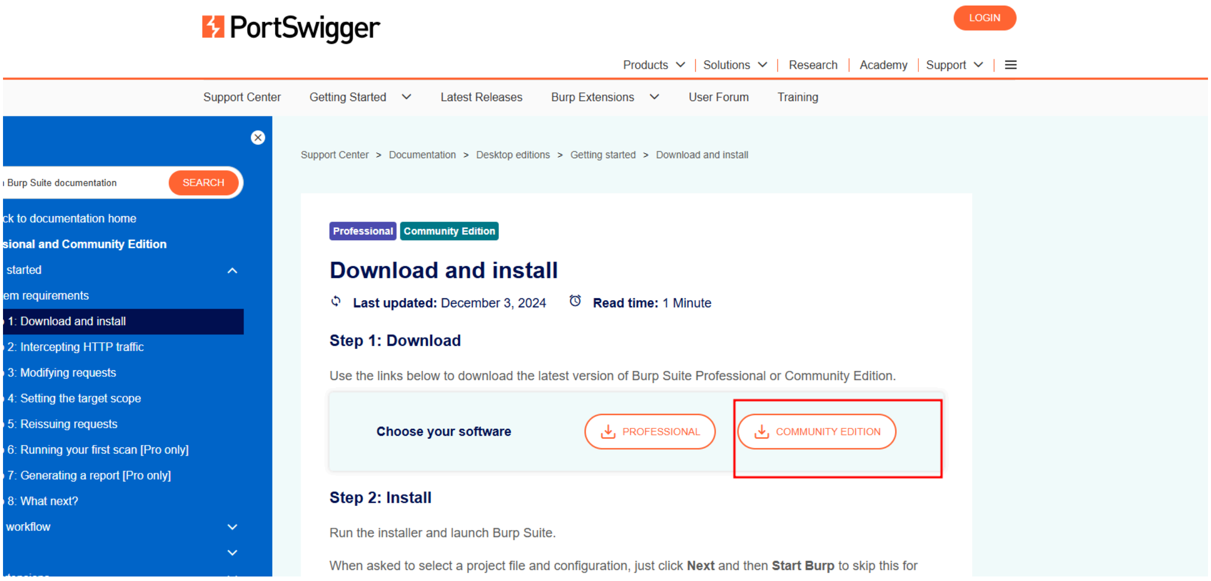
Name: Chetan Satone
Prn no. 008

Download Burp suite


PortSwigger
LOGIN
Products | Solutions | Research | Academy | Support
Support Center
Getting Started
Latest Releases
Burp Extensions
User Forum
Training
Burp Suite documentation
SEARCH
ck to documentation home
sional and Community Edition
started
em requirements
1: Download and install
2: Intercepting HTTP traffic
3: Modifying requests
4: Setting the target scope
5: Reissuing requests
6: Running your first scan [Pro only]
7: Generating a report [Pro only]
8: What next?
workflow
Support Center > Documentation > Desktop editions > Getting started > Download and install
Professional
Community Edition

Download and install

Last updated: December 3, 2024 **Read time:** 1 Minute

Step 1: Download

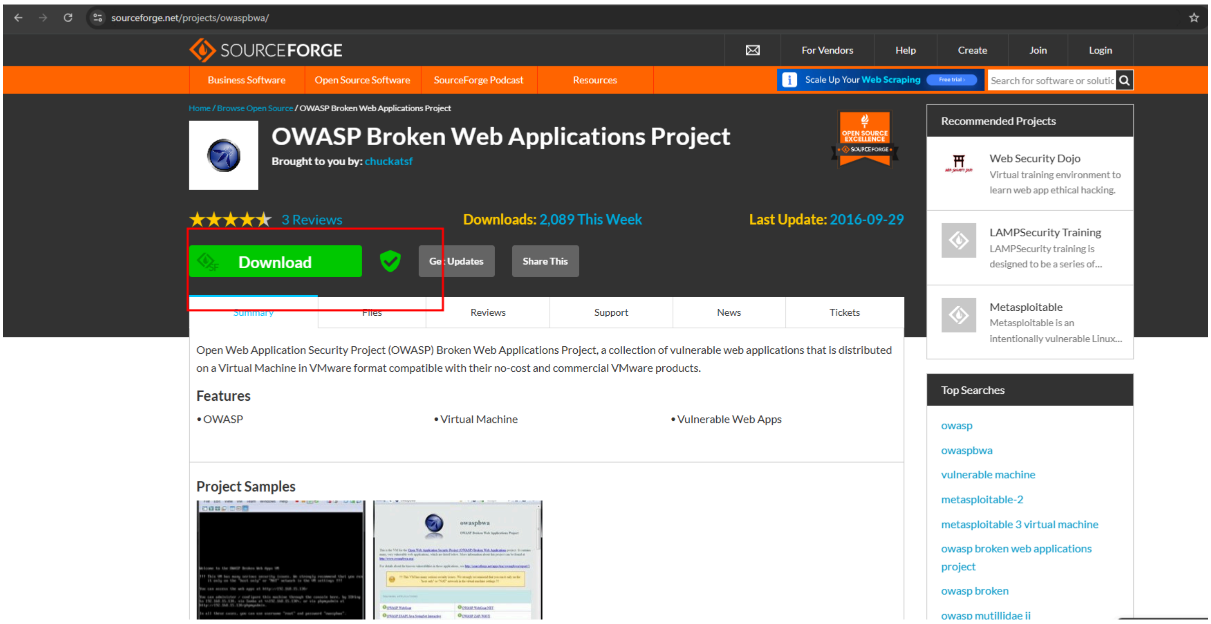
Use the links below to download the latest version of Burp Suite Professional or Community Edition.

Choose your software PROFESSIONAL COMMUNITY EDITION

Step 2: Install

Run the installer and launch Burp Suite.

When asked to select a project file and configuration, just click **Next** and then **Start Burp** to skip this for



OWASP Broken Web Applications Project

Brought to you by: chuckatsf

★★★★★ 3 Reviews **Downloads:** 2,089 This Week **Last Update:** 2016-09-29

Open Web Application Security Project (OWASP) Broken Web Applications Project, a collection of vulnerable web applications that is distributed on a Virtual Machine in VMware format compatible with their no-cost and commercial VMware products.

Features

- OWASP
- Virtual Machine
- Vulnerable Web Apps

Project Samples

Recommended Projects

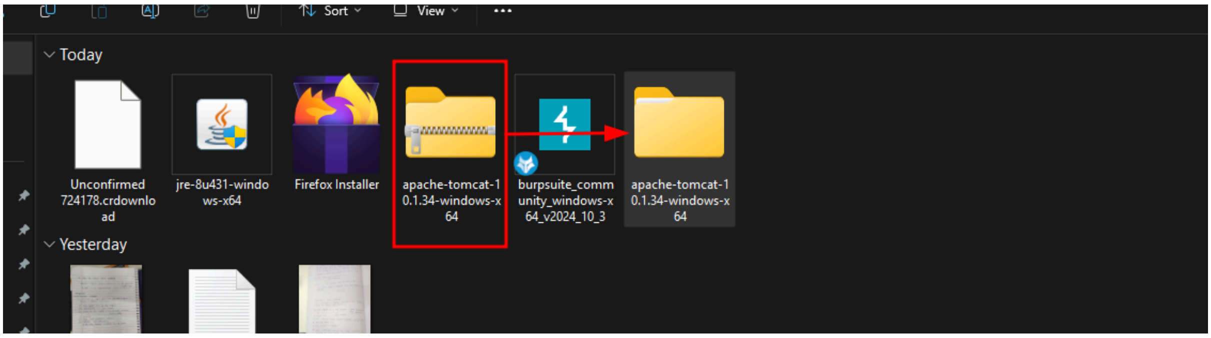
Web Security Dojo
Virtual training environment to learn web app ethical hacking.

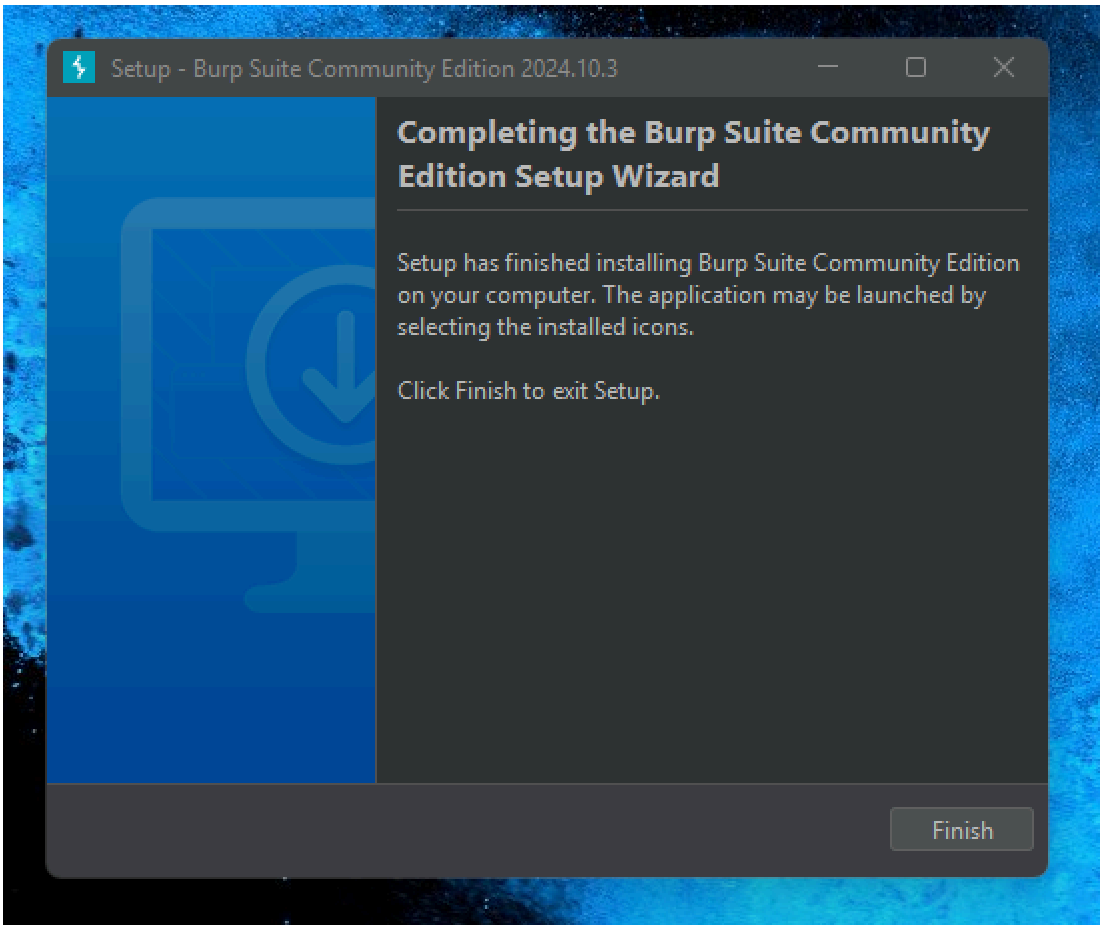
LAMPSecurity Training
LAMPSecurity training is designed to be a series of...

Metasploitable
Metasploitable is an intentionally vulnerable Linux...

Top Searches

owasp
owaspbwa
vulnerable machine
metasploitable-2
metasploitable 3 virtual machine
owasp broken web applications project
owasp broken
owasp mutillidae ii

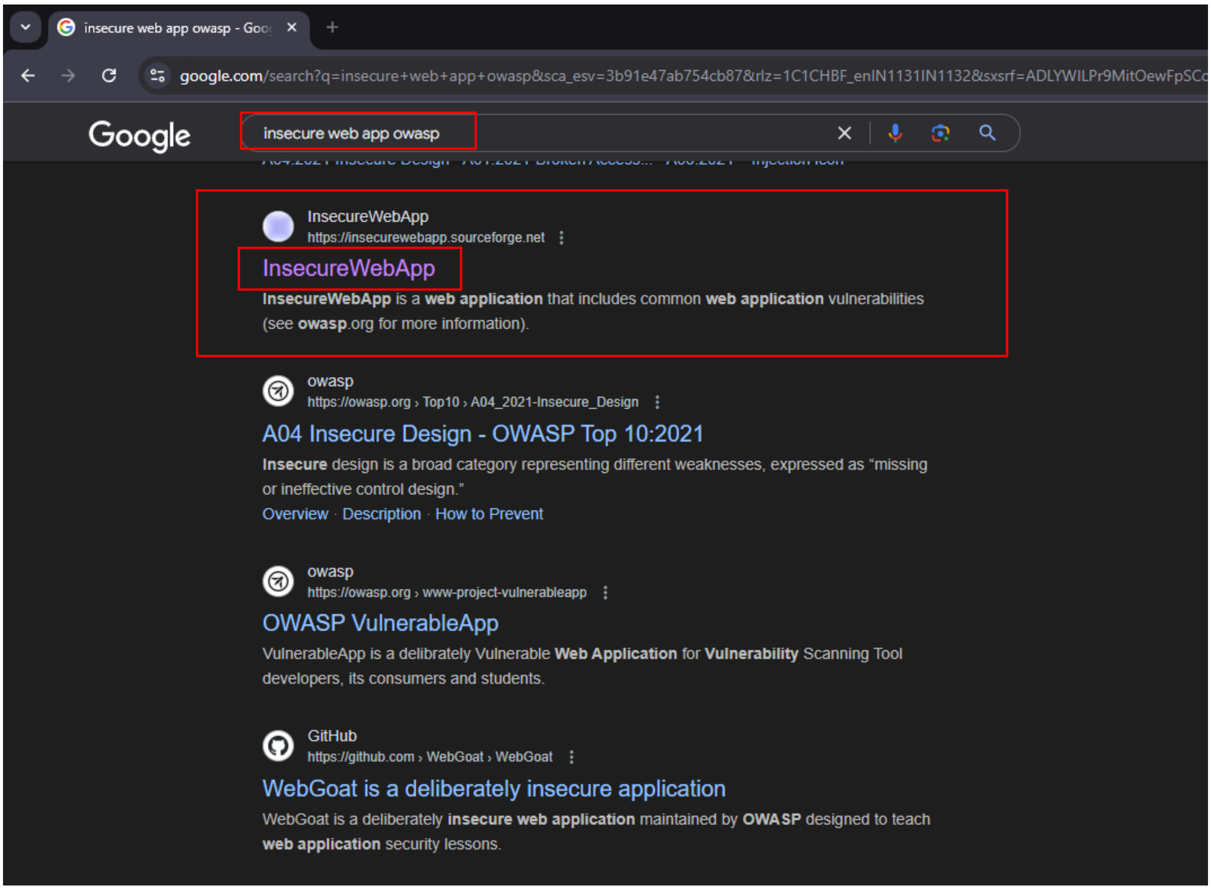

Sort
View
Today
Unconfirmed 724178.crdownload
jre-8u431-windows-x64
Firefox Installer
apache-tomcat-10.1.34-windows-x64
burpsuite_community_windows-x64_v2024_10_3
apache-tomcat-10.1.34-windows-x64
Yesterday



Completing the Burp Suite Community Edition Setup Wizard

Setup has finished installing Burp Suite Community Edition on your computer. The application may be launched by selecting the installed icons.

Click Finish to exit Setup.



insecure web app owasp - Goo
google.com/search?q=insecure+web+app+owasp&sca_esv=3b91e47ab754cb87&rlz=1C1CHBF_enIN1131IN1132&sxsrf=ADLYWILPr9MitOewFpSCo
Google
insecure web app owasp

InsecureWebApp
https://insecurewebapp.sourceforge.net

InsecureWebApp

InsecureWebApp is a **web application** that includes common **web application** vulnerabilities (see **owasp**.org for more information).

owasp
https://owasp.org › Top10 › A04_2021-Insecure_Design

A04 Insecure Design - OWASP Top 10:2021

Insecure design is a broad category representing different weaknesses, expressed as "missing or ineffective control design."

Overview · Description · How to Prevent

owasp
https://owasp.org › www-project-vulnerableapp

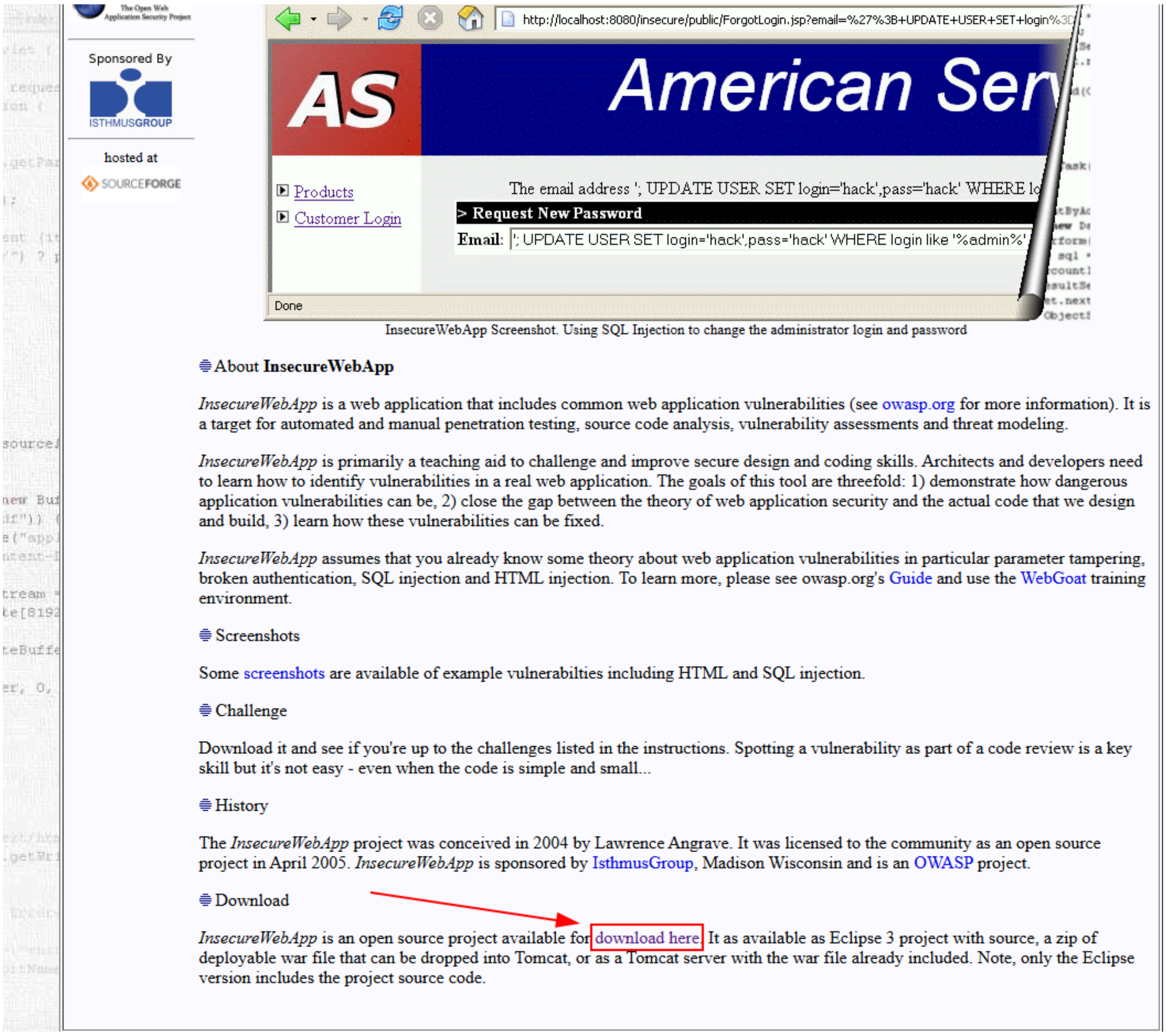
OWASP VulnerableApp

VulnerableApp is a delibrately Vulnerable **Web Application** for **Vulnerability** Scanning Tool developers, its consumers and students.

GitHub
https://github.com › WebGoat › WebGoat

WebGoat is a deliberately insecure application

WebGoat is a deliberately **insecure web application** maintained by **OWASP** designed to teach **web application** security lessons.



http://localhost:8080/insecure/public/ForgotLogin.jsp?email=%27%3B+UPDATE+USER+SET+login%3D

The email address '; UPDATE USER SET login='hack',pass='hack' WHERE lo

> Request New Password

Email: '; UPDATE USER SET login='hack',pass='hack' WHERE login like '%admin%'

InsecureWebApp Screenshot. Using SQL Injection to change the administrator login and password

About **InsecureWebApp**

InsecureWebApp is a web application that includes common web application vulnerabilities (see owasp.org for more information). It is a target for automated and manual penetration testing, source code analysis, vulnerability assessments and threat modeling.

InsecureWebApp is primarily a teaching aid to challenge and improve secure design and coding skills. Architects and developers need to learn how to identify vulnerabilities in a real web application. The goals of this tool are threefold: 1) demonstrate how dangerous application vulnerabilities can be, 2) close the gap between the theory of web application security and the actual code that we design and build, 3) learn how these vulnerabilities can be fixed.

InsecureWebApp assumes that you already know some theory about web application vulnerabilities in particular parameter tampering, broken authentication, SQL injection and HTML injection. To learn more, please see owasp.org's Guide and use the WebGoat training environment.

Screenshots

Some screenshots are available of example vulnerabilties including HTML and SQL injection.

Challenge

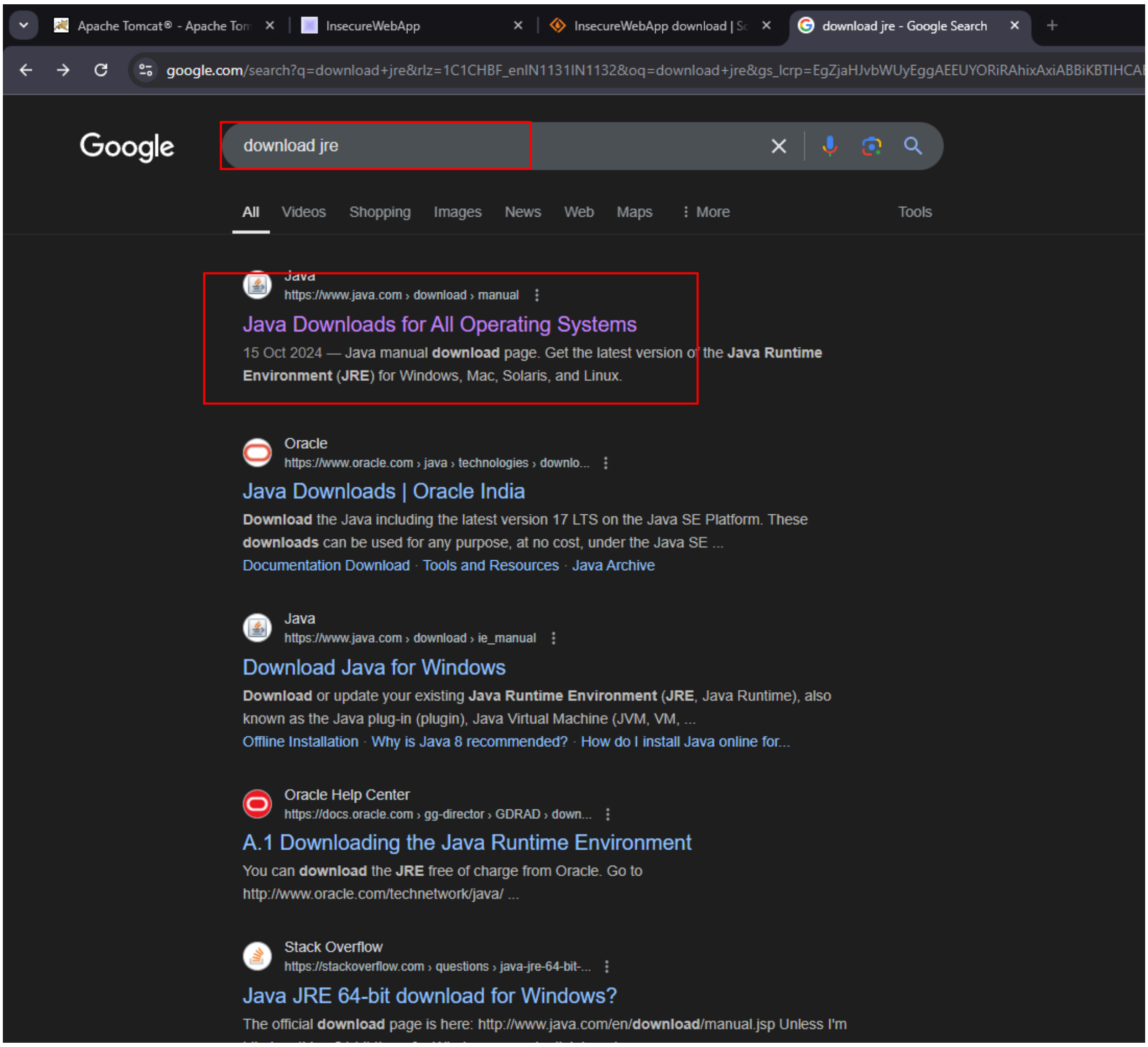
Download it and see if you're up to the challenges listed in the instructions. Spotting a vulnerability as part of a code review is a key skill but it's not easy - even when the code is simple and small...

History

The *InsecureWebApp* project was conceived in 2004 by Lawrence Angrave. It was licensed to the community as an open source project in April 2005. *InsecureWebApp* is sponsored by IsthmusGroup, Madison Wisconsin and is an OWASP project.

Download

InsecureWebApp is an open source project available for download here. It as available as Eclipse 3 project with source, a zip of deployable war file that can be dropped into Tomcat, or as a Tomcat server with the war file already included. Note, only the Eclipse version includes the project source code.


Apache Tomcat® - Apache Tom
InsecureWebApp
InsecureWebApp download | Sc
download jre - Google Search
google.com/search?q=download+jre&rlz=1C1CHBF_enIN1131IN1132&oq=download+jre&gs_lcrp=EgZjaHJvbWUyEggAEEUYORiRAhixAxiABBiKBTIHCAE
Google
download jre
All
Videos
Shopping
Images
News
Web
Maps
More
Tools

Java
https://www.java.com › download › manual

Java Downloads for All Operating Systems

15 Oct 2024 — Java manual **download** page. Get the latest version of the **Java Runtime Environment** (**JRE**) for Windows, Mac, Solaris, and Linux.

Oracle
https://www.oracle.com › java › technologies › downlo...

Java Downloads | Oracle India

Download the Java including the latest version 17 LTS on the Java SE Platform. These **downloads** can be used for any purpose, at no cost, under the Java SE ...

Documentation Download · Tools and Resources · Java Archive

Java
https://www.java.com › download › ie_manual

Download Java for Windows

Download or update your existing **Java Runtime Environment** (**JRE**, Java Runtime), also known as the Java plug-in (plugin), Java Virtual Machine (JVM, VM, ...

Offline Installation · Why is Java 8 recommended? · How do I install Java online for...

Oracle Help Center
https://docs.oracle.com › gg-director › GDRAD › down...

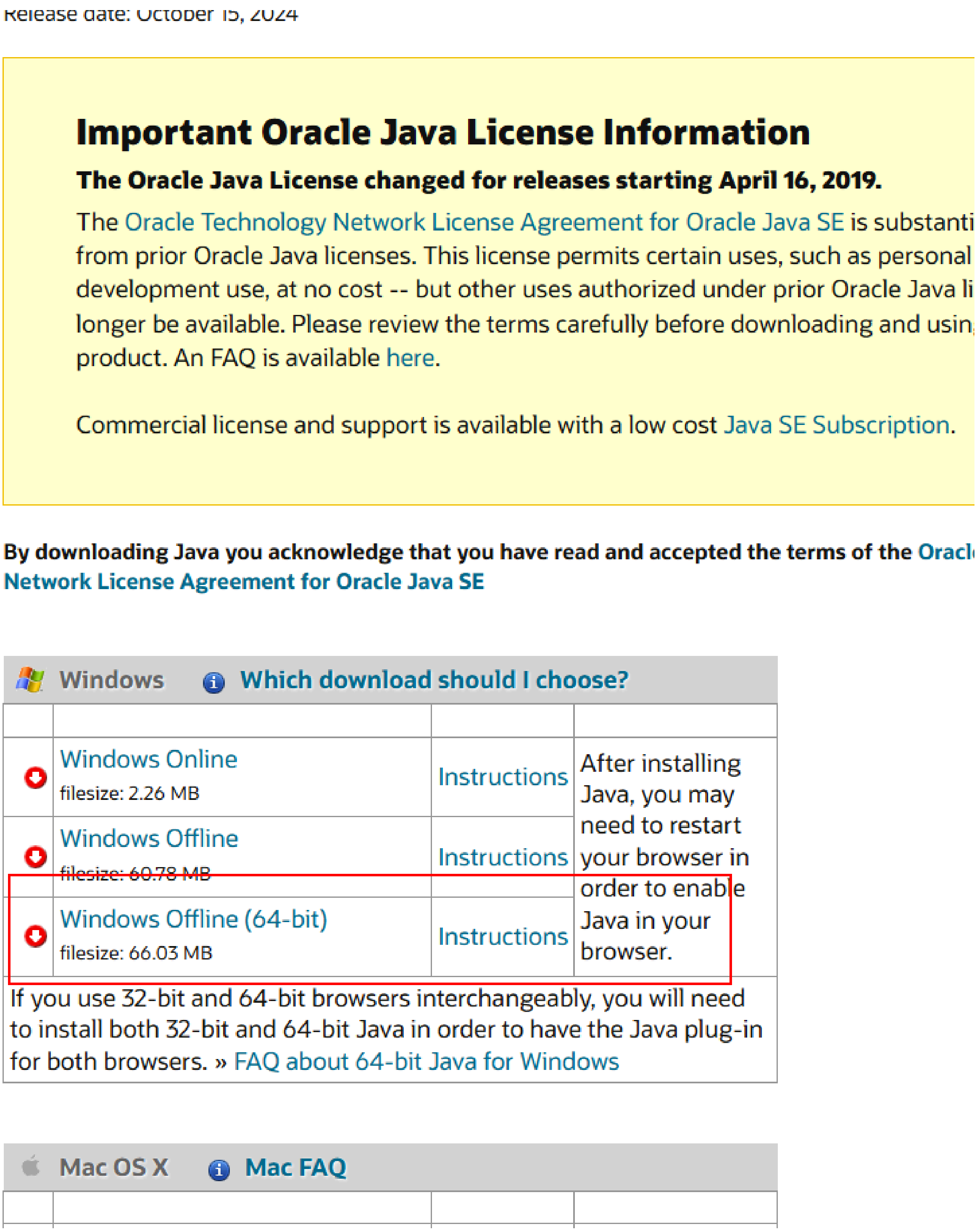
A.1 Downloading the Java Runtime Environment

You can **download** the **JRE** free of charge from Oracle. Go to http://www.oracle.com/technetwork/java/ ...

Stack Overflow
https://stackoverflow.com › questions › java-jre-64-bit-...

Java JRE 64-bit download for Windows?

The official **download** page is here: http://www.java.com/en/**download**/manual.jsp Unless I'm



Release date: October 15, 2024

Important Oracle Java License Information

The Oracle Java License changed for releases starting April 16, 2019.

The Oracle Technology Network License Agreement for Oracle Java SE is substanti
from prior Oracle Java licenses. This license permits certain uses, such as personal
development use, at no cost -- but other uses authorized under prior Oracle Java li
longer be available. Please review the terms carefully before downloading and usin
product. An FAQ is available here.

Commercial license and support is available with a low cost Java SE Subscription.

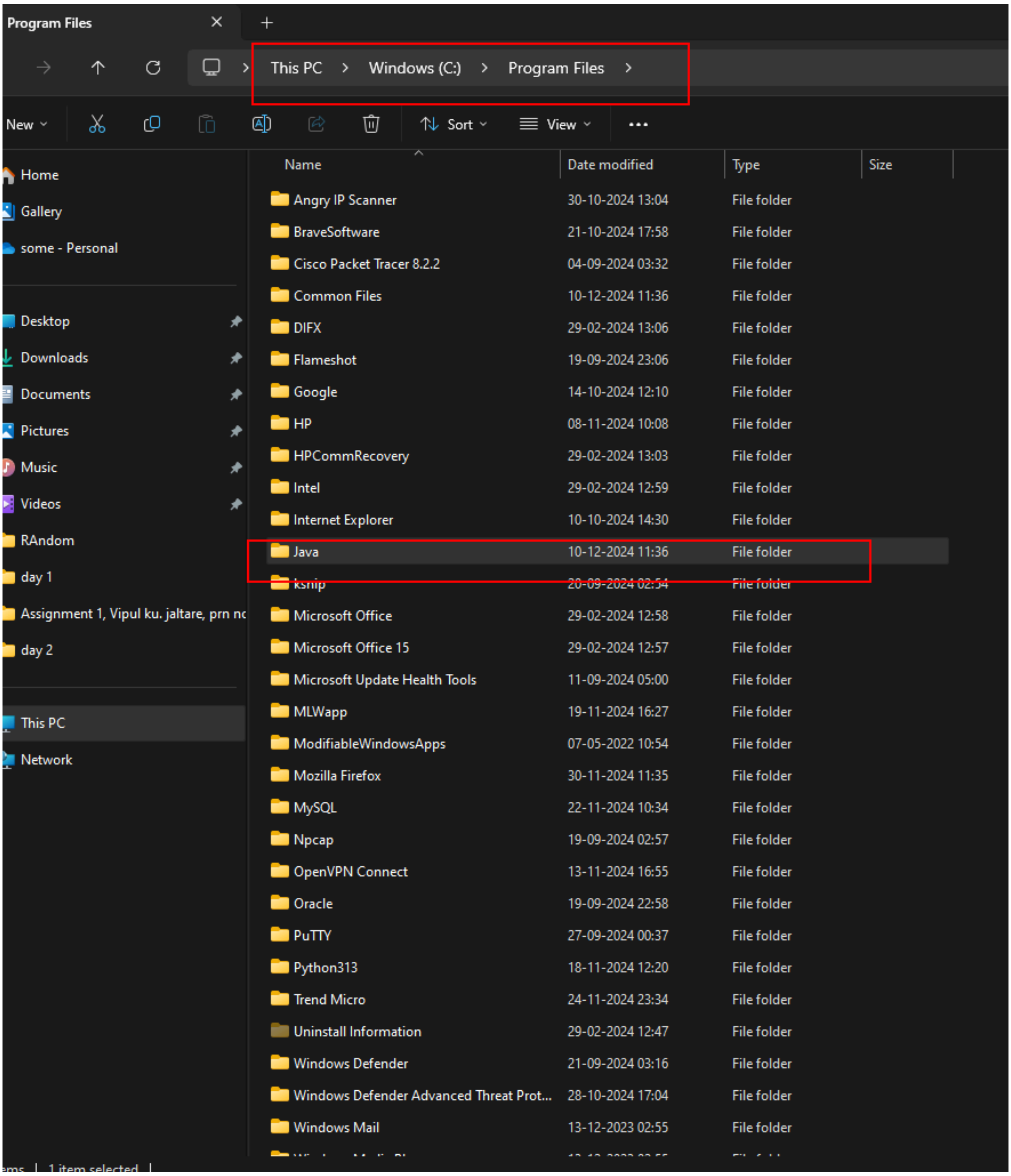
By downloading Java you acknowledge that you have read and accepted the terms of the Oracl
Network License Agreement for Oracle Java SE

Windows Which download should I choose?

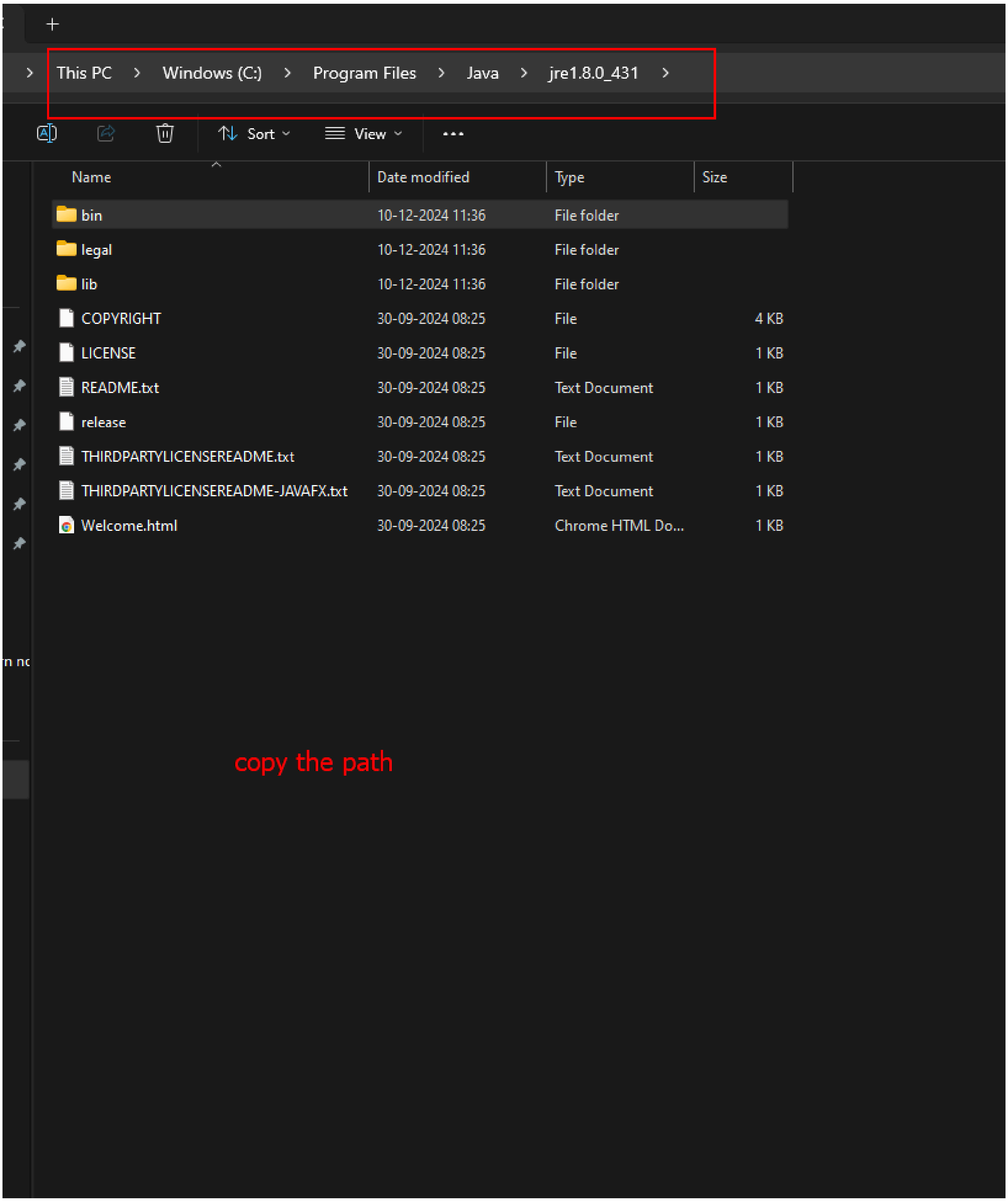
	Windows Online filesize: 2.26 MB	Instructions	After installing Java, you may need to restart your browser in order to enable Java in your browser.
	Windows Offline filesize: 60.78 MB	Instructions	
	Windows Offline (64-bit) filesize: 66.03 MB	Instructions	

If you use 32-bit and 64-bit browsers interchangeably, you will need to install both 32-bit and 64-bit Java in order to have the Java plug-in for both browsers. » FAQ about 64-bit Java for Windows

Mac OS X Mac FAQ



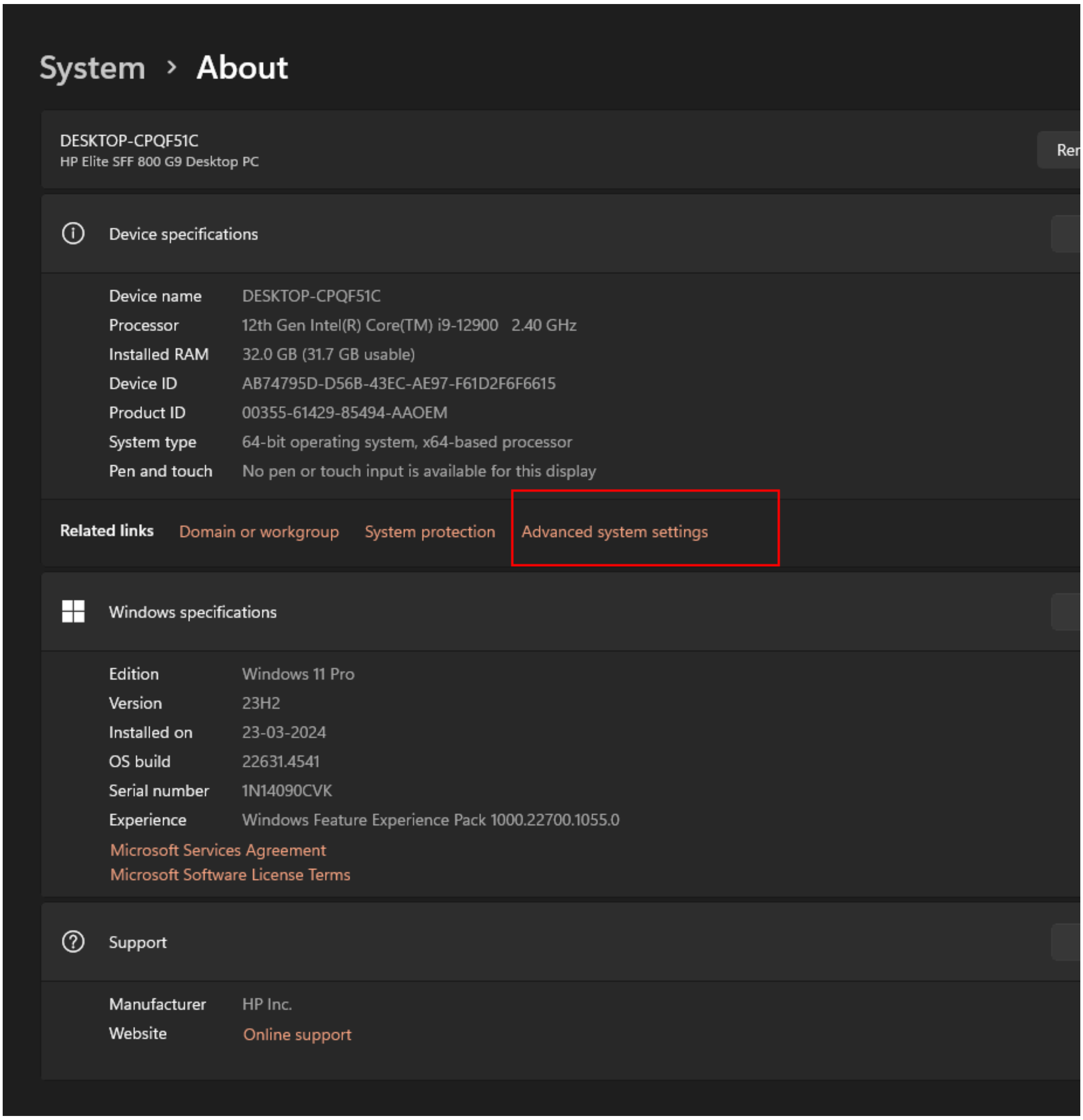
Name	Date modified	Type	Size
Angry IP Scanner	30-10-2024 13:04	File folder	
BraveSoftware	21-10-2024 17:58	File folder	
Cisco Packet Tracer 8.2.2	04-09-2024 03:32	File folder	
Common Files	10-12-2024 11:36	File folder	
DIFX	29-02-2024 13:06	File folder	
Flameshot	19-09-2024 23:06	File folder	
Google	14-10-2024 12:10	File folder	
HP	08-11-2024 10:08	File folder	
HPCommRecovery	29-02-2024 13:03	File folder	
Intel	29-02-2024 12:59	File folder	
Internet Explorer	10-10-2024 14:30	File folder	
Java	10-12-2024 11:36	File folder	
ksnip	20-09-2024 02:54	File folder	
Microsoft Office	29-02-2024 12:58	File folder	
Microsoft Office 15	29-02-2024 12:57	File folder	
Microsoft Update Health Tools	11-09-2024 05:00	File folder	
MLWapp	19-11-2024 16:27	File folder	
ModifiableWindowsApps	07-05-2022 10:54	File folder	
Mozilla Firefox	30-11-2024 11:35	File folder	
MySQL	22-11-2024 10:34	File folder	
Npcap	19-09-2024 02:57	File folder	
OpenVPN Connect	13-11-2024 16:55	File folder	
Oracle	19-09-2024 22:58	File folder	
PuTTY	27-09-2024 00:37	File folder	
Python313	18-11-2024 12:20	File folder	
Trend Micro	24-11-2024 23:34	File folder	
Uninstall Information	29-02-2024 12:47	File folder	
Windows Defender	21-09-2024 03:16	File folder	
Windows Defender Advanced Threat Prot...	28-10-2024 17:04	File folder	
Windows Mail	13-12-2023 02:55	File folder	



This PC > Windows (C:) > Program Files > Java > jre1.8.0_431 >

Name	Date modified	Type	Size
bin	10-12-2024 11:36	File folder	
legal	10-12-2024 11:36	File folder	
lib	10-12-2024 11:36	File folder	
COPYRIGHT	30-09-2024 08:25	File	4 KB
LICENSE	30-09-2024 08:25	File	1 KB
README.txt	30-09-2024 08:25	Text Document	1 KB
release	30-09-2024 08:25	File	1 KB
THIRDPARTYLICENSEREADME.txt	30-09-2024 08:25	Text Document	1 KB
THIRDPARTYLICENSEREADME-JAVAFX.txt	30-09-2024 08:25	Text Document	1 KB
Welcome.html	30-09-2024 08:25	Chrome HTML Do...	1 KB

copy the path



System › About

DESKTOP-CPQF51C
HP Elite SFF 800 G9 Desktop PC

Device specifications

Device name	DESKTOP-CPQF51C
Processor	12th Gen Intel(R) Core(TM) i9-12900 2.40 GHz
Installed RAM	32.0 GB (31.7 GB usable)
Device ID	AB74795D-D56B-43EC-AE97-F61D2F6F6615
Product ID	00355-61429-85494-AAOEM
System type	64-bit operating system, x64-based processor
Pen and touch	No pen or touch input is available for this display

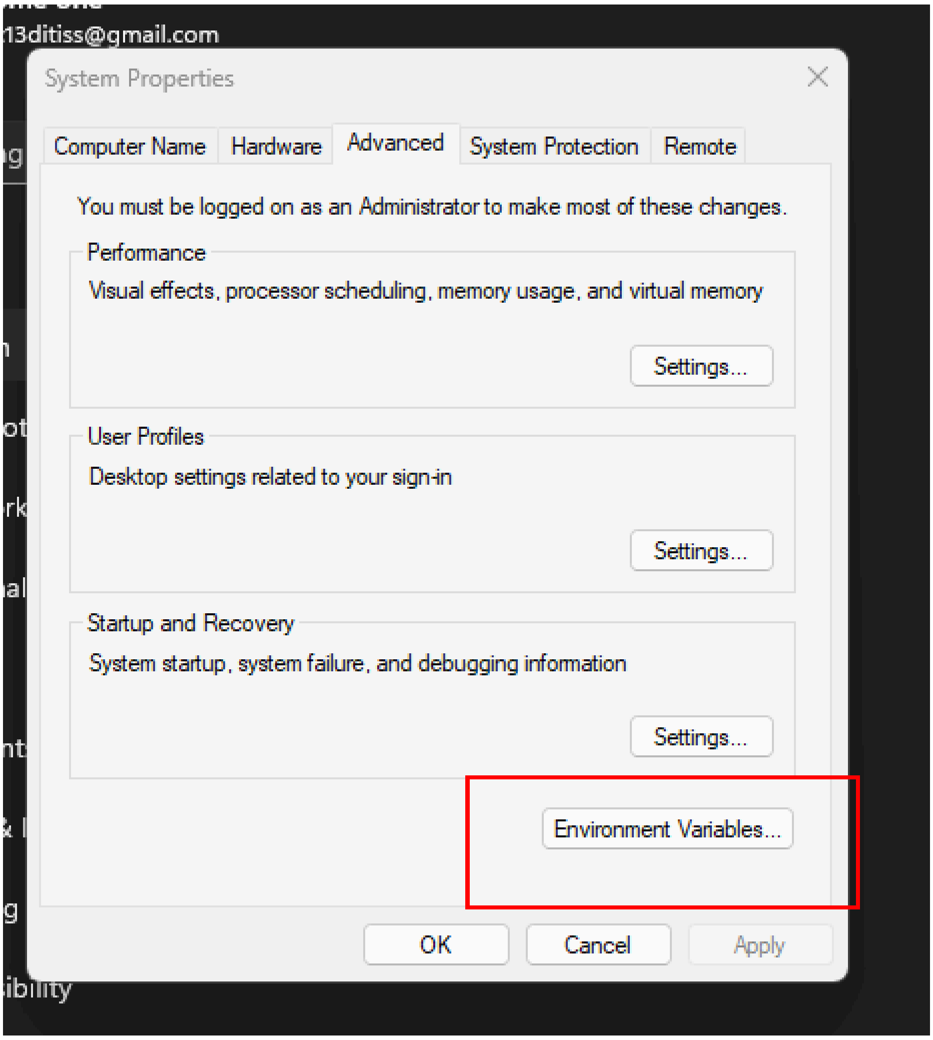
Windows specifications

Edition	Windows 11 Pro
Version	23H2
Installed on	23-03-2024
OS build	22631.4541
Serial number	1N14090CVK
Experience	Windows Feature Experience Pack 1000.22700.1055.0

Microsoft Services Agreement
Microsoft Software License Terms

Support

Manufacturer	HP Inc.
Website	Online support



You must be logged on as an Administrator to make most of these changes.

Performance

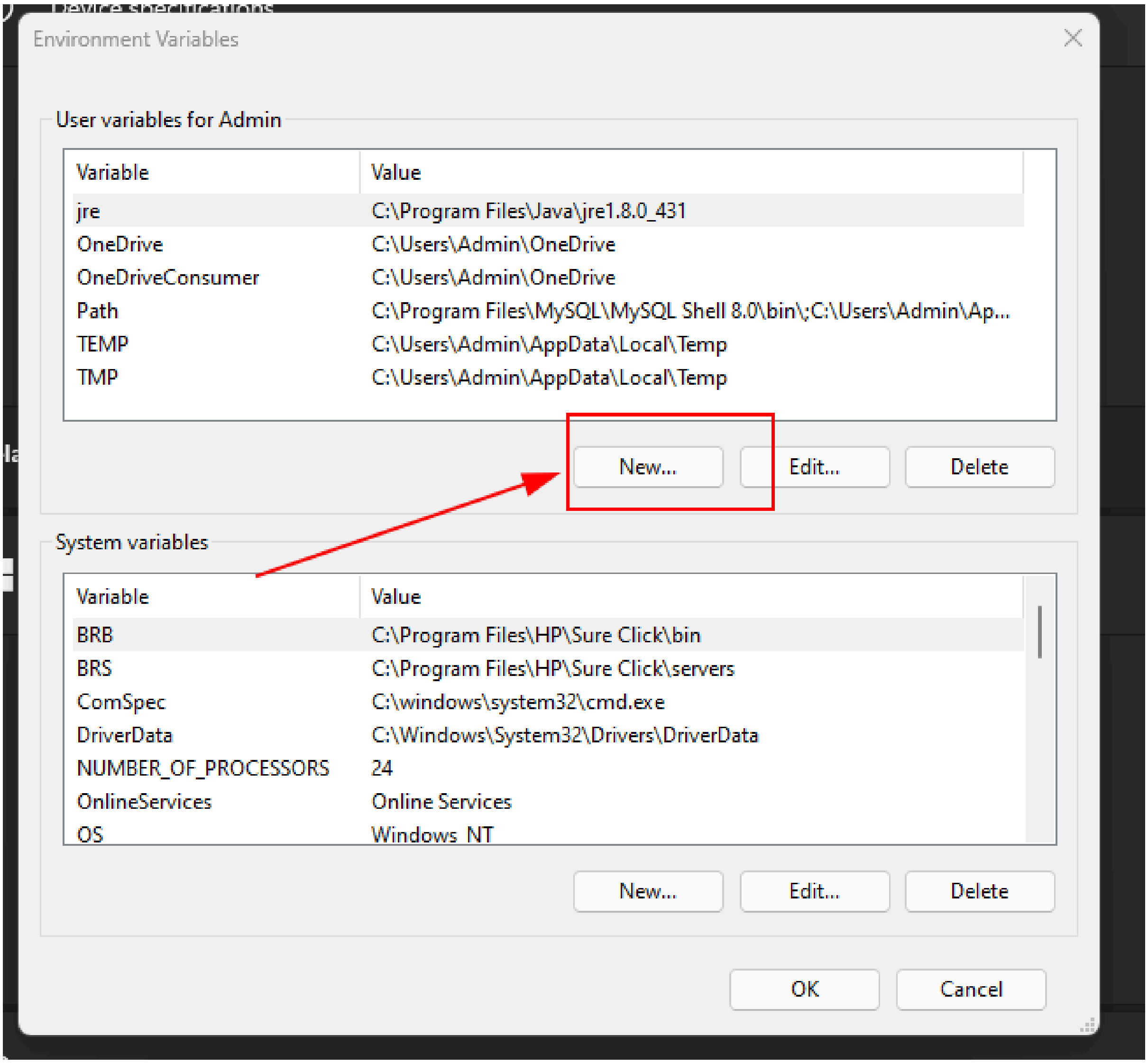
Visual effects, processor scheduling, memory usage, and virtual memory

User Profiles

Desktop settings related to your sign-in

Startup and Recovery

System startup, system failure, and debugging information



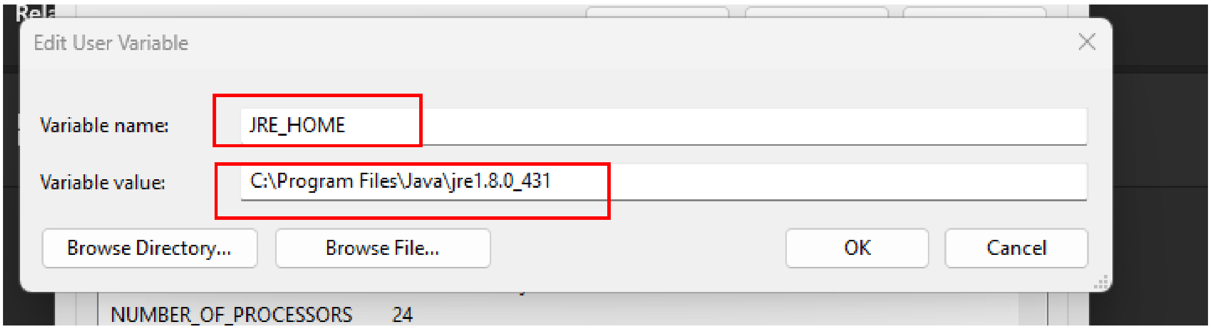
Environment Variables

User variables for Admin

Variable	Value
jre	C:\Program Files\Java\jre1.8.0_431
OneDrive	C:\Users\Admin\OneDrive
OneDriveConsumer	C:\Users\Admin\OneDrive
Path	C:\Program Files\MySQL\MySQL Shell 8.0\bin\;C:\Users\Admin\Ap...
TEMP	C:\Users\Admin\AppData\Local\Temp
TMP	C:\Users\Admin\AppData\Local\Temp

System variables

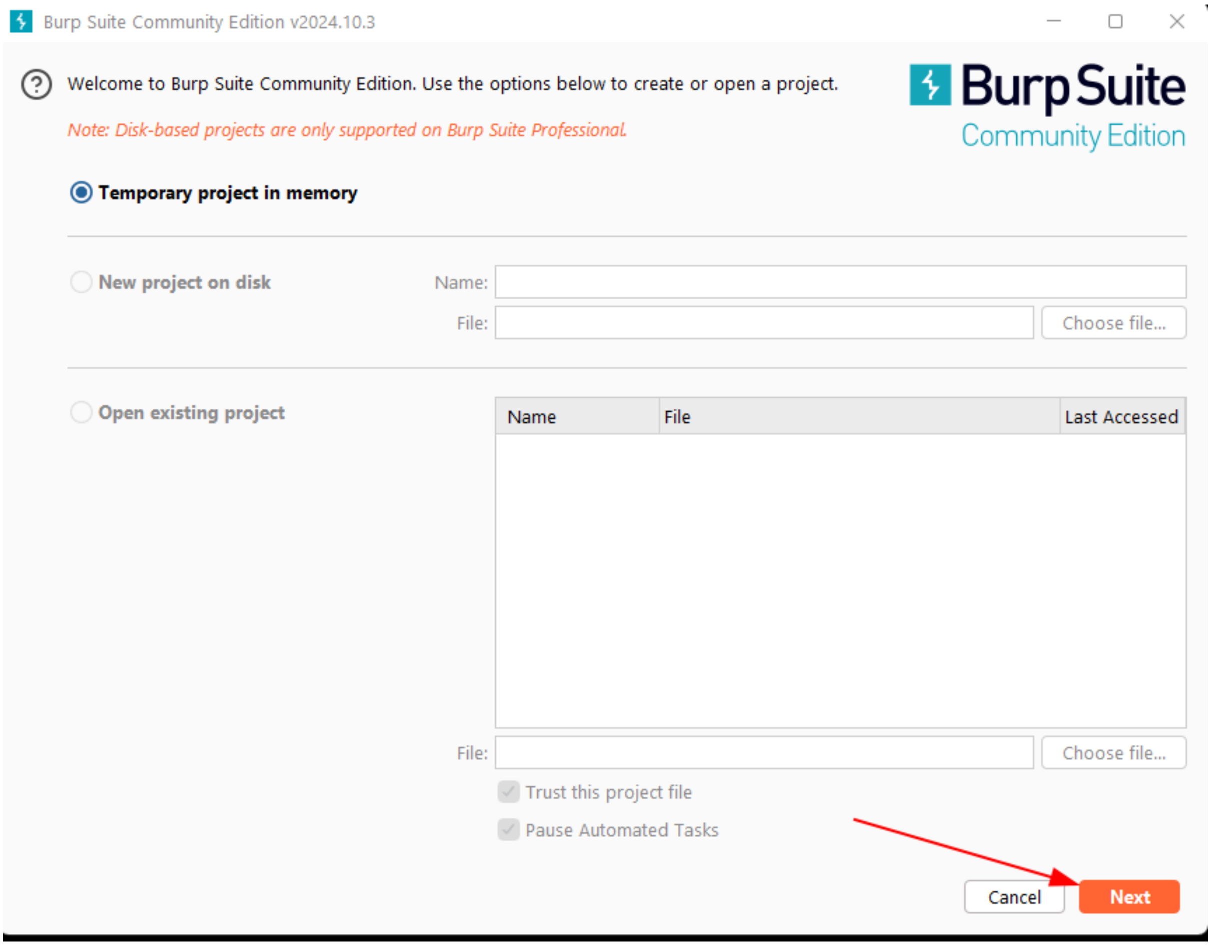
Variable	Value
BRB	C:\Program Files\HP\Sure Click\bin
BRS	C:\Program Files\HP\Sure Click\servers
ComSpec	C:\windows\system32\cmd.exe
DriverData	C:\Windows\System32\Drivers\DriverData
NUMBER_OF_PROCESSORS	24
OnlineServices	Online Services
OS	Windows_NT



Edit User Variable

Variable name: JRE_HOME

Variable value: C:\Program Files\Java\jre1.8.0_431



Burp Suite Community Edition v2024.10.3

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 in memory**

○ **New project on disk**

Name:

File:

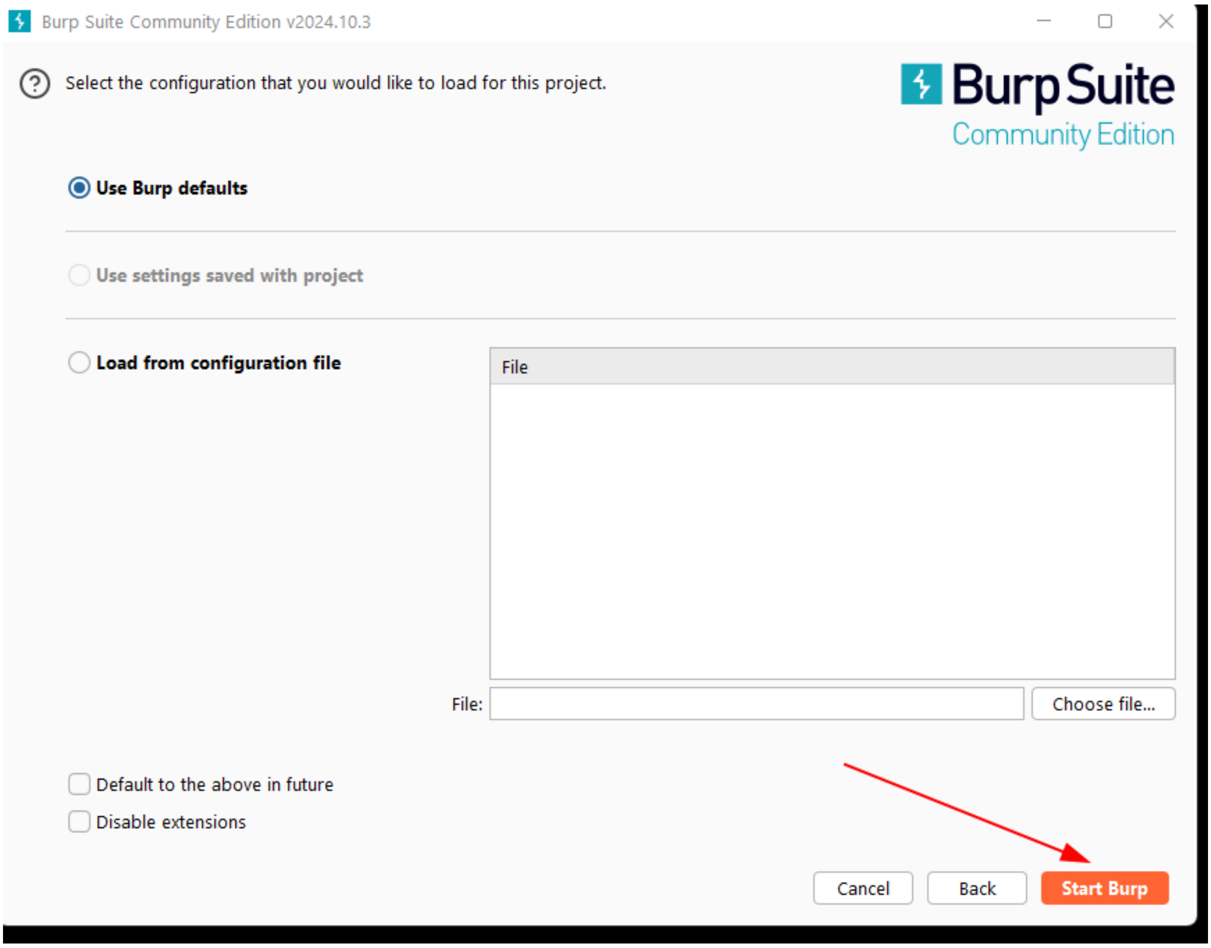
○ **Open existing project**

Name	File	Last Accessed

File:

☑ Trust this project file

☑ Pause Automated Tasks



Select the configuration that you would like to load for this project.

● Use Burp defaults

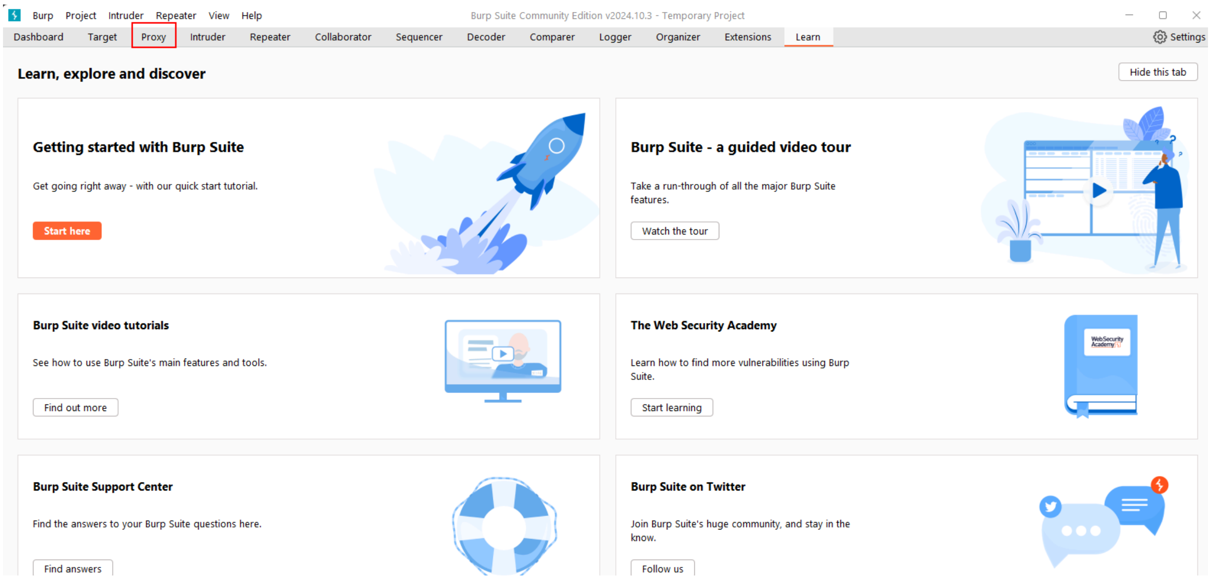
○ Use settings saved with project

○ Load from configuration file

File:

□ Default to the above in future

□ Disable extensions


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2024.10.3 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Hide this tab
Start here
Watch the tour
Find out more
Start learning
Find answers
Follow us

Learn, explore and discover

Getting started with Burp Suite

Get going right away - with our quick start tutorial.

Burp Suite - a guided video tour

Take a run-through of all the major Burp Suite features.

Burp Suite video tutorials

See how to use Burp Suite's main features and tools.

The Web Security Academy

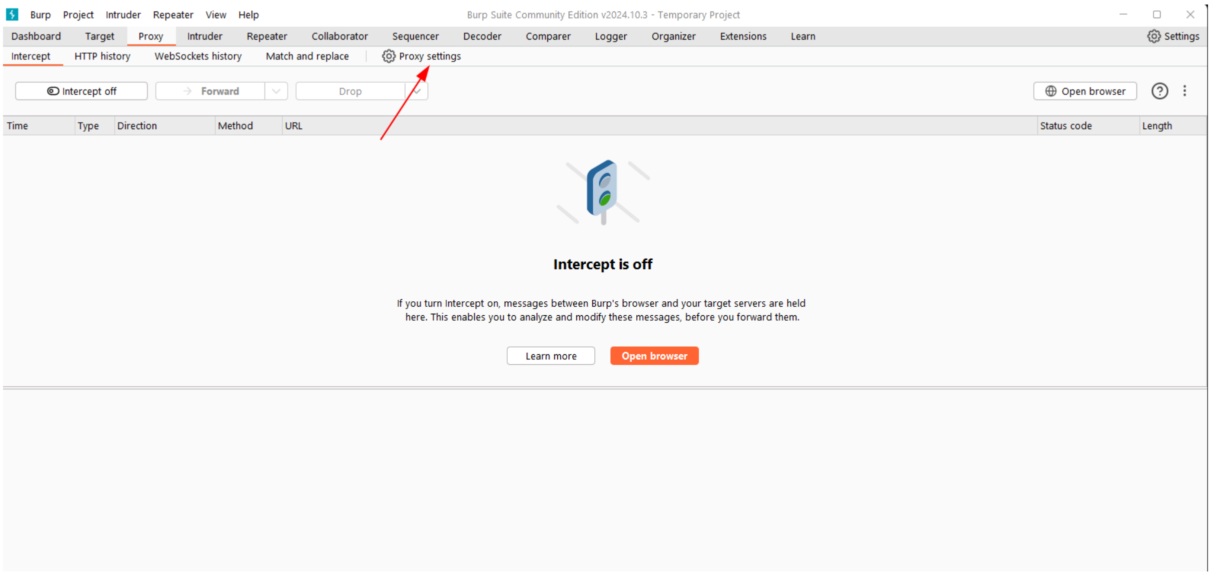
Learn how to find more vulnerabilities using Burp Suite.

Burp Suite Support Center

Find the answers to your Burp Suite questions here.

Burp Suite on Twitter

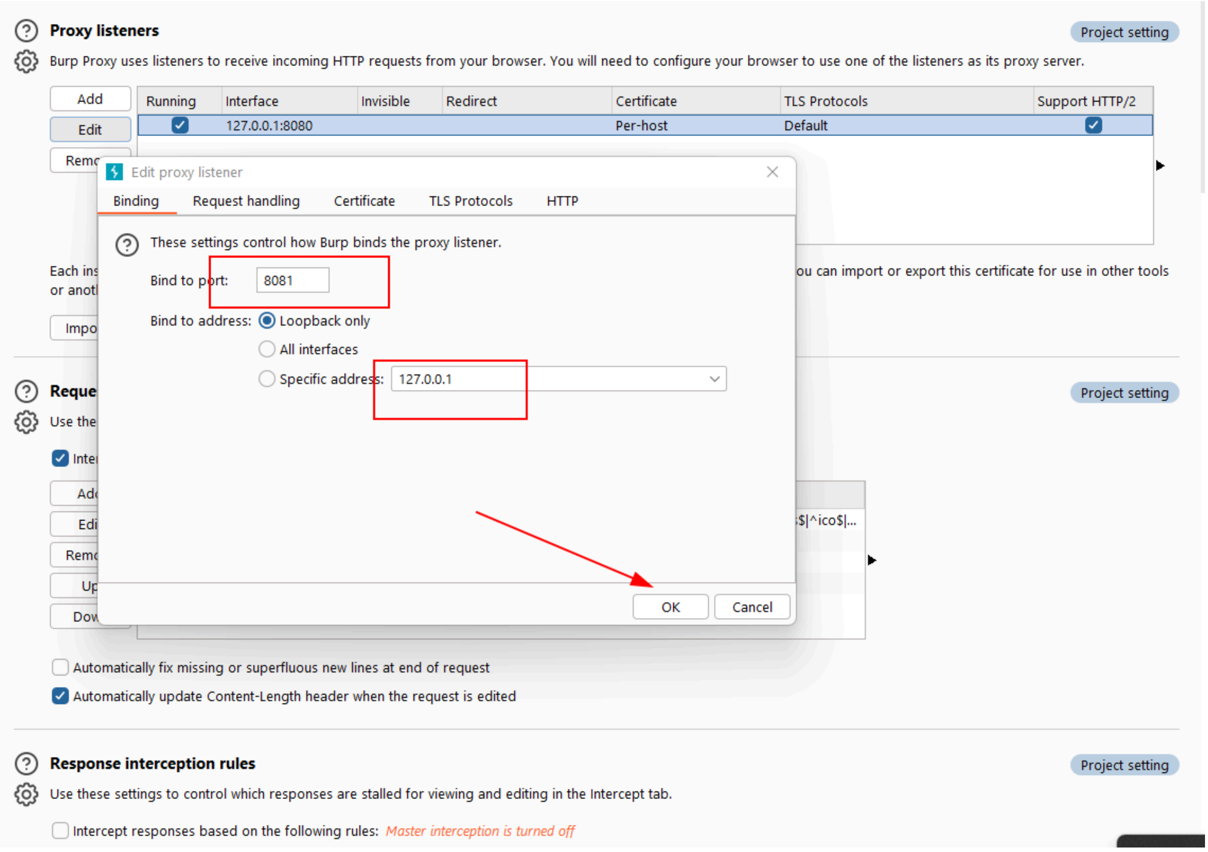
Join Burp Suite's huge community, and stay in the know.



Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2024.10.3 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Match and replace
Proxy settings
Intercept off
Forward
Drop
Open browser
Time Type Direction Method URL Status code Length
Learn more
Open browser

Intercept is off

If you turn Intercept on, messages between Burp's browser and your target servers are held here. This enables you to analyze and modify these messages, before you forward them.



Proxy listeners

Project setting

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	TLS Protocols	Support HTTP/2
☑	127.0.0.1:8080			Per-host	Default	☑

Add
Edit
Remo
Each ins
or anot
Impo
ou can import or export this certificate for use in other tools
Reque
Use the
Inte
Ad
Edi
Remo
Up
Dow
$|^ico$|...

Edit proxy listener

Binding Request handling Certificate TLS Protocols HTTP

These settings control how Burp binds the proxy listener.

Bind to port: 8081

Bind to address: ● Loopback only

○ All interfaces

○ Specific address: 127.0.0.1

□ Automatically fix missing or superfluous new lines at end of request

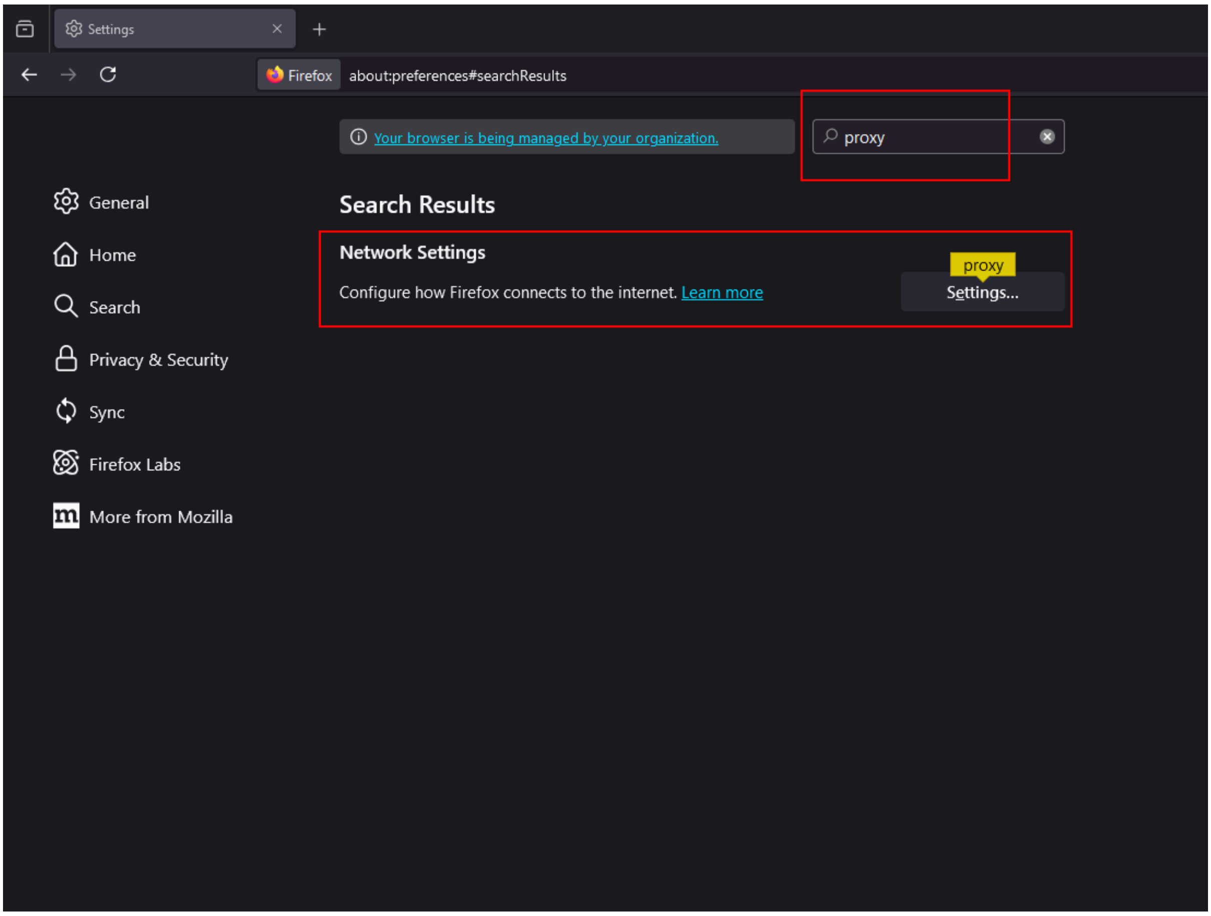
☑ Automatically update Content-Length header when the request is edited

Response interception rules

Project setting

Use these settings to control which responses are stalled for viewing and editing in the Intercept tab.

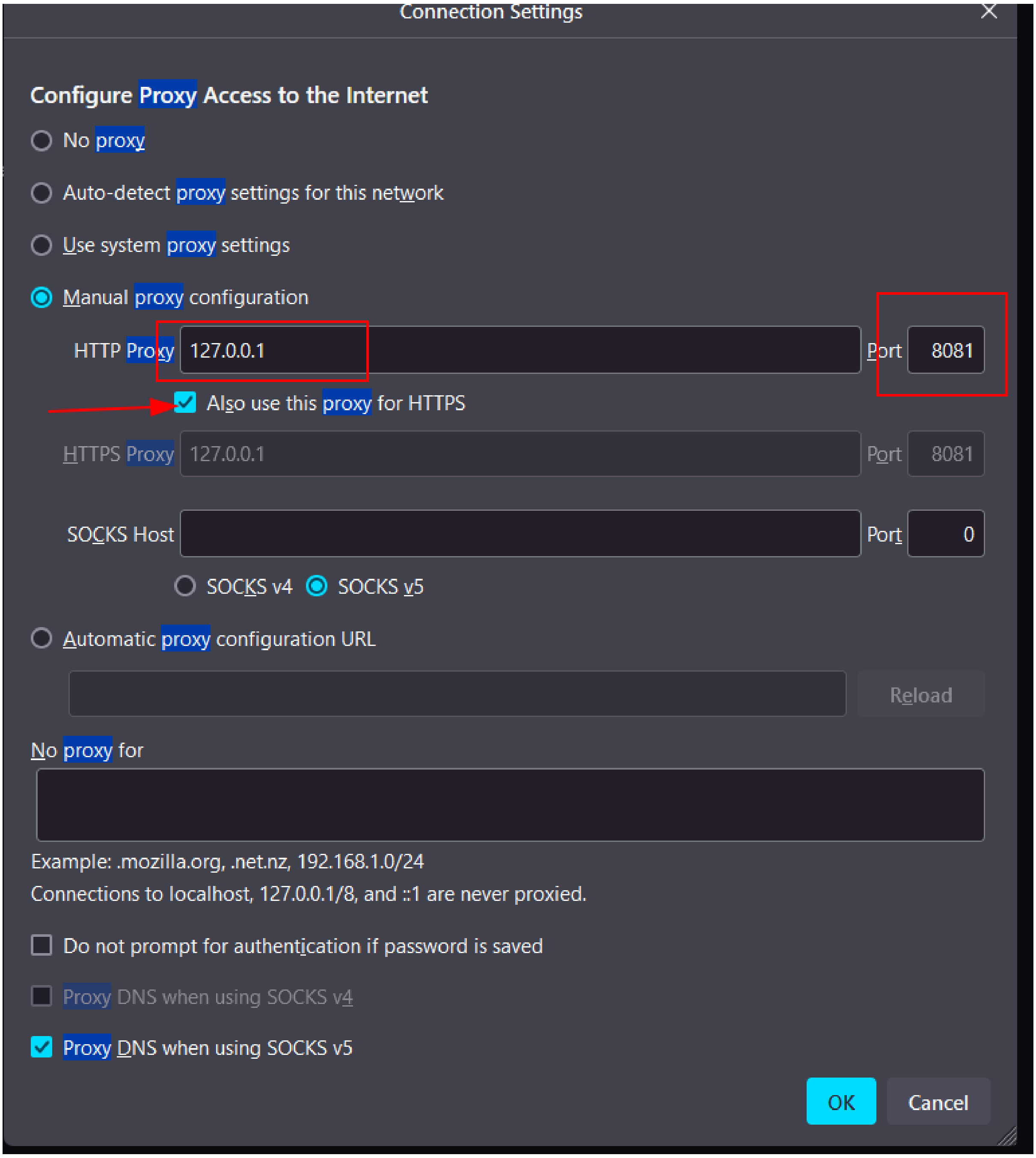
□ Intercept responses based on the following rules: *Master interception is turned off*



Search Results

Network Settings

Configure how Firefox connects to the internet. Learn more



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 8081

☑ Also use this proxy for HTTPS

HTTPS Proxy 127.0.0.1 Port 8081

SOCKS Host Port 0

○ SOCKS v4 ● SOCKS v5

○ Automatic proxy configuration URL

No proxy for

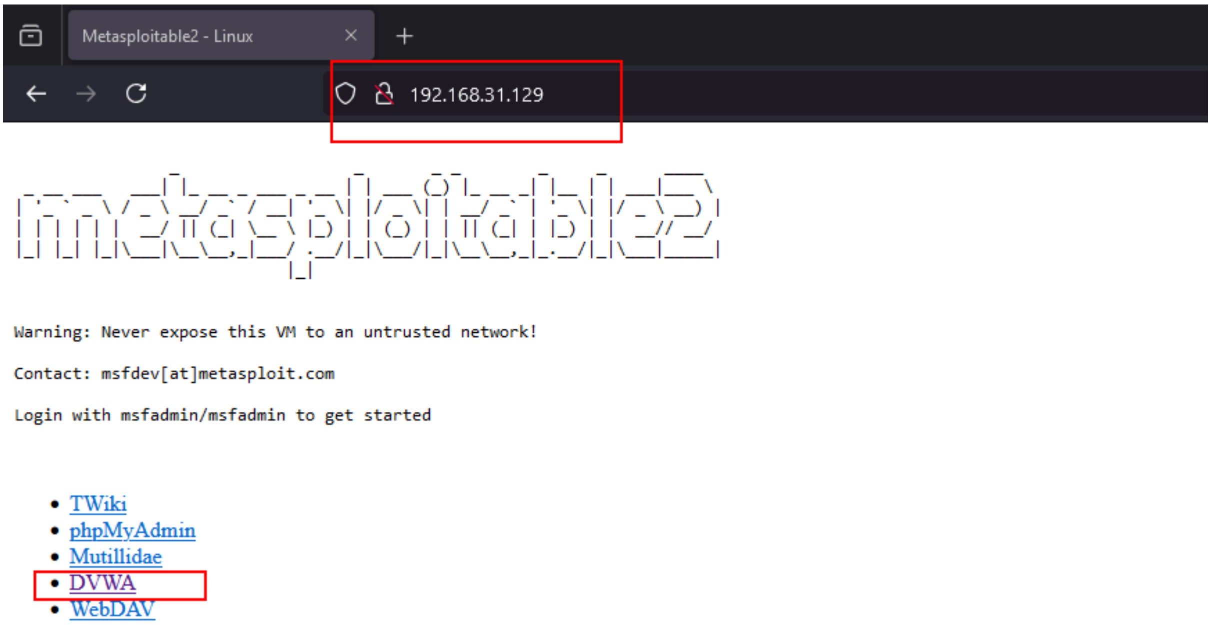
Example: .mozilla.org, .net.nz, 192.168.1.0/24

Connections to localhost, 127.0.0.1/8, and ::1 are never proxied.

□ Do not prompt for authentication if password is saved

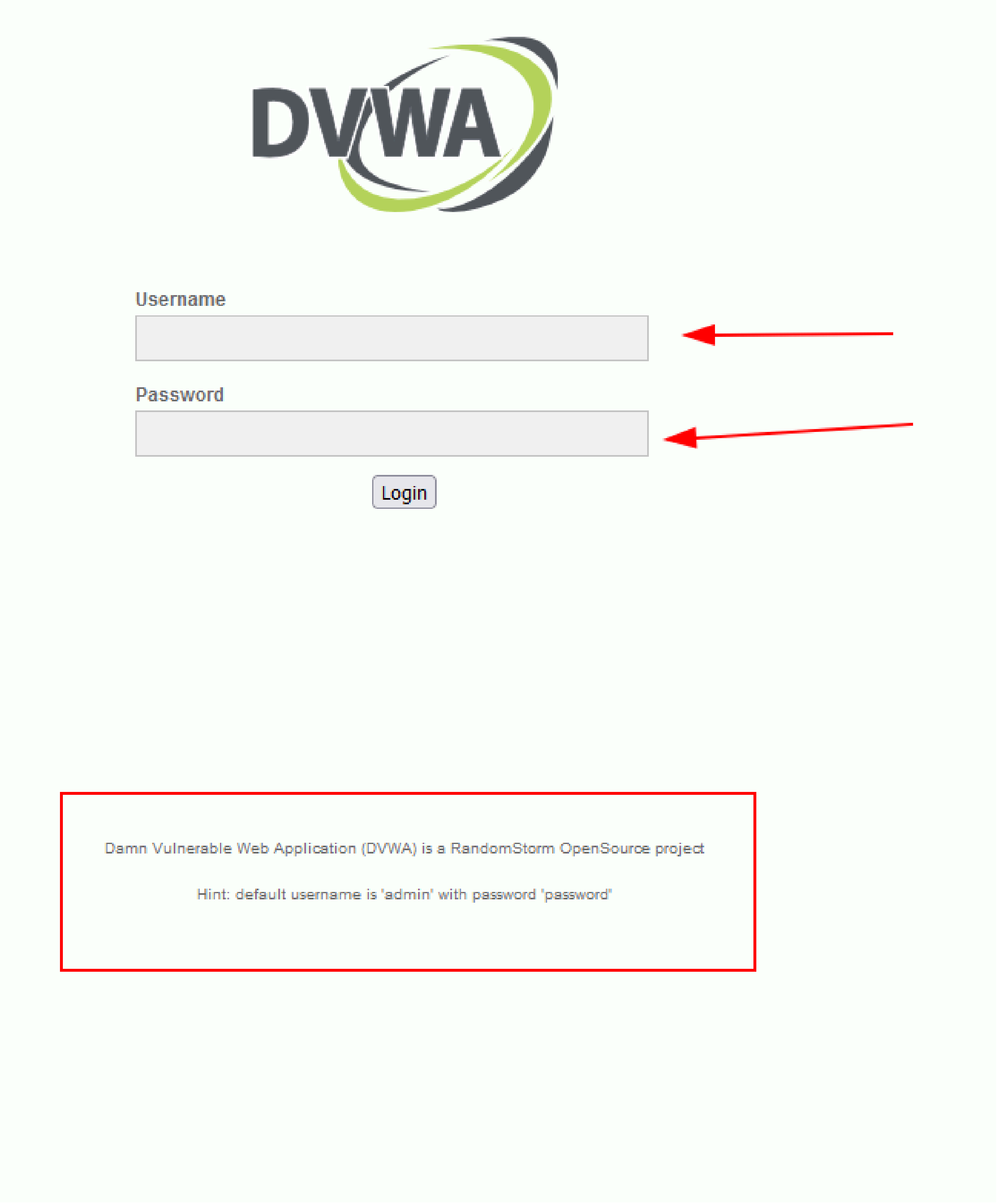
□ Proxy DNS when using SOCKS v4

☑ Proxy DNS when using SOCKS v5



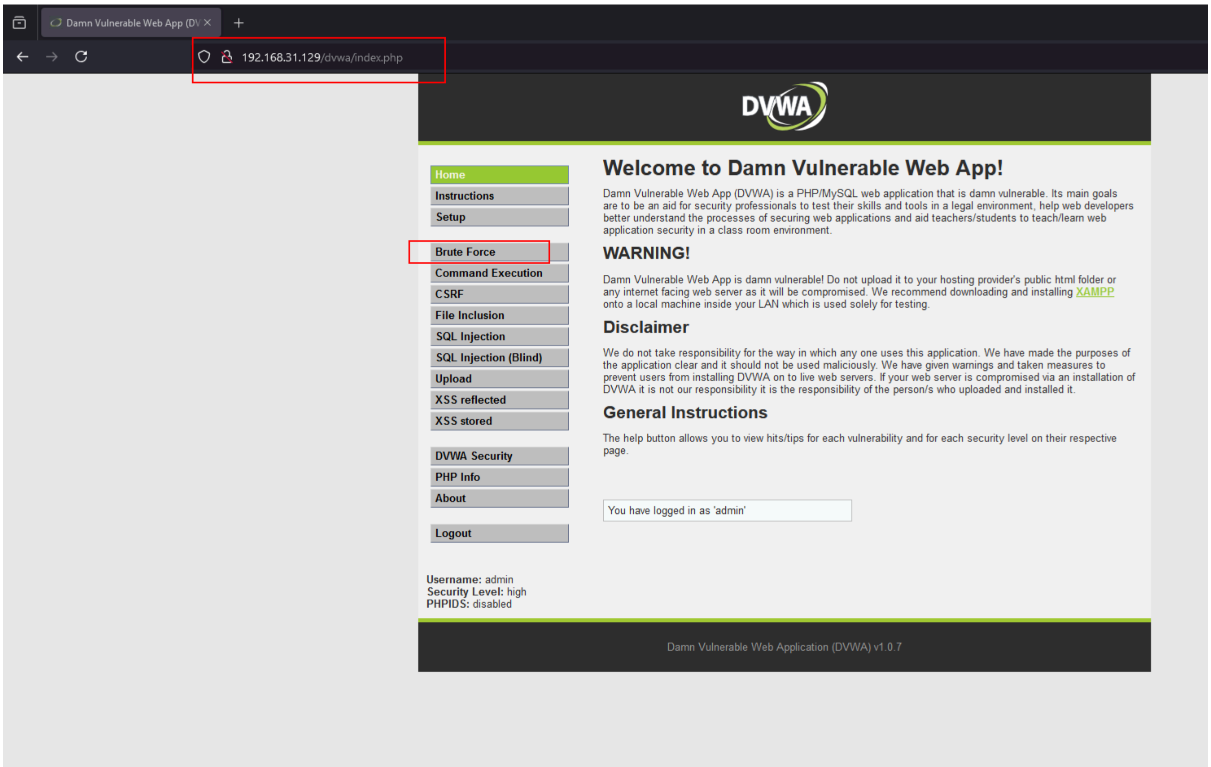
```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV



Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project

Hint: default username is 'admin' with password 'password'



Welcome to Damn Vulnerable Web App!

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

WARNING!

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing XAMPP onto a local machine inside your LAN which is used solely for testing.

Disclaimer

We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

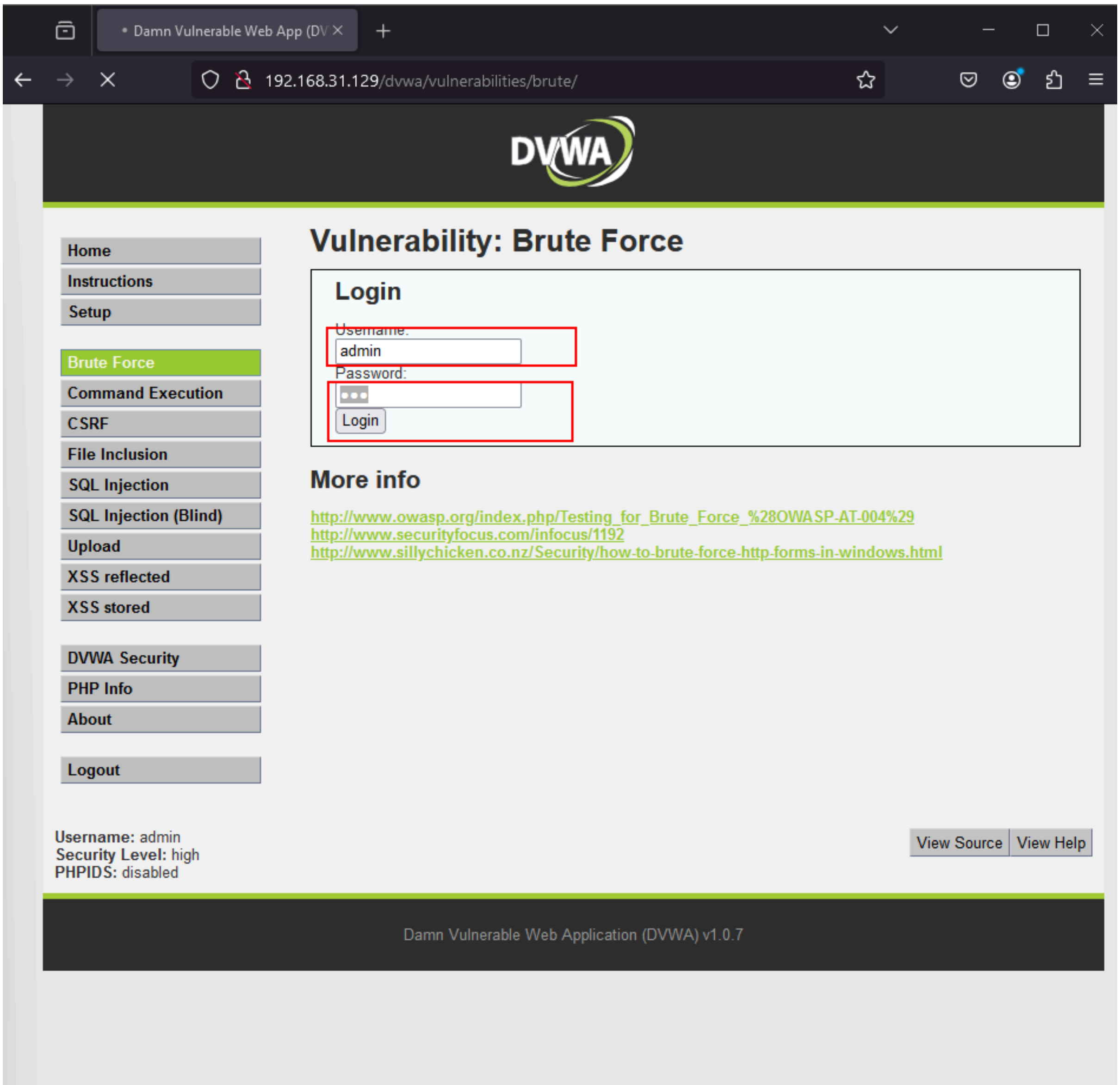
General Instructions

The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.

You have logged in as 'admin'

Username: admin
Security Level: high
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7



Vulnerability: Brute Force

Login

Username: admin

Password: ●●●

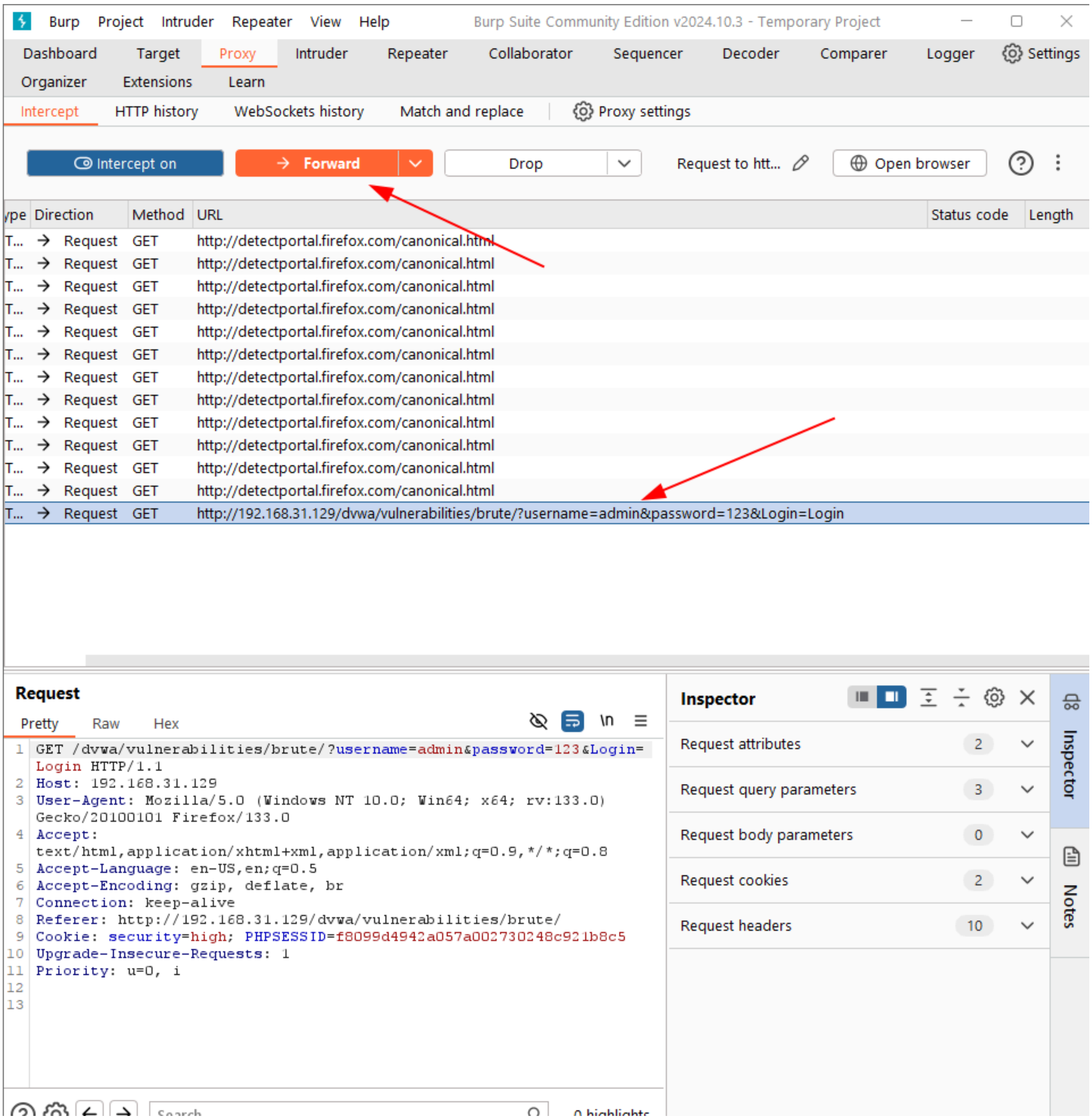
Login

More info

http://www.owasp.org/index.php/Testing_for_Brute_Force_%28OWASP-AT-004%29
http://www.securityfocus.com/infocus/1192
http://www.sillychicken.co.nz/Security/how-to-brute-force-http-forms-in-windows.html

Username: admin
Security Level: high
PHPIDS: disabled

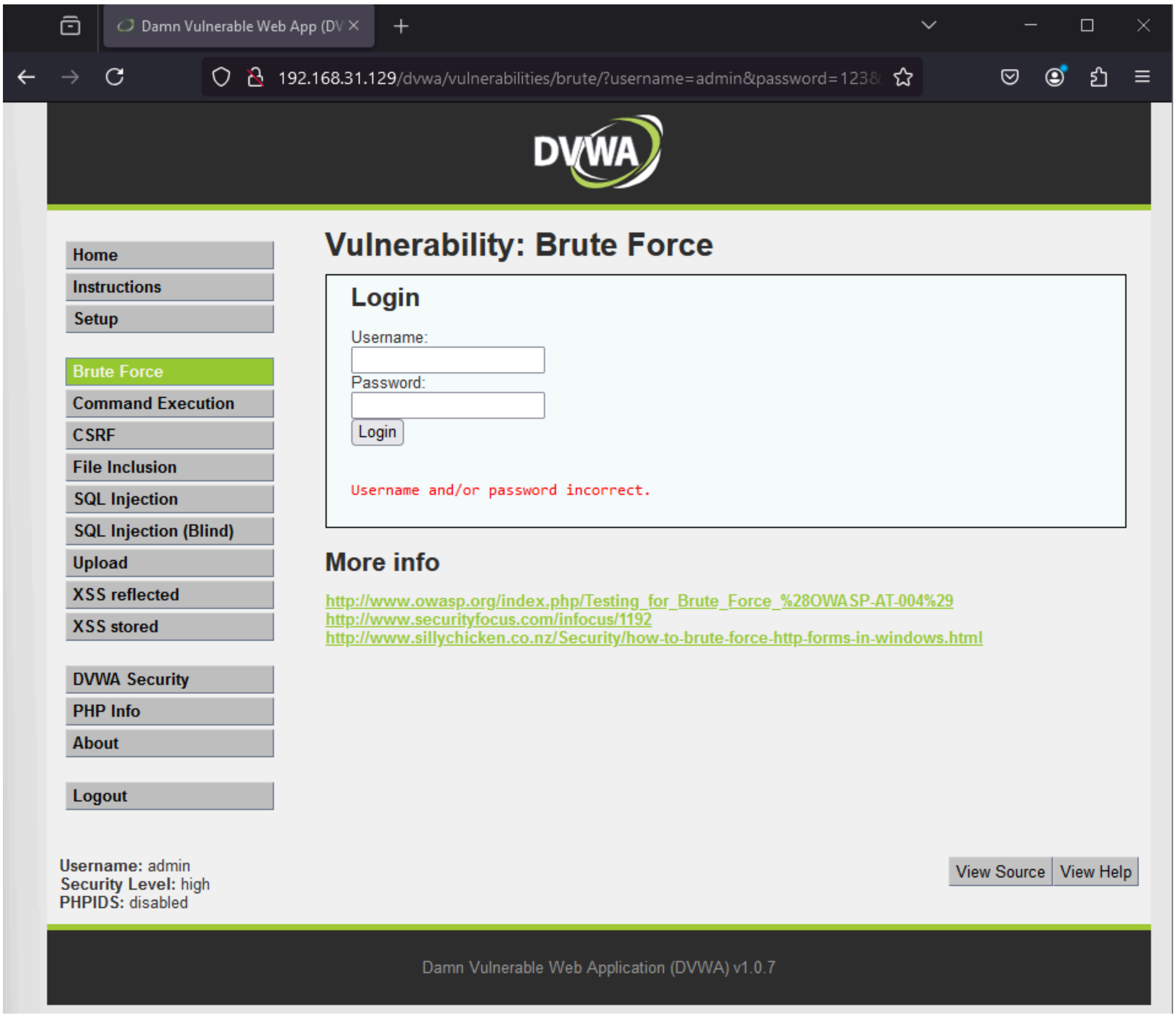
Damn Vulnerable Web Application (DVWA) v1.0.7


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2024.10.3 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Settings
Organizer Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on
Forward
Drop
Request to htt...
Open browser

ype	Direction	Method	URL	Status code	Length
T...	→ Request	GET	http://detectportal.firefox.com/canonical.html		
T...	→ Request	GET	http://detectportal.firefox.com/canonical.html		
T...	→ Request	GET	http://detectportal.firefox.com/canonical.html		
T...	→ Request	GET	http://detectportal.firefox.com/canonical.html		
T...	→ Request	GET	http://detectportal.firefox.com/canonical.html		
T...	→ Request	GET	http://detectportal.firefox.com/canonical.html		
T...	→ Request	GET	http://detectportal.firefox.com/canonical.html		
T...	→ Request	GET	http://detectportal.firefox.com/canonical.html		
T...	→ Request	GET	http://detectportal.firefox.com/canonical.html		
T...	→ Request	GET	http://detectportal.firefox.com/canonical.html		
T...	→ Request	GET	http://detectportal.firefox.com/canonical.html		
T...	→ Request	GET	http://detectportal.firefox.com/canonical.html		
T...	→ Request	GET	http://192.168.31.129/dvwa/vulnerabilities/brute/?username=admin&password=123&Login=Login		

```
GET /dvwa/vulnerabilities/brute/?username=admin&password=123&Login=
Login HTTP/1.1
Host: 192.168.31.129
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0)
Gecko/20100101 Firefox/133.0
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, br
Connection: keep-alive
Referer: http://192.168.31.129/dvwa/vulnerabilities/brute/
Cookie: security=high; PHPSESSID=f8099d4942a057a002730248c921b8c5
Upgrade-Insecure-Requests: 1
Priority: u=0, i


```

Request attributes	2
Request query parameters	3
Request body parameters	0
Request cookies	2
Request headers	10



Vulnerability: Brute Force

Login

Username:

Password:

Login

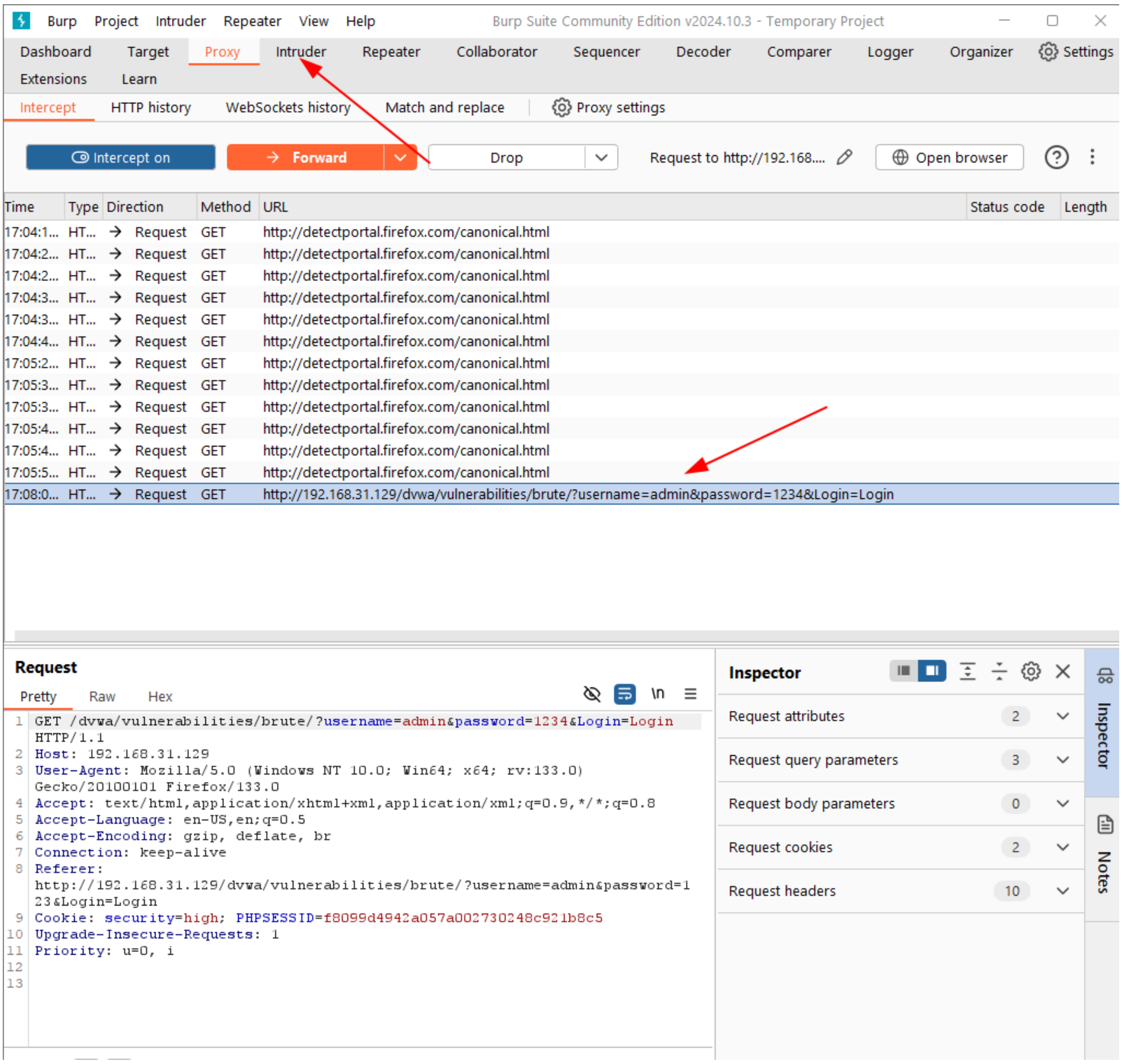
```
Username and/or password incorrect.
```

More info

http://www.owasp.org/index.php/Testing_for_Brute_Force_%28OWASP-AT-004%29
http://www.securityfocus.com/infocus/1192
http://www.sillychicken.co.nz/Security/how-to-brute-force-http-forms-in-windows.html

Username: admin
Security Level: high
PHPIDS: disabled

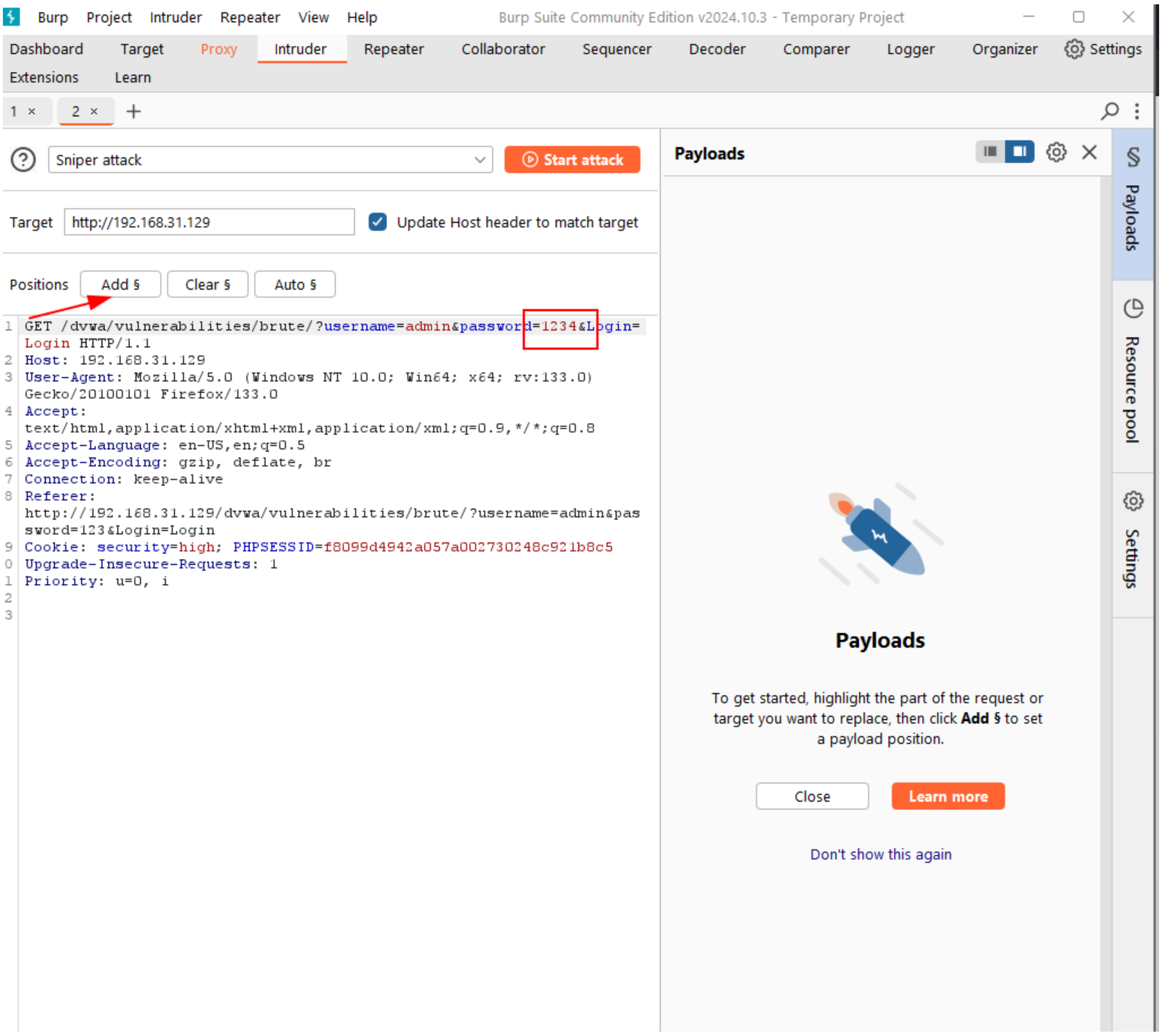
Damn Vulnerable Web Application (DVWA) v1.0.7



Time	Type	Direction	Method	URL	Status code	Length
17:04:1...	HT...	→ Request	GET	http://detectportal.firefox.com/canonical.html		
17:04:2...	HT...	→ Request	GET	http://detectportal.firefox.com/canonical.html		
17:04:2...	HT...	→ Request	GET	http://detectportal.firefox.com/canonical.html		
17:04:3...	HT...	→ Request	GET	http://detectportal.firefox.com/canonical.html		
17:04:3...	HT...	→ Request	GET	http://detectportal.firefox.com/canonical.html		
17:04:4...	HT...	→ Request	GET	http://detectportal.firefox.com/canonical.html		
17:05:2...	HT...	→ Request	GET	http://detectportal.firefox.com/canonical.html		
17:05:3...	HT...	→ Request	GET	http://detectportal.firefox.com/canonical.html		
17:05:3...	HT...	→ Request	GET	http://detectportal.firefox.com/canonical.html		
17:05:4...	HT...	→ Request	GET	http://detectportal.firefox.com/canonical.html		
17:05:4...	HT...	→ Request	GET	http://detectportal.firefox.com/canonical.html		
17:05:5...	HT...	→ Request	GET	http://detectportal.firefox.com/canonical.html		
17:08:0...	HT...	→ Request	GET	http://192.168.31.129/dvwa/vulnerabilities/brute/?username=admin&password=1234&Login=Login		

```
GET /dvwa/vulnerabilities/brute/?username=admin&password=1234&Login=Login
HTTP/1.1
Host: 192.168.31.129
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0)
Gecko/20100101 Firefox/133.0
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, br
Connection: keep-alive
Referer:
http://192.168.31.129/dvwa/vulnerabilities/brute/?username=admin&password=1
23&Login=Login
Cookie: security=high; PHPSESSID=f8099d4942a057a002730248c921b8c5
Upgrade-Insecure-Requests: 1
Priority: u=0, i


```

Request attributes	2
Request query parameters	3
Request body parameters	0
Request cookies	2
Request headers	10



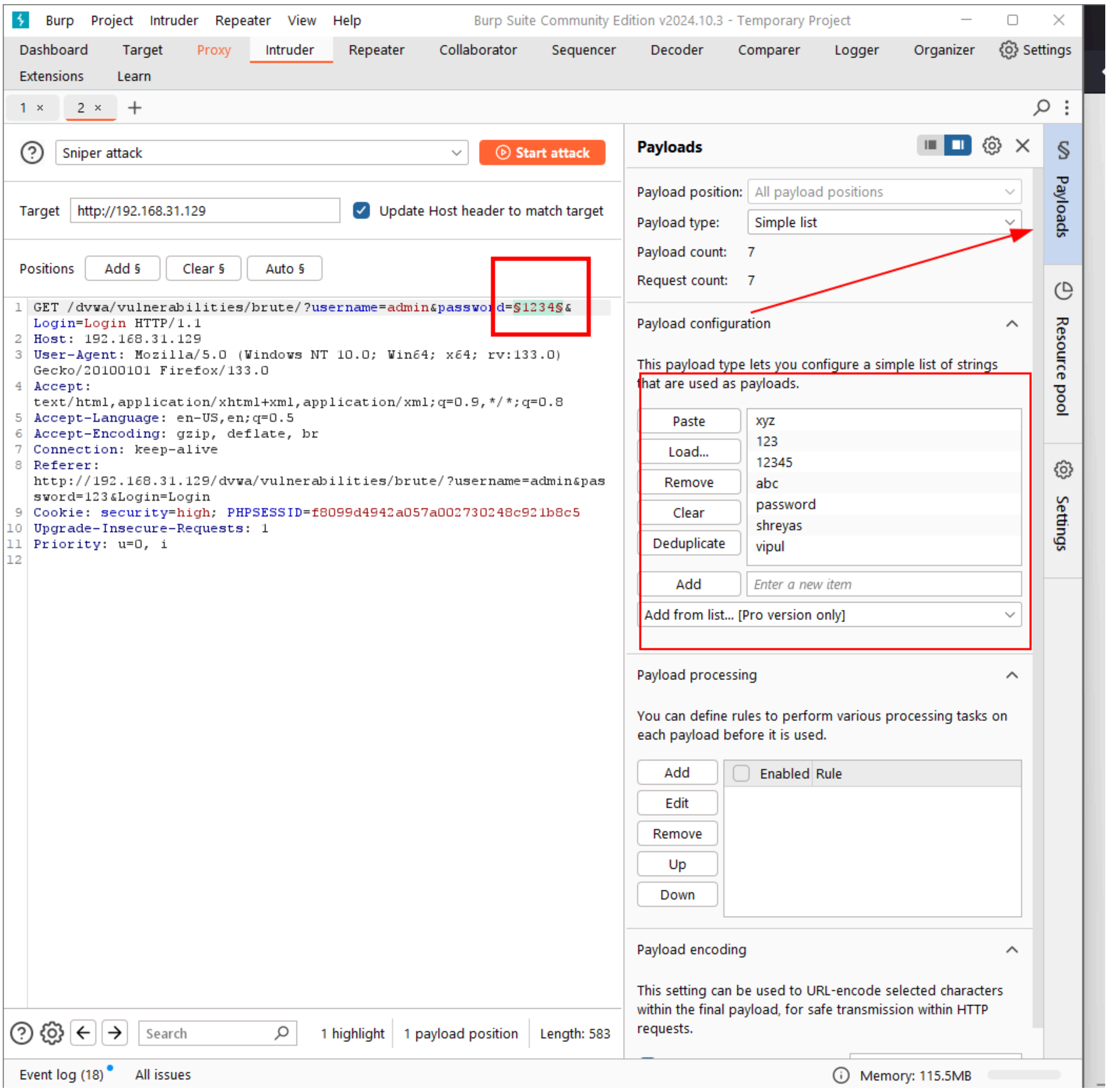
Target http://192.168.31.129

☑ Update Host header to match target

```
GET /dvwa/vulnerabilities/brute/?username=admin&password=1234&Login=Login HTTP/1.1
Host: 192.168.31.129
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/133.0
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, br
Connection: keep-alive
Referer: http://192.168.31.129/dvwa/vulnerabilities/brute/?username=admin&password=123&Login=Login
Cookie: security=high; PHPSESSID=f8099d4942a057a002730248c921b8c5
Upgrade-Insecure-Requests: 1
Priority: u=0, i

```

Payloads

To get started, highlight the part of the request or target you want to replace, then click **Add §** to set a payload position.



Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2024.10.3 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Settings
Extensions Learn
1 × 2 ×
Start attack
Payloads
Resource pool
Settings
Paste
Load...
Remove
Clear
Deduplicate
Add
Edit
Remove
Up
Down
Search
Event log (18)
All issues
Memory: 115.5MB

Sniper attack

Target: http://192.168.31.129 ☑ Update Host header to match target

Positions: Add § Clear § Auto §

```
GET /dvwa/vulnerabilities/brute/?username=admin&password=§1234§&
Login=Login HTTP/1.1
Host: 192.168.31.129
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0)
Gecko/20100101 Firefox/133.0
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, br
Connection: keep-alive
Referer:
http://192.168.31.129/dvwa/vulnerabilities/brute/?username=admin&pas
sword=123&Login=Login
Cookie: security=high; PHPSESSID=f8099d4942a057a002730248c921b8c5
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

1 highlight | 1 payload position | Length: 583

Payload position: All payload positions
Payload type: Simple list
Payload count: 7
Request count: 7

Payload configuration

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

- xyz
- 123
- 12345
- abc
- password
- shreyas
- vipul

Enter a new item

Add from list... [Pro version only]

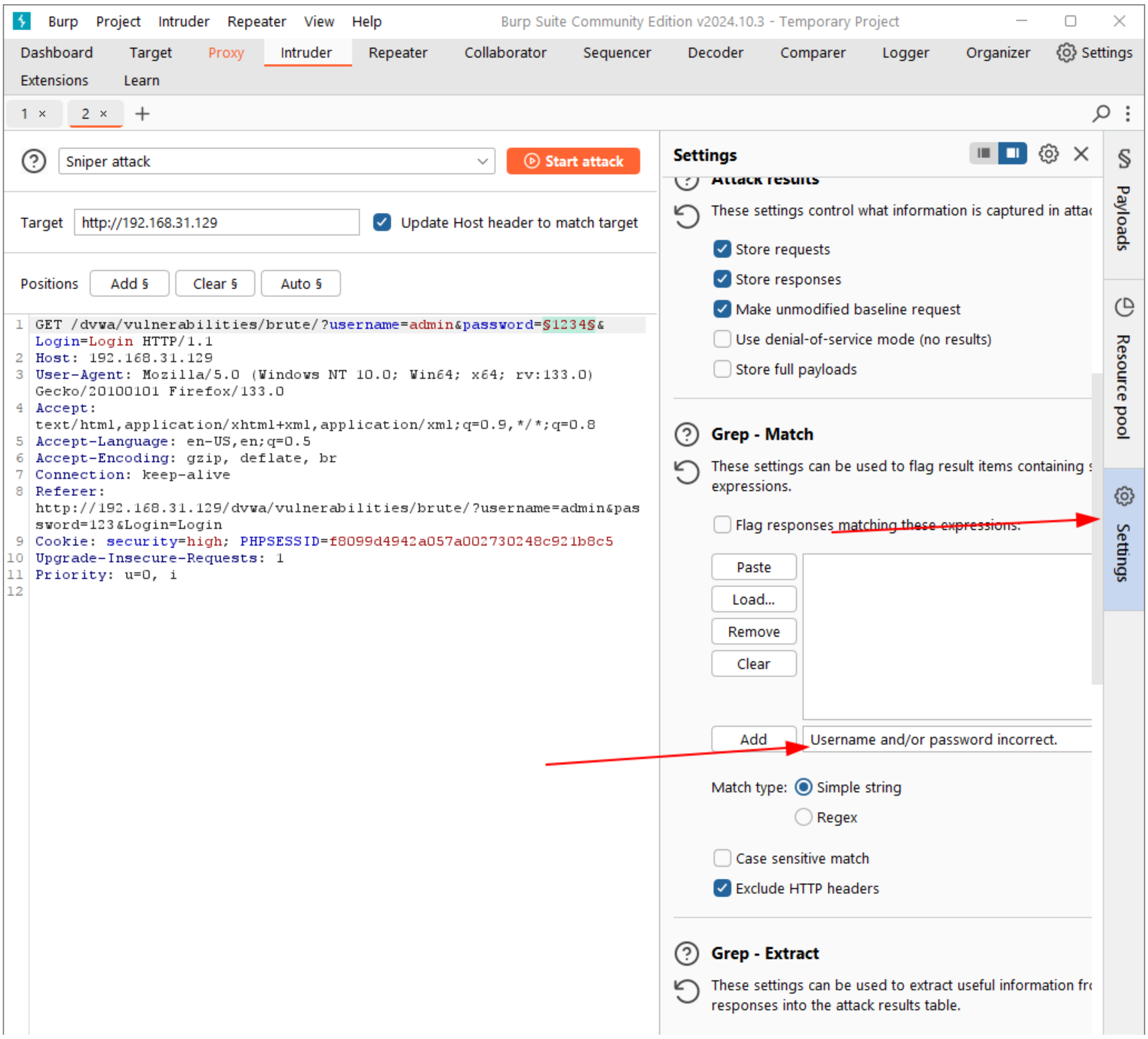
Payload processing

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

□ Enabled | Rule

Payload encoding

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



Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2024.10.3 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Settings
Extensions Learn
1 × 2 × +
Payloads
Resource pool
Settings

Sniper attack

Start attack

Target http://192.168.31.129 ☑ Update Host header to match target

Positions Add § Clear § Auto §

```
GET /dvwa/vulnerabilities/brute/?username=admin&password=§1234§&
Login=Login HTTP/1.1
Host: 192.168.31.129
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0)
Gecko/20100101 Firefox/133.0
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, br
Connection: keep-alive
Referer:
http://192.168.31.129/dvwa/vulnerabilities/brute/?username=admin&pas
sword=123&Login=Login
Cookie: security=high; PHPSESSID=f8099d4942a057a002730248c921b8c5
Upgrade-Insecure-Requests: 1
Priority: u=0, i

```

Settings

Attack results

These settings control what information is captured in attac

☑ Store requests

☑ Store responses

☑ Make unmodified baseline request

□ Use denial-of-service mode (no results)

□ Store full payloads

Grep - Match

These settings can be used to flag result items containing s expressions.

□ Flag responses matching these expressions:

Paste
Load...
Remove
Clear

Add Username and/or password incorrect.

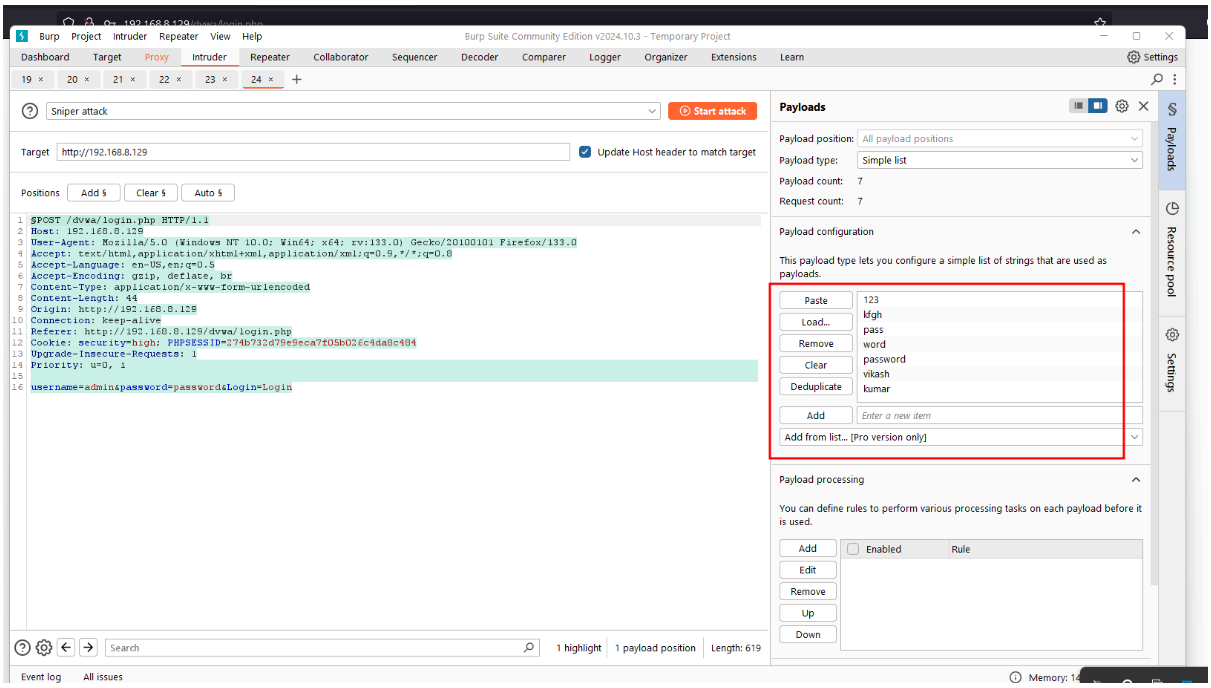
Match type: ● Simple string ○ Regex

□ Case sensitive match

☑ Exclude HTTP headers

Grep - Extract

These settings can be used to extract useful information fr responses into the attack results table.



Burp Suite Community Edition v2024.10.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
19 × 20 × 21 × 22 × 23 × 24 ×
Start attack
Positions Add § Clear § Auto §
Payloads
Resource pool
Settings
Paste
Load...
Remove
Clear
Deduplicate
Add
Enter a new item
Add from list... [Pro version only]
Add
Edit
Remove
Up
Down
Search
1 highlight
1 payload position
Length: 619
Event log
All issues
Memory: 14

Sniper attack

Target: http://192.168.8.129

☑ Update Host header to match target

```
§POST /dvwa/login.php HTTP/1.1
Host: 192.168.8.129
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/133.0
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, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 44
Origin: http://192.168.8.129
Connection: keep-alive
Referer: http://192.168.8.129/dvwa/login.php
Cookie: security=high; PHPSESSID=274b732d79e9eca7f05b026c4da8c484
Upgrade-Insecure-Requests: 1
Priority: u=0, i

username=admin&password=password&Login=Login
```

Payload position: All payload positions
Payload type: Simple list
Payload count: 7
Request count: 7

Payload configuration

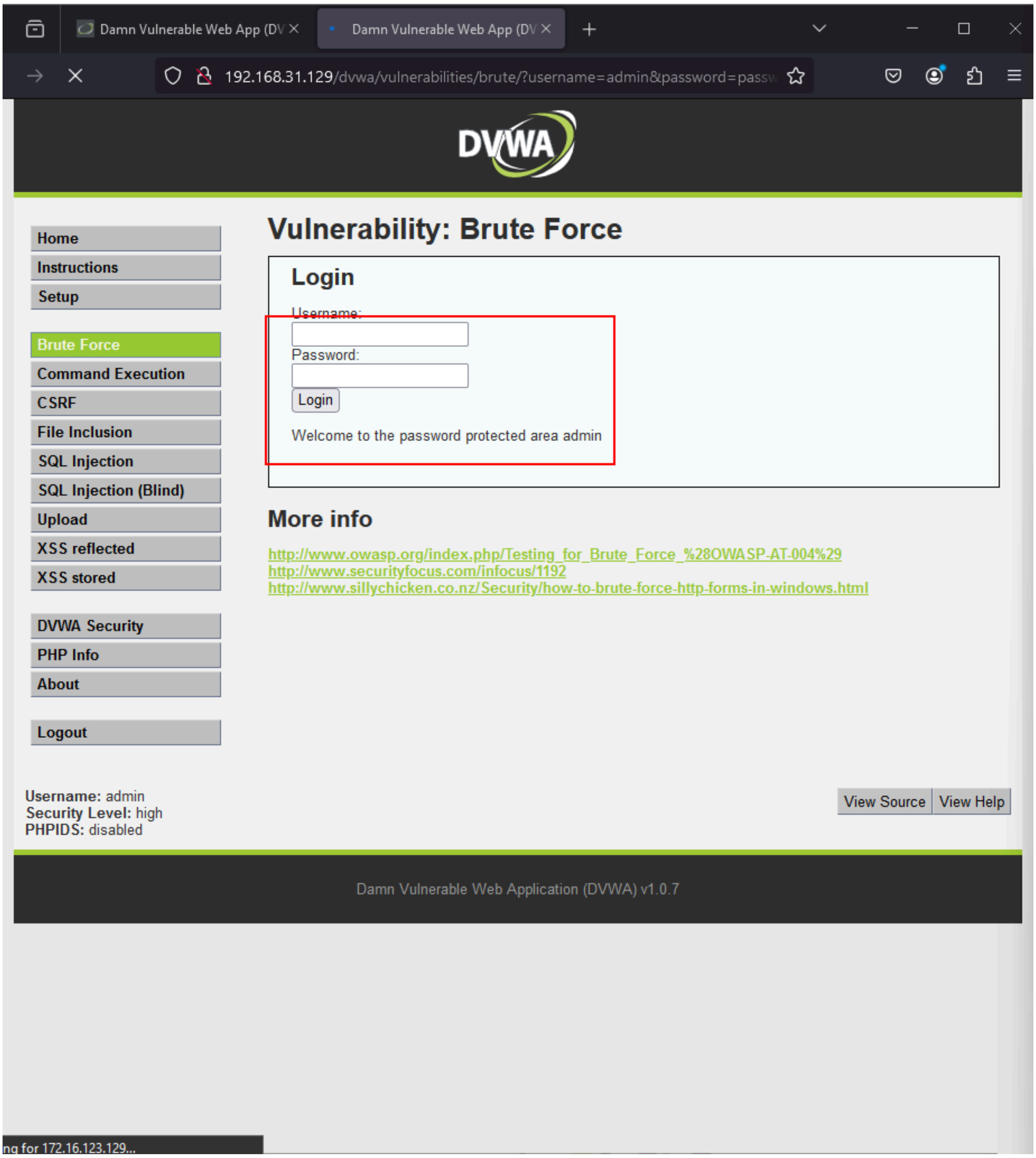
This payload type lets you configure a simple list of strings that are used as payloads.

```
123
kfgh
pass
word
password
vikash
kumar
```

Payload processing

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

□ Enabled	Rule



Vulnerability: Brute Force

Login

Username:

Password:

Login

Welcome to the password protected area admin

More info

http://www.owasp.org/index.php/Testing_for_Brute_Force_%28OWASP-AT-004%29
http://www.securityfocus.com/infocus/1192
http://www.sillychicken.co.nz/Security/how-to-brute-force-http-forms-in-windows.html

Username: admin
Security Level: high
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7