

# assignment-4

## What is Burp Suite?

Burp Suite is a widely used cybersecurity testing tool developed by PortSwigger. It is designed for security testing web applications, and it's particularly popular among ethical hackers, penetration testers, and security professionals. Burp Suite helps identify various security vulnerabilities in web applications, allowing developers and security teams to address these issues before they can be exploited by malicious actors.



## Why Burp Suite?

1. **Comprehensive Web Application Testing:** Burp Suite offers a wide range of tools for testing web applications, including scanning for common vulnerabilities like cross-site scripting (XSS), SQL injection, and more.
2. **User-Friendly Interface:** It provides a user-friendly and intuitive interface, making it accessible for both beginners and experienced security professionals.
3. **Active and Passive Scanning:** Burp Suite can actively scan web applications for vulnerabilities, but it also allows for passive scanning to identify potential issues passively while you browse the application.
4. **Extensive Support for Various Protocols:** It supports HTTP, HTTPS, and other protocols, which is crucial for testing applications that use secure connections.

5. **Advanced Crawling and Scanning:** Burp Suite can automatically crawl an application, identifying various paths and inputs. It then applies various scanning techniques to find vulnerabilities.
6. **Repeater and Intruder Tools:** These tools allow for manual testing of requests and responses, and automated fuzzing of input parameters to identify vulnerabilities.
7. **Session Management and Analysis:** It helps manage user sessions and analyze session tokens and cookies, which is crucial for identifying security issues related to session management.
8. **Integration and Extensibility:** Burp Suite can be extended with plugins and has robust support for integration with other tools and frameworks, allowing for customized testing workflows.

## Features of Burp Suite:

1. **Proxy:** Allows you to intercept and modify HTTP/S traffic between your browser and the target application.
2. **Spider:** Automatically discovers and maps out the structure of a website, identifying all accessible content.
3. **Scanner:** Scans for a wide range of web vulnerabilities including SQL injection, cross-site scripting (XSS), remote command execution, and more.
4. **Intruder:** Performs automated attacks on web applications, allowing you to test for a wide range of vulnerabilities by customizing requests.
5. **Repeater:** Provides a simple interface for manually manipulating and re-sending individual HTTP requests.
6. **Sequencer:** Analyzes the quality of randomness in tokens or session IDs.
7. **Decoder:** Provides various tools for transforming and decoding data.
8. **Comparer:** Allows you to compare two pieces of data, which is useful for identifying differences in responses.
9. **Extensibility:** Burp Suite can be extended with custom plugins and integrations, allowing you to tailor it to your specific needs.
10. **Collaborator:** Helps identify out-of-band vulnerabilities by providing a unique domain for interacting with the application.

11. **Session Handling:** Manages user sessions and helps identify security issues related to session tokens and cookies.
12. **Reporting:** Generates detailed reports of vulnerabilities identified during testing.

## Test the vulnerabilities of testfire.net

testfire vul scab / Plugin #104743  
[Back to Vulnerability Group](#)

Configure Audit Trail Launch Report Export

Hosts 1 Vulnerabilities 17 History 1

**MEDIUM** TLS Version 1.0 Protocol Detection

**Description**

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

**Solution**

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

**See Also**

<https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00>

**Output**

TLSv1 is enabled and the server supports at least one cipher.

To see debug logs, please visit individual host

Port	Hosts
443 / tcp / www	65.61.137.117

**Plugin Details**

Severity: Medium  
ID: 104743  
Version: 1.10  
Type: remote  
Family: Service detection  
Published: November 22, 2017  
Modified: April 19, 2023

**Risk Information**

Risk Factor: Medium  
**CVSS v3.0 Base Score 6.5**  
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N  
CVSS v2.0 Base Score: 6.1  
CVSS v2.0 Vector: CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N

**Vulnerability Information**

Asset Inventory: True

**Reference Information**

CWE: 327

Hosts 1

Vulnerabilities 17

History 1

LOW

## SSL/TLS Diffie-Hellman Modulus &lt;= 1024 Bits (Logjam)

&lt; &gt;

## Plugin Details

✎

## Description

The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits. Through cryptanalysis, a third party may be able to find the shared secret in a short amount of time (depending on modulus size and attacker resources). This may allow an attacker to recover the plaintext or potentially violate the integrity of connections.

## Solution

Reconfigure the service to use a unique Diffie-Hellman moduli of 2048 bits or greater.

## See Also

<https://weakdh.org/>

## Output

Vulnerable connection combinations :

```
SSL/TLS version : TLSv1.0
Cipher suite    : TLS1_CK_DHE_RSA_WITH_AES_256_CBC_SHA
Diffie-Hellman MODP size (bits) : 1024
Warning - This is a known static Oakley Group2 modulus. This may make
the remote host more vulnerable to the Logjam attack.
Logjam attack difficulty : Hard (would require nation-state resources)
```

[more...](#)

To see debug logs, please visit individual host

Port ^

Hosts

443 / tcp / www	65.61.137.117
-----------------	---------------

Severity:	Low
ID:	83875
Version:	1.40
Type:	remote
Family:	Misc.
Published:	May 28, 2015
Modified:	December 5, 2022

## VPR Key Drivers

Threat Recency: No recorded events  
Threat Intensity: Very Low  
Exploit Code Maturity: Unproven  
Age of Vuln: 730 days +  
Product Coverage: Very High  
CVSSv3 Impact Score: 1.4  
Threat Sources: No recorded events

## Risk Information

Vulnerability Priority Rating (VPR): 4.5  
Risk Factor: Low  
**CVSS v3.0 Base Score 3.7**  
CVSS v3.0 Vector:  
CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N  
CVSS v3.0 Temporal Vector:

Hosts 1

Vulnerabilities 17

History 1

INFO

## HTTP Server Type and Version

&gt;

## Plugin Details

✎

## Description

This plugin attempts to determine the type and the version of the remote web server.

## Output

The remote web server type is :

Apache-Coyote/1.1

To see debug logs, please visit individual host

Port ^

Hosts

443 / tcp / www	65.61.137.117
-----------------	---------------

80 / tcp / www	65.61.137.117
----------------	---------------

8080 / tcp / www	65.61.137.117
------------------	---------------

Severity:	Info
ID:	10107
Version:	1.141
Type:	remote
Family:	Web Servers
Published:	January 4, 2000
Modified:	October 30, 2020

## Risk Information

Risk Factor: None

## Vulnerability Information

Asset Inventory: True

## Reference Information

IAVT: 0001-T-0931

Hosts 1

Vulnerabilities 17

History 1

INFO

SSL Cipher Block Chaining Cipher Suites Supported

< >

Plugin Details

✎

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

<https://www.openssl.org/docs/manmaster/man1/ciphers.html>  
<http://www.nessus.org/u?cc4a822a>  
<https://www.openssl.org/~bodo/tls-cbc.txt>

Severity: Info  
ID: 70544  
Version: 1.3  
Type: remote  
Family: General  
Published: October 22, 2013  
Modified: February 3, 2021

Output

Here is the list of SSL CBC ciphers supported by the remote server :

High Strength Ciphers (>= 112-bit key)

Name	Code	KEX	Auth	Encryption	MAC
-----	-----	----	----	-----	----
DHE-RSA-AES128-SHA	0x00, 0x33	DH	RSA	AES-CBC(128)	SHA1
DHE-RSA-AES256-SHA	0x00, 0x39	DH	RSA	AES-CBC(256)	SHA1
ECDHE-RSA-AES128-SHA	0xC0, 0x13	ECDH	RSA	AES-CBC(128)	SHA1
more...					

To see debug logs, please visit individual host

Port ^

Hosts

443 / tcp / www

65.61.137.117

Risk Information

Risk Factor: None

paavankumar.s

21BAI1527