

A decorative graphic on the left side of the slide consisting of white and light blue lines that resemble a circuit board or a network diagram, with small circles at various points.

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!

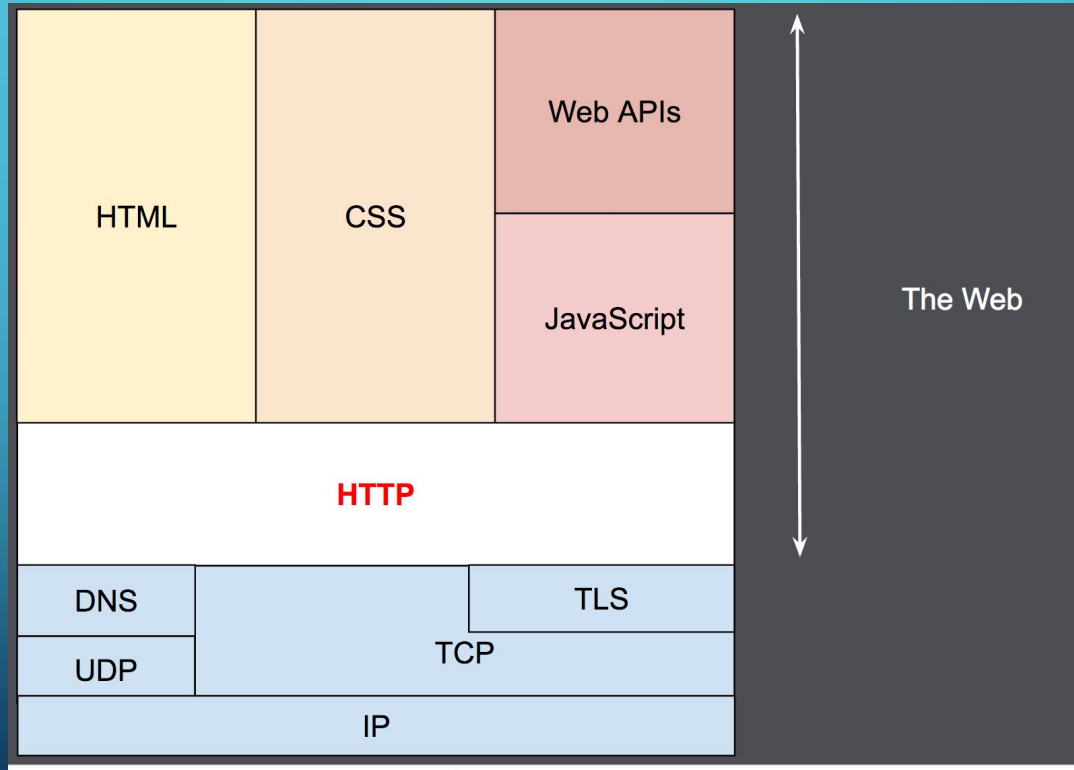


Disclaimer #2

Why not OWASP ZAP?

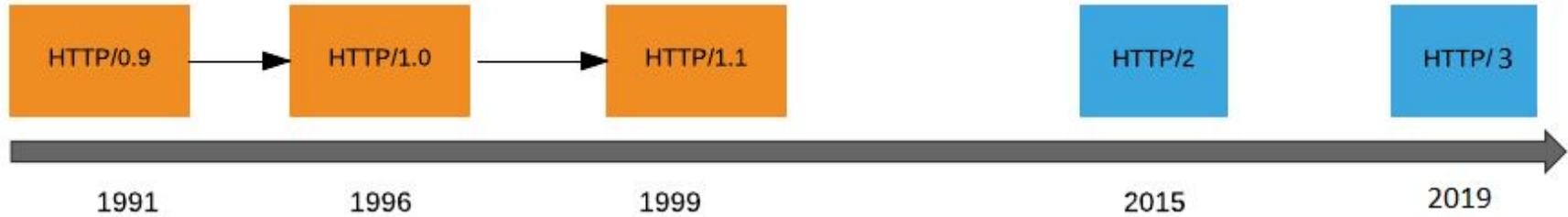


HTTP 101 - Intro

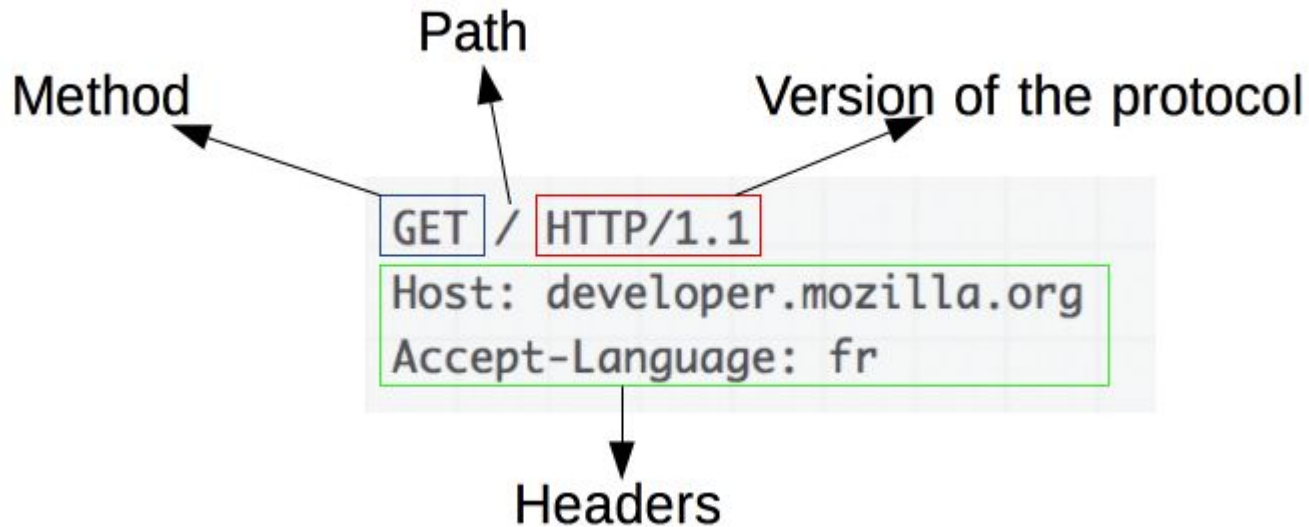


<https://developer.mozilla.org/en-US/docs/Web/HTTP/Overview>

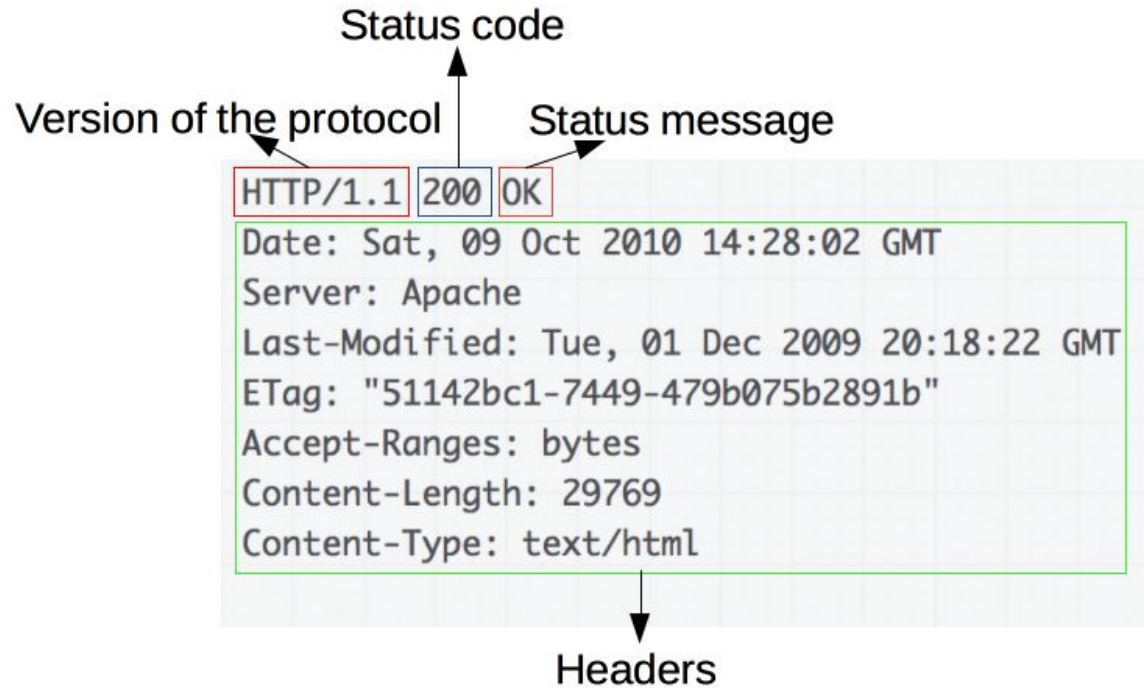
HTTP 101 - Timeline



Request - Client



Response - Server



HTTP Requests Demo

The background is a blue gradient with white circuit-like lines and circles in the corners, resembling a stylized electronic board.

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: dGhIbG9uZ2Nvbgo=

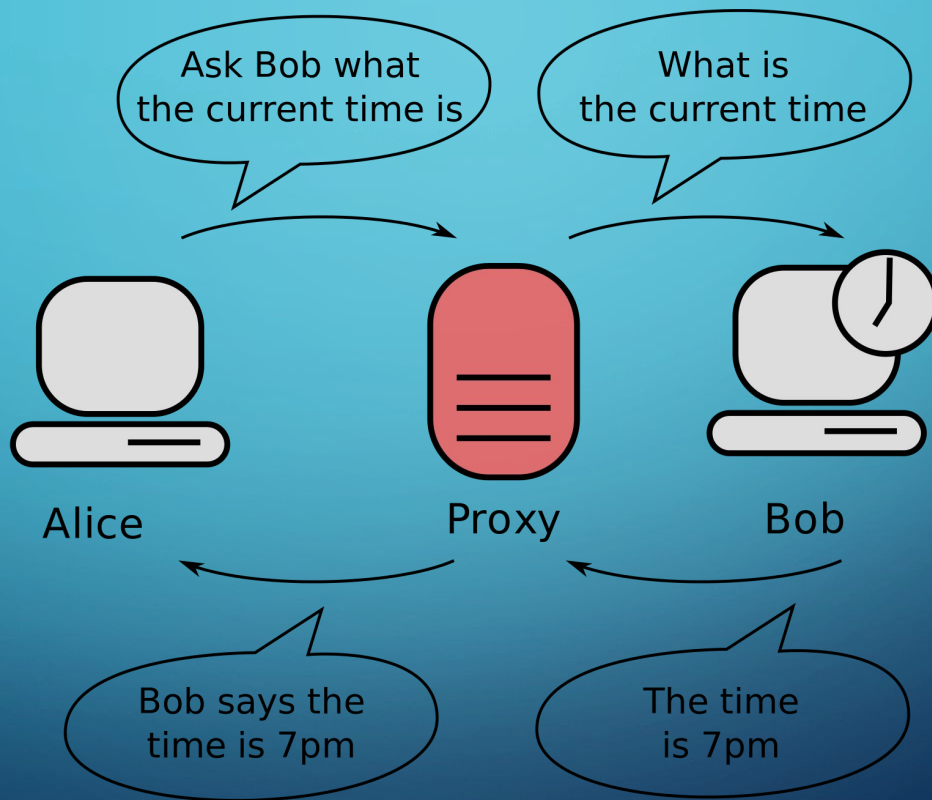
- Hash - SHA-1, SHA-2, bcrypt, scrypt, PBKDF2, argon2

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 Edition v2.1.04

Welcome to Burp Suite Community Edition. Use the options below to create or open a project.

Note: Disk-based projects are only supported on Burp Suite Professional.

☒ Temporary project

☐ New project on disk

Name:

File:

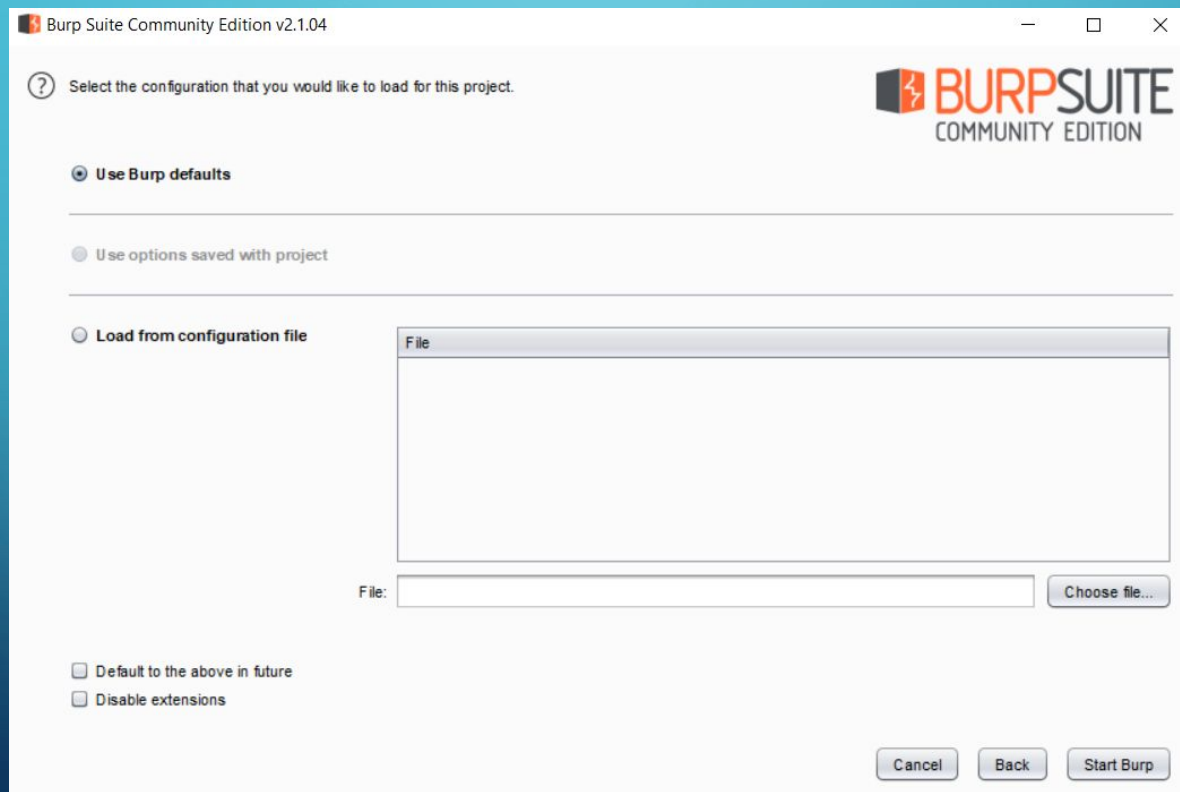
☐ Open existing project

Name	File
------	------

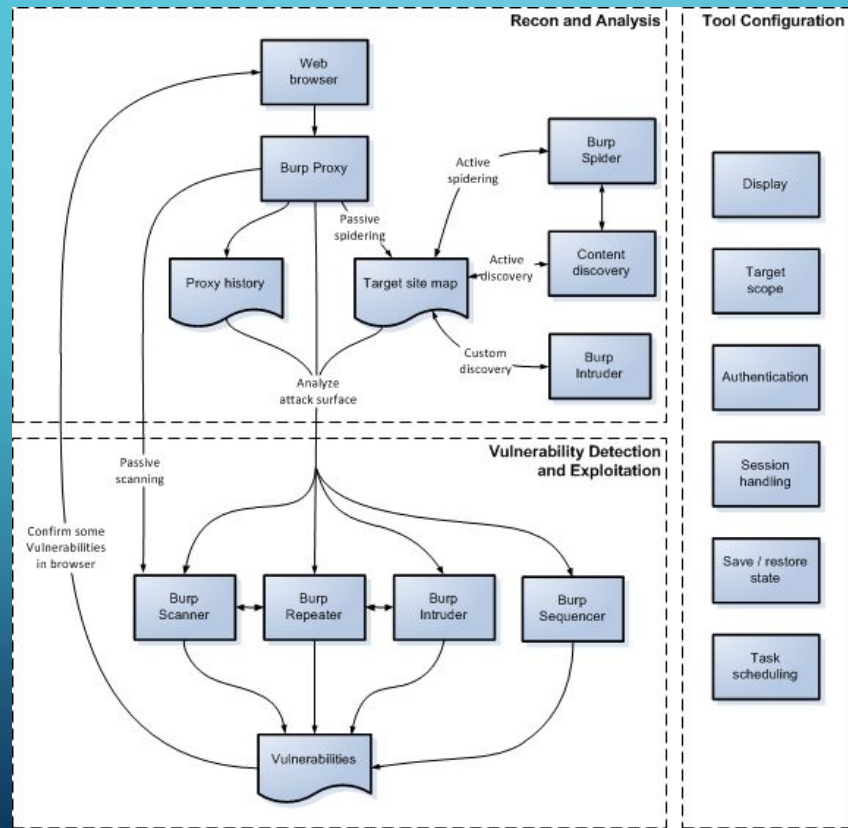
File:

☒ Pause Automated Tasks

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

The background is a blue gradient. In the corners, there are decorative white lines resembling circuit traces or a stylized city skyline. These lines include small circles at various points, suggesting nodes or connections.

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

Burp Suite Documentation

Documentation

▼ Desktop editions

- ▶ Getting started
- ▶ Scanning web sites
- ▶ Penetration testing
- ▶ Mobile testing
- ▶ Extensibility
- ▶ Troubleshooting
- ▶ Dashboard
- ▶ Tools
- ▶ Useful functions
- ▶ Options

▶ Scanner

▶ Burp Collaborator

▶ Burp Infiltrator

Contents

[Support Center >> Documentation](#)

[Enterprise](#)

[Professional](#)

[Community](#)

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

Burp Suite Community Edition v2.1.04 - Temporary Project

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	
Authz		☆☆☆☆☆		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 2018	
Bypass WAF		☆☆☆☆☆		29 Mar 2017	
CO2		☆☆☆☆☆		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	
CustomDeserialzier		☆☆☆☆☆		06 Feb 2017	
CVSS Calculator		☆☆☆☆☆		30 Mar 2017	
Decoder Improved		☆☆☆☆☆		30 Oct 2019	
Decompressor		☆☆☆☆☆		19 Jun 2018	

Refresh list Manual install

.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=%2c0IAHfichsdoigjKLAsgjghajkljgSDGsjdg1SDJg9SDJGsdgjSGJDDsasdfja9sdfjasdfja0sdfja
... [1000 lines later] ...
sct100%24ct100%24InnerContentPlaceholder%24Element_42%24ct100%24FrmLogin%24TxtUsername_intern
al=username&sct100%24ct100%24InnerContentPlaceholder%24Element_42%24ct100%24FrmLogin%24TxtPass
word_internal=password&sct100%24ct100%24InnerContentPlaceholder%24Element_42%24ct100%24BtmLogi
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: ☆☆☆☆☆

Popularity:

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.


Add Edit Remove	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
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

- | | |
|--|--|
| <input checked="" type="checkbox"/> HTML | <input checked="" type="checkbox"/> Other text |
| <input checked="" type="checkbox"/> Script | <input type="checkbox"/> Images |
| <input checked="" type="checkbox"/> XML | <input checked="" type="checkbox"/> Flash |
| <input type="checkbox"/> CSS | <input type="checkbox"/> 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

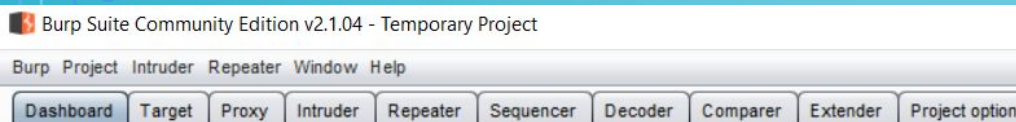
Port

Show all

Hide all

Revert changes

Dashboard v2.x



Tasks + New scan + New live task ⏸ ⚙ ? ➦ 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.

15 items added to site map

23 responses processed

0 responses queued

Capturing:



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

Site Map

- http://zero.webappsecurity.com
 - /
 - index.html
 - resources
 - css
 - img
 - js
 - search.html

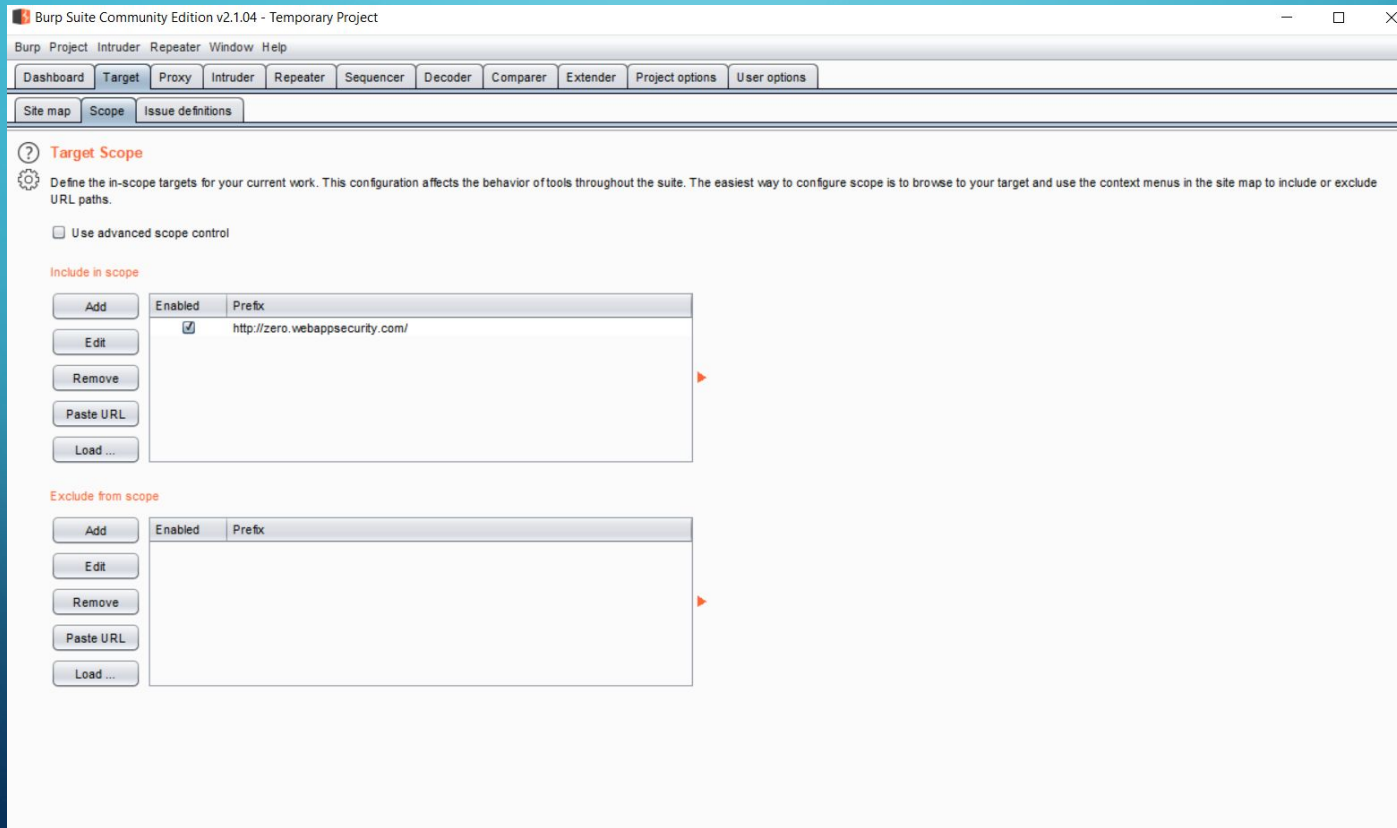
Host	Method	URL	Params	Status	Length	MIME type	Title	Comment	Time request
http://zero.webappsecurity.com	GET	/		200	12755	HTML	Zero - Personal Banking ...		21:44:04 1 N
http://zero.webappsecurity.com	GET	/resources/js/bootstrap....		200	27278	script			21:44:04 1 N
http://zero.webappsecurity.com	GET	/resources/js/jquery-1.8....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

Request **Response**

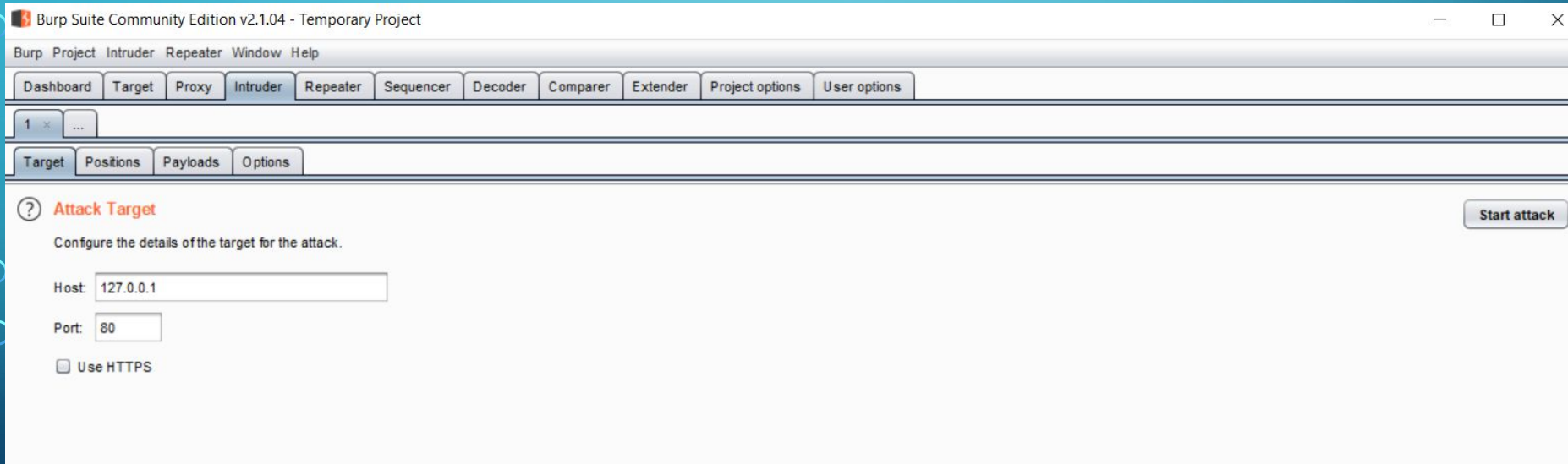
Raw **Headers** **Hex**

```
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



Intruder - Target



Intruder - Positions

The screenshot shows the Burp Suite Community Edition v2.1.04 interface. The main window is titled "Burp Suite Community Edition v2.1.04 - Temporary Project". The menu bar includes "Burp", "Project", "Intruder", "Repeater", "Window", and "Help". The toolbar contains buttons for "Dashboard", "Target", "Proxy", "Intruder", "Repeater", "Sequencer", "Decoder", "Comparer", "Extender", "Project options", and "User options". The "Intruder" tab is active, and the "Positions" sub-tab is selected. The "Payload Positions" section is visible, with a "Start attack" button. The "Attack type" is set to "Sniper". The main area displays an HTTP request with placeholders for payloads: `POST /example?p1=$p1val$p2=$p2val$ HTTP/1.0`, `Cookie: c=$cval$`, `Content-Length: 17`, and `p3=$p3val$p4=$p4val$`. On the right side, there are buttons for "Add \$", "Clear \$", "Auto \$", and "Refresh".

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 x ...

Target Positions Payloads Options

? **Payload Positions** Start attack

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.

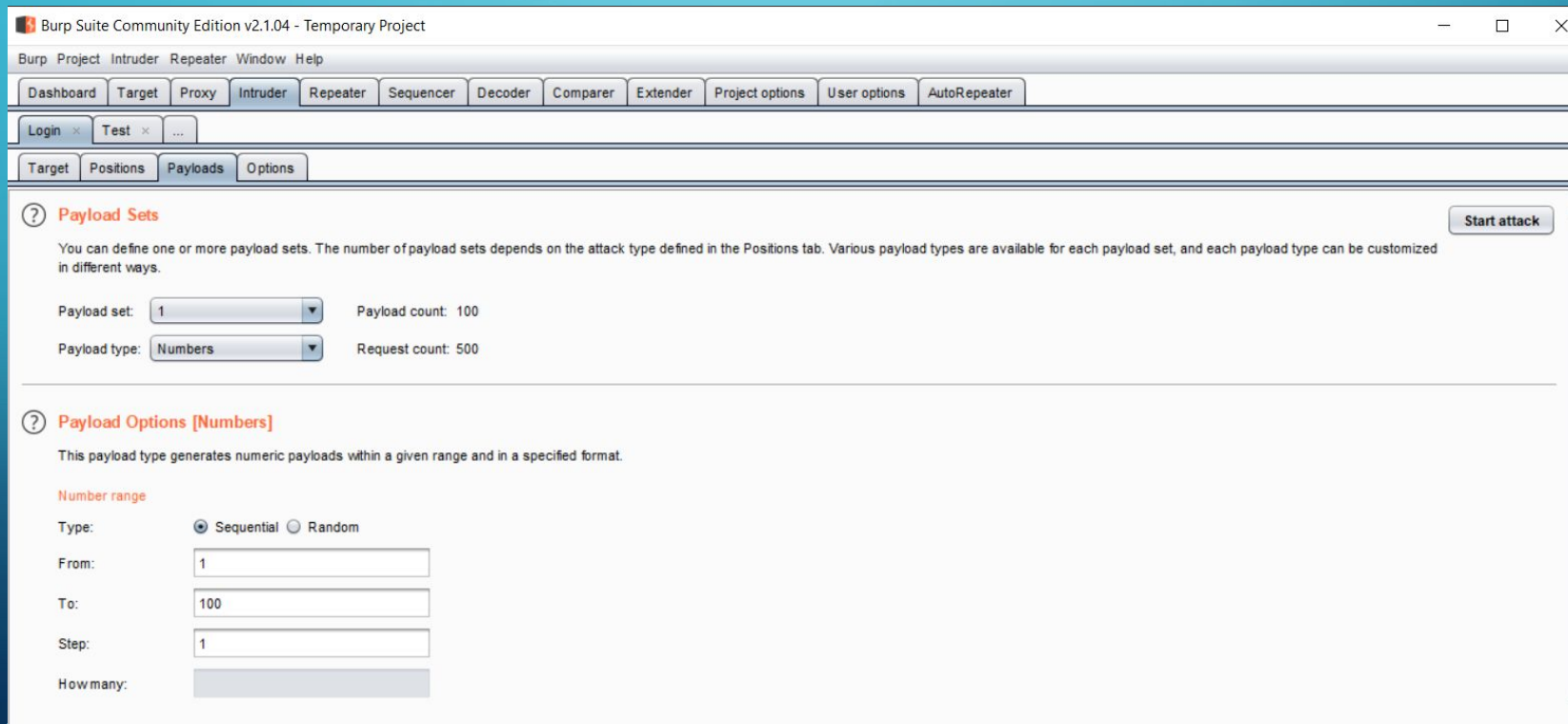
Attack type: Sniper

```
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 - Temporary Project window. The 'Intruder' tab is selected in the top navigation bar. Below the navigation bar, the 'Payloads' sub-tab is active. The main content area displays the 'Payload Sets' configuration section. It includes a 'Start attack' button in the top right corner. The 'Payload Sets' section contains a description: '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.' Below this, there are two rows of configuration options: 'Payload set: 1' with a dropdown arrow, 'Payload count: 100', 'Payload type: Numbers' with a dropdown arrow, and 'Request count: 500'. A horizontal line separates this section from the 'Payload Options [Numbers]' section below. The 'Payload Options [Numbers]' section includes a description: 'This payload type generates numeric payloads within a given range and in a specified format.' It also has a 'Number range' section with 'Type:' set to 'Sequential' (radio button selected) and 'Random' (radio button unselected). Below 'Type:' are four input fields: 'From:' with value '1', 'To:' with value '100', 'Step:' with value '1', and 'How many:' with an empty field.

Burp Suite Community Edition v2.1.04 - Temporary Project

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

Login x Test x ...

Target Positions **Payloads** Options

? **Payload Sets** Start attack

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: 1 Payload count: 100

Payload type: Numbers 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: 1

To: 100

Step: 1

How many:

Intruder - Options

The screenshot shows the Burp Suite Community Edition v2.1.04 - Temporary Project window. The 'Intruder' tab is selected in the top navigation bar. Below the navigation bar, the 'Options' sub-tab is active. The main content area is divided into two sections: 'Request Headers' and 'Request Engine'. The 'Request Headers' section has a 'Start attack' button and two checked options: 'Update Content-Length header' and 'Set Connection: close'. The 'Request Engine' section has a note about some options not being available in the Community Edition. It includes input fields for 'Number of threads' (1), 'Number of retries on network failure' (3), 'Pause before retry (milliseconds)' (2000), and 'Throttle (milliseconds)' (Fixed at 0). There are also radio buttons for 'Start time' (Immediately, In 10 minutes, Paused).

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

Login Test ...

Target Positions Payloads Options

Request Headers

Start attack

These settings control whether Intruder updates the configured request headers during attacks.

- ☒ Update Content-Length header
- ☒ Set Connection: close

Request Engine

These settings control the engine used for making HTTP requests when performing attacks.

Note: Some of these options are not available in the Community Edition of Burp.

Number of threads: 1

Number of retries on network failure: 3

Pause before retry (milliseconds): 2000

Throttle (milliseconds): ☒ Fixed 0

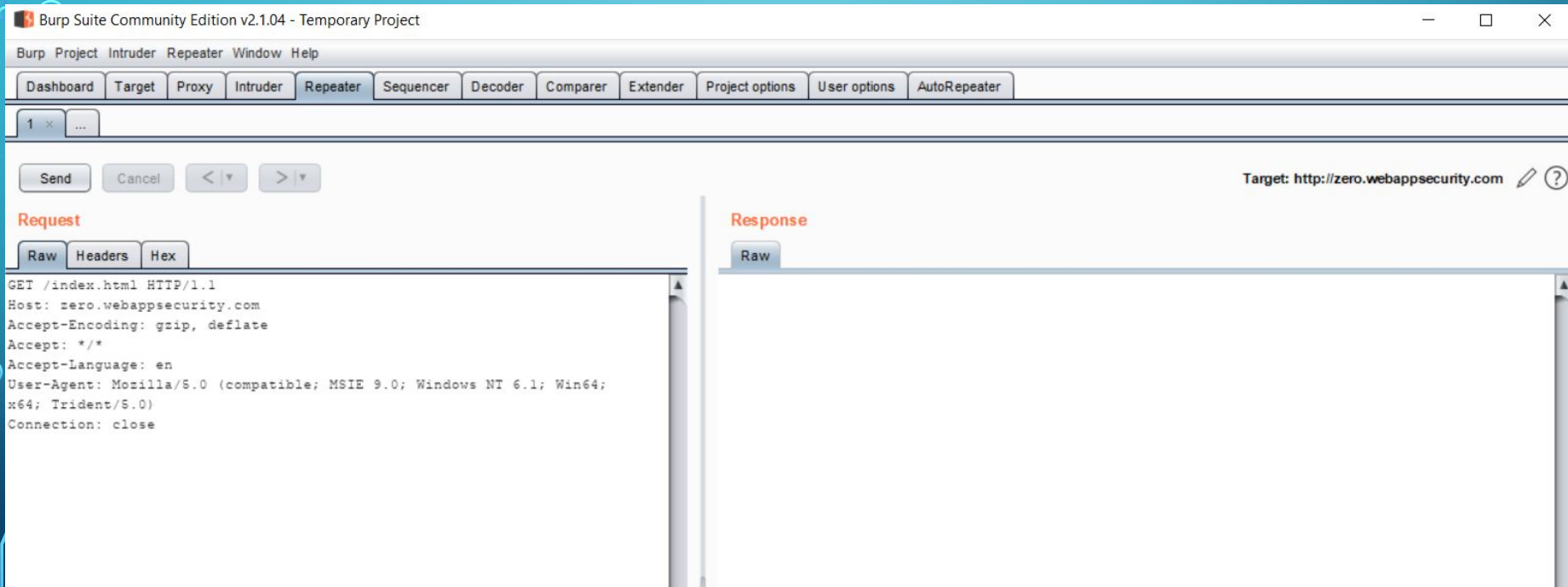
☐ Variable: start 0 step 30000

Start time: ☒ Immediately

☐ In 10 minutes

☐ Paused

Repeater



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/1.1Host: support.portswigger.netUser-Agent: Mozilla/5...
2	256	GET /robots.txt HTTP/1.1Host: support.portswigger.netUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:70.0) Gecko/201...

Paste

Load

Remove

Clear

Select item 2:

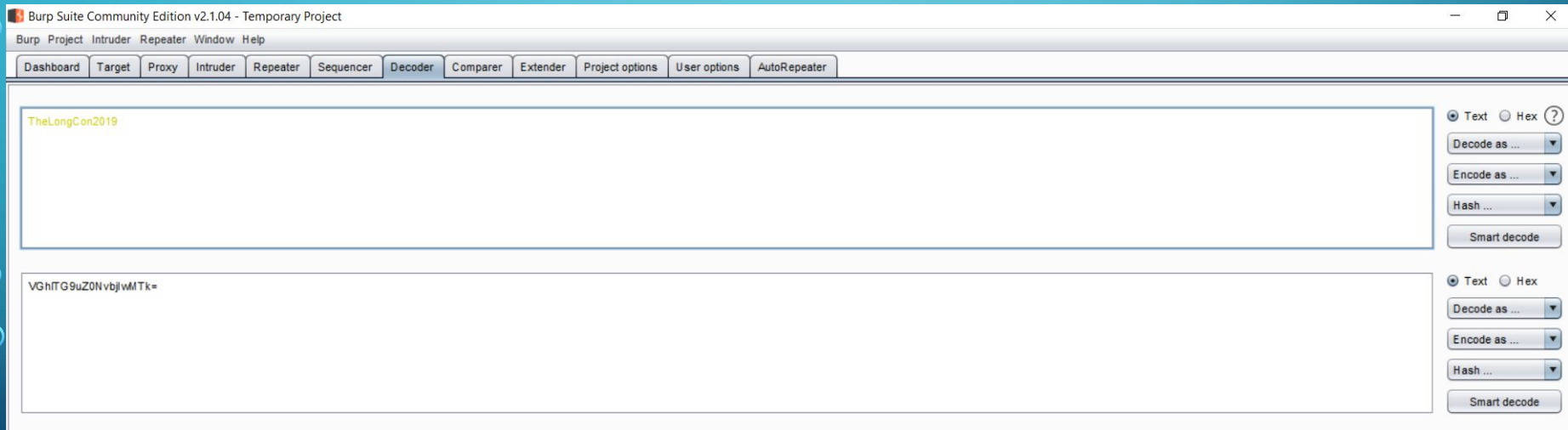
#	Length	Data
1	563	GET /customer/portal/theme_attachments/24245?cb=1487754866309 HTTP/1.1Host: support.portswigger.netUser-Agent: Mozilla/5...
2	256	GET /robots.txt HTTP/1.1Host: support.portswigger.netUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:70.0) Gecko/201...

Compare ...

Words

Bytes

Decoder



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=PLLKT__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