Выполнил студент группы 2345 Романенко Кирилл

Как составить отличный отчёт о найденной уязвимости:

https://habr.com/ru/company/vyshtech/blog/352078/

1. Составьте отчет об уязвимости, которая рассмотрена в примере 1 и позволяет залить шелл на удаленный сервер.

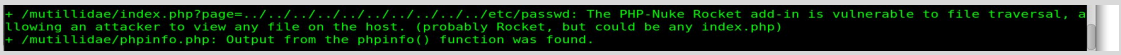
На сайте http://192.168.56.11/mutillidae разрешено индексирование каталогов. Это позволяет получать доступ к информации, хранящейся в каталогах на сервере.

Где найдена уязвимость

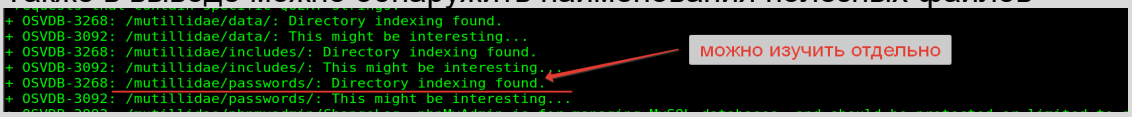
Уязвимость расположена по адресу http://192.168.56.11/mutillidae.
Наименование продукта: Metasploitable 3 Linux virtual machine.

Технические детали обнаружения и воспроизведения

Уязвимость можно обнаружить, просканировав ресурс http://192.168.56.11/mutillidae. Вывод **nikto -h:**



Также в выводе можно обнаружить наименования полезных файлов



Выводы и рекомендации по устранению

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

- Запретить просмотр каталогов в веб-сервере.

Используемое программное обеспечение

- Сканер nikto.

2. Составьте отчет об уязвимости, рассмотренной в одном из примеров предыдущего урока.

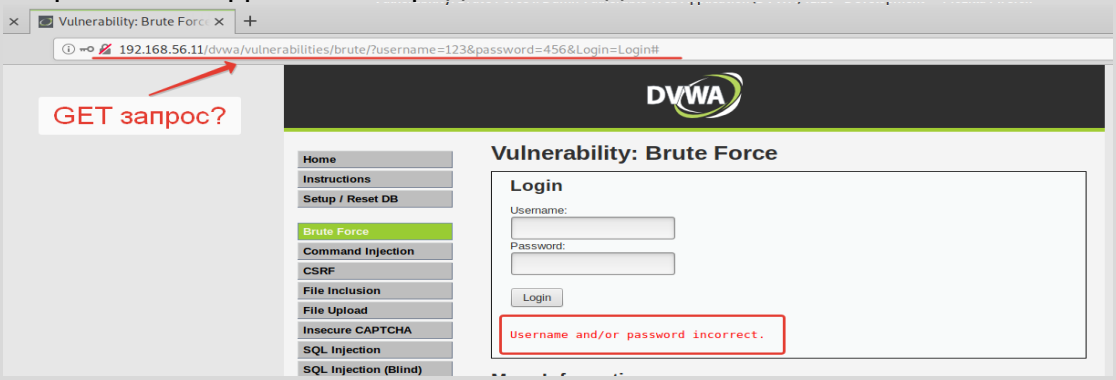
На сайте http://192.168.56.103/mutillidae/index.php?page=login.php неограничено число попыток ввода логина и пароля. Это позволяет подобрать сочетание логин/пароль к большинству учётных записей, в том числе администратора, и войти в систему.

Где найдена уязвимость

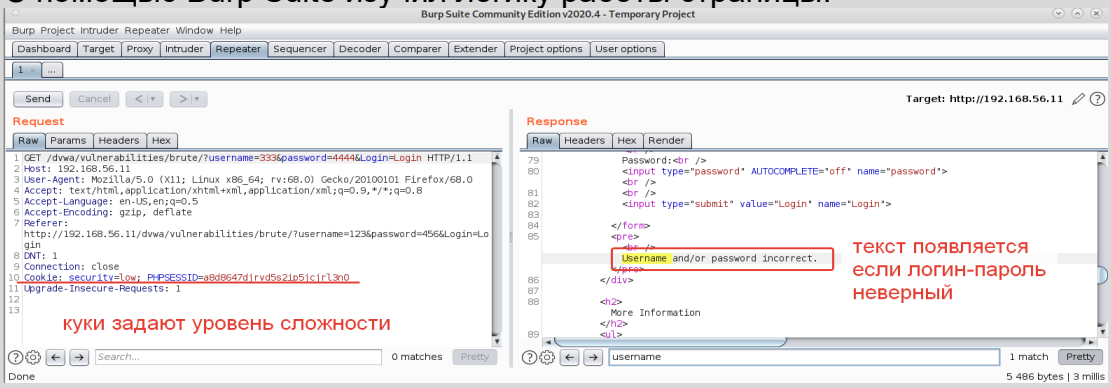
Уязвимость расположена по адресу http://192.168.56.11/dvwa/vulnerabilities/brute.
Наименование продукта: DVWA brute

Технические детали обнаружения и воспроизведения

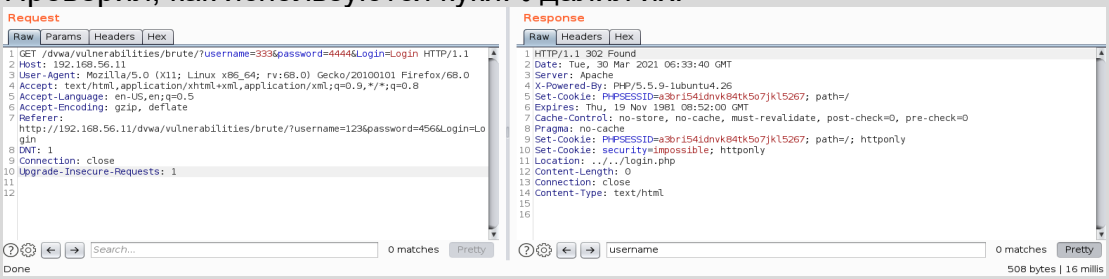
Уязвимость можно обнаружить, введя пару логин/пароль. Вывод окна отличается, если логин валиден.
Также видно, что для передачи данных используется, скорее всего, GET-запрос без шифрования передаваемых данных.



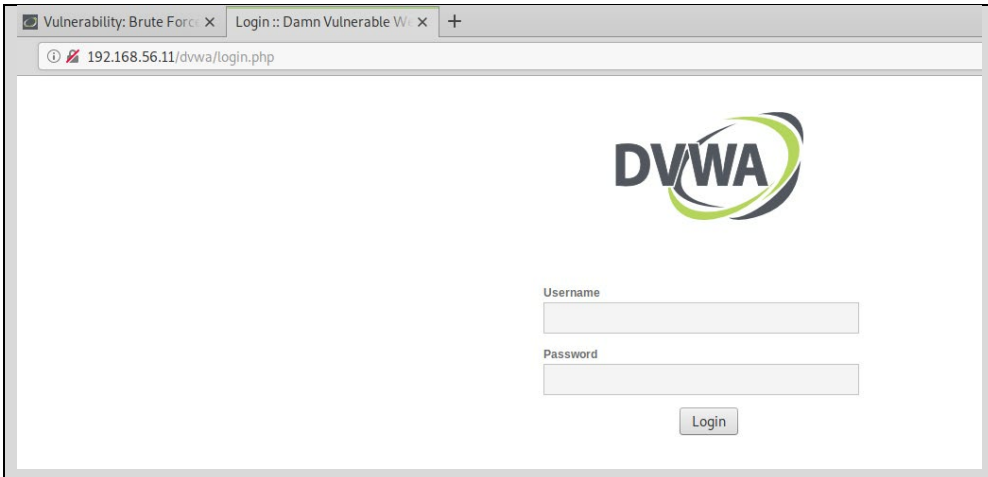
С помощью Burp Suite изучил логику работы страницы:



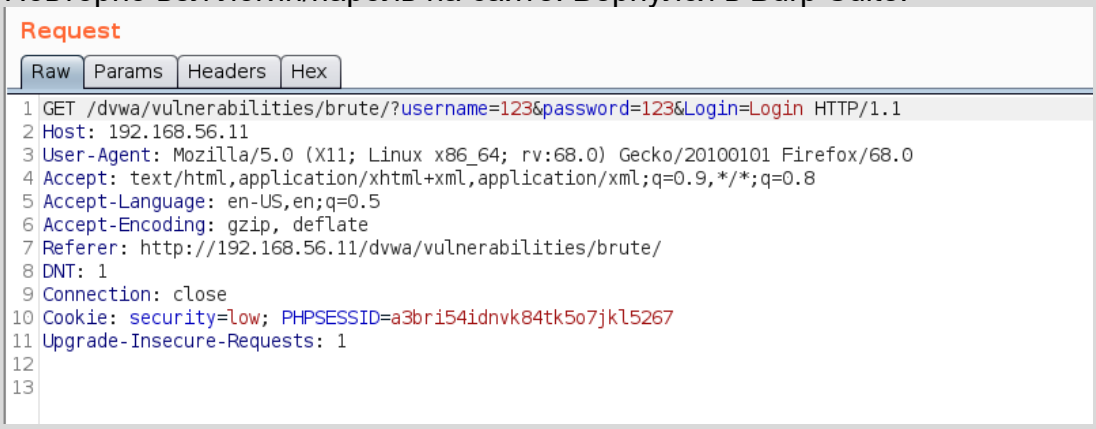
Проверил, как используются куки. Удалил их:



Сработал редирект (кож ответа – 302) и назначается новые куки. Перекинуло на новую страницу аутентификации



Повторно вёл логин/пароль на сайте. Вернулся в Burp Suite.



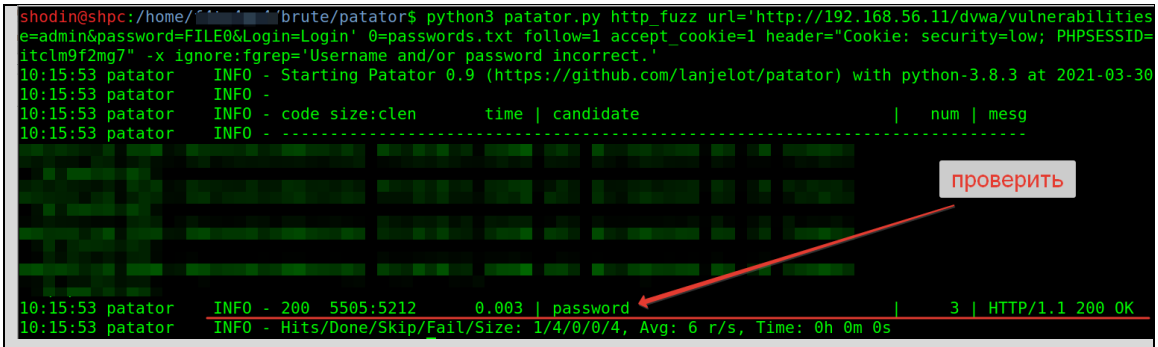
Значение параметра PHPSESSID изменилось. Куки используются при аутентификации и влияют на выполнение запроса (без нее запрос не пройдет).

Выполнил атаку bruteforce с помощью утилиты patator
Исходные данные: - Это GET запрос.
- Целевые параметры – username и password.
- Без кук запрос не сработает.

Запрос:

python3 patator.py http_fuzz url='http://192.168.56.11/dvwa/vulnerabilities/brute/?username=admin&password=FILE0&Login=Login' 0=passwords.txt follow=1 accept_cookie=1 header="Cookie: security=low; PHPSESSID=2c8ee3c3ulltd2ditclm9f2mg7" -x ignore:fgrep='Username and/or password incorrect.'

Результат:



Выводы и рекомендации по устранению

Уязвимость позволяет выполнить подбор логина/пароля для любой учётной записи. В итоге, получим доступ к конфиденциальной информации. Не требует дополнительных уязвимостей для эксплуатации. Рекомендации по устранению:

- Использовать шифрование при передаче логина/пароля на сервер,
- Удалить различие ответа сервера при неудачной аутентификации между неверный «логин и пароль» и неверный «пароль»,
- Установить ограничение на кол-во попыток в кол-ве 5 штук,
- Добавить двухфакторную аутентификацию.

Используемое программное обеспечение

- Firefox web browser
- Burp Suite
- Сканер patator

3. * Изучите внимательно пример 3. К раскрытию какой конфиденциальной информации может привести такая атака? Ответ обоснуйте.
4. * Сможет ли злоумышленник найти список пользователей bwapp, используя только сканер nikto? И если «ДА», то позволит ли найденная информация войти в систему? Ответ обоснуйте.