



Burp Suite

Quick intro

Interface

The screenshot shows the Burp Suite Community Edition v2023.10.3.7 interface. The top menu bar includes Burp, Project, Intruder, Repeater, View, and Help. Below it, the main toolbar contains Dashboard, Target, Proxy, Intruder, Repeater, Collaborator, Sequencer, Decoder, Comparer, Logger, Organizer, and Extensions. The Proxy tab is selected and highlighted with a red box. The Tasks panel on the left shows a list of tasks, with the first task '1. Live passive crawl from Proxy (all traffic)' selected. The Event log at the bottom shows a message 'Proxy service started on 127.0.0.1'. A thought bubble overlay with the text 'Αυτά θα μας απασχολήσουν και περισσότερο' (These will occupy us even more) is positioned over the Proxy tab and the first task. The Issue activity panel on the right shows a list of issues, including 'Suspicious input transformation (reflect...)', 'SMTP header injection', 'Serialized object in HTTP message', 'Cross-site scripting (DOM-based)', 'XML external entity injection', 'External service interaction (HTTP)', 'Web cache poisoning', 'Server-side template injection', 'SQL injection', and 'OS command injection'.

Αυτά θα μας απασχολήσουν και περισσότερο

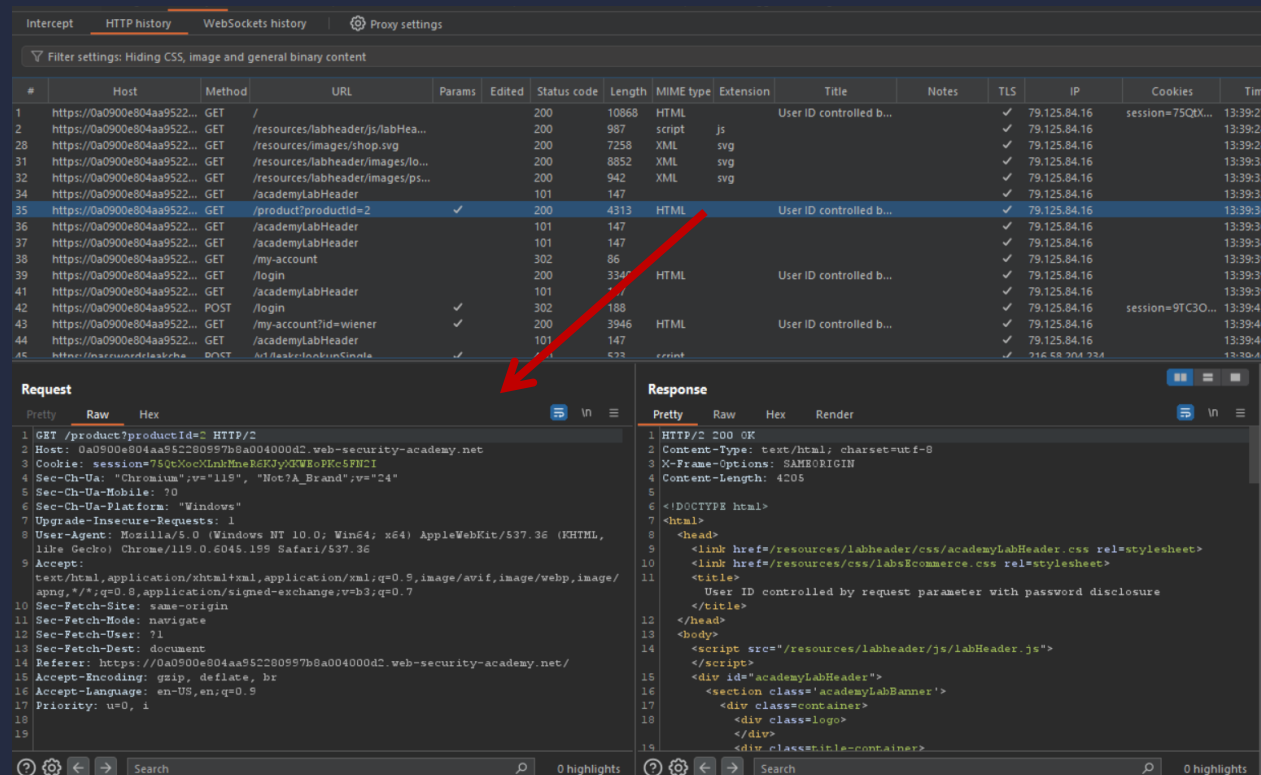
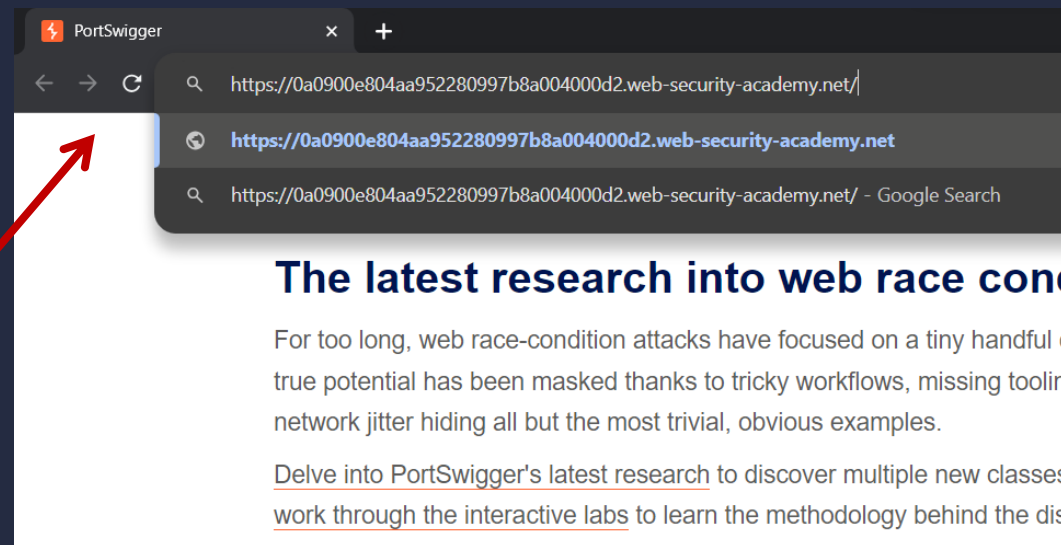
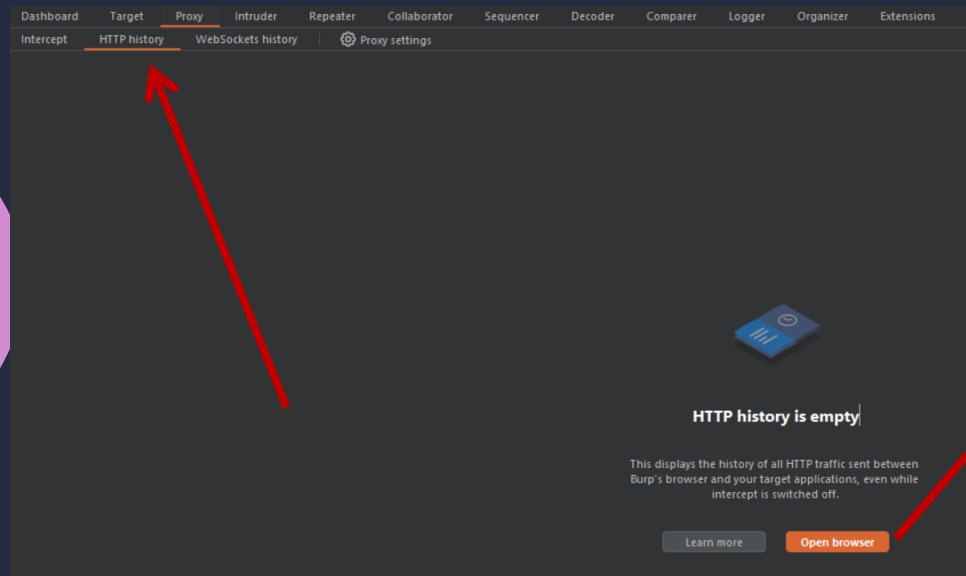
Source	Issue type	Host	Path	Insertion point
Task 0	Suspicious input transformation (reflect...	http://insecure-ban...	/url-shorten	input parameter
Task 0	SMTP header injection	http://insecure-web...	/contact-us	from parameter
Task 0	Serialized object in HTTP message	http://insecure-ban...	/blog	
Task 0	Cross-site scripting (DOM-based)	https://insecure-ban...	/	
Task 0	XML external entity injection	https://vulnerable-w...	/product/stock	request body
Task 0	External service interaction (HTTP)	https://insecure-we...	/product	Referer HTTP heade
Task 0	Web cache poisoning	http://insecure-ban...	/contact-us	
Task 0	Server-side template injection	http://insecure-ban...	/user-homepage	input parameter
Task 0	SQL injection	https://vulnerable-w...	/	TrackingId cookie
Task 0	OS command injection	https://insecure-we...	/feedback/submit	subject parameter

Είναι ένα web exploitation took kit

- **Burp proxy**: Μπαίνει ανάμεσα στον υπολογιστή σου και το web server καταγράφοντας όλα requests και τα responses
- **Repeater**: Παίρνει ένα request που έχουμε κάνει και μας δίνει την δυνατότητα να κάνουμε ότι αλλαγές θέλουμε και να δούμε τι response θα μας επιστρέψει ο server
- **Intruder** : Κάνει περίπου ότι ο repeater αλλα μας επιτρέπει να κάνουμε αυτόματα πολλά requests αλλάζοντας κάποια παράμετρο για κάποιο εύρος τιμών
- **Intercept** : Κάνει πάυση στην αυτόματη αποστολή των request καθώς αλληλεπιδρούμε με τον burp browser και μας επιτρέπει δυναμικά να τα επεξεργαζόμαστε.

Burp Proxy

Επιλέγοντας το proxy και ανοίγοντας τον browser του burp μπορούμε να προσθέσουμε την ιστοσελίδα που μας απασχολεί. Όλα τα request που θα στείλουμε και ό,τι response πάρουμε από τον server θα μας εμφανίζεται στο **HTTP history** καθώς όλα περνάνε μέσα από το proxy του burp.



Repeater

Στο HTTP history μπορούμε να διαλέξουμε το request που μας ενδιαφέρει και να το στείλουμε στο tool που μας ενδιαφέρει. Για παράδειγμα τώρα θέλουμε να χρησιμοποιήσουμε τον **repeater**

The screenshot shows the Burp Suite interface. The top pane displays the HTTP history with a list of requests. Request 156, a GET request to `/my-account?id=wiener`, is selected. The bottom pane shows the details of this request in the 'Request' tab, with the 'Raw' view selected. The raw request is as follows:

```
1 GET /my-account?id=wiener HTTP/2
2 Host: 0aa7001b048143658061d1fc001700ed.web-secur
3 Cookie: session=qvcnjsBRpNlnGYGXEjibL6pof6BU46n
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64
  like Gecko) Chrome/119.0.6045.199 Safari/537.36
7 Accept:
  text/html,application/xhtml+xml,application/xml
  apng, */*;q=0.8,application/signed-exchange;v=b3
8 Sec-Fetch-Site: same-origin
9 Sec-Fetch-Mode: navigate
10 Sec-Fetch-User: ?1
11 Sec-Fetch-Dest: document
```

On the right side, the Repeater tool is open, showing a list of actions for the selected request. The 'Send to Repeater' action is highlighted, with the keyboard shortcut 'Ctrl+R' displayed next to it. Other actions include 'Add to scope', 'Scan', 'Send to Intruder', 'Send to Sequencer', 'Send to Organizer', 'Send to Comparer (request)', 'Send to Comparer (response)', 'Show response in browser', 'Request in browser', 'Engagement tools [Pro version only]', 'Show new history window', 'Add notes', 'Highlight', 'Delete item', 'Clear history', and 'Copy URL'.

1 x +

Send

Cancel

< ▾

> ▾

Target: https://0aa7001b048143658061d1fc001

Request

Pretty

Raw

Hex

1

GET /my-account?id=wiener HTTP/2

2

Host: 0aa7001b048143658061d1fc001700ed.web-security-academy.net

3

Cookie: session=qwcnjsBBpNlnCYGXEjibL6pof6BU46nL

4

Cache-Control: max-age=0

5

Upgrade-Insecure-Requests: 1

6

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.199 Safari/537.36

7

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

8

Sec-Fetch-Site: same-origin

9

Sec-Fetch-Mode: navigate

10

Sec-Fetch-User: ?1

11

Sec-Fetch-Dest: document

12

Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"

13

Sec-Ch-Ua-Mobile: ?0

14

Sec-Ch-Ua-Platform: "Windows"

15

Referer: https://0aa7001b048143658061d1fc001700ed.web-security-academy.net/login

16

Accept-Encoding: gzip, deflate, br

17

Accept-Language: en-US,en;q=0.9

18

Priority: u=0, i

19

20

Response

Pretty

Raw

Hex

Render

Ανοίγοντας το tab του repeater βλέπουμε ότι έχει φορτώσει το request που του στείλαμε. Μας αφήνει να αλλάξουμε ό,τι παράμετρο θέλουμε σαν plain text και να το στείλουμε για να δούμε το response

Send

Cancel

Target: https://0aa7001b048143658061d1fc0017

Request

Pretty

Raw

Hex

```
1 GET /my-account?id=administrator HTTP/2
2 Host: 0aa7001b048143658061d1fc001700ed.web-security-academy.net
3 Cookie: session=qwcjnjsBFPnlnGYGXEjibL6pof6BU46nL
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
  like Gecko) Chrome/119.0.6045.199 Safari/537.36
7 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
  png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
8 Sec-Fetch-Site: same-origin
9 Sec-Fetch-Mode: navigate
10 Sec-Fetch-User: ?1
11 Sec-Fetch-Dest: document
12 Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
13 Sec-Ch-Ua-Mobile: ?0
14 Sec-Ch-Ua-Platform: "Windows"
15 Referer: https://0aa7001b048143658061d1fc001700ed.web-security-academy.net/login
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: en-US,en;q=0.9
18 Priority: u=0, i
19
20
```

Για παράδειγμα, εδώ αλλάζουμε την παράμετρο id από weiner που ήταν πριν σε administrator. Πατώντας send μας εμφανίζει στα δεξιά το response

Response

Pretty

Raw

Hex

Render

```
54 </div>
55 <div id=account-content>
56   <p>
57     Your username is: administrator
58   </p>
59   <form class="login-form" name="change-email-form" action="
60     /my-account/change-email" method="POST">
61     <label>
62       Email
63     </label>
64     <input required type="email" name="email" value="">
65     <input required type="hidden" name="csrf" value="
66       qqh8WA7Zwd08Fh5ozTGKlMM0QavCyT4d">
67     <button class='button' type='submit'>
68       Update email
69     </button>
70   </form>
71   <form class="login-form" action="/my-account/change-password" method="POST"
72   >
73     <br/>
74     <label>
75       Password
76     </label>
77     <input required type="hidden" name="csrf" value="
78       qqh8WA7Zwd08Fh5ozTGKlMM0QavCyT4d">
79     <input required type=password name=password value='0vsvyz8yw4f27sdlc8pi'
80     />
81     <button class='button' type='submit'>
82       Update password
83     </button>
84   </form>
85 </div>
86 </div>
87 </section>
88 <div class="footer-wrapper">
89 </div>
90 </div>
91 </body>
92 </html>
93
```


Intruder

- Όπως και με τον Repeater, στέλνουμε το request που μας ενδιαφέρει στον Intruder
- Έπειτα μας δίνονται μερικές επιλογές για την επίθεση που θέλουμε να κάνουμε (επιλέγοντας ποια πεδία του request θέλουμε να δοκιμάσουμε και τι είδους payloads θέλουμε να χρησιμοποιήσουμε)

Στο παρακάτω παράδειγμα βλέπουμε ένα login page. Θέλουμε να δοκιμάσουμε μια λίστα από ονόματα και κωδικούς που μας έχουν δοθεί και υποψιαζόμαστε ότι μπορεί να λειτουργούν κάποια από αυτά ως credentials

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: ☒ Update Host header to match target

1 POST /login HTTP/2
2 Host: 0a81006903a08fa88190570e001000dd.web-security-academy.net
3 Cookie: session=02QNVL25kzJ84A5pBF2JdESg2AmbdXoW5
4 Content-Length: 32
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Not_A Brand";v="8", "Chromium";v="120"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Windows"
9 Upgrade-Insecure-Requests: 1
10 Origin: https://0a81006903a08fa88190570e001000dd.web-security-academy.net
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.71 Safari/537.36
13 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: https://0a81006903a08fa88190570e001000dd.web-security-academy.net/login
19 Accept-Encoding: gzip, deflate, br
20 Accept-Language: en-US,en;q=0.9
21 Priority: u=0, i
22
23 username=fd&password=%2Cmk1cvns4

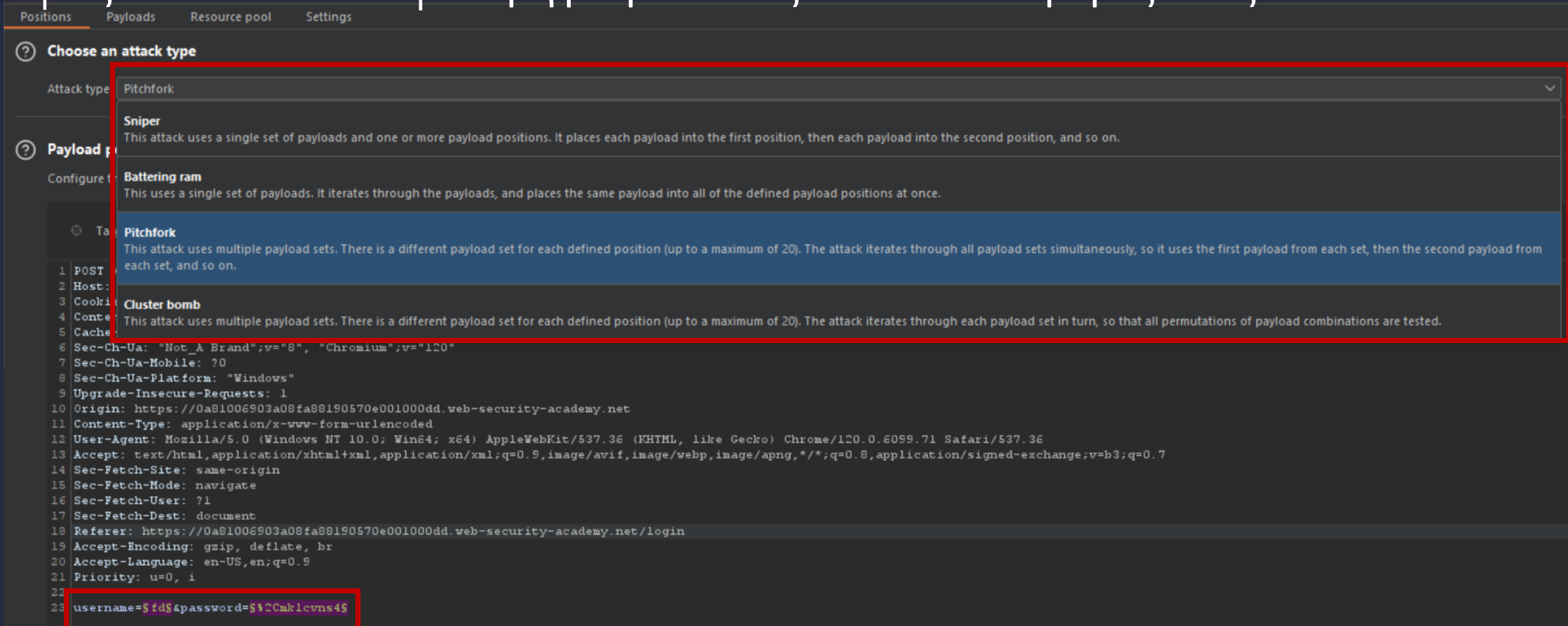
Buttons: Add \$, Clear \$, Auto \$, Refresh

0 payload positions Length: 1018

0 highlights Clear

Επιλέγοντας τα όρια του πεδίου που θέλουμε και πατώντας add, προσθέτουμε το σημείο που θα εισάγει το burp τα payloads που θα του ορίσουμε

- Αφου προσθέσουμε τα σημεία που θέλουμε να εισάγουμε τα payloads μας παρατηρήστε ότι αλλάζει χρώμα η γραμματοσειρά και έχουμε τον χαρακτήρα $\$$ που ορίζει τα payload positions.
- Αναλόγως τις περιστάσεις διαλέγουμε ανάλογο attack type για τις ανάγκες μας. Το ίδιο το burp περιγράφει ποιες είναι οι διαφορές τους.



The screenshot shows the Burp Suite interface with the 'Choose an attack type' dialog open. The 'Pitchfork' attack type is selected and highlighted in blue. The dialog also shows descriptions for 'Sniper', 'Battering ram', and 'Cluster bomb'.

Choose an attack type

Attack type: Pitchfork

Sniper
This attack uses a single set of payloads and one or more payload positions. It places each payload into the first position, then each payload into the second position, and so on.

Battering ram
This uses a single set of payloads. It iterates through the payloads, and places the same payload into all of the defined payload positions at once.

Pitchfork
This attack uses multiple payload sets. There is a different payload set for each defined position (up to a maximum of 20). The attack iterates through all payload sets simultaneously, so it uses the first payload from each set, then the second payload from each set, and so on.

Cluster bomb
This attack uses multiple payload sets. There is a different payload set for each defined position (up to a maximum of 20). The attack iterates through each payload set in turn, so that all permutations of payload combinations are tested.

Configure the attack:

1 POST
2 Host:
3 Cookie:
4 Content-Type:
5 Cache-Control:
6 Sec-Ch-Ua: "Not_A_Brand";v="8", "Chromium";v="120"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Windows"
9 Upgrade-Insecure-Requests: 1
10 Origin: https://0a81006903a08fa88190570e001000dd.web-security-academy.net
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.71 Safari/537.36
13 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: https://0a81006903a08fa88190570e001000dd.web-security-academy.net/login
19 Accept-Encoding: gzip, deflate, br
20 Accept-Language: en-US,en;q=0.9
21 Priority: u=0, i
22
23 username=\$fd\$password=\$12Cmklcvns4\$

Στο tab payloads του Intruder μπορούμε να ορίσουμε καλύτερα πώς θα είναι τα payloads μας. Πχ μπορεί σε ένα πεδίο να θέλουμε να δοκιμάσουμε αριθμούς από το 2 μέχρι το 20, άρα θα διαλέξουμε numbers στο payload type

The screenshot shows the 'Payloads' tab in the Burp Suite Intruder tool. The 'Payload sets' section is active, showing a configuration for a payload set. The 'Payload set' dropdown is set to '2' and the 'Payload count' is '1'. The 'Payload type' dropdown is set to 'Simple list' and the 'Request count' is '0'. A red box highlights the 'Payload set' and 'Payload type' dropdowns. Below the dropdowns, a list of payload types is visible, including 'Simple list', 'Runtime file', 'Custom iterator', 'Character substitution', 'Case modification', 'Recursive grep', 'Illegal Unicode', 'Character blocks', 'Numbers', 'Dates', 'Brute forcer', 'Null payloads', 'Character frobber', 'Bit flipper', and 'Username generator'. The 'Simple list' option is selected. To the left of the list, there are buttons for 'Paste', 'Load ...', 'Remove', 'Clear', 'Deduplicate', and 'Add'. At the bottom, there is a text input field with the placeholder 'Add from list ... [Pro version only]'.

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 2 Payload count: 1

Payload type: Simple list Request count: 0

Simple list

Runtime file

Custom iterator

Character substitution

Case modification

Recursive grep

Illegal Unicode

Character blocks

Numbers

Dates

Brute forcer

Null payloads

Character frobber

Bit flipper

Username generator

Paste

Load ...

Remove

Clear

Deduplicate

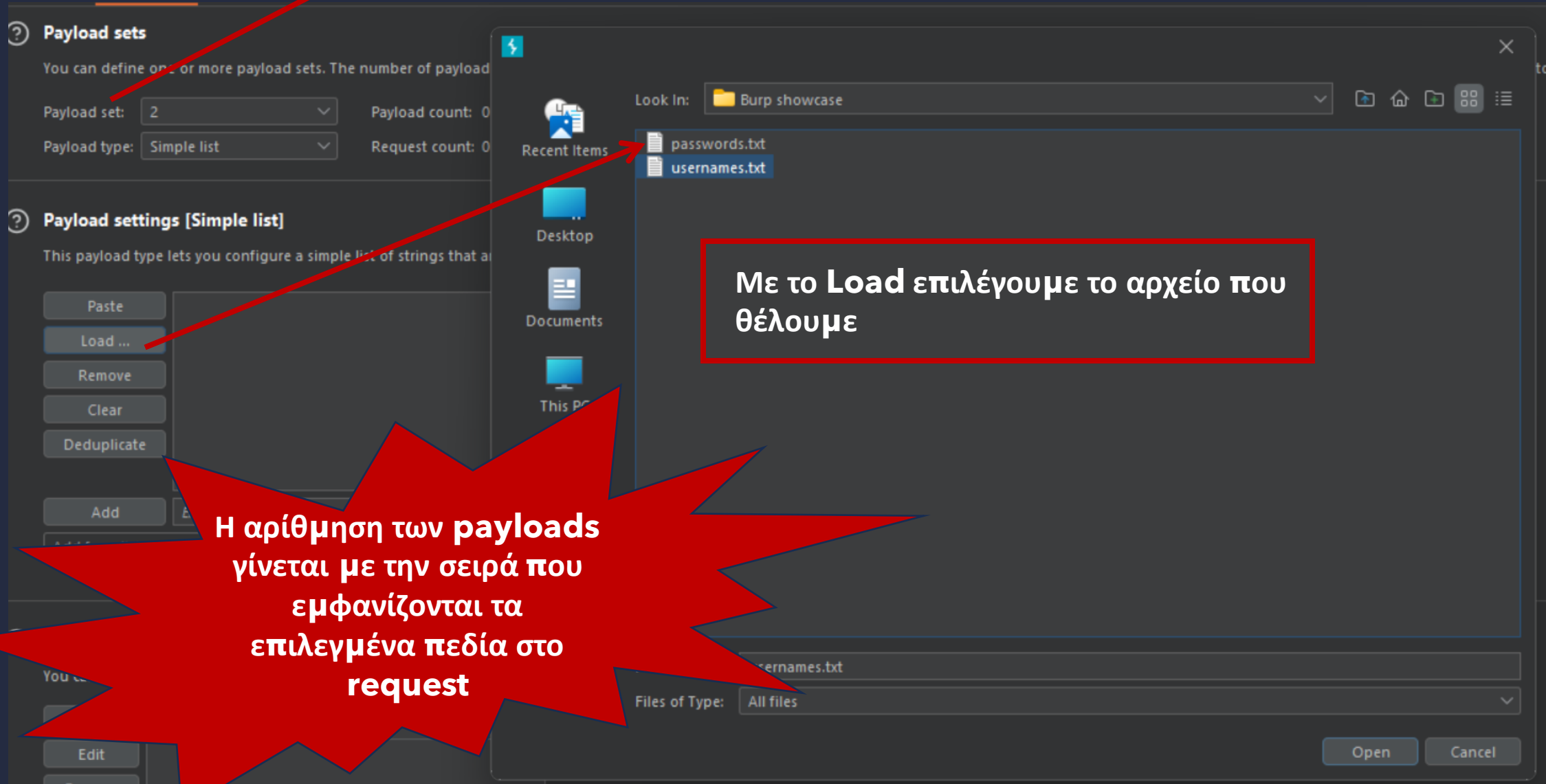
Add

Add from list ... [Pro version only]

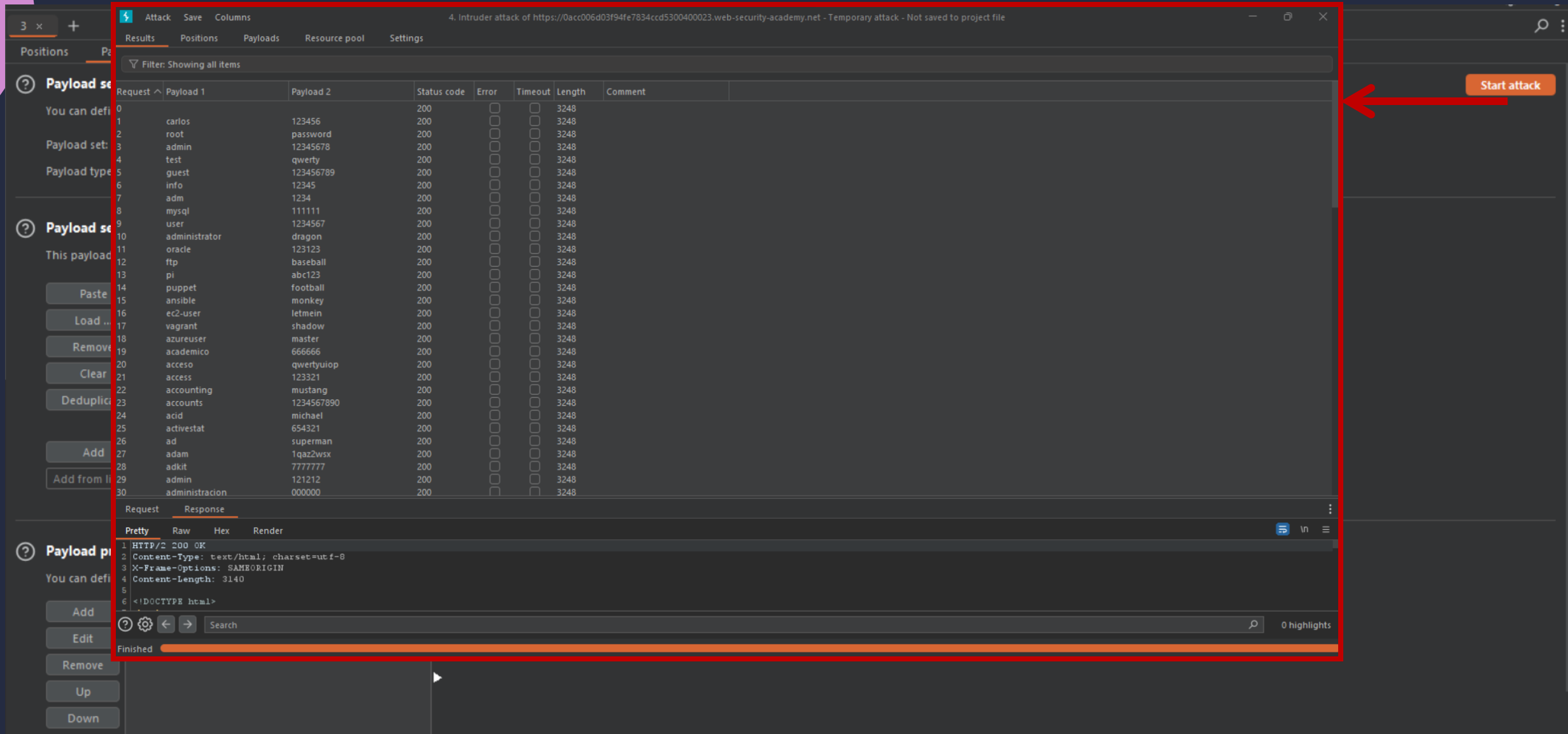
This payload type is used to generate a list of strings that are used as payloads.

Στην δική μας περίπτωση θα διαλέξουμε **simple list** για να του δώσουμε το αρχείο με τα **usernames** και το αρχείο με τα **passwords**

Το Payload set λέει ποιο σύνολο payload επεξεργαζόμαστε αυτήν την στιγμή πχ τώρα προσθέτουμε Passwords από το αρχείο passwords.txt στο δεύτερο set και αντίστοιχα θα προσθέσουμε τα usernames στο πρώτο set



Πατώντας Start attack αρχίζει να δοκιμάζει 1 προς 1 τα στοιχεία από τις δυο λίστες που του δώσαμε. Μπορούμε να παρακολουθήσουμε αναλυτικά τα requests που κάνει και τα responses που λαμβάνει το burp



The screenshot shows the Burp Suite interface during a brute-force attack. The 'Attack' tab is selected, showing a table of requests. The table has columns for Request, Payload 1, Payload 2, Status code, Error, Timeout, Length, and Comment. The status code for all requests is 200. The 'Start attack' button is visible in the top right corner, and a red arrow points from it to the table.

Request	Payload 1	Payload 2	Status code	Error	Timeout	Length	Comment
0			200			3248	
1	carlos	123456	200			3248	
2	root	password	200			3248	
3	admin	12345678	200			3248	
4	test	qwerty	200			3248	
5	guest	123456789	200			3248	
6	info	12345	200			3248	
7	adm	1234	200			3248	
8	mysql	111111	200			3248	
9	user	1234567	200			3248	
10	administrator	dragon	200			3248	
11	oracle	123123	200			3248	
12	ftp	baseball	200			3248	
13	pi	abc123	200			3248	
14	puppet	football	200			3248	
15	ansible	monkey	200			3248	
16	ec2-user	letmein	200			3248	
17	vagrant	shadow	200			3248	
18	azureuser	master	200			3248	
19	academico	666666	200			3248	
20	acceso	qwertyuiop	200			3248	
21	access	123321	200			3248	
22	accounting	mustang	200			3248	
23	accounts	1234567890	200			3248	
24	acid	michael	200			3248	
25	activestat	654321	200			3248	
26	ad	superman	200			3248	
27	adam	1qaz2wsx	200			3248	
28	adkit	7777777	200			3248	
29	admin	121212	200			3248	
30	administracion	000000	200			3248	

The bottom panel shows the 'Request' and 'Response' tabs. The 'Request' tab is selected, showing the raw HTTP request. The response is also visible in the 'Response' tab.

```
1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 3140
5
6 <!DOCTYPE html>
```

Intercept

Είναι μια λειτουργία που αφού την ενεργοποιήσουμε, κάθε request που γίνεται όσο αλληλεπιδρούμε με τον burp browser πριν σταλθεί στον server, το κρατάει το intercept για να το επεξεργαστούμε και να το στείλουμε χειροκίνητα.

- Με το forward του λέμε να στείλει το request, ενώ με το drop να μην το στείλει. Με το intercept is on/off ανοιγοκλείνουμε το intercept.
- Το Request που βλέπουμε είναι ό,τι πρόκειται να σταλεί στον server και μπορούμε να το επεξεργαστούμε όπως θέλουμε

The screenshot shows the Burp Suite interface with the Proxy tab selected. The 'Intercept' sub-tab is active, displaying a request to `https://0ab3002704dc13d18177757400a90075.web-security-academy.net:443` from IP `[79.125.84.16]`. The 'Intercept is on' button is highlighted. Below the request details, the 'Raw' tab is selected, showing the raw HTTP request text:

```
1 GET / HTTP/1.1
2 Host: 0ab3002704dc13d18177757400a90075.web-security-academy.net
3 Sec-Ch-Ua: "Not_A Brand";v="8", "Chromium";v="120"
4 Sec-Ch-Ua-Mobile: ?0
5 Sec-Ch-Ua-Platform: "Windows"
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.71 Safari/537.36
8 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
9 Sec-Fetch-Site: none
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-User: ?1
12 Sec-Fetch-Dest: document
13 Accept-Encoding: gzip, deflate, br
14 Accept-Language: en-US,en;q=0.9
15 Priority: u=0, i
16 Connection: close
17
18
```

Χρήσιμο υλικό

Μερικά Labs για να πειραματιστείτε περαιτέρω με το Burp Suite :

- <https://portswigger.net/web-security/access-control/lab-user-role-controlled-by-request-parameter>
- <https://portswigger.net/web-security/access-control/lab-user-id-controlled-by-request-parameter-with-password-disclosure>
- <https://portswigger.net/web-security/access-control/lab-unprotected-admin-functionality>

Για όσους θέλουν να μάθουν περισσότερα για το burp και για το web :

- <https://portswigger.net/web-security>
- <https://tryhackme.com/room/burpsuitebasics>
- <https://tryhackme.com/room/burpsuiterepeater>
- <https://owasp.org/www-project-juice-shop/>