# 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>**

, …

```
}
```

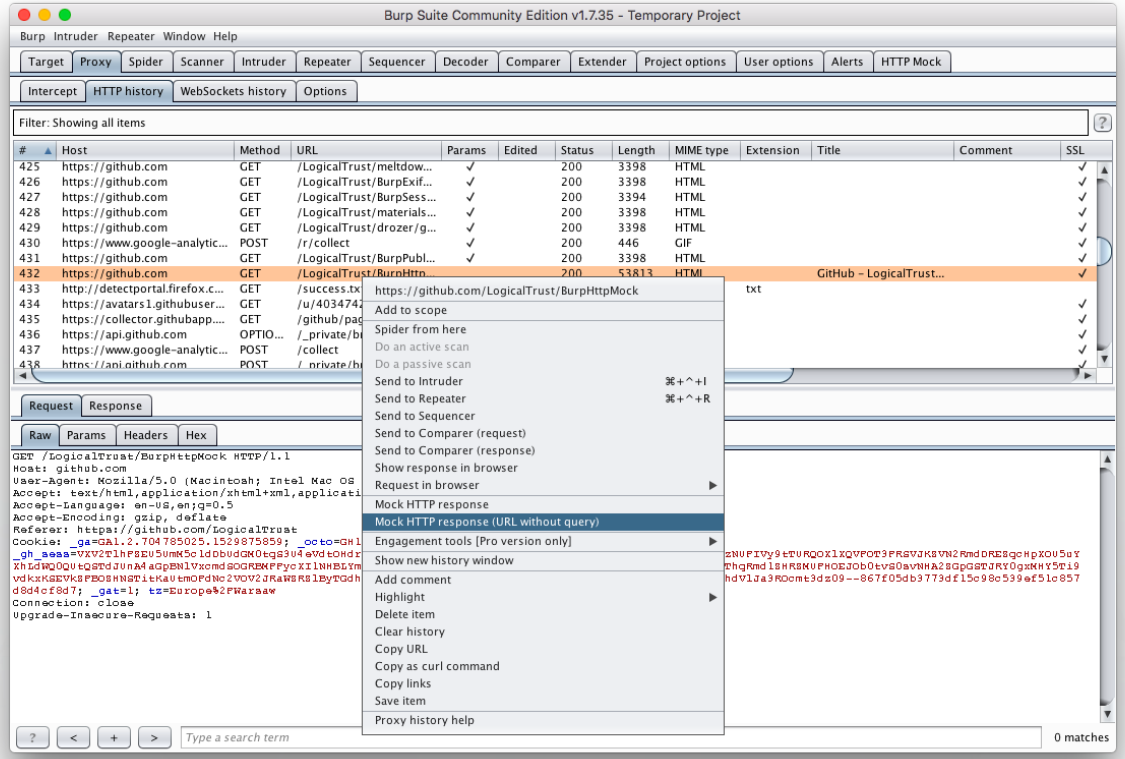
# Example Use Case: DRM Bypass

- 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!

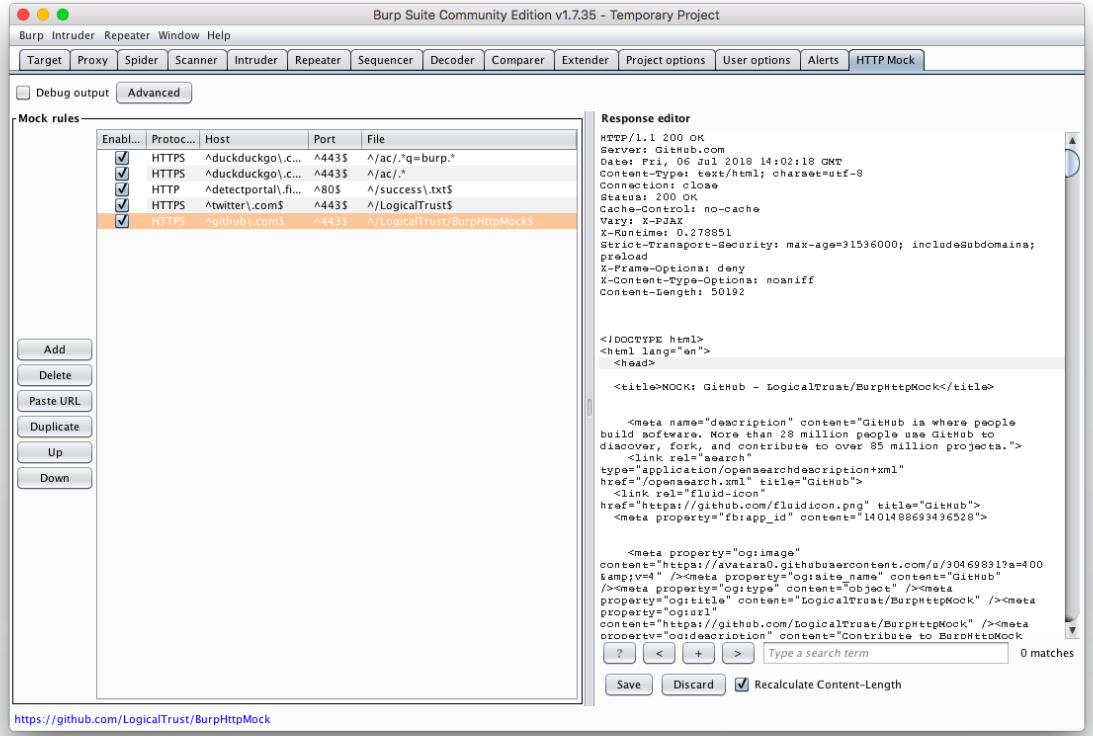
# Burp HTTP Mock Extension

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

# Demo!



# Demo!


Burp Suite Community Edition v1.7.35 - Temporary Project
Burp Intruder Repeater Window Help
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
HTTPS ^duckduckgo\.c... ^443$ ^/ac/.*q=burp.*
HTTPS ^duckduckgo\.c... ^443$ ^/ac/.*
HTTP ^detectportal\.fi... ^80$ ^/success\.txt$
HTTPS ^twitter\.com$ ^443$ ^/LogicalTrust$
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: 0.278851
Strict-Transport-Security: max-age=31536000; includeSubdomains; preload
X-Frame-Options: deny
X-Content-Type-Options: nosniff
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&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 BurpHttpMock
?
<
+
>
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

independent security evaluators