

# Burp Suite

## Description

Burp Suite est une suite d'outils dédiée à la découverte et à l'exploitation de vulnérabilités et/ou langages web côté serveur et côté client. Cet outil, développé par PortSwigger, est spécialement conçu pour évaluer la sécurité des applications web. Il offre une gamme complète de fonctionnalités pour analyser, détecter et exploiter de potentielles vulnérabilités et interagir plus facilement avec des applications web.

## Installation

Voici le guide d'installation pour l'outil Burp Suite :

### Étape 1 : Téléchargement de Burp Suite

Rendez vous sur le site officiel de PortSwigger (<https://portswigger.net/burp/communitydownload>) pour télécharger la version Community de Burp Suite, qui est gratuite.

```
wget https://portswigger.net/burp/releases/download/latest -O burp-suite-community-edition-latest.jar
```

### Étape 2 : Installation de Java

Burp Suite nécessite Java pour fonctionner. Si Java n'est pas déjà installé sur votre système, vous pouvez l'installer en utilisant votre gestionnaire de paquets. Par exemple, sur Ubuntu, vous pouvez utiliser :

```
sudo apt-get install default-jre
```

### Étape 3 : Lancement de Burp Suite

Pour lancer Burp Suite, utilisez la commande suivante en spécifiant le chemin vers le fichier JAR que vous avez téléchargé :

```
java -jar burp-suite-community-edition-latest.jar
```

### Étape 4 : Configuration du Proxy

- Burp Suite agit comme un proxy entre votre navigateur web et le serveur cible. Vous devez configurer votre navigateur pour utiliser le proxy Burp. Par défaut, Burp écoute sur le port 8080. Modifiez les paramètres de proxy de votre navigateur pour utiliser 127.0.0.1 (localhost) avec le port 8080.
- Vous pouvez également utiliser l'extension "Foxy Proxy" afin de faciliter le changement ou la désactivation/activation du proxy ou de sa configuration.

## Cas d'utilisation

- **Interception de requêtes HTTP** : Burp Suite intercepte les requêtes HTTP, ce qui permet de manipuler plus facilement et d'analyser les données (requêtes) transmises entre le navigateur et le serveur.
- **Analyse de vulnérabilités** : Burp Suite permet d'identifier automatiquement des vulnérabilités courantes telles que les vulnérabilités de type XSS (Cross Site Scripting), les injections SQL, les problèmes de sécurité liés aux cookies, etc.
- **Suite d'outils intégrée** : Burp Suite intègre une variété d'outils, y compris un scanner de vulnérabilités, un repeater, un intruder, un sequencer, un decoder, etc. Ce panel d'outil polyvalent facilite l'analyse d'une application web dans sa globalité.

## Fonctionnalités principales

- **Scanner de vulnérabilités** : rechercher automatiquement des failles de sécurité dans une application web cible.
- **Repeater** : rejouer une requête HTTP en ayant la possibilité de la modifier (tester différentes valeurs dans différents paramètres par exemple) et avoir un aperçu de la réponse afin de la renvoyer directement sur l'application.
- **Intruder** : cibler un paramètre dans l'application afin d'effectuer une attaque par brute force sur celui-ci à partir d'un dictionnaire ou en testant toutes les combinaisons de lettres/chiffres possibles.

# Exemple d'exploitation ou d'utilisation

Supposons que vous soyez chargé de tester la sécurité d'un site web e-commerce qui utilise une méthode HTTP inhabituelle, autre que GET et POST, pour l'accès à certaines ressources sensibles. Si une authentification sur les répertoires sensibles ne prend pas en compte cette méthode HTTP, un attaquant pourrait potentiellement avoir accès à ces ressources non autorisées. Vous déduisez ainsi que cette méthode inhabituelle pourrait poser un risque de sécurité si un attaquant l'utilise et contourne l'authentification trop permissive de l'application en question. Vous pouvez ainsi utiliser Burp Suite pour tester de modifier la méthode HTTP afin de contourner l'authentification et essayer d'accéder à ces ressources auxquelles vous n'êtes normalement pas autorisé d'accéder.

- Interception d'une requête classique par la méthode GET

```

GET /web-seur/ch2/ HTTP/1.1
Host: challenge01.root-me.org
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/117.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: _ga_SRTSKX09J7=GSI.1.1695366826.82.1.1695367424.0.0.0; _ga=GAI.1.498696629.1674478589
Upgrade-Insecure-Requests: 1

```

- Redirection de la requête dans l'Intruder

Choose an attack type

Attack type: Cluster bomb

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://challenge01.root-me.org

```

GET /web-seur/ch2/ HTTP/1.1
Host: challenge01.root-me.org
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/117.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: _ga_SRTSKX09J7=GSI.1.1695366826.82.1.1695367424.0.0.0; _ga=GAI.1.498696629.1674478589
Upgrade-Insecure-Requests: 1

```

- Redirection de la requête dans le Repeater et aperçu de la réponse

Request

Response

```

HTTP/1.1 200 OK
Server: nginx
Date: Fri, 06 Oct 2023 09:04:19 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Vary: Accept-Encoding
Content-Length: 270

```

```

<html>
  <body>
    <link rel='stylesheet' property='stylesheet' id='s' type='text/css' href='/template/s.css' media='all' />
    <iframe id='iframe' src='https://www.root-me.org/?page=externe_header'>
    </iframe>
    <h2>
      Wrong user-agent: you are not the "admin" browser!
    </h2>
  </body>
</html>

```

- Décodage d'une chaîne de caractère encodée en base64

Two hex dump panes are shown. The top pane contains a long URL: "MW1f0jB0xRfZnxhZyE=". The bottom pane contains the message "1m\_n0t\_4\_flag". Both panes have "Text" selected and "Smart decode" checked.

- Ajout d'extensions

Name	Installed	Rating	Popularity	Last updated	System imp...	Detail
.NET Beautifier	Installed	5 stars	High	23 Jan 2017	Low	
403 Bypasser	Installed	5 stars	Medium	27 Sep 2022	Low	Requires Burp ...
SGC API Parser	Installed	5 stars	Medium	23 Sep 2021	Low	
Active Scan++	Installed	5 stars	High	10 Aug 2023	Low	Requires Burp ...
Add & Track Custom Iss...	Installed	5 stars	Medium	25 Feb 2023	Low	Requires Burp ...
Add Custom Header	Installed	5 stars	Medium	08 Jul 2020	Low	
Add to SiteMap+	Installed	5 stars	Medium	28 Nov 2022	Low	
Additional CSRF Checks	Installed	5 stars	Medium	14 Dec 2018	Low	
Additional Scanner Chec...	Installed	5 stars	Medium	21 Dec 2018	Low	Requires Burp ...
Adhoc Payload Process...	Installed	5 stars	Medium	31 Jan 2024	Low	
AES Killer - decrypt AES tr...	Installed	5 stars	Medium	13 May 2021	Low	
AES Payloads	Installed	5 stars	Medium	04 Feb 2022	Low	Requires Burp ...
Agartha - LFI, RCE, SQLI, ...	Installed	5 stars	Medium	28 Jul 2023	Medium	
Anonymous Cloud, Conf...	Installed	5 stars	Medium	17 Jan 2023	Low	Requires Burp ...
Anti-CSRF Token From R...	Installed	5 stars	Medium	28 Feb 2023	Low	
Asset Discovery	Installed	5 stars	Medium	12 Sep 2019	Low	Requires Burp ...
Attack Surface Detector	Installed	5 stars	Medium	16 Dec 2021	Low	
Auth Analyzer	Installed	5 stars	Medium	20 Dec 2022	Low	
Authentication Token O...	Installed	5 stars	Medium	08 Mar 2023	Low	
AuthMatrix	Installed	5 stars	Medium	15 Oct 2021	Low	
Authz	Installed	5 stars	Medium	01 Jul 2014	Low	
Auto-Drop Requests	Installed	5 stars	Medium	10 Feb 2022	Low	
AutoRepeater	Installed	5 stars	Medium	06 Jun 2023	Low	
AutORIZer	Installed	5 stars	Medium	10 Feb 2022	Low	Requires Burp ...
Autowasp	Installed	5 stars	Medium	06 Jun 2023	Low	Requires Burp ...
AWS Security Checks	Installed	5 stars	Medium	18 Jan 2016	Medium	Requires Burp ...
AWS Signer	Installed	5 stars	Medium	08 Jun 2022	Low	
AWS Sig4	Installed	5 stars	Medium	03 Aug 2023	Medium	
Backslash Powered Scan...	Installed	5 stars	Medium	10 Oct 2023	Low	Requires Burp ...
Backup Finder	Installed	5 stars	Medium	04 Aug 2020	Low	
Batch Scan Report Gene...	Installed	5 stars	Medium	04 Feb 2022	Low	Requires Burp ...
BCheck Helper	Installed	5 stars	Medium	13 Oct 2023	Low	Requires Burp ...
BeanStack - Stack-trace ...	Installed	5 stars	Medium	04 Feb 2022	Low	Requires Burp ...
Blazer	Installed	5 stars	Medium	01 Feb 2017	Low	
Blazor Traffic Processor	Installed	5 stars	Medium	21 Sep 2023	Low	
Bookmarks	Installed	5 stars	Medium	21 May 2020	Low	
Bradamsa	Installed	5 stars	Medium	02 Jul 2014	Low	
Brida, Burp to Frida brid...	Installed	5 stars	Medium	15 Aug 2023	Low	

**.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=%20IAhfi0hsdigjKLAsqjghajklgjSDGsjdglsDgjg9SDJGsdqjSGJDSSasdfja9sdjfaj0sdfja ... [1000 lines later] ...
&ct10%24t100%24InnerContentPlaceHolder%24Element_4%24c1t100%24FormLogin%24TxUsername_intern
al+username&ct100%24t100%24InnerContentPlaceHolder%24Element_4%24c1t100%24FormLogin%24TxPass
word_internal+password&ct100%24t100%24InnerContentPlaceHolder%24Element_4%24c1t100%248tLogIn n=Login
```

will be displayed like this:

```
__VIEWSTATE=<snipped out for sanity>&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.

**Estimated system impact**

Overall: Low

Memory	CPU	Time	Scanner
Low	Low	Low	Low

**Author:** Nadeem Douba  
**Version:** 0.3  
**Source:** <https://github.com/portswigger/dotnet-beautifier>  
**Updated:** 23 Jan 2017  
**Rating:** 5 stars  
**Popularity:** 1000

[Install](#) [Submit rating](#)

From:  
 / - Les cours du BTS SIO

Permanent link:  
[/doku.php/systeme/outils/burpsuite?rev=1750428069](https://doku.php/systeme/outils/burpsuite?rev=1750428069)

Last update: 2025/06/20 16:01

