Министерство образования Республики Беларусь

Учреждение образования

“Брестский государственный технический университет”

Кафедра интеллектуально-информационных технологий

Лабораторная работа №2

По дисциплине: «Современные средства вычислительной техники»

Выполнил:

студент 3 курса

группы ИИ-21

Романко Н.А.

Проверил:

Соловчук А. М.

Брест 2024

Цель работы: пройти машину на сайте HackTheBox

Для данной работы выбрал машину «TwoMillion» с IP-адресом: 10.10.11.221

Для того чтобы убедится что мы подключены к машине, выполним команду ping: Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Мы подключены, теперь просканируем этот IP при помощи nmap:

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Видно что есть два открытых порта: 22 shh и 80 http

Перейдем по нашему ip и увилим такой сайт:

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

На сайте есть окно «Invite» можно заметить что он обращается к «inviteapi.min.js»

Изображение выглядит как текст, снимок экрана, программное обеспечение, Значок на компьютере

Автоматически созданное описание

В нем содержится данный код:  
eval(

function (p, a, c, k, e, d) {

e = function (c) {

return c.toString(36)

};

if (!''.replace(/^/, String)) {

while (c--) {

d[c.toString(a)] = k[c] ||

c.toString(a)

}

k = [

function (e) {

return d[e]

}

];

e = function () {

return '\\w+'

};

c = 1

};

while (c--) {

if (k[c]) {

p = p.replace(new RegExp('\\b' + e(c) + '\\b', 'g'), k[c])

}

}

return p

}(

'1 i(4){h 8={"4":4};$.9({a:"7",5:"6",g:8,b:\'/d/e/n\',c:1(0){3.2(0)},f:1(0){3.2(0)}})}1 j(){$.9({a:"7",5:"6",b:\'/d/e/k/l/m\',c:1(0){3.2(0)},f:1(0){3.2(0)}})}',

24,

24,

'response|function|log|console|code|dataType|json|POST|formData|ajax|type|url|success|api/v1|invite|error|data|var|verifyInviteCode|makeInviteCode|how|to|generate|verify'.split('|'),

0,

{

}

)

)

Если упростить данный код, то можно найти обращение к «/api/v1/invite/how/to/generate», сделаем запрос к этому адрессу: Изображение выглядит как текст, снимок экрана, Шрифт, программное обеспечение

Автоматически созданное описание

Видно что вид шифрования ROT13 что является шифром Цезаря. После расшифровки текста в data получаем данный текст «In order to generate the invite code, make a POST request to /api/v1/invite/generate»

Сделаем запрос к этому адресу: Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Видим опять зашифрованный текст, внешне он похож на кодировку Base64, попробуем расшифровать. В итоге получили текст «FKNT3-1RFKR-4E489-4MDT4», скорее всего это и есть код приглашения

После ввода нас перевело на страницу регистрации Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

Попробуем зарегистрироваться пустыми данными и введем эти же данные при входе

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

Смогли войти на сайт

Попробуем обратиться к api сайта при помощи нашего cookie(его получим при нажатии на кнопку connection pack на странице Access)

Изображение выглядит как текст, снимок экрана, программное обеспечение

Автоматически созданное описание

Теперь сделаем тоже самое, но с /api/v1 для нахождения конечной точки

Получаем такой список

Изображение выглядит как текст, снимок экрана

Автоматически созданное описание

При попытке обратится по адресу «http://2million.htb/api/v1/admin/settings/update», получаем ошибку о неверном типе данных:  
Изображение выглядит как текст, снимок экрана, программное обеспечение

Автоматически созданное описание  
это произошло изза того что api работает с форматом JSON, модифицируем запрос с дополнительными данными:

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

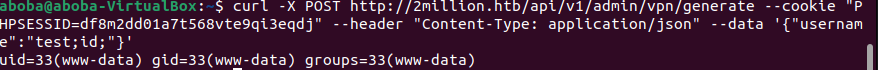
В итоге мы получили доступ администратора к сайту

Теперь обратимся к «http://2million.htb/api/v1/admin/vpn/generate» тк у нас есть доступ администратора

curl -X POST http://2million.htb/api/v1/admin/vpn/generate --cookie "PHPSESSID=df8m2dd01a7t568vte9qi3eqdj" --header "Content-Type: application/json" --data '{"username":"test"}'

Данный код будет генерировать большое количество данных которые используются для VPN

Попробуем получить доступ к получению удаленного доступа:



Команда успешно выполнена

В итоге мы через уязвимость можем обращаться к данным сайта, например к БД такой коммандой «curl -X POST http://2million.htb/api/v1/admin/vpn/generate --cookie "PHPSESSID=df8m2dd01a7t568vte9qi3eqdj" --header "Content-Type: application/json" --data '{"username":"test; cat Database.php #"}'»

Подключимся к БД с полученными данными:

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Теперь мы находимся в базе данных как администратор

При просмотре файлов находим user-flag: Изображение выглядит как текст, Шрифт, снимок экрана

Автоматически созданное описание

Флаг верный

Также нам «пришел» email, прочитаем его и увилим данное содержание:  
Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

В письме упоминается уязвимость ядра, посотрим на версию ядра и узнаем что это «5.15.70-051570-generic». У данной версии есть уязвимость «CVE-2023–0386» которая позволяет обычным пользователям выполнять root команды.

Можно найти данную уязвимость на гитхабе, воспользуемся ею

Изображение выглядит как текст, снимок экрана, число, программное обеспечение

Автоматически созданное описание

Скинем данный эксплоит на сервер распакуем и запустим его

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Мы получили root доступ и тут есть файл root.txt

В нем и содержится ключ

Машина успешно взломана

Изображение выглядит как текст, снимок экрана, дизайн

Автоматически созданное описание

Вывод: научился взламывать машины на сайте HackTheBox