



burp

もくじ

- Burpの使い方
- ハンズオン
 - ブラウザの通信に干渉する
 - 試行錯誤・挙動確認
 - 乏しいループ機能体験

実際に使ってみるのが、
早いと思うのでハンズオンがメインとなります

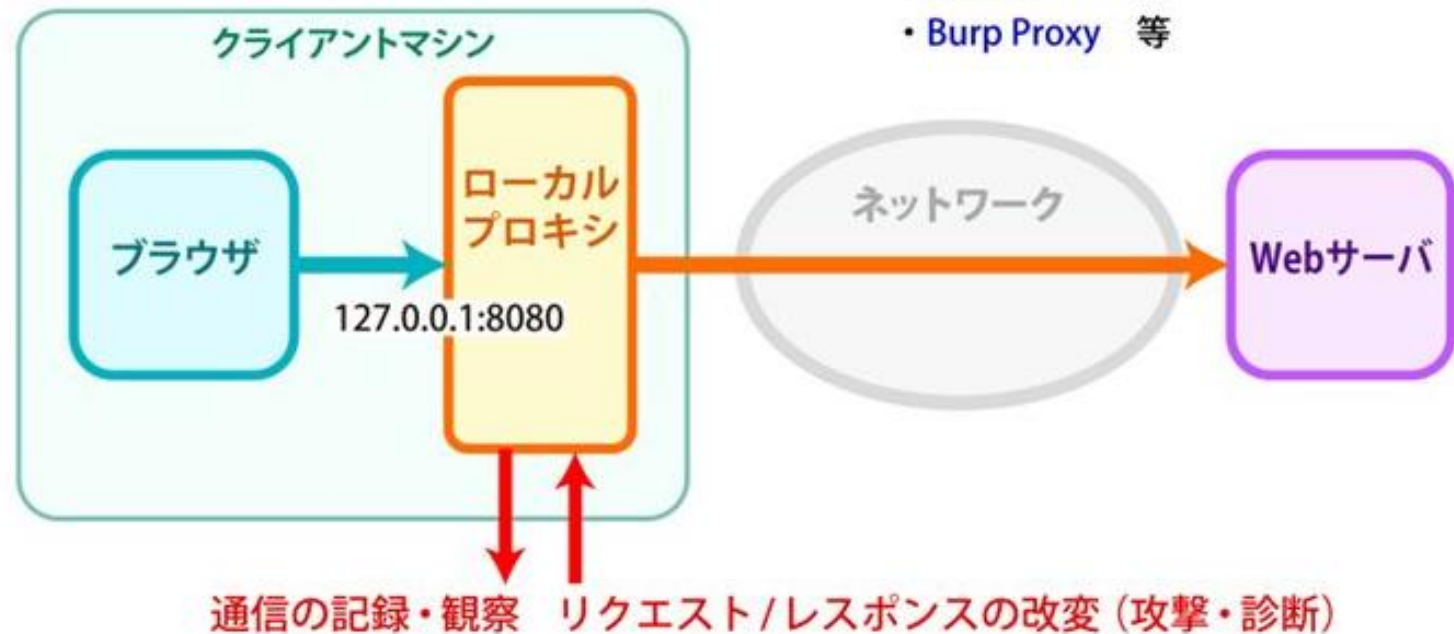
Burp suite とは？

プロキシツール

- ブラウザとwebサーバの通信を一度仲介する
- 通信内容をburpsuiteにて書き換えることができる

ローカルプロキシツールの例

- OWASP ZAP
- Fiddler
- Burp Proxy 等



<https://www.as-lab.net/150713/>

有名なプロキシツール

- Burp suite

有料版があり、無料版にスキャナーはついていない



- OWASP ZAP

オープンソースでスキャナー機能もついている



インストール

- Community をダウンロード

<https://portswigger.net/burp>



Google Translate

Products | Solutions | Research

Download Burp Suite Community Edition

Burp Suite Community Edition is a feature-limited set of manual tools for exploring web security. Proxy your HTTPS traffic, edit and repeat requests, decode data, and more. [Download the latest version here.](#)

Alternatively, try hacking like the pros do - with a [free trial of Burp Suite Professional](#). It's packed with [power features](#) - including an automated vulnerability scanner, the ability to save your work, and an unthrottled version of burp intruder.

[Download the latest version](#)

インストール

- Kali linux プリインストール
- Windowsで使う方法

<https://qiita.com/HowToPlay/items/bcea7ab8c07c4ea1afac>

基本的な機能

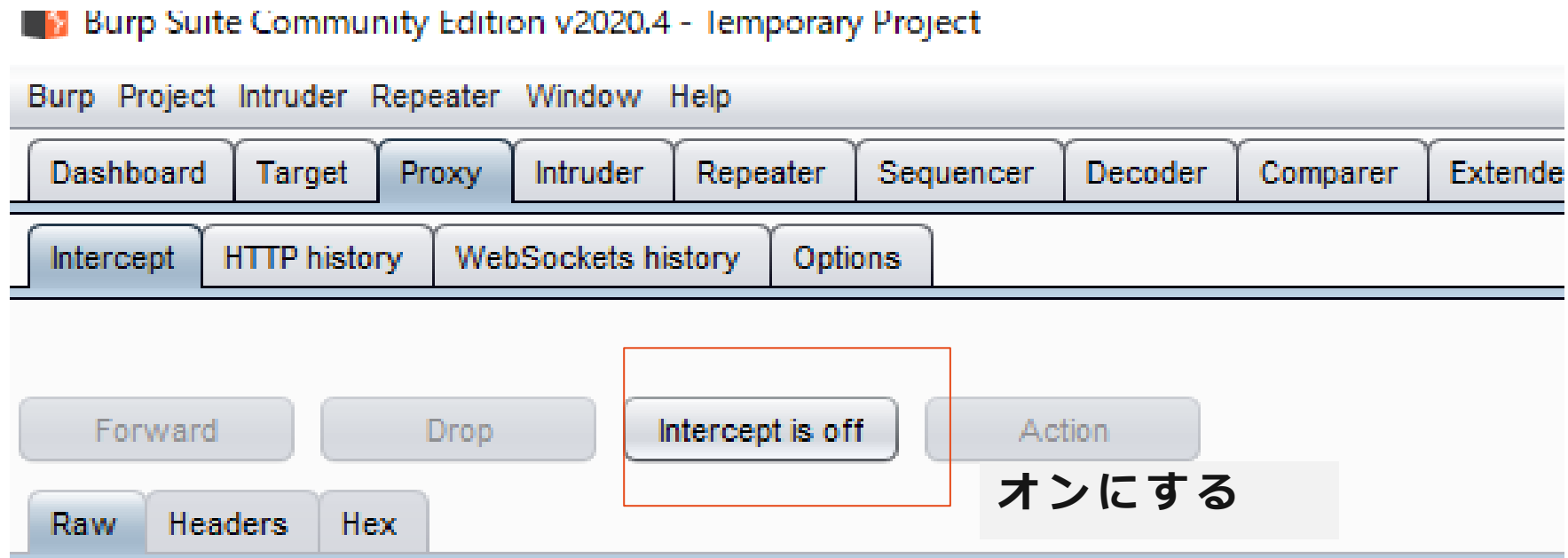
- Intercept
ブラウザの通信を仲介して、書き換える
- Repeater
単独でHTTPを送信できる
- Intruder
任意の文字列を変数として、変化させながら送信を繰り返す

Intercept

- ブラウザとwebサーバ間の通信に干渉して、通信を書き換えれる
- リクエストとレスポンスの両方いじれる
- 書き換えた後はブラウザに反映される

intercept

- Interceptをオンにする
(proxy)->(intercept)->(intercept is off)



Intercept-書き換え

- ブラウザから送られた通信が表示される

The screenshot displays the Burp Suite Community Edition v2020.4 interface. On the left, a web browser window shows the URL `https://http2020.herokuapp.com/get.php` and the page content `view GET parametar:get`. Below the page content is a form with an input field containing `aiueo` and a `submit` button. On the right, the Burp Suite interface shows the `Intercept` tab selected. The `HTTP history` tab is also visible. The `Request to https://http2020.herokuapp.com:443 [52.86.204.72]` is displayed. The `Raw` tab is selected, showing the following request details:

```
1 GET /get.php?get=aiueo HTTP/1.1
2 Host: http2020.herokuapp.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: ja,en-US;q=0.7,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: https://http2020.herokuapp.com/get.php
9 Upgrade-Insecure-Requests: 1
10
11
```

- 書き換え後、(Forward)をクリック

```
php?get=aiueo HTTP/1.1
Host: http2020.herokuapp.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win
Accept: text/html,application/xhtml+xml,application/javascript;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Connection: close
Host: http2020.herokuapp.com/get
```



```
GET /get.php?get=kakiku HTTP/1.1
Host: http2020.herokuapp.com
User-Agent: Mozilla/5.0 (Windows NT
Accept: text/html,application/xhtml
Connection: close
```

書き換え結果

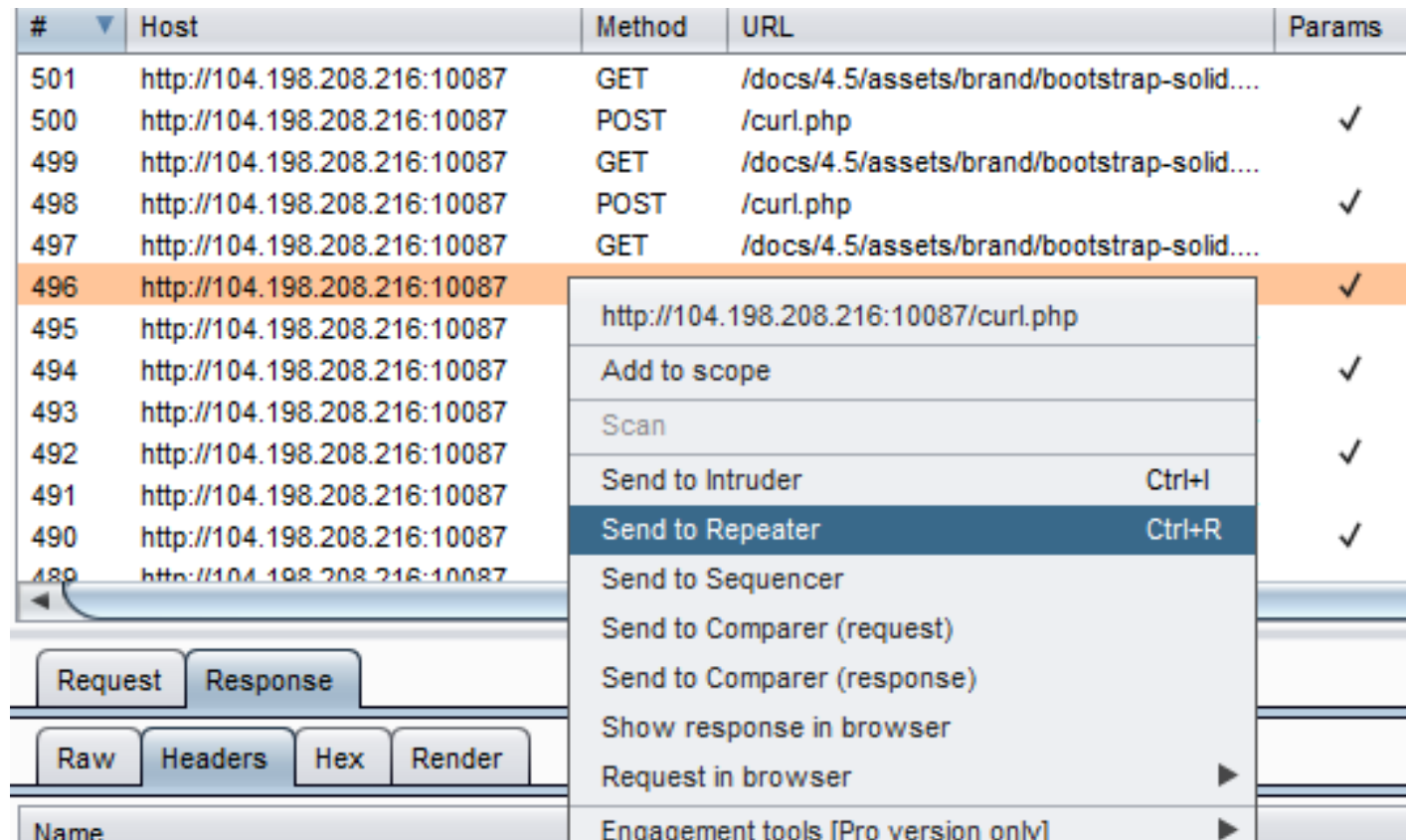
get: kakiku

submit

Repeater(HTTPを自分で書いてレスポンスを確認できる)

- 使い方

(Proxy)->(HTTP history)->(任意の履歴)->(send to repeater)



Repeater

- 左のrequestを書き換えて、(send)を押すと右にレスポンスが返ってくる

The screenshot displays the Repeater tool interface, which is used for sending and receiving HTTP requests and responses. The interface is divided into two main sections: Request and Response.

Request Section:

- Buttons: Send, Cancel, < | ▾, > | ▾
- Target: <https://http2020.herokuapp.com>
- Request Details (Raw tab):
 - 1 GET /get.php?get=aiueo HTTP/1.1
 - 2 Host: http2020.herokuapp.com
 - 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101 Firefox/78.0
 - 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
 - 5 Accept-Language: ja,en-US;q=0.7,en;q=0.3
 - 6 Accept-Encoding: gzip, deflate
 - 7 Referer: https://http2020.herokuapp.com/get.php?get=a
 - 8 Connection: close
 - 9 Upgrade-Insecure-Requests: 1
 - 0 Cache-Control: max-age=0

Response Section:

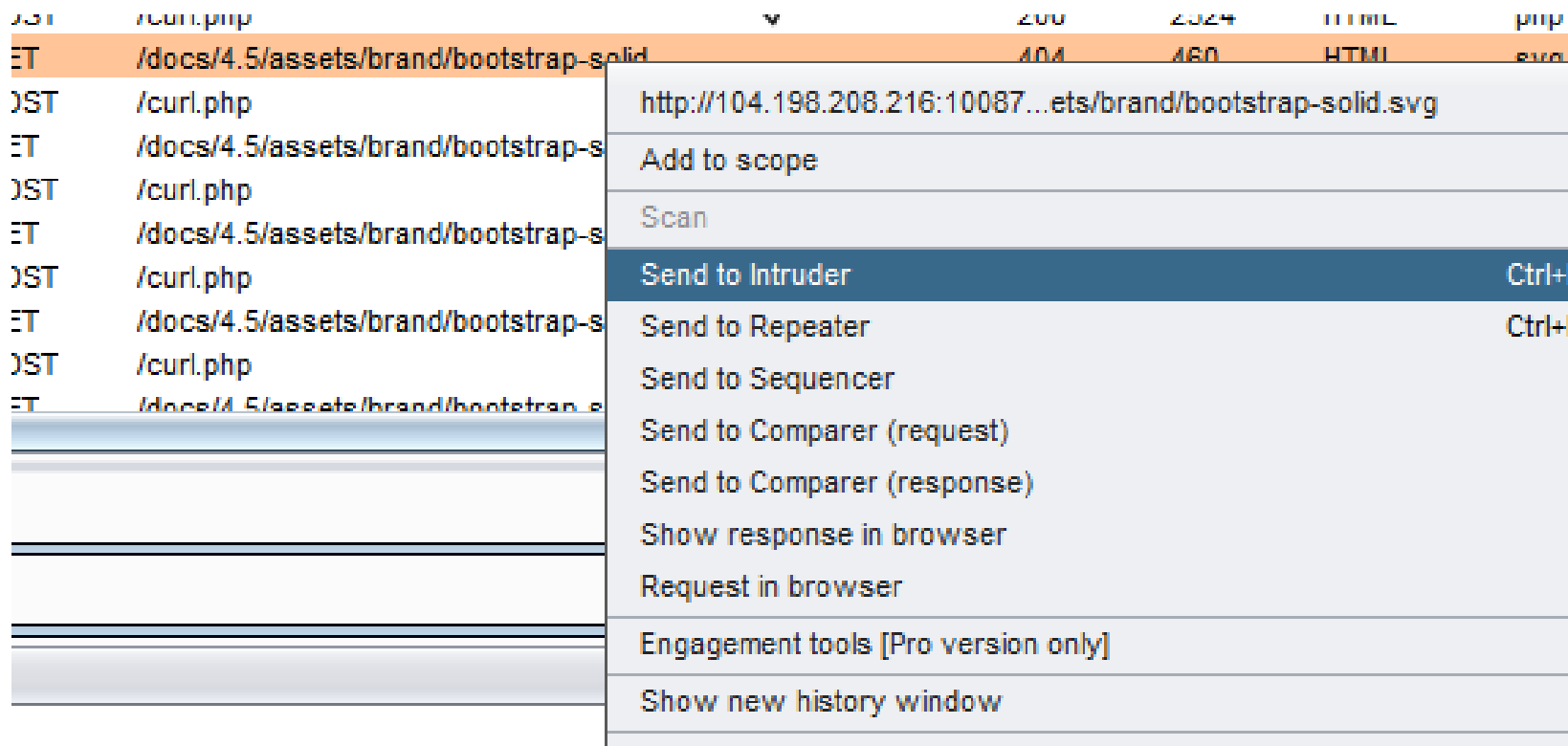
- Buttons: Raw, Headers, Hex, Render
- Response Details (Raw tab):
 - 1 HTTP/1.1 200 OK
 - 2 Connection: close
 - 3 Date: Sat, 11 Jul 2020 10:53:14 GMT
 - 4 Server: Apache
 - 5 Content-Type: text/html; charset=UTF-8
 - 6 Via: 1.1 vegur
 - 7 Content-Length: 241
 - 8
 - 9 <h1>
 - 10 view GET parametar:get
 - 11 </h1>
 - 12 get: aiueo<!DOCTYPE html>
 - 13 <html lang="ja">
 - 14 <head>
 - 15 </head>
 - 16 <body>

- 任意のHTTPに変数を設けて、変化させながら送信し続けれる
- 変数には、数字や文字列のリストを指定できる。
- 同じリクエストを送信し続けることも可能

Intruder(繰り返し送信)

使い方

(Proxy)->(HTTP history)->(任意の履歴)->(send to intruder)



Intruder(繰り返し送信)

- 変数部分にマークを付ける

```
1 GET /get.php?get=$ai++a$ HTTP/1.1
2 Host: http2020.herokuapp.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101
  Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: ja,en-US;q=0.7,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Referer: https://http2020.herokuapp.com/get.php?get=a
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11
12
```

Add \$

Clear \$

Auto \$

Refresh

Intruder(繰り返し送信)

- ペイロードを選択
 - Wordlistをコピーできる
 - ++する変数にしたりなどできる

) Payload Sets

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

Payload set: Payload count: 10

Payload type: Request count: 10

) Payload Options [Numbers]

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type: ☒ Sequential ☐ Random

From:

To:

Step:

How many:

Number format

Base: ☒ Decimal ☐ Hex

Min integer digits:

Max integer digits:

Min fraction digits:

Max fraction digits:

Decoder(URL encode や decode)

- 右側の画面からdecodeするかencodeするかを選ぶ

select user from table;

%73%65%6c%65%63%74%20%75%73%65%72%20%66%72%6f%6d%20%74%61%6

☒ Text ☐ Hex ?

Decode as ...

Encode as ...

Plain
URL
HTML
Base64
ASCII hex
Hex
Octal
Binary
Gzip

Smart decode

Decoder

- Base 64をかけた後に、URLencodeをつけたりできる

The image shows a web-based decoder tool interface with three rows of input and output fields. Each row has a large text area on the left and a control panel on the right.

Row 1:

- Input: `select user from table;`
- Controls: ☒ Text ☐ Hex (plus a help icon)
- Output: (empty)

Row 2:

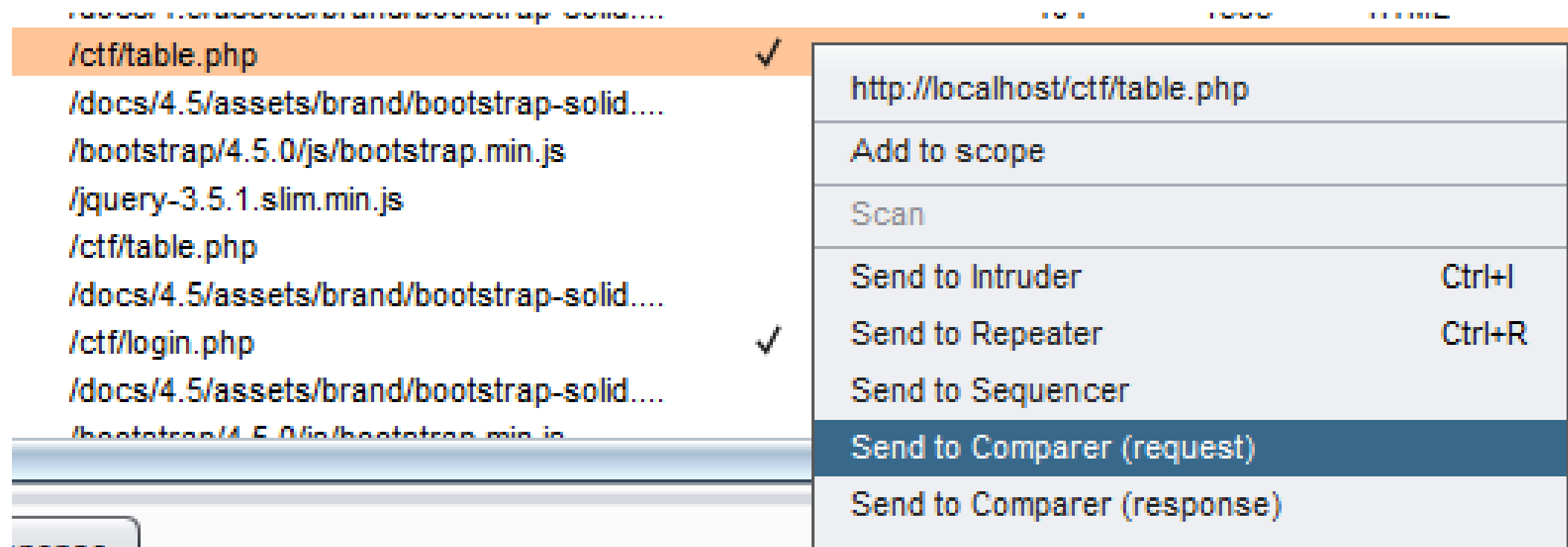
- Input: `c2VsZWN0IHVzZXIgaZnJvbSB0YWJsZTs=`
- Controls: ☒ Text ☐ Hex
- Output: (empty)

Row 3:

- Input: `%63%32%56%73%5a%57%4e%30%49%48%56%7a%5a%58%49%67%5a%6e%4a%7`
- Controls: ☒ Text ☐ Hex
- Output: (empty)

Comparer(通信の比較)

- 比べたい通信を項目に追加 (二つ)



Comparer

- 二つを選択したうえで words かbytesを選ぶ

Comparer ?

This function lets you do a word- or byte-level comparison between different data. You can load, paste, or send data here from other tools and then select the comparison you want to perform.

Select item 1:

#	Length	Data
2	515	POST /ctf/login.php HTTP/1.1Host: localhostUser-Agent: Mozilla/5....
3	512	POST /ctf/login.php HTTP/1.1Host: localhostUser-Agent: Mozilla/5....

Paste

Load

Remove

Clear

Select item 2:

#	Length	Data
2	515	POST /ctf/login.php HTTP/1.1Host: localhostUser-Agent: Mozilla/5....
3	512	POST /ctf/login.php HTTP/1.1Host: localhostUser-Agent: Mozilla/5....

Compare ...

Words

Bytes

Comparer

- 結果

Word compare of #2 and #3 (3 differences)

Length: 515

☒ Text ☐ Hex

```
POST /ctf/login.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101
Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: ja,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 31
Origin: http://localhost
Connection: close
Referer: http://localhost/ctf/login.php
Upgrade-Insecure-Requests: 1

username=userb&password=aaabbbb
```

Length: 512

☒ Text ☐ Hex

```
POST /ctf/login.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101
Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: ja,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 28
Origin: http://localhost
Connection: close
Referer: http://localhost/ctf/login.php
Upgrade-Insecure-Requests: 1

username=user1&password=aaaa
```

Key: Modified Deleted Added

☐ Sync views

小機能の紹介

その1

- Hiddenパラメータをブラウザで表示

(proxy)->(Options)->(Response Modification)



Response Modification



These settings are used to perform automatic modification of responses.

- ☒ Unhide hidden form fields
 - ☒ Prominently highlight unhidden fields
- ☐ Enable disabled form fields
- ☐ Remove input field length limits
- ☐ Remove JavaScript form validation
- ☐ Remove all JavaScript
- ☐ Remove <object> tags
- ☐ Convert HTTPS links to HTTP
- ☐ Remove secure flag from cookies

その1

- 要素名と値が出てくる



Hidden field
[appActionToken]

QvsC8ZIEevAHQTWIdLAB1Kg1CGIj3D

Hidden field [appAction]

SIGNIN_PWD_COLLECT

Hidden field
[subPageType]

SignInClaimCollect

Hidden field
[openid.return_to]

ape:aHR0cHM6Ly93d3cuYW1hem9uLmNvI

Hidden field [prevRID]

ape:UjAxSkU4VIM2S0NNUjhCVzJRU0c=

その2

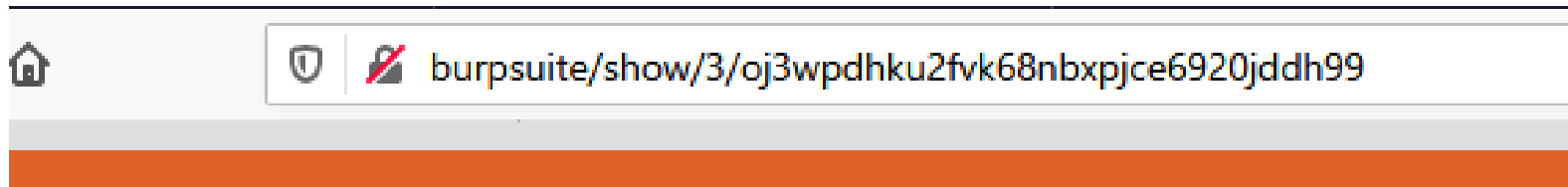
- Repeaterなどで出したリクエストからのレスポンスをブラウザで表示

```
5 Connection: close
6 Content-Type: text/html; charset=UTF-8
7 X-Content-Encoding-Over-Network: gzip
8 Content-Length: 2821
9
0
1
2 <!-- doctype ht
3 <html lang="
4
5 <head>
6 <!-- Req
7 <meta ch
8 <meta na
9
0 <!-- Boo
```

Scan	
Send to Intruder	Ctrl+I
Send to Repeater	Ctrl+R
Send to Sequencer	
Send to Comparer	
Send to Decoder	
Show response in browser	
Request in browser	▶
Engagement tools (Pro version only)	▶

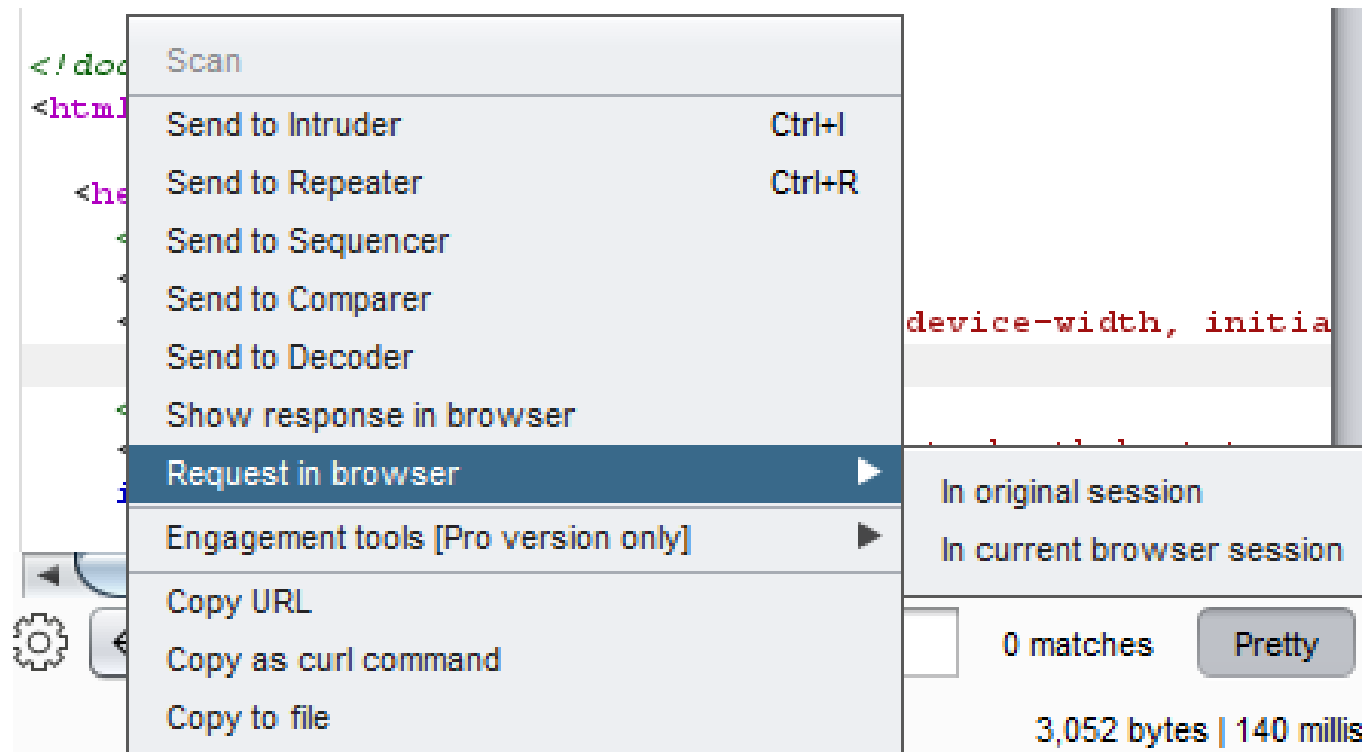
その2

- リンクをコピーして、ブラウザに張り付け



その2

- ブラウザからリクエストを改めて送ることもできる



その3

- リクエスト及びレスポンスの自動的書き換え

? Match and Replace

⚙ These settings are used to automatically replace parts of requests and responses passing through the Proxy.

Add	Enabled	Item	Match	Replace	Type	Co
Edit Remove Up Down	<input type="checkbox"/>	Request header	^User-Agent.*\$	User-Agent: Mozilla/4.0 (compatible...	Regex	Em
	<input type="checkbox"/>	Request header	^User-Agent.*\$	User-Agent: Mozilla/5.0 (iPhone; CP...	Regex	Em
	<input type="checkbox"/>	Request header	^User-Agent.*\$	User-Agent: Mozilla/5.0 (Linux; U; A...	Regex	Em
	<input type="checkbox"/>	Request header	^If-Modified-Since.*\$		Regex	Re
	<input type="checkbox"/>	Request header	^If-None-Match.*\$		Regex	Re
	<input type="checkbox"/>	Request header	^Referer.*\$		Regex	Hid
	<input type="checkbox"/>	Request header	^Accept-Encoding.*\$		Regex	Re
	<input type="checkbox"/>	Response header	^Set-Cookie.*\$		Regex	Ign

その3

- 設定した置換ルールを、
[リクエスト ・ レスポンス] [ヘッダ ・ ボディ] を選べる
- ルールの記述は正規表現に対応している

CTFでの利用例

- CPAWCTF q15 redirect

<https://ctf.cpaw.site/questions.php?qnum=15>

Q15.[Web] Redirect

100pt

このURLにアクセスすると、他のページにリダイレクトされてしまうらしい。
果たしてリダイレクトはどのようにされているのだろうか...

<http://q15.ctf.cpaw.site>

※この問題のサーバへの攻撃はお止め下さい

- サーバーからのレスポンスも傍受するように設定する



Intercept Server Responses



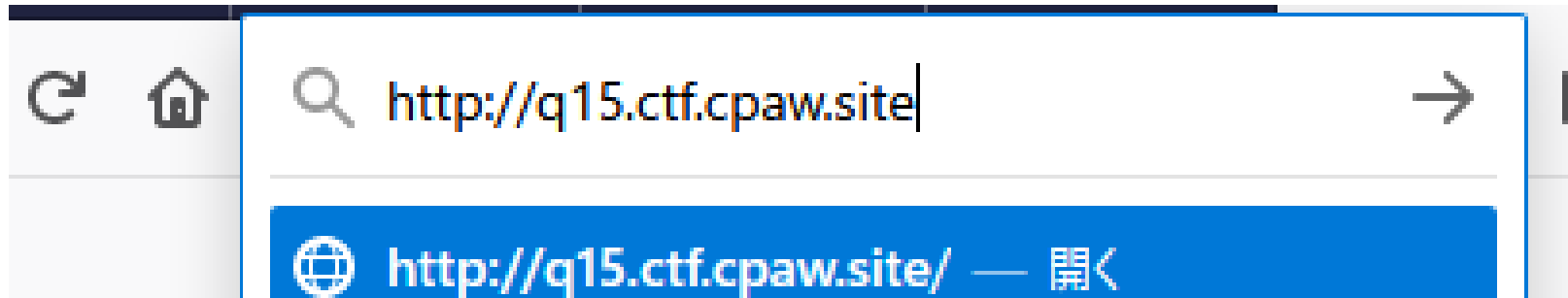
Use these settings to control which responses are stalled for viewing and editing in the Intercept tab.



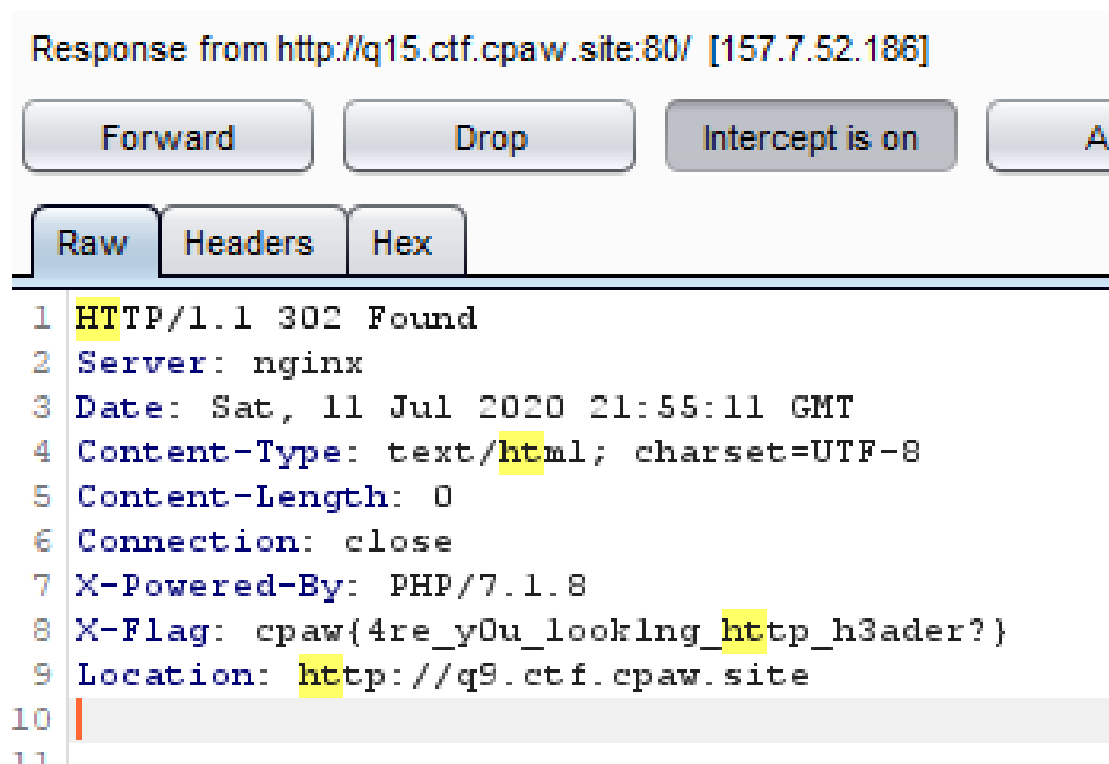
Intercept responses based on the following rules: *Master interception is turned off*

Add	Enabled	Operator	Match type	Relationship	Condition
	<input checked="" type="checkbox"/>		Content type header	Matches	text
Edit	<input type="checkbox"/>	Or	Request	Was modified	
	<input type="checkbox"/>	Or	Request	Was intercepted	
Remove	<input type="checkbox"/>	And	Status code	Does not match	^304\$
	<input type="checkbox"/>	And	URL	Is in target scope	
Up					
Down					

- 指定urlをブラウザにて入力



- 何度か(Forward)ボタンをクリックすると、
302 not found が返ってくる



The screenshot shows the 'Raw' tab of a web browser's developer tools. The title bar indicates the response is from 'http://q15.ctf.cpaw.site:80/ [157.7.52.186]'. Below the title bar are buttons for 'Forward', 'Drop', 'Intercept is on', and 'Accept'. The 'Raw' tab is selected, showing the raw HTTP response. The response is an HTTP 302 Found status. The headers include 'Server: nginx', 'Date: Sat, 11 Jul 2020 21:55:11 GMT', 'Content-Type: text/html; charset=UTF-8', 'Content-Length: 0', 'Connection: close', 'X-Powered-By: PHP/7.1.8', 'X-Flag: cpaw{4re_y0u_looking_http_h3ader?}', and 'Location: http://q9.ctf.cpaw.site'. The body of the response is empty.

```
Response from http://q15.ctf.cpaw.site:80/ [157.7.52.186]
Forward Drop Intercept is on Accept
Raw Headers Hex
1 HTTP/1.1 302 Found
2 Server: nginx
3 Date: Sat, 11 Jul 2020 21:55:11 GMT
4 Content-Type: text/html; charset=UTF-8
5 Content-Length: 0
6 Connection: close
7 X-Powered-By: PHP/7.1.8
8 X-Flag: cpaw{4re_y0u_looking_http_h3ader?}
9 Location: http://q9.ctf.cpaw.site
10
11
```

簡単な例題

Login 問題

- <http://34.69.119.25:10085/>

poo_validation

Let's Login Challenge(๑ '人')

Username

Password

max-length=10

Submit

Login 問題

- コードの中にadminのパスワードが入っています

```
<form action="index.php" method="post">
<!--
    debug
    user::admin
    pass::password12345698910

-->
<div class="form-group">
<label for="exampleInputEmail">Username</label>
<input type="text" class="form-control" name="username" aria-describedby="emailHelp">
</div>
<div class="form-group">
<label for="exampleInputPassword1">Password</label>
<input type="password" class="form-control" name="password" maxlength="16">
<small id="emailHelp" class="form-text text-muted">
```

ログイン問題

- パスワードが十文字しか入りません

Password

●●●●●●●●●●

max-length=10



ログイン問題

- Htmlを見ると、max-lengthによる制限があります
- ブラウザで書き換えてあげればよいですが、せっかくなのでburpsuiteを使って解いてみましょう。

```
<!--debug user::admin pass::password12345698910-->
▶ <div class="form-group"> ... </div>
▼ <div class="form-group">
  <label for="exampleInputPassword1">Password</label>
  <input class="form-control" type="password" name="password" maxlength="10">
  ▶ <small id="emailHelp" class="form-text text-muted"> ... </small>
```

ログイン問題

- ブラウザによる制限をなくしてみる

Response Modification



These settings are used to perform automatic modification of responses.

- ☐ Unhide hidden form fields
 - ☐ Prominently highlight unhidden fields
- ☐ Enable disabled form fields
- ☒ Remove input field length limits
- ☐ Remove JavaScript form validation
- ☐ Remove all JavaScript
- ☐ Remove <object> tags
- ☐ Convert HTTPS links to HTTP
- ☐ Remove secure flag from cookies

ログイン問題

- 上記設定をもって、再表示すればブラウザで10文字以上入力できる

リダイレクト問題

- Aさんがログイン済みユーザー専用のwebページを送ってきました
- コードミスはないかなあ

<http://34.69.119.25:10086/table.php>

リダイレクト問題

- ユーザ限定ページなのに、responseを見るとhtmlが入っています。
- リダイレクトを消せば、ブラウザでレスポンスが見れそうです

```
-HTTP/1.1 302 Found
Date: Wed, 15 Jul 2020 11:26:23 GMT
Server: Apache/2.4.38 (Debian)
Location: login.php
Content-Length: 2008
Connection: close
Content-Type: text/html; charset=UTF-8
```

```
<!-- doctype html -->
<html lang="en">

<head>
<!-- Required meta tags -->
<meta charset="utf-8">
<meta name="viewport" content="width=device-width, initial-

<!-- Bootstrap CSS -->
<link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.1.0/css/bootstrap.min.css" integrity="sha384-CW6PUM0NB9Si8FEvAoXDh/H36dy0sb/JUS8jV8/35jPrOQeRV2oQeVTuMcs81kgMg=">
```

Task.phpのレスポンス

リダイレクト問題

- Locationヘッダは302,301,201の時しか意味をなさないので、302を書き換えてあげればよい

リダイレクト問題

- Burpの機能を用いて、レスポンスを書き換えます

The screenshot shows the Burp Suite interface. On the left, the 'Match and Replace' tab is active, displaying a table of rules. The 'Enabled' column has checkboxes, and the 'Item' column lists 'Request header' and 'Response header'. The last 'Response header' row is selected. To the right of the table are buttons: 'Add', 'Edit', 'Remove', 'Up', and 'Down'. Below this is the 'TLS Pass Through' section. An 'Edit match/replace rule' dialog box is open in the center, showing the configuration for a rule. The 'Type' is set to 'Response header', 'Match' is '302 Found', and 'Replace' is '200 OK'. There is a 'Comment' field and a 'Regex match' checkbox. The dialog has 'OK' and 'Cancel' buttons at the bottom right. In the background, a list of intercepted responses is visible, with one entry highlighted in orange.

Match and Replace

These settings are used to automatically replace parts of requests and responses passing through the Proxy.

Enabled	Item
<input type="checkbox"/>	Request header
<input type="checkbox"/>	Response header
<input type="checkbox"/>	Request header
<input type="checkbox"/>	Request header
<input type="checkbox"/>	Response header
<input type="checkbox"/>	Response header
<input checked="" type="checkbox"/>	Response header

Edit match/replace rule

Specify the details of the match/replace rule.

Type: Response header

Match: 302 Found

Replace: 200 OK

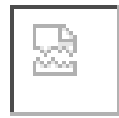
Comment:

☐ Regex match

OK Cancel

リダイレクト問題

- すると、get flagというボタンが見えるのでボタンを押せばフラグが見えます！



[replace!](#)

get flag

clpwn{replace and browser view}

今回省いた内容

- 自前証明書を利用してhttpsサイトの通信を傍受する

<https://www.securesky-tech.com/column/naruhodo/02.html>

参考

<https://www.securesky-tech.com/column/naruhodo/01.html>

<https://www.securesky-tech.com/column/naruhodo/02.html>

日本語ドキュメント

<https://burp-resources-ja.webappsec.jp/Documentation/burp/documentation/desktop/getting-started/index.html>

ひまつぶし-burp関係ないです

- <http://34.69.119.25:10087/curl.php>

LFI問題です。

Flagはルートディレクトリにflag.txtとして設置しています。

ひまつぶし

- <https://www.php.net/manual/ja/wrappers.file.php>

[file:///flag.txt](#)でみることができます。