Индивидуальный проект - этап 5

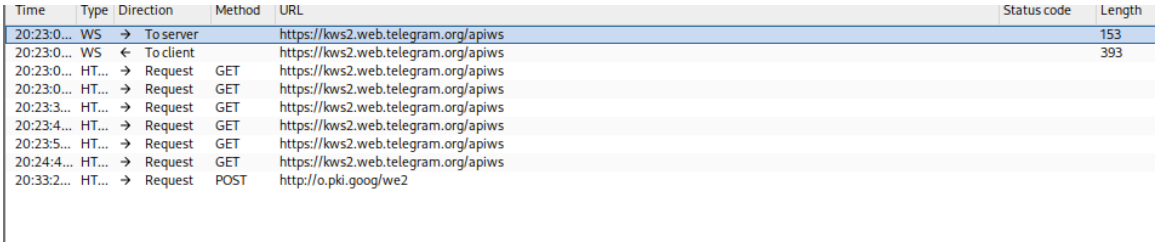
Использование BurpSuite

Овезов Мерген

Содержание

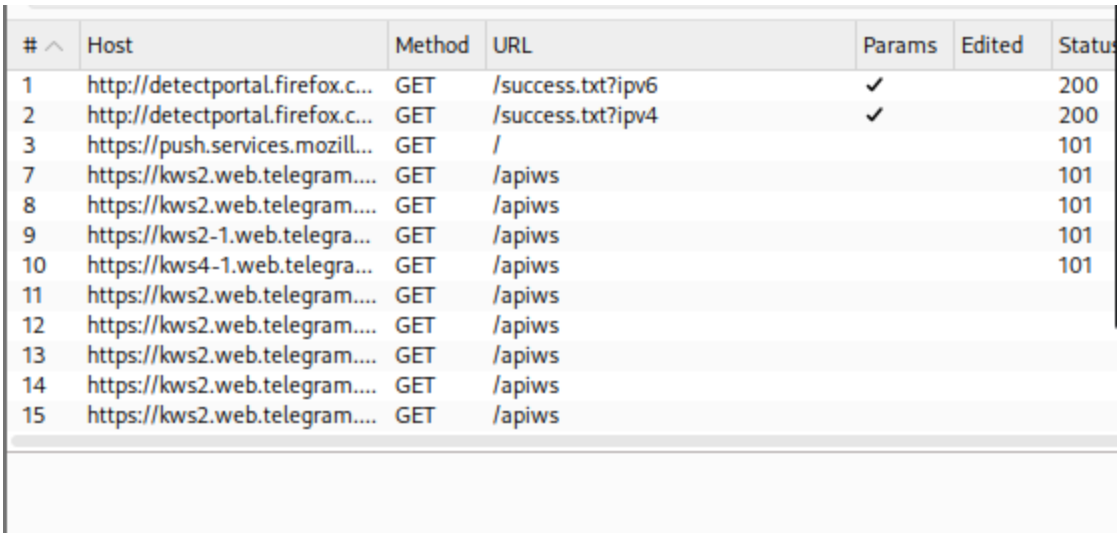
Освоить работу с инструментом Burp Suite для перехвата, анализа и модификации HTTP-запросов/ответов веб-приложения DVWA, а также для поиска уязвимостей.

Запустить Burp Suite.Настроить прокси в Burp Suite на `127.0.0.1:8080`. В браузере включить ручной прокси `127.0.0.1:8080` и установить сертификат Burp в «Доверенные центры сертификации». Включить перехват.В браузере открыть DVWA, выполнить вход и зафиксировать перехваченные запросы. Вкладка “HTTP history” — выбрать запрос.Отправить запрос в Repeater.



Time	Type	Direction	Method	URL	Status code	Length
20:23:0...	WS	→ To server		https://kws2.web.telegram.org/apiws		153
20:23:0...	WS	← To client		https://kws2.web.telegram.org/apiws		393
20:23:0...	HT...	→ Request	GET	https://kws2.web.telegram.org/apiws		
20:23:0...	HT...	→ Request	GET	https://kws2.web.telegram.org/apiws		
20:23:3...	HT...	→ Request	GET	https://kws2.web.telegram.org/apiws		
20:23:4...	HT...	→ Request	GET	https://kws2.web.telegram.org/apiws		
20:23:5...	HT...	→ Request	GET	https://kws2.web.telegram.org/apiws		
20:24:4...	HT...	→ Request	GET	https://kws2.web.telegram.org/apiws		
20:33:2...	HT...	→ Request	POST	http://o.pki.goog/we2		

Figure 1: окно Intercept с перехваченным запросом



#	Host	Method	URL	Params	Edited	Status
1	http://detectportal.firefox.c...	GET	/success.txt?ipv6	✓		200
2	http://detectportal.firefox.c...	GET	/success.txt?ipv4	✓		200
3	https://push.services.mozill...	GET	/			101
7	https://kws2.web.telegram....	GET	/apiws			101
8	https://kws2.web.telegram....	GET	/apiws			101
9	https://kws2-1.web.telegra...	GET	/apiws			101
10	https://kws4-1.web.telegra...	GET	/apiws			101
11	https://kws2.web.telegram....	GET	/apiws			
12	https://kws2.web.telegram....	GET	/apiws			
13	https://kws2.web.telegram....	GET	/apiws			
14	https://kws2.web.telegram....	GET	/apiws			
15	https://kws2.web.telegram....	GET	/apiws			

Figure 2: вкладка HTTP history с выбранным запросом

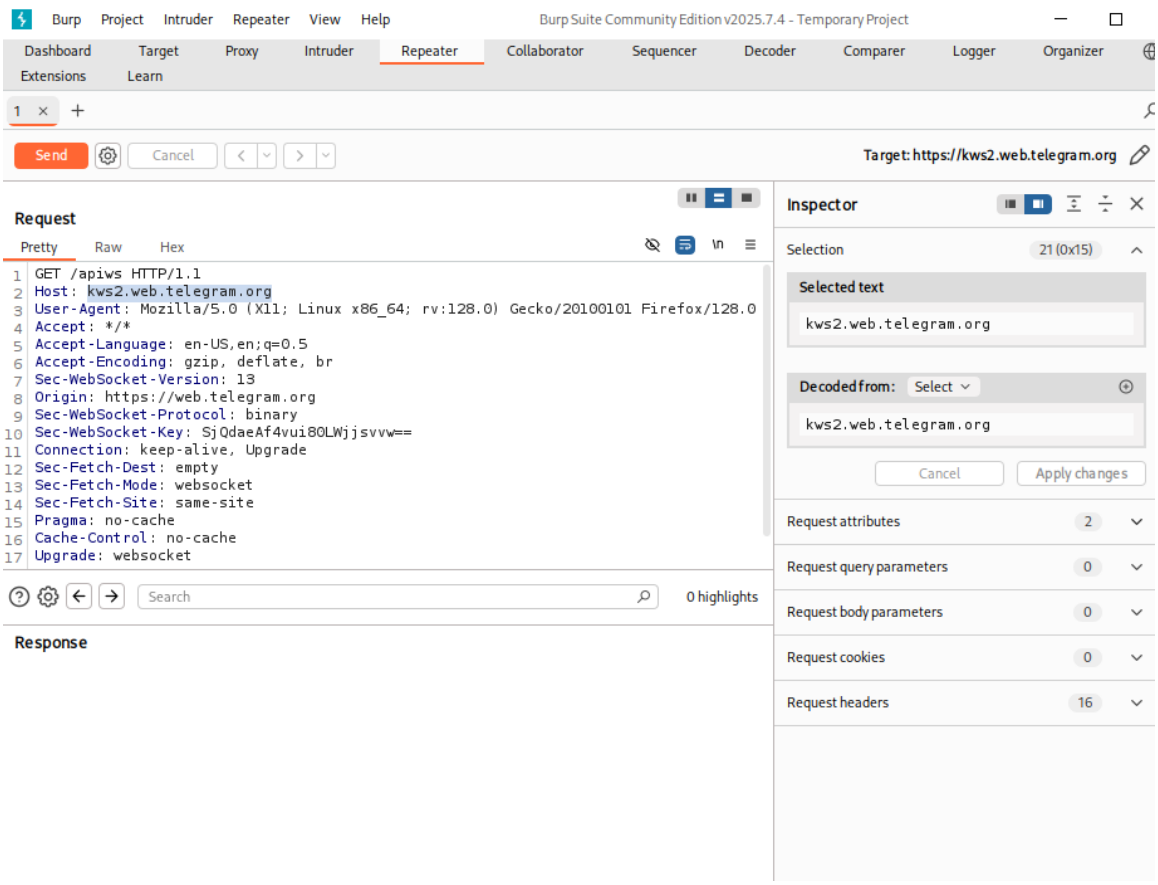


Figure 3: вкладка Repeater с изменённым запросом и ответом сервера

3 Вывод

Burp Suite позволяет детально анализировать взаимодействие клиента и сервера. - Инструмент полезен для поиска уязвимостей, тестирования валидации данных и проведения атак типа SQL Injection, XSS и др. - Для защиты необходимо фильтровать и проверять все входящие данные на стороне сервера.