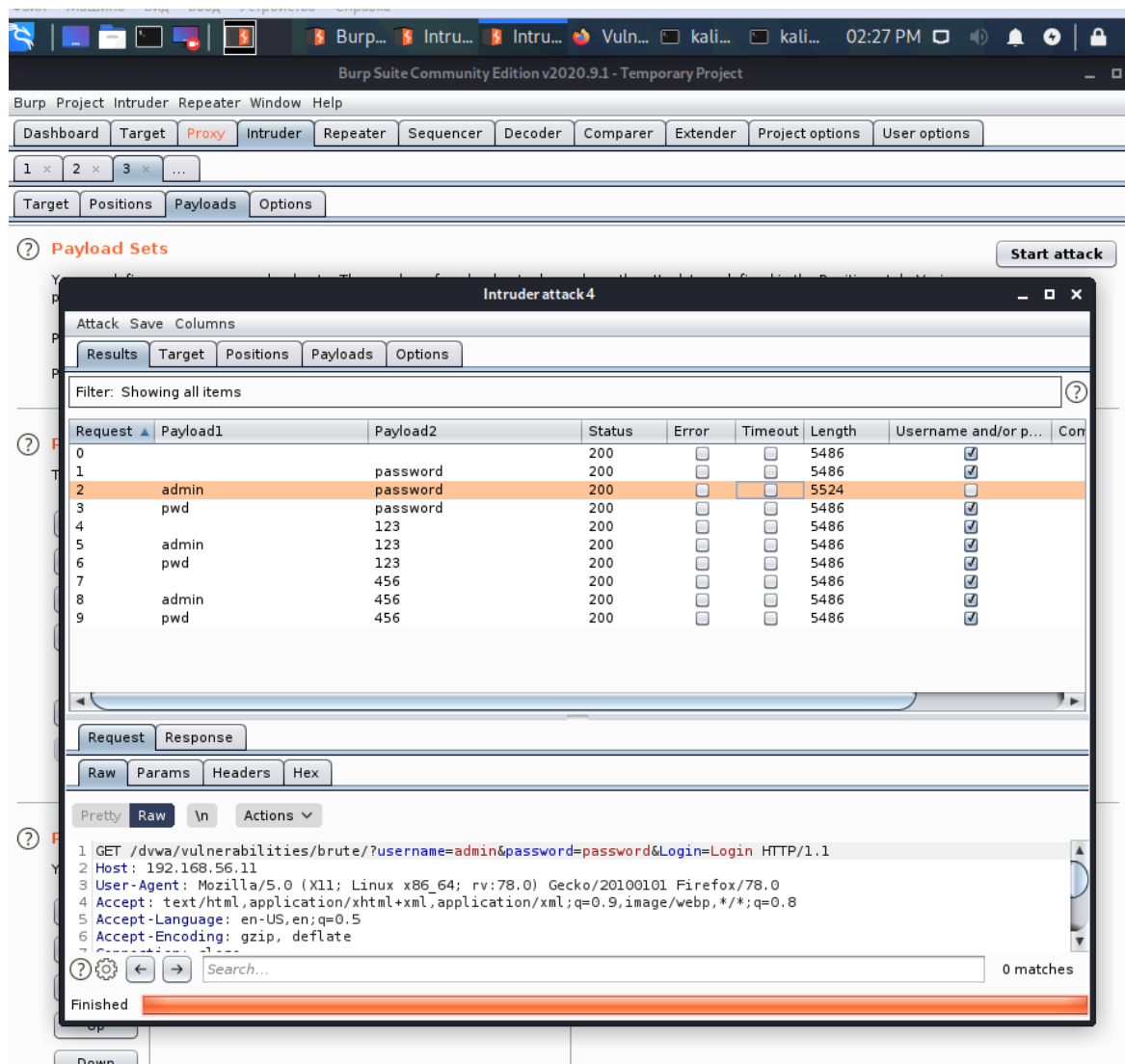


Домашнее задание:

1. Имеется логин `admin` и пароль `у030E#jb`, которые были заданы администратором для входа в систему с использованием веб-формы. Можно ли считать такую комбинацию логина и пароля безопасной для защиты от брутфорса? Ответ обоснуйте.
2. Подберите логин и пароль к странице `bruteforce` сервиса `dvwa` на уровне сложности `LOW`. Приложите к ответу описание решения задания и скриншот(ы), подтверждающие решение.
3. Подберите логин и пароль к странице `Broken Auth.` - `Weak Passwords` сервиса `bwarr` на уровне сложности `LOW`. Приложите к ответу описание решения задания и скриншот(ы), подтверждающие решение.

1. Логин `admin` используется очень часто, поэтому будет вычислен мгновенно (в случае, если на сайте есть признаки, по которым можно определить существование такого логина, а такие признаки есть почти всегда). Пароль содержит специальные символы и разные регистры, соответственно кажется надежным. Итого, чтобы усложнить брутфорсеру задачу следует использовать не такой явный логин, например `4)^\^!/|/`

2. Тут в общем по сути повторение сделанного на вебинаре. Сначала подбираем логин `admin` а потом включаем подбор с условием `Username and/or password incorrect`. Там где такой надписи нет правильное сочетание логин/пароль.



Vulnerability: Brute Force

Login

Username:

Password:

Login

Welcome to the password protected area admin



3. В общем тоже самое но пришлось додуматься до test.

The screenshot shows the Burp Suite interface with the Intruder attack results window open. The window displays a table of attack results for 'Intruder attack 4'. The table has columns: Request, Payload1, Payload2, Status, Error, Timeout, Length, Invalid, and Comment. The results show a successful login for the 'test' payload.

Request	Payload1	Payload2	Status	Error	Timeout	Length	Invalid	Comment
43	root	bug	200			13710		
44	manager	bug	200			13710		
45	bee	bug	200			13710		
46	bug	bug	200			13710		
47	admin	bug	200			13710		
48	test	bug	200			13710		
49	admin	test	200			13710		
50	administrator	test	200			13710		
51	root	test	200			13710		
52	manager	test	200			13710		
53	bee	test	200			13710		
54	bug	test	200			13710		
55	admin	test	200			13710		
56	test	test	200			13709		

/ Broken Auth. - Weak Passwords /

Enter your credentials.

Login:

Password:

Login

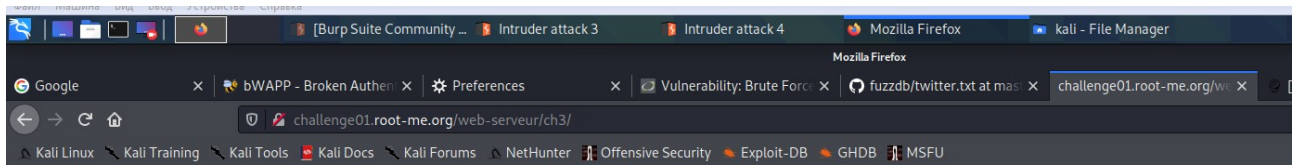
Successful login!

Домашнее задание (повышенная сложность):

1. * Протестируйте пример 3 (с настройкой `mod_evasive`) на практике. Приложите к ответу описание решения задания и скриншот(ы), подтверждающие решение.
2. * Решите задание <http://challenge01.root-me.org/web-serveur/ch3/> методом брутфорса (требуется регистрация на root-me.org). Приложите к ответу описание решения задания и скриншот(ы), подтверждающие решение.

2.

admin – admin



Bien joué, vous pouvez utiliser ce mot de passe pour valider le challenge

Well done, you can use this password to validate the challenge



68 Challenges

Results	Name	Validations	Number of points ?
✖	HTML - Source code	49% 104095	5
✖	HTTP - IP restriction bypass	1% 515	10
✖	HTTP - Open redirect	19% 40016	10
✖	HTTP - User-agent	25% 51815	10
✔	Weak password	33% 70432	10