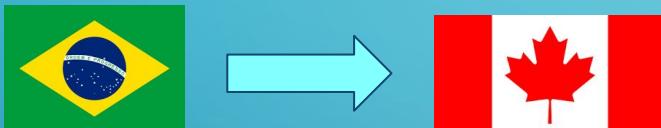


Web Hacking 101: Burping for fun and maybe some profit

Magno (Logan) Rodrigues

magnologan at gmail dot com

“WHO AM I? ARE YOU SURE YOU WANNA KNOW?”
- Parker, Peter (Spider Man 2002)



InfoSec/AppSec Specialist / CompTIA Instructor

Focusing on AppSec Testing, DevSecOps and Secure Coding

Founder of JampaSec and OWASP Paraíba - www.jampasec.com

Speaker at TheLongCon, RoadSecSP, MindTheSecRJ, BSidesSP...

Martial Artist, Investor, Gamer and Bug Bounty Hunter

Agenda

- Web Hacking 101
 - Intro & Timeline
 - Requests & Responses
 - Headers & Methods
 - Status Codes, Sessions & Cookies
 - Encoding x Hashing x Crypto
 - Proxy & Web Proxy
- BurpSuite Community v2
 - Proxy & Target
 - Dashboard & Spider
 - Intruder & Repeater
 - Comparer & Decoder



Disclaimer #1

I'm not a BurpSuite Expert!

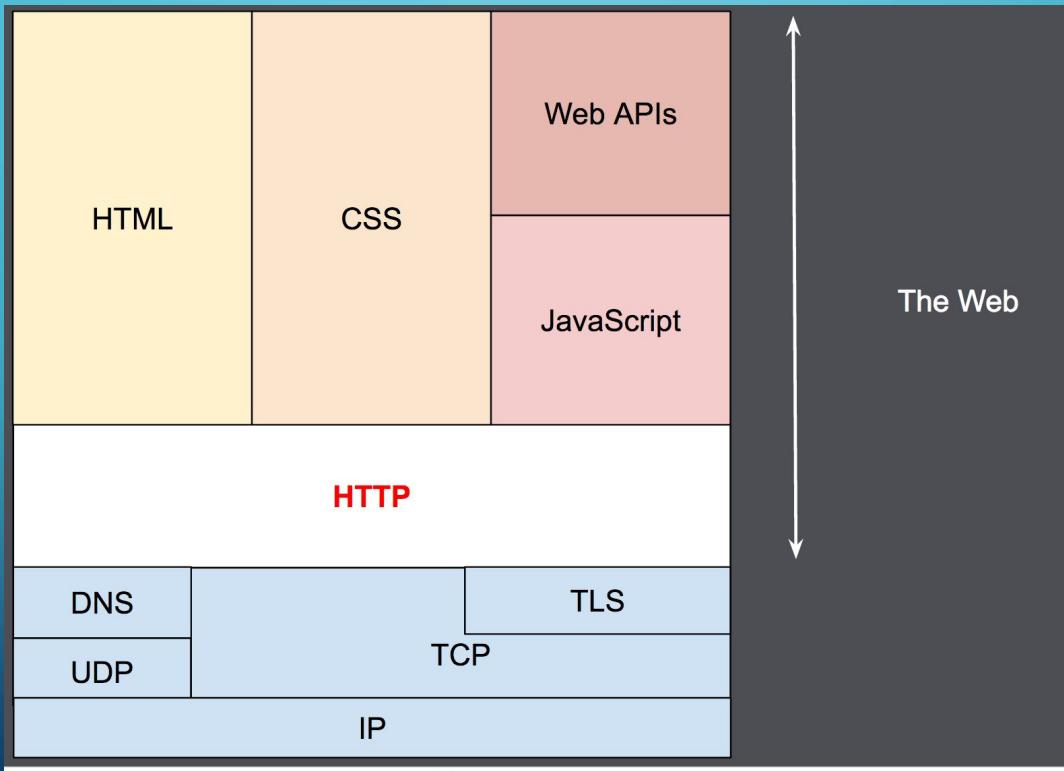


Disclaimer #2

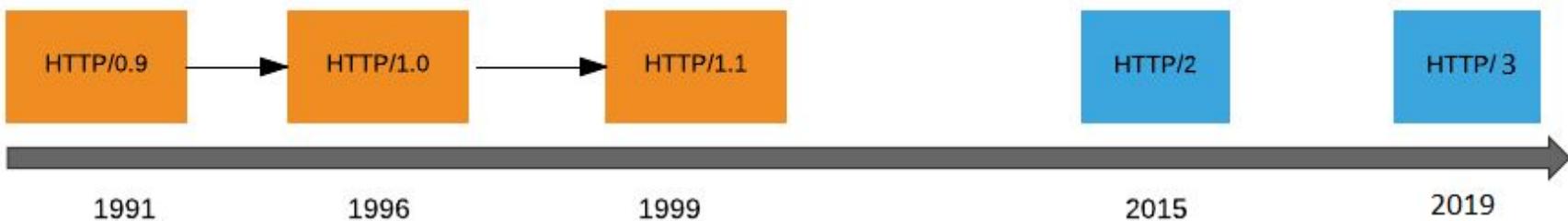
Why not OWASP ZAP?



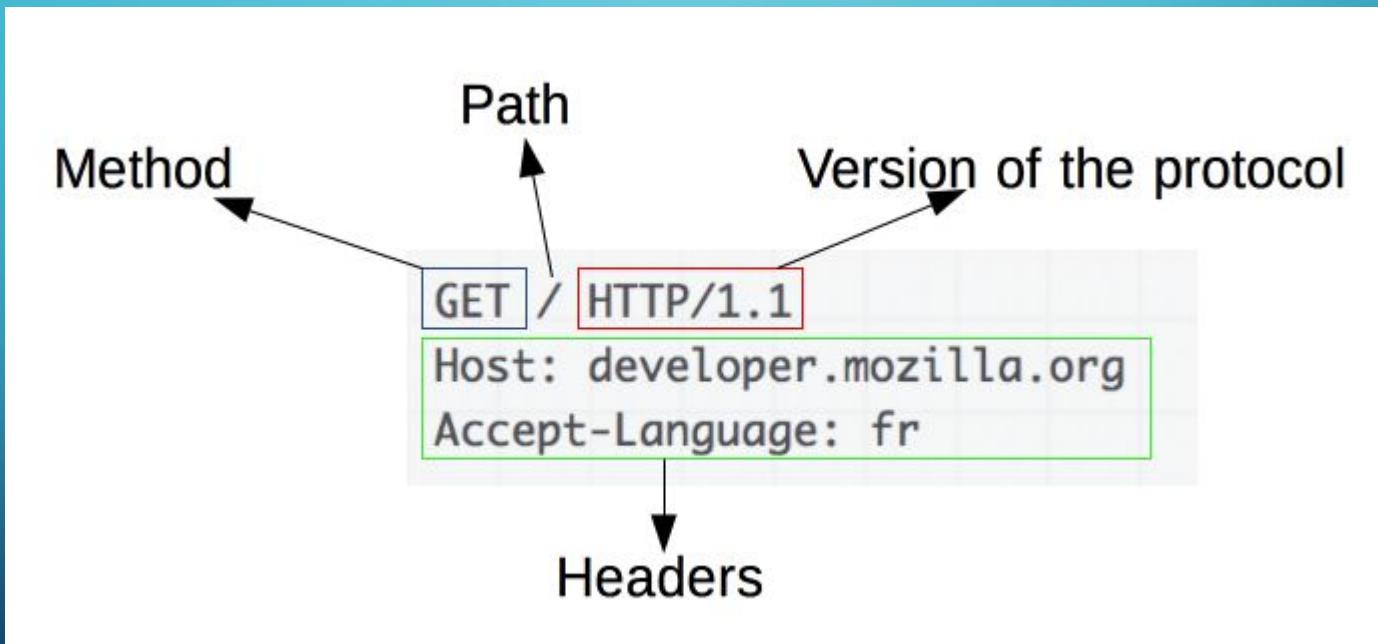
HTTP 101 - Intro



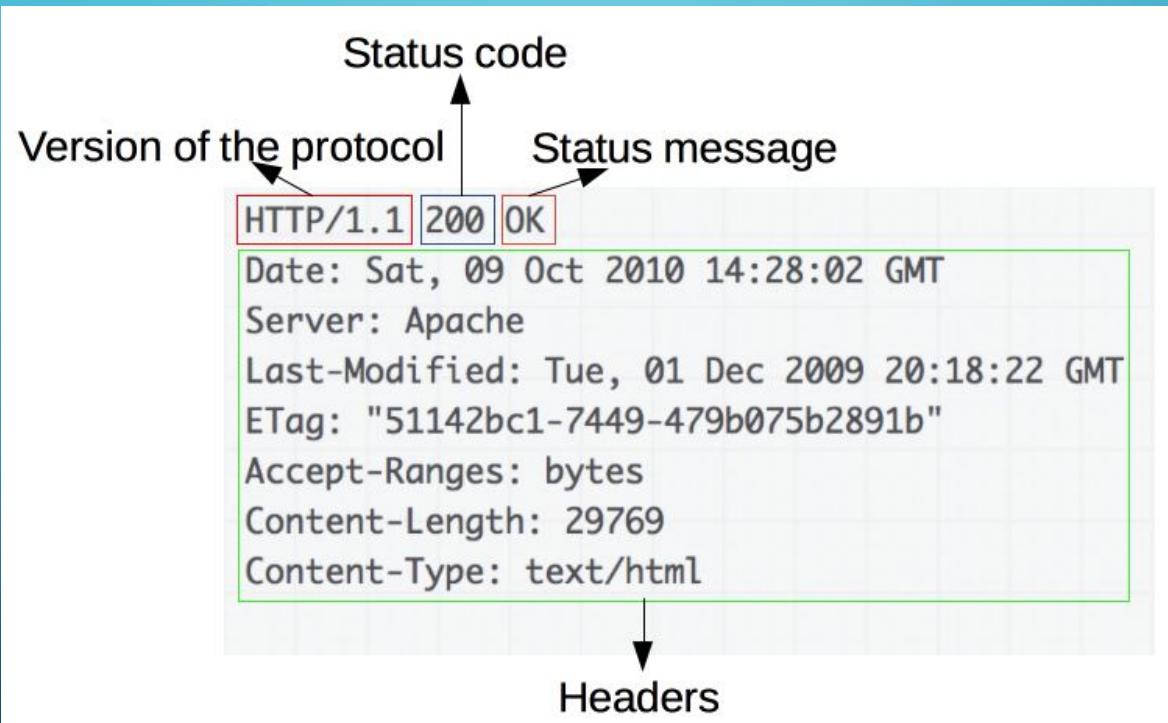
HTTP 101 - Timeline



Request - Client



Response - Server



HTTP Requests Demo

HTTP Headers

- Allow the client and the server to pass additional information with the request or the response
- Used in **Name:Value** format
- Can be grouped in four different categories:
 - General Header
 - Request Header
 - Response Header
 - Entity Header

HTTP Methods

- GET - Request data from a specific resource.
Ex: GET /form.php?param1=x¶m2=y
- POST - Send data to be processed
Ex: POST /form.php HTTP / 1.1
Host: www.site.ca
param1=x¶m2=y

Other HTTP Methods

HEAD - Same as GET but only returns headers

PUT - Puts a certain resource on the server.

DELETE - Remove certain resource.

OPTIONS - Returns the methods supported by server

TRACE - Echoes the received request to check if any changes have been made by intermediate servers.

HTTP Status Codes

They are divided into 5 categories:

- Informational (100-199)
- Success (200-299)
- Redirect (300-399)
- Client Error (400-499)
- Server Error (500-599)

Sessions and Cookies

- To manage the client session (Session ID)
- Reminds server of user and their preferences
- Are subject to capture, manipulation and fraud, if not protected
- Widely used in most web applications today



Encoding x Hash x Crypto

- Encoding - HTML, URL, Unicode, Base64

Not encryption, can be reversed. Ex: dGhlbG9uZ2Nvbgo=

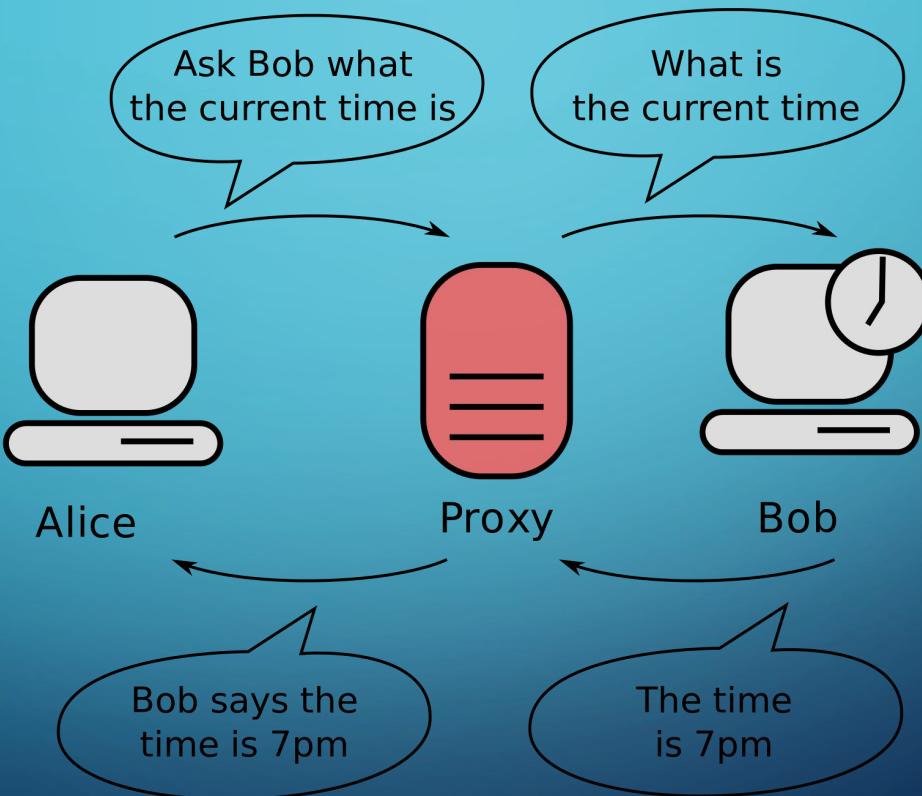
- Hash - SHA-1, SHA-2, bcrypt, scrypt, PBKDF2, argon2

It's not encryption, it's one-way functions and can't be reversed. Used for integrity and passwords. Ex: 9E107D9D372BB6826BD81D3542A419D6

- Encryption - DES, RSA, AES

Encryption itself can be reversed but need the cryptographic key. Used mostly for Confidentiality. Can be Symmetric or Asymmetric

Proxy

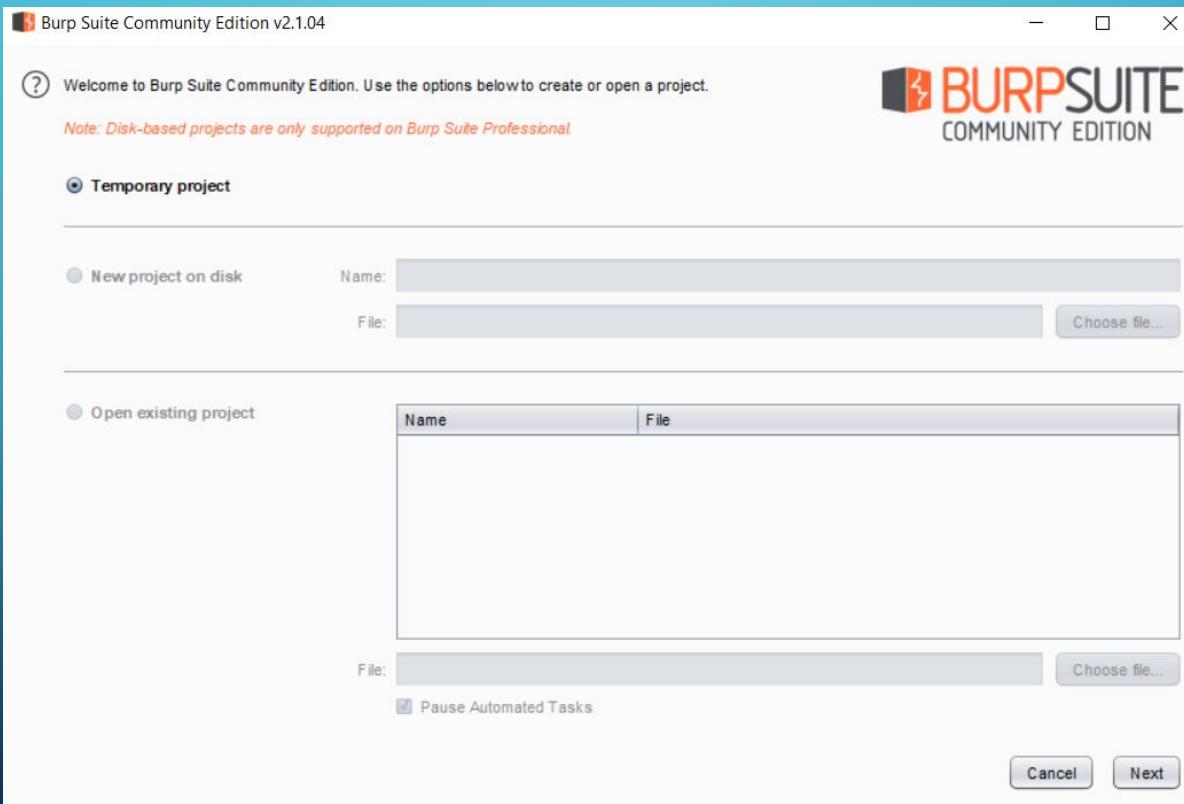


Burp Suite

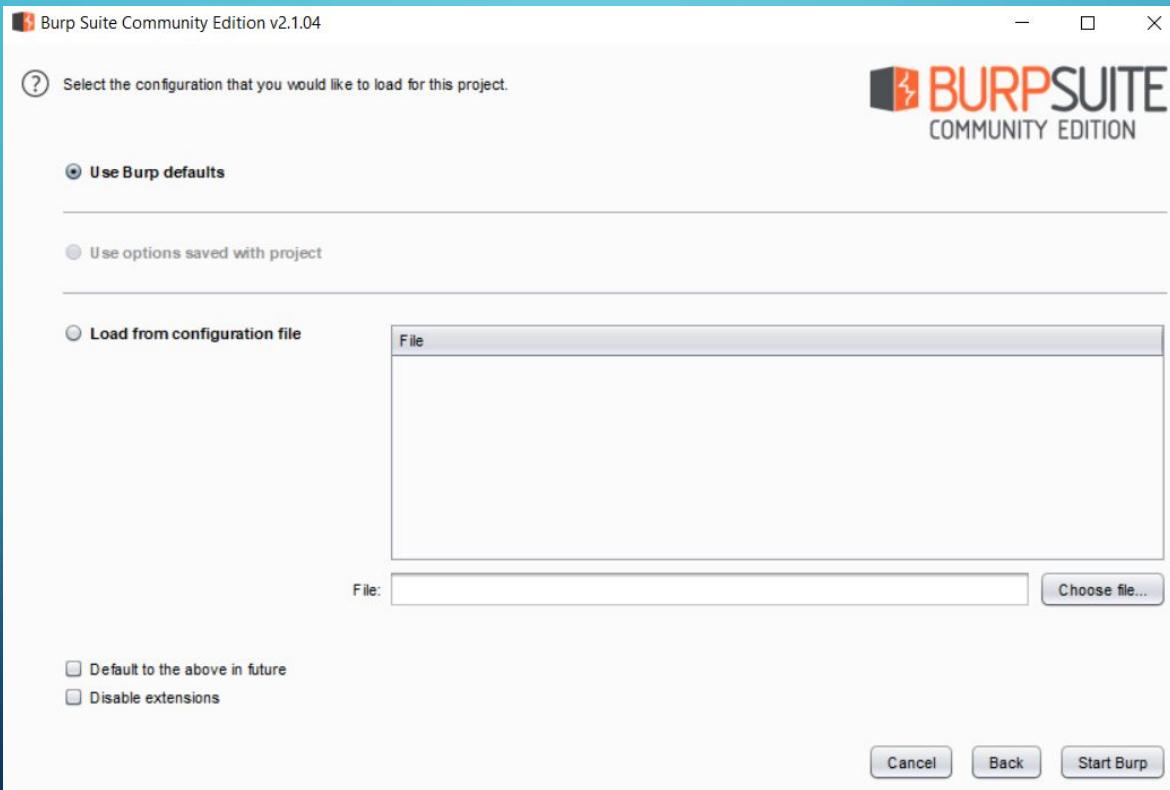


- It is an intercepting HTTP proxy (and WebSockets)
- An integrated platform for performing security testing of web applications
- Developed and maintained by PortSwigger
- It currently has three editions: Community, Professional and Enterprise
- Written in Java

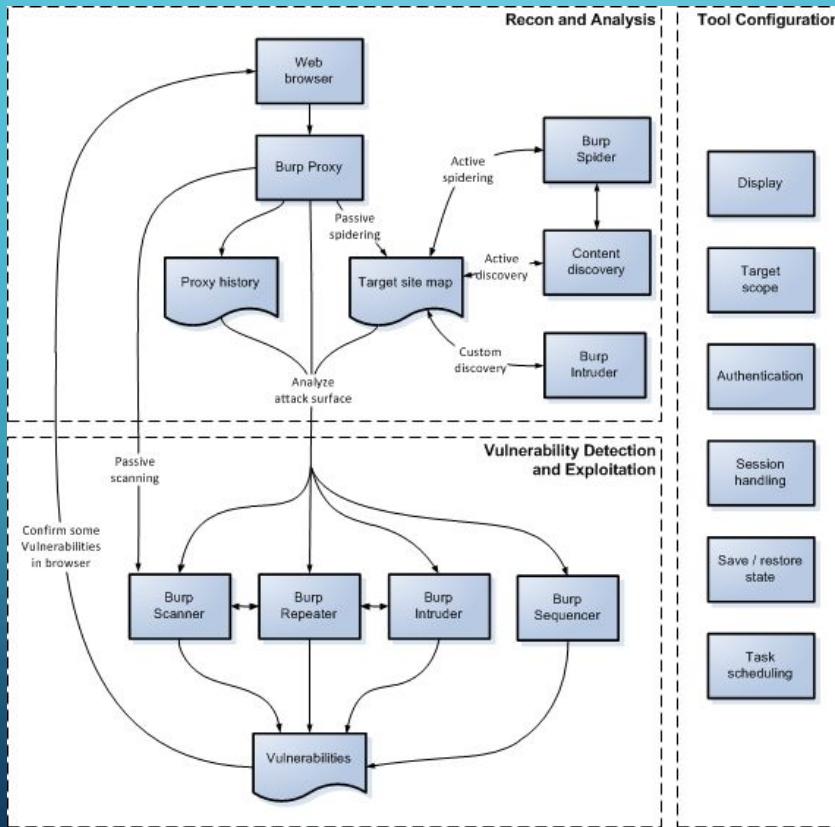
Burp Suite Community



Burp Suite Community



Burp Pentest Workflow



OWASP Vulnerable Web Applications Directory Project

App Name / Link	Technology	Author	Notes
Acuart	PHP	Acunetix	Art shopping
Acublog	.NET	Acunetix	Blog
Acuforum	ASP	Acunetix	Forum
Altoro Mutual		IBM/Watchfire	(jsmith/Demo1234)
BGA Vulnerable BANK App	.NET	BGA Security	
Crack Me Bank		Trustwave	
Enigma Group		Enigma Group	
Gruyere	Python	Google	
Firing Range		Google	Source code
Hackademic Challenges Project	PHP - Joomla	OWASP	
Hacker Challenge		PCTechtips	
Hackazon	AJAX, JSON, XML, Gwt, AMF	NTObjectives	Project page
Hacking Lab		Hacking Lab	
Hack.me		eLearnSecurity	Beta
HackThisSite		HackThisSite	Basic & Realistic (web) Missions
hackxor			First 2 levels online (algo/smurf), rest offline
Juice Shop	Javascript	OWASP	Demo instance. Do not use for massive attacks/scans!

https://www.owasp.org/index.php/OWASP_Vulnerable_Web_Applications_Directory_Project

Burp Demo

Burp Suite Configuration

- Use a browser extension like FoxyProxy or SwitchyOmega to quickly enable or disable Burp
- Make sure you add Burp's SSL certificate to the browser
- Other things that might be useful:
 - Add your target to the scope
 - Disable browser XSS Protection
 - Disable intercept by default

Burp Suite Documentation

The screenshot shows the Burp Suite Documentation homepage. The left sidebar has a dark header with the Burp Suite logo and "Burp Suite Documentation". Below it is a navigation menu with the following structure:

- Documentation** (highlighted in orange)
- Desktop editions** (highlighted in orange)
- ▶ Getting started
- ▶ Scanning web sites
- ▶ Penetration testing
 - Mobile testing
 - Extensibility
 - Troubleshooting
- ▶ Dashboard
- ▶ Tools
- ▶ Useful functions
- ▶ Options
- ▶ Scanner
- ▶ Burp Collaborator
- ▶ Burp Infiltrator
- Contents

The main content area has a light gray background. At the top, there is a breadcrumb trail: [Support Center](#) >> [Documentation](#). Below the breadcrumb are three tabs: **Enterprise** (purple), **Professional** (blue), and **Community** (gray). The **Burp Suite documentation** section is highlighted in red. A descriptive paragraph follows, along with links to other documentation pages.

Burp Suite documentation

This documentation describes the functionality of all editions of Burp Suite and related components. Use the links below to get started:

[Burp Suite Professional and Community editions](#) >>
[Burp Suite Enterprise Edition](#) >>
[Burp Scanner](#) >>
[Burp Collaborator](#) >>
[Burp Infiltrator](#) >>
[Full documentation contents](#) >>

Extender - BApp Store

B Burp Suite Community Edition v2.1.04 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Extensions BApp Store APIs Options

BApp Store

The BApp Store contains Burp extensions that have been written by users of Burp Suite, to extend Burp's capabilities.

Name	Installed	Rating	Popularity	Last updated	Detail
.NET Beautifier		★★★★★	—	23 Jan 2017	
Add Custom Header		★★★★★	—	18 Sep 2018	
Additional CSRF Checks		★★★★★	—	14 Dec 2018	
Attack Surface Detector		★★★★★	—	08 Mar 2019	
AuthMatrix		★★★★★	—	02 Feb 2018	
Autz		★★★★★	—	01 Jul 2014	
Auto Repeater	✓	★★★★★	—	04 Apr 2018	
Auto-Drop Requests		★★★★★	—	07 Oct 2019	
Authorize		★★★★★	—	28 Nov 2018	
AWS Signer		★★★★★	—	18 Oct 2019	
Blazer		★★★★★	—	01 Feb 2017	
Bradamsa		★★★★★	—	02 Jul 2014	
Brida, Burp to Frida bridge		★★★★★	—	04 Oct 2018	
Browser Repeater		★★★★★	—	01 Jul 2014	
Burp Chat		★★★★★	—	23 Jan 2017	
Burp CSJ		★★★★★	—	23 Mar 2015	
BurpeFish		★★★★★	—	21 Nov 2018	
BurpSmartBuster		★★★★★	—	22 Jan 2016	
Bypass WAF		★★★★★	—	29 Mar 2017	
C02		★★★★★	—	20 Jul 2017	
Command Injection Attacker		★★★★★	—	27 Jun 2018	
Commentator		★★★★★	—	16 Jul 2018	
Content Type Converter		★★★★★	—	23 Jan 2017	
Copy as Node Request		★★★★★	—	09 Apr 2019	
Copy as PowerShell Requests		★★★★★	—	31 Jan 2018	
Copy As Python-Requests		★★★★★	—	18 Jun 2019	
CSP Auditor		★★★★★	—	15 Aug 2017	
CSRF Token Tracker		★★★★★	—	14 Feb 2017	
CSurfer		★★★★★	—	10 Nov 2015	
Custom Logger		★★★★★	—	01 Jul 2014	
Custom Parameter Handler		★★★★★	—	10 Apr 2019	
Custom Send To		★★★★★	—	18 Jun 2019	
CustomSerializer		★★★★★	—	06 Feb 2017	
CVSS Calculator		★★★★★	—	30 Mar 2017	
Decoder Improved		★★★★★	—	30 Oct 2019	
Decompressor		★★★★★	—	19 Jun 2018	

.NET Beautifier

This extension beautifies .NET requests to make the body parameters more human readable. Built-in parameters like __VIEWSTATE have their values masked. Form field names have the auto-generated part of their name removed.

Requests are only beautified in contexts where they can be edited, such as the Proxy intercept view.

For example, a .NET request with the following body:

```
__VIEWSTATE=%2ciAIHfchohsdigjKLASgjhaklgjSDGsjdg1SDJg9SDJGsdgjSGJDDsasdfja0sdjfja
... (1000 lines later) ...
&ct100%24ctl00%24InnerContentPlaceHolder%24Element_42%24ctl100%24FrmLogin%24TxtUsername_intern
al%username%ct100%24ctl00%24InnerContentPlaceHolder%24Element_42%24ctl100%24FrmLogin%24TxtPass
word_internal=password&ct100%24ctl100%24InnerContentPlaceHolder%24Element_42%24ctl100%24BtnLogi
n=Login
```

will be displayed like this:

```
__VIEWSTATE=&TxtUsername_internal=username&TxtPassword_internal=password&BtnLogin=Login
```

This is done without compromising the integrity of the underlying message so you can edit parameter values and the request will be correctly reconstructed. You can also send the beautified messages to other Burp tools, and they will be handled correctly.

Author: Nadeem Douba
Version: 0.3
Source: <https://github.com/portswigger/dotnet-beautifier>
Updated: 23 Jan 2017

Rating: ★★★★★ Submit rating
Popularity: —

Install

Refresh list Manual install ...

Proxy - Options

Burp Suite Community Edition v2.1.04 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Intercept HTTP history WebSockets history Options

Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.

Running	Interface	Invisible	Redirect	Certificate
<input checked="" type="checkbox"/>	127.0.0.1:8090			Per-host

Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating SSL connections. You can import or export this certificate for use in other tools or another installation of Burp.

Import / export CA certificate Regenerate CA certificate

Proxy - Intercept

Burp Suite Community Edition v2.1.04 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Intercept HTTP history WebSockets history Options

Request to http://zero.webappsecurity.com:80 [54.82.22.214]

Forward Drop Intercept is on Action

Raw Headers Hex

```
GET / HTTP/1.1
Host: zero.webappsecurity.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:70.0) Gecko/20100101 Firefox/70.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Proxy - HTTP History

Burp Suite Community Edition v2.1.04 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Intercept HTTP history WebSockets history Options

Logging of out-of-scope Proxy traffic is disabled [Re-enable](#)

Filter: Hiding CSS, image and general binary content [?](#)

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	SSL	IP	C
1	http://zero.webappsecurity.com	GET	/			200	12755	HTML		Zero - Personal Banking ...			54.82.22.214	
2	http://zero.webappsecurity.com	GET	/robots.txt			404	1194	HTML	txt	Apache Tomcat/7.0.70 - ...			54.82.22.214	
6	http://zero.webappsecurity.com	GET	/resources/js/jquery-1.8.2.min.js			200	93816	script	js				54.82.22.214	
7	http://zero.webappsecurity.com	GET	/resources/js/placeholders.min.js			200	5993	script	js				54.82.22.214	
8	http://zero.webappsecurity.com	GET	/resources/js/bootstrap.min.js			200	27278	script	js				54.82.22.214	
13	http://zero.webappsecurity.com	GET	/favicon.ico			404	1196	HTML	ico	Apache Tomcat/7.0.70 - ...			54.82.22.214	
14	http://zero.webappsecurity.com	GET	/			200	12755	HTML		Zero - Personal Banking ...			54.82.22.214	
18	http://zero.webappsecurity.com	GET	/resources/js/placeholders.min.js			304	142	script	js				54.82.22.214	
19	http://zero.webappsecurity.com	GET	/resources/js/bootstrap.min.js			304	143	script	js				54.82.22.214	
20	http://zero.webappsecurity.com	GET	/resources/js/jquery-1.8.2.min.js			304	143	script	js				54.82.22.214	

Proxy - HTTP History

Filter: Hiding CSS, image and general binary content



Filter by request type

- Show only in-scope items
- Hide items without responses
- Show only parameterized requests

Filter by MIME type

- HTML Other text
- Script Images
- XML Flash
- CSS Other binary

Filter by status code

- 2xx [success]
- 3xx [redirection]
- 4xx [request error]
- 5xx [server error]

Filter by search term [Pro only]

-
- Regex
- Case sensitive
- Negative search

Filter by file extension

- Show only:
- Hide:

Filter by annotation

- Show only commented items
- Show only highlighted items

Filter by listener

-
- Port

Show all

Hide all

Revert changes

Dashboard v2.x

Burp Suite Community Edition v2.1.04 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options

Tasks

+ New scan + New live task II G ? New live task

Filter Running Paused Finished

1. Live passive crawl from Proxy (all traffic)

Add links. Add item itself, same domain and URLs in suite scope.

Capturing:

15 items added to site map
23 responses processed
0 responses queued

Scan details Scan configuration Resource pool

Task Type

- Live audit (Pro version only)
- Live passive crawl

Choose predefined task...

Tools Scope

Select the tools whose traffic will be inspected to select items that are processed by the live task.

- Proxy
- Repeater
- Intruder

URL Scope

Define which items are processed by the live task, based on their URL.

- Everything
- Suite scope
- Custom scope

Deduplication

Select whether items to be processed are deduplicated based on their URL and parameter names. Use this option to avoid processing the same item more than once.

- Ignore duplicate items based on URL and parameter names



Spidering

Target - Site Map

Burp Suite Community Edition v2.1.04 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Site map Scope Issue definitions

Logging of out-of-scope Proxy traffic is disabled Re-enable

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders ?

Host	Method	URL	Params	Status	Length	MIME type	Title	Comment	Time requested
http://zero.webappsecurity.com	GET	/		200	12755	HTML	Zero - Personal Banking ...		21:44:04 1 N
	GET	/index.html		200	27278	script			21:44:04 1 N
resources	GET	/resources/js/bootstrap....		200	93816	script			21:44:04 1 N
	GET	/resources/js/jquery-1.8....		200	5993	script			21:44:04 1 N
	GET	/resources/js/placeholde...		200					
	GET	/index.html							
	GET	/search.html							

Request Response

Raw Headers Hex

GET / HTTP/1.1
Host: zero.webappsecurity.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:70.0) Gecko/20100101 Firefox/70.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1

Target - Scope

Burp Suite Community Edition v2.1.04 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Site map Scope Issue definitions

Target Scope

Define the in-scope targets for your current work. This configuration affects the behavior of tools throughout the suite. The easiest way to configure scope is to browse to your target and use the context menus in the site map to include or exclude URL paths.

Use advanced scope control

Include in scope

Enabled	Prefix
<input checked="" type="checkbox"/>	http://zero.webappsecurity.com/

Exclude from scope

Enabled	Prefix

Intruder - Target

Burp Suite Community Edition v2.1.04 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

1 × ...

Target Positions Payloads Options

Attack Target

Configure the details of the target for the attack.

Host: 127.0.0.1

Port: 80

Use HTTPS

Start attack

Intruder - Positions

Burp Suite Community Edition v2.1.04 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

1 × ...

Target Positions Payloads Options

Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Start attack

Attack type: Sniper

```
POST /example?p1=$p1val$p2=$p2val$ HTTP/1.0
Cookie: c=$cval$
Content-Length: 17
$p3=$p3val$p4=$p4val$
```

Add \$ Clear \$ Auto \$ Refresh

Intruder - Payloads

The screenshot shows the Burp Suite Community Edition v2.1.04 interface, specifically the Intruder - Payloads tab. The window title is "Burp Suite Community Edition v2.1.04 - Temporary Project". The menu bar includes Burp, Project, Intruder, Repeater, Window, and Help. The top navigation bar has tabs for Dashboard, Target, Proxy, Intruder (which is selected), Repeater, Sequencer, Decoder, Comparer, Extender, Project options, User options, and AutoRepeater. Below the navigation bar, there are three tabs: Login, Test (selected), and Under the Test tab, there are four sub-tabs: Target, Positions, Payloads (selected), and Options.

Payload Sets

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

Payload set: Payload count: 100
Payload type: Request count: 500

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:
Howmany:

Start attack

Intruder - Options

The screenshot shows the Burp Suite Community Edition interface with the title bar "Burp Suite Community Edition v2.1.04 - Temporary Project". The menu bar includes "Burp", "Project", "Intruder", "Repeater", "Window", and "Help". The top navigation bar has tabs for "Dashboard", "Target", "Proxy", "Intruder" (which is selected), "Repeater", "Sequencer", "Decoder", "Comparer", "Extender", "Project options", "User options", and "AutoRepeater". Below the tabs are two dropdown menus: "Login" and "Test". The main content area has tabs for "Target", "Positions", "Payloads", and "Options" (which is selected). The "Request Headers" section contains a note about updating headers during attacks, with two checked checkboxes: "Update Content-Length header" and "Set Connection: close". A "Start attack" button is located in the top right of this section. The "Request Engine" section contains a note about engine settings for attacks, followed by several configuration fields: "Number of threads" (set to 1), "Number of retries on network failure" (set to 3), "Pause before retry (milliseconds)" (set to 2000), "Throttle (milliseconds)" (radio button set to "Fixed" with value 0, and "Variable" option with start at 0 and step at 30000), and "Start time" (radio button set to "Immediately", and "Paused" option).

Repeater

Burp Suite Community Edition v2.1.04 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options AutoRepeater

1 × ...

Send Cancel < | > | Response Target: http://zero.webappsecurity.com

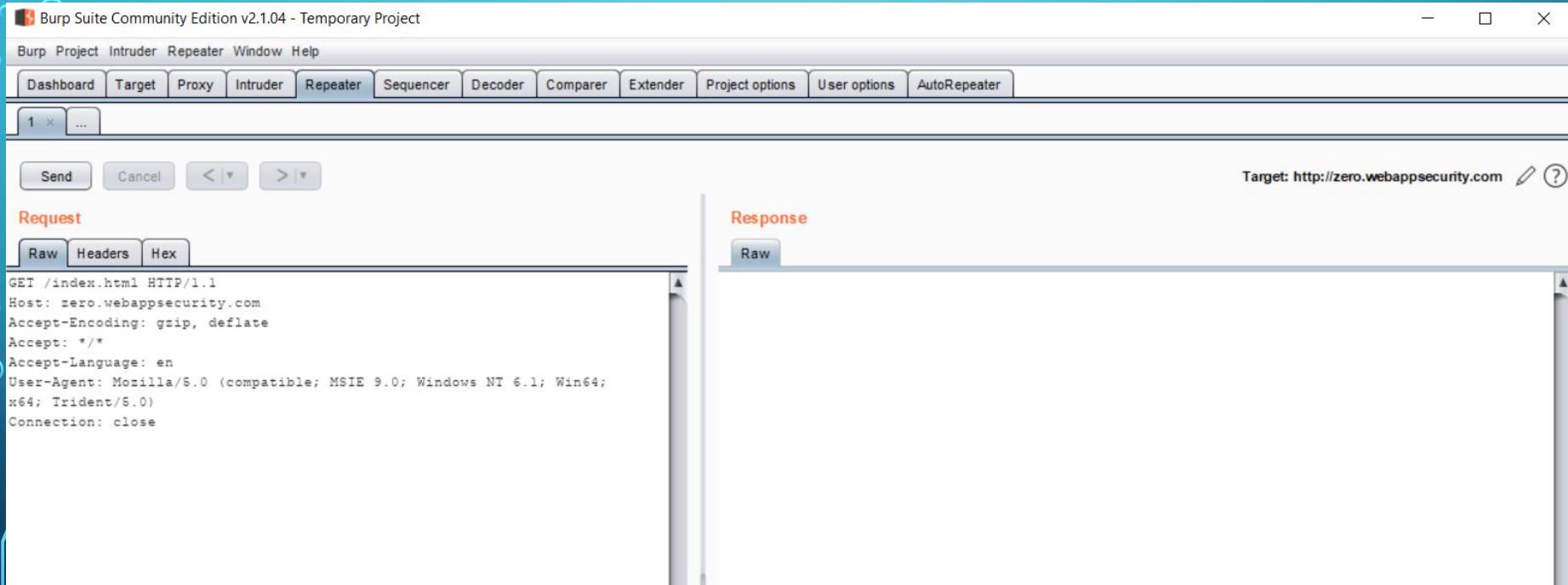
Request

Raw Headers Hex

```
GET /index.html HTTP/1.1
Host: zero.webappsecurity.com
Accept-Encoding: gzip, deflate
Accept: /*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64;
x64; Trident/5.0)
Connection: close
```

Response

Raw



Comparer

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
1	563	GET /customer/portal/theme_attachments/24245?cb=1487754866309 HTTP/1.1 Host: support.portswigger.net User-Agent: Mozilla/5...
2	256	GET /robots.txt HTTP/1.1 Host: support.portswigger.net User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:70.0) Gecko/201...

Paste Load Remove Clear

Select item 2:

#	Length	Data
1	563	GET /customer/portal/theme_attachments/24245?cb=1487754866309 HTTP/1.1 Host: support.portswigger.net User-Agent: Mozilla/5...
2	256	GET /robots.txt HTTP/1.1 Host: support.portswigger.net User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:70.0) Gecko/201...

Compare ... Words Bytes

Decoder

Burp Suite Community Edition v2.1.04 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options AutoRepeater

TheLongCon2019

VGhITG9uZ0NvbjlwMTk=

Text Hex ?
Decode as ...
Encode as ...
Hash ...
Smart decode

Text Hex ?
Decode as ...
Encode as ...
Hash ...
Smart decode

Next Steps

Take a look at Burp's Extensions:

- Auto-Repeater
- Turbo Intruder

Checkout The Cyber Mentor's Web Hacking Course:

https://www.youtube.com/playlist?list=PLKKT_MCUeixCoi2jtP2Jj8nZzM4MOzBL

Thank you! Obrigado!

Questions?

Contacts:

@magnologan

magnologan at gmail dot com



References

WAHH v2 - <https://www.amazon.ca/Web-Application-Hackers-Handbook-Exploiting/dp/1118026470>

Tangled Web - <https://www.amazon.ca/Tangled-Web-Securing-Modern-Applications/dp/1593273886/>

Hacker 101 - <https://www.hacker101.com/>

BugCrowd University - https://github.com/bugcrowd/bugcrowd_university

Web Security Academy - <https://portswigger.net/web-security>

The Amazing Burp Suite - Ricardo Iramar - BSides SP 0xF