

Lab Objective: To exploit input validation vulnerabilities in a web application (DVWA) to execute arbitrary system commands (Command Injection) and validate the NIDS capability to detect the exfiltration of sensitive system files.

System Setup Details: (Oracle VirtualBox v7.2.6)

Analyst: *SecurityOnion* (IP Address: 192.168.1.50)

Network Adapter 1: Bridged, Network Adapter 2: Internal Network (inet)

Attacker: *Kali* (IP Address: 10.10.10.6)

Network Adapter 1: Internal Network (inet, promiscuous mode: Deny)

Victim: *Metasploitable* (IP Address: 10.10.10.5)

Network Adapter 1: Internal Network (inet, promiscuous mode: Allow All)

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:bb:8c:14
          inet addr:10.10.10.5  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:febb:8c14/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:12 errors:0 dropped:0 overruns:0 frame:0
          TX packets:26 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:768 (768.0 B)  TX bytes:6092 (5.9 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:138 errors:0 dropped:0 overruns:0 frame:0
          TX packets:138 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:42061 (41.0 KB)  TX bytes:42061 (41.0 KB)
```

Target System Configuration (Metasploitable):


- **IP Address:** *10.10.10.5* confirmed via *ifconfig*.
- **Status:** Interface *eth0* is UP and reachable on the internal *10.10.10.0/24* subnet.
- **Role:** This asset hosts intentionally vulnerable services (FTP, HTTP, MySQL) to serve as the target for Red Team operations.

```
(kali㉿kali)-[~]  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 10.10.10.6 netmask 255.255.255.0 broadcast 10.10.10.255  
    inet6 fe80::ea04:4f16:f236:6e1d prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:63:b0:05 txqueuelen 1000 (Ethernet)  
    RX packets 7 bytes 2394 (2.3 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 26 bytes 3008 (2.9 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 8 bytes 480 (480.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 8 bytes 480 (480.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
(kali㉿kali)-[~]  
$ ping -c 4 10.10.10.5  
PING 10.10.10.5 (10.10.10.5) 56(84) bytes of data.  
64 bytes from 10.10.10.5: icmp_seq=1 ttl=64 time=5.23 ms  
64 bytes from 10.10.10.5: icmp_seq=2 ttl=64 time=29.1 ms  
64 bytes from 10.10.10.5: icmp_seq=3 ttl=64 time=0.561 ms  
64 bytes from 10.10.10.5: icmp_seq=4 ttl=64 time=0.531 ms  
  
— 10.10.10.5 ping statistics —  
4 packets transmitted, 4 received, 0% packet loss, time 3033ms  
rtt min/avg/max/mdev = 0.531/8.852/29.091/11.840 ms
```

Attacker Connectivity & Reachability Check:

- **IP Address:** *10.10.10.6* (Static Assignment).
- **Connectivity Test:** Successful ICMP Echo (Ping) requests to the target (*10.10.10.5*) confirm network path availability and low latency (<1ms), verifying the virtual switch configuration.



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

Welcome to Damn Vulnerable Web App!

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

WARNING!

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing [XAMPP](#) onto a local machine inside your LAN which is used solely for testing.

Disclaimer

We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

General Instructions

The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.

Username: admin
Security Level: low

Target Assessment:

- **Target Selection:** Accessed the "Damn Vulnerable Web App" (DVWA) hosted on the victim server (*Metasploitable*) (<http://10.10.10.5/dvwa>) and verified the Security Level was set to "Low" to simulate an application with no input filtering.


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

[Brute Force](#)
[Command Execution](#)

Vulnerability: Command Execution

Ping for FREE

Enter an IP address below:



[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:

```

PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.041 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.038 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.046 ms

--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.038/0.041/0.046/0.008 ms
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh

```

Payload Injection:

- Vulnerability Identification:** The "Command Execution" tool takes user input (an IP address) and passes it directly to the system shell without sanitization.
- Payload Execution:** Injected the malicious command `127.0.0.1; cat /etc/passwd`. The semicolon (;) acts as a command separator, allowing the attacker to chain a second command (`cat`) to read the system's master user file.
- Result:** The application displayed the contents of `/etc/passwd` (visible in the screenshot as `root:x:0:0...`), confirming successful Remote Code Execution (RCE).

3

ET ATTACK_RESPONSE Possible /etc/passwd via HTTP (linux style)

suricata

medium

2002034

ALERT DETAILS

GUIDED ANALYSIS

timestamp	2026-02-18T01:48:16.411Z
data_stream.dataset	suricata
data_stream.namespace	so
data_stream.type	logs
destination.ip	10.10.10.6
destination.port	52462
dns.query.name	root[3a]x[3a]0[3a]0[3a]root[3a]root[3a]/
ecs.version	8.0.0
elastic_agent.id	648238bc-3c1f-4b10-85ed-96ec3e362862
elastic_agent.snapshot	false
elastic_agent.version	8.18.8
event.category	network
event.dataset	suricata.alert
event.ingested	2026-02-18T01:48:16.573Z
event.module	suricata
event.severity	2
event.severity_label	medium
input.type	log
log.file.path	/ism/suricata/eve-2026-02-18-01:14.json
log.id.uid	655385157299968
log.offset	18680
message	["timestamp":"2026-02-18T01:48:16.411622+0000","flow_id":655385157299968,"in_iface":"bond0","event_type":"alert","src_ip":"10.10.10.5","src_port":80,"dest_ip":"10.10.10.6","dest_port":52462,"proto":"TCP","ip_v4":{"pkts_src":{"wire pcap"},"metadata":{"flowbits":{"http.dottedquadhost"},"community_id":"135ae02yG108W89okJnCQT2dkn","tx_id":0,"alert":{"action":"allowed","gid":1,"signature_id":2002034,"rev":13,"signature":"ET ATTACK_RESPONSE Possible /etc/passwd via HTTP (linux style)","category":"Information Leak"},"severity":2,"metadata":{"confidence":"Medium","created_at":{"2010_07_30"},"signature_severity":"Unknown"},"updated_at":{"2024_03_12"},"rule":{"alert http \$HOME_NET any -> \$EXTERNAL_NET any (msg:"ET ATTACK_RESPONSE Possible /etc/passwd via HTTP (linux style)"; flow:established,to_client; file.data; content:"root[3a]x[3a]0[3a]0[3a]root[3a]root[3a]"; nocase; classtype:successful-recon-limited; sid:2002034; rev:13; metadata:created_at 2010_07_30; confidence Medium; signature_severity Unknown; updated_at 2024_03_13;"},"files":{"filename":"/dev/vulnerabilities/exec"},"gaps":false,"state":"CLOSED","stored":false,"size":6291,"tx_id":0},"app_prot":"http","direction":"to_client","sourceip nottable":"HTTP/1.1 200 OK","date Wed 18 Feb 2026 01:29:26 GMT","inServer Apache/2.2.8.1 (Ubuntu) DAV/2/Unix-Proprietary-Rv

Overview

ET ATTACK_RESPONSE Possible /etc/passwd via HTTP (linux style)

Summary

This rule detects the transmission of a file over HTTP containing the structure of a Linux-style /etc/passwd file, which is indicative of a potential attack response exposing sensitive system information. It specifically looks for patterns in data returned to a client that match the format of entries in the /etc/passwd file, starting with the "root" user entry.

Status: Enabled

+

Enabled	Type	Track/Regex	IPVar	Created
No data available				

Data Exfiltration Detection (NIDS):

- Alert Identification:** The Security Onion sensor triggered a specific alert: *ET ATTACK_RESPONSE Possible /etc/passwd via HTTP*.
- Traffic Analysis:** The alert flagged traffic originating from the Victim (10.10.10.5) and destined for the Attacker (10.10.10.6).
- Forensic Significance:** The "ATTACK_RESPONSE" category is critical here. It indicates that the NIDS didn't just see an attack attempt; it inspected the data leaving the server and confirmed that the sensitive file (*/etc/passwd*) was actually successfully transmitted back to the attacker.