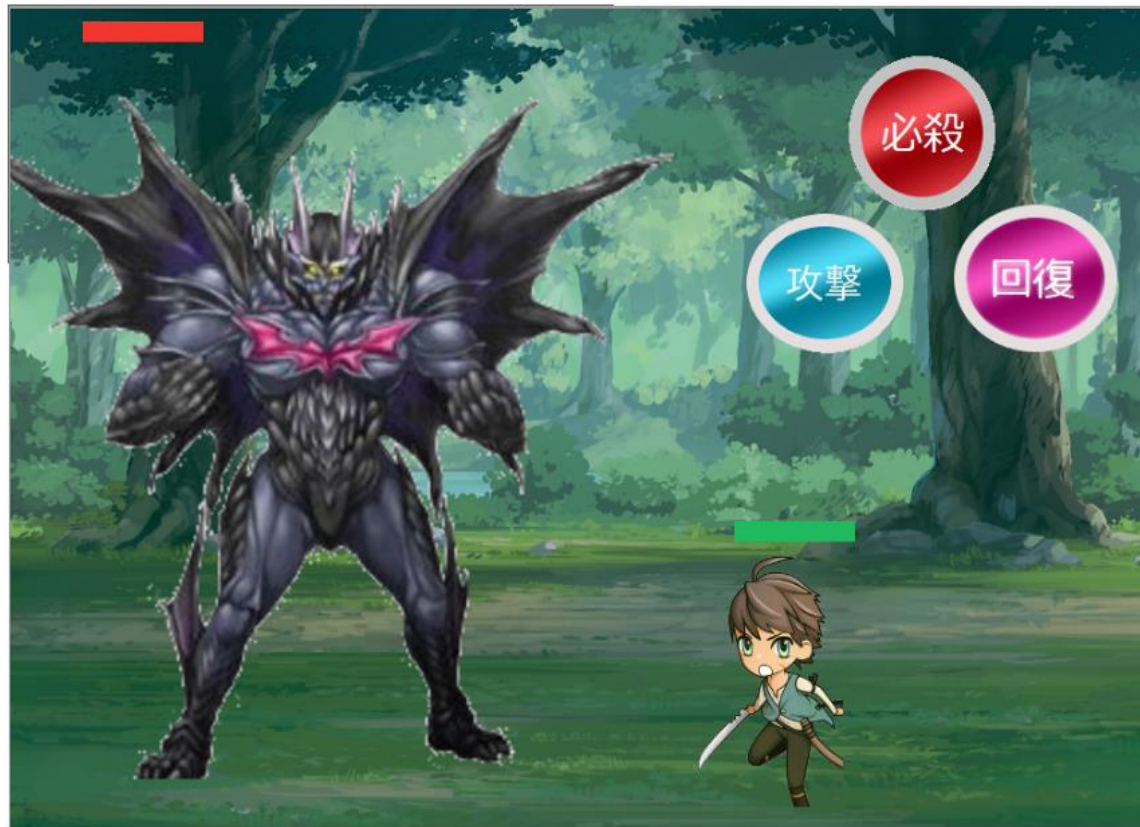


起動したら「learn.secret.jp」と検索し、
RPGをチュートリアルまで進めてください。

LV10にしよう！



LV10にしよう！



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

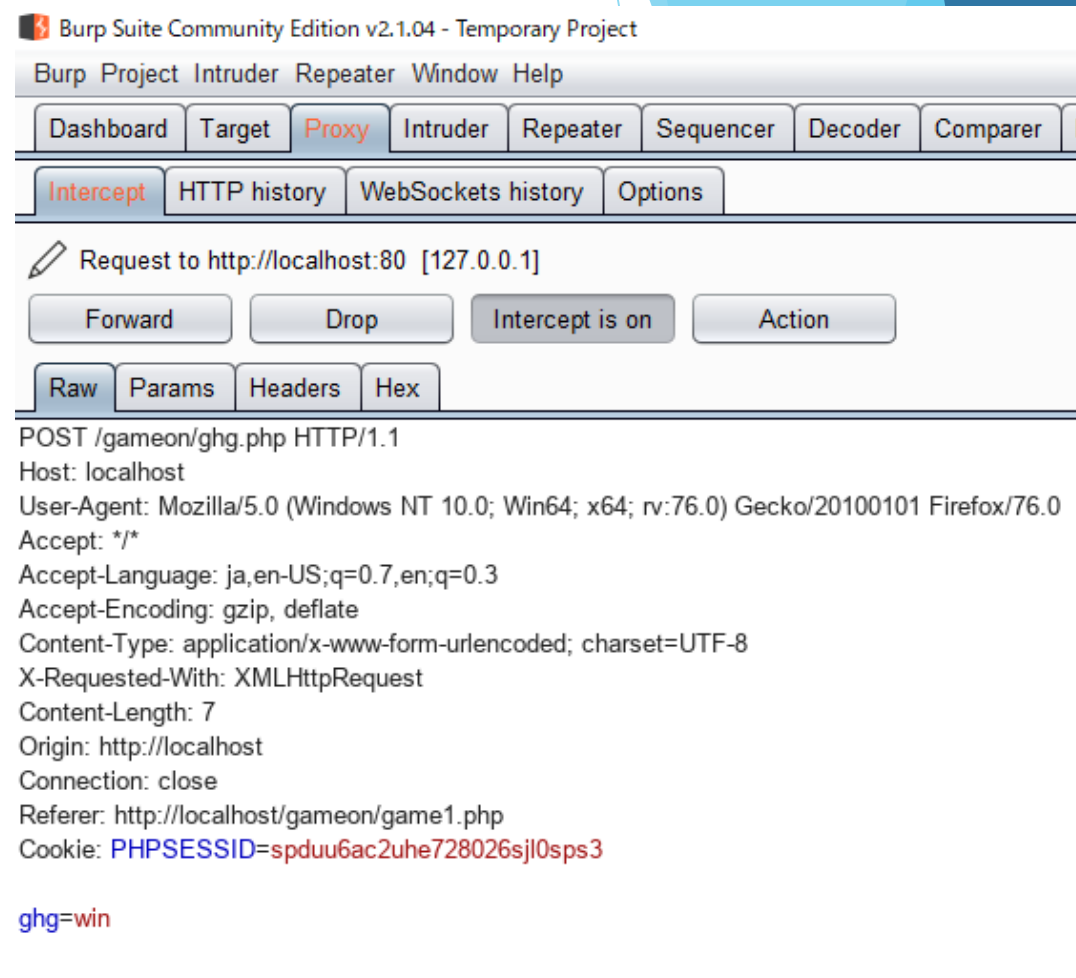
この手順が終わったら敵を倒そう！

LV10にしよう！



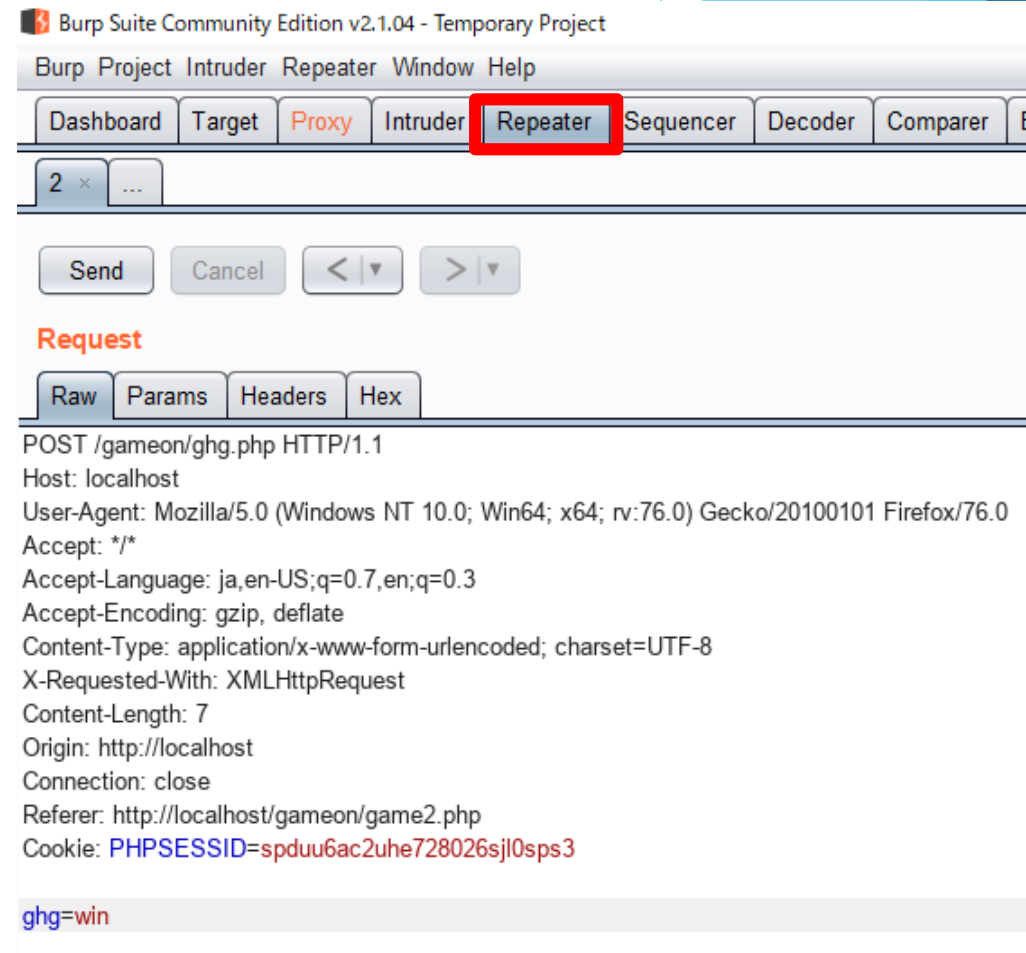
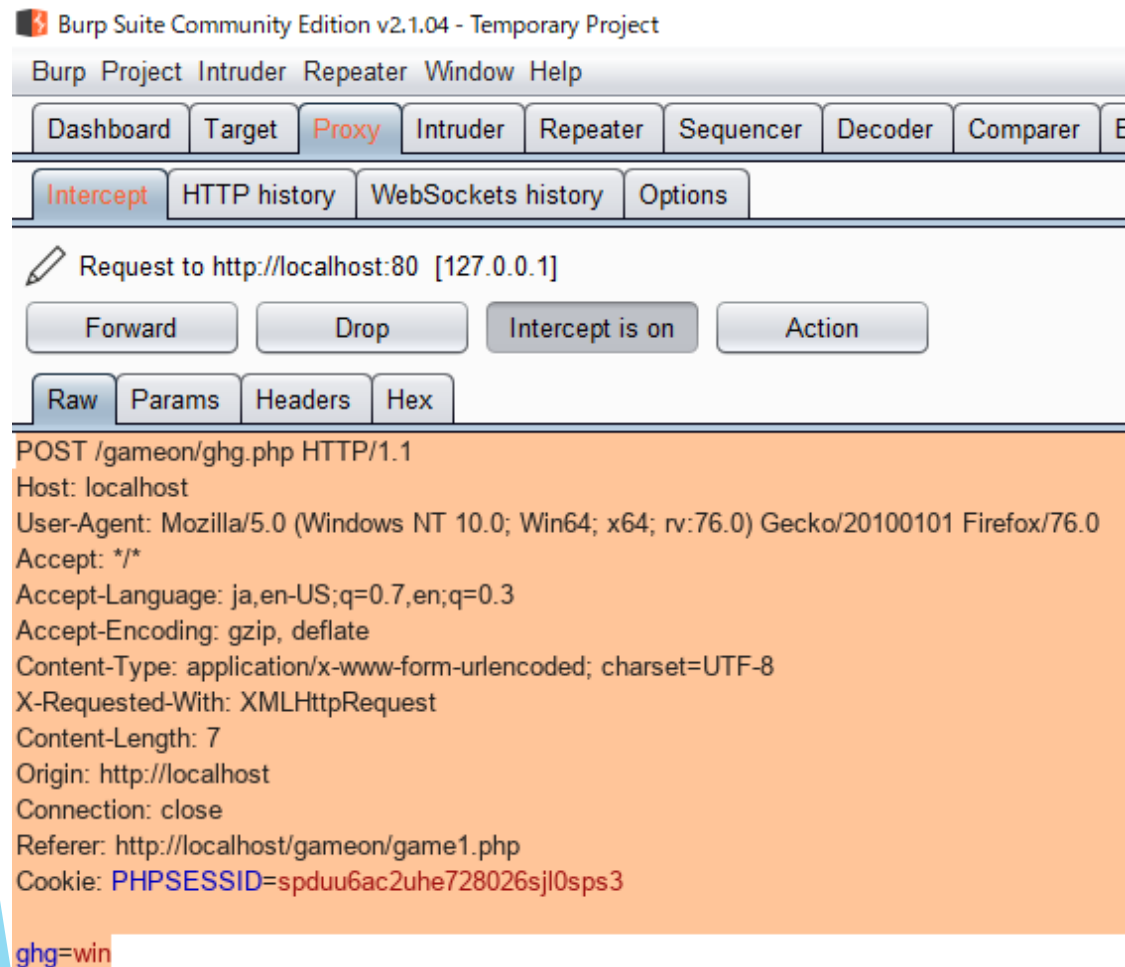
WIN

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！



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！

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

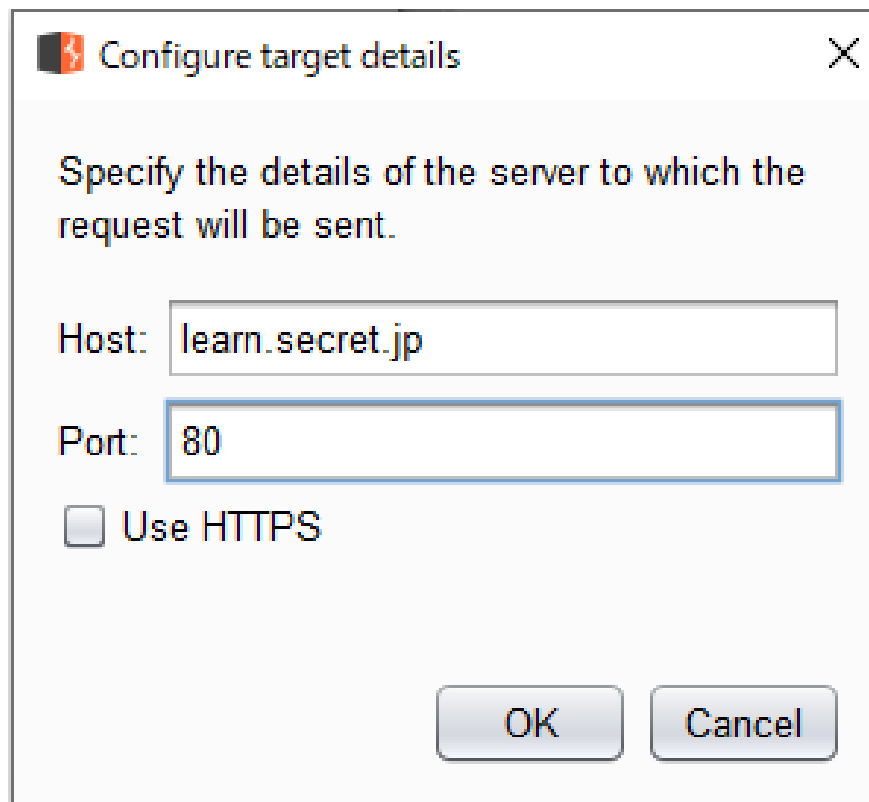
Response

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！



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

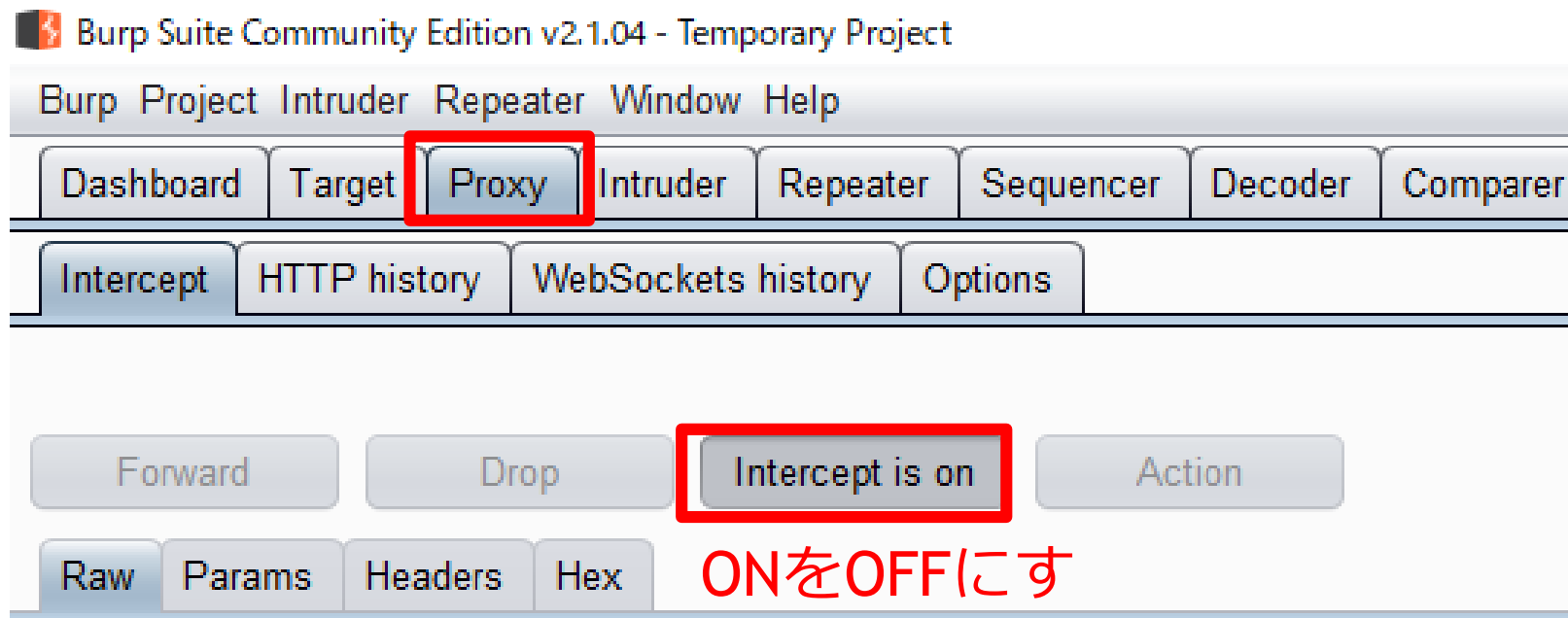
Sandを押したときこの画面が出てきたら・・・

Host:learn.secret.jp

Port:80

と入力してOKを押そう！

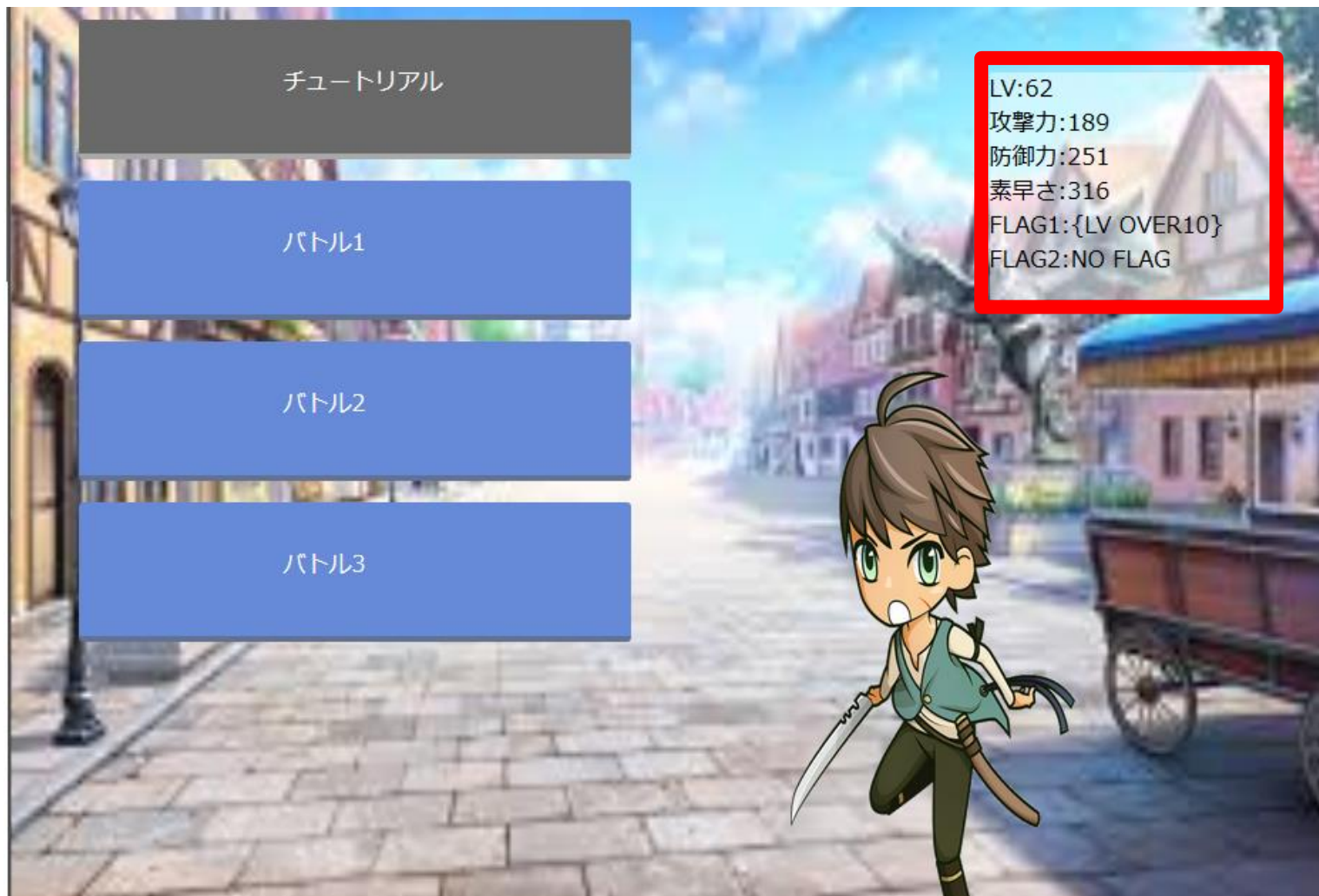
LV10にしよう！



ONをOFFにする！

通信が始まる！

LV10にしよう！



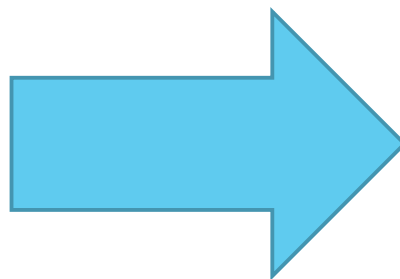
レベルが上がってFLAG1にLV10達成のメッセージが出てくる！

何が起こったのか（説明）

Before



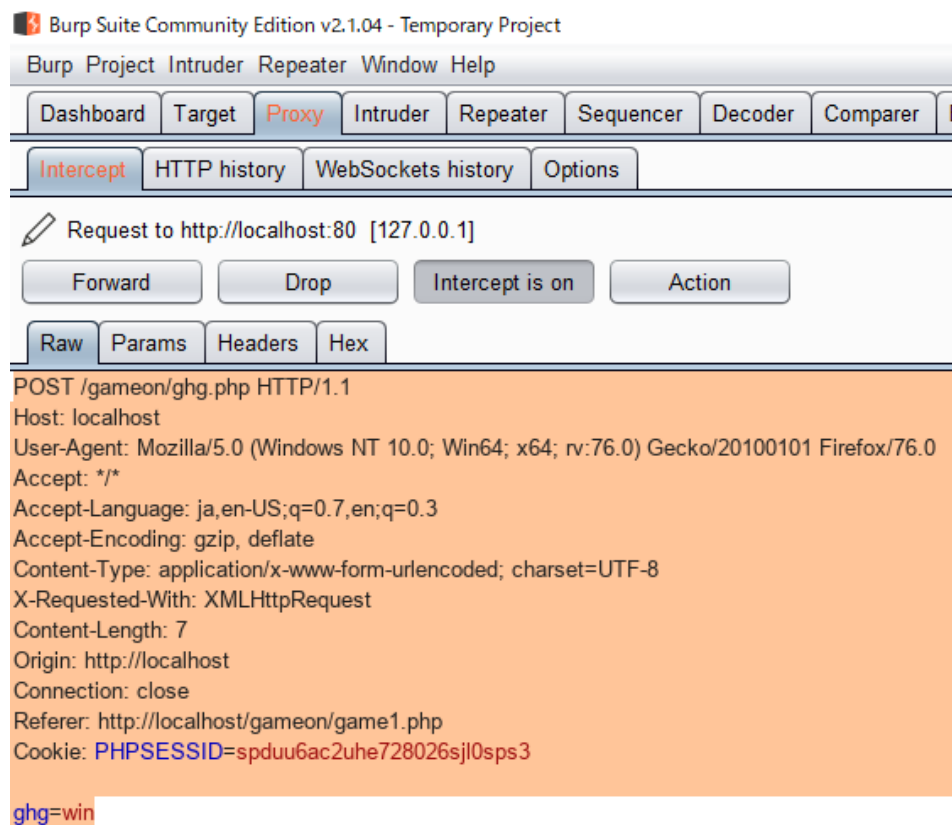
一回の戦いで



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・・・



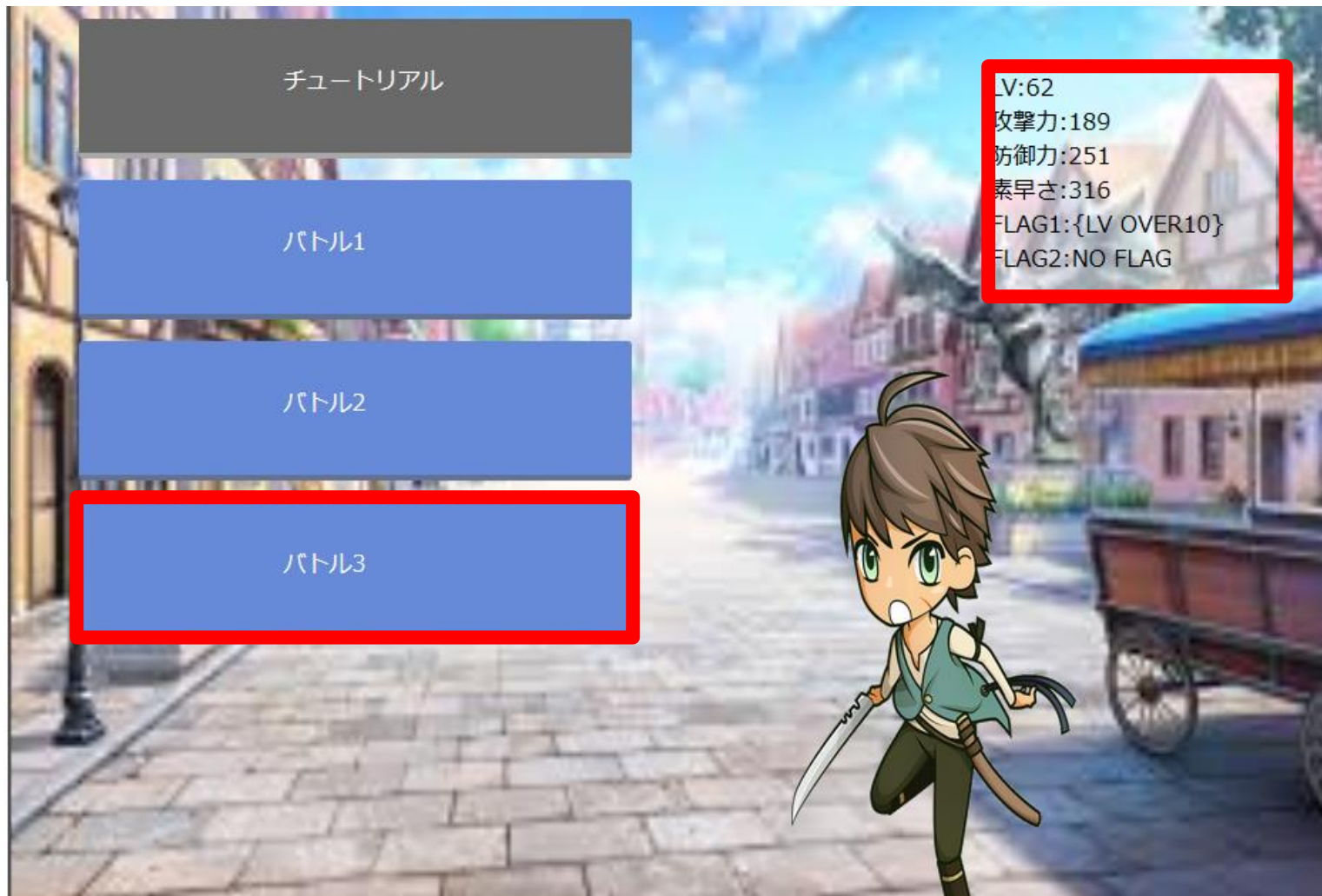
SANTENDO Scratch（経験
値）

× クリックした回数 =



強くなる！

最終ボスを倒そう！



FLAG2を手に入れよう！

最終ボスを倒そう！



LOSE

最終ボスは...何をしても絶対勝てません！

最終ボスを倒そう！

では、どうしたらいいか...？



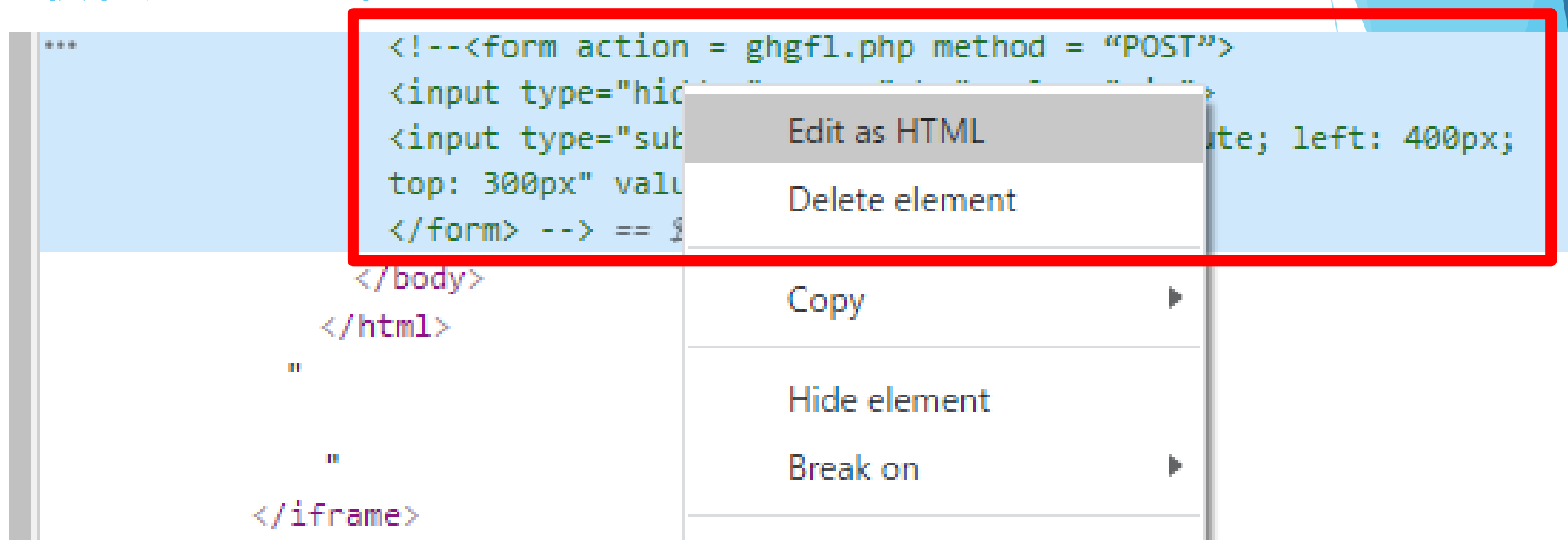
最終ボスを倒そう！

ボスの画面で
Fn+F12を押すと...

文字がたくさん
出てきます！

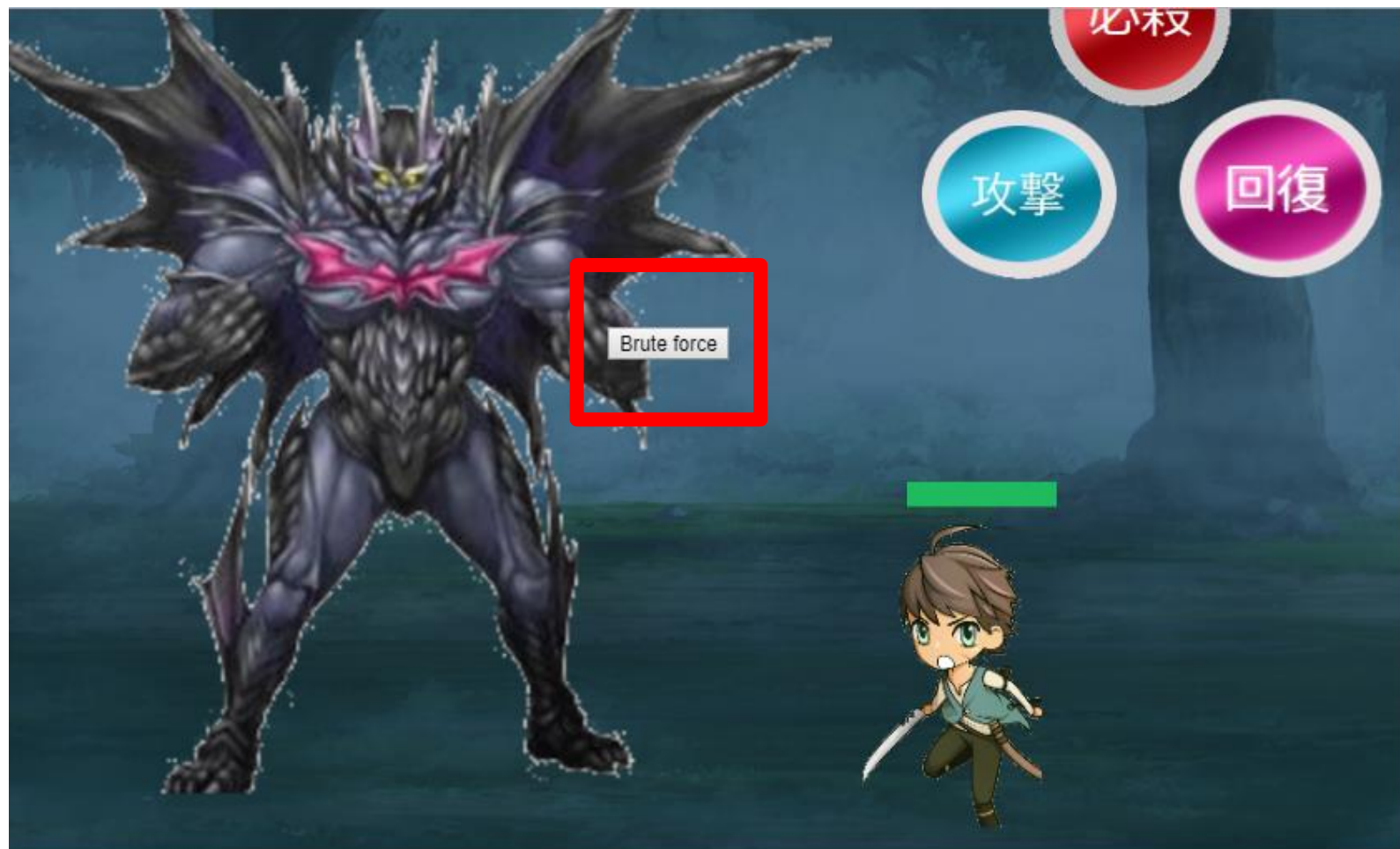
```
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<html> スクロール
<head> ... </head>
<body oncontextmenu="return false"> event
  <div id="center">
    <iframe src="game1.php" scrolling="no" width="940" height="640">
      #document
      <!DOCTYPE html>
      <html> event
      <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="batorfl.js"></script>
        <style type="text/css"> ... </style>
        <!--FLAG{LV OVER10}-->
      </head>
      <body>
        <div id="enchant-stage" style="position: absolute; font-size: 12px; -moz-text-size-adjust: none; width: 940px; height: 640px;"> ... </div> event
        <!--
        <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>
  </iframe>
  <h2>戦闘画面の説明</h2>
  
</div>
</body>
</html>
```

最終ボスを倒そう！



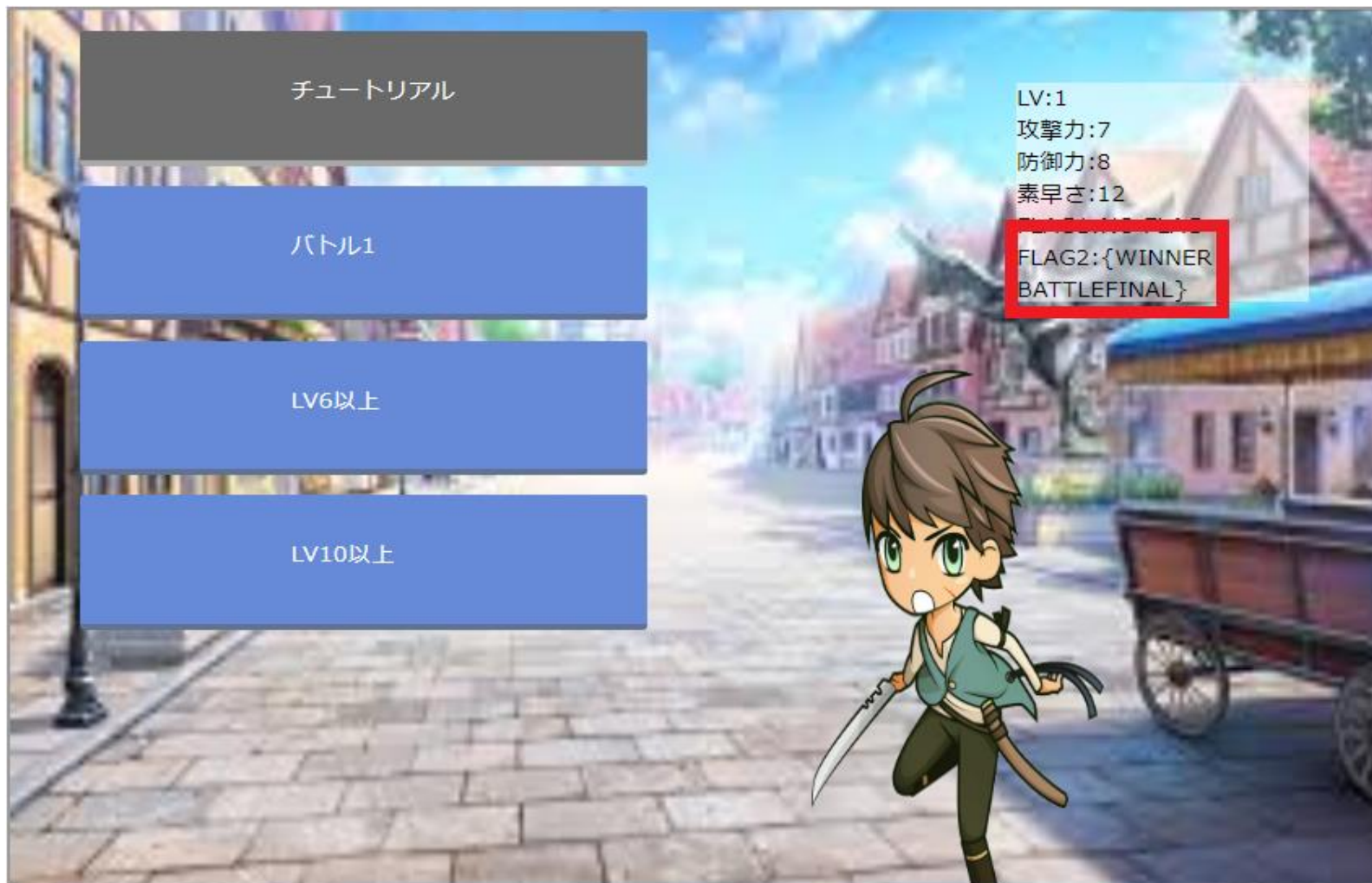
実は<body>から</body>の間に隠しボタンが隠れてます！
右クリックし、「Edit as HTML」を押して
<!--と-->を消してみよう！

最終ボスを倒そう！



すると、ボタンが現れます！ 押してみると...

最終ボスを倒そう！



FLAG2が手に入る！

説明



ボタンを押したことによって戦わずに勝つことができた！