

Burp it up

by Santiago

This presentation is only for education purposes.

Before assessing a web application, ask for consent.

Agenda

1. Setup
2. Intro to BurpSuite
 - 2.1. BurpSuite Professional vs. Community Edition
3. A little bit of Hypertext Transfer Protocol (HTTP)
4. Using Burp
 - 4.1. Proxy
 - 4.2. Repeater
 - 4.3. Decoder
 - 4.4. Comparer
 - 4.5. Sequencer
 - 4.6. Intruder
 - 4.7. Extender
5. Resources and References

Setup

Setup

- Ubuntu 20.04
 - BurpSuite Community Edition
 - Docker
 - Damn Vulnerable Web Application (DVWA)



Intro to BurpSuite

Intro to BurpSuite

- Application designed for web application security assessments.
- Framework that includes tools and allows extensions.
- Included tools:
 - Proxy
 - Repeater
 - Decoder
 - Comparer
 - Sequencer
 - Intruder
 - Extender

BurpSuite Professional vs. Community Edition

Burp Suite Community Edition

Essential manual toolkit - perfect for learning more about AppSec.

- ✓ HTTP(s) / WebSockets proxy and history.
- ✓ Essential tools - Repeater, Decoder, Sequencer, and Comparer.
- ✓ Burp Intruder (demo).

- ✓ **Everything in Community Edition, plus ...**
- ✓ Project files (save your work).
- ✓ Orchestrate custom attacks (Burp Intruder - full version).
- ✓ Web vulnerability scanner.
- ✓ Pro-exclusive BApp extensions.
- ✓ Search function.
- ✓ Auto and manual OAST testing (Burp Collaborator).
- ✓ Automatically crawl and discover content to test.
- ✓ And much more ...

Burp Suite Professional

Faster, more reliable security testing for AppSec professionals.

BUY NOW - \$399

A little bit of Hypertext Transfer Protocol (HTTP)

A little bit of Hypertext Transfer Protocol (HTTP)

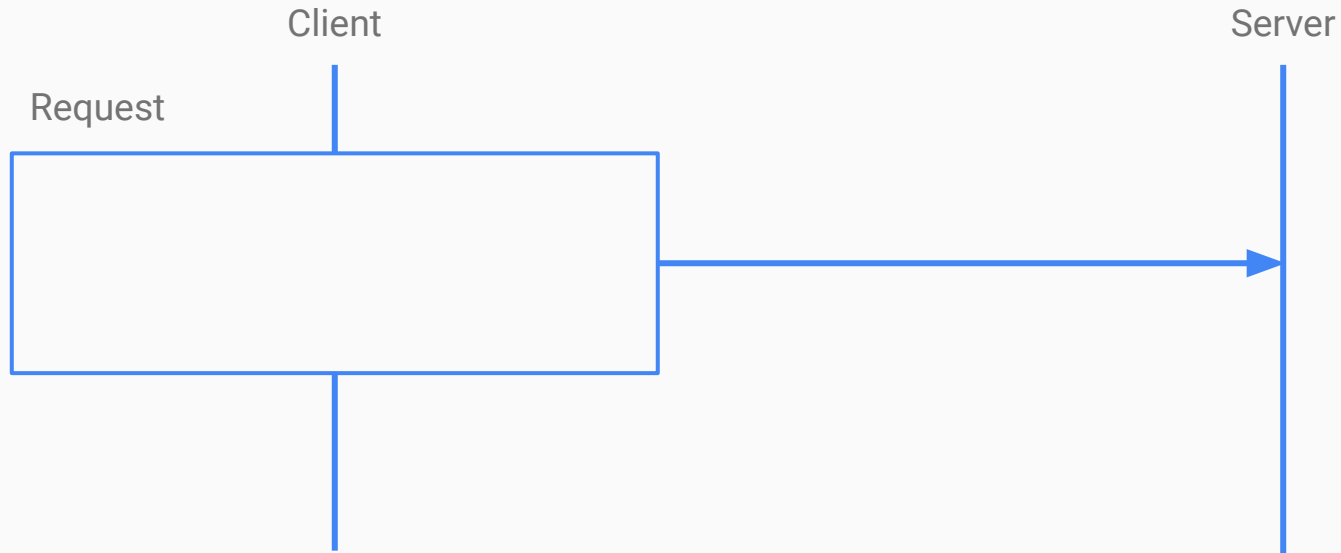
Client



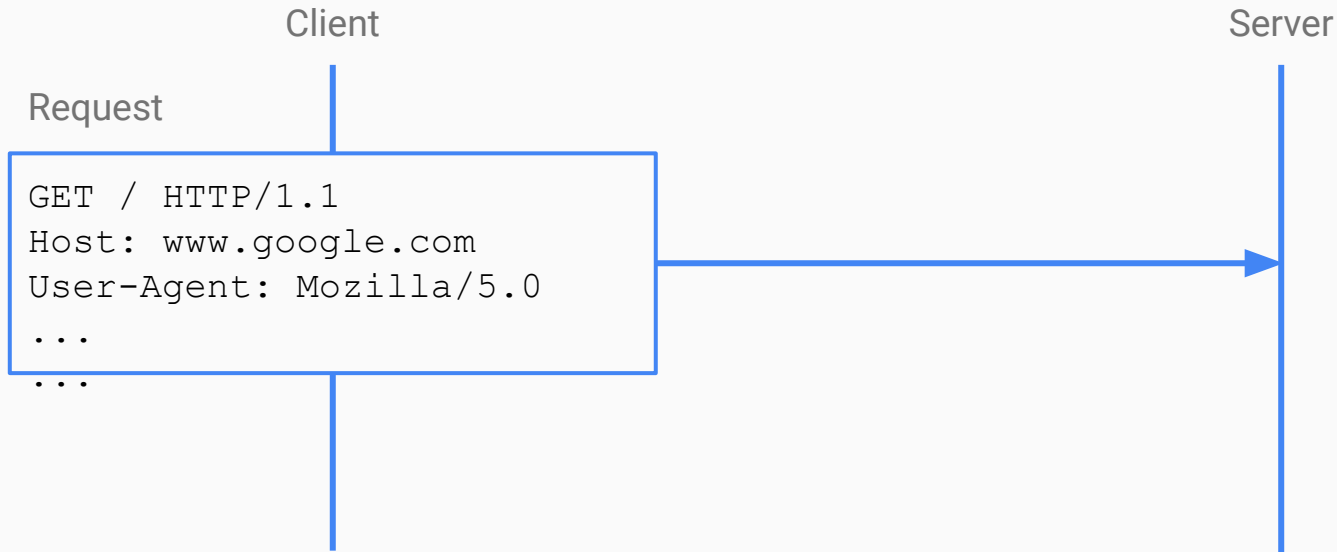
Server



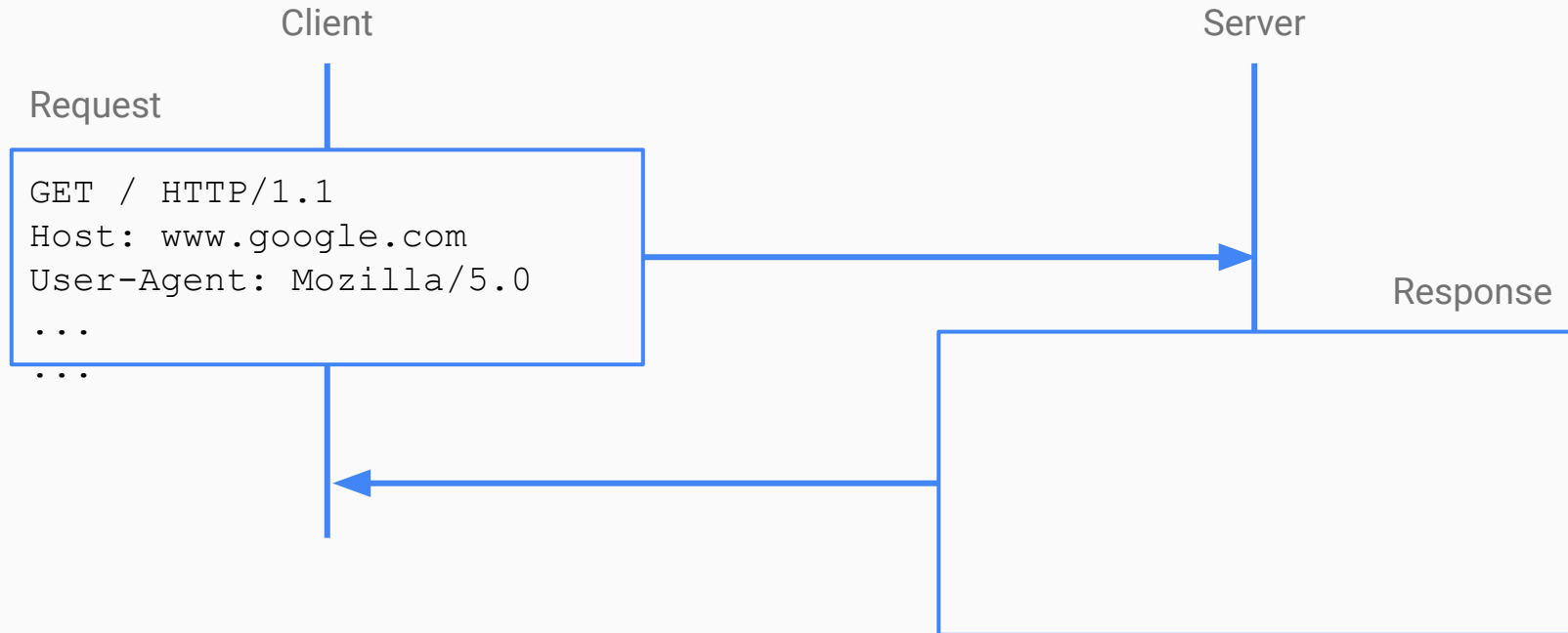
A little bit of Hypertext Transfer Protocol (HTTP)



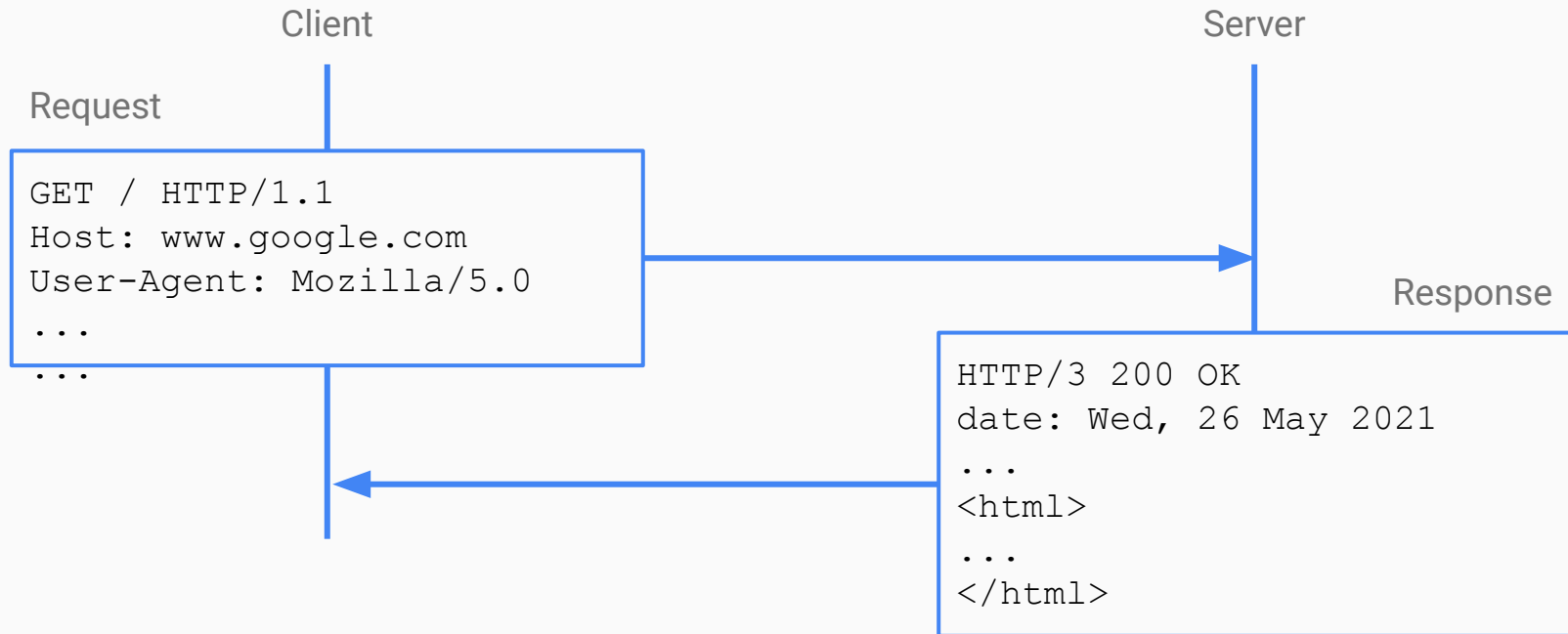
A little bit of Hypertext Transfer Protocol (HTTP)



A little bit of Hypertext Transfer Protocol (HTTP)



A little bit of Hypertext Transfer Protocol (HTTP)



Using BurpSuite

Proxy

Proxy:

- Application that sits between the client and the server.
- Might see and modify HTTP messages.

BurpSuite Proxy:

- Inspect and modify the content of HTTP requests before they are sent to the server.
- See the history of all the requests and its responses.
- Highlight requests in history.
- Send requests to other tools.

Repeater

- Re-send messages.
- Modify and send messages.
- Craft new messages and send them.
- Requests can be named and organized.
- Further modifications to request are tracked.

Decoder

- Encode and decode data into:
 - Base64
 - URL
 - Hex
 - Binary
- Hash data into:
 - MD2, MD4, MD5.
 - SHA1, SHA2, SHA3

Comparer

- Compare two different requests or two different responses.
- Highlights what has been modified, deleted, or added.

Sequencer

- Analyzes the entropy of data.
- Sends multiple requests and compare the randomness of the different responses.

Intruder

- Send multiple modified requests.
- Modifications are based on rules set by the analyst.

Types of attacks:

- Sniper
- Bettering
- Pitchfork
- Cluster bomb

- CE does not include the full version.
 - Throttled
 - No payloads

Extender

- Install external extensions to Burp.
- Extensions are used to handle information, or to add specific attacks
- Some of the extensions are only available to BurpSuite Pro.
- Users can develop extensions for BurpSuite in Java and Python.
- Python extensions need Jython.

Resources and References

Resources

Learn more about Web Security:

- Portswigger's Web Academy (Free)
 - Theory and exercises
 - <https://portswigger.net/web-security>

Practice Web Assessment:

- Hacker101(Free)
 - <https://www.hacker101.com/>
- Tryhackme (Freemium)
 - Guides and challenges
 - <https://tryhackme.com/>
- HackTheBox (Freemium)
 - <https://www.hackthebox.eu/>

References

<https://portswigger.net/burp/documentation/desktop/getting-started/installing-burp>

<https://www.digitalocean.com/community/tutorials/how-to-install-and-use-docker-on-ubuntu-20-04>

<https://github.com/digininja/DVWA>

<https://datatracker.ietf.org/doc/html/rfc2616>

<https://portswigger.net/burp/documentation/desktop/tools/intruder/positions>

<https://github.com/danielmiessler/SecLists>

<https://github.com/swisskyrepo/PayloadsAllTheThings>

<https://www.jython.org>