DCIT

Ukázková závěrečná zpráva: penetrační test webové aplikace PORTÁL

Zhotovitel: **DCIT, a.s.**

Vinohradská 2828/151
130 00 Praha 3

www.dcit.cz

Adresát: **Zákazník, s.r.o.**

Autoři: Ing. Jan Novák, OSCP
Mgr. Josef Novotný, CEH

Datum vyhotovení: 25. června 2024

Počet stran: 20

Verze: 1.0

Obsah

Přílohy

1 Úvod

Tento dokument obsahuje výsledky penetračního testu, jehož provedením byla pověřena společnost DCIT, a.s. (dále jen DCIT). Penetrační test měl v praxi ověřit funkčnost zabezpečení webové aplikace společnosti Zákazník, s.r.o. (dále jen Zákazník).

V průběhu provedeného **penetračního testu webové aplikace** byly k dispozici autentizační údaje. Provedený penetrační test mimo jiné simuloval pokusy o zneužití oprávnění přidělených běžnému uživateli testované aplikace k útoku na jiného uživatele aplikace, případně i na aplikaci samotnou.

Dokument je rozdělen do několika částí:

- **Manažerský souhrn** – stručný průřez průběhu testů společně s výsledky.
- **Popis testu** – popis metodiky testu.
- **Zjištěné skutečnosti** – nedostatky a další významné informace zjištěné během provádění testu.
- **Shrnutí doporučení** – přehled doporučení, kterými lze odstranit nedostatky nalezené v průběhu testu.

V této zprávě jsou popsána zjištění učiněná během testů i doporučení z nich vyplývající. Zpráva či její přílohy mohou obsahovat uživatelská hesla a jiné citlivé údaje. Příjemce dokumentu řídí přístup k dokumentu ve vnitřním prostředí dle svých pravidel a potřeb.

2 Manažerský souhrn

2.1 Přehled výsledků penetračního testu

Následující tabulka shrnuje hodnocení zabezpečení webové aplikace:

Testovaná oblast	PORTÁL
Informace o aplikaci [WSTG-INFO]	💣
Konfigurace serveru [WSTG-CONF]	💣
Správa uživatelských účtů [WSTG-IDNT]	😐
Autentizace [WSTG-ATHN]	☠
Autorizace [WSTG-ATHZ]	☠
Správa session [WSTG-SESS]	☹
Validace vstupních dat [WSTG-INPV]	💣
Zpracování chybových stavů [WSTG-ERRH]	😐
Kryptografické nedostatky [WSTG-CRYP]	i
Aplikační logika [WSTG-BUSLOGIC]	☹
Zranitelnosti na klientské straně [WSTG-CLIENT]	☺
Ostatní zjištění	😐
Celkové hodnocení	☠

Hodnocení každé testované oblasti odpovídá nejzávažnějšímu nálezu, který byl v dané oblasti objeven. Význam symbolů je popsán v kapitole o metodice hodnocení závažnosti nálezů. Pro přehlednou práci s doporučeními je vhodná tabulka v kapitole 5.

2.2 Hlavní nálezy

V této kapitole uvádíme nejdůležitější nálezy ve zkrácené podobě, plné znění je uvedeno dále v těle závěrečné zprávy.

☠ N6: Dostupné rozhraní pro správu s výchozím jménem a heslem

Server obsluhující webový portál má volně přístupné konfigurační rozhraní na adrese https://vzor-aplikace.cz/admin/login.jsp. Toto rozhraní vyžaduje přihlášení pomocí jména a hesla. Tyto údaje byly ponechány na výchozích hodnotách `admin`.

Přidáním nové aplikace jsme získali možnost spouštět a nahrávat na server vlastní kód jako uživatel `AppUser`.

Tímto způsobem tak útočník získá nejen kontrolu nad serverem a aplikacemi, které jsou na něm provozovány, ale i přístup do vnitřní sítě, do které je tento server připojen.

Doporučení: Změnit výchozí přihlašovací údaje, zakázat vzdálený přístup k rozhraní pro správu provozovaných webových aplikací.

☠ N8: Nedostatečné řízení přístupu v sekci Nastavení

V sekci `Nastavení` si uživatel může změnit osobní údaje. V požadavku, který odpovídá této akci, se vyskytuje parametr `Username`, který identifikuje uživatele, kterého se týká změna. Server však nekontroluje, že se jedná o uživatele aktuální seance. Pokud je tedy parametr `Username` změněn na hodnotu jiného uživatele, **je změna provedena jemu**.

Doporučení: Opravit řízení přístupu na místě popsaném v nálezu.

N10: SQL injection

V testované aplikaci byla nalezena slabina typu SQL injection. Zranitelnost byla detekována v parametru `Keyword`, který se vyskytuje v HTTP požadavku, který slouží pro prohledávání a filtrování nahraných souborů.

Zmíněný požadavek lze modifikovat a získat tak libovolná data z databáze. **V databázi se vyskytují hashe hesel, jména a příjmení uživatelů, e-maily, rodná čísla a další.**

Doporučení: Implementovat systematickou obranu proti útoku typu *SQL injection*.

2.3 Závěr

Penetrační test prokázal přítomnost několika kritických slabin a řadu dalších, méně závažných. **Uvedené slabiny ohrožují data uživatelů, dostupnost aplikace, provozovanou infrastrukturu, včetně interní sítě zákazníka.**

Celkem bylo vydáno 14 doporučení ke zlepšení celkové úrovně bezpečnosti. Na základě našich zjištění hodnotíme celkovou bezpečností úroveň testované aplikace PORTÁL jako nevyhovující. Dokud nebudou alespoň nejzávažnější slabiny opraveny, doporučujeme aplikaci okamžitě znepřístupnit pro přístup z internetu.

3 Popis testu

3.1 Předmět testu

Předmětem testu byla webová aplikace PORTÁL společnosti Zákazník, s.r.o. dostupná na adrese https://vzor-aplikace.cz.

Jde o webovou aplikaci pro klienty společnosti Zákazník, kteří mají produkt `PORTÁL`. Pomocí webového rozhraní mohou klienti:

- ukládat různé soubory,
- spravovat svůj účet a vzájemně komunikovat.

3.2 Podmínky testování

Testování bylo prováděno na testovacím prostředí za použití následujících testovacích účtů.

Uživatel	ID uživatele	Registrované tel. číslo	E-mailová adresa
dcittest1	cbab0bc5-a230-433d-ae48-c7836071d46e	+420 123 456 789	dcittest1@dcit.cz
dcittest2	6724456e-e3da-4fcc-a47f-88cd113dbe0c	+420 234 567 891	dcittest2@dcit.cz
dcittest3	305026b7-fb87-4747-9ec3-ba53af8b61ca	+420 345 678 912	dcittest3@dcit.cz

3.3 Provedené testy

Test webové aplikace vycházel z metodiky OWASP Web Security Testing Guide (WSTG). Byly též využívány naše vlastní zkušenosti a postupy. Zvláštní důraz byl kladen na manuální průzkum aplikace podpořený automatizovanými skeny zranitelností.

Následující výčet shrnuje techniky a nástroje použité při testování webové aplikace k odhalení, případně i praktickému ověření, výskytu jejích slabin:

- průzkum struktury provozované aplikace, analýza její funkčnosti a komunikace mezi serverem a klientem a identifikace potenciálních slabých míst,
- automatizované testy nalezených webových serverů systémy Nessus a nuclei,
- slovníkové útoky a jiné testy WWW stránek nástrojem ffuf na různých místech adresářové struktury poskytovaných stránek,
- (polo)automatizované testy webové aplikace systémem Burp Suite Professional,
- testy autentizačních mechanismů aplikace a způsobů, jakým je udržován kontext uživatelské seance,
- útoky hrubou silou nebo slovníkovými metodami za účelem odhalení uživatelských jmen nebo hesel, hodnoty session cookies, jmen souborů nebo adresářů apod.,
- útoky hrubou silou za účelem nepřímého získání určitých citlivých informací (tzv. data mining),
- manipulace s URL, parametry dotazů nebo jinými daty zasílanými klientem na server za účelem vyvolání chybových stavů, špatného řízení přístupu nebo odhalení nedostatečné kontroly vstupních dat (SQL injection, cross site scripting, HTTP response splitting apod.),
- pokusy o obejití případných kontrol na klientské části aplikace (např. JavaScript),

- pokusy o obejití případných kontrol na serverové části aplikace, zejména pomocí změn kódování přenášených dat, alternativními (ekvivalentními) přepisy nebo jinou manipulací,
- pokusy o útoky na slabé mechanismy řízení uživatelských seancí metodami fixace (session fixation), predikce (session prediction) a únosu (session hijacking),
- kontrola výskytu nežádoucích funkcí či souborů (demonstračních, testovacích),
- jiné specifické a doplňující testy.

Při většině prováděných testů byl využíván program Burp Suite Professional.

3.4 Limity provedených testů

Upozorňujeme, že vzhledem k rozsahu testované aplikace a omezenému času pro její testování nemusely být zjištěny veškeré bezpečnostní nedostatky. Jedná se o omezení vyplývající z povahy penetračních testů.

Zejména upozorňujeme na skutečnost, že funkce `Změnit e-mail` v sekci `Nastavení` nebyla v době testování funkční, a proto nemohla být otestována.

Dne 20. 6. 2024 byla aplikace v době od 14 do 16 hodin mimo provoz.

3.5 Limity aplikovatelných doporučení

Upozorňujeme na skutečnost, že veškerá doporučení, která v této zprávě uvádíme, jsou pouze informativního charakteru a nemusí být aplikovatelná na provozované systémy.

Provozovatel si musí být vědom skutečnosti, že v případě uplatnění těchto doporučení je nutné tyto změny předem odzkoušet v testovacím provozu po určitou dobu, jestli nedochází k nežádoucím stavům, poškození nebo k jiným předem nepredikovatelným situacím. Testovací a produkční systémy musí být identické.

Uvedená doporučení vycházejí z informací, které jsme měli k dispozici v čase testu, a jedná se spíše o obecná řešení, která jsou používaná pro definované bezpečnostní problémy.

Dodavatel neručí při použití těchto doporučení za případné škody, dodatečně vzniklé náklady, nebo jinou finanční újmu, která může vzniknout při jejich aplikaci.

3.6 Průběh testu a harmonogram

Testy byly prováděny přibližně v následujících krocích:

Datum	Činnost
12. 6. 2024	úvodní schůzka, zahájení testování, seznámení se s aplikací
13. - 21. 6. 2024	automatizované a manuální testování
24. - 25. 6. 2024	ověřování výsledků, tvorba závěrečné zprávy

Některé doplňující testy pro upřesnění nebo ověření zjištěných informací mohly být provedeny v jiných termínech.

Test byl proveden převážně z IP adres 10.20.30.40 a 10.20.30.60, některé dílčí testy mohly být provedeny z IP adres z rozsahu 10.125.250.0/24.

3.7 Metodika hodnocení závažnosti nálezů

V rámci popisu nálezů a doporučení jsou pro zpřehlednění použity piktogramy s následujícím významem:

i **Pozorování (INFO)**
Takto jsou označovány nálezy a informace, které nemají samy o sobě významný dopad

na bezpečnost, nicméně považujeme za důležité je uvést z hlediska udržení kontextu a komplexního pohledu na testovanou/auditovanou oblast.

😐 **Připomínka (LOW)**
Takto jsou označovány nálezy s méně významným dopadem. Tímto způsobem jsou také označovány zranitelnosti, u nichž nelze odhadnout míru závažnosti problému v konkrétním prostředí zákazníka. Jsou obvykle následovány doporučením k odstranění těchto problémů, ale vzhledem k jejich charakteru není pro udržení dobré úrovně zabezpečení nutné opatření realizovat ihned, spíše je brát v úvahu v případě dalšího rozvoje aplikace nebo systému, který je uvedeným nálezem zranitelný (např. nová verze aplikace nebo upgrade middleware).

☹ **Nedostatek (MEDIUM)**
Takto jsou označovány nálezy s nezanedbatelným dopadem. Tímto způsobem jsou také označovány zranitelnosti, u nichž nelze odhadnout skutečnou míru závažnosti problému v konkrétním prostředí zákazníka. Vždy jsou následovány doporučením k odstranění tohoto nedostatku. Vzhledem k charakteru těchto nálezů je vhodné doporučená opatření realizovat (kategorie nice-to-have).

🧨 **Slabina (HIGH)**
Takto jsou označovány nálezy s velkým možným dopadem. Vždy jsou následovány doporučením k odstranění problému. Realizace doporučených opatření v tomto případě je nutná pro dosažení dobré úrovně zabezpečení (kategorie need-to-have).
Oprava nálezů této úrovně by měla být ověřena retestem.

☠ **Velká slabina/průnik (CRITICAL)**
Takto jsou označovány nálezy s velkým možným dopadem a zároveň velkou pravděpodobností jejich zneužití, případně jde o průnik narušující zabezpečení testovaných zařízení a/nebo sítě. Může se jednat o částečný nebo úplný provedený průnik nebo je takto označen pouze scénář možného útoku, který ale nebyl z různých, např. časových důvodů, během testu demonstrován. Realizace doporučených opatření v tomto případě je bezpodmínečně nutná v nejbližším možném termínu (nikoliv až za měsíc v době periodického záplatování apod.).
Oprava nálezů této úrovně musí být ověřena retestem.

☺ **Zlepšení / Pozitivní informace**
Tímto způsobem jsou ve zprávě označovány pozitivní hodnocení, a to jak pozorovaná zlepšení oproti předchozím penetračním testům, tak nálezy, které zabránily většímu zneužití konkrétních slabin.

Mimo určení závažnosti dle naší metodiky zpráva obsahuje též hodnocení podle stupnice CVSS (Common Vulnerability Scoring System). Ačkoli je v obou případech využívána stejná klasifikační škála, hodnocení nemusí být totožná a mohou se odchylovat oběma směry. Náš přístup se snaží zohledňovat širší kontext, který nemusí být vždy popsatelný pomocí CVSS koeficientů.

4 Zjištěné skutečnosti

4.1 Aplikace PORTÁL

4.1.1 Informace o aplikaci [WSTG-INFO]

Předmětem testu byla webová aplikace PORTÁL vyvíjená společností Zákazník, s.r.o. Tato aplikace umožňuje:

- registraci a správu uživatelského profilu,
- komunikaci mezi přihlášenými uživateli,
- ukládání a sdílení souborů s dalšími uživateli (případně i neregistrovanými v systému).

Uživatel se autentizuje pomocí jména, hesla a dalšího faktoru, kterým je kód zaslaný prostřednictvím SMS zprávy na registrované mobilní číslo.

Registrace je ověřována zasláním e-mailu.

Aplikace je dostupná na veřejné IP adrese 123.123.123.123 pod doménovým jménem https://vzor-aplikace.cz.

Na testovaném serveru (IP 123.123.123.123) byly během testování nalezeny následující otevřené porty:

Port/protokol	Služba	Verze
80/tcp	http	Apache httpd
443/tcp	ssl/https	Apache httpd

Oskenovány byly všechny TCP porty a 200 nejčastěji používaných UDP portů.

N1: Interní údaje dostupné ve veřejných repozitářích

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:L/A:L				Score:
Attack Vector:	Network	Scope:	Changed	
Attack Complexity:	High	Confidentiality:	Low	**6.5**
Privileges Required:	None	Integrity:	Low	
User Interaction:	None	Availability:	Low	(Medium)

Vyhledáváním klíčových slov souvisejících s aplikací (jako například `vzor.aplikace` a `Zákazník PORTÁL`) z otevřených zdrojů (tzv. OSINT) se podařilo najít repozitář obsahující potenciálně citlivá data.

Nalezený repozitář je dostupný na adrese https://github.com/repozitar-jednoho-z-vyvojaru/vzoraplikace. Tento repozitář mimo jiné obsahuje i skripty související s nasazením aplikace. Vzhledem ke skutečnosti, že soubory jsou 2-3 roky staré, není zřejmé, kolik z informací dostupných v tomto repozitáři je aktuálních. Za největší problém však považujeme výskyt plaintextového hesla k doménovému účtu v souboru `/ssh/user.sh`:

```
#!/bin/bash

touch domain_users.txt
key_path="ssh_keys"

for i in $(ls ~/ssh_keys); do
    USR=$(ldapsearch -D "vyvojar@zakaznik.company" -w "secretPassword123" "$i")
    if [[ $? -eq 0 ]] ; then
        echo $USR >> domain_users.txt
        mv ~/ssh_keys/$i "$key_path"/$i
        break
    fi
done
```

Funkčnost tohoto hesla nebyla testována.

Doporučení: Odstranit interní informace z veřejně dostupných repozitářů.

N2: Dostupné soubory `.js.map`

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N				Score:
Attack Vector:	Network	Scope:	Unchanged	
Attack Complexity:	Low	Confidentiality:	None	**0.0**
Privileges Required:	None	Integrity:	None	
User Interaction:	None	Availability:	None	(None)

Pro některé poskytované JavaScriptové soubory byly na serveru nalezené soubory `.js.map`. Tyto soubory lze použít k získání původních zdrojových kódů, což je v případě moderních aplikací s obfuskovaným JavaScriptem pro útočníka přínosné. Z čitelných zdrojových kódů lze lépe odhadovat fungování aplikace.

Na testovacím prostředí je přítomnost `.js.map` souborů pochopitelná a v pořádku. Pro nasazení do produkce je ale doporučujeme odstranit.

Doporučení: Na produkčním prostředí odstranit dostupnost `.js.map` souborů.

4.1.2 Konfigurace serveru [WSTG-CONF]

N3: Zastaralá verze a konfigurace webového serveru

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H				Score:
Attack Vector:	Network	Scope:	Unchanged	
Attack Complexity:	Low	Confidentiality:	None	**7.5**
Privileges Required:	None	Integrity:	None	
User Interaction:	None	Availability:	High	(High)

Webový server do odpovědí na HTTP požadavky přidává hlavičku `Server`:

```
HTTP/1.1 200
Date: Mon, 24 Jun 2024 07:52:19 GMT
Content-Type: text/html; charset=UTF-8
Strict-Transport-Security: max-age=31536000
Server: Apache/2.2.19 (Win64)
Content-Length: 61078
...
```

Na základě této hlavičky se server identifikuje jako `Apache 2.2.19`.

Apache řady 2.2 není oficiálně podporovaný již od července 2017, nelze ale vyloučit případné backportování oprav objevených chyb od třetí strany, například Linuxové distribuce.

Tato verze serveru je v defaultní konfiguraci náchylná k útoku Slowloris (CVE-2017-7670), který způsobuje odepření přístupu k serveru (DoS) pomocí pomalu zasílaných požadavků. Po dohodě se zadavatelem testu byla tato zranitelnost prakticky ověřena a úspěšně demonstrována.

Návod pro vhodné nastavení serveru Apache, aby útok *Slowloris* vůči němu nebyl efektivní, lze nalézt například na https://www.acunetix.com/blog/articles/slow-http-dos-attacks-mitigate-apache-http-server/.

Doporučení: Ověřit, jestli je server pravidelně aktualizovaný. Zvážit přechod na aktuální verzi Apache. Upravit konfiguraci serveru kvůli ochraně před útokem Slowloris.

😐 **N4: Chybějící bezpečnostní HTTP hlavičky**

CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:N				Score:
Attack Vector:	Network	Scope:	Unchanged	
Attack Complexity:	High	Confidentiality:	None	**0.0**
Privileges Required:	None	Integrity:	None	
User Interaction:	Required	Availability:	None	(None)

Obecně lze doporučit využívání následujících bezpečnostních HTTP hlaviček:

- `Content-Security-Policy` (*CSP*) – komplexní hlavička, která deklaruje, odkud mohou být do stránky vkládány jednotlivé zdroje,
- `Referrer-Policy` – umožňuje kontrolovat a omezit hodnotu hlavičky `Referer` v HTTP požadavku při odkazování na jiné stránky,
- `Strict-Transport-Security` (*HSTS*) – vynucuje příští přístup pouze pomocí šifrovaného spojení,
- `X-Frame-Options` – znemožňuje vnořit webovou aplikaci do jiné stránky pomocí HTML rámů (lze nahradit direktivou u CSP, ale vzhledem ke kompatibilitě se staršími prohlížeči je vhodnější uvést i samostatnou hlavičku),
- `X-Content-Type-Options: nosniff` – zakazuje webovým prohlížečům tzv. *Content guessing*.

Hlavičky `Strict-Transport-Security` a `X-Content-Type-Options` je vhodné přidávat do každé odpovědi serveru. Ostatní mají praktický dopad pouze, pokud server vrací HTML kód, ale pro zjednodušení konfigurace serveru mohou být přítomny i jindy.

Testovaný server využívá pouze hlavičky `X-Frame-Options: sameorigin` a `Strict-Transport-Security: max-age=31536000`.

Přidáním dalších vhodně nakonfigurovaných hlaviček lze v prohlížeči využít více bezpečnostních mechanizmů a snížit tak šanci zneužití případné zranitelnosti.

Mimo výše uvedených hlaviček je na serveru využívána též hlavička `X-XSS-Protection`, která zapíná v prohlížeči filtr proti XSS. Přítomnost této hlavičky byla v minulosti doporučována, ale v současné době od ní prohlížeče ustupují. XSS filtry nikdy nebyly příliš účinné a hlavička tak nabízela falešný pocit bezpečí. Místo této hlavičky je doporučováno vhodně nakonfigurovat CSP, což má větší praktický dopad. Přítomnost hlavičky stále vnímáme pozitivně, ale v aktuálních verzích prohlížečů bude mít efekt pouze v Safari a MS Internet Exploreru (Chrome, Edge a Opera podporu zrušily, Firefox ji nikdy nezavedl).

Doporučení: Zvážit doplnění uvedených hlaviček do konfigurace webového serveru.

4.1.3 Správa uživatelských účtů [WSTG-IDNT]

ℹ Registrace uživatelů je vykonávána na základě e-mailové adresy a hesla. Po vyplnění registračního formuláře je zaslán e-mail, jehož součástí je odkaz sloužící pro aktivaci účtu. Po aktivaci účtu je potřeba vykonat registraci telefonního čísla, které bude sloužit jako druhý faktor při autentizaci do aplikace.

😐 **N5: Enumerace e-mailových adres uživatelů**

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N				Score:
Attack Vector:	Network	Scope:	Unchanged	
Attack Complexity:	Low	Confidentiality:	Low	**5.3**
Privileges Required:	None	Integrity:	None	
User Interaction:	None	Availability:	None	(Medium)

Aplikace umožňuje enumeraci e-mailových adres registrovaných osob na základě chybových hlášek přihlašovacího formuláře – hlášky se liší při pokusu o přihlášení pomocí e-mailové adresy neregistrované a registrované osoby.

Při použití e-mailové adresy `dcittest_not_existing@dcit.cz` odpoví server s chybovou hláškou `"Unknown user"`, zatím co při použití adresy `dcittest1@dcit.cz` server odpoví s hláškou `"Invalid password"`.

Takové chování lze proto využít pro enumeraci e-mailových adres registrovaných uživatelů.

Doporučení: Zvážit generalizaci chybových hlášek při neúspěšném přihlášení.

4.1.4 Autentizace [WSTG-ATHN]

Pro autentizaci do aplikace je vyžadována dvoufaktorová autentizace. Uživatelé testované aplikace se musí přihlásit a to pomocí e-mailové adresy a hesla. Jako druhý faktor slouží SMS zpráva na registrované mobilní číslo.

N6: Dostupné rozhraní pro správu s výchozím jménem a heslem

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H				Score:
Attack Vector:	Network	Scope:	Changed	
Attack Complexity:	Low	Confidentiality:	High	**10.0**
Privileges Required:	None	Integrity:	High	
User Interaction:	None	Availability:	High	(Critical)

Server obsluhující webový portál má volně přístupné konfigurační rozhraní na adrese https://vzor-aplikace.cz/admin/login.jsp. Toto rozhraní vyžaduje přihlášení pomocí jména a hesla. Tyto údaje byly ponechány na výchozích hodnotách `admin`.

Přihlášením pod tímto účtem útočník získá nejen detailní přehled o konfiguraci serveru a provozovaných aplikacích, včetně jejich zdrojových kódů, ale i možnost tyto aplikace upravovat nebo přidávat nové.

Přidáním nové aplikace jsme získali možnost spouštět a nahrávat na server vlastní kód jako uživatel `AppUser`.

Tímto způsobem tak útočník získá nejen kontrolu nad serverem a aplikacemi, které jsou na něm provozovány, ale i přístup do vnitřní sítě, do které je tento server připojen.

Průzkumem konfigurace a okolní sítě jsme získali přístup k dalším konfiguračním a monitorovacím rozhraním, na kterých byly použity stejné výchozí přihlašovací údaje. Nalezené rozhraní jsou:

- `Publisher API` na adrese https://10.0.1.123/api,
- rozhraní `Flux CD` na adrese https://10.0.1.222:3030/apps.

Tyto další rozhraní nebyly součástí rozsahu zadání testu, proto jsme nezjišťovali další možnosti jejich zneužití.

Víme, že se jedná se o virtualizované stroje testovacího prostředí dostupné pouze z vnitřní sítě, přesto navrhujeme postupovat podle následujícího doporučení.

Doporučení: Změnit výchozí přihlašovací údaje, zakázat vzdálený přístup k rozhraní pro správu provozovaných webových aplikací.

N7: Hádání hesel uživatelů

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N				Score:
Attack Vector:	Network	Scope:	Unchanged	
Attack Complexity:	High	Confidentiality:	Low	**3.7**
Privileges Required:	None	Integrity:	None	
User Interaction:	None	Availability:	None	(Low)

Na straně serveru nebyl pozorován mechanizmus blokující počet pokusů o přihlášení. Útočník se může pokusit bez omezení hádat hesla jednotlivých uživatelů. Vzhledem k vyžadované komplexitě hesel by takový útok pravděpodobně nebyl příliš úspěšný, přesto doporučujeme implementovat některé z protiopatření, nebo jejich kombinaci:

- po větším počtu neúspěšných pokusů o přihlášení vyžadovat vyplnění CAPTCHA,
- zavést omezený počet neúspěšných pokusů o přihlášení na konkrétní uživatelský účet z jedné IP adresy po určitý (exponenciálně se prodlužující) časový interval,
- případně aplikovat jinou kombinaci možných protiopatření na základě OWASP doporučení.

Doporučení: Zvážit implementaci některé z popsaných metod ochrany proti hádání hesel uživatelů.

4.1.5 Autorizace [WSTG-ATHZ]

N8: Nedostatečné řízení přístupu v sekci Nastavení

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H				Score:
Attack Vector:	Network	Scope:	Unchanged	
Attack Complexity:	Low	Confidentiality:	High	**8.8**
Privileges Required:	Low	Integrity:	High	
User Interaction:	None	Availability:	High	(High)

V sekci `Nastavení` si uživatel může změnit heslo. V požadavku, který odpovídá této akci, se vyskytuje parametr `Username`, který identifikuje uživatele, kterého se změna týká. Server však nekontroluje, že se jedná o uživatele aktuální seance. Pokud je tedy parametr `Username` změněn na hodnotu jiného uživatele, je změna provedena na **cizím uživatelském účtu**.

Tento útok jsme prakticky vyzkoušeli na dvou testovacích účtech (`dcittest1` a `dcittest2`).

Ukázka požadavku na změnu hesla jiného uživatele:

```
POST /nastaveni HTTP/1.1
Host: vzor-aplikace.cz
Cookie: SESSIONID=session_of_dcittest1_5d5025e96b08f32384aabfd1cbfd3c4f

{
    "Username": "dcittest2"
    "Password": "Set_by_dcittest1"
}
```

Odpověď serveru byla následující:

```
HTTP/1.1 200 OK
Server: Apache 2.2.19
Content-Type: application/json

{
  "Message": "Heslo uživatele dcittest2 úspěšně změněno."
}
```

Odpověď serveru nasvědčuje tomu, že heslo bylo úspěšně změněno. Správnost této hypotézy byla ověřena a potvrdili jsme, že libovolný uživatel může pomocí tohoto požadavku měnit hesla jiných uživatelů.

Doporučení: Opravit řízení přístupu u požadavku na změnu uživatelského hesla v sekci `Nastavení`.

4.1.6 Správa session [WSTG-SESS]

Pro udržení uživatelské session se využívá cookie `SESSIONID`, která je obdržena po úspěšném přihlášení uživatele.

N9: Session fixation cookie `SESSIONID`

CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:L/A:N				Score:
Attack Vector:	Network	Scope:	Unchanged	
Attack Complexity:	High	Confidentiality:	High	**5.9**
Privileges Required:	None	Integrity:	Low	
User Interaction:	Required	Availability:	None	(Medium)

Hodnota cookie `SESSIONID` by se měla měnit při každé změně stavu uživatelské seance, tj. při přihlášení i při odhlášení. V aplikaci ale při přihlášení ke změně nedochází.

Chybějící změna cookie při přihlášení představuje riziko zejména na sdíleném počítači. Pokud by na něm zůstal otevřený webový prohlížeč a útočník z něj přečetl hodnotu cookie, může tak získat přístup do seance jiného uživatele, který se na počítači do aplikace přihlásí.

Pokud by aplikace obsahovala zranitelnost XSS, lze zároveň session fixation někdy využít společně s touto zranitelností. Útočník může hodnotu cookie v některých případech přečíst či nastavit a rovnou uživatele přesměrovat na přihlašovací dialog.

Při odhlášení jde především o správné ukončení seance na serverové straně. Obecně doporučovaným a nejjistějším postupem je starou seanci zahodit a založit zcela novou.

Doporučení: Měnit hodnotu cookie `SESSIONID` při každé změně stavu uživatelské seance, tedy při přihlášení i při odhlášení.

4.1.7 Validace vstupních dat [WSTG-INPV]

N10: SQL Injection

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N				Score:
Attack Vector:	Network	Scope:	Changed	
Attack Complexity:	Low	Confidentiality:	High	**7.7**
Privileges Required:	Low	Integrity:	None	
User Interaction:	None	Availability:	None	(High)

Aplikace umožňuje prohledávání a filtrování souborů nahraných přihlášeným uživatelem. Toto vyhledávaní je zranitelné na útok s názvem SQL Injection, který spočívá v tom, že uživatelský vstup je bez dostatečného ošetření vložen do SQL dotazu vykonávaného serverem. Tato zranitelnost útočníkovi umožňuje modifikovat dotazy nad databází a tak dle práv přidělených dotazovacímu účtu manipulovat a enumerovat data z databázového stroje.

Pro enumeraci dat z databáze je možné využít pravě požadavek pro filtrování nahraných souborů. Ukázku požadavku, který vylistuje všechny soubory (nejen ty nahrané přihlášeným uživatelem) lze vidět níže:

```
POST /files/list HTTP/1.1
Host: vzor-aplikace.cz
Cookie: [...]
Content-Length: 137
Content-Type: application/json

{
  "ClassIds": [
    20
  ],
  "Keyword": "' OR '1' = '1';-- ",
  "Regex": false,
}
```

V databázi se vyskytují hashe hesel, jména a příjmení uživatelů, e-maily, rodná čísla a další. Získaná data jsou prezentována v příloze A.

Doporučení: Implementovat systematickou obranu proti útoku typu *SQL injection*. Je třeba se vyvarovat přímého vkládání dat od uživatele do SQL dotazu. Pokud to je možné, využívat vázané proměnné. Vzhledem k dlouhodobé přítomnosti zranitelnosti doporučujeme po její opravě také změnu hesel všech uživatelů.

4.1.8 Zpracování chybových stavů [WSTG-ERRH]

😐 **N11: Detailní chybová hlášení**

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N				Score:
Attack Vector:	Network	Scope:	Unchanged	
Attack Complexity:	Low	Confidentiality:	Low	**5.3**
Privileges Required:	None	Integrity:	None	
User Interaction:	None	Availability:	None	(Medium)

Vhodnou manipulací se vstupními parametry (např. při pokusech o testování slabin typu SQL injection nebo cross-site scripting) nebo procházením stránek webové aplikace v určitém aplikací nepředpokládaném sledu (reload stránek, otevírání stránek v nových oknech/panelech prohlížeče, vracení se na předchozí stránky pomocí tlačítek prohlížeče) se podařilo dosáhnout v aplikaci chybových stavů.

Například:

```
Warning: odbc_fetch_array() expects parameter /1 to be resource, boolean given in D:\app\i
ndex_new.php on line 188

note: The full stack trace of the root cause is available in the Apache/2.2.19 logs
```

Útočník může detailní chybová hlášení využít k získání detailnějších informací o vnitřní struktuře aplikace, provozovaných typech a verzích software, případně o zrovna vyvolané chybě. Tyto informace může použít k efektivnějšímu zacílení dalších útoků.

Doporučení: Doporučujeme nastavit server tak, aby uživateli nezobrazoval interní chybové hlášení a varování prozrazující strukturu aplikace a verze provozovaného softwaru. Z bezpečnostního hlediska je ideální, pokud budou všechny chybové stavy maskovány jednotným, uživatelsky přívětivým hlášením.

4.1.9 Kryptografické nedostatky [WSTG-CRYP]

ℹ Všechny požadavky zaslané pomocí nešifrovaného kanálu na port 80/tcp jsou přesměrovávány na šifrovanou variantu komunikace. Pro komunikaci s aplikací je tedy reálně vždy využito šifrované spojení.

ℹ Jak již bylo uvedeno, server do HTTP odpovědí přidává hlavičku HSTS (HTTP Strict Transport Security), která prohlížeč informuje, že veškerá komunikace má být prováděna pouze šifrovaným kanálem. Slouží tedy jako ochrana před potenciálním vyzrazením citlivých dat.

ℹ Server prokazuje svou totožnost certifikátem vydaným na jméno `vzor-aplikace.cz` a podepsaným certifikační autoritou `PORTÁL CA 2024`. Certifikát je platný do 1. ledna 2025.

ℹ Server umožňuje šifrované spojení pouze pomocí protokolu TLSv1.2 za použití následujících šifrových suit:

Šifrová suita
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

ℹ **N12: Není podporováno TLSv1.3**

CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:N				Score:
Attack Vector:	Network	Scope:	Unchanged	
Attack Complexity:	High	Confidentiality:	None	**0.0**
Privileges Required:	None	Integrity:	None	
User Interaction:	Required	Availability:	None	(None)

TLSv1.3 přináší oproti TLSv1.2 zlepšení ve výkonu (kratší handshake) i bezpečnosti (jsou podporovány pouze šifrové suity v současné době považované za bezpečné). Tento protokol je

již podporován v aktuálních verzích všech rozšířených prohlížečů i webových serverů a mnoho provozu v internetu ho již využívá.

Považujeme proto za vhodné ho alternativně nabídnout. Jedinou překážkou může být využívání starých verzí softwaru na serverové straně, které nemusejí ještě TLSv1.3 podporovat.

Doporučení: Je-li to možné, zapnout podporu pro TLSv1.3. Případně zařadit zapnutí tohoto protokolu na seznam naplánovaných úkolů.

4.1.10 Aplikační logika [WSTG-BUSLOGIC]

☹ **N13: Nahrání souboru s libovolnou příponou**

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N				Score:
Attack Vector:	Network	Scope:	Unchanged	
Attack Complexity:	High	Confidentiality:	None	**3.7**
Privileges Required:	None	Integrity:	Low	
User Interaction:	None	Availability:	None	(Low)

Pomocí POST požadavku na adresu https://vzor-aplikace.cz/files/upload je možné na server nahrávat soubory. Aplikace má umožňovat nahrání pouze souborů následujících typů:

```
".bmp", ".doc", ".docx", ".jpeg", ".jpg", ".ods", ".odt", ".pdf", ".png",
".rtf", ".txt", ".xls", ".xlsx"
```

Dle chování serveru se zdá, že server pouze kontroluje, zda název souboru obsahuje povolenou příponou. Takovou ochranu lze snadno obejít. Například `exe` soubor `evil.exe` by bylo možné nahrát s názvem `evil.txt.exe`. Server v názvu najde jednu z přípon z povoleného seznamu a nahrání takového souboru umožní, i když se ve skutečnosti jedná o nepovolený spustitelný soubor. Takový soubor je možné nahrát následujícím požadavkem:

```
POST /files/upload
Host: vzor-aplikace.cz
Cookie: [...]
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:125.0) Gecko/20100101 Firefox/125.0
Content-Type: multipart/form-data; boundary=---------------------------942617861651212707
3978744889
Content-Length: 5240

-----------------------------942661786165121270739787448 89
Content-Disposition: form-data; name="p_files"; filename="evil.txt.exe"
Content-Type: application/x-msdownload

MZ[...]

-----------------------------942661786165121270739787448 89--
```

Nahraný soubor je následně možné znovu stáhnout, případně sdílet s ostatními uživateli.

Kromě opravy kontroly přípon souborů doporučujeme také kontrolovat typ souboru na základě validace formátu jeho obsahu.

Jak správně validovat nahrávané soubory je popsáno např. zde https://cheatsheetseries.owasp.org/cheatsheets/File_Upload_Cheat_Sheet.html.

Mimo výše zmíněné server pravděpodobně nepoužívá žádnou ochranu formou antiviru – je možné úspěšně nahrát testovací řetězec EICAR.

Doporučení: Zlepšit validaci nahrávaných souborů. Nahrávané soubory kontrolovat antivirem.

4.1.11 Zranitelnosti na klientské straně [WSTG-CLIENT]

ℹ Chyby na klientské straně aplikace nebyly nalezeny. Z bezpečnostního hlediska bez připomínek.

4.1.12 Ostatní zjištění

😐 N14: Skripty třetích stran

CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:N/A:N				Score:
Attack Vector:	Network	Scope:	Unchanged	
Attack Complexity:	High	Confidentiality:	Low	**2.6**
Privileges Required:	Low	Integrity:	None	
User Interaction:	Required	Availability:	None	(Low)

Do webové stránky je includované velké množství externích JavaScriptových souborů. Tím, že tyto skripty jsou pod kontrolou třetí strany, vzniká zde možnost injektáže neočekávaného či potenciálně škodlivého kódu do testované stránky.

Například do přihlašovací stránky jsou vkládány soubory:

```
https://apis.google.com/js/client.js?onload=initPicker
https://apis.google.com/_/scs/apps-
static/_/js/k=oz.gapi.cs.N66Isqjx8x4.O/m=client/rt=j/sv=1/d=1/ed=1/am=AQ/rs=AGLTdCPMOemdvO
A3jeM2urHnkcbgcgtFHg/cb=gapi.loaded_0
https://c.imedia.cz/js/retargeting.js
https://connect.facebook.net/en_US/fbevents.js
https://connect.facebook.net/signals/config/2422123804475125?v=2.9.39&r=stable
https://d70shl7vidtft.cloudfront.net/ecmtr-2.4.2.js
https://gate.gopay.cz/gp-gw/js/embed.js
https://login.affial.com/scripts/8m338kj
https://px4.ads.linkedin.com/collect?v=2&fmt=js&pid=2216180&time=1620721904580&url=https%3
A%2F%2Fapp.test.signi.tech%2Flogin%3Fredirect_to%3Dundefined&liSync=true&e_ipv6=AQLBHCMT_S
wJ7QAAAXlajboWaxRzFZXtS5v8hnjSjnnHCPfqB9BhTadroE9OPeQzk
https://snap.licdn.com/li.lms-analytics/insight.min.js
https://storage.googleapis.com/workbox-cdn/releases/4.3.1/workbox-core.prod.js
https://storage.googleapis.com/workbox-cdn/releases/4.3.1/workbox-precaching.prod.js
https://storage.googleapis.com/workbox-cdn/releases/4.3.1/workbox-sw.js
https://t.leady.com/dR7v9y12W62bk78W/L.js
https://www.google-analytics.com/analytics.js
https://www.googletagmanager.com/gtm.js?id=GTM-NV7B4EH
https://www.gstatic.com/charts/loader.js?key=AIzbSyD4k525LTtjaqiuDIu6Jw5qs1e1IVMUIrE
```

Doporučení: Využívané skripty třetích stran stáhnout na webový server pod kontrolou provozovatele webové stránky a ze zdrojového kódu webové stránky se odkazovat na tyto kopie. Alternativně je možné při vkládání skriptů využívat parametr `integrity`, který obsahuje hash odkazovaného souboru.

5 Shrnutí doporučení

ID	Název	H.	CVSS	Doporučení
N1	Interní údaje dostupné ve veřejných repozitářích		6.5	Odstranit interní informace z veřejně dostupných repozitářů.
N2	Dostupné soubory `.js.map`		0.0	Na produkčním prostředí odstranit dostupnost `.js.map` souborů.
N3	Zastaralá verze a konfigurace webového serveru		7.5	Ověřit, jestli je server pravidelně aktualizovaný. Zvážit přechod na aktuální verzi Apache. Upravit konfiguraci serveru kvůli ochraně před útokem Slowloris.
N4	Chybějící bezpečnostní HTTP hlavičky		0.0	Zvážit doplnění uvedených hlaviček do konfigurace webového serveru.
N5	Enumerace e-mailových adres uživatelů		5.3	Zvážit generalizaci chybových hlášek při neúspěšném přihlášení.
N6	Dostupné rozhraní pro správu s výchozím jménem a heslem		10.0	Změnit výchozí přihlašovací údaje, zakázat vzdálený přístup k rozhraní pro správu provozovaných webových aplikací.
N7	Hádání hesel uživatelů		3.7	Zvážit implementaci některé z popsaných metod ochrany proti hádání hesel uživatelů.
N8	Nedostatečné řízení přístupu v sekci Nastavení		8.8	Opravit řízení přístupu u požadavku na změnu uživatelského hesla v sekci `Nastavení`.
N9	Session fixation cookie `SESSIONID`		5.9	Měnit hodnotu cookie `SESSIONID` při každé změně stavu uživatelské seance, tedy při přihlášení i při odhlášení.
N10	SQL Injection		7.7	Implementovat systematickou obranu proti útoku typu *SQL injection*. Je třeba se vyvarovat přímého vkládání dat od uživatele do SQL dotazu. Pokud to je možné, využívat vázané proměnné. Vzhledem k dlouhodobé přítomnosti zranitelnosti doporučujeme po její opravě také změnu hesel všech uživatelů.
N11	Detailní chybová hlášení		5.3	Doporučujeme nastavit server tak, aby uživateli nezobrazoval interní chybové hlášení a varování prozrazující strukturu aplikace a verze provozovaného softwaru. Z bezpečnostního hlediska je ideální, pokud budou všechny chybové stavy maskovány jednotným, uživatelsky přívětivým hlášením.
N12	Není podporováno TLSv1.3		0.0	Je-li to možné, zapnout podporu pro TLSv1.3. Případně zařadit zapnutí tohoto protokolu na seznam naplánovaných úkolů.
N13	Nahrání souboru s libovolnou příponou		3.7	Zlepšit validaci nahrávaných souborů. Nahrávané soubory kontrolovat antivirem.
N14	Skripty třetích stran		2.6	Využívané skripty třetích stran stáhnout na webový server pod kontrolou provozovatele webové stránky a ze zdrojového kódu webové stránky se odkazovat na tyto kopie. Alternativně je možné při vkládání

ID	Název	H.	CVSS	Doporučení
				skriptů využívat parametr `integrity`, který obsahuje hash odkazovaného souboru.

Legenda
- i Pozorování (INFO)
- 😐 Připomínka (LOW)
- ☹ Nedostatek (MEDIUM)
- Slabina (HIGH)
- (Částečný) průnik (CRITICAL)

Příloha A Data získaná přes zranitelnost SQL injection

Zde by byla obsažena data získaná v průběhu testu.