Day 13: Exploiting Insecure Deserialization

The task is to identify a vulnerable application, exploit an insecure deserialization vulnerability using Burp Suite in Swigger Lab, and demonstrate its impact. This report outlines the steps taken and the findings of this practical exercise.

Insecure deserialization is a critical security vulnerability that occurs when an application deserializes untrusted data without proper validation, potentially enabling an attacker to execute arbitrary code, gain unauthorized access, or disrupt the application's functionality.

Step 1: Identifying Swigger Lab and the Vulnerable Application:

I selected Swigger Lab as the environment for this practical exercise, known for its realistic and educational web security challenges.

Within Swigger Lab, I identified a vulnerable application that was intentionally designed to contain an insecure deserialization vulnerability.

Step 2: Initial Testing:

I initiated initial testing of the vulnerable application to confirm the presence of the insecure deserialization vulnerability.

Step 3: Burp Suite Configuration:

I configured Burp Suite, a widely used web security testing tool, to intercept and manipulate requests and responses.

Step 4: Payload Crafting:

Leveraging Burp Suite's capabilities, I crafted payloads specifically designed to trigger the insecure deserialization vulnerability within the application.

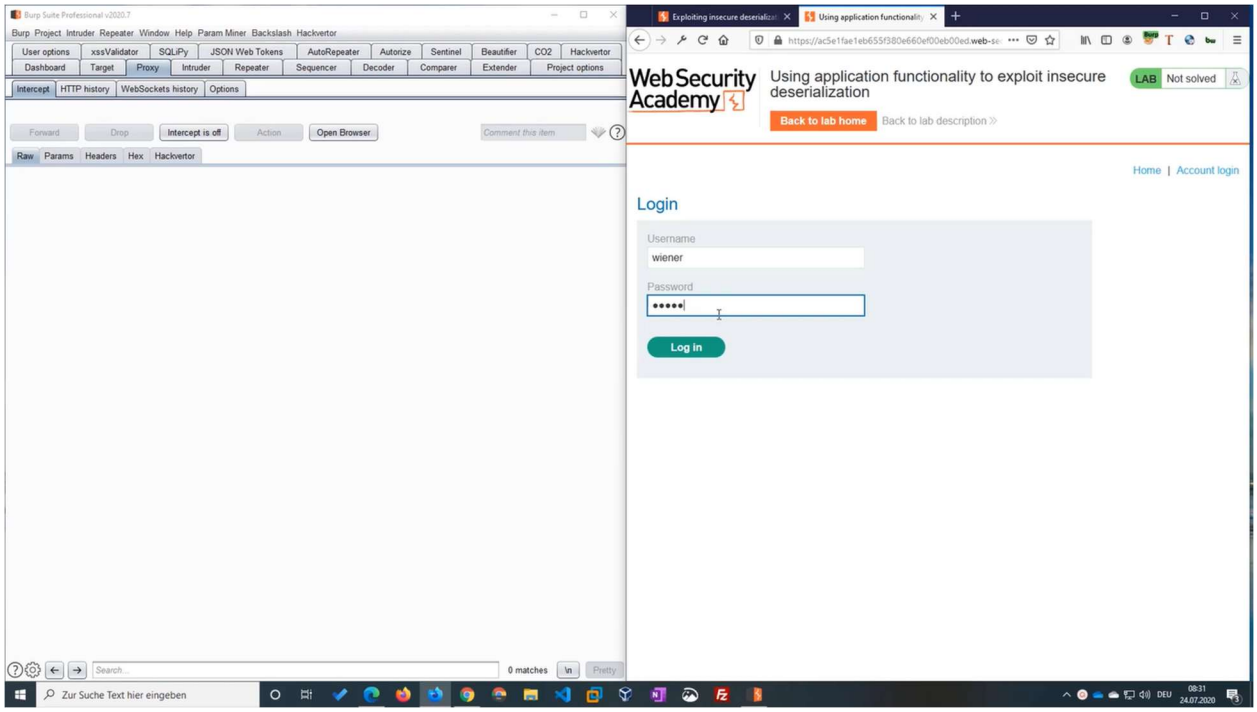
Step 5: Exploitation Using Burp Suite:

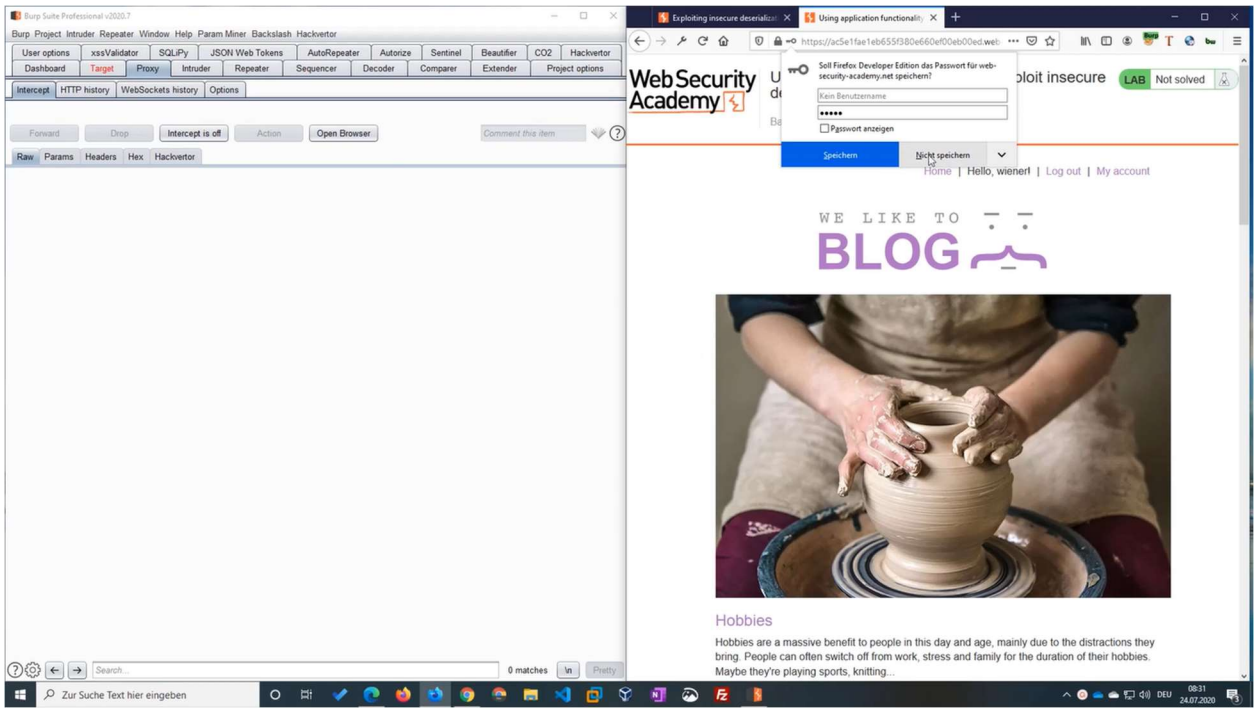
I injected the crafted payloads into the application, particularly in areas where deserialization of user-supplied data occurred.

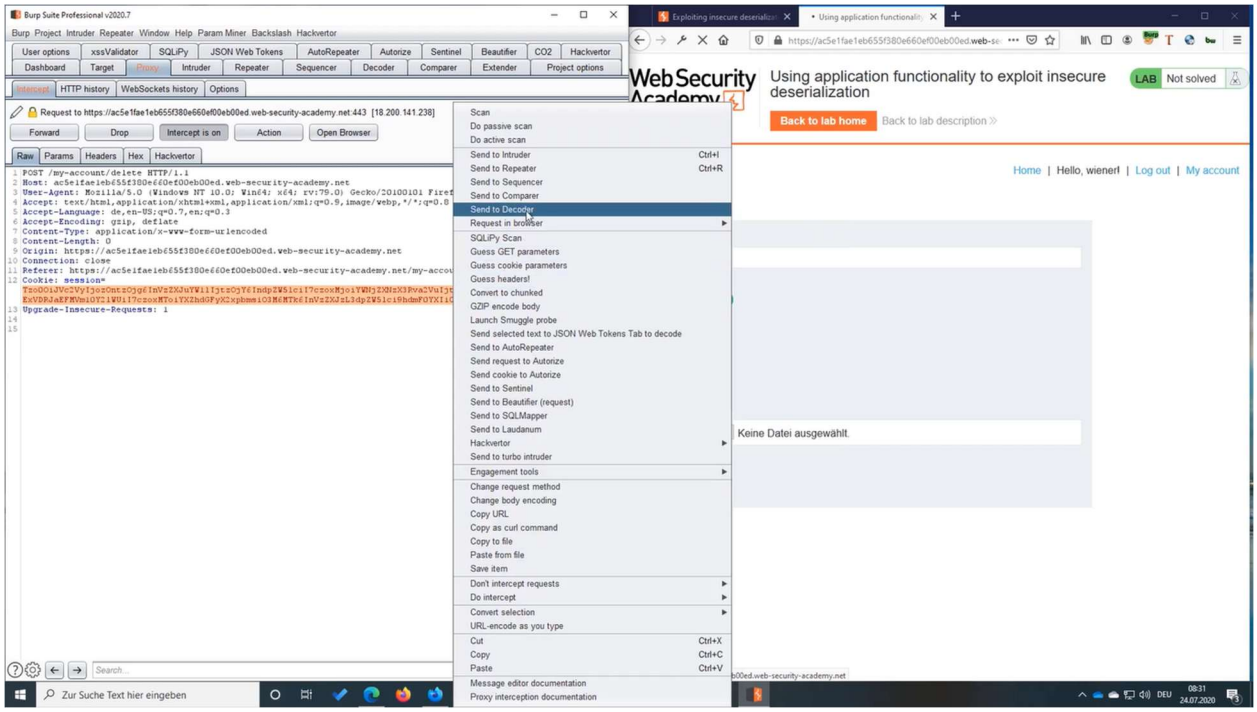
I leveraged Burp Suite to intercept and modify requests and responses, facilitating the exploitation process.

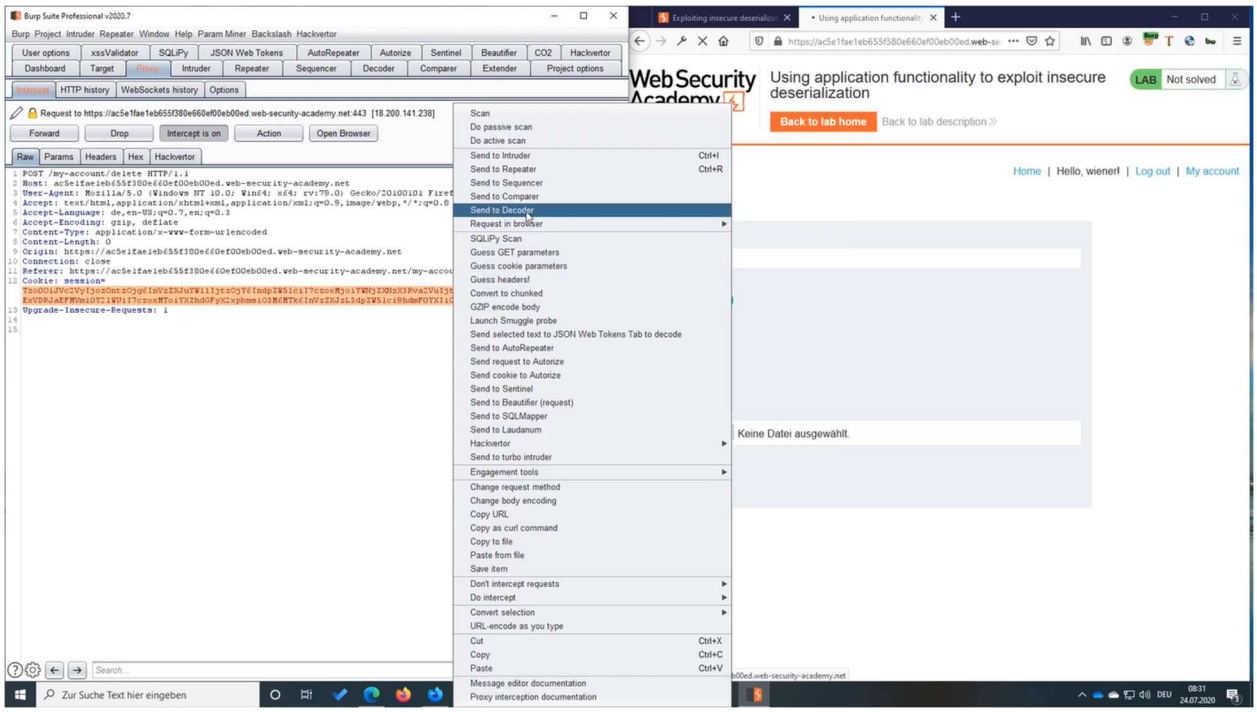
Step 6: Demonstrating Impact:

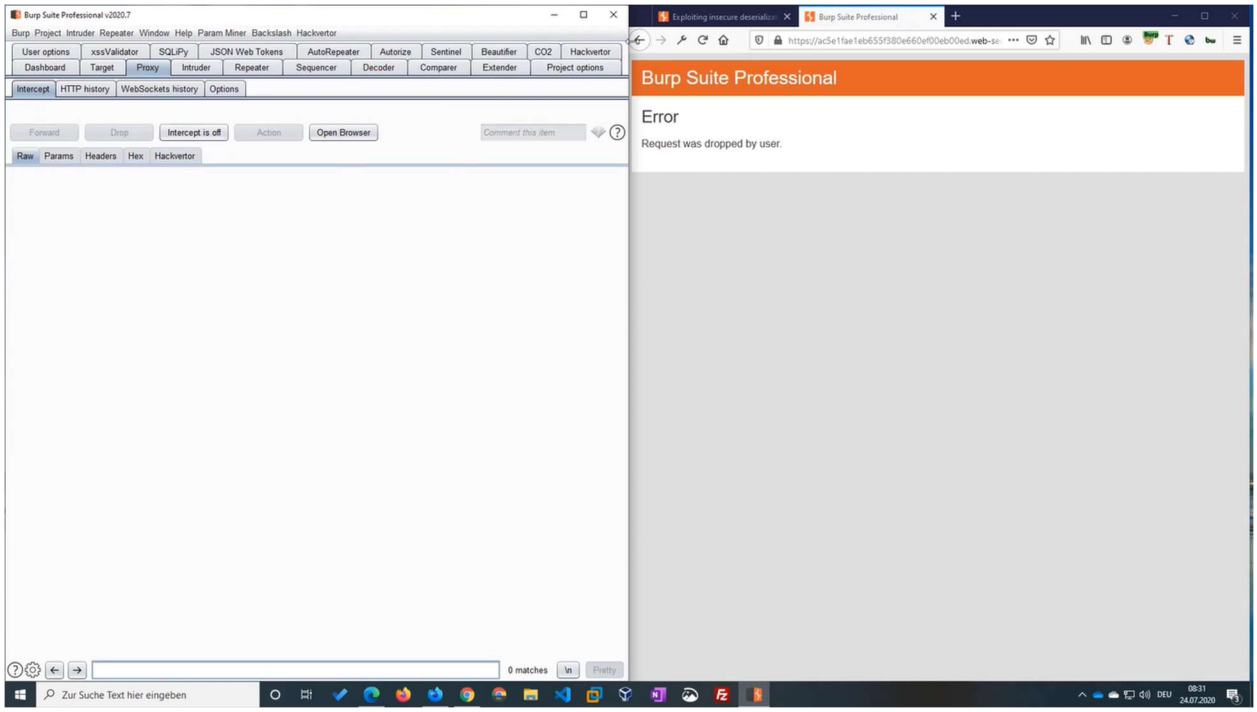
Upon successful exploitation, I documented the impact, which included actions performed, data accessed, or disruptions caused by the insecure deserialization vulnerability.

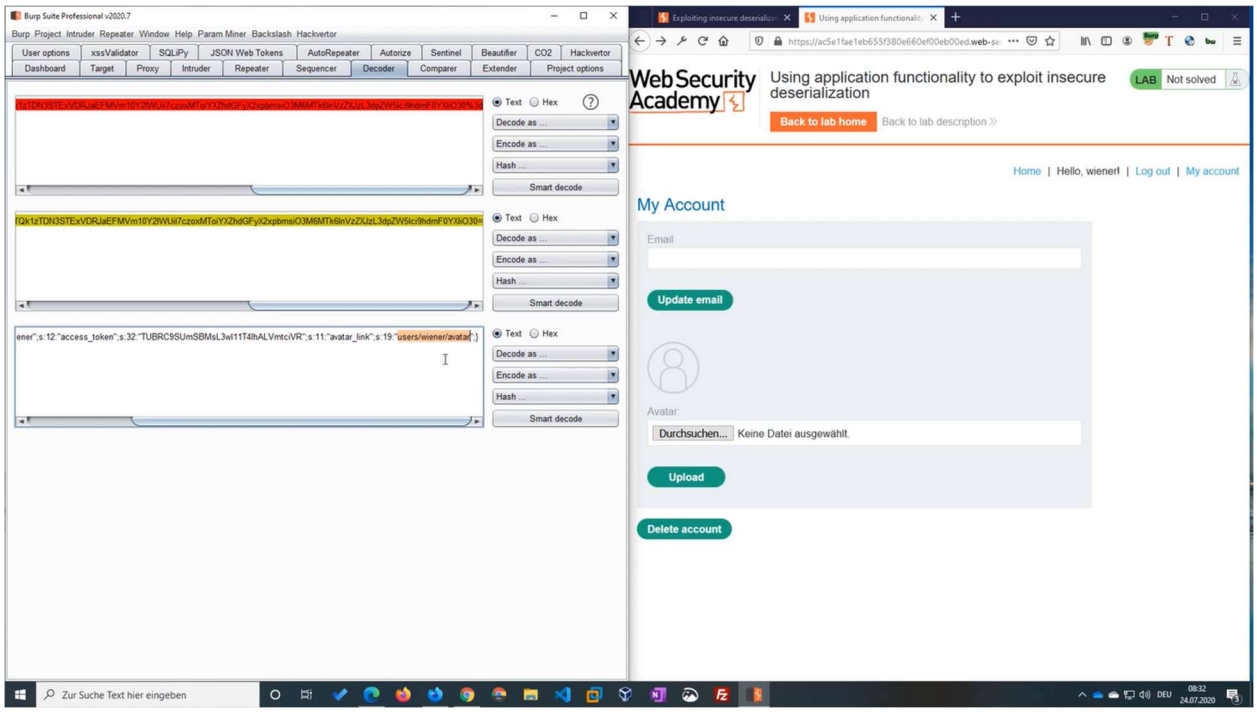

Burp Suite Professional v2020.7
Burp Project Intruder Repeater Window Help Param Miner Backslash Hackvertor
User options xssValidator SQLiPy JSON Web Tokens AutoRepeater Autorize Sentinel Beautifier CO2 Hackvertor
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is off Action Open Browser
Raw Params Headers Hex Hackvertor
Web Security Academy
Using application functionality to exploit insecure deserialization
LAB Not solved
Back to lab home
Back to lab description
Home | Account login
Login
Username
wiener
Password
Log in

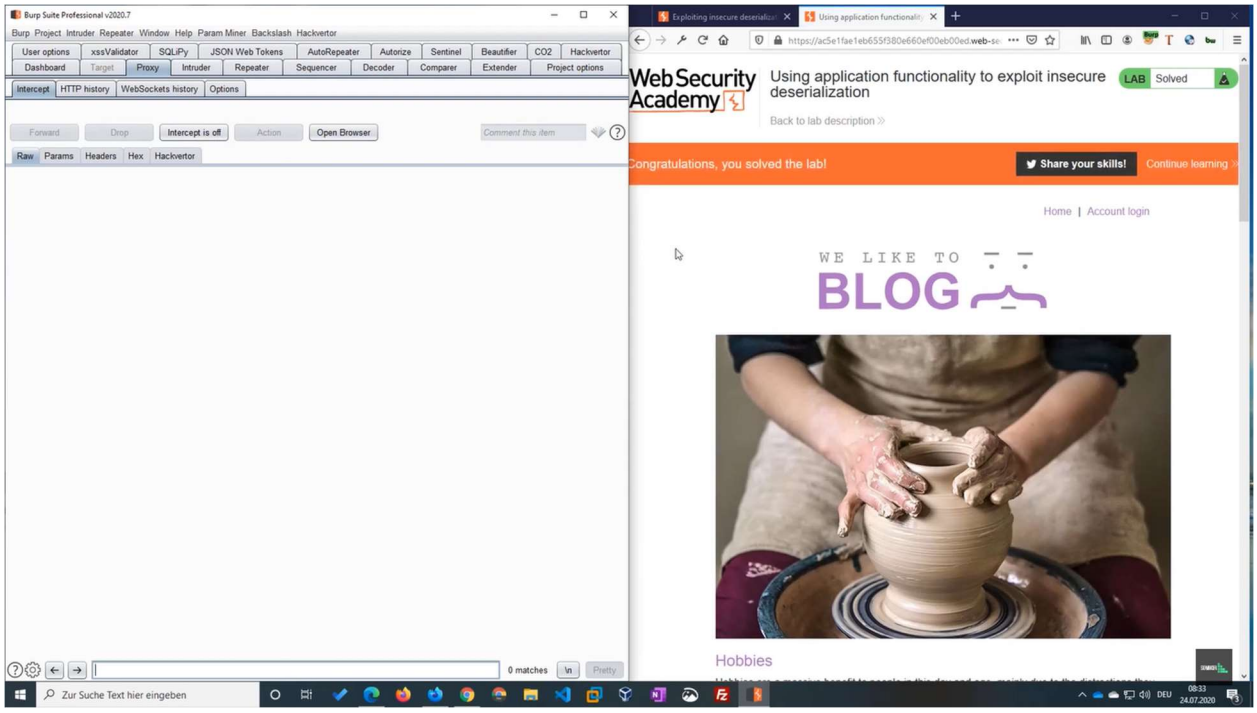

Burp Suite Professional v2020.7
Burp Project Intruder Repeater Window Help Param Miner Backslash Hackvertor
User options xssValidator SQLiPy JSON Web Tokens AutoRepeater Autorize Sentinel Beautifier CO2 Hackvertor
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is off Action Open Browser
Raw Params Headers Hex Hackvertor
Web Security Academy
LAB Not solved
Soll Firefox Developer Edition das Passwort für web-security-academy.net speichern?
Kein Benutzername
Passwort anzeigen
Speichern
Nicht speichern
Home | Hello, wiener! | Log out | My account
WE LIKE TO
BLOG
Hobbies
Hobbies are a massive benefit to people in this day and age, mainly due to the distractions they bring. People can often switch off from work, stress and family for the duration of their hobbies. Maybe they're playing sports, knitting...


Burp Suite Professional v2020.7
Request to https://ac5e1fae1eb655f380e660ef00eb00ed.web-security-academy.net:443 [18.200.141.238]
Forward
Drop
Intercept is on
Action
Open Browser
Raw
Params
Headers
Hex
Hackvertor
POST /my-account/delete HTTP/1.1
Host: ac5e1fae1eb655f380e660ef00eb00ed.web-security-academy.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:79.0) Gecko/20100101 Firef
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: de,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
Origin: https://ac5e1fae1eb655f380e660ef00eb00ed.web-security-academy.net
Connection: close
Referer: https://ac5e1fae1eb655f380e660ef00eb00ed.web-security-academy.net/my-accou
Cookie: session=
Upgrade-Insecure-Requests: 1
Scan
Do passive scan
Do active scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Request in browser
SQLiPy Scan
Guess GET parameters
Guess cookie parameters
Guess headers!
Convert to chunked
GZIP encode body
Launch Smuggle probe
Send selected text to JSON Web Tokens Tab to decode
Send to AutoRepeater
Send request to Autorize
Send cookie to Autorize
Send to Sentinel
Send to Beautifier (request)
Send to SQLMapper
Send to Laudanum
Hackvertor
Send to turbo intruder
Engagement tools
Change request method
Change body encoding
Copy URL
Copy as curl command
Copy to file
Paste from file
Save item
Don't intercept requests
Do intercept
Convert selection
URL-encode as you type
Cut Ctrl+X
Copy Ctrl+C
Paste Ctrl+V
Message editor documentation
Proxy interception documentation
Web Security Academy
Using application functionality to exploit insecure deserialization
LAB Not solved
Back to lab home
Back to lab description
Home | Hello, wiener! | Log out | My account
Keine Datei ausgewählt
Zur Suche Text hier eingeben
DEU
08:31
24.07.2020


Burp Suite Professional v2020.7
Request to https://ac5e1fae1eb655f380e660ef00eb00ed.web-security-academy.net:443 [18.200.141.238]
Forward
Drop
Intercept is on
Action
Open Browser
Raw
Params
Headers
Hex
Hackvertor
POST /my-account/delete HTTP/1.1
Host: ac5e1fae1eb655f380e660ef00eb00ed.web-security-academy.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:79.0) Gecko/20100101 Firef
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: de,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
Origin: https://ac5e1fae1eb655f380e660ef00eb00ed.web-security-academy.net
Connection: close
Referer: https://ac5e1fae1eb655f380e660ef00eb00ed.web-security-academy.net/my-accou
Cookie: session=
Upgrade-Insecure-Requests: 1
Scan
Do passive scan
Do active scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Request in browser
SQLiPy Scan
Guess GET parameters
Guess cookie parameters
Guess headers!
Convert to chunked
GZIP encode body
Launch Smuggle probe
Send selected text to JSON Web Tokens Tab to decode
Send to AutoRepeater
Send request to Autorize
Send cookie to Autorize
Send to Sentinel
Send to Beautifier (request)
Send to SQLMapper
Send to Laudanum
Hackvertor
Send to turbo intruder
Engagement tools
Change request method
Change body encoding
Copy URL
Copy as curl command
Copy to file
Paste from file
Save item
Don't intercept requests
Do intercept
Convert selection
URL-encode as you type
Cut Ctrl+X
Copy Ctrl+C
Paste Ctrl+V
Message editor documentation
Proxy interception documentation
Web Security Academy
Using application functionality to exploit insecure deserialization
LAB Not solved
Back to lab home
Back to lab description
Home | Hello, wiener! | Log out | My account
Keine Datei ausgewählt
Zur Suche Text hier eingeben
DEU
08:31
24.07.2020


Burp Suite Professional v2020.7
Burp Project Intruder Repeater Window Help Param Miner Backslash Hackvertor
User options xssValidator SQLiPy JSON Web Tokens AutoRepeater Autorize Sentinel Beautifier CO2 Hackvertor
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is off Action Open Browser
Comment this item
Raw Params Headers Hex Hackvertor
0 matches
Burp Suite Professional
Error
Request was dropped by user.


Burp Suite Professional v2020.7
Decoder
Text Hex
Decode as ...
Encode as ...
Hash ...
Smart decode
Web Security Academy
Using application functionality to exploit insecure deserialization
LAB Not solved
Back to lab home
Back to lab description
Home | Hello, wiener! | Log out | My account
My Account
Email
Update email
Avatar:
Durchsuchen... Keine Datei ausgewählt.
Upload
Delete account



Conclusion:

web application using Burp Suite in Swigger Lab. By identifying and exploiting this vulnerability, I gained practical experience in understanding the risks associated with insecure deserialization and its potential impact.

Insecure deserialization is a severe security concern that can lead to unauthorized code execution and data breaches. Such exercises serve as invaluable learning experiences and underscore the importance of proactive security testing and securing applications against deserialization vulnerabilities.