



OWASP

Open Web Application
Security Project

BurpSuite Primer & Extensions Deep-Dive

- Dhanashree C. Kulkarni

About the Speaker

Application Security Engineer with Paycor Inc.

In addition to Pentesting Web and mobile applications, her focus areas include working with development teams to help build security in the SDLC.

Formerly worked as a Security consultant and Team lead with Security services providing companies in Telecom and Healthcare domains and is CISSP certified.



OWASP
Open Web Application
Security Project

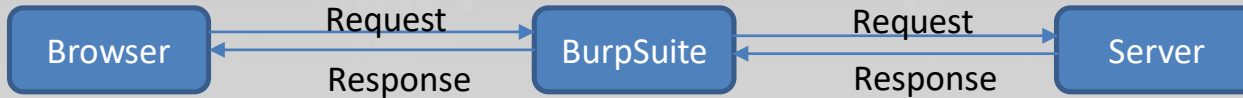
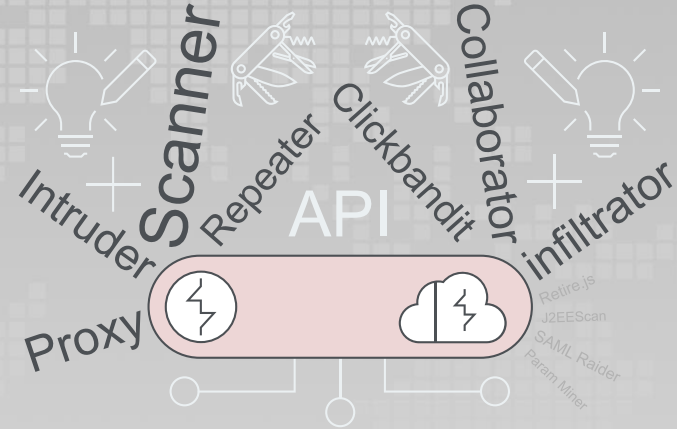
Agenda

- Introduction to BurpSuite
- Configuration on Browser
- BurpSuite tools
 - Interceptor, Repeater, Intruder, Decoder, Collaborator
- Other useful features
- Extensions



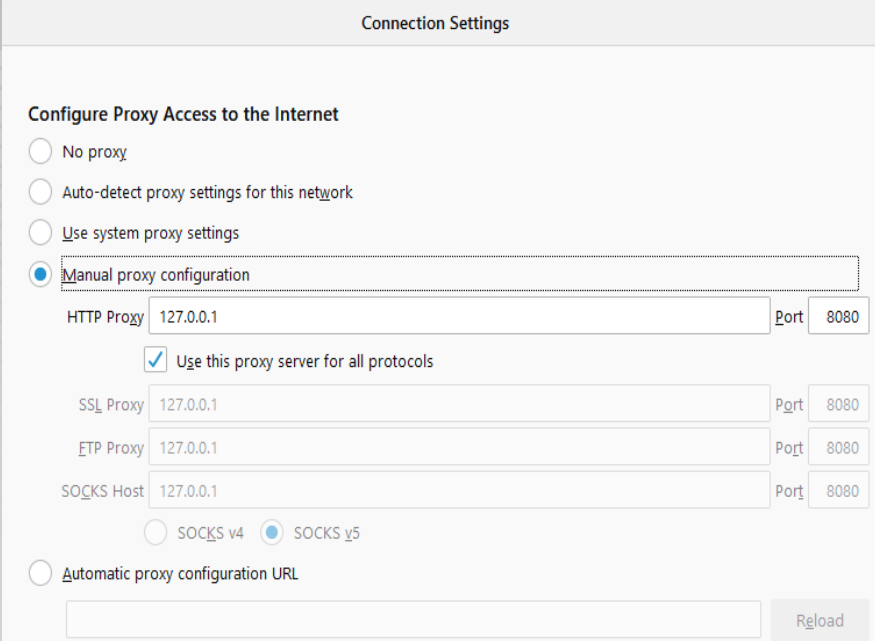
Introduction to BurpSuite

- BurpSuite is called the Swiss Army knife of Appsec tools
- Burp Proxy is an intercepting web proxy that operates as a man-in-the-middle between the end browser and the target web application.
- It lets you intercept, inspect and modify the raw traffic passing in both directions.



Configuring BurpSuite on browser

- BurpSuite is available in Enterprise, Professional and Community Edition
- Community Edition is free to use and can be downloaded from [here](#).
- It is preferred to use BurpSuite with Firefox, to prevent it from interfering with the network traffic
- Select the Manual Proxy configuration under Network settings and update the configuration



The screenshot shows the 'Connection Settings' dialog box in Burp Suite. The 'Manual proxy configuration' option is selected. The HTTP Proxy is set to 127.0.0.1 on port 8080. The checkbox 'Use this proxy server for all protocols' is checked. The SSL Proxy, FTP Proxy, and SOCKS Host are also set to 127.0.0.1 on port 8080. The SOCKS version is set to v5. The 'Automatic proxy configuration URL' option is not selected.

Connection Settings

Configure Proxy Access to the Internet

☐ No proxy

☐ Auto-detect proxy settings for this network

☐ Use system proxy settings

☒ Manual proxy configuration

HTTP Proxy 127.0.0.1 Port 8080

☒ Use this proxy server for all protocols

SSL Proxy 127.0.0.1 Port 8080

FTP Proxy 127.0.0.1 Port 8080

SOCKS Host 127.0.0.1 Port 8080

☐ SOCKS v4 ☒ SOCKS v5

☐ Automatic proxy configuration URL

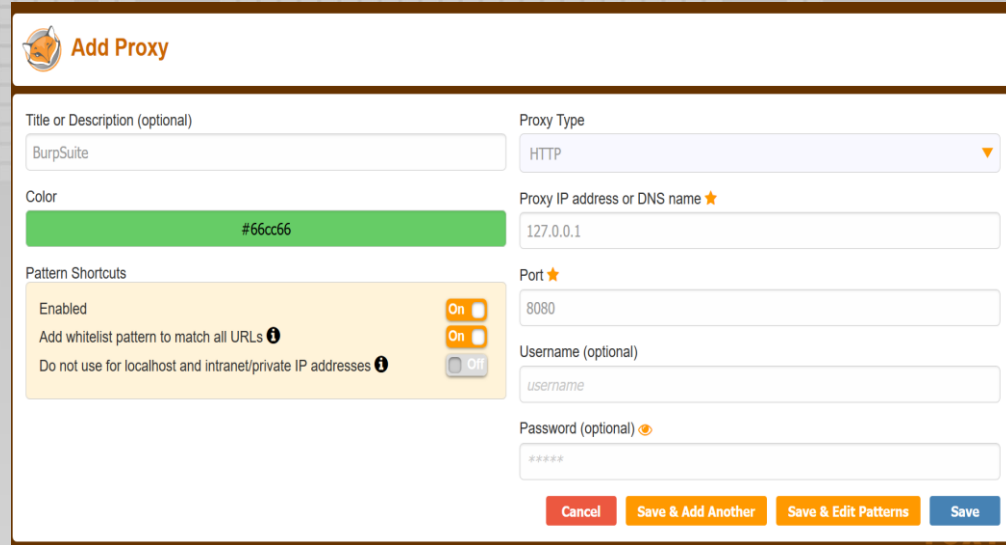
Reload

No proxy for



Configuring BurpSuite on browser

- Setting up the Manual Proxy requires to turn it On/Off each time a request has to be intercepted.
- Foxy Proxy addon is a fuss-free alternative to switching the proxy each time from the Network Settings.
- Just need to toggle it anytime we want the Manual proxy to be set



The screenshot shows the 'Add Proxy' dialog box in Burp Suite. The dialog has a title bar with the Burp Suite logo and the text 'Add Proxy'. The main content area is divided into several sections:

- Title or Description (optional):** A text input field containing 'BurpSuite'.
- Color:** A color selection bar showing a green color with the hex code '#66cc66'.
- Pattern Shortcuts:** A section with two toggle switches. The first is labeled 'Enabled' and is turned 'On'. The second is labeled 'Add whitelist pattern to match all URLs' and is also turned 'On'. Below these is a label 'Do not use for localhost and intranet/private IP addresses' with an information icon.
- Proxy Type:** A dropdown menu set to 'HTTP'.
- Proxy IP address or DNS name:** A text input field containing '127.0.0.1'.
- Port:** A text input field containing '8080'.
- Username (optional):** A text input field containing 'username'.
- Password (optional):** A password input field with masked characters '*****'.

At the bottom of the dialog, there are four buttons: 'Cancel', 'Save & Add Another', 'Save & Edit Patterns', and 'Save'.

Configuring BurpSuite on browser

1 Burp Suite Professional v1.7.33 - Temporary Project - licensed to Bugcrowd [4 user license]

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

Intercept HTTP history WebSockets history Options **2**

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"/>	127.0.0.1:8080			Per-host

3 Each installation of Burp generates its own CA certificate that is used to intercept requests. You will need to import this certificate into your browser.

Import / export CA certificate Regenerate CA certificate

Intercept Client Requests

Use these settings to control which requests are stalled for viewing.

☒ Intercept requests based on the following rules:

Enabled	Operator	Match type	Relationship	Condition
<input checked="" type="checkbox"/>		File extension	Does not match	(*gif\$ *jpg\$ *png\$ *css\$ *js\$ *ico\$)
<input type="checkbox"/>	Or	Request	Contains parameters	
<input type="checkbox"/>	Or	HTTP method	Does not match	(get post)
<input type="checkbox"/>	And	URL	Is in target scope	

☐ Automatically fix missing or superfluous new lines at end of request
☒ Automatically update Content-Length header when the request is edited

Add a new proxy listener

Binding Request handling Certificate

These settings control how Burp binds the proxy listener.

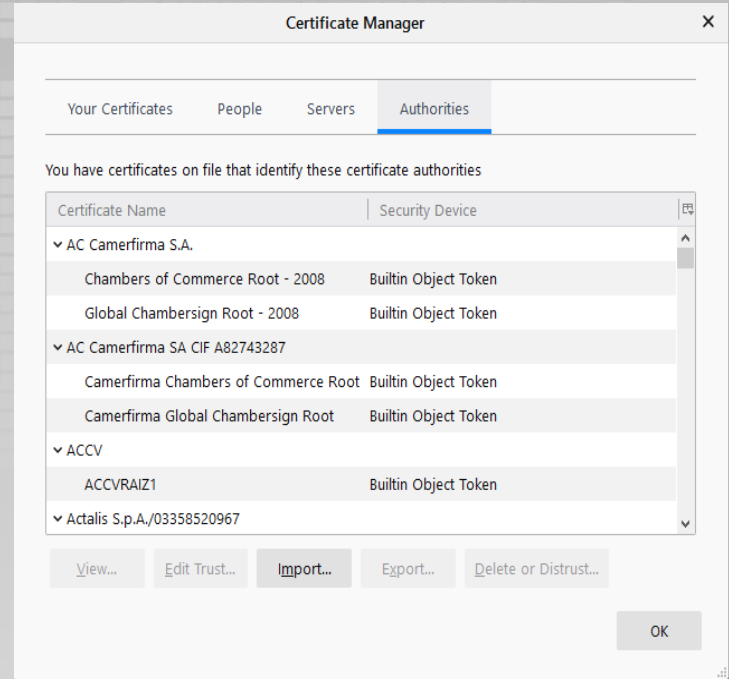
Bind to port:

Bind to address: ☒ Loopback only
☐ All interfaces
☐ Specific address:

BurpSuite Proxy Settings

Configuring BurpSuite on browser

- Navigate to <http://burp> from the browser and download and install the Burp certificate (from the link on the top right corner) OR
- Download the certificate from the Import/Export CA certificate option under Proxy Listeners (export in DER format)
- Import this certificate under Browser's certificate settings and choose it to identify websites.



Browser Certificate settings



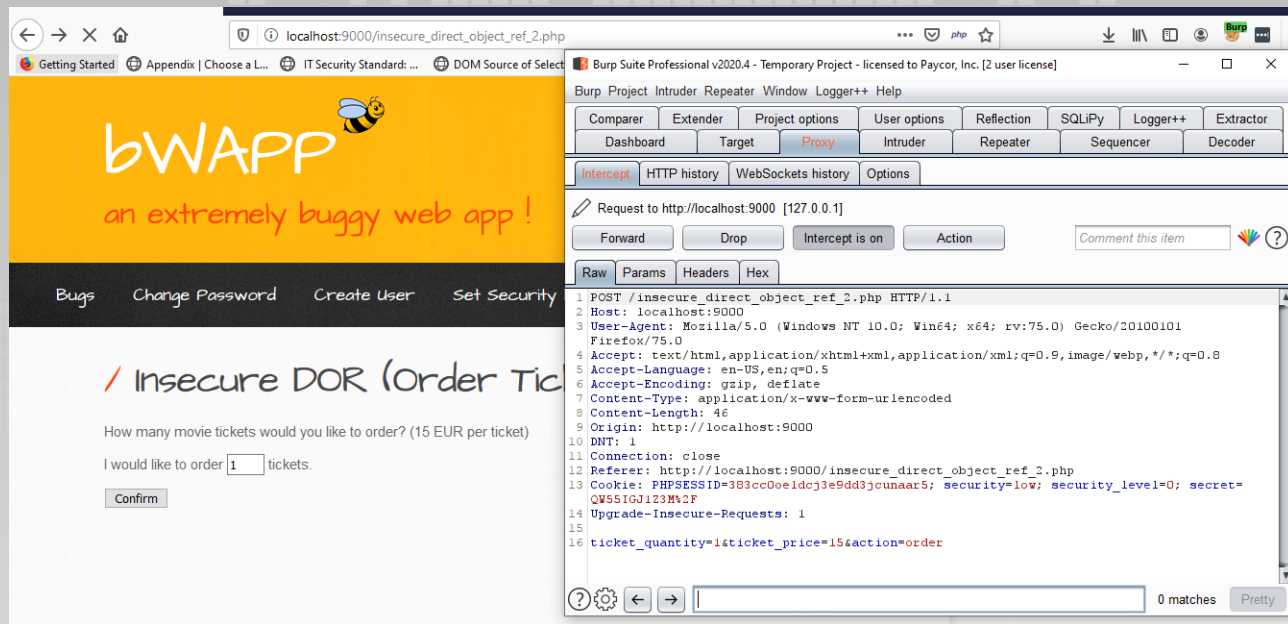
Test Targets

- OWASP Juice Shop
- DVWA
- BWApp
- Test sites – [Webinspect](#) , [Acunetix](#)



BurpSuite Tools: Proxy

- Most basic function of BurpSuite
- Used to Tamper requests and responses
- Usage
 - Observing the Raw Request, finding hidden parameters
 - Tampering the request before sending it to the server
 - Bypassing client side validations



Forward the Request to send it to the server, or **Drop** the request to Reject it

BurpSuite Tools: Repeater

- Simple tool for manipulating and reissuing individual requests and analyzing responses
- Works like a scratchpad while testing applications
- Usage
 - Replaying the request without having to run the scenarios on front-end
 - Manipulating the parameter values to observe the change in Response
- Select 'Send to Repeater' on right click to send the intercepted Request to Repeater

The screenshot displays the BurpSuite Repeater tool interface. The top menu bar includes Dashboard, Target, Proxy, Intruder, Repeater, Sequencer, Decoder, Comparer, Extender, Project options, User options, Reflection, SQUIPy, Logger++, and Extractor. The Repeater tab is active, showing a list of requests (1 to 23) and a 'Send' button. The 'Request' tab is selected, displaying the following raw request:

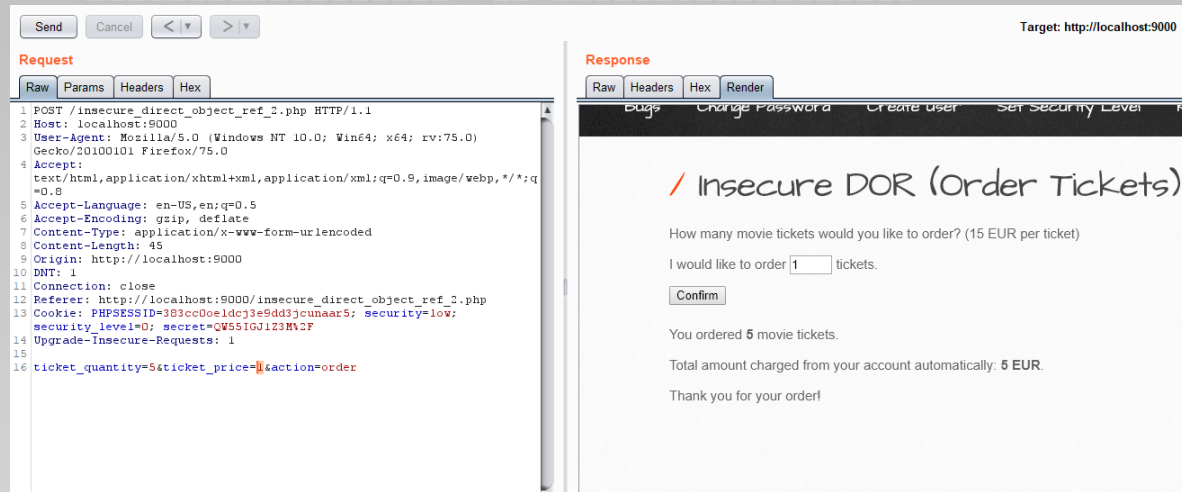
```
1 POST /insecure_direct_object_ref_2.php HTTP/1.1
2 Host: localhost:9000
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:75.0)
  Gecko/20100101 Firefox/75.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 46
9 Origin: http://localhost:9000
10 DNT: 1
11 Connection: close
12 Referer: http://localhost:9000/insecure_direct_object_ref_2.php
13 Cookie: PHPSESSID=383cc0e1dc33e9dd33cunaar5; security=low;
  security_level=0; secret=QW55IGJ1Z3M4ZWF
14 Upgrade-Insecure-Requests: 1
16 ticket_quantity=1&ticket_price=15&action=order
```

The 'Response' tab is also visible, showing the raw response from the target (http://localhost:9000). The response content is as follows:

```
Raw Headers Hex Render
Bugz Change Password Create User Set Security Level
/ Insecure DOR (Order Tickets)
How many movie tickets would you like to order? (15 EUR per ticket)
I would like to order 1 tickets.
Confirm
You ordered 1 movie tickets.
Total amount charged from your account automatically: 15 EUR.
Thank you for your order!
```

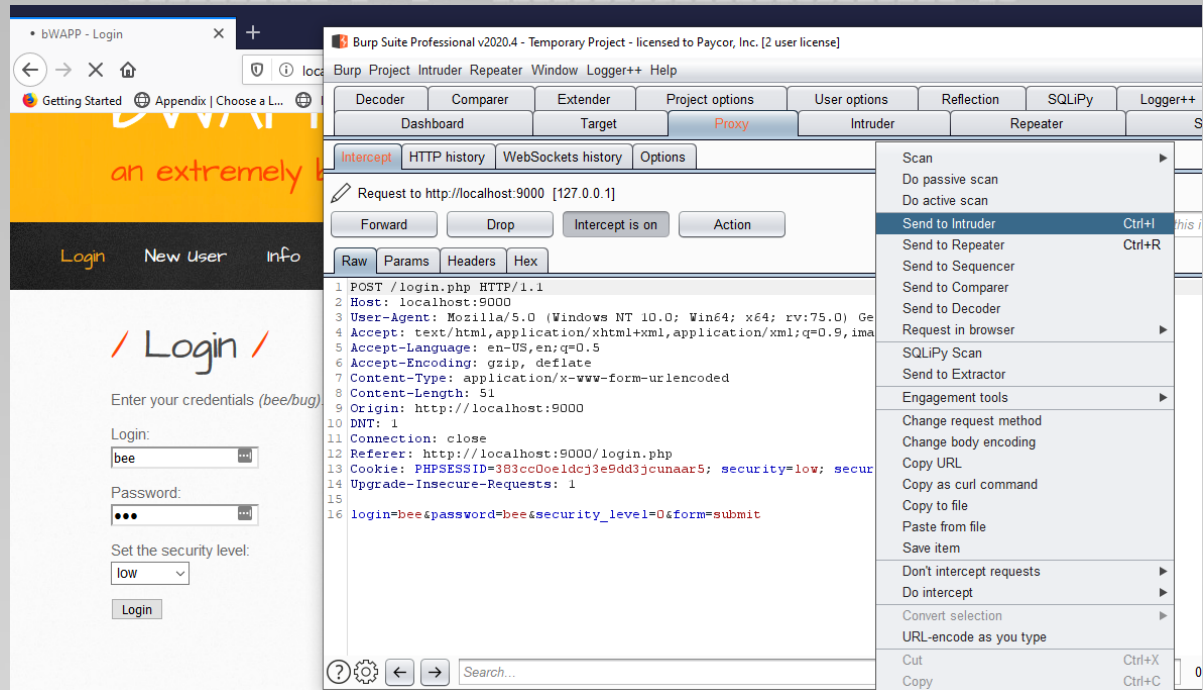
BurpSuite Tools: Repeater

- Simple tool for manipulating and reissuing individual requests and analyzing responses
- Works like a scratchpad while testing applications
- Usage
 - Replaying the request without having to run the scenarios on front-end
 - Manipulating the parameter values to observe the change in Response
- Select 'Send to Repeater' on right click to send the intercepted Request to Repeater



BurpSuite Tools: Intruder

- A powerful tool for carrying out automated attacks against applications
- Usage
 - Brute-forcing login requests is the most common use
 - Fuzzing the parameter with a range of values
 - This can be further used to exploit an Injection attack.
- Select 'Send to Intruder' on right click to send the intercepted Request to Intruder



BurpSuite Tools: Intruder

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.

Attack type:

```
1 POST /login.php HTTP/1.1
2 Host: localhost:9000
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:75.0) Gecko/20100101 Firefox/75.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 51
9 Origin: http://localhost:9000
10 DNT: 1
11 Connection: close
12 Referer: http://localhost:9000/login.php
13 Cookie: PHPSESSID=383cc0e1dcj3e9dd3jcunaar5; security=low; security_level=0
14 Upgrade-Insecure-Requests: 1
15
16 login=bee&password=$bee&security_level=0&form=submit
```

Start attack

Add \$
Clear \$
Auto \$
Refresh

Target Positions Payloads Options

Payload set: Payload count: 16
Payload type: Request count: 16

? Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste	Password967
Load ...	Password@1
Remove	Password12345
Clear	Hello@Spring
	Spring@2020
	Covid@2019
	Password123

Add

Add from list ...

? Payload Processing

Click on 'Start Attack' once the Payload Options are set, to start the attack

BurpSuite Tools: Intruder

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	error	exce...	illegal	invalid	fail	stack	access
5	Spring@2020	200	<input type="checkbox"/>	<input type="checkbox"/>	4430	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	Covid@2019	200	<input type="checkbox"/>	<input type="checkbox"/>	4430	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7	Password123	200	<input type="checkbox"/>	<input type="checkbox"/>	4430	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8	Password456	200	<input type="checkbox"/>	<input type="checkbox"/>	4430	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9	Password928	200	<input type="checkbox"/>	<input type="checkbox"/>	4430	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10	foo	200	<input type="checkbox"/>	<input type="checkbox"/>	4430	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11	bar	200	<input type="checkbox"/>	<input type="checkbox"/>	4430	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12	password	200	<input type="checkbox"/>	<input type="checkbox"/>	4430	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
13	passwd	200	<input type="checkbox"/>	<input type="checkbox"/>	4430	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
14	bug	302	<input type="checkbox"/>	<input type="checkbox"/>	502	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
15	bee	200	<input type="checkbox"/>	<input type="checkbox"/>	4430	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
16	flower	200	<input type="checkbox"/>	<input type="checkbox"/>	4430	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Request Response

Raw Headers Hex

```
1 HTTP/1.1 302 Found
2 Date: Mon, 04 May 2020 07:29:43 GMT
3 Server: Apache/2.4.7 (Ubuntu)
4 X-Powered-By: PHP/5.5.9-1ubuntu4.22
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
7 Pragma: no-cache
8 Set-Cookie: PHPSESSID=931016md0j20821rj19h3dsgc2; path=/
9 Set-Cookie: security_level=0; expires=Tue, 04-May-2021 07:29:43 GMT; Max-Age=31536000; path=/
10 Location: portal.php
11 Content-Length: 0
12 Connection: close
```

0 matches Pretty



BurpSuite Tools: Intruder - Payload Processing

Results

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.

Attack type:

Sniper

1 GET / HTTP/1.1

2 Host: 127.0.0.1

3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:75.0) Gecko/20100101 Firefox/75.0

4 Accept:

5 text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8

6 Accept-Language: en-US,en;q=0.5

7 Accept-Encoding: gzip, deflate

8 DNT: 1

9 Connection: close

10 Upgrade-Insecure-Requests: 1

11 Authorization: Basic \$2m5vOmJhcg==\$

12

Add \$

Clear \$

Auto \$

Refresh

?

⚙

⏪

⏩

Search...

0 matches

Pretty

Clear

Results

Target

Positions

Payloads

Options

?

Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

Add

Edit

Remove

Up

Down

Enabled	Rule
<input checked="" type="checkbox"/>	Add Prefix: foo:
<input checked="" type="checkbox"/>	Base64-encode

?

Payload Encoding

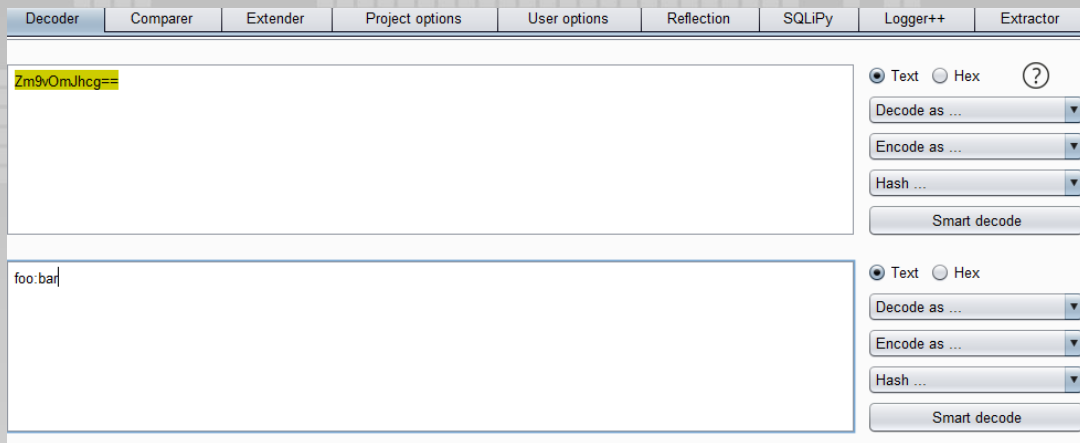
This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

☐ URL-encode these characters:



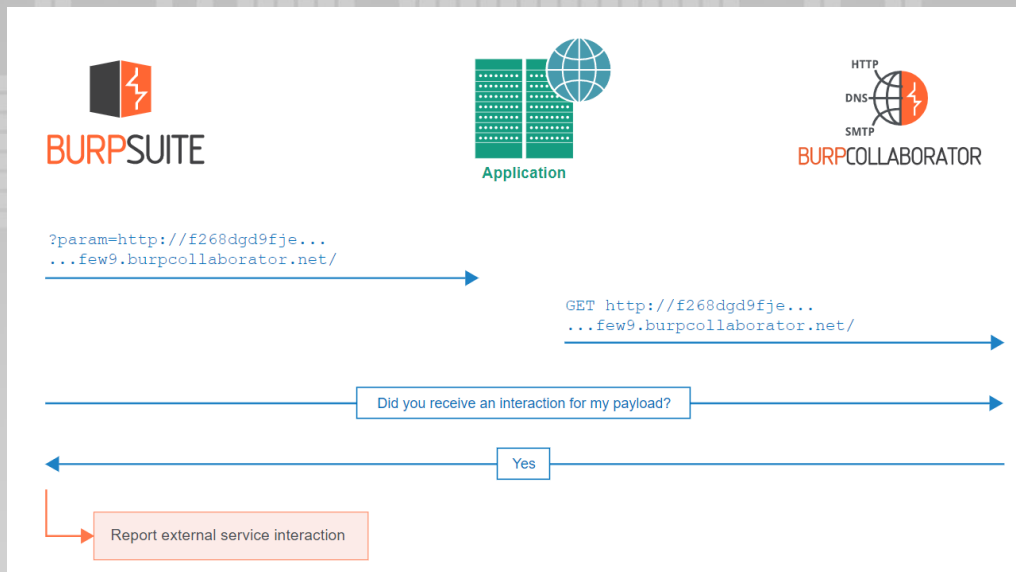
BurpSuite Tools: Decoder

- Used to Encode/Decode values in different encoding/hashing formats
- The Smart decode feature detect and decodes the data by analyzing it's encoding type
- Usage
 - Encode/Decode parameter/token values
 - Encoding payloads for filter invasion



BurpSuite Tools: Collaborator

- Network service that Burpsuite uses to discover external service interaction
- Usage
 - Detect blind injection attacks and service specific vulnerabilities.
 - External service interaction.
 - Can also be used to validate SSRF issues



Source: <https://portswigger.net/burp/documentation/collaborator>

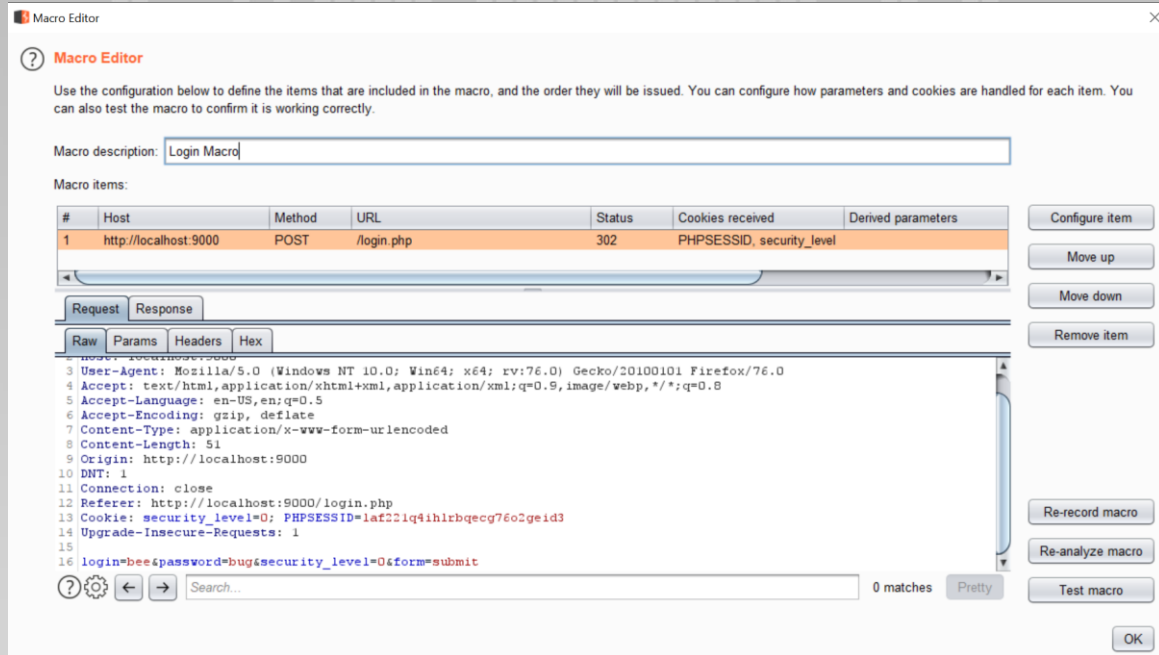
**Lets move on to a useful but often ignored feature
of BurpSuite..**



OWASP
Open Web Application
Security Project

Recording Macros in BurpSuite

- Macros direct Burp to follow a set of steps on hitting certain conditions
- Usage
 - Most commonly used for keeping the session active while scanning/spidering the site or performing any automated attack



What's more fun? BurpSuite features can be Extended..



OWASP
Open Web Application
Security Project

BurpSuite Tools: Extender

- There are numerous apps available on the BApp Store for adding functionality to your already loaded BurpSuite
- Prerequisites – The locations of the interpreter jar files should be mentioned under 'Options'

The screenshot shows the 'Options' tab in the Burp Suite Extender. It has sections for 'Python Environment' and 'Ruby Environment'. Each section includes instructions on how to set up the environment for running extensions and fields to specify the location of the interpreter JAR files.

Python Environment

These settings let you configure the environment for executing extensions that are written in Python. To use Python extensions, you will need to download Jython, which is a Python interpreter implemented in Java.

Location of Jython standalone JAR file:

Folder for loading modules (optional):

Ruby Environment

These settings let you configure the environment for executing extensions that are written in Ruby. To use Ruby extensions, you will need to download JRuby, which is a Ruby interpreter implemented in Java. Note that you can either configure the location of the JRuby JAR file here, or you can load the JAR file on startup via the Java classpath.

Location of JRuby JAR file:

The screenshot shows the 'BApp Store' tab in the Burp Suite Extender. It displays a list of available extensions with columns for Name, Installed, Rating, Popularity, Last updated, and Detail. Below the list, there are buttons for 'Refresh list' and 'Manual install ...'. On the right side, there is a section titled 'Using Burp Extensor' with a list of instructions and a 'Submit rating' button.

Name	Installed	Rating	Popularity	Last updated	Detail
.NET Beautifier		☆☆☆☆☆	→	23 Jan 2017	
Active Scan++		☆☆☆☆☆	→	13 Jun 2019	Pro extension
Add & Track Custom Issues		☆☆☆☆☆	→	03 Mar 2020	Pro extension
Add Custom Header		☆☆☆☆☆	→	18 Sep 2018	
Additional CSRF Checks		☆☆☆☆☆	→	14 Dec 2018	
Additional Scanner Checks		☆☆☆☆☆	→	21 Dec 2018	Pro extension
Adhoc Payload Processors		☆☆☆☆☆	→	06 Nov 2019	
AES Payloads		☆☆☆☆☆	→	28 Aug 2015	Pro extension
Anti-CSRF Token From Ref...		☆☆☆☆☆	→	28 Feb 2020	
Asset Discovery		☆☆☆☆☆	→	12 Sep 2019	Pro extension
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	✓	☆☆☆☆☆	→	17 Mar 2020	
AWS Security Checks		☆☆☆☆☆	→	18 Jan 2018	Pro extension
AWS Signer		☆☆☆☆☆	→	18 Oct 2019	
AWS Sigv4		☆☆☆☆☆	→	28 Apr 2020	
Backslash Powered Scanner		☆☆☆☆☆	→	19 Aug 2019	Pro extension
Batch Scan Report Generator		☆☆☆☆☆	→	03 Oct 2017	Pro extension
BeanStack - Stack-trace Fl...		☆☆☆☆☆	→	23 Mar 2020	Pro extension
Blazer		☆☆☆☆☆	→	01 Feb 2017	
Bookmarks		☆☆☆☆☆	→	26 Mar 2020	

Using Burp Extensor

1. If a request requires a value from a response, right click on that request and select 'Send to Extensor'. Then find a response where the client receives this value from, and select 'Send to Extensor'.
2. Go to the Extensor tab to view a Comparer-like interface, and select the request and response needed, then click 'Go'.
3. Within the newly created tab, highlight the content of the request which needs to be replaced, and the content of the response which contains the value to be inserted. Adjust the scope as necessary, and click 'Turn Extensor on'.
4. Once turned on, Extensor will look for occurrences of the regex listed in the request and response panels, and extract or insert data appropriately. It will also update the 'Value to insert' field with the newest value extracted.

Please consult the extension's Github page for a more complete tutorial.

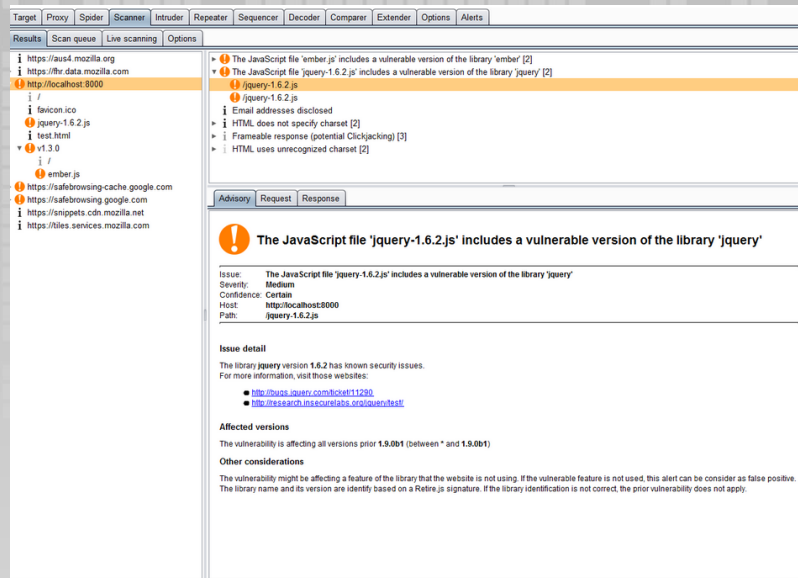
Author: Will Strei
Version: 1.0
Source: <https://github.com/portswigger/token-extractor>
Updated: 29 Oct 2018

Rating: ☆☆☆☆☆
Popularity: →

Extensions to improve your BurpSuite features

- **Vulnerable Libraries scanners**

- Retire.js (Pro)
 - Integrate Retire.js repository to find vulnerable JavaScript libraries
- Software Vulnerability scanner (Pro)
 - This extension scans for vulnerabilities in detected software versions using the [Vulners.com](https://vulners.com) API



Source: <https://github.com/portswigger/retire-js>

Extensions to improve your BurpSuite features

- **Formatting the Request/Responses**

- Json Beautifier
 - This is a Burp Extension for beautifying JSON output.
- .Net beautifier
 - A BurpSuite extension for beautifying .NET message parameters and hiding some of the extra clutter that comes with .NET web apps (i.e. __VIEWSTATE).
- BurpBeautifier
 - BurpSuite extension for beautifying request/response body, supporting JS, JSON, HTML, XML format

- **Request minimization**

- Request minimizer
 - Performs HTTP request minimization. It deletes parameters that are not relevant such as: random ad cookies, cachebusting nonces, etc.

Extensions to improve your BurpSuite features

- **Input validations related**

- SQLiPy
 - A plugin for Burp Suite that integrates SQLMap using the SQLMap API
- CO2
 - Collection on enhancements for BurpSuite. SQLmapper is one of the module for running SQL map directly
- Reflected Parameters (Pro)
 - This extension monitors traffic and looks for request parameter values (longer than 3 characters) that are reflected in the response.

- **Authorization checks**

- Autorize
 - Autorize helps in finding authorization vulnerabilities in an application.
 - It is sufficient to give to the extension the cookies of a low privileged user and navigate the website with a high privileged user. The extension automatically repeats every request with the session of the low privileged user and detects authorization vulnerabilities.

Extensions to improve your BurpSuite features

- **Logging requests**
 - Logger++
 - Logs requests and responses from all Burp Suite tools, like the Repeater, Intruder, Proxy etc.
 - The extension allows advanced filters to be defined to highlight interesting entries or filter logs to only those which match the filter.
 - To enable logs to be used in other systems, the table can also be uploaded to elasticsearch or exported to CSV.
 - Log Requests to SQLite
 - This extension keeps a trace of every HTTP request that has been sent via BURP, in an SQLite database. This is useful for keeping a record of exactly what traffic a pen tester has generated.
- **Collaborator Everywhere**
 - This is a Burp Suite Pro extension which augments your in-scope proxy traffic by injecting non-invasive headers designed to reveal backend systems by causing pingbacks to Burp Collaborator.
- **SSL Scanner**

Questions



OWASP
Open Web Application
Security Project

Additional resources

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

<https://portswigger.net/training>

<https://www.bugcrowd.com/hackers/bugcrowd-university/>

Video Tutorials

HackerOne: <https://www.youtube.com/watch?v=LSqC9qgEMiQ>

BurpSuite basics: <https://www.youtube.com/watch?v=G3hpAeoZ4ek>

These are some test sites to get started learning

<https://xss-game.appspot.com/>

There are plenty of vulnerable web Applications that you can set up to start testing with Burp and understanding Appsec vulnerabilities. Some are listed below:

- Damn Vulnerable Web Application (DVWA)
- OWASP Juiceshop
- Buggy Web App – BWApp



OWASP
Open Web Application
Security Project