Описание уязвимости

В каталоге uploads домена http://192.168.56.11 выявлен разрешенный http метод PUT. Данная уязвимость позволяет загружать на сервер несанкционированные файлы, которые могут повлиять на конфиденциальность и целостность информационной системы.

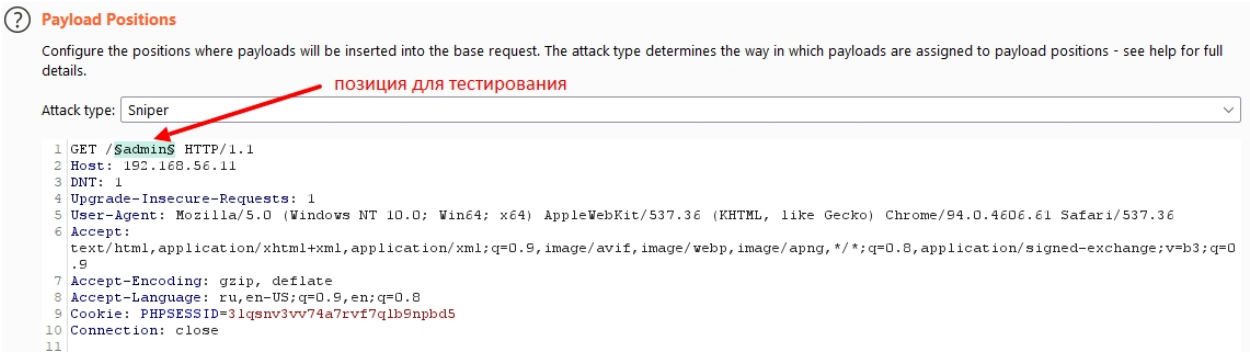
Где найдена уязвимость

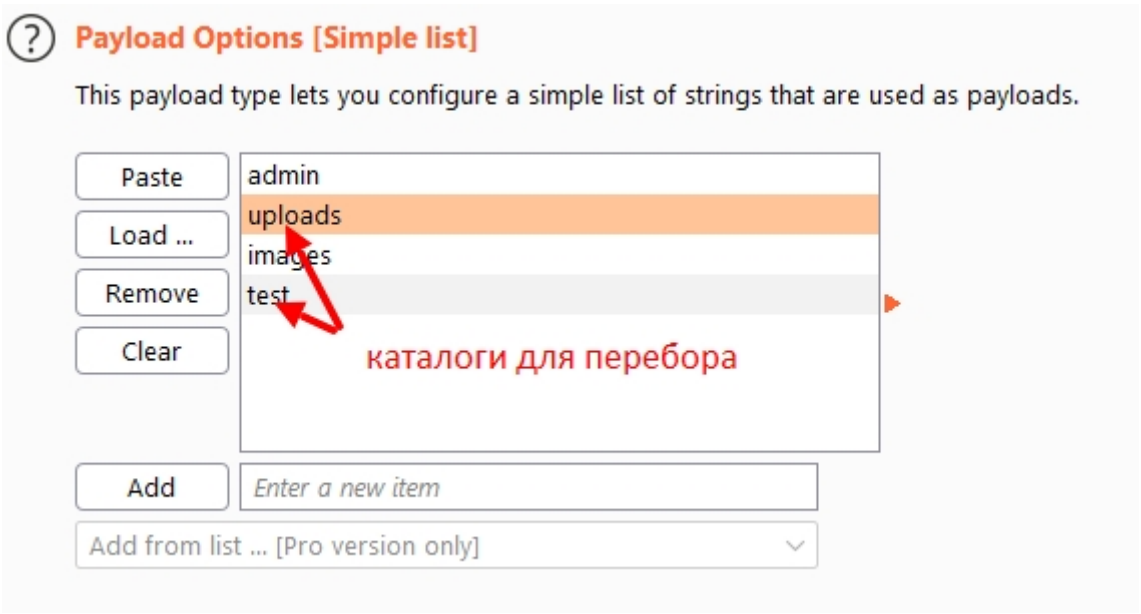
Уязвимость расположена по адресу http://192.168.56.11/uploads/.

Наименование продукта: Metasploitable 3 Linux virtual machine.

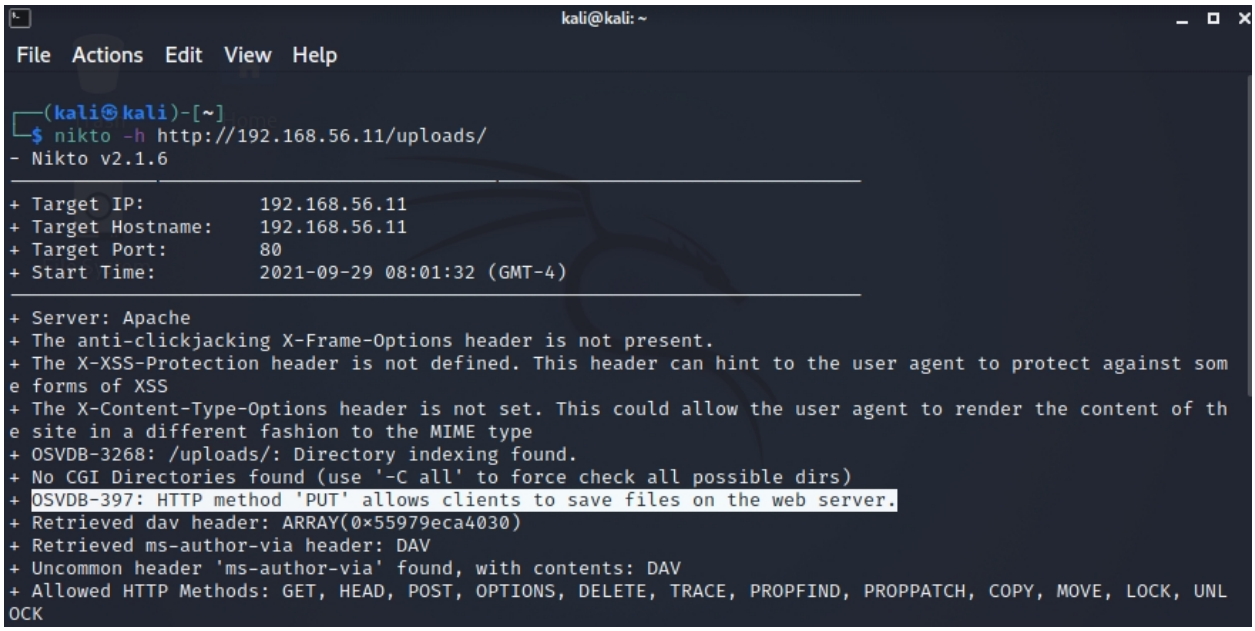
Технические детали обнаружения и воспроизведения

Найти уязвимый каталог удалось, перебрав наиболее часто используемые каталоги в Burp Suite CE >> Intruder:





Обнаружить уязвимость в каталоге uploads удалось, проанализировав его утилитой nikto, специализирующейся на поиске веб уязвимостей.



Эксплуатировать уязвимость возможно следующей командой:

curl -I -X PUT -T phpshellmetasploit.php http://192.168.56.11:80/uploads/shell21.php

Данная команда создаст файл shell21.php в уязвимой директории сервера и загрузит в него содержимое файла *phpshellmetasploit.php*.

В дальнейшем к этому файлу можно будет обратиться по адресу http://192.168.56.11/uploads/shell21.php, тем самым запустив его исполнение.

Выводы и рекомендации по устранению

Уязвимость позволяет получить контроль сервера и доступ к конфиденциальной информации. Не требует дополнительных уязвимостей для эксплуатации. Рекомендации по устранению:

- Запретить метод PUT для каталога uploads в конфигурации apache.

Используемое программное обеспечение

- Burp suite CE
- Google Chrome
- Kali Linux VM