

Sensitive Data Exposure

Overview

Sensitive Data Exposure involves the unintentional exposure of sensitive data which was not properly protected or cryptographically-secured. If sensitive data is stored in plain text or encrypted with a weak or deprecated encryption algorithm it can easily be recovered following an attack such as SQL injection. For instance, if a password database uses simple hashes to store user passwords and an attacker is somehow able to gain access to the database, the attacker may be able to look up these hashed passwords in something called a rainbow table. A rainbow table is a precomputed table containing the output of cryptographic hash functions, specifically used for cracking password hashes. If the hashed passwords are listed in the rainbow table, the attacker now has a list of viable user passwords.

There is a wide spectrum of encryption algorithms available. In this project, we decided to utilize the following encoding scheme and encryption algorithms in order to test their abilities at preventing Sensitive Data Exposure following an SQL injection.

Base64

Base64 is a binary-to-text encoding scheme designed to transfer data stored in a binary format over channels which support textual data. It is widely used on the Web due to its ability to embed image, sound, HTML and CSS files, and is also commonly used for sending email attachments. It translates binary data represented in an ASCII string format into a radix-64 representation. Base64 is not an encryption algorithm per se - it simply encodes some piece of data into an alternate syntax and it can be decoded by anyone.

Message-Digest Algorithm 5 (MD5)

The MD5 message-digest algorithm is a commonly-used hash function, originally designed to be a secure cryptographic hash for authenticating digital signatures. It is able to process any length of message as input and generate a 128-bit hash (or 'message digest') as output. It is no longer considered to be a secure cryptographic function due its numerous vulnerabilities. For instance, MDS is particularly vulnerable to collision attacks; that is, when two distinct inputs produce identical hashes. It can still, however, be used as a non-cryptographic checksum to verify data integrity and detect unintentional data corruption.

Secure Hash Algorithm 256 (SHA-256)

SHA-256 is a member of the family of Secure Hash Algorithms (SHA), a set of cryptographic hash functions designed by the National Security Agency (NSA). The number '256' which forms part of its name indicates that it produces a hash value of 256 bits. It is a fast and very popular cryptographic hashing function with a wide range of applications, including password hashing in

Linux systems and verification of Bitcoin transactions. SHA-256 is constructed using the Merkle-Damgård structure, a method of building a collision-resistant hash function from a one-way compression function. Although this method of construction makes it secure, it actually makes it vulnerable to length extension attacks.

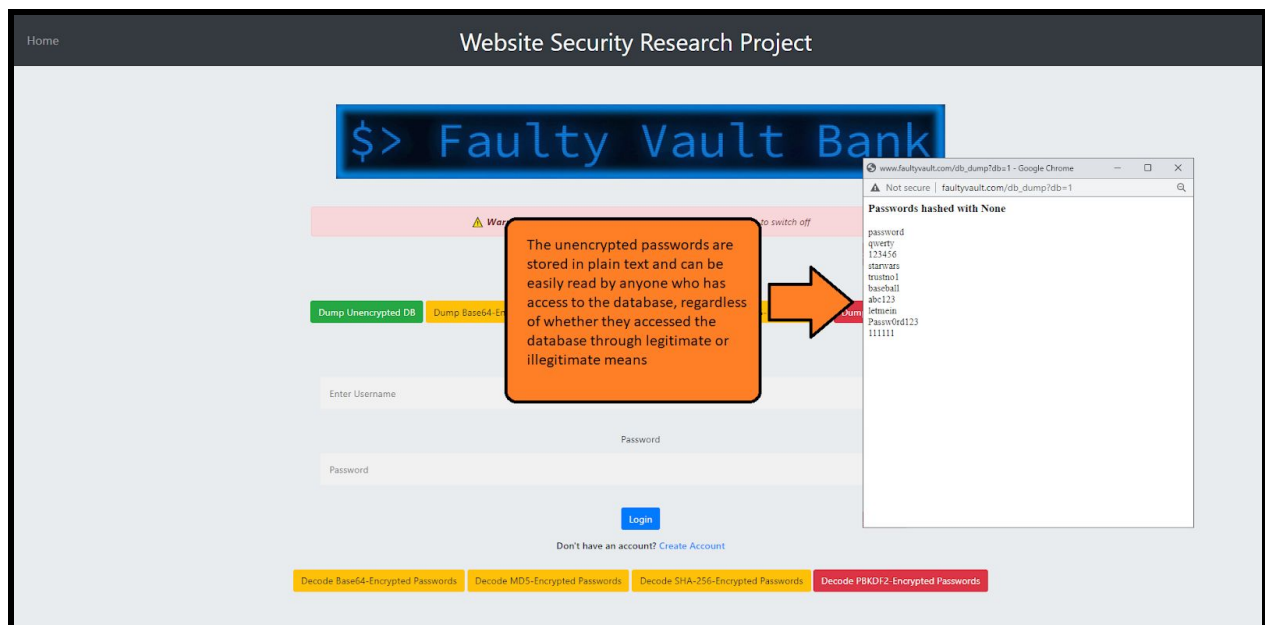
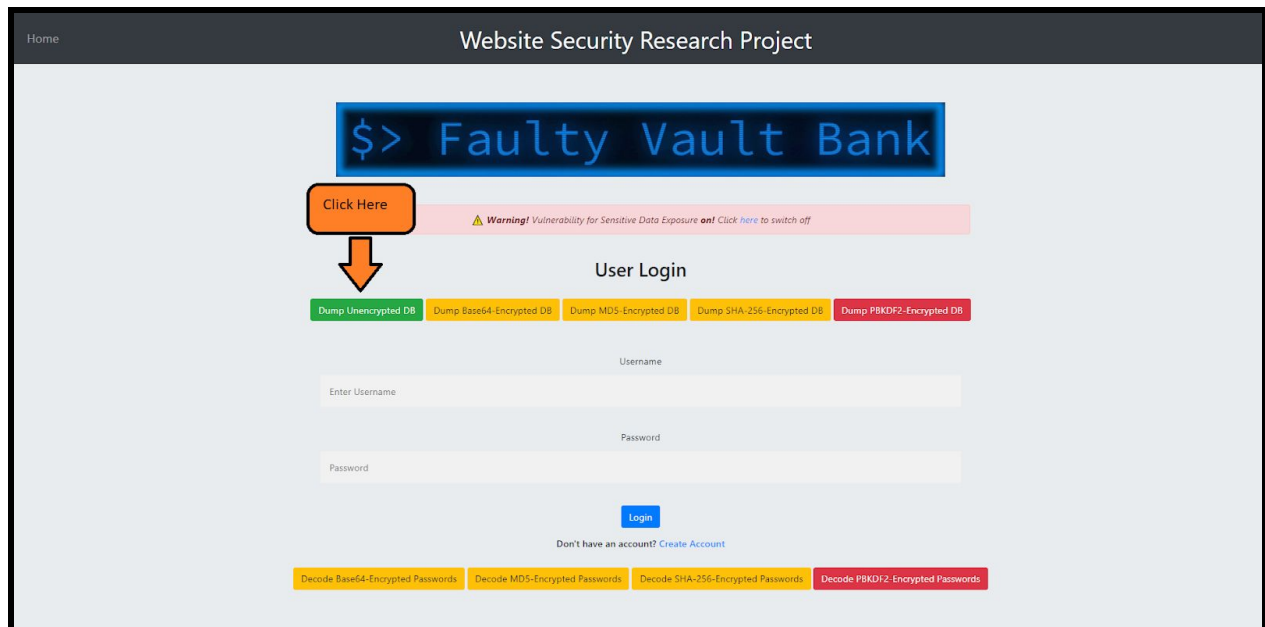
Password-Based Key Derivation Function 2 (PBKDF2)

PBKDF2 is a key derivation function which is part of the RSA Laboratories' Public-Key Cryptography Standards (PKCS) series. RFC 8018 (2017) recommends PBKDF2 for password hashing. PBKDF2 is resistant to dictionary and rainbow table attacks. It utilizes a pseudorandom function such as a hash-based message authentication code (HMAC) and applies this to the inputted password. It then adds a salt value; that is, a random string of data, to the input. It repeats this process over and over again in order to generate a derived key which it uses as its cryptographic key in successive operations. PBKDF2 is slow by design. Fortunately, the additional computational work required to produce the cryptographic key, known as key stretching, makes password cracking much more difficult.

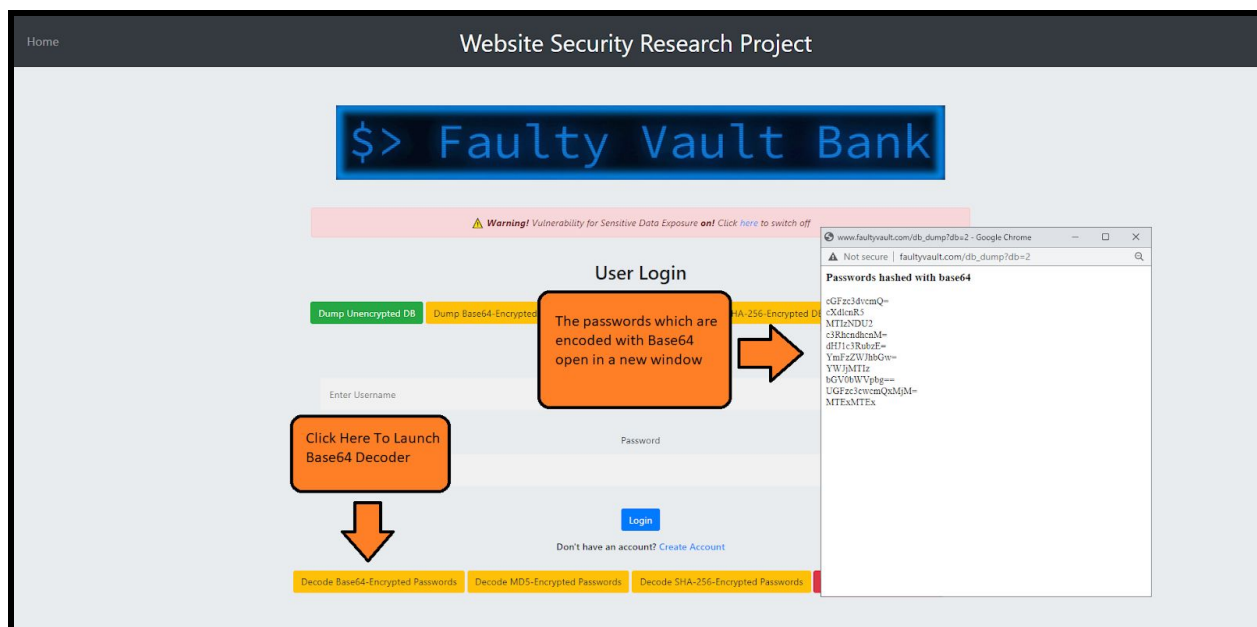
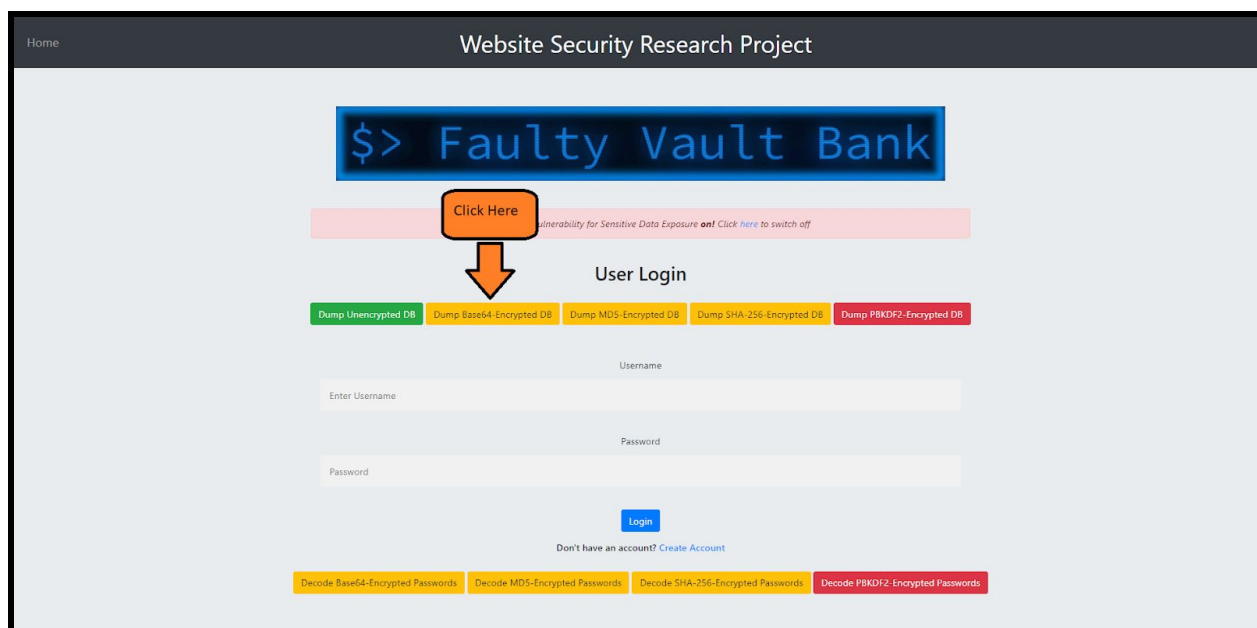
Attempts to Decrypt the Passwords

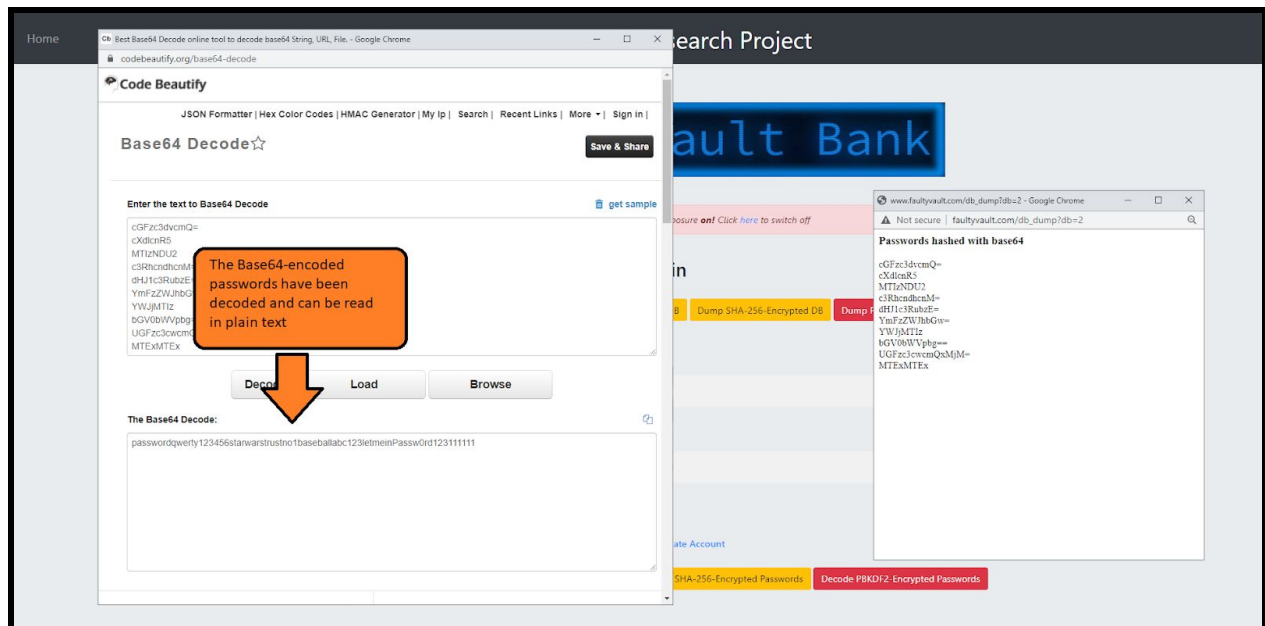
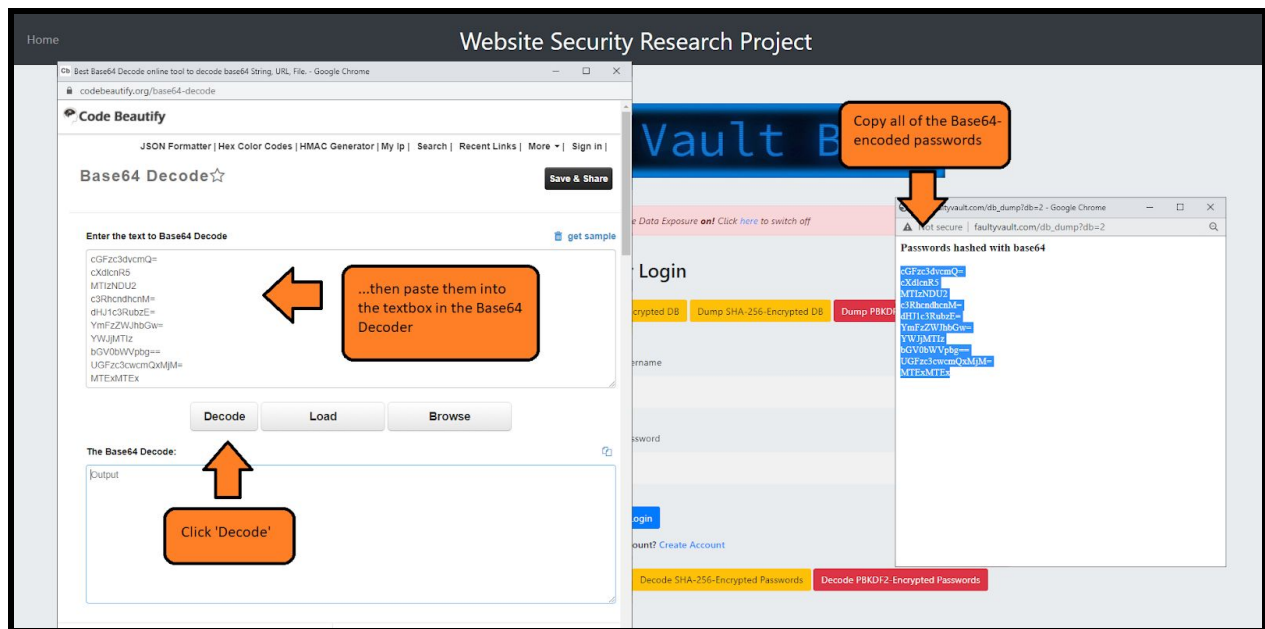
In the following scenario the website's database was dumped following an SQL injection, exposing user passwords. In each case, the passwords are encrypted with different encryption or encoding algorithms, and in one case the passwords stored in plain text. We attempt to crack the passwords.

Unencrypted Passwords Stored in the Database

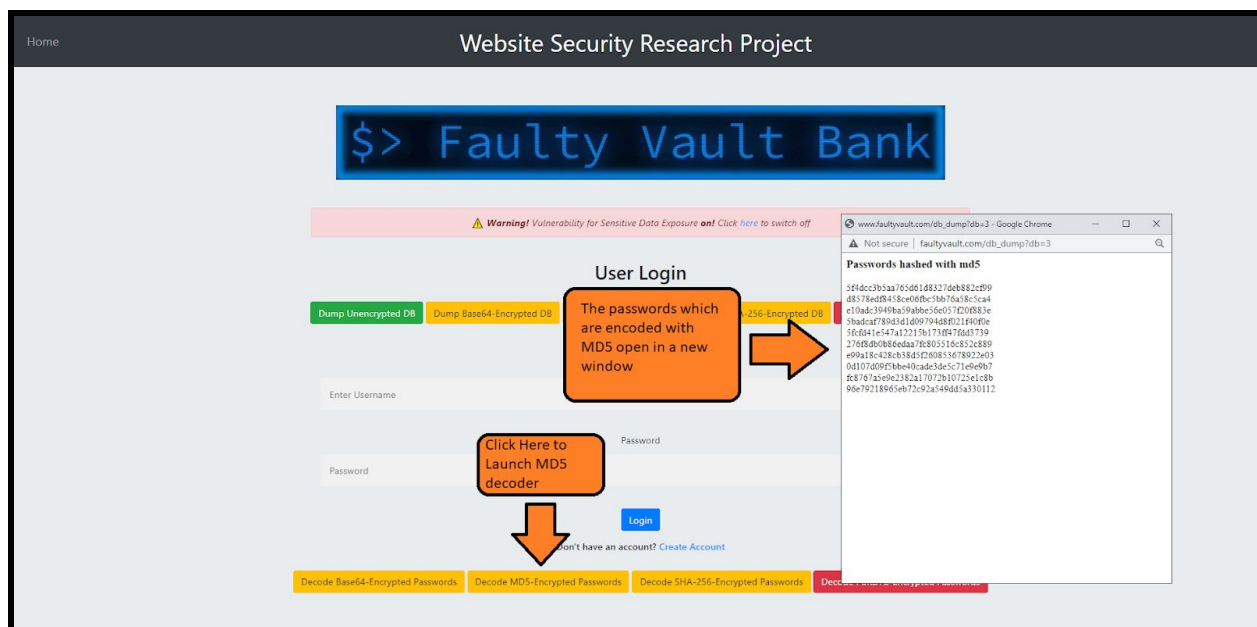
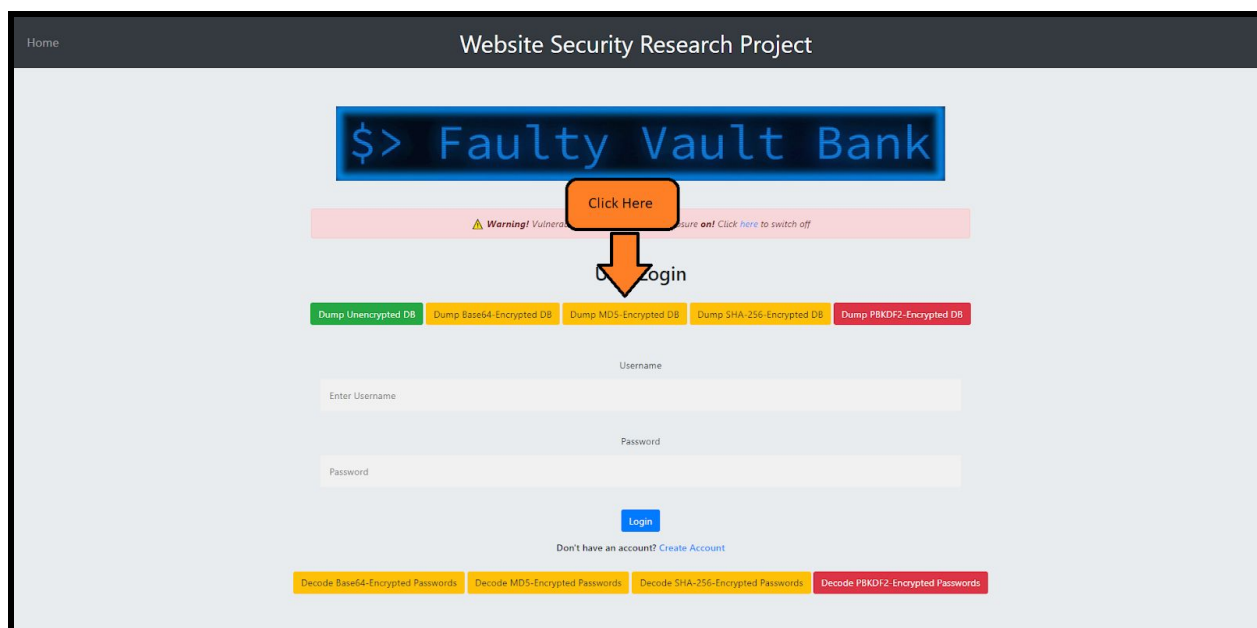


Base-64-Encrypted Passwords Stored in the Database

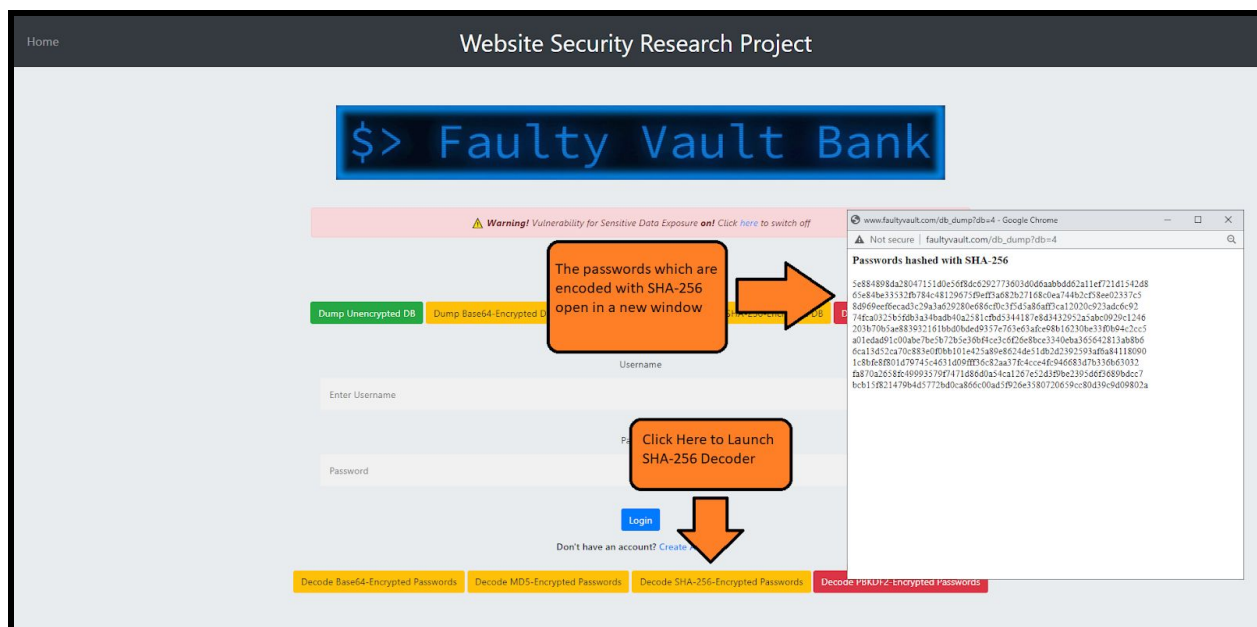
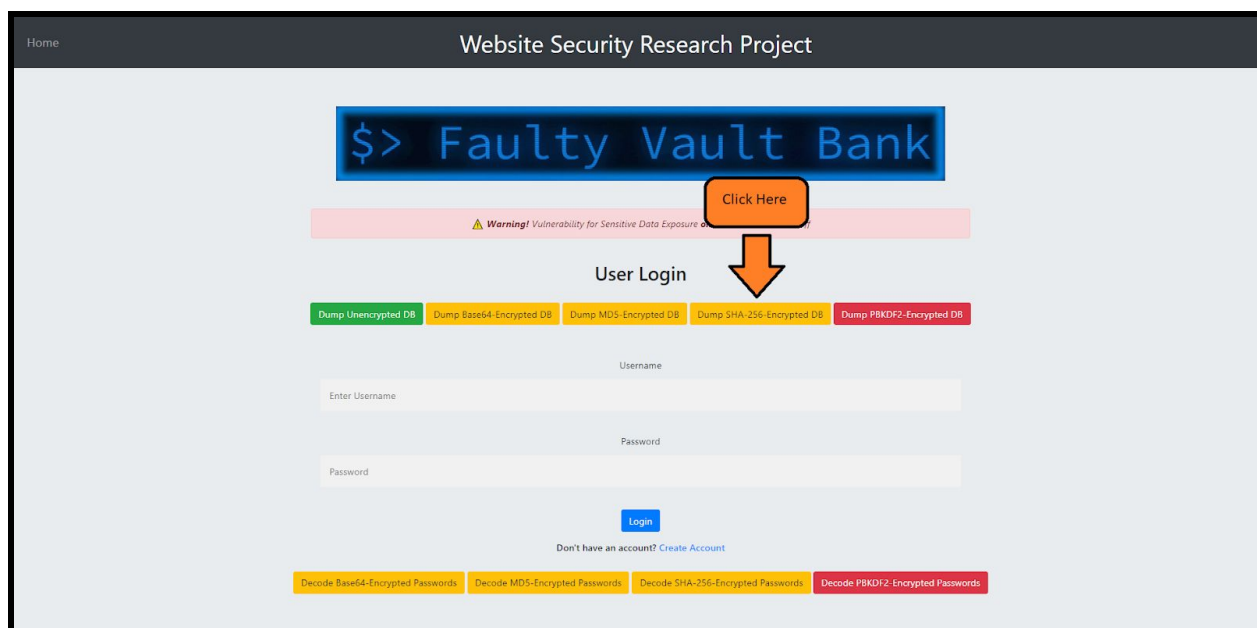




MD5-Encrypted Passwords Stored in the Database



SHA-256-Encrypted Passwords Stored in the Database



Home

Website Security Research Project

CrackStation - Online Password Hash Cracking - MD5, SHA1, Linux, Rainbow Tables, etc. - Google Chrome

crackstation.net

CrackStation

Defuse.ca · Twitter

CrackStation Password Hashing Security Defuse Security

Free Password Hash Cracker

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

5e884898da28047151d0e5f8dc6292773603d06aabbdd62a11e7721d1542d8
65e84be33532b784c48129675f9ef73a682b27168c0ea744b2cf58e02337c5
8d0f69eeffecad3c29a3a629280e68fc3f5d5a8eaff3ca12020c923adcc92
74fc4e12505fd03a34ba0b40a2581c7b05344187d6d5432952a5ab0929c1246
203b70b5a683932161b0b0b0d03576763d3afce90162306c3f0b94c2cc5
a03da491c00abe7be5b7205c30f4cc1d526bce134bea3056a2313ab0b6
kca15d52ca70c885e0f0b101e425a89e624de51db2d2392593af6aa4118090
1c0bf68f08d479745c461d0dff7f36c0a2a3774cc4cf3466d3d7b31063032
f4870a26588e49993579f7471d86da54ca1267e243f9be2395d6f3689bdc7
bcb15f821479b4d5772b0ca866c00ad5f926c3580720659cc8d39c9d09802a

I'm not a robot

reCAPTCHA

Privacy · Terms

Crack Hashes

Supports: LM, NTLM, md4, md5, md5(md5_hex), md5-hex, sha1, sha224, sha256, sha384, sha512, ripemd160, whirlpool, MySQL 4.1+ (sha1sha1_bin), Qubos2, BackupDefaults

Download CrackStation's Wordlist

...then paste them into the textbox in the SHA-256 Decoder

After selecting the reCAPTCHA box, click on 'Crack Hashes'

lt Ba

Copy all of the SHA-256-encoded passwords

www.faultyvault.com?db=4 - Google Chrome

Not secure faultyvault.com/db_dump?db=4

Passwords hashed with SHA-256

5e884898da28047151d0e5f8dc6292773603d06aabbdd62a11e7721d1542d8
65e84be33532b784c48129675f9ef73a682b27168c0ea744b2cf58e02337c5
8d0f69eeffecad3c29a3a629280e68fc3f5d5a8eaff3ca12020c923adcc92
74fc4e12505fd03a34ba0b40a2581c7b05344187d6d5432952a5ab0929c1246
203b70b5a683932161b0b0b0d03576763d3afce90162306c3f0b94c2cc5
a03da491c00abe7be5b7205c30f4cc1d526bce134bea3056a2313ab0b6
kca15d52ca70c885e0f0b101e425a89e624de51db2d2392593af6aa4118090
1c0bf68f08d479745c461d0dff7f36c0a2a3774cc4cf3466d3d7b31063032
f4870a26588e49993579f7471d86da54ca1267e243f9be2395d6f3689bdc7
bcb15f821479b4d5772b0ca866c00ad5f926c3580720659cc8d39c9d09802a

SHA-256-Encoded DB Dump

Decoded Passwords

Decode PKDIZ-Encoded Passwords

Home

Website Security Research Project

CrackStation - Online Password Hash Cracking - MD5, SHA1, Rainbow Tables, etc. - Google Chrome

crackstation.net

CrackStation

Defuse.ca · Twitter

CrackStation Password Hashing Security Defuse Security

Free Password Hash Cracker

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

I'm not a robot

reCAPTCHA

Privacy · Terms

Crack Hashes

Supports: LM, NTLM, md4, md5, md5(md5_hex), md5-hex, sha1, sha224, sha256, sha384, sha512, ripemd160, whirlpool, MySQL 4.1+ (sha1sha1_bin), Qubos2, BackupDefaults

The SHA-256-encoded passwords have been decoded and can be read in plain text

t Bank

www.faultyvault.com/db_dump/db=4 - Google Chrome

Not secure faultyvault.com/db_dump?db=4

Passwords hashed with SHA-256

5e884898da28047151d0e5f8dc6292773603d06aabbdd62a11e7721d1542d8
65e84be33532b784c48129675f9ef73a682b27168c0ea744b2cf58e02337c5
8d0f69eeffecad3c29a3a629280e68fc3f5d5a8eaff3ca12020c923adcc92
74fc4e12505fd03a34ba0b40a2581c7b05344187d6d5432952a5ab0929c1246
203b70b5a683932161b0b0b0d03576763d3afce90162306c3f0b94c2cc5
a03da491c00abe7be5b7205c30f4cc1d526bce134bea3056a2313ab0b6
kca15d52ca70c885e0f0b101e425a89e624de51db2d2392593af6aa4118090
1c0bf68f08d479745c461d0dff7f36c0a2a3774cc4cf3466d3d7b31063032
f4870a26588e49993579f7471d86da54ca1267e243f9be2395d6f3689bdc7
bcb15f821479b4d5772b0ca866c00ad5f926c3580720659cc8d39c9d09802a

Encrypted DB Dump

Decoded Passwords

Decode PKDIZ-Encoded Passwords

Hash	Type	Result
5e884898da28047151d0e5f8dc6292773603d06aabbdd62a11e7721d1542d8	SHA-256	Password
65e84be33532b784c48129675f9ef73a682b27168c0ea744b2cf58e02337c5	SHA-256	admin
8d0f69eeffecad3c29a3a629280e68fc3f5d5a8eaff3ca12020c923adcc92	SHA-256	123456
74fc4e12505fd03a34ba0b40a2581c7b05344187d6d5432952a5ab0929c1246	SHA-256	stars
203b70b5a683932161b0b0b0d03576763d3afce90162306c3f0b94c2cc5	SHA-256	trustno1
a03da491c00abe7be5b7205c30f4cc1d526bce134bea3056a2313ab0b6	SHA-256	basel1
kca15d52ca70c885e0f0b101e425a89e624de51db2d2392593af6aa4118090	SHA-256	ab0123
1c0bf68f08d479745c461d0dff7f36c0a2a3774cc4cf3466d3d7b31063032	SHA-256	1qaz!@WSX
f4870a26588e49993579f7471d86da54ca1267e243f9be2395d6f3689bdc7	SHA-256	Password123
bcb15f821479b4d5772b0ca866c00ad5f926c3580720659cc8d39c9d09802a	SHA-256	111111

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

PBKDF2-Encrypted Passwords Stored in the Database

The image displays two screenshots of the 'Faulty Vault Bank' website, illustrating the process of accessing and decoding PBKDF2-encrypted passwords.

Top Screenshot: The website header shows 'Home' and 'Website Security Research Project'. The main banner reads '\$> Faulty Vault Bank'. A warning message states: 'Warning! Vulnerability for Sensitive Data Exposure on! Click here to switch off'. A 'Click Here' button with a downward arrow points to the 'User Login' section. Below the login form, there are five buttons: 'Dump Unencrypted DB', 'Dump Base64-Encrypted DB', 'Dump MD5-Encrypted DB', 'Dump SHA-256-Encrypted DB', and 'Dump PBKDF2-Encrypted DB'. The 'Dump PBKDF2-Encrypted DB' button is highlighted in red. Below the login form, there are four buttons: 'Decode Base64-Encrypted Passwords', 'Decode MD5-Encrypted Passwords', 'Decode SHA-256-Encrypted Passwords', and 'Decode PBKDF2-Encrypted Passwords'. The 'Decode PBKDF2-Encrypted Passwords' button is highlighted in red.

Bottom Screenshot: This screenshot shows the same website with an additional browser window open. The browser window title is 'www.faultyvault.com/db_dump?db=5 - Google Chrome'. The address bar shows 'faultyvault.com/db_dump?db=5'. The page content shows 'Passwords hashed with PBKDF2' followed by a long list of hexadecimal strings. An orange box with the text 'The passwords which are encoded in PBKDF2 open in a new window' has an arrow pointing to the browser window. Another orange box with the text 'Click Here to Launch PBKDF2 Decoder' has an arrow pointing to the 'Decode PBKDF2-Encrypted Passwords' button.

Website Security Research Project

CrackStation - Online Password Hash Cracking - MD5, SHA1, Linux, Rainbow Tables, etc. - Google Chrome

crackstation.net

CrackStation

Defuse.ca · Twitter

CrackStation Password Hashing Security Defuse Security

Free Password Hash Cracker

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

```
0b1ba3faecf01679d521413f9b5fed20473c7f06df9e918150b18ab0917fb2
d271b5263636d5b7f638135d7ead0be2daf3e8951a10e29845e7851834522
7276774cfb0d56eb2f0ca986b32566b150e8427f0929f04c947f4f4ccc
7f47a4fa8a56ab16f263cf5dab01c630b20f7f186e4408f95f0c94a774b233b
599d75e68d193e2a0ff0676124b61a74ba860527fda2515339d2030e2e436c
504ac1c085a546780f01f75d6c372ba031f53106c2600c14834a005af93
1b78299f27f6d8a0681a44f83424303fca20b0d4c928a8f229fd151eef
1b1845e6c391409869814a1354ad21986c5a44c71665a7b65f63b6ef
73d6c1fed682d61c905c3d934023d5f186b0950e6340546663d5df354d1
43014d2fe04d6cf0fabb1665d3039eebb0a7ea99fa363dab7ada7152aef
```

I'm not a robot

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-hlf, sha1, sha224, sha256, sha384, sha512, ripemd160, sha3, sha3-224, sha3-256, sha3-384, sha3-512, blake2b, blake2s, blake2sp, blake2bp, blake2bp256, blake2bp512, blake2bp1024, blake2bp2048, blake2bp4096, blake2bp8192, blake2bp16384, blake2bp32768, blake2bp65536, blake2bp131072, blake2bp262144, blake2bp524288, blake2bp1048576, blake2bp2097152, blake2bp4194304, blake2bp8388608, blake2bp16777216, blake2bp33554432, blake2bp67108864, blake2bp134217728, blake2bp268435456, blake2bp536870912, blake2bp1073741824, blake2bp2147483648, blake2bp4294967296, blake2bp8589934592, blake2bp17179869184, blake2bp34359738368, blake2bp68719476736, blake2bp137438953472, blake2bp27487790688, blake2bp54975581376, blake2bp109951162752, blake2bp219902325504, blake2bp439804651008, blake2bp879609302016, blake2bp1759218040032, blake2bp3518436080064, blake2bp7036872160128, blake2bp14073744320256, blake2bp28147488640512, blake2bp56294977281024, blake2bp1125899545442048, blake2bp2251799090884096, blake2bp45035981817984, blake2bp90071963635968, blake2bp180143927271936, blake2bp360287854543872, blake2bp720575709087776, blake2bp14411514181555552, blake2bp28823028363111104, blake2bp57646056726222208, blake2bp115292113444444448, blake2bp230584224488888896, blake2bp461168448977777792, blake2bp922336897955555584, blake2bp1844673795911111168, blake2bp3689347591822222336, blake2bp7378695183844444672, blake2bp14757390376768888896, blake2bp2951478075353777792, blake2bp5902956150711555544, blake2bp118059123103431111088, blake2bp2361182462068622222176, blake2bp472236492413724444432, blake2bp94447298482748888864, blake2bp18889459697497777728, blake2bp37778919394995555552, blake2bp75557839799911111104, blake2bp15111567999922222208, blake2bp3022313999944444432, blake2bp6044627999988888864, blake2bp12089245999977777728, blake2bp24178491999955555552, blake2bp48356983999911111104, blake2bp96713967999922222208, blake2bp19342795999944444432, blake2bp38685591999988888864, blake2bp77371183999977777728, blake2bp154742367999955555552, blake2bp309484735999911111104, blake2bp618969471999922222208, blake2bp1237939895999944444432, blake2bp2475879791999988888864, blake2bp4951759583999977777728, blake2bp9903519167999955555552, blake2bp1980703835999911111104, blake2bp3961407671999922222208, blake2bp7922815343999944444432, blake2bp1584563068999988888864, blake2bp316912617999977777728, blake2bp633825235999955555552, blake2bp1267650471999911111104, blake2bp2535300943999922222208, blake2bp5070601887999944444432, blake2bp1014120377999988888864, blake2bp202824075999977777728, blake2bp405648151999955555552, blake2bp811296303999911111104, blake2bp162259267999922222208, blake2bp324518535999944444432, blake2bp649037071999988888864, blake2bp129807443999977777728, blake2bp259614887999955555552, blake2bp519229775999911111104, blake2bp103845951999922222208, blake2bp207691903999944444432, blake2bp415383807999988888864, blake2bp830767615999977777728, blake2bp166153523999955555552, blake2bp332307047999911111104, blake2bp664614095999922222208, blake2bp1329228011999944444432, blake2bp265845603999988888864, blake2bp531691207999977777728, blake2bp1063382415999955555552, blake2bp2126764831999911111104, blake2bp4253529663999922222208, blake2bp850705931999944444432, blake2bp1701411867999988888864, blake2bp340282373999977777728, blake2bp680564747999955555552, blake2bp136112954999911111104, blake2bp27222590999922222208, blake2bp54445181999944444432, blake2bp10889363999988888864, blake2bp21778727999977777728, blake2bp43557455999955555552, blake2bp87114911999911111104, blake2bp174228223999922222208, blake2bp348456447999944444432, blake2bp696912895999988888864, blake2bp13938257999977777728, blake2bp27876515999955555552, blake2bp55753031999911111104, blake2bp111506063999922222208, blake2bp223012127999944444432, blake2bp446024255999988888864, blake2bp892048511999977777728, blake2bp1784097031999955555552, blake2bp356819407999911111104, blake2bp713638815999922222208, blake2bp1427277631999944444432, blake2bp285455527999988888864, blake2bp570911055999977777728, blake2bp114182211999955555552, blake2bp228364423999911111104, blake2bp456728847999922222208, blake2bp913457695999944444432, blake2bp182691531999988888864, blake2bp365383063999977777728, blake2bp730766127999955555552, blake2bp146153225999911111104, blake2bp292306451999922222208, blake2bp584612903999944444432, blake2bp1169224807999988888864, blake2bp233844961999977777728, blake2bp467689923999955555552, blake2bp935379847999911111104, blake2bp18707596999922222208, blake2bp37415193999944444432, blake2bp74830387999988888864, blake2bp149660775999977777728, blake2bp299321551999955555552, blake2bp598643103999911111104, blake2bp119728663999922222208, blake2bp239457327999944444432, blake2bp478914655999988888864, blake2bp957829311999977777728, blake2bp191565863999955555552, blake2bp383131727999911111104, blake2bp766263455999922222208, blake2bp153250691999944444432, blake2bp306501383999988888864, blake2bp613002767999977777728, blake2bp122600551999955555552, blake2bp245201103999911111104, blake2bp490402207999922222208, blake2bp980804415999944444432, blake2bp196160883999988888864, blake2bp392321767999977777728, blake2bp784643531999955555552, blake2bp156928703999911111104, blake2bp313857407999922222208, blake2bp627714815999944444432, blake2bp125542883999988888864, blake2bp251085767999977777728, blake2bp50217153999955555552, blake2bp100434307999911111104, blake2bp200868615999922222208, blake2bp40173723999944444432, blake2bp803474463999988888864, blake2bp160694895999977777728, blake2bp321389791999955555552, blake2bp642779583999911111104, blake2bp128555917999922222208, blake2bp257111835999944444432, blake2bp514223671999988888864, blake2bp102844735999977777728, blake2bp205689471999955555552, blake2bp411378943999911111104, blake2bp822757887999922222208, blake2bp164551577999944444432, blake2bp329103155999988888864, blake2bp658206311999977777728, blake2bp131641263999955555552, blake2bp263282527999911111104, blake2bp526565055999922222208, blake2bp105313011999944444432, blake2bp210626023999988888864, blake2bp421252047999977777728, blake2bp842504095999955555552, blake2bp16850081999911111104, blake2bp33700163999922222208, blake2bp67400327999944444432, blake2bp134800655999988888864, blake2bp269601311999977777728, blake2bp53920263999955555552, blake2bp107840527999911111104, blake2bp215681055999922222208, blake2bp431362111999944444432, blake2bp86272423999988888864, blake2bp172544847999977777728, blake2bp345089695999955555552, blake2bp6901793999911111104, blake2bp13803587999922222208, blake2bp27607175999944444432, blake2bp55214355999988888864, blake2bp110428711999977777728, blake2bp220857423999955555552, blake2bp441714847999911111104, blake2bp883429695999922222208, blake2bp176685931999944444432, blake2bp353371863999988888864, blake2bp706743727999977777728, blake2bp141347555999955555552, blake2bp282695103999911111104, blake2bp565390207999922222208, blake2bp113078041999944444432, blake2bp226156083999988888864, blake2bp452312167999977777728, blake2bp90462433999955555552, blake2bp180924867999911111104, blake2bp361849735999922222208, blake2bp723699471999944444432, blake2bp144739895999988888864, blake2bp289479791999977777728, blake2bp578959583999955555552, blake2bp115791196999911111104, blake2bp2315823999922222208, blake2bp4631647999944444432, blake2bp9263295999988888864, blake2bp18525911999977777728, blake2bp37051823999955555552, blake2bp74103647999911111104, blake2bp148207295999922222208, blake2bp2964145999944444432, blake2bp5928291999988888864, blake2bp11856583999977777728, blake2bp23713167999955555552, blake2bp47426335999911111104, blake2bp94852671999922222208, blake2bp18970543999944444432, blake2bp37941087999988888864, blake2bp75882175999977777728, blake2bp15176171999955555552, blake2bp30352343999911111104, blake2bp60704687999922222208, blake2bp121409375999944444432, blake2bp24281875999988888864, blake2bp48563751999977777728, blake2bp97127503999955555552, blake2bp19425507999911111104, blake2bp38851015999922222208, blake2bp77702031999944444432, blake2bp15540407999988888864, blake2bp31080815999977777728, blake2bp62161631999955555552, blake2bp124323263999911111104, blake2bp24864651999922222208, blake2bp49729303999944444432, blake2bp99458607999988888864, blake2bp19891721999977777728, blake2bp39783443999955555552, blake2bp79566887999911111104, blake2bp15913377999922222208, blake2bp31826755999944444432, blake2bp63653511999988888864, blake2bp127307031999977777728, blake2bp254614063999955555552, blake2bp509228127999911111104, blake2bp101845627999922222208, blake2bp203691255999944444432, blake2bp407382511999988888864, blake2bp814765023999977777728, blake2bp162953047999955555552, blake2bp325906095999911111104, blake2bp6518121999922222208, blake2bp13036243999944444432, blake2bp26072487999988888864, blake2bp52144975999977777728, blake2bp10428991999955555552, blake2bp20857983999911111104, blake2bp41715967999922222208, blake2bp83431935999944444432, blake2bp16686387999988888864, blake2bp33372775999977777728, blake2bp66745551999955555552, blake2bp133491103999911111104, blake2bp266982207999922222208, blake2bp53396441999944444432, blake2bp106792883999988888864, blake2bp213585767999977777728, blake2bp42717153999955555552, blake2bp85434307999911111104, blake2bp170868615999922222208, blake2bp34173723999944444432, blake2bp683474463999988888864, blake2bp136694895999977777728, blake2bp273389791999955555552, blake2bp546779583999911111104, blake2bp109355917999922222208, blake2bp218711835999944444432, blake2bp437423671999988888864, blake2bp87484735999977777728, blake2bp174969595999955555552, blake2bp3499391999911111104, blake2bp6998783999922222208, blake2bp139975663999944444432, blake2bp279951327999988888864, blake2bp559902655999977777728, blake2bp111980527999955555552, blake2bp223961055999911111104, blake2bp447922111999922222208, blake2bp89584423999944444432, blake2bp179168867999988888864, blake2bp35833771999977777728, blake2bp71667543999955555552, blake2bp143327887999911111104, blake2bp28665577999922222208, blake2bp57331155999944444432, blake2bp114662311999988888864, blake2bp22932423999977777728, blake2bp45864847999955555552, blake2bp91729695999911111104, blake2bp18345391999922222208, blake2bp36690783999944444432, blake2bp73381567999988888864, blake2bp14676313999977777728, blake2bp29352627999955555552, blake2bp58705255999911111104, blake2bp117410511999922222208, blake2bp23482103999944444432, blake2bp46964207999988888864, blake2bp93928415999977777728, blake2bp18784831999955555552, blake2bp37569663999911111104, blake2bp75139327999922222208, blake2bp150278655999944444432, blake2bp30055731999988888864, blake2bp60111463999977777728, blake2bp120222867999955555552, blake2bp24044573999911111104, blake2bp48089147999922222208, blake2bp96178295999944444432, blake2bp19235591999988888864, blake2bp38471183999977777728, blake2bp76942367999955555552, blake2bp15384735999911111104, blake2bp30769471999922222208, blake2bp61538943999944444432, blake2bp12307787999988888864, blake2bp24615575999977777728, blake2bp49231151999955555552, blake2bp98462303999911111104, blake2bp196924607999922222208, blake2bp39384921999944444432, blake2bp78769843999988888864, blake2bp157539687999977777728, blake2bp31507937999955555552, blake2bp63015875999911111104, blake2bp12603175999922222208, blake2bp25206351999944444432, blake2bp50412703999988888864, blake2bp100825467999977777728, blake2bp20165093999955555552, blake2bp40330187999911111104, blake2bp80660375999922222208, blake2bp16132075999944444432, blake2bp32264151999988888864, blake2bp64528303999977777728, blake2bp129056607999955555552, blake2bp25811321999911111104, blake2bp51622643999922222208, blake2bp10324527999944444432, blake2bp20649055999988888864, blake2bp41298111999977777728, blake2bp82596223999955555552, blake2bp165192447999911111104, blake2bp3303848999922222208, blake2bp6607697999944444432, blake2bp13215395999988888864, blake2bp26430791999977777728, blake2bp52861583999955555552, blake2bp105723767999911111104, blake2bp21144753999922222208, blake2bp42289507999944444432, blake2bp84579015999988888864, blake2bp16915803999977777728, blake2bp33831607999955555552, blake2bp67663215999911111104, blake2bp13532643999922222208, blake2bp27065287999944444432, blake2bp54130575999988888864, blake2bp10826115999977777728, blake2bp21652231999955555552, blake2bp43304463999911111104, blake2bp86608927999922222208, blake2bp17321685999944444432, blake2bp34643371999988888864, blake2bp69286743999977777728, blake2bp138573487999955555552, blake2bp27714697999911111104, blake2bp55429395999922222208, blake2bp1108587999944444432, blake2bp2217175999988888864, blake2bp4434351999977777728, blake2bp8868703999955555552, blake2bp17737407999911111104, blake2bp35474815999922222208, blake2bp70949631999944444432, blake2bp14189927999988888864, blake2bp28379855999977777728, blake2bp56759711999955555552, blake2bp113519427999911111104, blake2bp22703885999922222208, blake2bp45407771999944444432, blake2bp90815543999988888864, blake2bp18163087999977777728, blake2bp36326175999955555552, blake2bp72652351999911111104, blake2bp14530471999922222208, blake2bp29060943999944444432, blake2bp58121887999988888864, blake2bp116243767999977777728, blake2bp23248753999955555552, blake2bp46497507999911111104, blake2bp92995015999922222208, blake2bp18599003999944444432, blake2bp37198007999988888864, blake2bp74396015999977777728, blake2bp148792031999955555552, blake2bp29758407999911111104, blake2bp59516815999922222208, blake2bp11903363999944444432, blake2bp23806727999988888864, blake2bp47613455999977777728, blake2bp95226911999955555552, blake2bp19045383999911111104, blake2bp38090767999922222208, blake2bp76181535999944444432, blake2bp15236307999988888864, blake2bp30472615999977777728, blake2bp60945231999955555552, blake2bp121730467999911111104, blake2bp24346093999922222208, blake2bp48692187999944444432, blake2bp97384375999988888864, blake2bp19476875999977777728, blake2bp38953751999955555552, blake2bp77907503999911111104, blake2bp15581507999922222208, blake2bp31163015999944444432, blake2bp62326031999988888864, blake2bp124652063999977777728, bl

Hardening Website

It is important to identify which data in your web application could be classified as sensitive and treat it accordingly, taking into account the relevant privacy laws and regulatory requirements. Sensitive data should not be stored or cached unnecessarily and should be safely discarded by the application or browser as soon as feasibly possible. Furthermore, sensitive data should never be stored or transmitted in plain text. All data in transit should be encrypted in accordance with a secure protocol such as TLS.

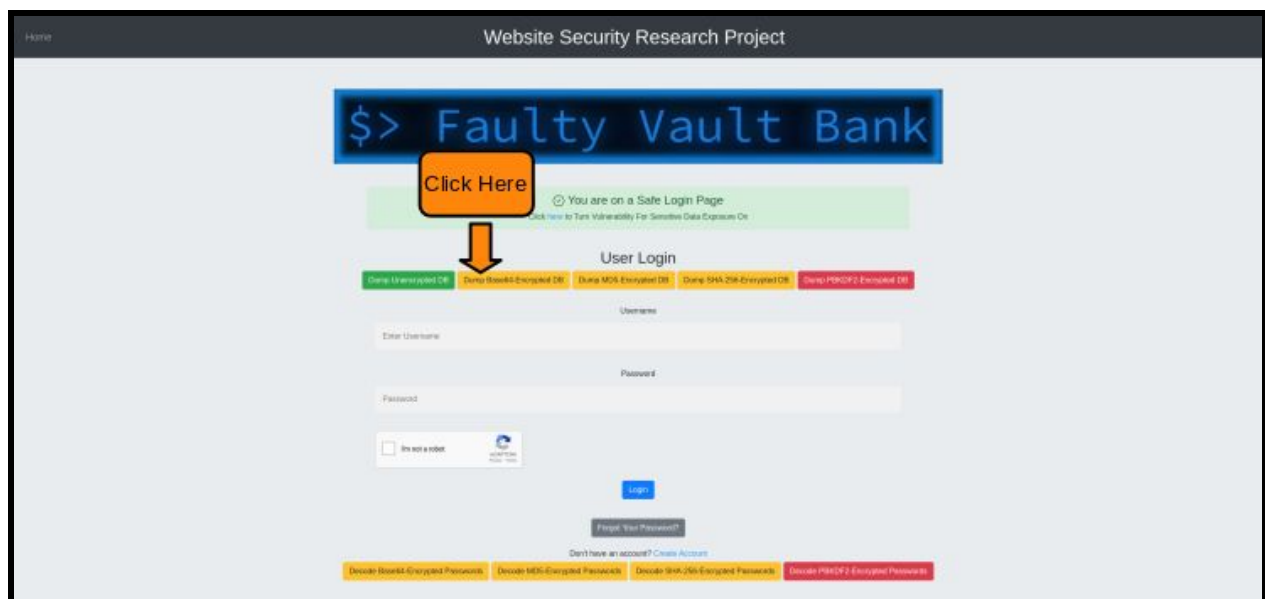
The best strategy of defense against sensitive data exposure is one which is multi-tiered. In addition to the above, implementation of a strong password policy plus encryption of stored passwords with a secure salted hashing function such as PBKDF2 is an effective way to safeguard sensitive data.

Attempts to Decrypt the Passwords Following Website Hardening

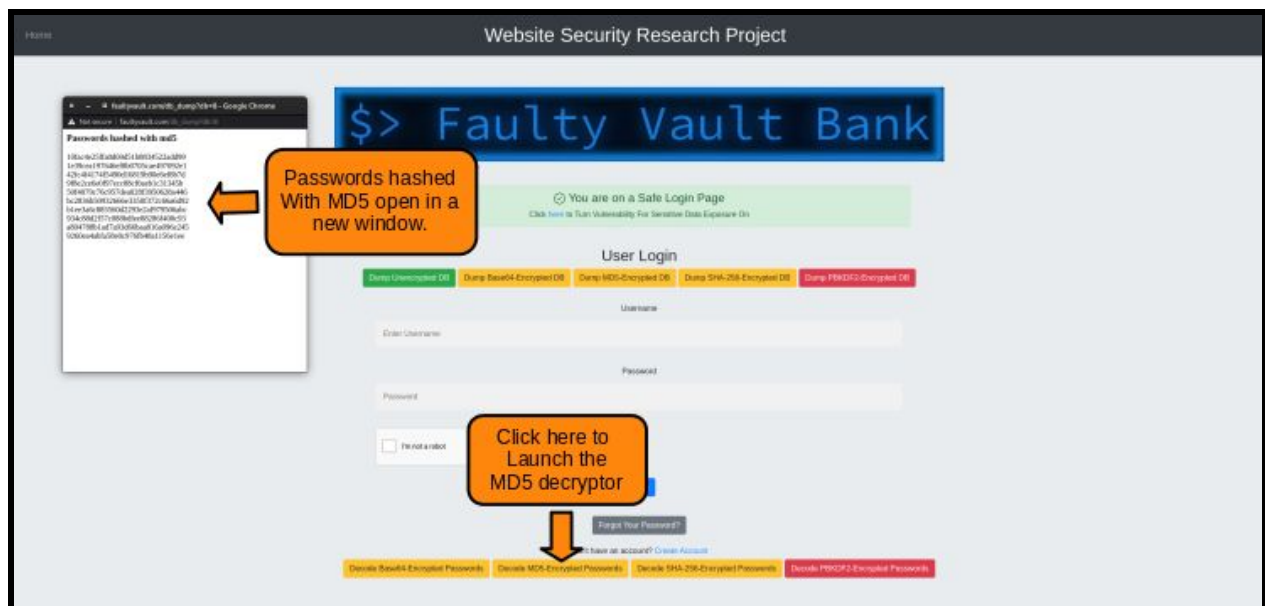
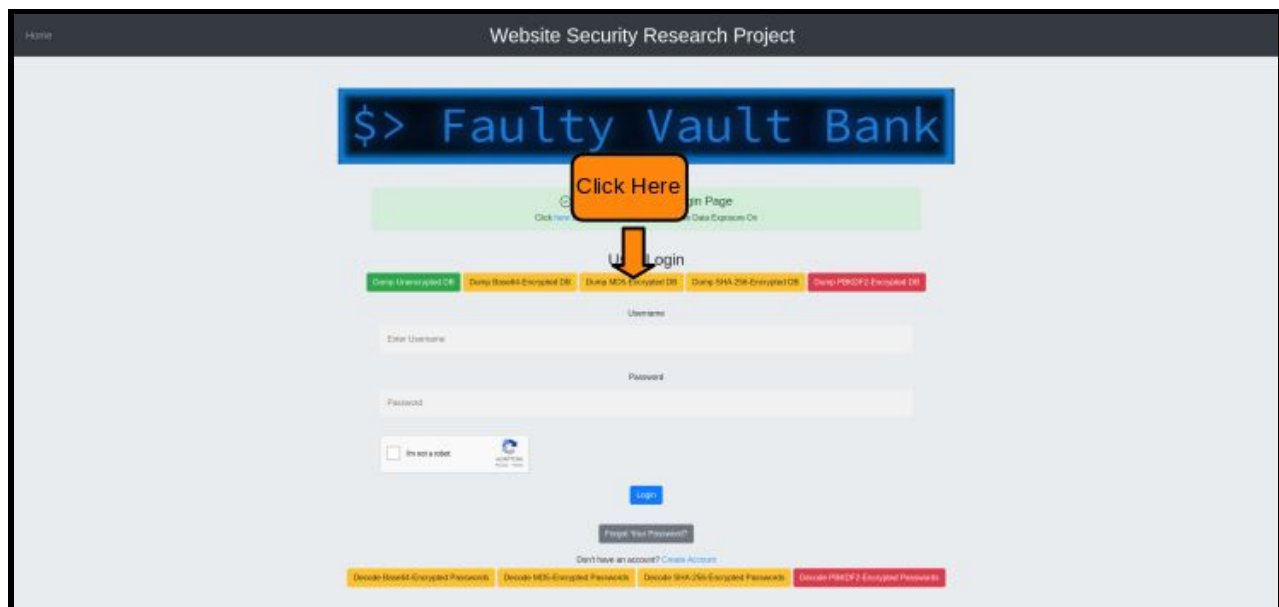
Please note: PBKDF2 is not able to be decrypted on either versions of the website so we do not include it in this section

Base-64-Encrypted Passwords Stored in the Database

***Base64 is not a hashing algorithm and should never be used to “encrypt” passwords.



MD5-Encrypted Passwords Stored in the Database



Website Security Research Project

Paste the copied passwords into the decryptor window that pops up. You will need to verify you are not a robot and then click "Crack Hashes"

Copy all the hashed passwords.

Free Password Hash Cracker

Enter up to 25 non-quoted hashes, one per line

CrackStation

Decipher Base64-Encoded Passwords | Decode MD5-Encoded Passwords | Decode SHA-256 Encrypted Passwords | Decode PBKDF2 Encrypted Passwords

Website Security Research Project

None of the passwords hashed with MD5 were able to be broken. This shows the importance of creating strong passwords. Even with weak hashing algorithms like MD5, strong passwords are very difficult to break.

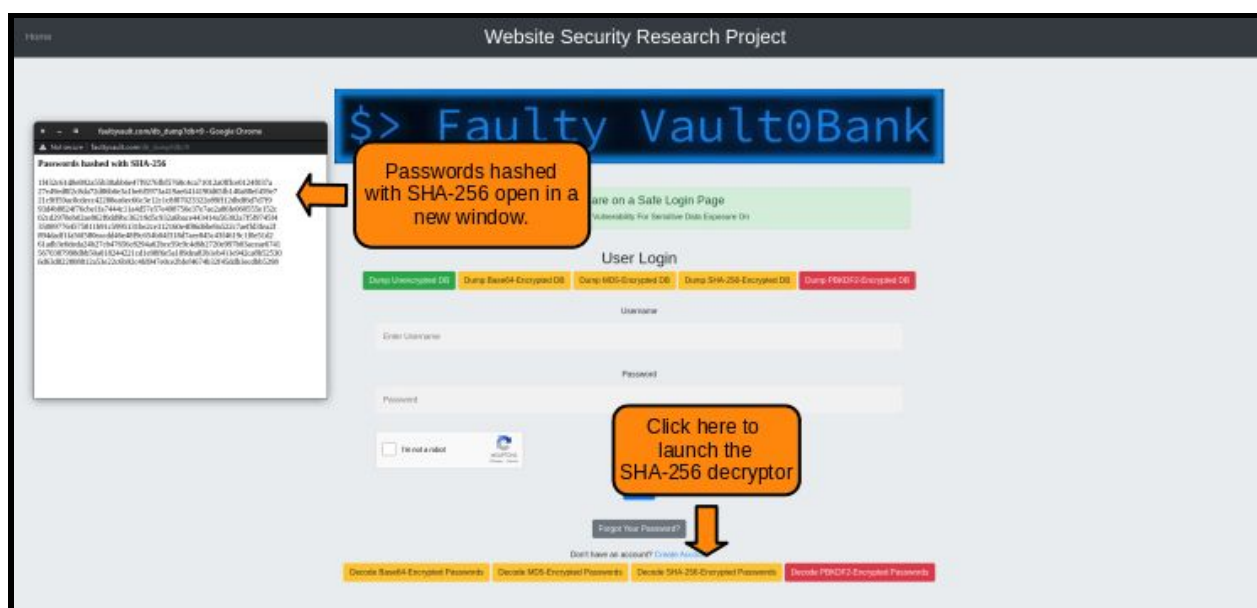
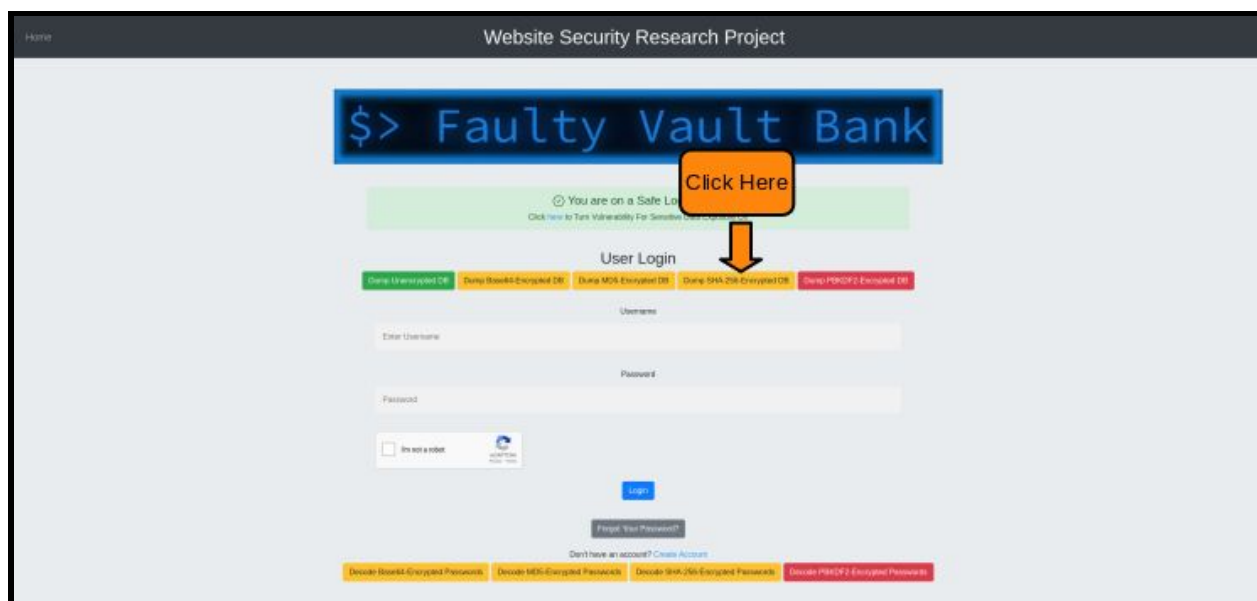
Free Password Hash Cracker

Enter up to 25 non-quoted hashes, one per line

Hash	Type	Result
5f4dcc3b5aa765261825866d882487e98	MD5	Failed
5d41402eea408a71b38d075893968166	MD5	Failed
5e1020524e61f6667f27278383083218	MD5	Failed
5c9cd0b9382bf34297fb551b2efad167	MD5	Failed
5d013e1457af1357f804a26f06e29a86	MD5	Failed
5f4dcc3b5aa765261825866d882487e98	MD5	Failed
5d41402eea408a71b38d075893968166	MD5	Failed
5e1020524e61f6667f27278383083218	MD5	Failed
5c9cd0b9382bf34297fb551b2efad167	MD5	Failed
5d013e1457af1357f804a26f06e29a86	MD5	Failed
5f4dcc3b5aa765261825866d882487e98	MD5	Failed
5d41402eea408a71b38d075893968166	MD5	Failed
5e1020524e61f6667f27278383083218	MD5	Failed
5c9cd0b9382bf34297fb551b2efad167	MD5	Failed
5d013e1457af1357f804a26f06e29a86	MD5	Failed
5f4dcc3b5aa765261825866d882487e98	MD5	Failed
5d41402eea408a71b38d075893968166	MD5	Failed
5e1020524e61f6667f27278383083218	MD5	Failed
5c9cd0b9382bf34297fb551b2efad167	MD5	Failed
5d013e1457af1357f804a26f06e29a86	MD5	Failed

Decipher Base64-Encoded Passwords | Decode MD5-Encoded Passwords | Decode SHA-256 Encrypted Passwords | Decode PBKDF2 Encrypted Passwords

SHA-256-Encrypted Passwords Stored in the Database



Resources

https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure

https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html

<https://docs.python.org/3/library/hashlib.html>

<https://searchsecurity.techtarget.com/definition/MD5>

https://en.wikipedia.org/wiki/MD5#Overview_of_security_issues

<https://www.geeksforgeeks.org/md5-hash-python/>

<https://www.geeksforgeeks.org/sha-in-python/>

<https://en.wikipedia.org/wiki/SHA-2>

<https://www.solarwindsmsp.com/blog/sha-256-encryption>

<https://crackstation.net/>

<https://crackstation.net/hashing-security.htm>

<https://www.safetynetdetectives.com/blog/the-most-hacked-passwords-in-the-world/>

<https://stackabuse.com/encoding-and-decoding-base64-strings-in-python/>

<https://codebeautify.org/base64-decode>

<https://en.wikipedia.org/wiki/Base64>

<https://stackoverflow.com/questions/28836837/is-base64-an-encryption-or-encoding-algorithm#:~:text=it%20is%20not%20considered%20as,content%2C%20so%20it's%20not%20encryption.&text=Base64%20is%20such%20an%20encoding,may%20not%20be%20handled%20correctly.>

<https://en.wikipedia.org/wiki/PBKDF2>

<https://security.stackexchange.com/questions/16354/whats-the-advantage-of-using-pbkdf2-vs-sha256-to-generate-an-aes-encryption-key>

<https://ropesec.com/articles/sensitive-data-exposure/>

https://en.wikipedia.org/wiki/Rainbow_table