

Burpsuite

Burp Suite est le proxy web le plus courant pour les tests de pénétration web.

Il dispose d'une excellente interface utilisateurs pour ses différentes fonctionnalités et fournit même un navigateur Chromium intégré pour tester les applications web.

Il existe une version commercial qui débloquent certaines fonctionnalités.

Installation

<https://portswigger.net/burp/releases>

```
seliatis@framework$ java -jar </path/to/burpsuite.jar>
```

Interception des requetes avec Burp

Naviguer vers Proxy puis intercept. Et activer avec intercept on



Burp Intruder

Type d'attaque

Sniper

Cette attaque place chaque charge utile dans chaque position de charge utile à tour de rôle. Elle utilise un seul ensemble de données utiles.

Le nombre total de requêtes générées par l'attaque est le produit du nombre de positions et du nombre de payloads dans l'ensemble de payloads.

Elle est utilisée pour analyser un certain nombre de paramètres de requête individuellement afin de détecter des vulnérabilités communes.

Batterie Ram

Cette attaque place la même charge utile dans toutes les positions de charge utile définies simultanément.

Elle est utile lorsqu'une attaque nécessite l'insertion de la même donnée à plusieurs endroits de la demande.

Exemple: nom d'utilisateur dans un cookie et dans le paramètre du corps.

Cluster Bomb

Cette attaque itère à travers un ensemble de charges utiles différentes pour chaque position définie. Les charges utilisées sont placées simultanément dans chaque position.

Exemple

Première demande

Position 1 = Première charge utilise de l'ensemble 1

Position 2 = Première charge utilise de l'ensemble 2

Deuxième demande:

Position 1 = Deuxième charge utilise de l'ensemble 1

Position 2 = Deuxième charge utilise de l'ensemble 2

Troisième demande:

Position 1 = Troisième charge utilise de l'ensemble 1

Position 2 = Troisième charge utilise de l'ensemble 2

Le nombre total de demandes générées par l'attaque correspond au nombre de charges utiles dans le plus


Utilisé pour une attaque qui nécessite l'insertion de données inconnues ou sans rapport entre elles à plusieurs endroits de la demande. (Utilisateur et mot de passes par exemple)

Repeater


```
1 POST /vulnerabilities/exec/ HTTP/1.1
2 Host: localhost:4280
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:127.0) Gecko/20100101 Firefox/127.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 26
9 Origin: http://localhost:4280
10 Connection: keep-alive
11 Referer: http://localhost:4280/vulnerabilities/exec/
12 Cookie: security-low; PHPSESSID=19207963850de5658cdc9938bfcebd2
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-User: ?1
18 Priority: u=1
19
20 ip=127.0.0.1Submit=Submit
```

Response

Pretty Raw Hex Render



Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

CSP Bypass

JavaScript

Authorisation Bypass

Open HTTP Redirect

DVWA Security

PHP Info

About

Logout

Vulnerability: Command Injection

Ping a device

Enter an IP address:

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data:
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.020 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.089 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.055 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.072 ms

--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3032ms
rtt min/avg/max/ndev = 0.020/0.059/0.089/0.025 ms
```

More Information

- <https://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution>
- <http://www.ss64.com/bash/>
- <http://www.ss64.com/nt/>
- https://owasp.org/www-community/attacks/Command_Injection

View Source View Help

Damn Vulnerable Web Application (DVWA)

Target: http://localhost:4280 HTTP/1

Inspector

Request attributes 2

Request query parameters 0

Request body parameters 2

Request cookies 2

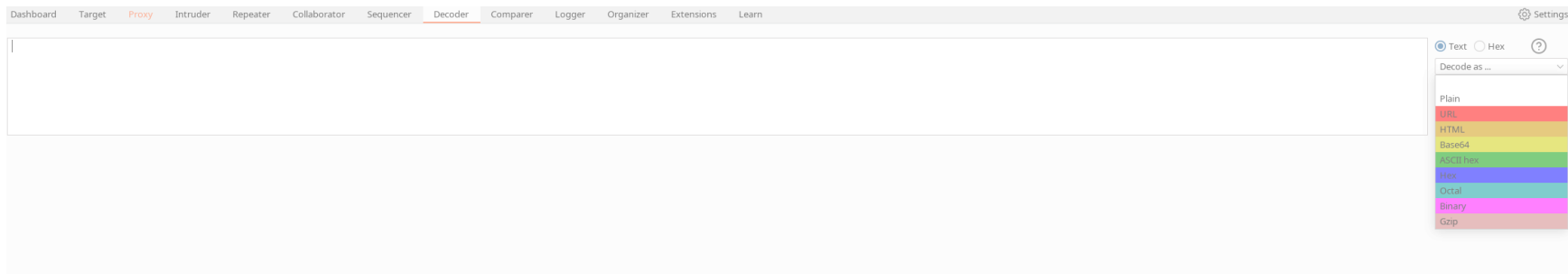
Request headers 17

Response headers 11


Notes

La répétition des requêtes nous permet de renvoyer toute requête web qui a déjà traversé le proxy web. Cela nous permet d'apporter des modifications rapides à toute demande avant de l'envoyer, puis d'obtenir la réponse dans nos outils sans intercepter et modifier chaque demande.

Encoding / Decoding



SGVsbG8gMjYwMA==

☒ Text ☐ Hex 

Decode as ...

Encode as ...

Hash ...

Smart decode

Hello 2600

☒ Text ☐ Hex

Decode as ...

Encode as ...

Hash ...

Smart decode

BurpSuite Scanner

Dispo dans la version PRO

2 Types: Passif et Actif

- Scanner Passif

l'analyse passive n'envoie pas de nouvelles requêtes, mais analyse la source des pages déjà visitées dans la cible/le champ d'application et tente ensuite d'identifier les vulnérabilités potentielles. Ceci est très utile pour une analyse rapide d'une cible spécifique, comme des balises HTML manquantes ou des vulnérabilités XSS potentielles basées sur le DOM. Cependant, sans envoyer de requêtes pour tester et vérifier ces vulnérabilités, une analyse passive ne peut que suggérer une liste de vulnérabilités potentielles. Cependant, le scanner passif de Burp fournit un niveau de confiance pour chaque vulnérabilité identifiée, ce qui est également utile pour classer les vulnérabilités potentielles par ordre de priorité.

- Scanner Actif

scan actif exécute un scan plus complet qu'un scan passif, comme suit :

- Il commence par exécuter un Crawl et un fuzzer web (comme dirbuster/ffuf) pour identifier toutes les pages possibles.
- Il exécute un balayage passif sur toutes les pages identifiées.
- Il vérifie chacune des vulnérabilités identifiées dans le cadre de l'analyse passive et envoie des requêtes pour les vérifier.
- Il effectue une analyse JavaScript pour identifier d'autres vulnérabilités potentielles.
- Il analyse divers points d'insertion et paramètres identifiés pour rechercher des vulnérabilités courantes comme XSS, l'injection de commande, l'injection de code SQL et d'autres vulnérabilités courantes sur le web.

Le scanner Burp Active est considéré comme l'un des meilleurs outils dans ce domaine et est fréquemment mis à jour pour détecter les nouvelles vulnérabilités Web identifiées par l'équipe de recherche de Burp.

Extension BurpSuite

BApp Store

DashboardTargetProxyIntruderRepeaterCollaboratorSequencerDecoderComparerLoggerOrganizerExtensions

InstalledBApp StoreAPIsBChecksExtensions settings

Total estimated system impact: **Low**

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	System imp...	Detail
Decoder Improved	✓	☆☆☆☆	<div></div>	19 févr. 2021	Medium	
JSON Decoder		☆☆☆☆	<div></div>	24 janv. 2017	Low	
NTLM Challenge Decoder		☆☆☆☆	<div></div>	25 mars 2021	Low	
Protobuf Decoder		☆☆☆☆	<div></div>	04 août 2021	Low	
SAML Encoder / Decoder		☆☆☆☆	<div></div>	01 juil. 2014	Low	
WebAuthn CBOR Decod...		☆☆☆☆	<div></div>	09 déc. 2022	Low	
WebSphere Portlet Stat...		☆☆☆☆	<div></div>	17 févr. 2015	Low	
XChromeLogger Decod...		☆☆☆☆	<div></div>	15 déc. 2021	Low	
Freddy, Deserialization ...		☆☆☆☆	<div></div>	02 avr. 2020	Medium	Requires Burp ...
JSON Web Token Attack...		☆☆☆☆	<div></div>	04 févr. 2022	Medium	
Look Over There		☆☆☆☆	<div></div>	01 mars 2023	Low	

Decoder Improved

Decoder Improved is a data transformation plugin for Burp

All of the Built-in Burp Decoder Modes

Decoder Improved supports all of decoder's encoding, decc SHA-256, SHA-384, and SHA-512.

Tabs

Like many of Burp Suite's features, Decoder Improved has s

Unicode Support

Decoder Improved is backed by arrays of Java Bytes that do

An Improved Hex Editor

Decoder Improved comes bundled with the Delta Hexadeci

.NET beautifier (Free)	J2EEScan (Pro)	Software Vulnerability Scanner (Pro)
Software Version Reporter (Pro)	Active Scan++ (Pro)	Additional Scanner Checks (Pro)
AWS Security Checks (Pro)	Backslash Powered Scanner (Pro)	Wsdler (Free)
Java Deserialization Scanner (Free)	C02 (Free)	Cloud Storage Tester (Pro)
CMS Scanner (Pro)	Error Message Checks (Pro)	Detect Dynamic JS (Pro)
Headers Analyzer (Pro)	HTML5 Auditor (Pro)	PHP Object Injection Check (Pro)
JavaScript Security (Pro)	Retire.JS (Pro)	CSP Auditor (Free)
Random IP Address Header (Free)	Autorize (Free)	CSRF Scanner (Pro)
JS Link Finder (Pro)		

Ressources pour s'entraîner a burp ou aux attaques web plus simplement.

<https://portswigger.net/web-security>

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

<https://ginandjuice.shop/>

Machines HTB / VulnLab / <https://www.vulnhub.com/>

<https://google-gruyere.appspot.com/start>

<https://ctf.hacker101.com/ctf>

Buggy Web Application (BWAPP) <http://www.itsecgames.com/>

<https://github.com/vavkamil/awesome-vulnerable-apps>

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