

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

В зависимости от того, где, когда, какими силами во время разработки жизни ресурса проводится исследование, соответственно заданным условиям и будет предоставляться отчет об уязвимости ресурса. За основу, в том числе в методичке, рассмотрена форма исследования на базе M r s t's L ( e u r t y e l e m e t L e y l e). В данном примере подобного рода отчет не будет иметь смысла, т.к. ресурс уже в стадии эксплуатации. Поэтому можно будет воспользоваться любым более-менее адекватным шаблоном для составления подобного рода отчета.

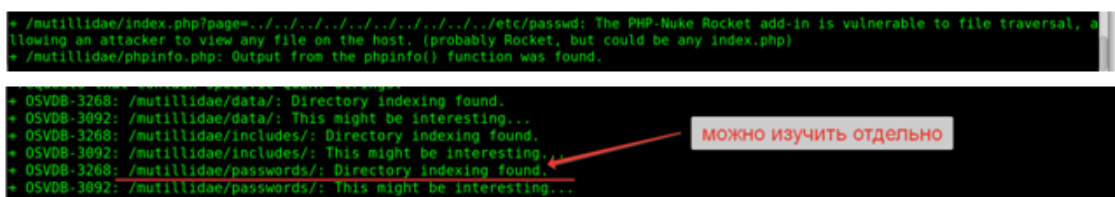
ассматриваемый ресурс:

htt : 1 2.1 . . 11 mut ll dae

спользуемое :

kt (O e u r e ( PL) веб-сервер сканер).

етапи обнаружения и воспроизведения:



```
* /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.

+ 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

1. Path Traversal - уязвимость, позволяющая получить доступ к файлам и директориям сервера за пределами корневой директории сайта. Как же может быть использована с URL-кодированием для обхода безопасности. В данном примере был получен доступ к файлу "passwd" своего рода "открывашка" для данного рода уязвимостей.
2. Файл "httpd.conf" - вся поднастройка сервера, настройки, конфигурации, а если при включенных allow\_url\_fopen и allow\_url\_include - прямое приглашение к LFI RFI уязвимостям.
3. Индексация директорий, в которых возможно хранится информация о паролях на данном ресурсе.

Выводы и рекомендации по устранению уязвимостей:

1. Запрет возможностей уязвимостей Path Traversal, зависит от типа, возможностей сервера, чаще всего достаточно обновления версии сервера для устранения подобной уязвимости.
2. Скрытие, переименование, закрытие доступа к данному файлу. Как минимум это усложнит работу злоумышленнику и даст возможное время для работы BlueTeam.
3. Скрытие, закрытие прямого доступа к файлам, относящимся к чувствительной информации ресурса, хэширование данных. Аналогично, полностью почти не возможно закрыть доступ, но увеличить время для реагирования - предоставит).

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

есурс:

htt : 1 2.1 . .1 3

айденная уязвимость:

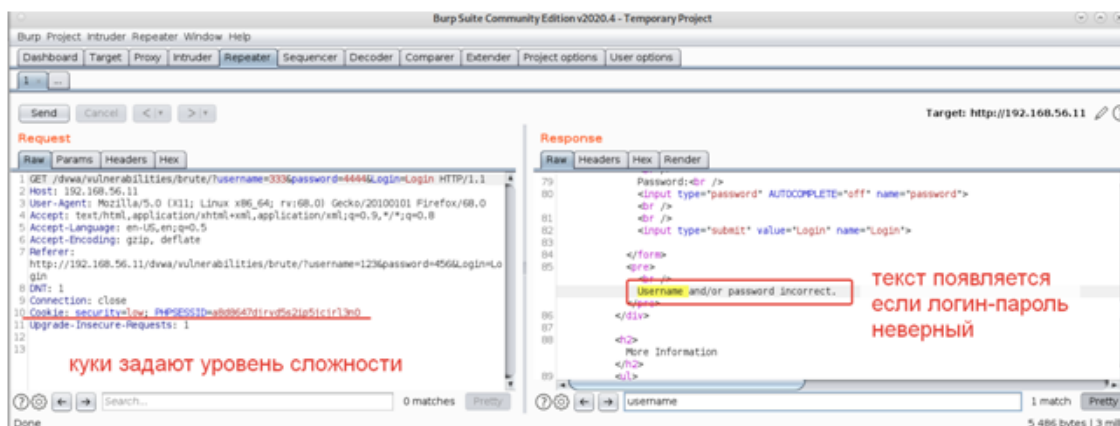
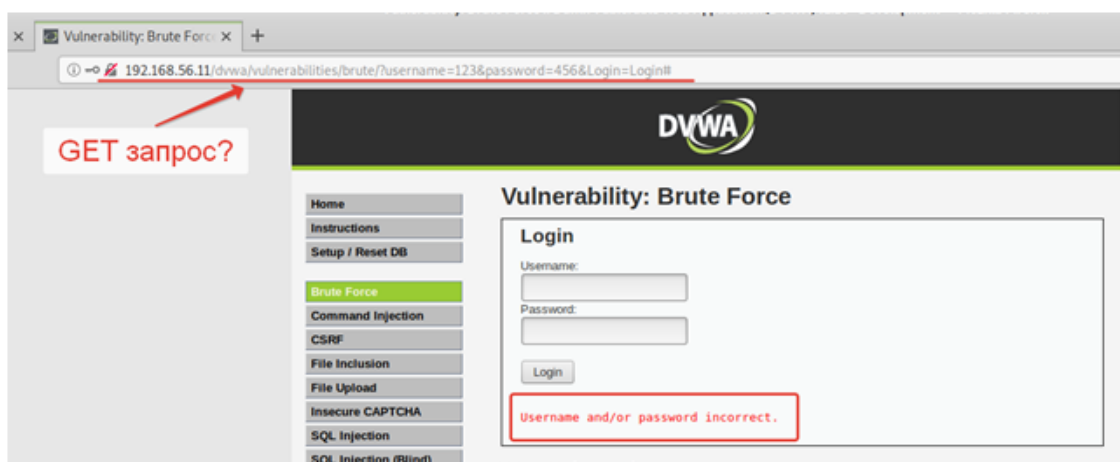
htt : 1 2.1 . .1 3 mut ll dae de . h a e l . h

етали обнаружения и воспроизведения уязвимости:

язвимость обнаружена при вводе пары логин пароль.

твет в зависимости от корректности ввода пары.

ля передачи данных используется Т-запрос без шифрования передаваемых данных.



зучая логику работы ресурса на этапе ввода пары через Burp Suite можно заметить определенное использование cookie.



При удалении cookie и отправке нового запроса - ресурс обрабатывает редиректом (код - 302), назначаются новые cookie для пользователя. Перенаправление на новую страницу аутентификации.

Далее при повторном вводе пары логин/пароль возвращаюсь в Вирр. Можно увидеть, что значение сессионной cookie поменялось. Без данного заголовка выполнение запроса не проходит на прямую.



Далее выполнялись атаки с помощью утилиты patator

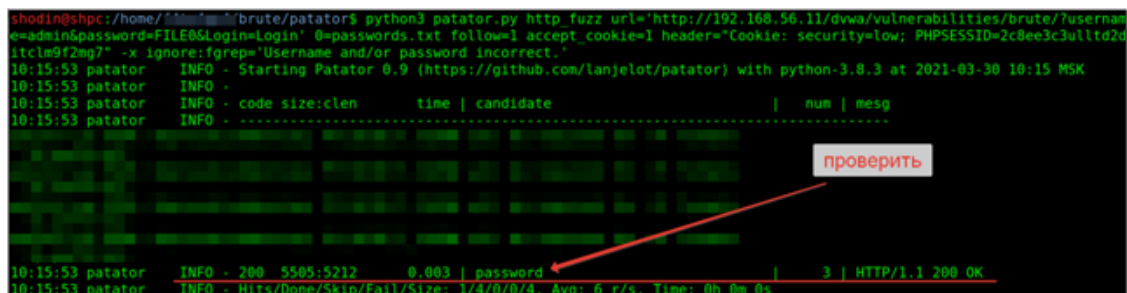
Исходные данные:

- 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:



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

Задания 3, 4 не выполнялись.