Assignment Project Exam Help

COMP6443 : Topic 2(Week 2)

https://powcoder.com

User Identity and Authentication

Add WeChat powcoder

A NOTE ON ETHICS / LEGALITY

- UNSW hosting this course is an extremely important step forward.
- We expect a high standard of professionalism from you, meaning:
  - Respect the property of others and the university
  - Always abide by the law and university regulations
  - Be considerate of others to ensure everyone has an equal learning experience
- Always check that you have written permission before performing a security test on a system

Assignment Project Exam Help

https://powcoder.com

Add WeChat powcoder

PLEASE BE SUPER CAREFUL WHENEVER YOU’RE GENERATING NETWORK TRAFFIC

“NOT-A-HOMEWORK”

What tools have you tried?

Assignment Project Exam Help

https://powcoder.com

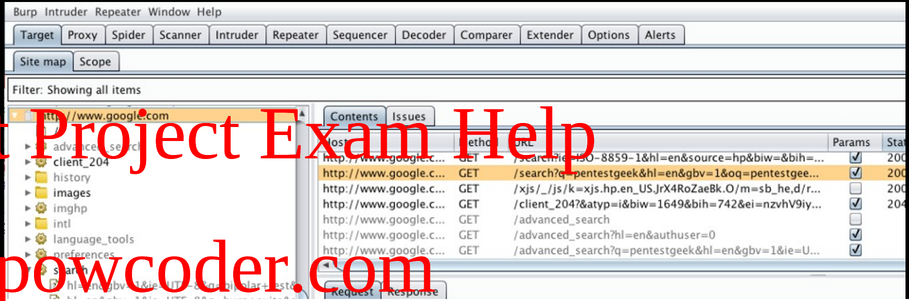
Add WeChat powcoder

“NOT-A-HOMEWORK”

What tools have you tried

- Burp
- Fiddler
- Wireshark
- nMap
- Nikto
- ZAP

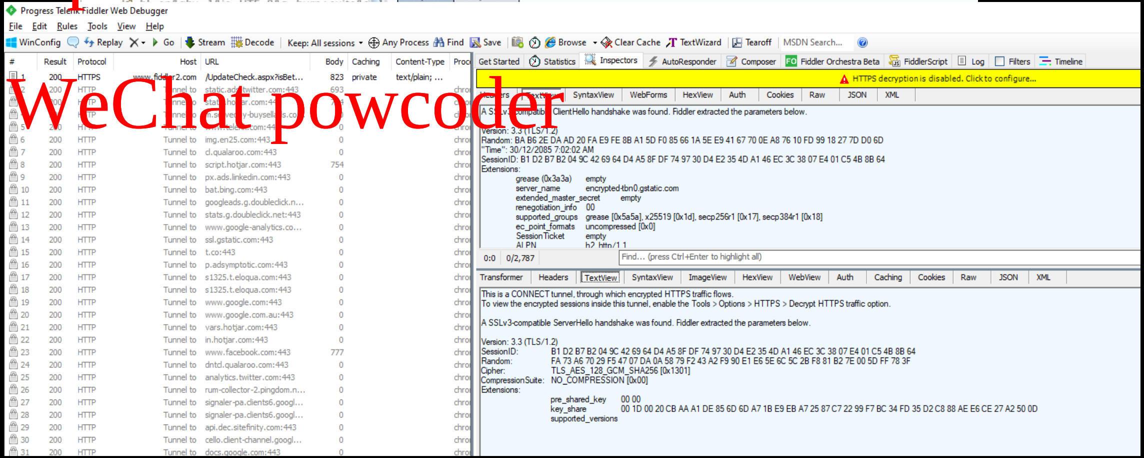
Assignment Project Exam Help
https://powcoder.com
Add WeChat powcoder


Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Site map Scope
Contents Issues
Request Response

Filter: Showing all items

- http://www.google.com
  - advanced_search
  - client_204
  - history
  - images
  - imghp
  - intl
  - language_tools
  - preferences
  - search
    - hl=en&gbv=1&ie=UTF-8&q=bipolar+test&

Host	Method	URL	Params	Status
http://www.google.c...	GET	/search?ie=ISO-8859-1&hl=en&source=hp&biw=&bih=...	☑	200
http://www.google.c...	GET	/search?q=pentestgeek&hl=en&gbv=1&oq=pentestgee...	☑	200
http://www.google.c...	GET	/xjs/_/js/k=xjs.hp.en_US.JrX4RoZaeBk.O/m=sb_he,d/r...	☐	200
http://www.google.c...	GET	/client_204?&atyp=i&biw=1649&bih=742&ei=nzvhV9iy...	☑	204
http://www.google.c...	GET	/advanced_search	☐	
http://www.google.c...	GET	/advanced_search?hl=en&authuser=0	☑	
http://www.google.c...	GET	/advanced_search?q=pentestgeek&hl=en&gbv=1&ie=U...	☑	


Progress Telerik Fiddler Web Debugger
File Edit Rules Tools View Help
WinConfig Replay Go Stream Decode Keep: All sessions Any Process Find Save Browse Clear Cache TextWizard Tearoff MSDN Search...
Get Started Statistics Inspectors AutoResponder Composer Fiddler Orchestra Beta FiddlerScript Log Filters Timeline
Headers TextView SyntaxView WebForms HexView Auth Cookies Raw JSON XML
Transformer Headers TextView SyntaxView ImageView HexView WebView Auth Caching Cookies Raw JSON XML

#	Result	Protocol	Host	URL	Body	Caching	Content-Type	Proc
1	200	HTTPS	www.fiddler2.com	/UpdateCheck.aspx?isBet...	823	private	text/plain; ...	
2	200	HTTP	Tunnel to	static.ads-twitter.com:443	693			chro
3	200	HTTP	Tunnel to	static.hotjar.com:443	754			chro
4	200	HTTP	Tunnel to	m.servedby-buysellads.com:443	0			chro
5	200	HTTP	Tunnel to	www.telerik.com:443	0			chro
6	200	HTTP	Tunnel to	img.en25.com:443	0			chro
7	200	HTTP	Tunnel to	cl.qualaroo.com:443	0			chro
8	200	HTTP	Tunnel to	script.hotjar.com:443	754			chro
9	200	HTTP	Tunnel to	px.ads.linkedin.com:443	0			chro
10	200	HTTP	Tunnel to	bat.bing.com:443	0			chro
11	200	HTTP	Tunnel to	googleads.g.doubleclick.n...	0			chro
12	200	HTTP	Tunnel to	stats.g.doubleclick.net:443	0			chro
13	200	HTTP	Tunnel to	www.google-analytics.co...	0			chro
14	200	HTTP	Tunnel to	ssl.gstatic.com:443	0			chro
15	200	HTTP	Tunnel to	t.co:443	0			chro
16	200	HTTP	Tunnel to	p.adsymptotic.com:443	0			chro
17	200	HTTP	Tunnel to	s1325.t.eloqua.com:443	0			chro
18	200	HTTP	Tunnel to	s1325.t.eloqua.com:443	0			chro
19	200	HTTP	Tunnel to	www.google.com:443	0			chro
20	200	HTTP	Tunnel to	www.google.com.au:443	0			chro
21	200	HTTP	Tunnel to	vars.hotjar.com:443	0			chro
22	200	HTTP	Tunnel to	in.hotjar.com:443	0			chro
23	200	HTTP	Tunnel to	www.facebook.com:443	777			chro
24	200	HTTP	Tunnel to	dntcl.qualaroo.com:443	0			chro
25	200	HTTP	Tunnel to	analytics.twitter.com:443	0			chro
26	200	HTTP	Tunnel to	rum-collector-2.pingdom.n...	0			chro
27	200	HTTP	Tunnel to	signaler-pa.clients6.googl...	0			chro
28	200	HTTP	Tunnel to	signaler-pa.clients6.googl...	0			chro
29	200	HTTP	Tunnel to	api.dec.sitefinity.com:443	0			chro
30	200	HTTP	Tunnel to	cello.client-channel.googl...	0			chro
31	200	HTTP	Tunnel to	docs.google.com:443	0			chro

⚠ HTTPS decryption is disabled. Click to configure...

```
A SSLv3-compatible ClientHello handshake was found. Fiddler extracted the parameters below.

Version: 3.3 (TLS/1.2)
Random: BA B6 2E DA AD 20 FA E9 FE 8B A1 5D F0 85 66 1A 5E E9 41 67 70 0E A8 76 10 FD 99 18 27 7D D0 6D
"Time": 30/12/2085 7:02:02 AM
SessionID: B1 D2 B7 B2 04 9C 42 69 64 D4 A5 8F DF 74 97 30 D4 E2 35 4D A1 46 EC 3C 38 07 E4 01 C5 4B 8B 64
Extensions:
        grease (0x3a3a)     empty
        server_name         encrypted-tbn0.gstatic.com
        extended_master_secret      empty
        renegotiation_info  00
        supported_groups    grease [0x5a5a], x25519 [0x1d], secp256r1 [0x17], secp384r1 [0x18]
        ec_point_formats    uncompressed [0x0]
        SessionTicket       empty
        ALPN                h2, http/1.1
```

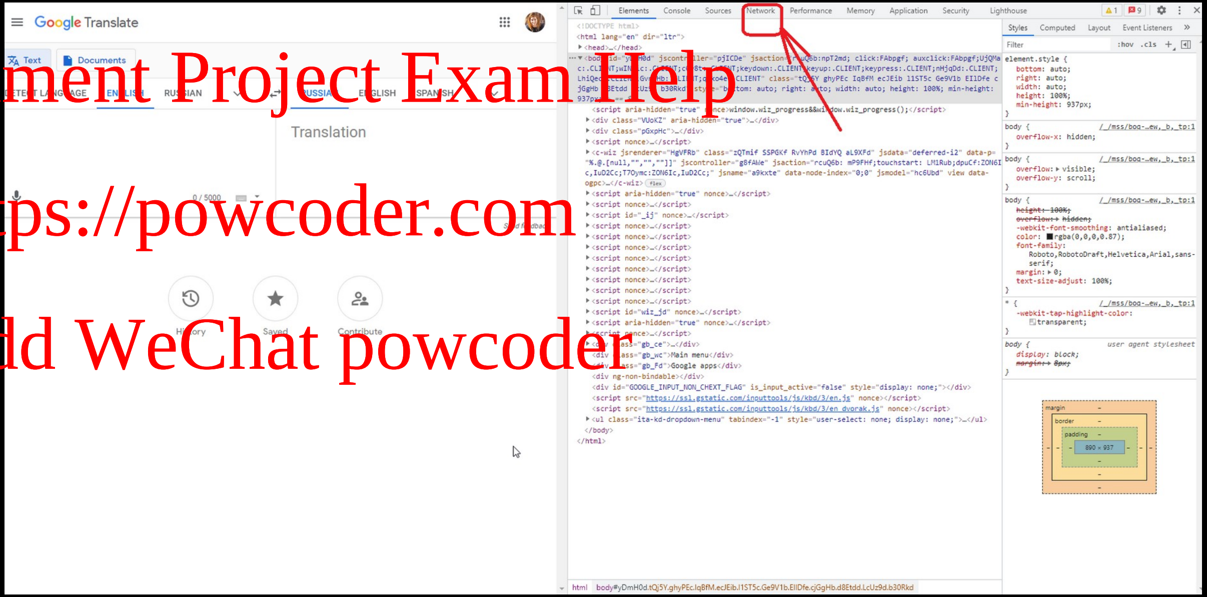
0:0 0/2,787 Find... (press Ctrl+Enter to highlight all)

```
This is a CONNECT tunnel, through which encrypted HTTPS traffic flows.
To view the encrypted sessions inside this tunnel, enable the Tools > Options > HTTPS > Decrypt HTTPS traffic option.

A SSLv3-compatible ServerHello handshake was found. Fiddler extracted the parameters below.

Version: 3.3 (TLS/1.2)
SessionID:          B1 D2 B7 B2 04 9C 42 69 64 D4 A5 8F DF 74 97 30 D4 E2 35 4D A1 46 EC 3C 38 07 E4 01 C5 4B 8B 64
Random:             FA 73 A6 70 29 F5 47 07 DA 0A 58 79 F2 43 A2 F9 90 E1 E6 5E 6C 5C 2B F8 81 B2 7E 00 5D FF 78 3F
Cipher:             TLS_AES_128_GCM_SHA256 [0x1301]
CompressionSuite:   NO_COMPRESSION [0x00]
Extensions:
                    pre_shared_key      00 00
                    key_share           00 1D 00 20 CB AA A1 DE 85 6D 6D A7 1B E9 EB A7 25 87 C7 22 99 F7 BC 34 FD 35 D2 C8 88 AE E6 CE 27 A2 50 0D
                    supported_versions
```

“NOT-A-HOMEWORK”

What have you seen?

- Requests
- Messages headers
- Files
- Page layouts



```
<!DOCTYPE html>
<html lang="en" dir="ltr">
▶<head>…</head>
▼<bod[illegible] id="y[illegible]H0d" jscontr[illegible]ller="pjICDe" jsaction="[illegible]uQ6b:npT2md; click:FAbpgf; auxclick:FAbpgf;UjQMa
c:.CLI[illegible]NT;wIN[illegible]c:.C[illegible]IENT;c[illegible]8t[illegible]CLIENT;keydown:.CLIENT;keyup:.CLIENT;keypress:.CLIENT;nHjqDd:.CLIENT;
LhiQe[illegible]Gv[illegible]Hb:[illegible]LIENT;q[illegible]ko4e[illegible]CLIENT" class="tQ[illegible]5Y ghyPEc IqBfM ecJEib l1ST5c Ge9V1b EIlDfe c
jGgHb [illegible]8Etdd [illegible]Uz[illegible] b30Rkd" style="b[illegible]ttom: auto; right: a[illegible]to; width: auto; height: 100%; min-height:
937px;[illegible]
   <script aria-hidden="true" nonce>window.wiz_progress&&window.wiz_progress();</script>
  ▶<div class="VUoKZ" aria-hidden="true">…</div>
  ▶<div class="pGxpHc">…</div>
  ▶<script nonce>…</script>
  ▶<c-wiz jsrenderer="HgVFRb" class="zQTmif SSPGKf RvYhPd BIdYQ aL9XFd" jsdata="deferred-i2" data-p=
  "%.@.[null,"","",""]]" jscontroller="g8fAWe" jsaction="rcuQ6b: mP9FHf;touchstart: LM1Rub;dpuCf:ZON6I
  c,IuD2Cc;T7Oymc:ZON6Ic,IuD2Cc;" jsname="a9kxte" data-node-index="0;0" jsmodel="hc6Ubd" view data-
  ogpc>…</c-wiz> flex
  ▶<script aria-hidden="true" nonce>…</script>
  ▶<script nonce>…</script>
  ▶<script id="_ij" nonce>…</script>
  ▶<script nonce>…</script>
  ▶<script nonce>…</script>
  ▶<script nonce>…</script>
  ▶<script nonce>…</script>
  ▶<script nonce>…</script>
  ▶<script nonce>…</script>
  ▶<script nonce>…</script>
  ▶<script nonce>…</script>
  ▶<script id="wiz_jd" nonce>…</script>
  ▶<script aria-hidden="true" nonce>…</script>
  ▶<script nonce>…</script>
  ▶<div class="gb_ce">…</div>
   <div class="gb_wc">Main menu</div>
   <div class="gb_Fd">Google apps</div>
   <div ng-non-bindable></div>
   <div id="GOOGLE_INPUT_NON_CHEXT_FLAG" is_input_active="false" style="display: none;"></div>
   <script src="https://ssl.gstatic.com/inputtools/js/kbd/3/en.js" nonce></script>
   <script src="https://ssl.gstatic.com/inputtools/js/kbd/3/en_dvorak.js" nonce></script>
  ▶<ul class="ita-kd-dropdown-menu" tabindex="-1" style="user-select: none; display: none;">…</ul>
 </body>
</html>
```

```
element.style {
  bottom: auto;
  right: auto;
  width: auto;
  height: 100%;
  min-height: 937px;
}
body {                                  /_/mss/boq-…ew,_b,_tp:1
  overflow-x: hidden;
}
body {                                  /_/mss/boq-…ew,_b,_tp:1
  overflow: ▶ visible;
  overflow-y: scroll;
}
body {                                  /_/mss/boq-…ew,_b,_tp:1
  ~~height: 100%;~~
  ~~overflow: ▶ hidden;~~
  -webkit-font-smoothing: antialiased;
  color: ■rgba(0,0,0,0.87);
  font-family:
     Roboto,RobotoDraft,Helvetica,Arial,sans-
     serif;
  margin: ▶ 0;
  text-size-adjust: 100%;
}
* {                                     /_/mss/boq-…ew,_b,_tp:1
  -webkit-tap-highlight-color:
     □transparent;
}
body {                          user agent stylesheet
  display: block;
  ~~margin: ▶ 8px;~~
}
```

Assignment Project Exam Help

https://powcoder.com

Add WeChat powcoder

IDENTITY

What is IDENTITY?

Assignment Project Exam Help

https://powcoder.com

Add WeChat powcoder

IDENTITY

What is DIGITAL identity?

Assignment Project Exam Help

- A digital identity is information on an entity used by computer systems to represent an external agent
- **ISO**/IEC 24760-1 "set of attributes related to an entity"
- Various National digital identity systems

https://powcoder.com

Add WeChat powcoder

IDENTITY ATTACKS

- Social
- Credential stealing
- Compromised/weak password
- MitM

Assignment Project Exam Help

https://powcoder.com

Add WeChat powcoder

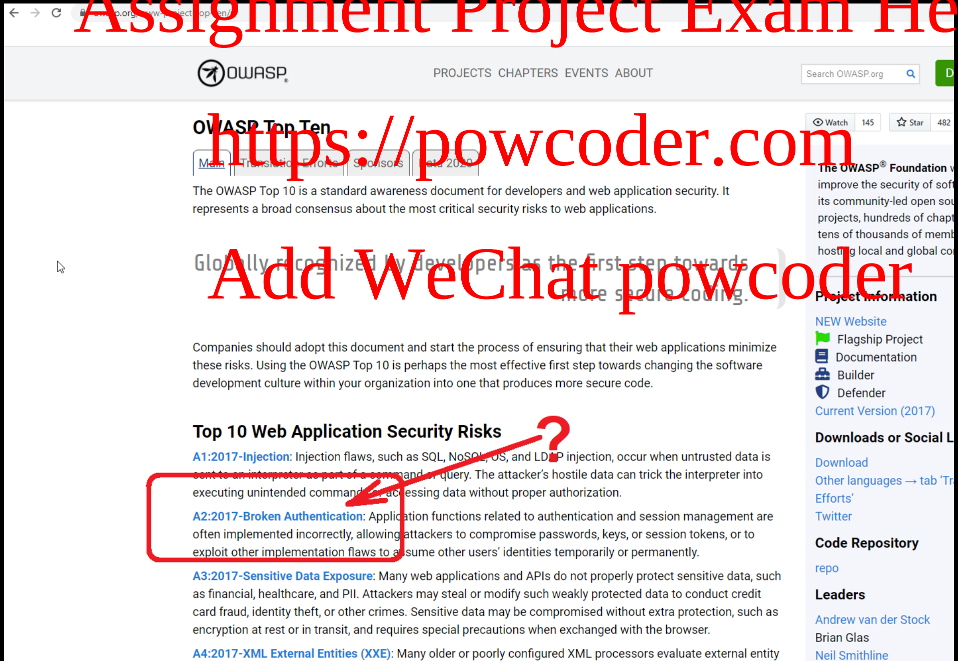
OWASP TOP TEN

https://owasp.org/www-project-top-ten/

Assignment Project Exam Help

https://powcoder.com

Add WeChat powcoder



OWASP Top Ten

The OWASP Top 10 is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications.

> Globally recognized by developers as the first step towards more secure coding.

Companies should adopt this document and start the process of ensuring that their web applications minimize these risks. Using the OWASP Top 10 is perhaps the most effective first step towards changing the software development culture within your organization into one that produces more secure code.

Top 10 Web Application Security Risks

A1:2017-Injection: Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

A2:2017-Broken Authentication: Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.

A3:2017-Sensitive Data Exposure: Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.

A4:2017-XML External Entities (XXE): Many older or poorly configured XML processors evaluate external entity

The OWASP® Foundation w
improve the security of soft
its community-led open sou
projects, hundreds of chapt
tens of thousands of memb
hosting local and global co

Project Information

NEW Website
Flagship Project
Documentation
Builder
Defender
Current Version (2017)

Downloads or Social L

Download
Other languages → tab 'Tr
Efforts'
Twitter

Code Repository

repo

Leaders

Andrew van der Stock
Brian Glas
Neil Smithline

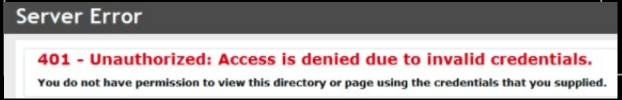
OVERVIEW

Authentication → Session Management → Access Control(Authorization)		
Is the user who they claim to be? If not	Is it still that user?	Is the user allowed to access this thing?

Assignment Project Exam Help

https://powcoder.com

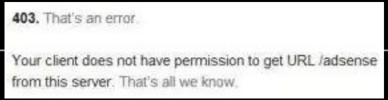
Add WeChat powcoder



Server Error

401 - Unauthorized: Access is denied due to invalid credentials.

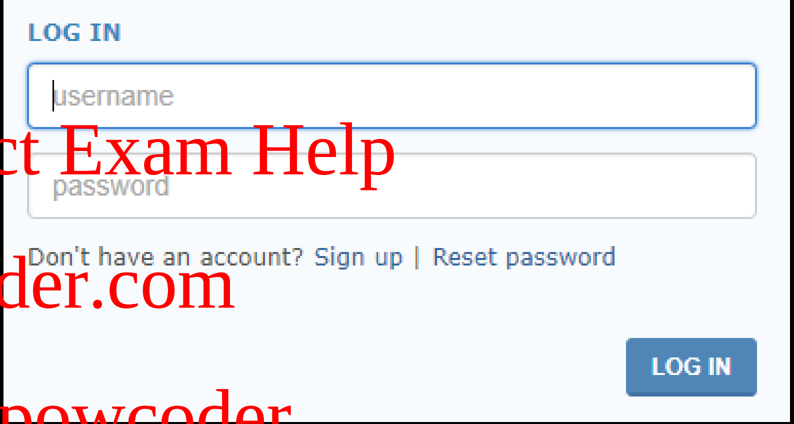
You do not have permission to view this directory or page using the credentials that you supplied.



403. That's an error.

Your client does not have permission to get URL /adsense from this server. That's all we know.

WEB AUTHENTICATION 2021



Assignment Project Exam Help

https://powcoder.com

Add WeChat powcoder

- Username / Password
  - Password reset via email
  - 2FA: SMS, Token, Apps (incl TOTP)
  - Active vs Passive 2FA
- Authentication can be delegated (e.g. SSO, Oauth, JWT)
- CAPTCHAs

BAD AUTHENTICATION 101

Assignment Project Exam Help

https://powcoder.com

Add WeChat powcoder

BAD AUTHENTICATION 101+1

Assignment Project Exam Help

https://powcoder.com

Add WeChat powcoder

BAD AUTHENTICATION 101

Assignment Project Exam Help

https://powcoder.com

Add WeChat powcoder

DEFAULT CREDENTIALS

“The ASD's investigation found that internet-facing services still had their default passwords, admin:admin and guest:guest.”

http://www.zdnet.com/article/secret-f-35-p-8-c-130-data-stolen-in-australian-defence-contractor-hack/

Assignment Project Exam Help

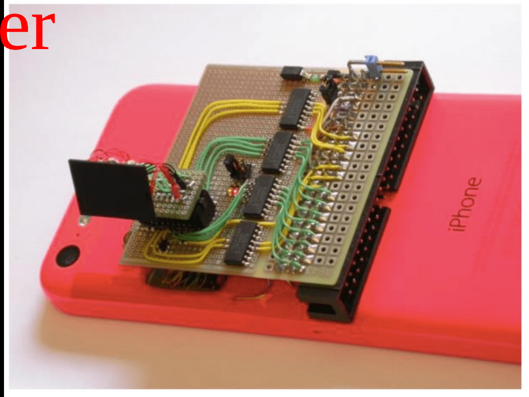
https://powcoder.com

Add WeChat powcoder

BRUTE FORCE (BEST FORCE)

- Attempt logins with common passwords
- Try known email + password combinations from previous breaches
  - 1 User, Many Passwords: Brute Force
  - Many Users, Many Passwords: “Credential Stuffing”
- Login rate-limiting and lockouts
  - CAPTCHA
  - Lockouts (iPhone)
- Proactive Monitoring
- User Communication

Assignment Project Exam Help
https://powcoder.com
Add WeChat powcoder



INFORMATION DISCLOSURE

Assignment Project Exam Help

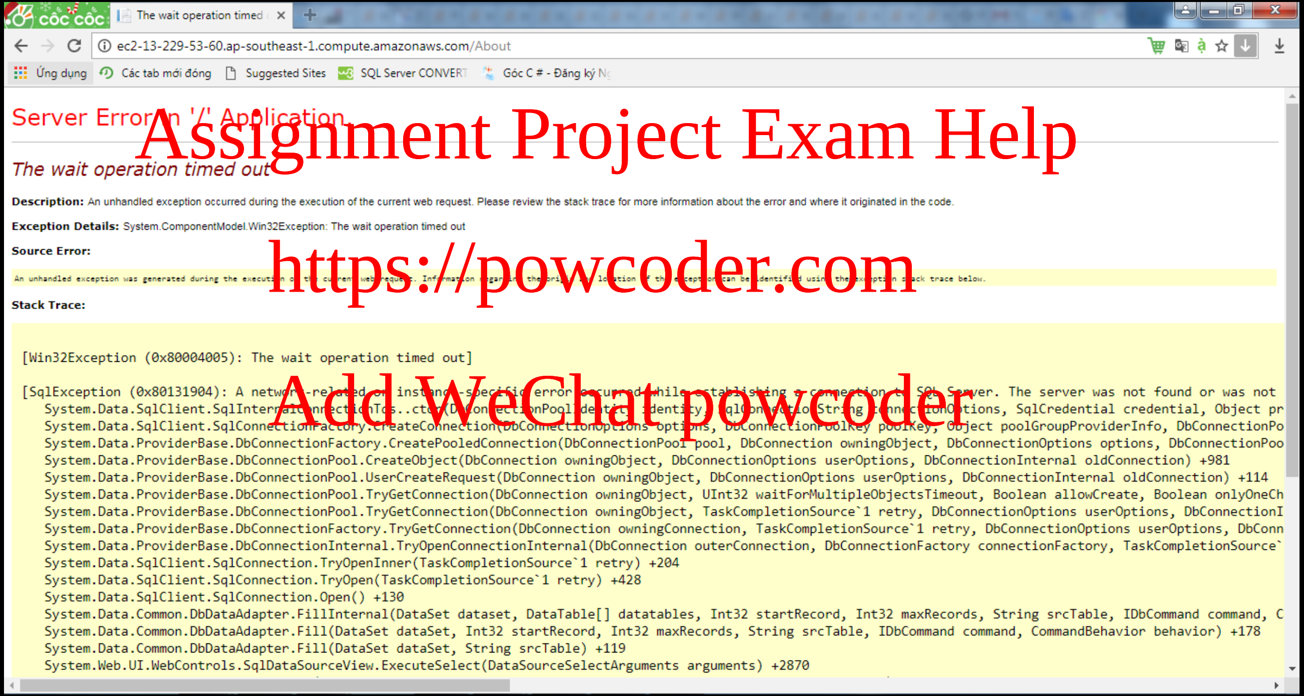
“Login failed: invalid username.”

https://powcoder.com

“Login failed: invalid username or password.”

Add WeChat powcoder

ERRORS HANDLING



Server Error in '/' Application.

The wait operation timed out

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.ComponentModel.Win32Exception: The wait operation timed out

Source Error:

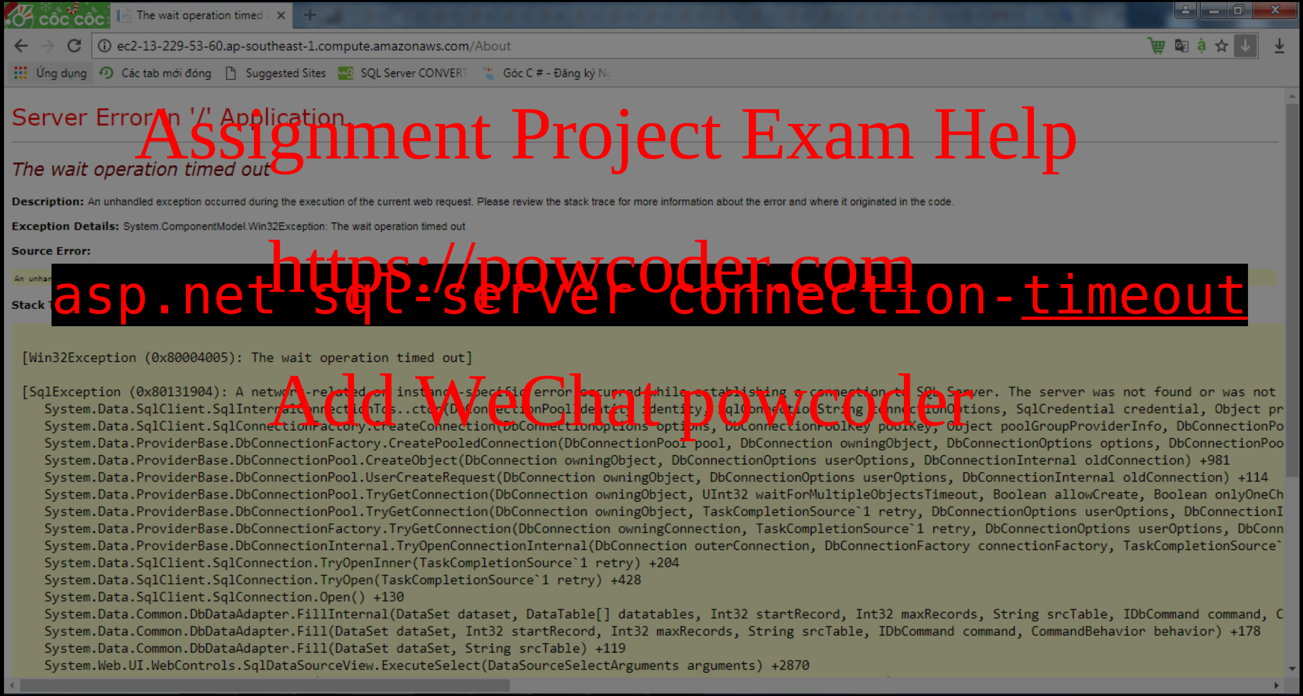
```
An unhandled exception was generated during the execution of the current web request. Information regarding the origin and location of the exception can be identified using the exception stack trace below.
```

Stack Trace:

```
[Win32Exception (0x80004005): The wait operation timed out]

[SqlException (0x80131904): A network-related or instance-specific error occurred while establishing a connection to SQL Server. The server was not found or was not
   System.Data.SqlClient.SqlInternalConnectionTds..ctor(DbConnectionPoolIdentity identity, SqlConnectionString connectionOptions, SqlCredential credential, Object pr
   System.Data.SqlClient.SqlConnectionFactory.CreateConnection(DbConnectionOptions options, DbConnectionPoolKey poolKey, Object poolGroupProviderInfo, DbConnectionPo
   System.Data.ProviderBase.DbConnectionFactory.CreatePooledConnection(DbConnectionPool pool, DbConnection owningObject, DbConnectionOptions options, DbConnectionPoo
   System.Data.ProviderBase.DbConnectionPool.CreateObject(DbConnection owningObject, DbConnectionOptions userOptions, DbConnectionInternal oldConnection) +981
   System.Data.ProviderBase.DbConnectionPool.UserCreateRequest(DbConnection owningObject, DbConnectionOptions userOptions, DbConnectionInternal oldConnection) +114
   System.Data.ProviderBase.DbConnectionPool.TryGetConnection(DbConnection owningObject, UInt32 waitForMultipleObjectsTimeout, Boolean allowCreate, Boolean onlyOneCh
   System.Data.ProviderBase.DbConnectionPool.TryGetConnection(DbConnection owningObject, TaskCompletionSource`1 retry, DbConnectionOptions userOptions, DbConnectionI
   System.Data.ProviderBase.DbConnectionFactory.TryGetConnection(DbConnection owningConnection, TaskCompletionSource`1 retry, DbConnectionOptions userOptions, DbConn
   System.Data.ProviderBase.DbConnectionInternal.TryOpenConnectionInternal(DbConnection outerConnection, DbConnectionFactory connectionFactory, TaskCompletionSource`
   System.Data.SqlClient.SqlConnection.TryOpenInner(TaskCompletionSource`1 retry) +204
   System.Data.SqlClient.SqlConnection.TryOpen(TaskCompletionSource`1 retry) +428
   System.Data.SqlClient.SqlConnection.Open() +130
   System.Data.Common.DbDataAdapter.FillInternal(DataSet dataset, DataTable[] datatables, Int32 startRecord, Int32 maxRecords, String srcTable, IDbCommand command, C
   System.Data.Common.DbDataAdapter.Fill(DataSet dataSet, Int32 startRecord, Int32 maxRecords, String srcTable, IDbCommand command, CommandBehavior behavior) +178
   System.Data.Common.DbDataAdapter.Fill(DataSet dataSet, String srcTable) +119
   System.Web.UI.WebControls.SqlDataSourceView.ExecuteSelect(DataSourceSelectArguments arguments) +2870
```

Assignment Project Exam Help
https://powcoder.com
Add WeChat powcoder

ERRORS HANDLING



Server Error in '/' Application.

The wait operation timed out

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.ComponentModel.Win32Exception: The wait operation timed out

Source Error:

An unhan

Stack T

asp.net sql-server connection-timeout

```
[Win32Exception (0x80004005): The wait operation timed out]

[SqlException (0x80131904): A network-related or instance-specific error occurred while establishing a connection to SQL Server. The server was not found or was not
   System.Data.SqlClient.SqlInternalConnectionTds..ctor(DbConnectionPoolIdentity identity, SqlConnectionString connectionOptions, SqlCredential credential, Object pr
   System.Data.SqlClient.SqlConnectionFactory.CreateConnection(DbConnectionOptions options, DbConnectionPoolKey poolKey, Object poolGroupProviderInfo, DbConnectionPo
   System.Data.ProviderBase.DbConnectionFactory.CreatePooledConnection(DbConnectionPool pool, DbConnection owningObject, DbConnectionOptions options, DbConnectionPoo
   System.Data.ProviderBase.DbConnectionPool.CreateObject(DbConnection owningObject, DbConnectionOptions userOptions, DbConnectionInternal oldConnection) +981
   System.Data.ProviderBase.DbConnectionPool.UserCreateRequest(DbConnection owningObject, DbConnectionOptions userOptions, DbConnectionInternal oldConnection) +114
   System.Data.ProviderBase.DbConnectionPool.TryGetConnection(DbConnection owningObject, UInt32 waitForMultipleObjectsTimeout, Boolean allowCreate, Boolean onlyOneCh
   System.Data.ProviderBase.DbConnectionPool.TryGetConnection(DbConnection owningObject, TaskCompletionSource`1 retry, DbConnectionOptions userOptions, DbConnectionI
   System.Data.ProviderBase.DbConnectionFactory.TryGetConnection(DbConnection owningConnection, TaskCompletionSource`1 retry, DbConnectionOptions userOptions, DbConn
   System.Data.ProviderBase.DbConnectionInternal.TryOpenConnectionInternal(DbConnection outerConnection, DbConnectionFactory connectionFactory, TaskCompletionSource`
   System.Data.SqlClient.SqlConnection.TryOpenInner(TaskCompletionSource`1 retry) +204
   System.Data.SqlClient.SqlConnection.TryOpen(TaskCompletionSource`1 retry) +428
   System.Data.SqlClient.SqlConnection.Open() +130
   System.Data.Common.DbDataAdapter.FillInternal(DataSet dataset, DataTable[] datatables, Int32 startRecord, Int32 maxRecords, String srcTable, IDbCommand command, C
   System.Data.Common.DbDataAdapter.Fill(DataSet dataSet, Int32 startRecord, Int32 maxRecords, String srcTable, IDbCommand command, CommandBehavior behavior) +178
   System.Data.Common.DbDataAdapter.Fill(DataSet dataSet, String srcTable) +119
   System.Web.UI.WebControls.SqlDataSourceView.ExecuteSelect(DataSourceSelectArguments arguments) +2870
```

Assignment Project Exam Help

https://powcoder.com

Add WeChat powcoder

TRANSPORT LAYER SECURITY (WHY?)

MitM attack: forces a victim's browser into communicating with an adversary in plain-text over HTTP, and the adversary proxies the modified content from an HTTPS server

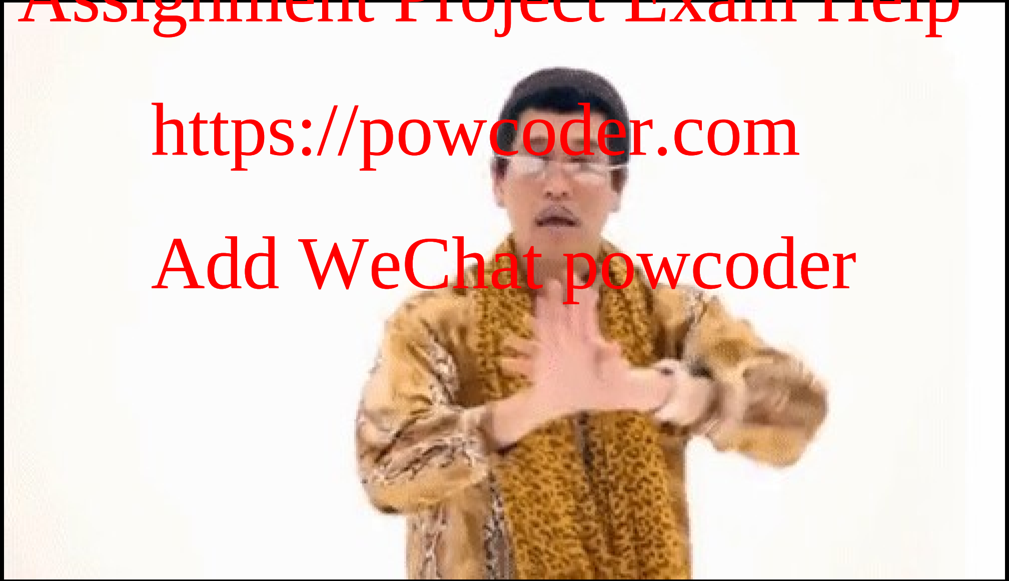
Assignment Project Exam Help

https://powcoder.com

Add WeChat powcoder

WIFI PINEAPPLE

Pen testing device for man-in-the-middle attacks



Assignment Project Exam Help

https://powcoder.com

Add WeChat powcoder

WIFI PINEAPPLE

Pen testing device for man-in-the-middle attacks

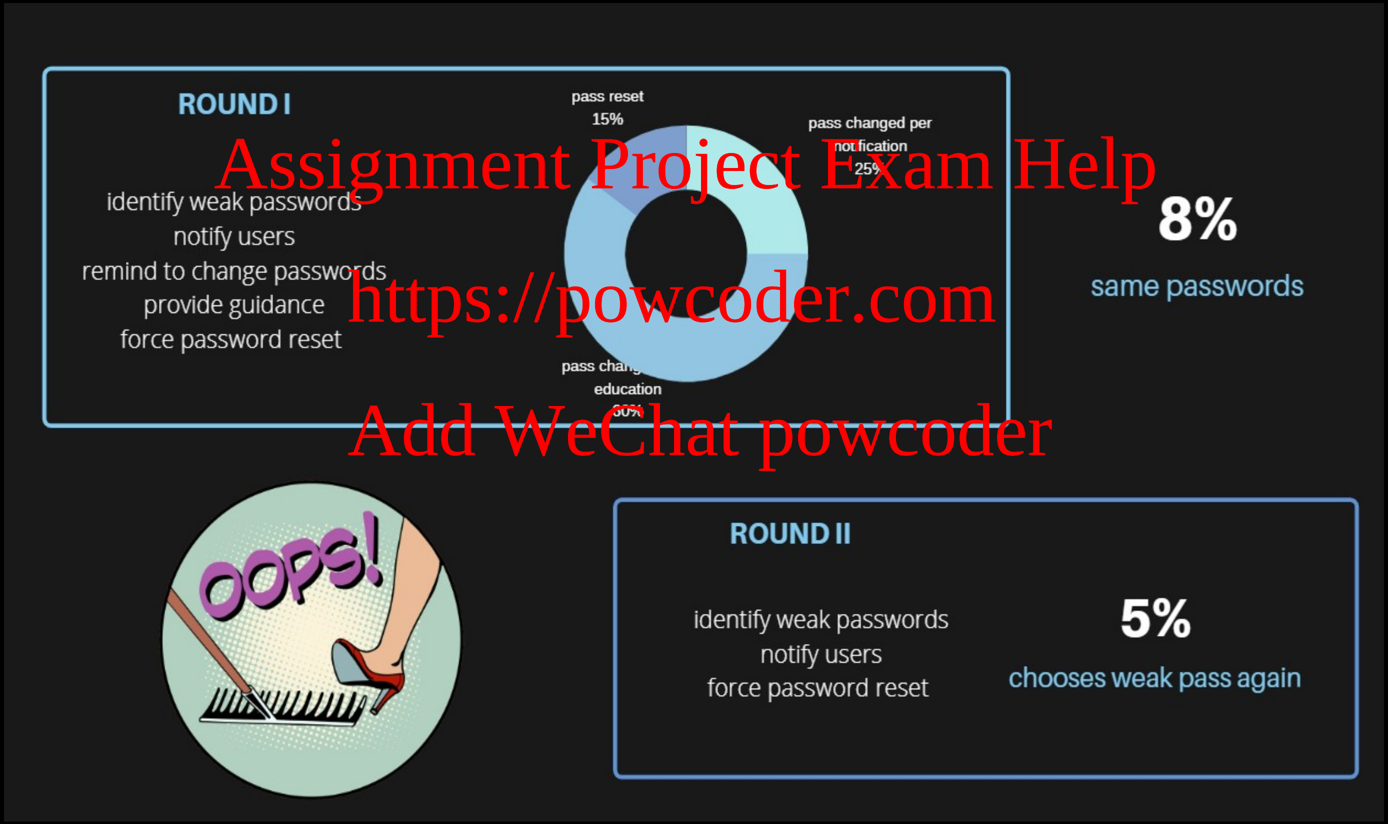
https://www.youtube.com/watch?v=fm-J_IToX5w

Assignment Project Exam Help

https://powcoder.com

Add WeChat powcoder

PASSWORDS



ROUND I

identify weak passwords
notify users
remind to change passwords
provide guidance
force password reset

pass reset 15%
pass changed per notification 25%
pass changed per education 60%
OOPS!

8%
same passwords

ROUND II

identify weak passwords
notify users
force password reset

5%
chooses weak pass again

Assignment Project Exam Help
https://powcoder.com
Add WeChat powcoder

WHAT IS ~~LOVE~~ HASH?

Assignment Project Exam Help

https://powcoder.com

Add WeChat powcoder

One way function

HASHING vs ENCRYPTION

Assignment Project Exam Help

https://powcoder.com

Add WeChat powcoder

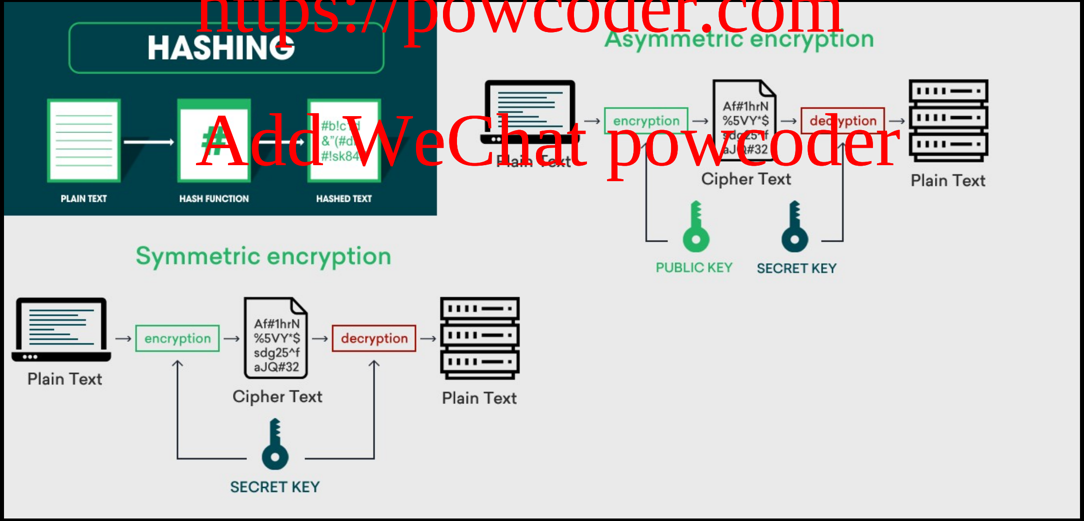
HASHING vs ENCRYPTION

Hash algorithm is based on one-way function. It is practically impossible to revert the result back

Encryption is based on plain text and a key and suppose to have a decryption algorithm.

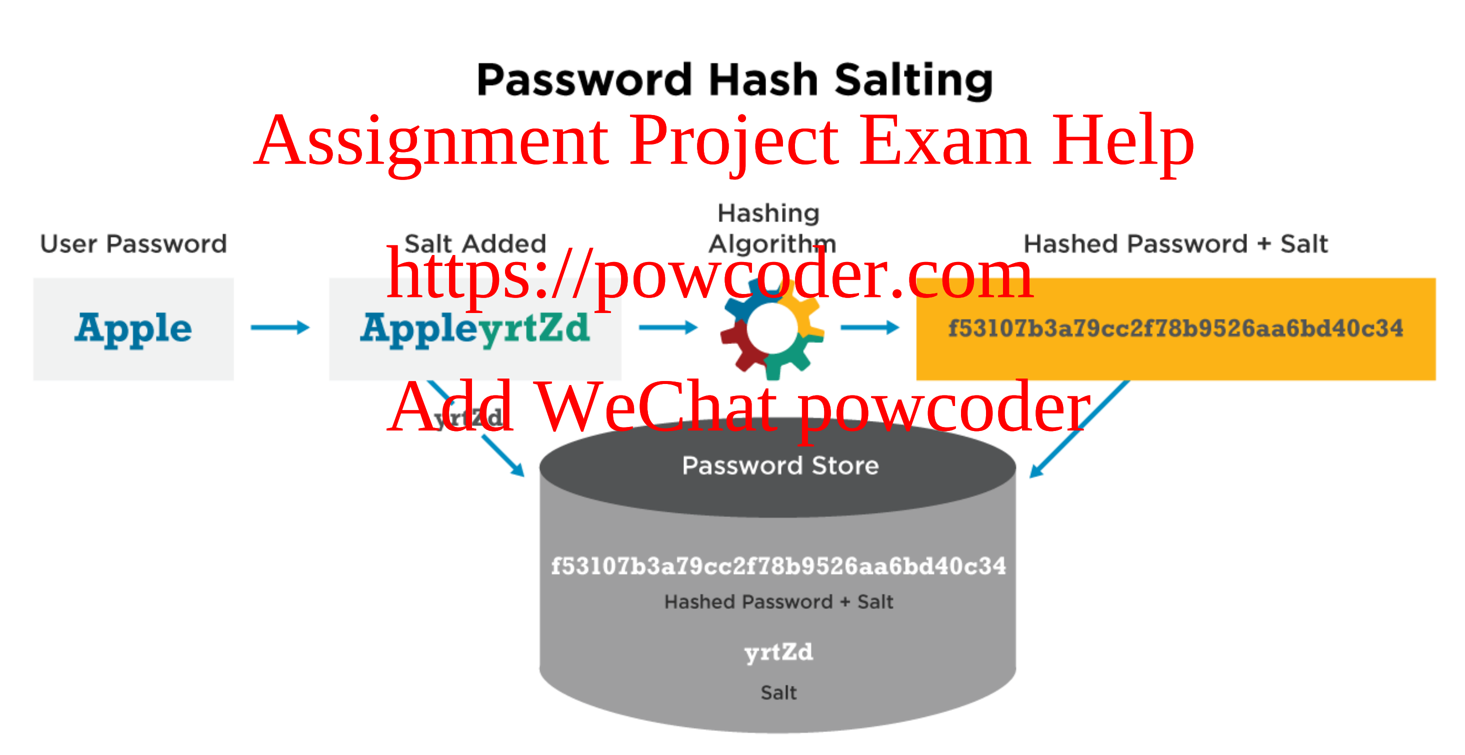
Assignment Project Exam Help

https://powcoder.com



Add WeChat powcoder

PASSWORD HASHES



Assignment Project Exam Help
https://powcoder.com
Add WeChat powcoder

RAINBOW TABLE AND PASSWORDS DBS

https://haveibeenpwned.com/Passwords

Assignment Project Exam Help

passwords obtained from previous data breaches

https://powcoder.com

Add WeChat powcoder

DEMO

https://youtu.be/IchpQBbGbrE

PASSWORD RESETS

- E-Mail
  - Doesn’t matter if I’ve got the user’s inbox
  - Is the reset link generated securely?
  - Can I generate a link securely?
- “Security” Questions
  - Can I get them off a user’s Facebook
  - Can I google the answer?
  - How many attempts do I get to answer these questions?

Password Security is
People Problem

Assignment Project Exam Help
https://powcoder.com
Add WeChat powcoder

2019 NIST PASSWORD GUIDELINES

8 character min (human) overwise 6 character min
* Support at least 64 characters max length
* support All ASCII characters (incl 0x20)
* NO truncation of password when processed
* Allow at least 10 password attempts before lockout
* No SMS for 2FA (one-time password from an app)

Assignment Project Exam Help
https://powcoder.com
Add WeChat powcoder

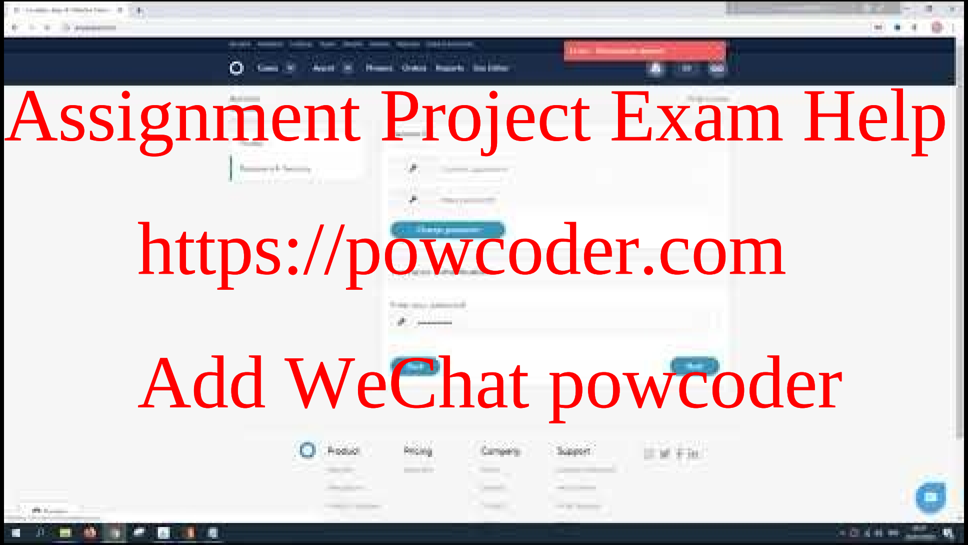
- Check password with known dictionaries
- No complexity requirements
- No password expiration period
- No password hints
- No knowledge-based authentication (no questions)

Few more examples

Assignment Project Exam Help
https://powcoder.com
Add WeChat powcoder

Shout out: 0xed1337

Few more examples



Assignment Project Exam Help

https://powcoder.com

Add WeChat powcoder

Shoutout: T-GOX Channel

How to do Good authentication?

- Good password policy
- Rate limiting
- Not allowing default usernames/passwords
- Not using weak hashing algorithms
- Multi Factor Authentication
- Application registration/forgot password logic

Assignment Project Exam Help
https://powcoder.com
Add WeChat powcoder

READING MATERIAL (REFERENCE)

- Authentication what why and how!! https://github.com/alex996/presentations/blob/master/auth.md

- Shopify Authentication Bypass https://www.youtube.com/watch?v=ZFst3-r-9Lg

- Google CTF https://www.youtube.com/watch?v=HOQzu0SQFWA

Assignment Project Exam Help
https://powcoder.com
Add WeChat powcoder

WEEK 2-3 ASSESSMENT

- If you’re unsure, ask.

Assignment Project Exam Help

https://powcoder.com

Add WeChat powcoder

Please call out if you get stuck.
Support one another, your tutors are here to help!

Assignment Project Exam Help

THANKS FOR LISTENING TO US RANT!

https://powcoder.com

questions? email: /openlearning

Add WeChat powcoder