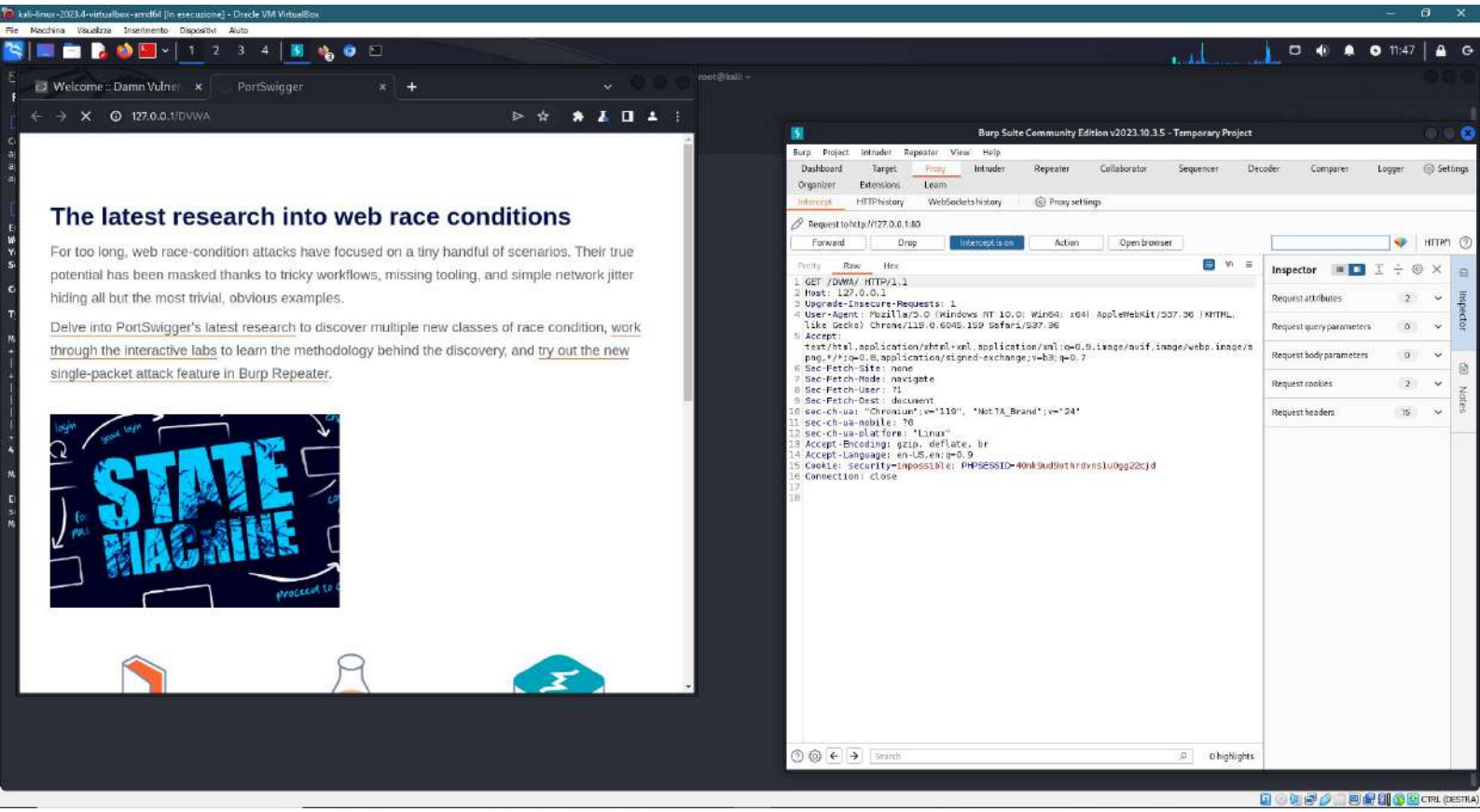
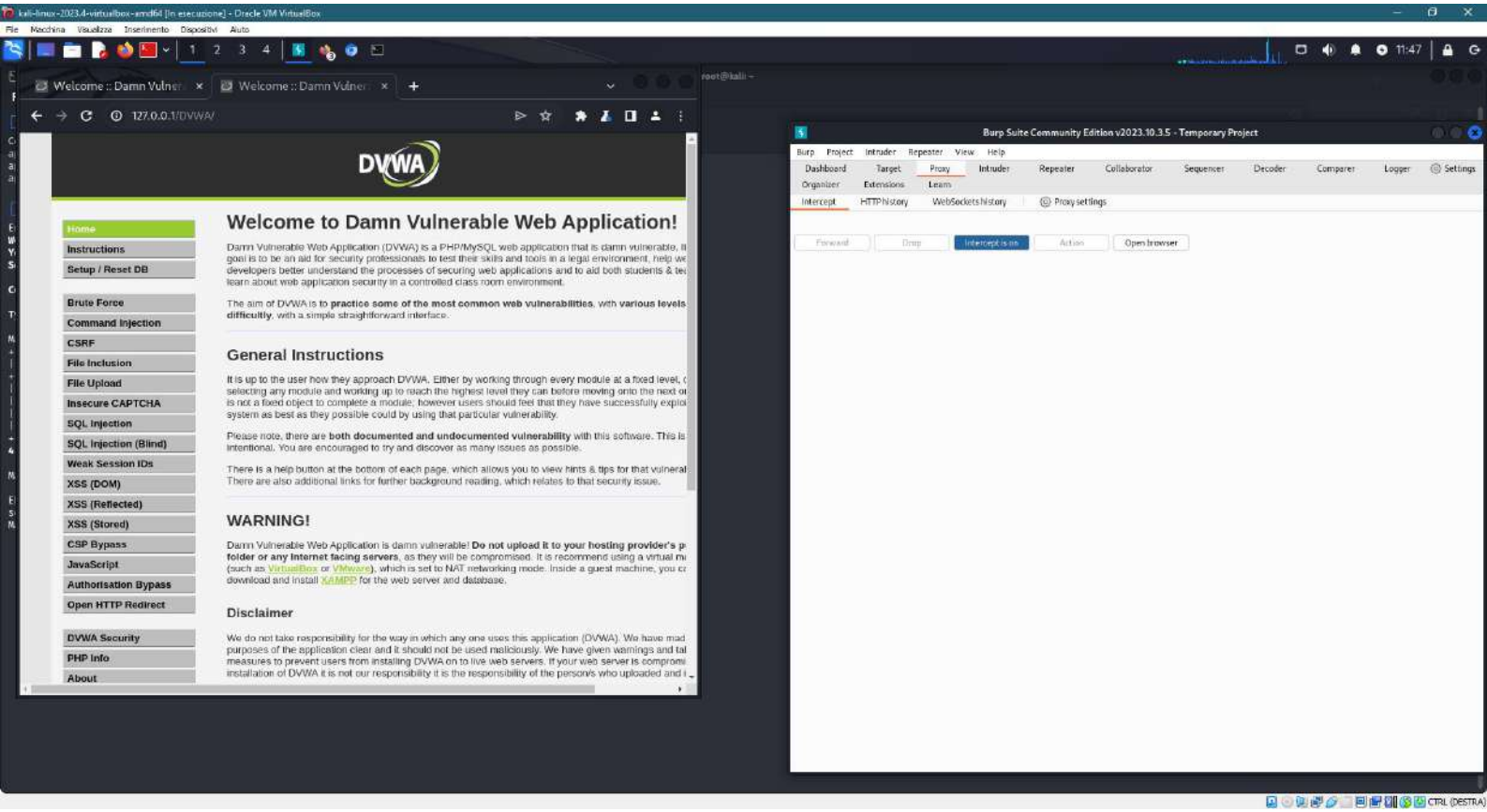
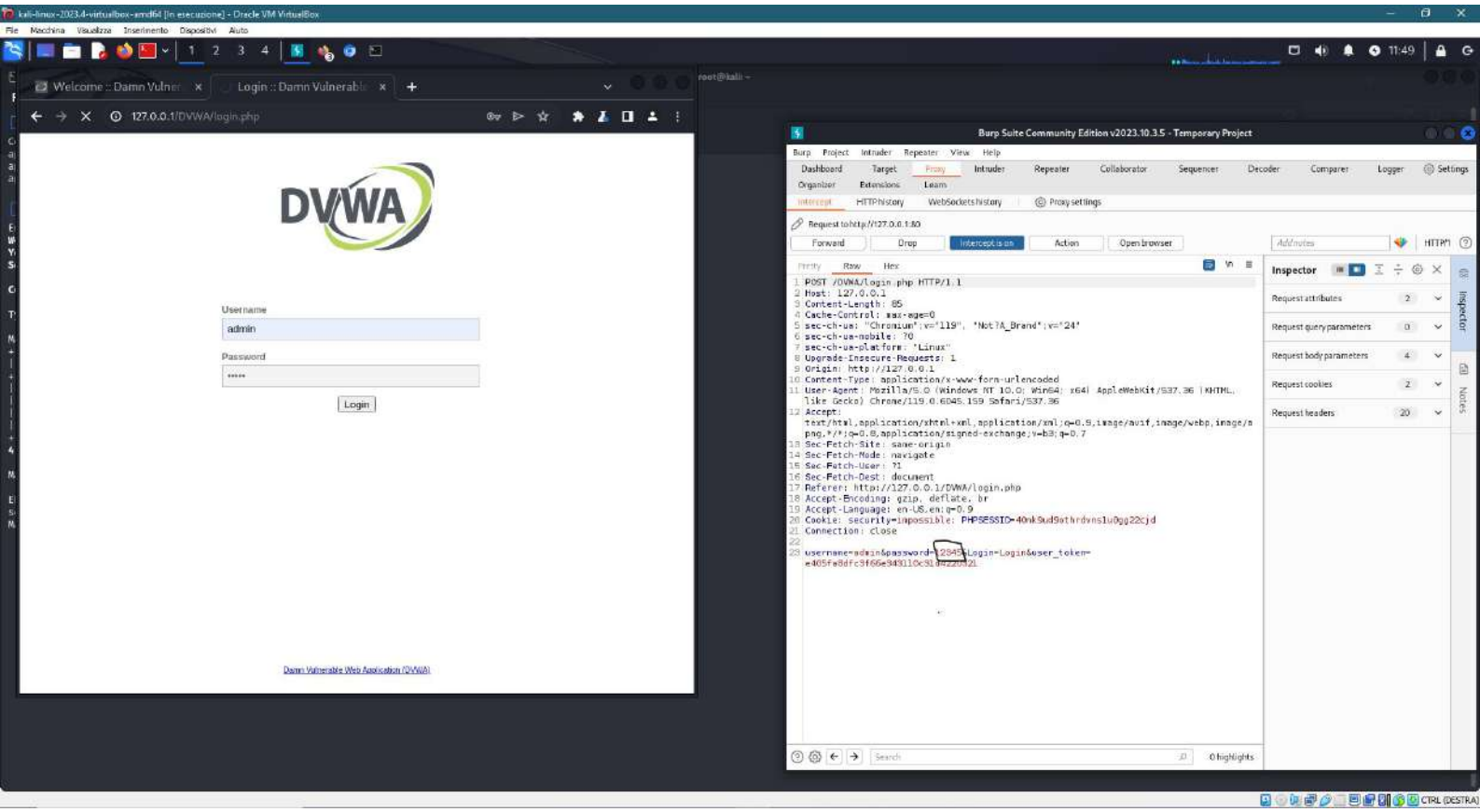
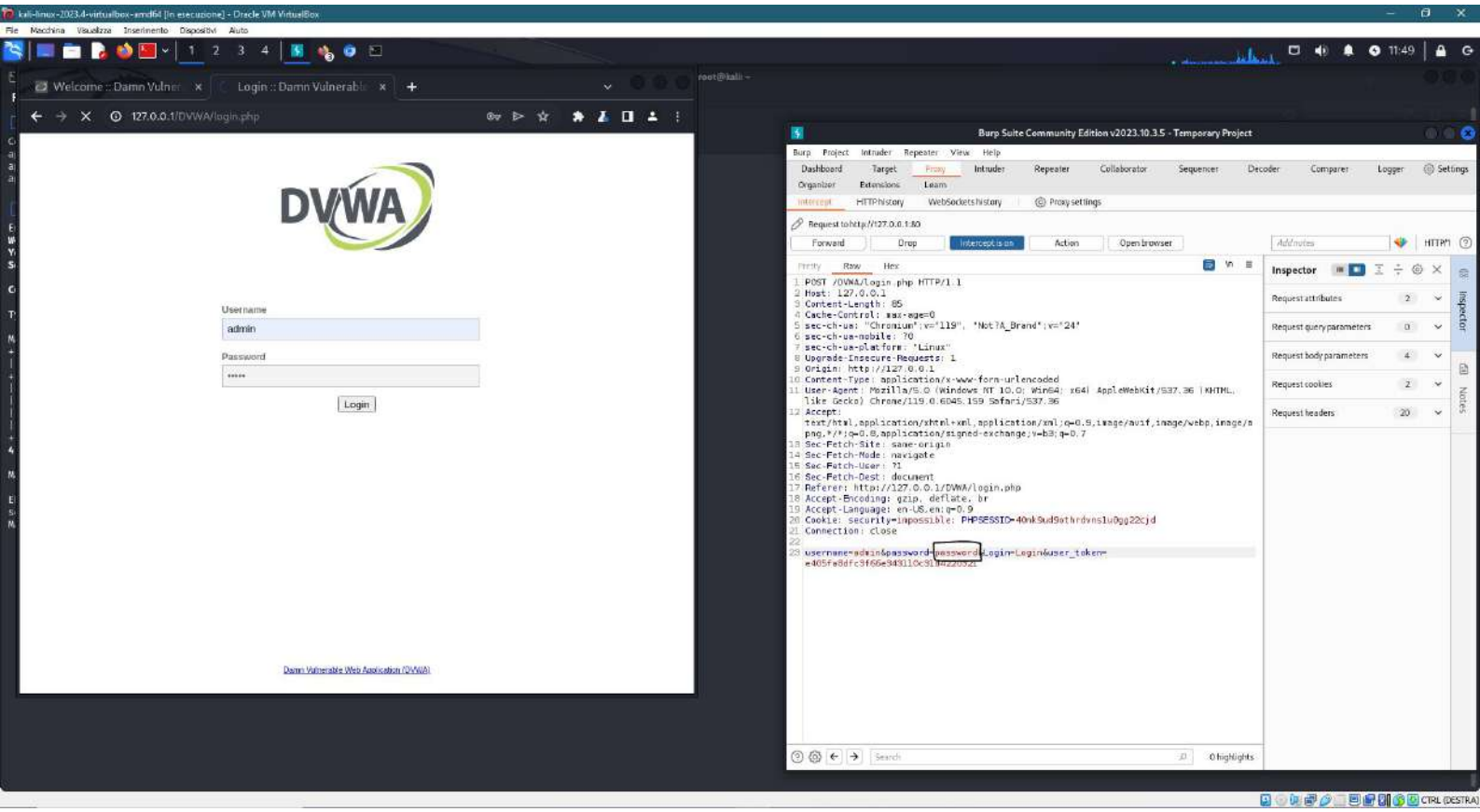

kali-linux-2023.4-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Welcome :: Damn Vulner
PortSwigger
127.0.0.1/DVWA
The latest research into web race conditions
For too long, web race-condition attacks have focused on a tiny handful of scenarios. Their true potential has been masked thanks to tricky workflows, missing tooling, and simple network jitter hiding all but the most trivial, obvious examples.
Delve into PortSwigger's latest research to discover multiple new classes of race condition, work through the interactive labs to learn the methodology behind the discovery, and try out the new single-packet attack feature in Burp Repeater.
STATE MACHINE
Burp Suite Community Edition v2023.10.3.5 - Temporary Project
Request to http://127.0.0.1:80
GET /DVWA/ HTTP/1.1
Host: 127.0.0.1
Upgrade-Insecure-Requests: 1
Inspector
Request attributes
Request query parameters
Request body parameters
Request cookies
Request headers
CTRL (DESTRA)


kali-linux-2023.4-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Welcome :: Damn Vulner
127.0.0.1/DVWA/
DVWA
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
Welcome to Damn Vulnerable Web Application!
General Instructions
WARNING!
Disclaimer
Burp Suite Community Edition v2023.10.3.5 - Temporary Project
Dashboard
Target
Proxy
Intruder
Repeater
Collaborator
Sequencer
Decoder
Comparer
Logger
Settings
Intercept
HTTP history
WebSockets history
Proxy settings
Forward
Drop
Intercept is on
Action
Open browser
CTRL (DESTRA)


kali-linux-2023.4-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Welcome :: Damn Vulner
Login :: Damn Vulnerable
127.0.0.1/DVWA/login.php
DVWA
Username
admin
Password
Login
Damn Vulnerable Web Application (DVWA)
Burp Suite Community Edition v2023.10.3.5 - Temporary Project
Request to http://127.0.0.1:80
Forward
Drop
Intercept is on
Action
Open browser
POST /DVWA/login.php HTTP/1.1
Host: 127.0.0.1
Content-Length: 85
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="119", "Not?A_Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
Origin: http://127.0.0.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://127.0.0.1/DVWA/login.php
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: security=impossible; PHPSESSID=40nk9ud9othrdvns1u0gg22cjd
Connection: close
username=admin&password=12345&Login=Login&user_token=
Inspector
Request attributes
Request query parameters
Request body parameters
Request cookies
Request headers
0 highlights
CTRL (DESTRA)


kali-linux-2023.4-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Welcome :: Damn Vulner
Login :: Damn Vulnerable
127.0.0.1/DVWA/login.php
DVWA
Username
admin
Password
Login
Damn Vulnerable Web Application (DVWA)
Burp Suite Community Edition v2023.10.3.5 - Temporary Project
Request to http://127.0.0.1:80
Forward
Drop
Intercept is on
Action
Open browser
POST /DVWA/login.php HTTP/1.1
Host: 127.0.0.1
Content-Length: 85
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="119", "Not?A_Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
Origin: http://127.0.0.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://127.0.0.1/DVWA/login.php
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: security=impossible; PHPSESSID=40nk9ud9othrdvns1u0gg22cjd
Connection: close
username=admin&password=password&Login=Login&user_token=
Inspector
Request attributes
Request query parameters
Request body parameters
Request cookies
Request headers
0 highlights
CTRL (DESTRA)