Burp Extension

File Uploading

Dashboard Target Proxy Intruder Repeater ... Extensions | Upload File |

| 1 × |

| Positions | Payloads   Upload history

Choose an upload mode

Upload mode : [   ]

→ Upload one file per one request.
→ Upload all flies in one request.

Payload positions

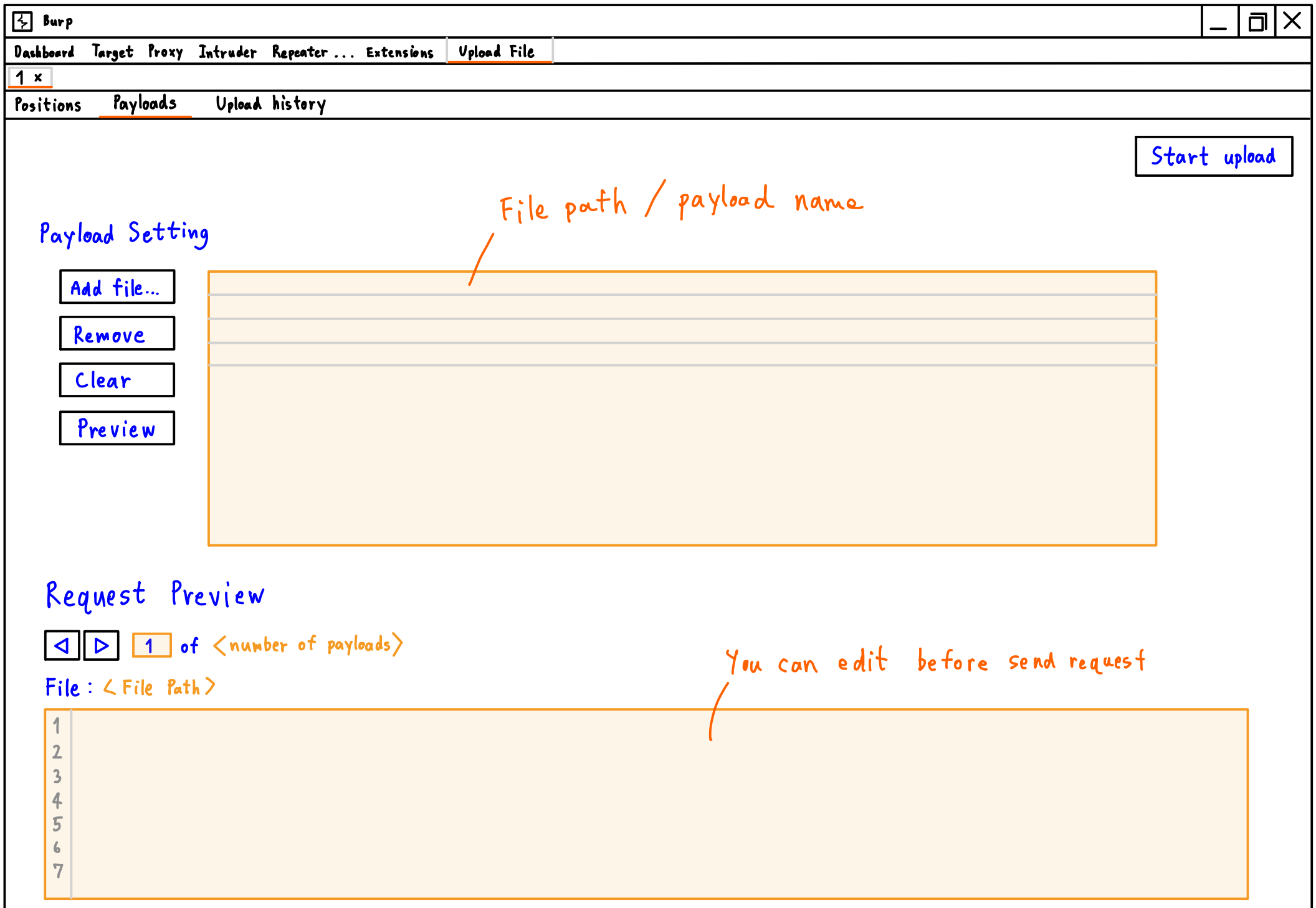Target : [   ]

```
1
2
3
4
5
6
```

Start upload

Add §

Clear §

Auto §

Refresh

Burp

Dashboard Target Proxy Intruder Repeater ... Extensions **Upload File**

1 ×

Positions **Payloads** Upload history

Start upload

File path / payload name

Payload Setting

Add file...

Remove

Clear

Preview

Request Preview

◁ ▷ 1 of ⟨number of payloads⟩

You can edit before send request

File : ⟨ File Path ⟩

```
1
2
3
4
5
6
7
```

Burp

1 ×

Positions   Payloads   Upload history

Start upload

#	URL	Method	File path	Status code	Length	Time

Request

```
1
2
3
4
5
6
7
```

Response

```
1
2
3
4
5
6
7
```

Inspector

Request

Pretty | Raw | Hex

```
1  POST /upload_endpoint HTTP/1.1
2  Host: example.com
3  Content-Length: [length]
4  Content-Type: multipart/form-data; boundary=Boundary
5
6  --Boundary
7  Content-Disposition: form-data; name="file1"; filename="myfile1.txt"
8  Content-Type: text/plain
9
10 [FILE1 CONTENTS]
11
12 --Boundary
13 Content-Disposition: form-data; name="file2"; filename="myfile2.jpg"
14 Content-Type: image/jpeg
15
16 [FILE2 CONTENTS]
17
18 --Boundary--
19
```

Ex.

Request

Pretty | Raw | Hex

```
1  POST / HTTP/1.1
2  [[ Less interesting headers ... ]]
3  Content-Type: multipart/form-data;
   boundary=---------------------------7353230313999631669938621 50
4  Content-Length: 834
5
6  -----------------------------7353230313999631669938621 50
7  Content-Disposition: form-data; name="text1"
8
9  text default
10 -----------------------------7353230313999631669938621 50
11 Content-Disposition: form-data; name="text2"
12
13 a b
14 -----------------------------7353230313999631669938621 50
15 Content-Disposition: form-data; name="file1"; filename="a.txt"
16 Content-Type: text/plain
17
18 Content of a.txt.
19
20 -----------------------------7353230313999631669938621 50
21 Content-Disposition: form-data; name="file2"; filename="a.html"
22 Content-Type: text/html
23
24 <!DOCTYPE html><title>Content of a.html.</title>
25
26 -----------------------------7353230313999631669938621 50
27 Content-Disposition: form-data; name="file3"; filename="binary"
28 Content-Type: application/octet-stream
29
30 a b
31 -----------------------------7353230313999631669938621 50--
```

Request

Pretty | Raw | Hex

```
1  PUT /upload_endpoint/myfile.txt HTTP/1.1
2  Host: example.com
3  Content-Length: [length]
4  Content-Type: text/plain
5
6  [FILE CONTENTS]
```

ไม่ค่อยปลอดภัยในการทำๆ
เพราะอาจเกิด file Overwriting กับไฟล์ที่อยู่ใน server

Request

Pretty | Raw | Hex

```
1  PATCH /upload_endpoint/myfile.txt HTTP/1.1
2  Host: example.com
3  Content-Length: [length]
4  Content-Type: multipart/form-data; boundary=Boundary
5
6  --Boundary
7  Content-Disposition: form-data; name="file"; filename="myfile.txt"
8  Content-Type: text/plain
9
10 [FILE CONTENTS]
11 --Boundary--
```

ไม่ค่อยเจอ

Request

Pretty | Raw | Hex

```
1  POST /upload HTTP/1.1
2  Host: example.com
3  Content-Length: [length]
4  Content-Type: application/octet-stream
5
6  [BINARY FILE CONTENTS]
```

Request

Pretty | Raw | Hex

```
1  POST /upload HTTP/1.1
2  Host: example.com
3  Content-Length: [length]
4  Content-Type: application/json
5
6  {
7      "filename": "myfile.txt",
8      "filedata": "[BASE64 ENCODED FILE CONTENTS]"
9  }
```

Request

Pretty | Raw | Hex

```
1  POST /upload HTTP/1.1
2  Host: example.com
3  Content-Length: [length]
4  Content-Type: application/xml
5
6  <file>
7      <filename>myfile.txt</filename>
8      <data>[FILE CONTENTS, POSSIBLY BASE64 ENCODED]</data>
9  </file>
```