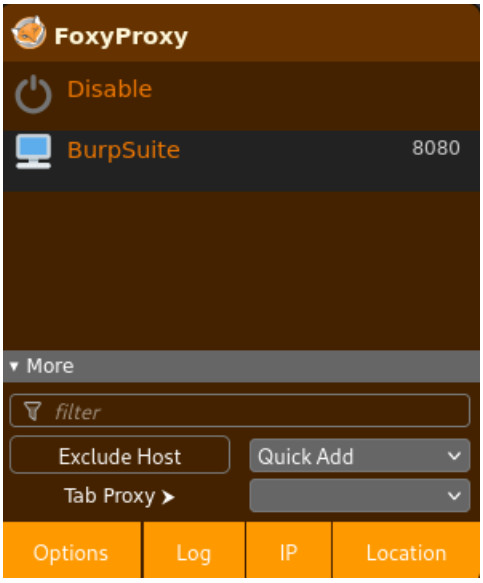
Write Up Apprentice Web Security Academy

Mutiara Setya Rini

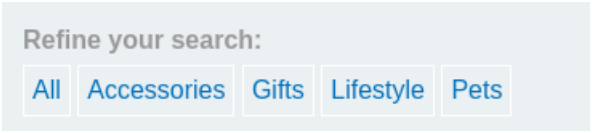
Daftar isi

SQL injection vulnerability in WHERE clause allowing retrieval of hidden data

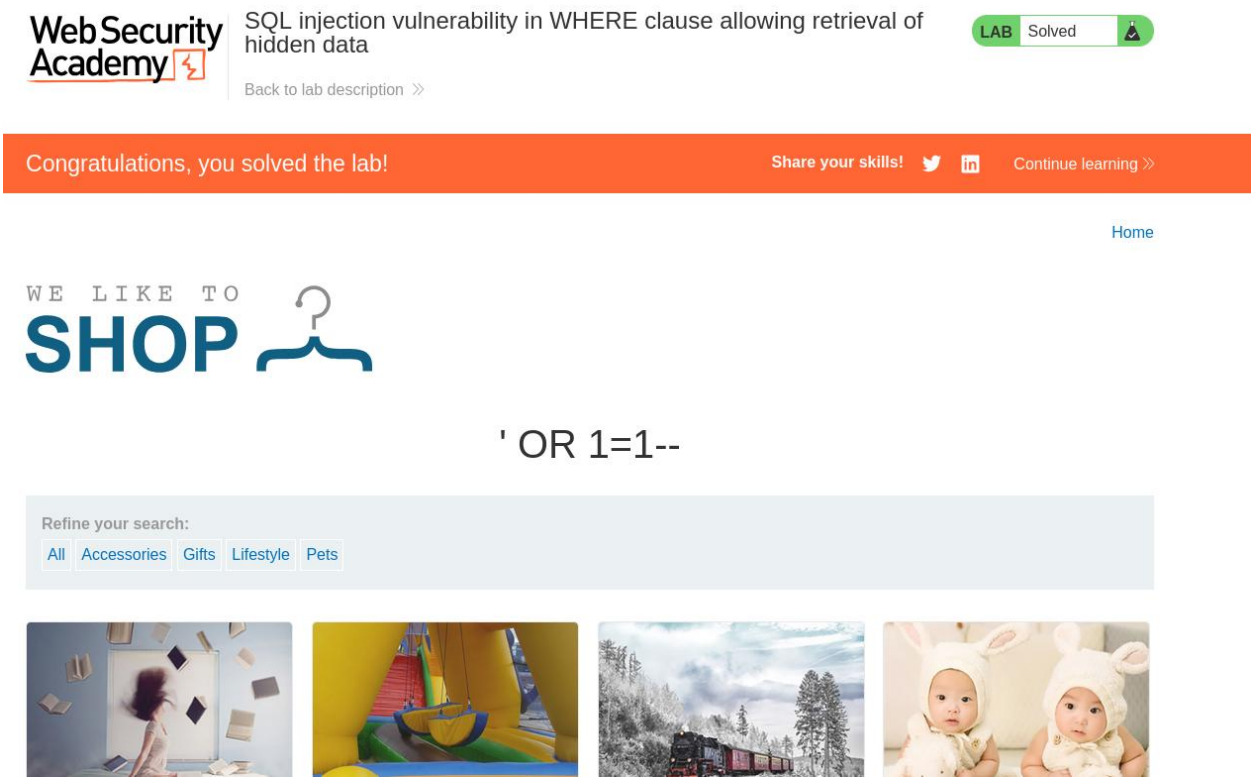
Buka/akses lab dari challenge ini. Kemudian aktifkan proxy burp suite yang sebelumnya telah disetting, saya menggunakan foxyproxy seperti di bawah ini :



Refresh lab kemudian pilih search Gifts



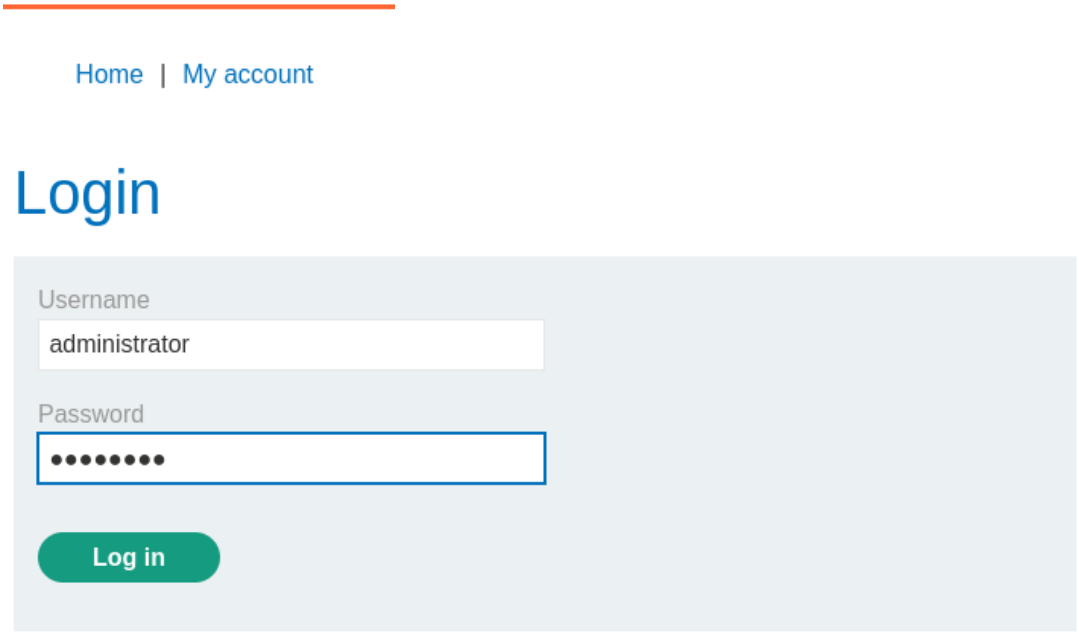
Di dalam intercept burpsuite akan terlihat request seperti ini dan ganti bagian Gifts menjadi ‘+OR+1=1--



Challenge telah berhasil terselesaikan.

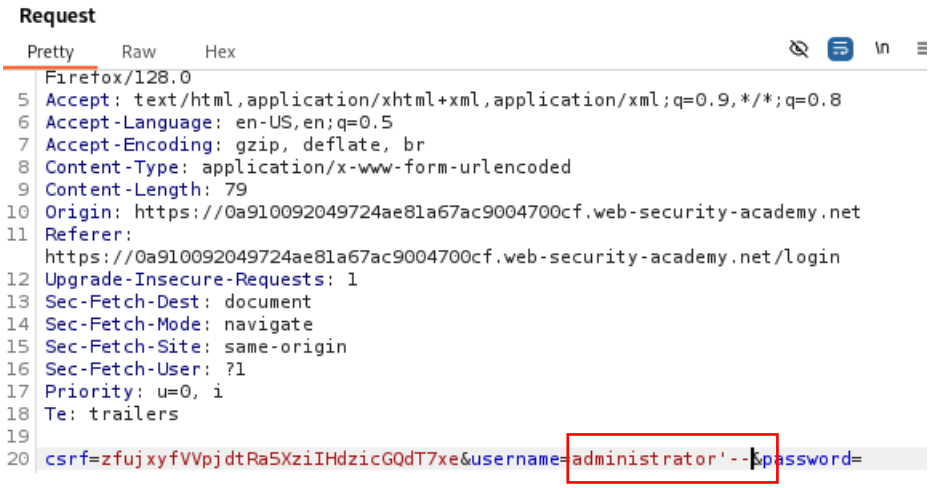
SQL injection vulnerability allowing login bypass

Buka lab dari challenge yang ada. Kemudian aktifkan proxy dan intercept burpsuite. Pilih menu my account pada lab.

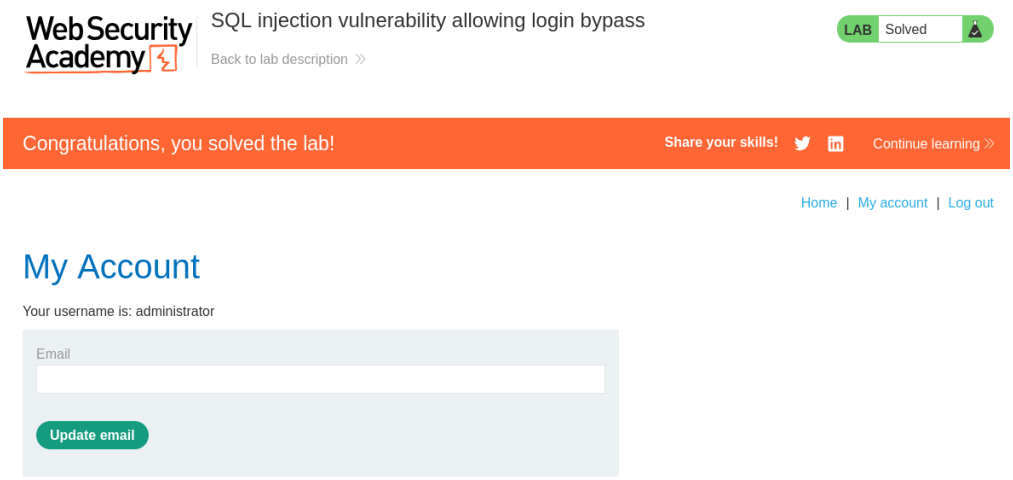


Kemudian isikan username dan password secara bebas/random. Nanti akan diubah menggunakan burpsuite.

Buka burpsuite dan forward sampai pada bagian seperti di bawah ini.



tambahkan '—di samping administrator dan forward hingga web lab berubah menjadi seperti ini :



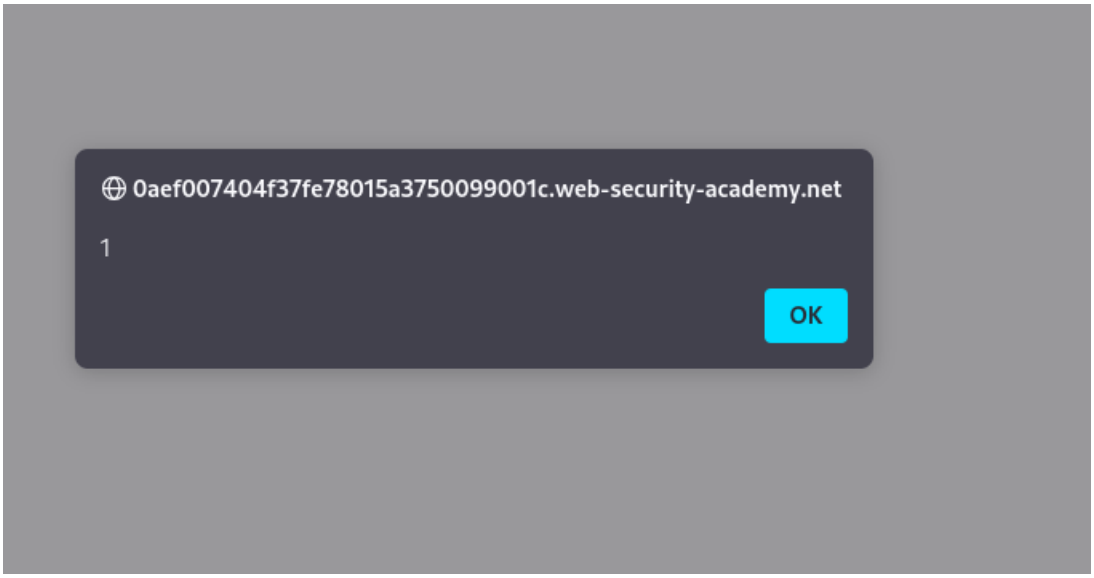
Challenge berhasil diselesaikan.

Reflected XSS into HTML context with nothing encoded

Buka lab, kemudian ketik <script>alert(1)</script> pada search box yang artinya :

<script> : tag html untuk menjalankan javascript

alert(1) : 1 di sini berarti jika input script berhasil akan aka notif pop up 1.



Terlihat bahwa setelah search dilakukan, muncul notif pop up 1 yang artinya script berhasil diinjeksi.

Challenge berhasil diselesaikan.

Stored XSS into HTML context with nothing encoded

Buka lab, kemudian pilih salah satu post dan klik view post.

Finding Inspiration

I don't care who you are or where you're from aren't just poignant Backstreet Boys lyrics, they also ring true in life, certainly as far as inspiration goes. We all lack drive sometimes, or perhaps we have the drive but...

View post

Tulis komentar berisi </script>alert(1)<script> dan isi nama, email, dan website random.

Leave a comment

Comment:

</script>alert(1)<script>

Name:

Miaw

Email:

miawmiaw@gmail.com

Website:

https://miawmiaw.com

Post Comment

Congratulations, you solved the lab! Share your skills! Continue learning »

Home

Thank you for your comment!

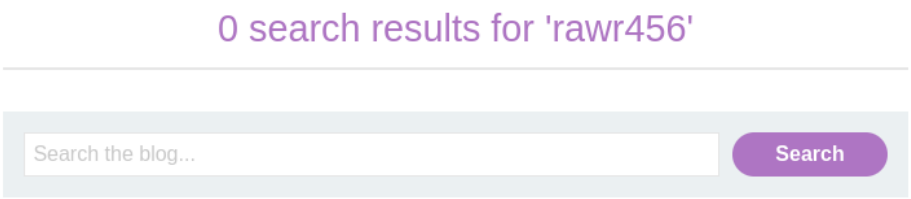
Your comment has been submitted.

< Back to blog

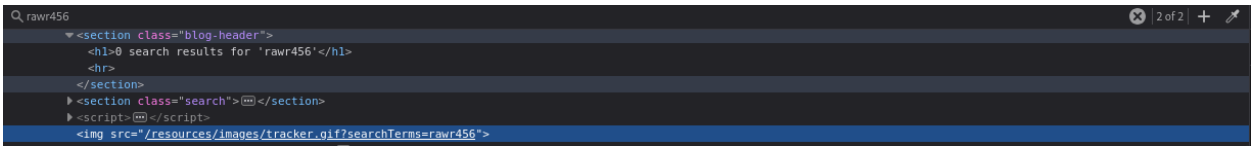
Challenge berhasil diselesaikan

DOM XSS in document.write sink using source location.search

Buka lab, kemudian search suatu string random dalam search box (aplhabet + angka). Selanjutnya akan muncul seperti ini :



Kemudian inspect pada page tersebut dan cari string rawr456.



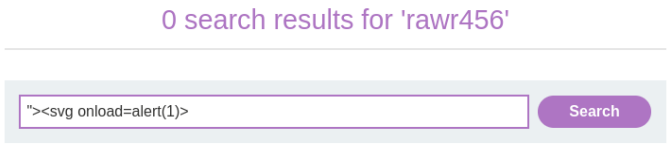
<img src="/resources/images/tracker.gif?searchTerms=rawr456">

ini mengindikasikan bahwa page tersebut menempatkan input rawr456 di searchTerms. Untuk melakukan XSS, kita mengganti rawr456 dengan payload yang sekiranya bisa membobol atribut dan menyisipkan tag lain. Dalam mengatasi challenge ini kita bisa menggunakan command `"><svg onload=alert(1)>` yang artinya :

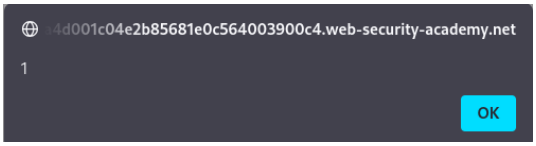
“> : menutup atribut dan tag yang ada di <imgsrc="/resources/images/tracker.gif?searchTerms=rawr456">

svg : tag html yang memiliki onload

onload=alert(1) : ketika svg dijalankan, alert(1) akan dieksekusi



Search command tersebut dan muncul notif 1 seperti di bawah ini yang berarti proses berhasil.



Challenge telah berhasil diselesaikan.