

Lab 4 – Analysing Website using Burp Suite

Task 1: Capturing request and response.

Capture request and response while signing up and signing in into your website. Signup and sign in using your name as username. Try with both correct and incorrect credentials.

Incorrect credentials

The screenshot displays the Burp Suite interface with a captured HTTP request and response. The 'Site map' on the left shows the target website structure. The 'History' table lists several requests, with the most recent one (POST /userinfo.php) highlighted. The 'Request' pane shows the raw HTTP request, and the 'Response' pane shows the raw HTTP response. The 'Inspector' pane on the right shows the request and response details.

| Host | Method | URL | Params | Status | Length | MIME type | Title | Comment | Time |
|----------------------------|--------|---------------|--------|--------|--------|-----------|----------------------|---------|---------------|
| http://testphp.vulnweb.com | GET | / | | 200 | 5175 | HTML | Home of Acunetix Art | | 23:15:41.2... |
| http://testphp.vulnweb.com | GET | /login.php | | 200 | 5740 | HTML | login page | | 23:15:54.2... |
| http://testphp.vulnweb.com | POST | /userinfo.php | | 302 | 253 | text | | | 23:16:58.2... |

Request

```
1 POST /userinfo.php HTTP/1.1
2 Host: testphp.vulnweb.com
3 Content-Length: 22
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://testphp.vulnweb.com
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74
  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 Referer: http://testphp.vulnweb.com/login.php
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Connection: close
14
15 username=admin&pass=admin
```

Response

```
1 HTTP/1.1 302 Found
2 Server: nginx/1.19.0
3 Date: Sat, 02 Apr 2022 17:46:43 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
6 X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
7 Location: login.php
8 Content-Length: 14
9
10 you must login
```

Inspector

- Request Attributes: 2
- Request Body Parameters: 2
- Request Headers: 12
- Response Headers: 7

Correct credentials

user info x +

← → ↻ ⚠ Not secure | testphp.vulnweb.com/userinfo.php

acunetix **acuart**

TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo | Logout test

search art go

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer

John Smith (test)

On this page you can visualize or edit you user information.

Name:

Credit card number:

E-Mail:

Phone number:

Address:

You have 0 items in your cart. You visualize you cart here.

About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

Burp Suite Community Edition v2022.2.4 - Temporary Project

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

Site map Scope Issue definitions

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

| Host | Method | URL | Params | Status | Length | MIME type | Title | Comment | Time request |
|----------------------------|--------|--------------------|--------|--------|--------|-----------|----------------------|---------|----------------|
| http://testphp.vulnweb.com | GET | / | | 200 | 5175 | HTML | Home of Acunetix Art | | 23:15:41 2 ... |
| http://testphp.vulnweb.com | GET | /login.php | | 200 | 5740 | HTML | login page | | 23:18:53 2 ... |
| http://testphp.vulnweb.com | POST | /userinfo.php | | ✓ 200 | 6211 | HTML | user info | | 23:18:56 2 ... |
| http://testphp.vulnweb.com | POST | /userinfo.php | | ✓ 302 | 253 | text | | | 23:16:58 2 ... |
| http://testphp.vulnweb.com | GET | /AJAX/index.php | | | | | | | |
| http://testphp.vulnweb.com | GET | /Flash/add.swf | | | | | | | |
| http://testphp.vulnweb.com | GET | /Mod_Rewrite_Shop/ | | | | | | | |
| http://testphp.vulnweb.com | GET | /artists.php | | | | | | | |
| http://testphp.vulnweb.com | GET | /cart.php | | | | | | | |
| http://testphp.vulnweb.com | GET | /testphp.php | | | | | | | |

Request

1 POST /userinfo.php HTTP/1.1
2 Host: testphp.vulnweb.com
3 Content-Length: 20
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://testphp.vulnweb.com
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 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 Referer: http://testphp.vulnweb.com/login.php
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Connection: close
14
15 username=test&pass=test

Response

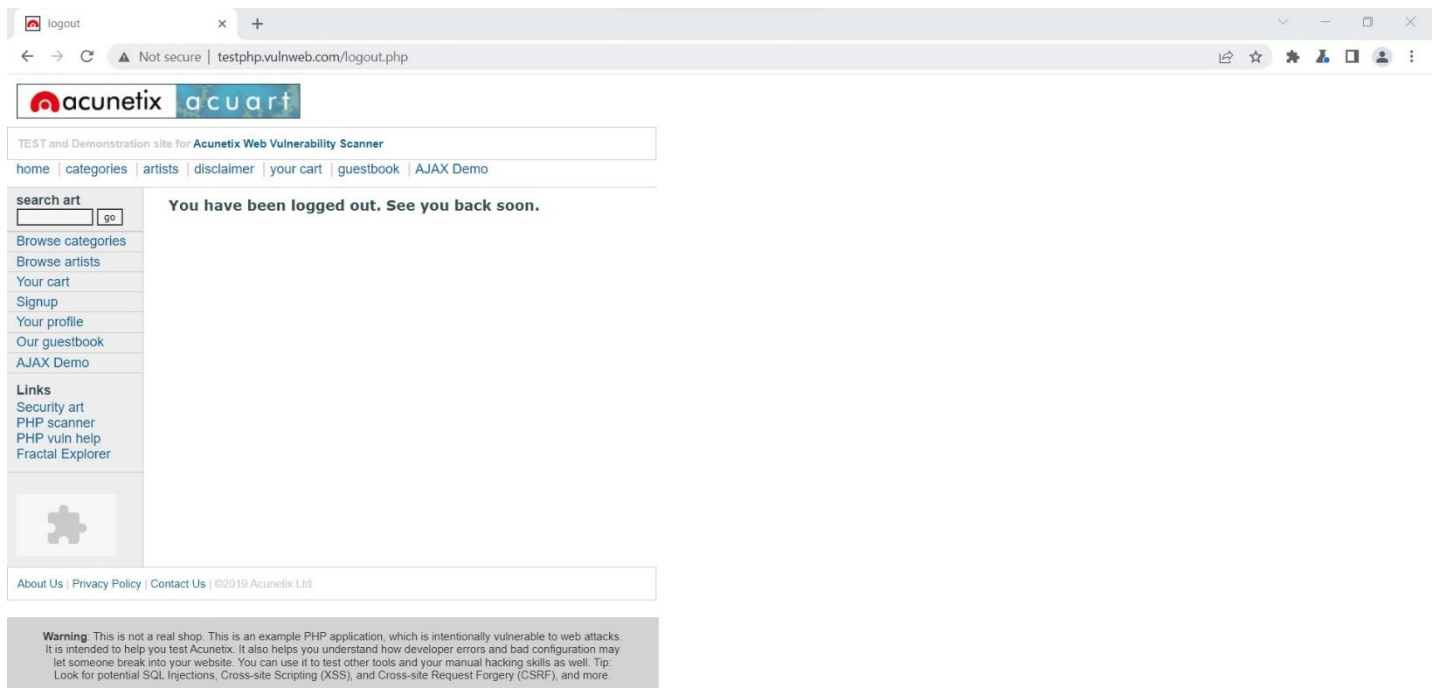
1 HTTP/1.1 200 OK
2 Server: nginx/1.19.0
3 Date: Sat, 02 Apr 2022 17:48:38 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
6 X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
7 Set-Cookie: login=test12Ptest
8 Content-Length: 5963
9
10 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
11 "http://www.w3.org/TR/html4/loose.dtd">
12 <html>
13 <!-- InstanceBegin
14 template="/Templates/main_dynamic_template.dwt.php"
15 codeOutsideHTMLIsLocked="false" -->
16 <head>
17 <meta http-equiv="Content-Type" content="text/html;
18 charset=iso-8859-2">
19 <!-- InstanceBeginEditable name="document_title_rgn" -->
20 <title>
21 user info
22 </title>
23 <!-- InstanceEndEditable -->
24 <!-- InstanceBeginEditable name="style_css" type="text/css">
25 <link rel="stylesheet" href="style.css" type="text/css">
26 <!-- InstanceBeginEditable name="headers_rgn" -->
27 <!-- here goes headers headers -->
28 <!-- InstanceEndEditable -->
29 <script language="JavaScript" type="text/JavaScript">
30 <!--

Inspector

Request Attributes 2
Request Body Parameters 2
Request Headers 12
Response Headers 7

Task 2: Use of repeater.

Repeat the requests captured in Task 1 and see what response is coming from server.



logout

Not secure | testphp.vulnweb.com/logout.php

acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

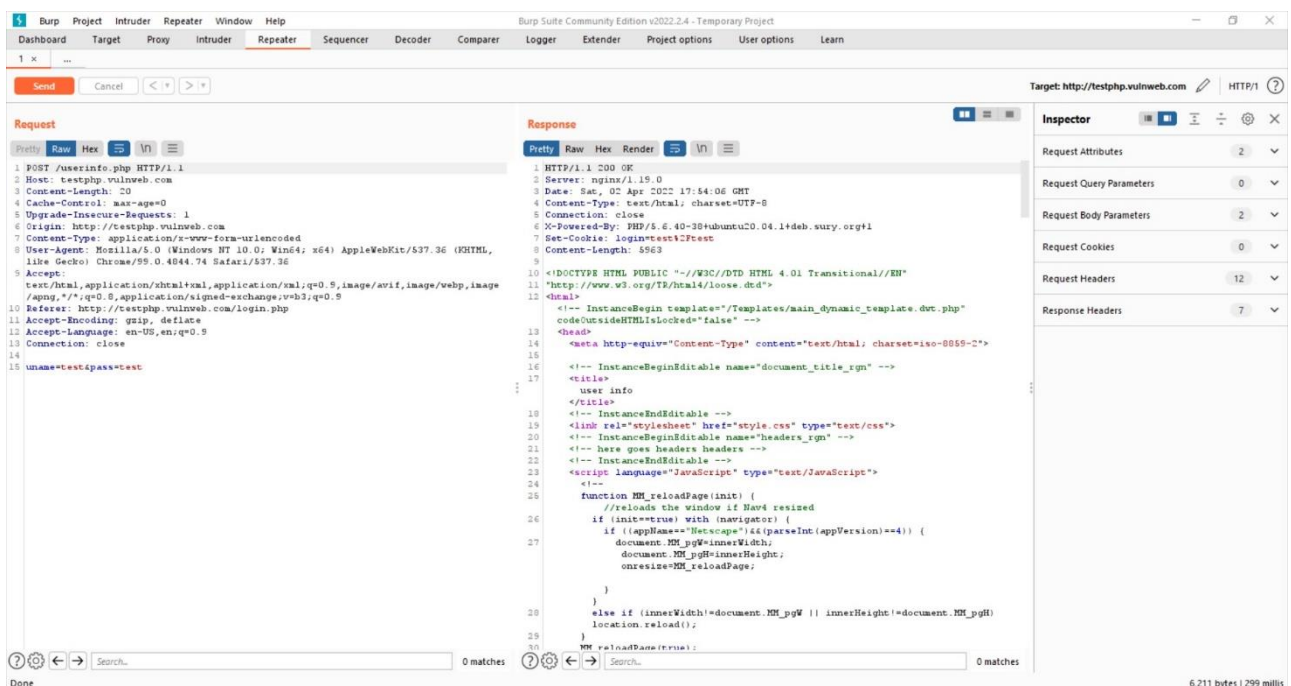
search art go

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer

About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

Warning This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.



Burp Suite Community Edition v2022.2.4 - Temporary Project

Dashboard | Target | Proxy | Intruder | Repeater | Sequencer | Decoder | Comparer | Logger | Extender | Project options | User options | Learn

Send Cancel < >

Target: http://testphp.vulnweb.com HTTP/1

Request

1 POST /userinfo.php HTTP/1.1
2 Host: testphp.vulnweb.com
3 Content-Length: 20
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://testphp.vulnweb.com
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 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=0.5
10 Referer: http://testphp.vulnweb.com/login.php
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.5
13 Connection: close
14
15 username=test&pass=test

Response

1 HTTP/1.1 200 OK
2 Server: nginx/1.19.0
3 Date: Sat, 02 Apr 2022 17:54:06 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
6 X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
7 Set-Cookie: login=test%2Ftest
8 Content-Length: 5563
9
10 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
11 "http://www.w3.org/TR/html4/loose.dtd">
12 <html>
13 <!-- InstanceBeginEditable name="main_dynamic_template.dvt.php" codeOutsideHTMLIsLocked="false" -->
14 <head>
15 <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">
16 <!-- InstanceBeginEditable name="document_title_tgn" -->
17 <title>
18 user info
19 </title>
20 <!-- InstanceEndEditable -->
21 <link rel="stylesheet" href="style.css" type="text/css">
22 <!-- InstanceBeginEditable name="headers_rgn" -->
23 <!-- here goes headers headers -->
24 <!-- InstanceEndEditable -->
25 <script language="JavaScript" type="text/JavaScript">
26 <!--
27 function NM_reloadPage(init) {
28 //reloads the window if Nav4 resized
29 if (init==true) with (navigator) {
30 if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
31 document.NM_pgW=innerWidth;
32 document.NM_pgH=innerHeight;
33 onresize=NH_reloadPage;
34 }
35 }
36 else if (innerWidth!=document.NM_pgW || innerHeight!=document.NM_pgH)
37 location.reload();
38 }
39 NH_reloadPage(true);
40 </script>
41 </head>
42 <body>
43 <!-- InstanceBeginEditable name="body_content" -->
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>
1001 <div>
1002 <div>
1003 <div>
1004 <div>
1005 <div>
1006 <div>
1007 <div>
1008 <div>
1009 <div>
1010 <div>
1011 <div>
1012 <div>
1013 <div>
1014 <div>
1015 <div>
1016 &

Task 3: Brute force.

Send a request to intruder and create 2 different payloads for usernames and passwords. Try cluster bomb attack type to find valid credential for that website.

The screenshot shows the Burp Suite Intruder tab with the 'Payloads' sub-tab selected. The 'Payload Sets' section indicates that you can define one or more payload sets. The configuration is as follows:

- Payload set: 1
- Payload count: 3
- Payload type: Simple list
- Request count: 15

The 'Payload Options [Simple list]' section explains that this payload type lets you configure a simple list of strings that are used as payloads. The list contains the following items:

- admin
- username
- test

Buttons for 'Paste', 'Load ...', 'Remove', 'Clear', and 'Deduplicate' are visible. An 'Add' button with a text input 'Enter a new item' and a dropdown 'Add from list ... [Pro version only]' are also present.

The screenshot shows the Burp Suite Intruder tab with the 'Payloads' sub-tab selected. The 'Payload Sets' section indicates that you can define one or more payload sets. The configuration is as follows:

- Payload set: 2
- Payload count: 5
- Payload type: Simple list
- Request count: 15

The 'Payload Options [Simple list]' section explains that this payload type lets you configure a simple list of strings that are used as payloads. The list contains the following items:

- 123456789
- qwerty
- password
- nopassword
- test

Buttons for 'Paste', 'Load ...', 'Remove', 'Clear', and 'Deduplicate' are visible. An 'Add' button with a text input 'Enter a new item' and a dropdown 'Add from list ... [Pro version only]' are also present.

The screenshot shows the Burp Suite Results tab with the 'Results' sub-tab selected. The table displays the results of the brute force attack, showing the request number, payload 1, payload 2, status, error, timeout, length, and comment.

| Requ... | Payload 1 | Payload 2 | Status | Error | Timeout | Length | Comment |
|---------|-----------|------------|--------|-------|---------|--------|---------|
| 0 | | | 200 | | | 6211 | |
| 1 | admin | 123456789 | 302 | | | 253 | |
| 2 | username | 123456789 | 302 | | | 253 | |
| 3 | test | 123456789 | 302 | | | 253 | |
| 4 | admin | qwerty | 302 | | | 253 | |
| 5 | username | qwerty | 302 | | | 253 | |
| 6 | test | qwerty | 302 | | | 253 | |
| 7 | admin | password | 302 | | | 253 | |
| 8 | username | password | 302 | | | 253 | |
| 9 | test | password | 302 | | | 253 | |
| 10 | admin | nopassword | 302 | | | 253 | |
| 11 | username | nopassword | 302 | | | 253 | |
| 12 | test | nopassword | 302 | | | 253 | |
| 13 | admin | test | 302 | | | 253 | |
| 14 | username | test | 302 | | | 253 | |
| 15 | test | test | 200 | | | 6211 | |