

Mocking HTTP APIs With Burp

Shea Polansky

2019-11-08
Shea Polansky
<https://polansky.co>
@0x5ca1e5



Motivation

- Simple HTTP Response Mocking
 - "isAdmin": false → "isAdmin": true
- Complex Application Manipulation
 - When built-in regex rules won't cut it

Example Use Case: DRM Bypass

GET /api/license?uid=<...>

```
base64 [
  {
    "license": {
      base64 [
        {
          "uid": <...>, "user": "...", "expiration": "...", ...
        }
      ],
    "signatures": [
      {
        base64 [
          {
            "cert": "...",
            "CA": "...",
            "signature": base64 [
              <pkcs7 signature data>
            ]
          }
        ],
        , ...
      }
    ]
  }
]
```

Example Use Case: DRM Bypass

- This protocol is *wack*
- App requires response in <2s
- Want other calls to go through as normal
- Normally would have to write a custom Burp plugin
- With this, just need a quick python script!

Burp HTTP Mock Extension

- Originally by Michal Dardas
- I added dynamic mocking
- Matches requests by regex, either lets through or transparently redirects to static/dynamic mock

Demo!

Burp Suite Community Edition v1.7.35 - Temporary Project

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts HTTP Mock

Intercept HTTP history WebSockets history Options

Filter: Showing all items

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	SSL
425	https://github.com	GET	/LogicalTrust/meltdow...	✓		200	3398	HTML				✓
426	https://github.com	GET	/LogicalTrust/BurpExif...	✓		200	3398	HTML				✓
427	https://github.com	GET	/LogicalTrust/BurpSess...	✓		200	3394	HTML				✓
428	https://github.com	GET	/LogicalTrust/materials...	✓		200	3398	HTML				✓
429	https://github.com	GET	/LogicalTrust/drozer/g...	✓		200	3398	HTML				✓
430	https://www.google-analytic...	POST	/r/collect	✓		200	446	GIF				✓
431	https://github.com	GET	/LogicalTrust/BurpPubl...	✓		200	3398	HTML				✓
432	https://github.com	GET	/LogicalTrust/BurpHttm...	✓		200	53813	HTML		GitHub - LogicalTrust...		✓
433	http://detectportal.firefox.c...	GET	/success.tx						txt			
434	https://avatars1.githubusercontent.com	GET	/u/403474...									✓
435	https://collector.githubapp...	GET	/github/pag...									✓
436	https://api.github.com	OPTIO...	/private/bi...									✓
437	https://www.google-analytic...	POST	/collect									✓
438	https://ani.github.com	POST	/private/bi...									✓

Request Response

Raw Params Headers Hex

GET /LogicalTrust/BurpHttpMock HTTP/1.1
Host: github.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS
Accept: text/html,application/xhtml+xml,application
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://github.com/LogicalTrust
Cookie: _ga=GA1.2.704795025.152975959; _octo=GH1
_gh_aaaa=HYVZclhPZu5um6CoIdbDdGK0eqs3U4vvdtohd
XtLdWQOguEQSTdJUnA4AGPBN1XcmdBGRKMFpyoX1LhNBLym
vdKxKSEVksFBOBHNTtLtkauEmOPNo2VOV2JfRANRSLByTcdh
d8d4cF8d7; _gat=1; _bz=Europe%2FWaraw
Connection: close
Upgrade-Insecure-Requests: 1

Mock HTTP response (URL without query)

Engagement tools [Pro version only]

Show new history window

Add comment

Highlight

Delete item

Clear history

Copy URL

Copy as curl command

Copy links

Save item

Proxy history help

Type a search term

0 matches

Demo!

Burp Suite Community Edition v1.7.35 - Temporary Project

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts HTTP Mock

☐ Debug output ☒ Advanced

Mock rules

Enabl...	Protoc...	Host	Port	File
<input checked="" type="checkbox"/>	HTTPS	^duckduckgo\.c...	^443\$	^/ac/"q=burp.*
<input checked="" type="checkbox"/>	HTTPS	^duckduckgo\.c...	^443\$	^/ac/"
<input checked="" type="checkbox"/>	HTTP	^detectportal\.fi...	^80\$	^/success\.txt\$
<input checked="" type="checkbox"/>	HTTPS	^twitter\.com\$	^443\$	^/LogicalTrust\$
<input checked="" type="checkbox"/>	HTTPS	^github\.com\$	^443\$	^/LogicalTrust/BurpHttpMock\$

Add
Delete
Paste URL
Duplicate
Up
Down

Response editor

```
HTTP/1.1 200 OK
Server: GitHub.com
Date: Fri, 06 Jul 2018 14:02:18 GMT
Content-Type: text/html; charset=utf-8
Connection: close
Status: 200 OK
Cache-Control: no-cache
Vary: X-PJAX
X-Runtime: 0.278951
Strict-Transport-Security: max-age=31536000; includeSubdomains; preload
X-Frame-Options: deny
X-Content-Type-Options: noaniff
Content-Length: 50192

<!DOCTYPE html>
<html lang="en">
<head>

<title>MOCK: GitHub - LogicalTrust/BurpHttpMock</title>

<meta name="description" content="GitHub is where people
build software. More than 28 million people use GitHub to
discover, fork, and contribute to over 85 million projects.">
<link rel="search"
type="application/opensearchdescription+xml"
href="/opensearch.xml" title="GitHub">
<link rel="fluid-icon"
href="https://github.com/fluidicon.png" title="GitHub">
<meta property="fb:app_id" content="1401488693436528">

<meta property="og:image"
content="https://avatars0.githubusercontent.com/u/30469831?s=400
&amp;v=4" />
<meta property="og:site_name" content="GitHub" />
<meta property="og:type" content="object" />
<meta property="og:title" content="LogicalTrust/BurpHttpMock" />
<meta property="og:url"
content="https://github.com/LogicalTrust/BurpHttpMock" />
<meta property="og:description" content="Contribute to BeroHttMock" />

? < > Type a search term 0 matches
Save Discard ☒ Recalculate Content-Length
```

<https://github.com/LogicalTrust/BurpHttpMock>

Installation

- In the BApp Store
 - Search “HTTP Mock”
- From my GitHub
 - Slightly faster updates
 - <https://github.com/ise-spolansky/BurpHttpMock>

[GitHub](#)



[PortSwigger BApp Store](#)



Questions?

Thank you!

2019-11-08
Shea Polansky
<https://polansky.co>
@0x5ca1e5

