
Практическое задание № 03. Уязвимость в Apache (CVE-2021-41773)

Опубликовано 25.10.2022

Дедлайн 08.11.2022

Задание:

Для выполнения задания необходима система с Linux.

1. Загрузить исходный код уязвимой версии (2.4.49) веб-сервера Apache по ссылке:
<https://archive.apache.org/dist/httpd/>

2. Откомпилировать и установить сервер на систему с помощью команд:

```
./configure  
make  
[sudo] make install
```

Замечание: может потребоваться установка зависимостей: `libapr` и `libapr-util`.

3. Включить модуль `mod_cgid` в файле конфигурации `httpd.conf`.
4. Запустить сервер с помощью команды.

```
[sudo] /usr/local/apache2/bin/apachectl -k start
```

Замечание: на вашей системе вместо `"/usr/local/apache2/bin/"` может быть другой путь.

5. При успешном запуске должна открываться ссылка в браузере:
`http://[machine_ip_address]/`
6. Используя общедоступные эксплойты, получить с другой машины удалённый доступ к машине с сервером (повесить бэкдор на одном из портов).

Ссылки:

1. <https://xakep.ru/2021/10/05/apache-path-traversal/>
2. <https://twitter.com/hackerfantastic/status/1445523524555186189>
3. <https://xakep.ru/2021/10/07/apache-rce/>

