### **Урок 5. Security misconfiguration**

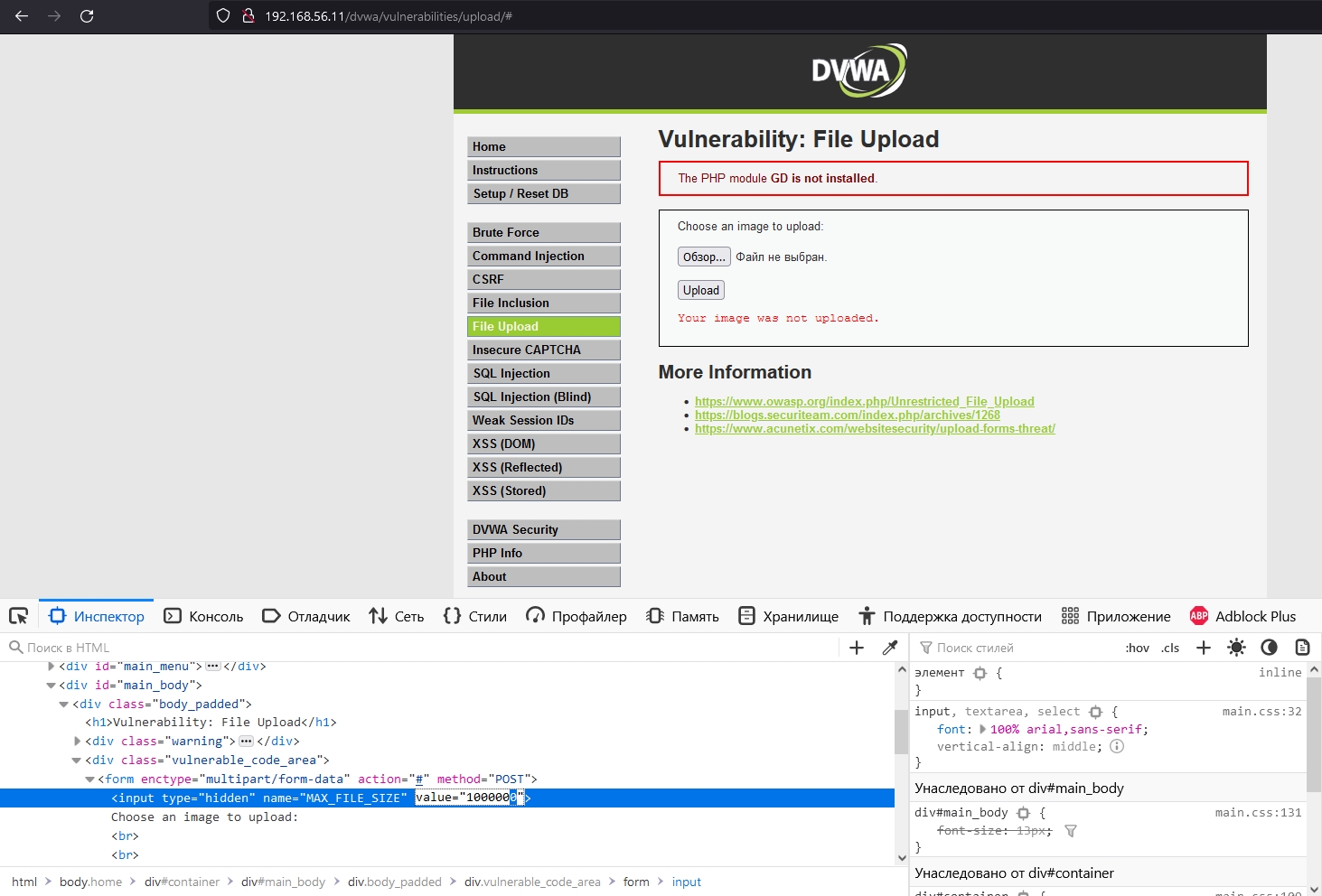
Задание 1:

Решите задание File Upload из проекта DVWA на уровне сложности Low так, чтобы получить шелл на исследуемом ресурсе.

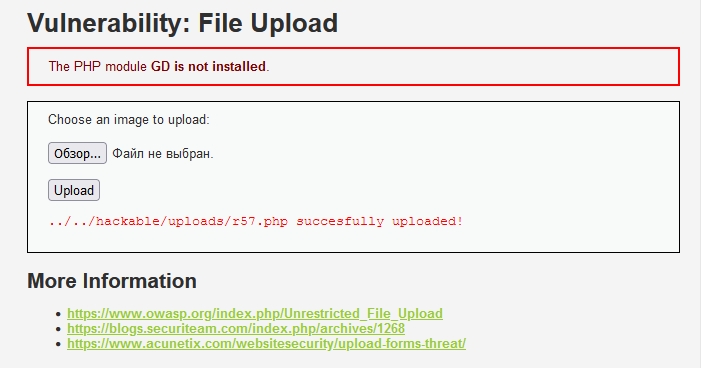
Решение:

Первое, что я сделал, - попробовал просто загрузить шелл r57.php. Не получилось.

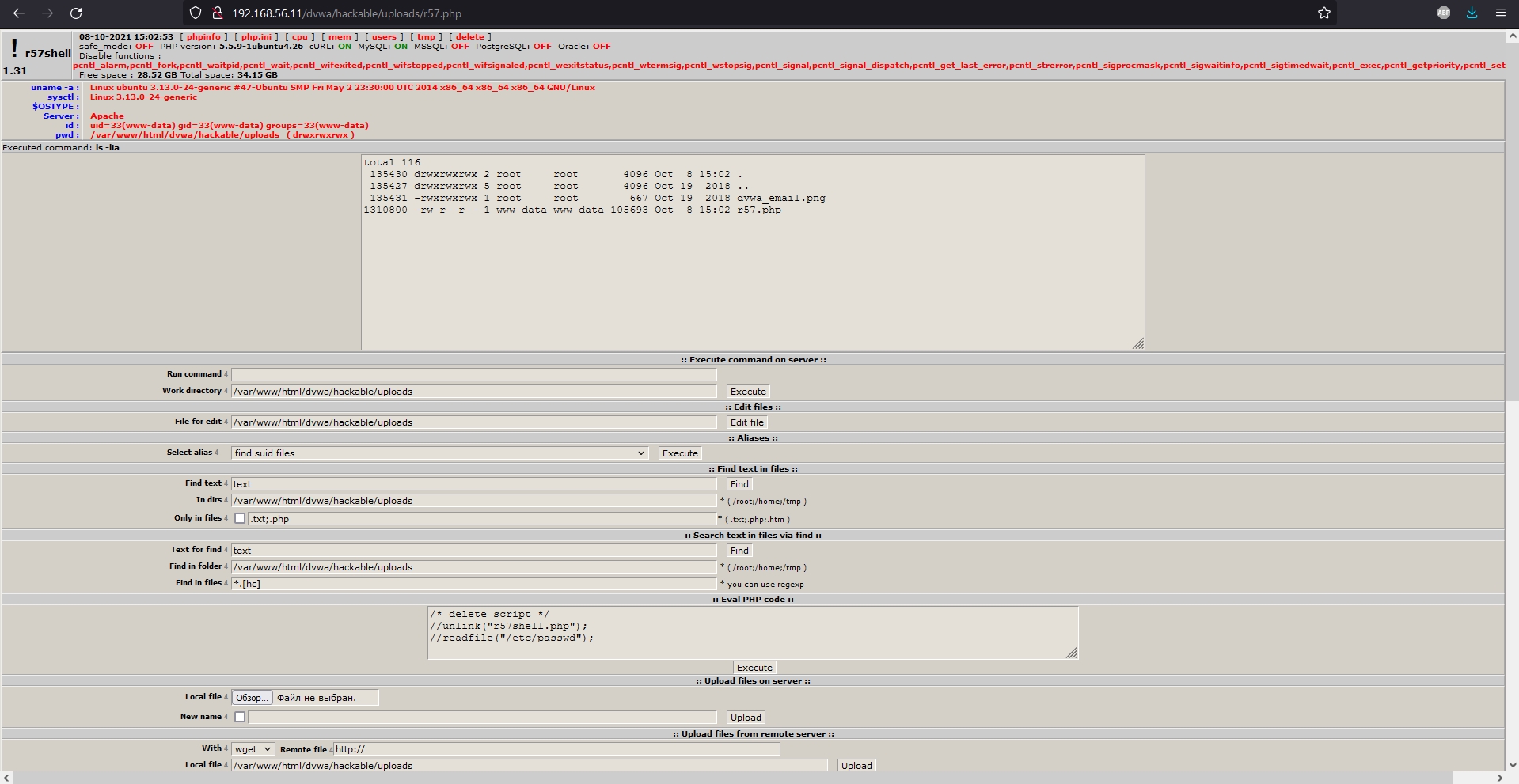
Второе — посмотрел в инструментах разработчика код и увидел ограничение по размеру загружаемого файла. Добавил нолик.



Повторил попытку загрузить шелл и получилось!



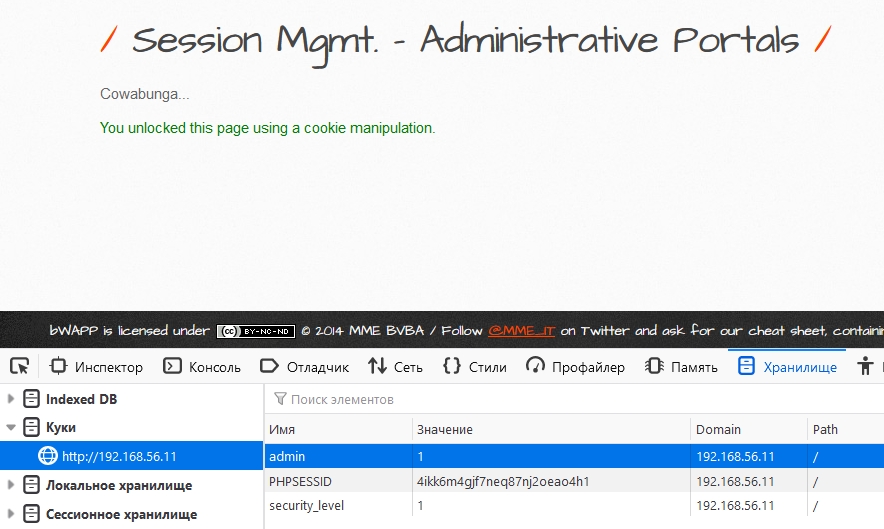
А вот и сам шелл:



Задание 2:  
 Решите задание “Session Mgmt. - Administrative Portals” из bwapp на уровне сложности medium.

Решение:

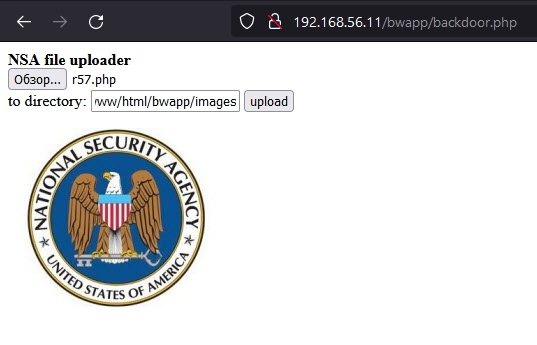
В подсказке, которую сложно было не заметить, написано «check the cookie», что я и сделал… Заменил в поле admin значение с 0 на 1 и обновил страницу.



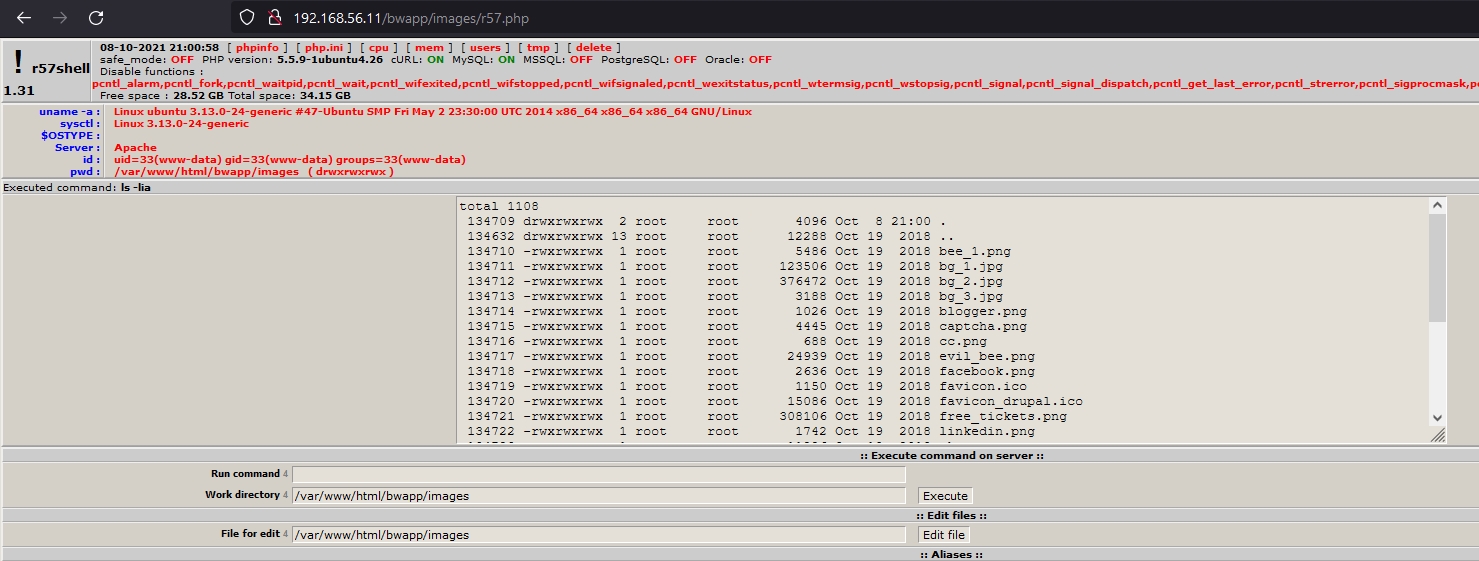
Задание 3:  
 Исследуйте страницу «Old, Backup & Unreferenced Files» проекта bwapp на наличие уязвимостей. Может ли злоумышленник использовать найденные уязвимости для проникновения на сервер? Ответ обоснуйте.

Решение:

Может. Если перейти на страницу backdoor.php, поправить путь, куда будет сохраняться загружаемый файл, то появляется возможность загружать любой файл на сервер:



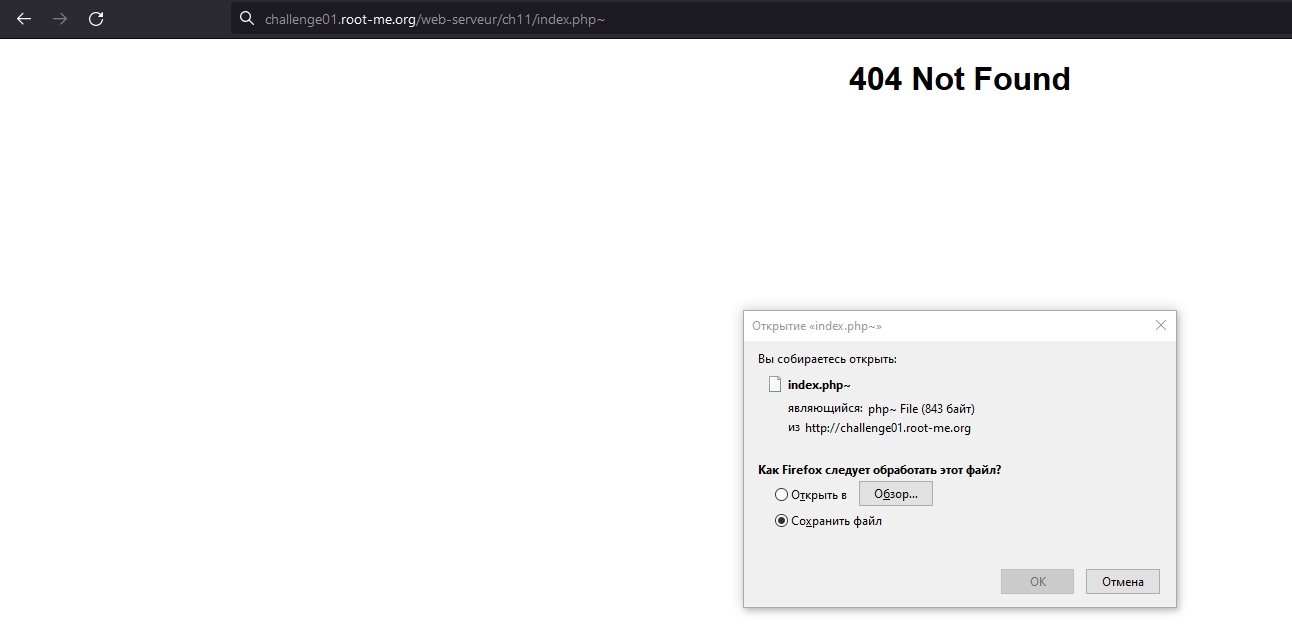
И вот результат:

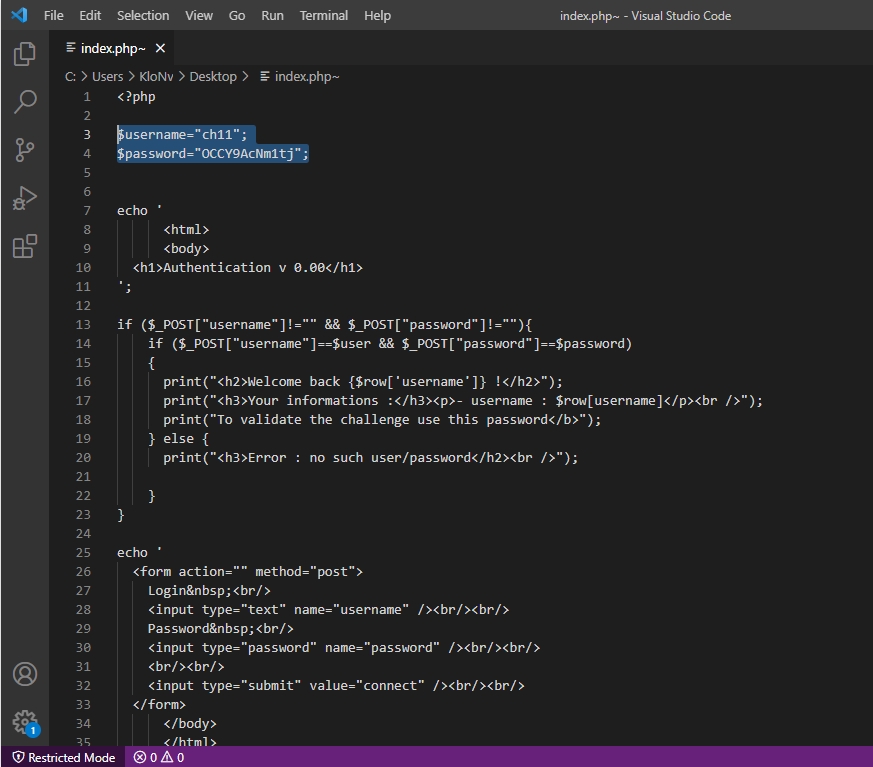
Через такой шелл уже можно управлять сервером.

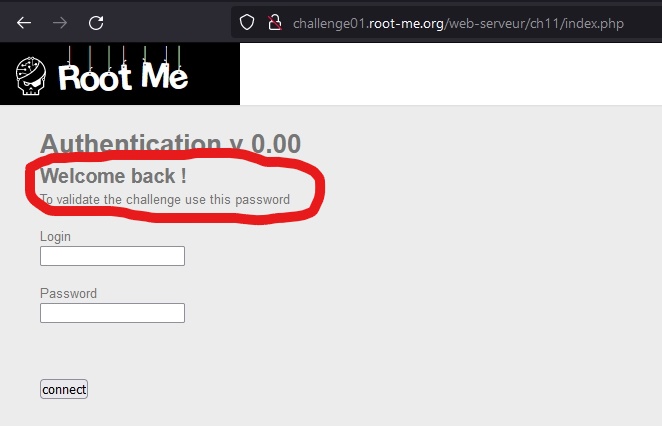
Задание 4:  
 \* Решите задание https://www.root-me.org/en/Challenges/Web-Server/Backup-file.

Решение:

Решил задание даже без брута. Перебрал несколько вариантов расширений бекапа индексного файла и угадал. Дописал в конце тильду и скачал бекап.

В нём уже была информация о логине и пароле:





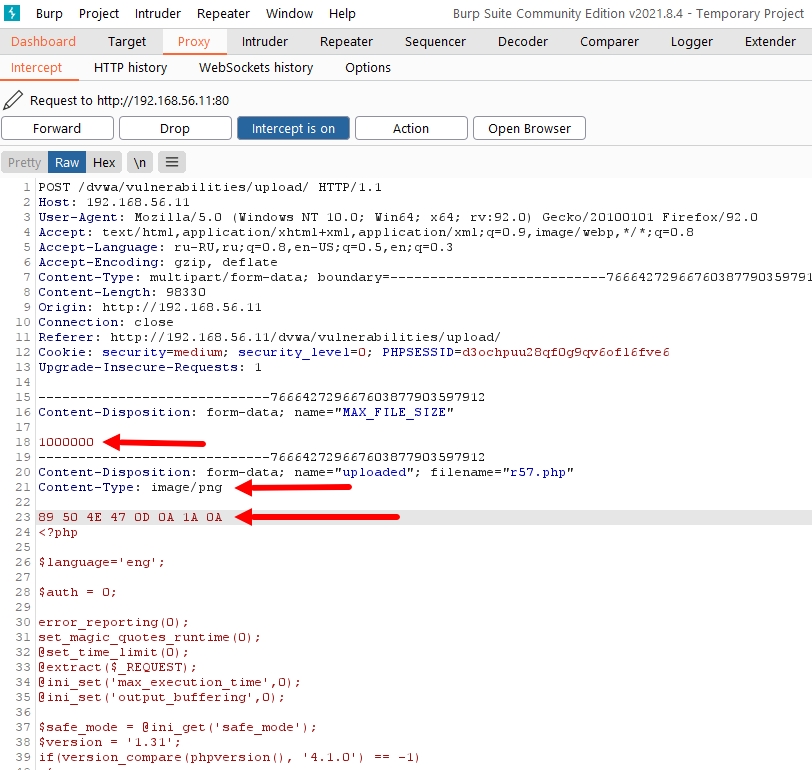
Задание 5:  
 \* Решите задание File Upload из проекта DVWA на уровне сложности Medium так, чтобы получить шелл на исследуемом ресурсе.

Решение:

Загрузил файл, в скрытом инпуте изменил максимальный размер загружаемого файла, отправил, перехватил запрос и отредактировал следующие поля:

MAX\_FILE\_SIZE и так уже был мной изменён ранее  
 Content-Type на image/png

и добавил magic byte от png



После данных манипуляций я смог отправить запрос дальше и загрузить файл:

