



appsec

Report

Blackhat test [redacted]

Dokument je součástí duševního vlastnictví společnosti APPSEC s.r.o. Dispoziční právo k dokumentu náleží [redacted]. Bez souhlasu autora je zakázáno dokument v celku či v částech reprodukovat, publikovat nebo jinak používat k libovolným účelům mimo projekt Blackhat test [redacted]. Nakládání s dokumentem se řídí zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, v aktuálním znění.

Obsah

1	Úvod	4
1.1	Disclaimer	4
1.2	Nástroje použité při testování	4
1.3	Postup testování	4
1.3.1	Reconnaissance - zjišťování informací o cíli	4
1.3.2	Weaponization - vytvoření a návrh útoku v případě zjištění použitelných skutečností	5
1.3.3	Delivery - snaha o doručení payloadu pro provedení útoku	5
1.3.4	Exploitation - samotné spuštění kódu / payloadu	5
1.3.5	Post exploitation fáze	6
1.4	Metodika hodnocení	6
1.5	Celkové zhodnocení bezpečnosti společnosti	6
1.5.1	Doporučení na další kroky	7
2	Popis útoku	9
2.1	Zjišťování informací o společnosti	9
2.1.1	Domény	9
2.1.2	E-mailové adresy	9
2.2	Sken bezpečnostních zranitelností	12
2.3	Fáze exploitace nalezených zranitelností	13
2.3.1	Úspěšná demonstrace odchycení FTP přihlašovacích údajů	13
2.3.2	Úspěšná demonstrace odchycení POP přihlašovacích údajů	14
2.3.3	Úspěšná exploitace zranitelnosti Heartbleed	14
2.3.4	Úspěšná exploitace informací z nalezeného .git adresáře, přístup k administraci webu	16
3	Sken bezpečnostních zranitelností	18
3.1	Server 10.0.0.1	18
3.1.1	Použitý FTP server ■	18
3.1.2	Podpora SSL verze 2 a 3 ■	19
3.1.3	SSL podporovány slabé šifry ■	20
3.1.4	Nedůvěryhodný SSL certifikát ■	21
3.1.5	SSL podporovány středně slabé šifry ■	22
3.1.6	Podporovány RC4 šifry ■	23
3.1.7	SSH povoleny slabé algoritmy ■	24
3.2	Server 10.0.0.2	25
3.2.1	Nedůvěryhodný SSL certifikát ■	25
3.3	Server 10.0.0.3	26
3.3.1	Nepodporovaný operační systém ■	26
3.3.2	POP nešifrovaná hesla při přenosu ■	27
3.3.3	SMTP nešifrovaná hesla při přenosu ■	28
3.3.4	Zranitelnost Heartbleed ■	29
3.3.5	Podpora SSL verze 2 a 3 ■	30
3.3.6	Nedůvěryhodný SSL certifikát ■	31

3.3.7	OpenSSL 'ChangeCipherSpec' MiTM zranitelnost	■	32
3.3.8	Podporováno SSL3, možný útok POODLE	■	33
3.3.9	SSL podporovány slabé šifry	■	34
3.3.10	SSL podporovány středně slabé šifry	■	35
3.3.11	Podporovány RC4 šifry	■	36
3.4	Server 10.0.0.4		37
3.4.1	SSL podporovány středně slabé šifry	■	37
3.5	Server 10.0.0.5		38
3.5.1	Nedůvěryhodný SSL certifikát	■	38
3.5.2	POP3 - STLS PLaintext Command Injection	■	39
3.5.3	Podpora SSL verze 2 a 3	■	40
3.5.4	SSL podporovány slabé šifry	■	41
3.5.5	IMAP - STARTTLS Plaintext Command Injection	■	42
3.5.6	SSL podporovány středně slabé šifry	■	43
3.5.7	Podporovány RC4 šifry	■	44
3.6	Webová aplikace example.local		45
3.6.1	Dostupný adresář .git	■	45
3.6.2	Chybí HSTS hlavička	■	46
3.6.3	Přihlašovací formulář s Autocomplete	■	47
3.6.4	Náchylnost na clickjacking	■	48
3.6.5	Chybějící parametry cookies - httpOnly	■	49
3.6.6	Chybějící parametry cookies - secure	■	50

1 Úvod

Blackhat test je snahou o přesnou simulaci hackerského útoku proti firmě, kterou si hacker vyhlédl k útoku a o níž nemá žádné dodatečné informace kromě identity firmy samotné. Cílem útočníka jsou většinou nějaká citlivá data společnosti. Dalšími cíly může být poškození společnosti, jejího dobrého jména, zneužití serverů či výpočetního výkonu společnosti (v současné době například těžení kryptoměn).

1.1 Disclaimer

Vzhledem k omezené časové a finanční dotaci pro testování nelze zaručit, že výsledky z testování jsou stoprocentně vyčerpávající z hlediska rozsahu testovaných systémů. Vzhledem ke snaze o minimální narušení chodu firmy nepoužíváme v žádné fázi Blackhat penetračního testování sociální inženýrství. Útočník by jej v případě skutečného útoku pravděpodobně nějakým způsobem použil. Buď v úvodní fázi pro získání informací o systémech nebo v pozdějších fázích již se znalostí některých potenciálně důvěryhodných informací. Jedním z dalších kroků po realizaci Blackhat testu, může být vedle kompletního manuálního penetračního testu, právě test organizace na sociální inženýrství, phishing, apod.

1.2 Nástroje použité při testování

- APPSEC Toolkit
- Nessus
- Metasploit Framework
- Burp Suite Pro
- Nmap
- FirefoxCookie Manager +, FireBug, FoxyProxy
- Kali Linux
- Nikto
- Python

1.3 Postup testování

Testy probíhaly na základě zkušeností a schopností testerů. Cílem testů bylo otestovat společnost tak, jak by ji testoval skutečný útočník, který si hledá zajímavý cíl pro napadení. Oproti reálnému útoku v žádné fázi nepoužíváme social engineering z časových důvodů a snahy o co nejmenší narušení chodu firmy.

1.3.1 Reconnaissance - zjišťování informací o cíli

Začátkem každého úspěšného i neúspěšného útoku je zjišťování co největšího počtu informací o společnosti, která se stala cílem útoku. K tomuto hacker používá různé dostupné informace, například z webové stránky společnosti, z webových vyhledávačů, z dalších veřejně dostupných zdrojů informací, například různé sociální sítě, darknet, webové stránky pro sdílení uživatelských dat jako pastebin, sdílení různých obrázků, dokumentů a další. Často používanou technikou pro zjištění informací o firmě je vydávání se za potenciálního partnera firmy a informace zjistit například na obchodní schůzce či na pohovoru na relevantní pracovní pozici. Součástí reconnaissance fáze je i vulnerability scan nalezených systémů. Systémy, které jsou službou nějaké třetí strany jsou z vulnerability scanů

vynechané z právních důvodů. Pro reconnaissance fázi vycházíme z OSINT frameworku dostupného na adrese <http://osintframework.com/>.

Z hlediska zjišťování informací o cíli jsou pro útočníka zajímavé především tyto 3 oblasti:

- domény / servery Doménová jména a IP adresy jsou pravděpodobně prvním z informací, které útočník ve vztahu ke společnosti, kterou se chystá napadnout, zjišťuje.
- emailové adresy Emailové adresy slouží primárně k zaměření útoku využívajících sociálního inženýrství a to nejen jako příjemce například připraveného malware, ale mohou sloužit i pro potvrzení odesílatele e-mailu a tím e-mailu dodat určitou věrohodnost v očích uživatele či klienta právě využitím existující e-mailové adresy.
- další skutečnosti, které mohou pomoci se zacílením útoku Veškeré další skutečnosti, které mohou útočníkovi pomoci v zacílení útoku na vybranou společnost. Často se jedná například o typ používaného software, hardware, jeho verze, používané služby třetích stran, sídlo společnosti, umístění kanceláří, míra fyzického zabezpečení kanceláří a podobně. V neposlední řadě se v této části objeví případné indikátory toho, že testovaná společnost byla napadena (například se mohou vyskytovat nějaká data společnosti na black marketech či na různých serverech pro sdílení dat, například typu pastebin). V případě našeho BlackHat testu se v této kategorii věnujeme pouze skutečnostem, které mají nějakou relevanci k technické stránce zabezpečení společnosti.

1.3.2 Weaponization - vytvoření a návrh útoku v případě zjištění použitelných skutečností

V případě, že útočník nalezne v první fázi takové nedostatky, které by bylo možné zneužít k přímému útoku na danou společnost a na daná aktiva, připraví útočník v této fázi samotný útok. Například v situaci, kdy útočník nalezne bezpečnostní chybu ve webové aplikaci společnosti, si připraví takový payload, který mu umožní dostat se k takovým informacím, které si dal za cíl získat. Například v případě útoku za pomoci sociálního inženýrství si v této fázi útočník připraví postup útoku, informace, které by v případě útoku mohl použít atd.

1.3.3 Delivery - snaha o doručení payloadu pro provedení útoku

V této fázi se útočník pokouší o "doručení útoku". V případě útoku na některou z webových či síťových aplikací společnosti jsou většinou využívány klasické vstupní kanály dané aplikace. V případě sociálního inženýrství jsou to pak různé možnosti, například využití e-mailu, doručení útoku přes USB flashdisk poslaný v rámci "marketingové kampaně" a další.

1.3.4 Exploitation - samotné spuštění kódu / payloadu

Ve chvíli, kdy je útok připraven a byl doručen na cílový systém či cílovému uživateli (v případě některých útoku sociálního inženýrství), je na čase, aby byl případný payload spuštěn. K tomu ve většině případů dochází automaticky po doručení payloadu. Může k tomu však v případě některých útoků docházet jako reakce na nějakou událost, například při přihlášení administrátora do systému či otevření neznámé přílohy uživatelem.

1.3.5 Post exploitation fáze

Následující body patří k post-exploitation fázi, kterou v rámci BlackHat testu běžně neprovádíme, nicméně je zde v krátkosti uvádíme pro celkovou představu.

Installation V této fázi dochází k instalaci zadních vrátek či malware v systému.

Command and Control Vytvoření a použití zadních vrátek či jiného komunikačního kanálu pro přístup k napadenému systému.

Actions on objectives Nyní již útočník má přístup k systému a dochází k "práci" na původním stanoveném úkolu, ať již se jedná o špionáž, sabotáž či jiné.

1.4 Metodika hodnocení

Metodika hodnocení celkového zabezpečení společnosti je speciálně navržena pro náš Blackhat test. V hodnocení vycházíme z několika základních skutečností zjištěných o systémech testované společnosti. Jsou to nalezené nedostatky, jejich závažnost, možnost exploitace nalezených zranitelností, důležitost případných získaných dat společnosti. Blackhat test je možno provádět opakovaně a díky systému hodnocení tak sledovat zlepšení, nebo zhoršení stavu bezpečnosti organizace v průběhu času.

Z těchto skutečností vytváříme zjednodušené hodnocení písmenem, kde písmeno A je nejlepší výsledek, písmeno E pak výsledek nejhorší. Hodnocení vždy doprovázíme obsáhlým vysvětlením a zdůvodněním. V následujícím seznamu jsou uvedeny jednotlivá hodnocení s krátkým popisem jakému systému by dané hodnocení bylo přiřazeno.

- **A** - systémy společnosti jsou velmi dobře zabezpečené, povětšinou sledují best practices a je z nich patrné, že správci jsou obeznámeni s problematikou informační bezpečnosti
- **B** - systémy společnosti jsou zabezpečené, nicméně nesledují best practices či obsahují málo závažné nedostatky, které ale nejsou samy o sobě zneužitelné útočníkem
- **C** - systémy společnosti mají některé bezpečnostní nedostatky, které se ale z různých důvodů nepodařilo exploitovat, například z důvodu časové náročnosti, nedostatečných zdrojů či nepříznivé situace
- **D** - systémy společnosti byly exploitovány a byla zajištěna data, která nicméně nejsou příliš závažného rázu
- **E** - systémy společnosti byly exploitovány, nalezená data jsou závažného rázu a jejich únik by mohl být pro společnost velkým problémem

1.5 Celkové zhodnocení bezpečnosti společnosti

V průběhu Blackhat testu bylo identifikováno 5 serverů a 1 webová aplikace. Jedná se o počet obvyklý pro malou až středně velkou firmu. Během bezpečnostního skenu byly nalezeny bezpečnostní nedostatky, které jsou uvedeny v dokumentu dále. Testované servery a webové aplikace nebyly povětšinou dobře zabezpečené, bylo identifikováno několik

závažných zranitelností související především se špatnou správou SSL/TLS (šifrování dat při přenosu) a chybějícími aktualizacemi serverů. Celkově oblast šifrování dat při přenosu není příliš dobře řešena, na systémech bylo zjištěno, že šifrování dat při přenosu často není vyžadováno, šifrovací certifikáty nejsou důvěryhodné či šifrování dat při přenosu používá již nevyhovující bezpečnostní konfigurace. Toto v obecné rovině umožňuje útočníkovi, který by se dostal k datovým přenosům po síti data odposlouchávat či modifikovat. Dále pak některé servery obsahují zranitelnosti, které je možno přímo exploitovat k získání citlivých dat společnosti [REDACTED] či jejích zákazníků.

Během testování se podařilo kompromitovat webovou aplikaci [REDACTED], což hodnotíme jako závažný problém pro společnost, jelikož daná webová aplikace je hlavní prezentací společnosti ve směru k internetovým uživatelům. Útočník může být schopen aplikaci libovolně upravovat, čímž může nejen narušit důvěryhodnost společnosti, ale může i prostřednictvím webové aplikace společnosti napadat návštěvníky jejího webu.

Celkový dojem, který útočník získal, naznačuje vzhledem k mnoha zranitelnostem, vysokou šanci na úspěch při dalším postupu v post-exploitation fázi. Fakt, že se organizace stará o IT dalších subjektů, významně zvyšuje atraktivnost pro útočníka. Při infiltraci existuje velká šance zneužití interních přístupů a informací [REDACTED] a tím snazší kompromitace jejích zákazníků. Během testu byla přímo zjištěna a exploitována zranitelnost vedoucí k přímému přístupu k e-mailovým datům zákazníků společnosti.

Ať už by se jednalo o cílený útok nebo činnost automatizovaných skriptů, v případě [REDACTED] existuje vysoká šance na úspěch široké škály aktivit, od získání citlivých údajů společnosti či jejích zákazníků, přes konkurenční boj až po zneužití výpočetních prostředků. Takové incidenty v praxi často vedou k poškození reputace, ztrátě významných zákazníků a zhoršení výkonnosti organizace.

Výsledné hodnocení společnosti:



1.5.1 Doporučení na další kroky

Vzhledem k nalezeným skutečnostem doporučujeme alespoň jedno provedení komplexního manuálního penetračního testu, jak webových aplikací, tak infrastruktury a dále provedení phishingového testu zaměstnanců.

Komplexní penetrační test může být časově i finančně náročný, tudíž doporučujeme se nejdříve zaměřit na ty systémy a aplikace, o kterých víte, že jsou nějakým způsobem významné. Za další je pak nezbytné podrobit veškeré systémy pravidelnému skenování zranitelností, aby se v budoucnu zamezilo, že se zbytečně neotevřou nové cesty, které by mohl útočník zneužít.

Doporučujeme také realizovat phishingový nebo social engineering test, který prověří

odolnost Vašich zaměstnanců na tyto formy útoku a formou hry je lépe připraví na případné pokusy o zneužití jejich důvěry třetími stranami.

Za zvážení stojí také zavedení systému řízení bezpečností informací (ISMS) nebo alespoň některých jeho prvků pro dlouhodobé zvyšování odolnosti Vaší organizace před ztrátami plynoucí z kybernetických rizik.

Ať už by se jednalo o cílený útok nebo činnost automatizovaných skriptů, zdá se, že v případě existuje vysoká šance na úspěch široké škály aktivit, od získání citlivých údajů, přes šíření kryptovirů, až po konkurenční boj nebo zneužití výpočetních prostředků. Zvýšené riziko vnímáme zejména z pohledu cílených útoků na státní subjekty, jehož je dodavatelem. Velmi často se útočníci zaměřují právě na dodavatele a takové útoky jsou obzvlášť nebezpečné a hůře detekovatelné. Popsané incidenty v praxi často vedou k poškození reputace, ztrátě významných zákazníků nebo partnerů a zhoršení výkonnosti organizace.

2 Popis útoku

2.1 Zjišťování informací o společnosti

Informace o společnosti byly zjišťovány z veřejně dostupných zdrojů tak, aby byl co nejlépe nasimulován způsob jak by postupoval útočník v případě, že by se rozhodl testovanou společnost napadnout. Žádné informace z jednání se zákazníkem (jako například informace o infrastruktuře, použitých systémech či jejich nastavení) nejsou v této fázi brány v úvahu.

Zdroje dat informací o společnosti byly tyto:

- webové vyhledávače
- sociální sítě
- darkmarkety
- webové služby pro sdílení textu, obrázků, zdrojových kódů, dat
- DNS služba
- webové stránky společnosti
- ostatní webové stránky
- seznamy škodlivých domén a IP adres
- veřejně známé zranitelnosti
- veřejně dostupné informace z doménových certifikátů
- veřejně dostupné informace z PGP klíčů
- whistleblowerské weby

2.1.1 Domény

Následující domény a jejich odpovídající IP adresy byly zjištěny během reconnaissance fáze. Zdrojem těchto domén jsou DNS záznamy, odkazy z jiných webových stránek, a provedená OSINT analýza využívající nejrůznějších zdrojů dat.

Doména	IP adresa / doména v případě služby třetí strany

Jednotlivé domény a IP adresy mohou být útočníkem zneužity k útoku. Poměrně k velikosti attack surface (= mimo jiné množství nalezených domén a IP adres) narůstá i riziko úspěšného útoku proti společnosti.

2.1.2 E-mailové adresy

Následující e-mailové adresy byly získány z veřejně dostupných webů a webových vyhledávačů.

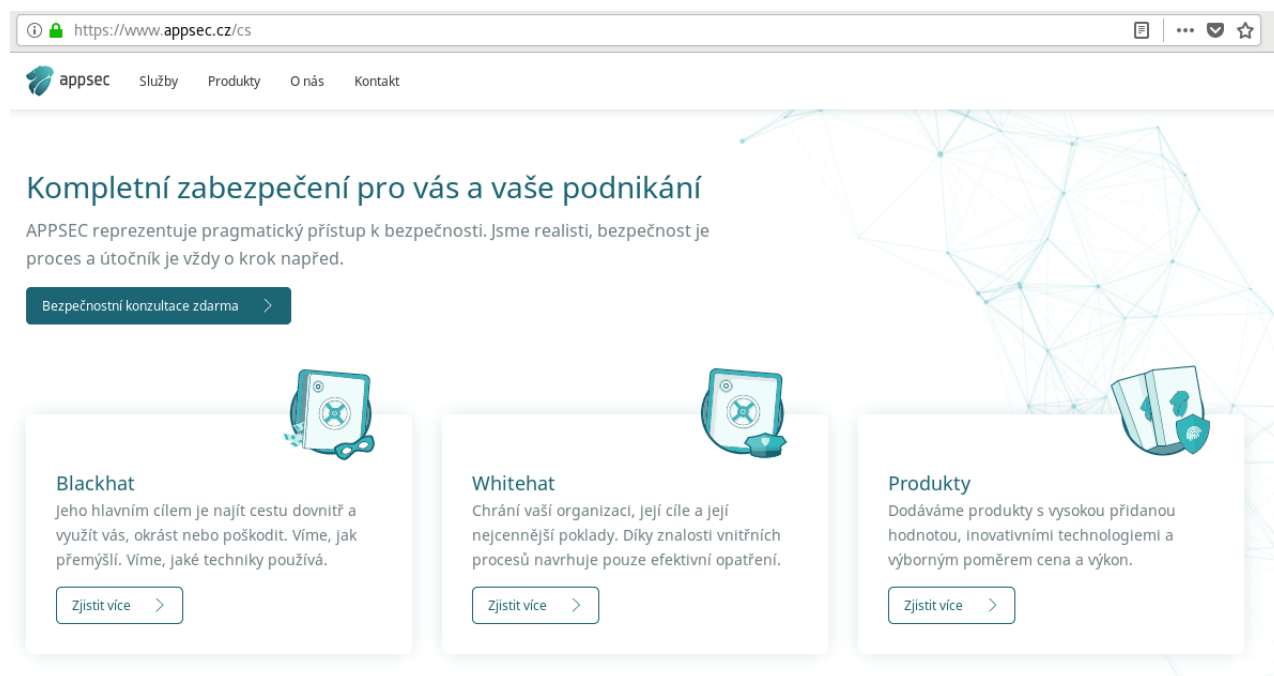
-

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

Během testu bylo zjištěno, že následující e-mailové adresy jsou v seznamu Have I Been Pwned, což je seznam internetových účtů asociovaných s danou e-mailovou adresou, které byly kompromitovány ať již hackery nebo únikem citlivých dat, často včetně hesel. Doporučujeme tedy pro následující e-mailové adresy změnu hesla pro případ, že by heslo bylo shodné s hesly uniklými.

- [redacted] - služba LinkedIn
- [redacted] - služba LinkedIn
- [redacted] - služba LinkedIn
- [redacted] - služba mall.cz

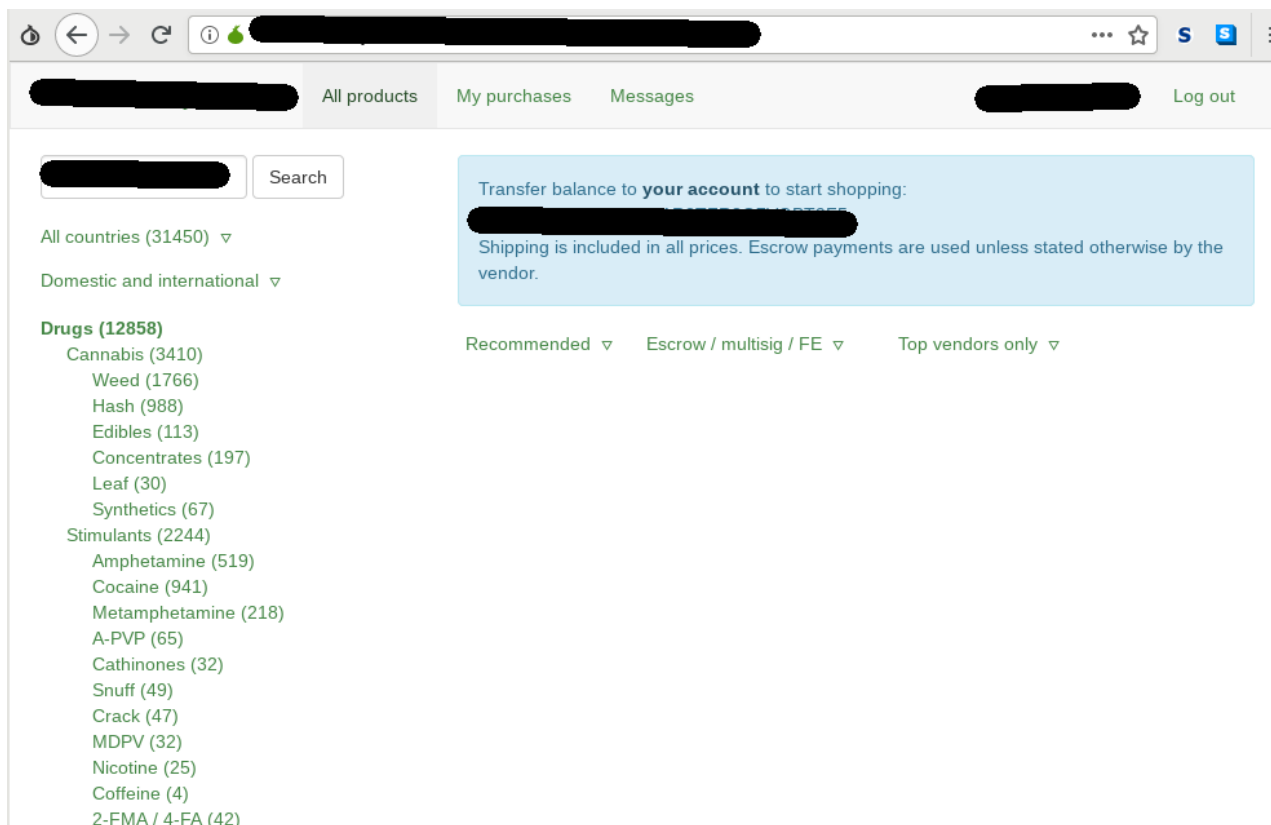
Veškeré tyto e-mailové adresy mohou být použity k phishingu či různých cíleným útokům jak na zaměstnance společnosti, tak i na její zákazníky. Zároveň i v případě, že by náhodou žádné z daných e-mailových adres již nebyly aktivní, stále mohou útočníkovi naznačit jaká struktura e-mailových adres je ve firmě používána.



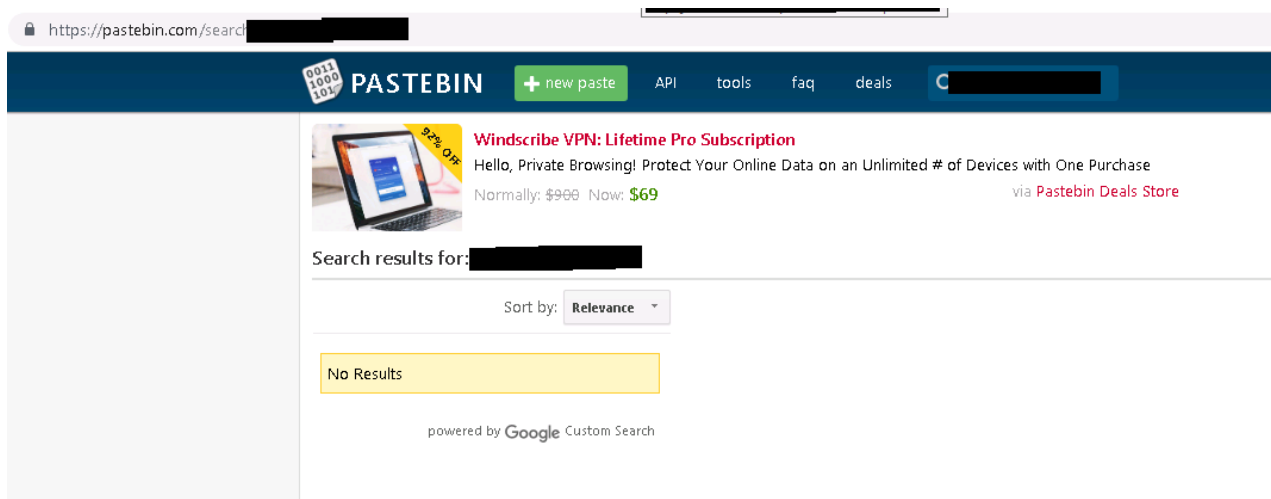
Obrázek 1: Domovská stránka společnosti



Obrázek 3: OSINT analýza v přehlednější podobě, resp. jeden z mnoha používaných nástrojů



Obrázek 4: Silk Road, jeden z nejznámějších darkmarketů (a jeden z mnoha zkoušených) neobsahuje žádné informace ze kterých by bylo možno usuzovat na hacknutí společnosti a následný prodej citlivých informací



Obrázek 5: Žádné relevantní citlivé informace týkající se společnosti nebyly na paste-bin.com nalezeny

2.2 Sken bezpečnostních zranitelností

Na základě informací zjištěných během fáze zjišťování informací o společnosti byly spuštěny skeny bezpečnostních zranitelností na nalezené systémy společnosti. A to jak přímo

na dané servery, tak na případné webové aplikace na nich, z důvodu specifík bezpečnostních zranitelností webových aplikací. Jedná se o prvotní fázi zjišťování potenciálních zranitelností v systémech. Jedná se o automatizované skeny zranitelností pomocí nástrojů, které jsou běžně útočníkům k dispozici. Identifikované systémy na které byly spuštěny skeny zranitelností jsou uvedeny v seznamu Domény. Během testování bylo zjištěno, že společnost používá bezpečnostní opatření zabráňující port skenu. Z důvodu omezené časové dotace k testování byl tento systém v průběhu testování vypnut pro skeny z naší testovací IP. Je pravděpodobné, že méně zkušeného útočníka takové bezpečnostní opatření odradí, nicméně v případě dostatečné časové dotace není problém většinu takových systémů obejít.

Scany zranitelností jsou současně s OSINT analýzou prvním a nejdůležitějším zdrojem informací pro útočníka, které v případě necílených útoků často rozhodují o tom, že útočník se na danou společnost “pořádne podívá” nebo si naopak najde jiný, jednodušší cíl k napadení.

2.3 Fáze exploitace nalezených zranitelností

Po dokončení skenování nalezených systémů (Kapitola 3) jsme provedli ruční důkladné ověření těch zranitelností, které byly bezpečnostním skenem hodnoceny jako závažné. Jedná se o fázi ve které útočník zkouší, zda je možné identifikované zranitelnosti exploituovat a získat tak z nich nějaký užitek. V případě Blackhat testu se snažíme o exploitaci takových zranitelností, na kterých lze nejlépe demonstrovat jejich závažnost a důležitost informační bezpečnosti. Vzhledem k omezené časové dotaci však neprovádíme však exploitaci všech nalezených zranitelností jako u klasického penetračního testu.

2.3.1 Úspěšná demonstrace odchycení FTP přihlašovacích údajů

Dalším potenciálním bezpečnostním nedostatkem, který může vést ke kompromitaci dat společnosti či jejich zákazníků je používání FTP serveru na IP adresách (nález 3.1.1). Na přiloženém snímku obrazovky je vidět, že přenášené přihlašovací údaje je možné zachytit při odposlechu na síti a to po celé délce od uživatele až k FTP serveru. Pro naše testování, vzhledem k omezené časové a finanční dotaci byly použity vymyšlené přihlašovací údaje username / password pro demonstraci samotného principu odchycení přihlašovacích údajů.

No.	Time	Source	Destination	Protocol	Length	Info
5	0.23055326			TCP	68	54833 > ftp [ACK] Seq=1 Ack=21 Win=29200 Len=0 TSval=17623829 TSecr=1968990065
6	18.73001221			TCP	68	54833 > ftp [FIN, ACK] Seq=1 Ack=21 Win=29200 Len=0 TSval=17642328 TSecr=1968990065
7	18.83887096			TCP	68	ftp > 54833 [FIN, ACK] Seq=21 Ack=2 Win=29056 Len=0 TSval=1968994717 TSecr=17642328
8	18.83890485			TCP	68	54833 > ftp [ACK] Seq=2 Ack=22 Win=29200 Len=0 TSval=17642437 TSecr=1968994717
9	27.01119485			TCP	76	40808 > ftp [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=17650609 TSecr=0 WS=128
10	27.80589952			TCP	76	ftp > 40808 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1273 SACK_PERM=1 TSval=1968996958 TSecr=17650609 WS=128
11	27.80594760			TCP	68	40808 > ftp [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=17651404 TSecr=1968996958
12	27.91313098			FTP		
13	27.91319406			TCP	68	40808 > ftp [ACK] Seq=1 Ack=21 Win=29312 Len=0 TSval=17651512 TSecr=1968996986
14	27.91347808			FTP	83	Request: USER uzivatel
15	28.05424439			TCP	68	ftp > 40808 [ACK] Seq=21 Ack=16 Win=29056 Len=0 TSval=1968997021 TSecr=17651512
16	28.12732603			FTP	102	Response: 331 Please specify the password.
17	28.12761162			FTP	80	Request: PASS heslo
18	28.27104372			TCP	68	ftp > 40808 [ACK] Seq=55 Ack=28 Win=29056 Len=0 TSval=1968997076 TSecr=17651726
19	30.98798034			FTP	90	Response: 530 Login incorrect.
20	30.98827277			TCP	68	40808 > ftp [FIN, ACK] Seq=28 Ack=77 Win=29312 Len=0 TSval=17654587 TSecr=1968997754
21	31.09654884			TCP	68	ftp > 40808 [FIN, ACK] Seq=77 Ack=29 Win=29056 Len=0 TSval=1968997782 TSecr=17654587
22	31.0968728			TCP	68	40808 > ftp [ACK] Seq=29 Ack=78 Win=29312 Len=0 TSval=17654695 TSecr=1968997782

▶ Frame 5: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface 0
 ▶ Linux cooked capture
 ▶ Internet Protocol Version 4, Src: [redacted]
 ▶ Transmission Control Protocol, Src Port: 54833 (54833), Dst Port: ftp (21), Seq: 1, Ack: 21, Len: 0

Obrázek 6: Odchycené ukázkové přihlašovací údaje username / password

2.3.2 Úspěšná demonstrace odchycení POP přihlašovacích údajů

Dalším potenciálním bezpečnostním nedostatkem, který může vést ke kompromitaci dat společnosti či jejich zákazníků je nevynucování šifrování POP na IP adrese [redacted] (nález 3.3.2). Na přiloženém snímku obrazovky je vidět, že přenášené přihlašovací údaje je možné zachytit při odposlechu na síti a to po celé délce od uživatele až k POP serveru. Pro naše testování, vzhledem k omezené časové a finanční dotaci byly použity vymyšlené přihlašovací údaje username / password pro demonstraci samotného principu odchycení přihlašovacích údajů.

Time	Source	Destination	Protocol	Length	Info
1	0.00000000		TCP	76	35140 > newacct [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=9224695 TSecr=0 WS=128
2	0.05218334		TCP	76	newacct > 35140 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1326 WS=256 SACK_PERM=1 TSval=8882056 TSecr=9224695
3	0.05224267		TCP	68	35140 > newacct [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=9224747 TSecr=8882056
4	0.10735936		POP3		
5	0.10740068		TCP	68	35140 > newacct [ACK] Seq=1 Ack=119 Win=29312 Len=0 TSval=9224802 TSecr=8882061
6	0.10800085		POP3	91	C: USER test@example.com
7	0.25561287		TCP	68	35140 > newacct [ACK] Seq=1 Ack=119 Win=29312 Len=0 TSval=9224803 TSecr=8882061
8	0.32835484		POP3	90	S: +OK test@example.com
9	0.32887388		POP3	80	C: PASS heslo
10	0.40645230		TCP	68	35140 > newacct [ACK] Seq=1 Ack=119 Win=29312 Len=0 TSval=9224804 TSecr=8882061
11	3.45490694		POP3	109	S: -ERR Unknown user or incorrect password
12	3.4557756		POP3	74	C: QUIT
13	3.57772667		TCP	68	newacct > 35140 [ACK] Seq=182 Ack=42 Win=65536 Len=0 TSval=8882408 TSecr=9228151
14	3.61684969		POP3		
15	3.61688845		TCP	68	newacct > 35140 [FIN, ACK] Seq=227 Ack=42 Win=65536 Len=0 TSval=8882410 TSecr=9228151
16	3.61715874		TCP	68	35140 > newacct [FIN, ACK] Seq=42 Ack=228 Win=29312 Len=0 TSval=9228312 TSecr=8882410
17	3.68376606		TCP	68	newacct > 35140 [ACK] Seq=228 Ack=43 Win=65536 Len=0 TSval=8882417 TSecr=9228312
18	76.5049837		TCP	76	35152 > newacct [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=9251200 TSecr=0 WS=128

Obrázek 7: Odchycené ukázkové přihlašovací údaje username / password

2.3.3 Úspěšná exploitace zranitelnosti Heartbleed

Heartbleed je bezpečnostní zranitelnost v OpenSSL způsobená programátorskou chybou čtení mimo hranice. Umožňuje útočníkovi získat obsah paměti procesu ve kterém je použita zranitelná verze OpenSSL. Jedná se o chybu z poloviny roku 2014, je tedy již přes 4 roky stará. I z toho důvodu je veřejně dostupné velké množství funkčních a jednoduše použitelných exploitů na tuto zranitelnost.

V průběhu vulnerability skenu byla tato zranitelnost nalezena (3.3.4) na některých službách na serveru [redacted]. Jelikož se jedná o jednoduše exploitovatelnou zranitel-

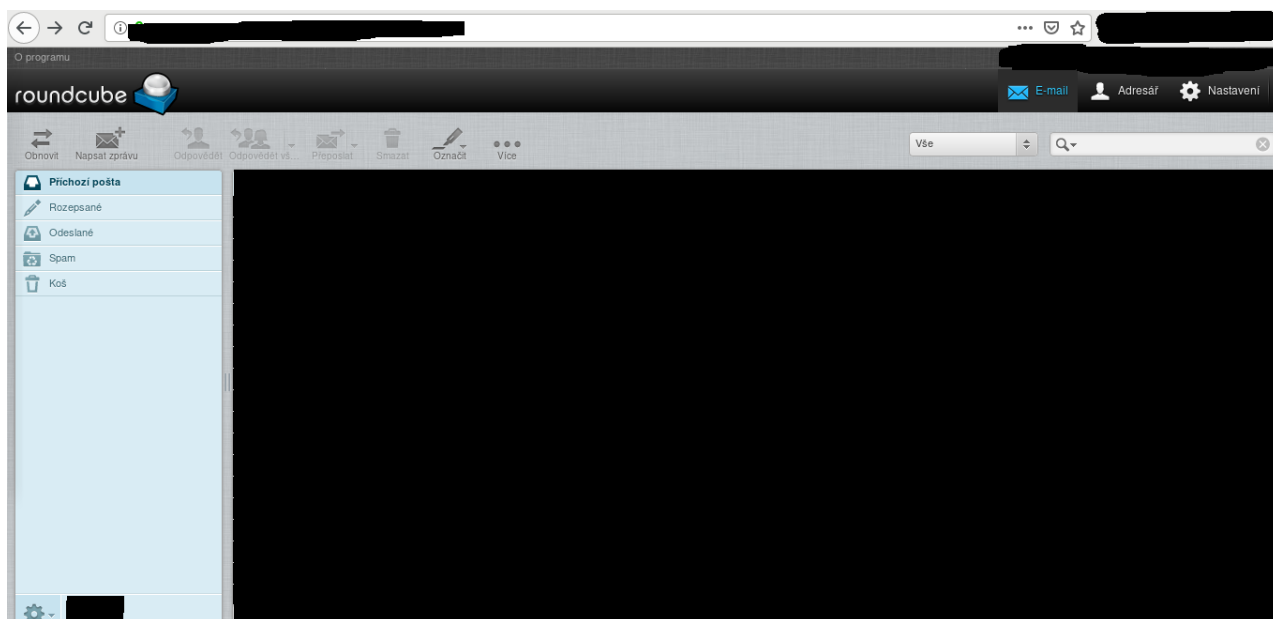
nost s prakticky jistými výsledky, je velmi pravděpodobné, že útočník by ji použil jako první.

Za použití exploitu pro získání obsahu paměti pomocí zranitelnost heartbleed jsme sestavili skript, který s časovými rozestupy získával obsah paměti procesu http s cílem identifikovat v paměti citlivé informace jako přihlašovací údaje, session cookies, různá hesla a další.

Konkrétní instance paměti získaná exploitováním zranitelnosti heartbleed obsahovala následující informace (anonymizováno):

```
[...]  
0310: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0320: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0330: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0340: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0350: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0360: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0370: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0380: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
[...]
```

Z obsahu získané paměti je možné identifikovat přihlašovací údaje do webmailu dostupného na adrese [REDACTED]. V tomto případě se jedná o přihlašovací jméno / e-mailovou adresu [REDACTED] s heslem [REDACTED]. Pravděpodobně se jedná o zaměstnance jednoho ze zákazníků společnosti [REDACTED]. Získané přihlašovací údaje byly úspěšně použity na serveru [REDACTED], jak je patrné z přiloženého snímku obrazovky.



Obrázek 8: Úspěšné přihlášení do e-mailové schránky zákazníka

V případě dostatečné časové dotace (tedy v případě dostatečné motivace útočníka) je útočník schopen tímto způsobem získat přístup ke všem přihlašovacím údajům všech uživatelů webmailu dostupného na adrese [REDACTED] a tím ke všem e-mailům, které jsou pro dané uživatelské účty na serveru dostupné.

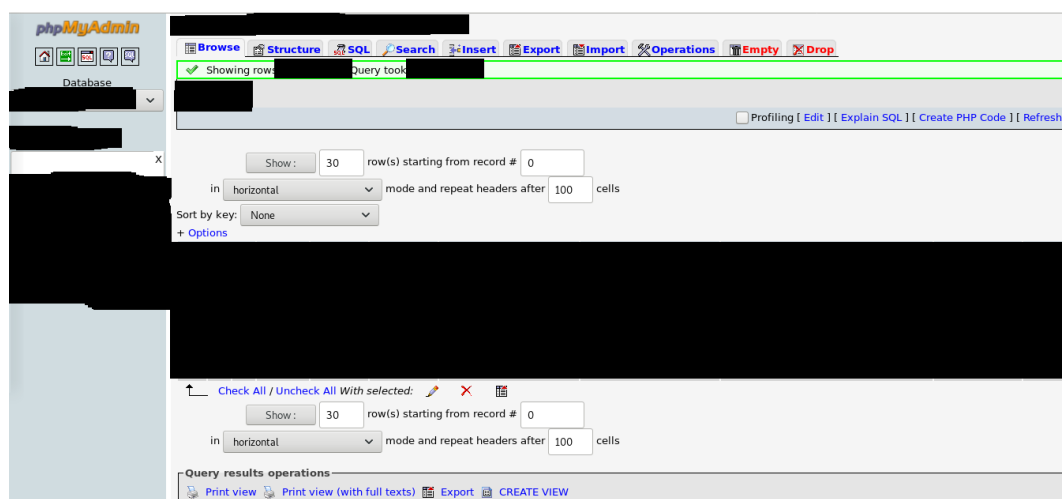
E-maily mohou obsahovat citlivé údaje o stavu firmy, zaměstnancích, platební morálce firmy a mnoho dalšího. Nález je o to závažnější, že se jedná o zákazníka, který služby testované společnosti využívá a předpokládá, že jsou dostatečně zabezpečené.

Přístup k e-mailovým schránkám všech zákazníků používajících server [REDACTED] je závažným nedostatkem, který je potřeba co nejdříve řešit.

2.3.4 Úspěšná exploitace informací z nalezeného .git adresáře, přístup k administraci webu

Během vulnerability skenu bylo zjištěno, že na webovém serveru [REDACTED] je dostupný adresář .git (nález 3.6.1). Jedná se o potenciálně závažnou zranitelnost, protože útočník může být schopen obsah .git adresáře stáhnout. Přesně takto jsme postupovali, pro automatizaci stahování .git adresáře jsme použili nástroj gitpillage.sh. Díky tomu jsme získali obsah .git adresáře a na základě toho i soubory v něm uložené. Jedním z těchto souborů byl [REDACTED]. Jedná se pravděpodobně o konfigurační soubor webové aplikace, jelikož v něm byly nalezeny přihlašovací údaje k MySQL databázi: [REDACTED] / [REDACTED].

Na umístění [REDACTED]/phpmyadmin (klasické umístění) se nachází aplikace phpMyAdmin, která umožňuje správu MySQL databáze přes webové rozhraní. Logickým krokem tedy bylo získané přihlašovací údaje vyzkoušet, což bylo úspěšné jak je možné vidět na následujícím snímku obrazovky.

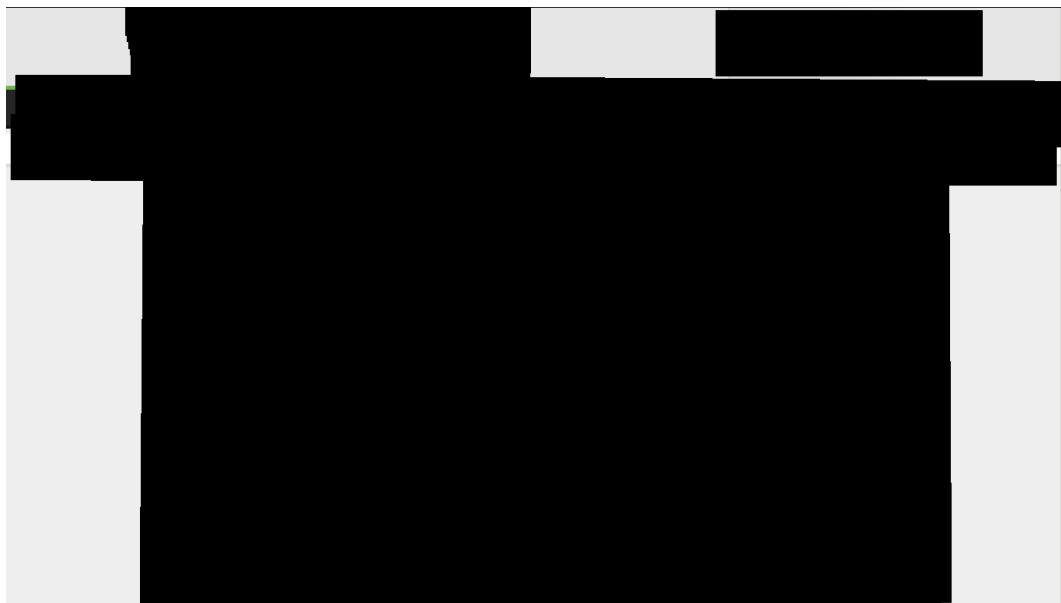


Obrázek 9: Úspěšné přihlášení do aplikace phpMyAdmin, seznam administrátorů webu

Z MySQL tabulky [REDACTED] je možné získat přihlašovací jména administrátorů webu [REDACTED] a hashe jejich přihlašovacích hesel. Během okamžiku bylo crackováním

hashů zjištěno, že hash [REDACTED] odpovídá řetězci [REDACTED], heslo pro uživatele [REDACTED] je tedy [REDACTED].

Na předpokládaném umístění [REDACTED]/admin se nachází vstup do administrace webu [REDACTED]. Přihlašovací údaje [REDACTED] / [REDACTED] fungují a umožňují útočnickovi modifikaci webové aplikace a poskytuje mu úplnou kontrolu nad ní. Útočník může se stránkou manipulovat, napadnou návštěvníky webu atd. a to s cílem poškození společnosti či napadení jejich návštěvníků.



Obrázek 10: Úspěšné přihlášení do administrace webu

3 Sken bezpečnostních zranitelností

3.1 Server 10.0.0.1

3.1.1 Použitý FTP server ■

Závažnost: Ovlivněné systémy:

■

•

Nález

Vzdálený ftp server umožňuje přihlášení pomocí jména a hesla přenášeného v nešifrované podobě sítí.

127.0.0.1 (tcp/21)

The remote FTP banner is :

220 FTP 1.2.3 Server (FTP) [127.0.0.1]

Riziko

Toto může vést k odchycení přihlašovacích údajů útočníkem a jejich zneužití.

Doporučení

Doporučujeme ftp nepoužívat a místo něho nasadit SFTP (součástí SSH) nebo FTPS (FTP přes SSL), které používají šifrované spojení.

3.1.2 Podpora SSL verze 2 a 3 ■

Závažnost: **Ovlivněné systémy:**



•



Nález

Během testu bylo zjištěno, že daná služba podporuje SSL verze 2 a/nebo 3. Ani jeden z těchto protokolů by již neměl být používán z důvodu vyskytujících se zranitelností a nedostatků.

Riziko

Protokoly SSL 2 a 3 již nejsou doporučeny pro zabezpečenou komunikaci, jelikož obsahují závažné nedostatky, které může případný útočník být schopen zneužít a získat tak přenášená data.

Doporučení

Doporučujeme ve všech aplikacích na všech serverech kde byla nalezena tato zranitelnost zakázat používání SSL 2 a 3, a používat výhradně TLS 1.1 či novější.

3.1.3 SSL podporovány slabé šifry ■

Závažnost: Ovlivněné systémy:

-
-
-

Nález

Bylo zjištěno, že v SSL jsou povoleny následující slabé šifry.

EXP-EDH-RSA-DES-CBC-SHA	Kx=DH(512)	Au=RSA	Enc=DES-CBC(40)	Mac=SHA1	export
EDH-RSA-DES-CBC-SHA	Kx=DH	Au=RSA	Enc=DES-CBC(56)	Mac=SHA1	
EXP-ADH-DES-CBC-SHA	Kx=DH(512)	Au=None	Enc=DES-CBC(40)	Mac=SHA1	export
EXP-ADH-RC4-MD5	Kx=DH(512)	Au=None	Enc=RC4(40)	Mac=MD5	export
ADH-DES-CBC-SHA	Kx=DH	Au=None	Enc=DES-CBC(56)	Mac=SHA1	
EXP-DES-CBC-SHA	Kx=RSA(512)	Au=RSA	Enc=DES-CBC(40)	Mac=SHA1	export
EXP-RC2-CBC-MD5	Kx=RSA(512)	Au=RSA	Enc=RC2-CBC(40)	Mac=MD5	export
EXP-RC4-MD5	Kx=RSA(512)	Au=RSA	Enc=RC4(40)	Mac=MD5	export
DES-CBC-SHA	Kx=RSA	Au=RSA	Enc=DES-CBC(56)	Mac=SHA1	

Riziko

Používání slabých šifrovacích algoritmů oslabuje použité šifrování a může vést až k jejich prolomení a získání citlivých dat útočníkem.

Doporučení

Doporučujeme nastavit daný server tak, aby tyto slabé šifry nebyly používány.

3.1.4 Nedůvěryhodný SSL certifikát ■

Závažnost: Ovlivněné systémy:



•



Nález

Bylo zjištěno, že na serveru je buď použit certifikát platný pro jinou doménu, je self-signed či podepsaný nedůvěryhodnou / neznámou certifikační autoritou.

Riziko

Používání certifikátu pro jinou doménu, self-signed certifikátu nebo certifikátu podepsaného neznámou certifikační autoritou snižuje důvěryhodnost a tím i bezpečnost šifrovaného spojení.

Doporučení

Doporučujeme vygenerování a používání certifikátu určeného pro danou doménu. Certifikát by měl být podepsán důvěryhodnou certifikační autoritou.

3.1.5 SSL podporovány středně slabé šifry ■

Závažnost: Ovlivněné systémy:



•

Nález

Během testu bylo zjištěno, že daná služba na dané adrese podporuje středně slabé šifry. Jedná se o následující šifry:

EDH-RSA-DES-CBC3-SHA	Kx=DH	Au=RSA	Enc=3DES-CBC(168)	Mac=SHA1
ADH-DES-CBC3-SHA	Kx=DH	Au=None	Enc=3DES-CBC(168)	Mac=SHA1
ECDHE-RSA-DES-CBC3-SHA	Kx=ECDH	Au=RSA	Enc=3DES-CBC(168)	Mac=SHA1
AECDH-DES-CBC3-SHA	Kx=ECDH	Au=None	Enc=3DES-CBC(168)	Mac=SHA1
DES-CBC3-SHA	Kx=RSA	Au=RSA	Enc=3DES-CBC(168)	Mac=SHA1

Riziko

Použití slabých šifrovacích algoritmů snižuje bezpečnost celého šifrovaného spojení.

Doporučení

Doporučujeme daný server nakonfigurovat tak, aby tyto středně slabé šifry nepodporoval. Konkrétní konfigurace se odvíjí od konkrétního serveru (apache, postfix, ...).

3.1.6 Podporovány RC4 šifry ■

Závažnost: Ovlivněné systémy:

■

•

Nález

Během testu bylo zjištěno, že webový server na kterém běží testovaná aplikace podporuje cipher suites, které používají RC4 šifry. Jedná se o následující cipher suites:

EXP-ADH-RC4-MD5	Kx=DH(512)	Au=None	Enc=RC4(40)	Mac=MD5	export
EXP-RC4-MD5	Kx=RSA(512)	Au=RSA	Enc=RC4(40)	Mac=MD5	export

Riziko

Algoritmus RC4 nekorektně pracuje se stavovými daty a klíčem během inicializační fáze. Toto může umožnit útočníkovi provést útok, který může vést k získání potenciálně citlivých informací.

Doporučení

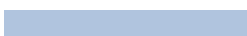
Doporučujeme v konfiguraci webového serveru vypnout podporu pro dané cipher suites.

3.1.7 SSH povoleny slabé algoritmy ■

Závažnost: **Ovlivněné systémy:**



•



Nález

V průběhu testu bylo zjištěno, že v SSH jsou povoleny tyto slabé algoritmy:

```
arcfour  
arcfour128  
arcfour256
```

Riziko

Dané algoritmy jsou slabé a nedostatečné. Neposkytují tedy dostatečnou ochranu přenášených dat.

Doporučení

Doporučujeme používat takové nastavení, které zajistí používání pouze bezpečných algoritmů.

3.2 Server 10.0.0.2

3.2.1 Nedůvěryhodný SSL certifikát ■

Závažnost: Ovlivněné systémy:



•



Nález

Bylo zjištěno, že na serveru je buď použit certifikát platný pro jinou doménu, je self-signed či podepsaný nedůvěryhodnou / neznámou certifikační autoritou.

Riziko

Používání certifikátu pro jinou doménu, self-signed certifikátu nebo certifikátu podepsaného neznámou certifikační autoritou snižuje důvěryhodnost a tím i bezpečnost šifrovaného spojení.

Doporučení

Doporučujeme vygenerování a používání certifikátu určeného pro danou doménu. Certifikát by měl být podepsán důvěryhodnou certifikační autoritou.

3.3 Server 10.0.0.3

3.3.1 Nepodporovaný operační systém ■

Závažnost: **Ovlivněné systémy:**

■

•

Nález

V průběhu testů bylo zjištěno, že na daném systému se nachází stará a nepodporovaná verze operačního systému.

Riziko

Pro nepodporovaný operační systém již nejsou vydávány bezpečnostní aktualizace. Pokud tedy byla objevena chyba, která se daného systému týká, není tato chyba opravena ve formě bezpečnostní aktualizace. Toto nechává otevřené dveře pro útočníky.

Doporučení

Důrazně doporučujeme nasadit nejnovější podporovaný operační systém s aktuálními aktualizacemi. Zároveň doporučujeme provádět pravidelné aktualizace.

3.3.2 POP nešifrovaná hesla při přenosu ■

Závažnost: Ovlivněné systémy:



•

Nález

Bylo zjištěno, že POP server umožňuje přihlášení jménem a heslem, které po síti putuje v nešifrované podobě.

Riziko

Toto umožňuje útočníkovi v průběhu přenosu přihlašovacích údajů je zachytit a zneužít.

Doporučení

Doporučujeme nasazení a používání výhradně TLS šifrovaného kanálu na SMTP server.

3.3.3 SMTP nešifrovaná hesla při přenosu ■

Závažnost: Ovlivněné systémy:

■

•

Nález

Bylo zjištěno, že SMTP server umožňuje přihlášení jménem a heslem, které po síti putuje v nešifrované podobě.

Riziko

Toto umožňuje útočníkovi v průběhu přenosu přihlašovacích údajů je zachytit a zneužít. V případě, že je použit některý z příkazů USER, AUTH PLAIN či AUTH LOGIN).

Doporučení

Doporučujeme nasazení a používání výhradně TLS šifrovaného kanálu na SMTP server.

3.3.4 Zranitelnost Heartbleed ■

Závažnost: Ovlivněné systémy:

-
-
-

Nález

Během testu bylo zjištěno, že server je náchylný na zranitelnost známou jako Heartbleed. Jedná se o information disclosure zranitelnost způsobenou programátorskou chybou čtení mimo hranice. V době testování této zranitelnosti byly v paměti k dispozici například tato data (anonymizováno):

```
[...]  
0310: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0320: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0330: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0340: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0350: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0360: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0370: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0380: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
[...]
```

Riziko

Posláním speciálně připraveného paketu je útočník schopen ze serveru získat až 64 KB paměti daného procesu. Tato paměť může obsahovat citlivé informace jako například hesla, soukromé klíče a jiná citlivá data.

Doporučení

Důrazně doporučuje aktualizovat OpenSSL na verzi 1.0.1g nebo novější.

3.3.5 Podpora SSL verze 2 a 3 ■

Závažnost: **Ovlivněné systémy:**



- [redacted]
- [redacted]

Nález

Během testu bylo zjištěno, že daná služba podporuje SSL verze 2 a/nebo 3. Ani jeden z těchto protokolů by již neměl být používán z důvodu vyskytujících se zranitelností a nedostatků.

Riziko

Protokoly SSL 2 a 3 již nejsou doporučeny pro zabezpečenou komunikaci, jelikož obsahují závažné nedostatky, které může případný útočník být schopen zneužít a získat tak přenášená data.

Doporučení

Doporučujeme ve všech aplikacích na všech serverech kde byla nalezena tato zranitelnost zakázat používání SSL 2 a 3, a používat výhradně TLS 1.1 či novější.

3.3.6 Nedůvěryhodný SSL certifikát ■

Závažnost: **Ovlivněné systémy:**

■	•	
	•	
	•	
	•	

Nález

Bylo zjištěno, že na serveru je buď použit certifikát platný pro jinou doménu, je self-signed či podepsaný nedůvěryhodnou / neznámou certifikační autoritou.

Riziko





Používání certifikátu pro jinou doménu, self-signed certifikátu nebo certifikátu podepsaného neznámou certifikační autoritou snižuje důvěryhodnost a tím i bezpečnost šifrovaného spojení.

Doporučení

Doporučujeme vygenerování a používání certifikátu určeného pro danou doménu. Certifikát by měl být podepsán důvěryhodnou certifikační autoritou.

3.3.7 OpenSSL 'ChangeCipherSpec' MiTM zranitelnost ■

Závažnost: Ovlivněné systémy:

- 
- 
- 
- 

Nález

Během testu bylo zjištěno, že použitá verze OpenSSL obsahuje zranitelnost man-in-the-middle známou jako ChangeCipherSpec. Jedná se o zranitelnost způsobenou reakcí na speciálně provedený handshake.

Riziko

Tato zranitelnost může útočnickovi umožnit dešifrovat nebo podvrhnout SSL zprávu tím způsobem, že je serveru řečeno aby zašifroval komunikaci ještě před výměnou klíče, čímž dochází k použití predikovatelných klíčů což umožňuje útočnickovi dešifrování potenciálně citlivých informací.

Doporučení

Doporučujeme aktualizovat OpenSSL na verzi 1.0.0m / 1.0.1h nebo novější.

3.3.8 Podporováno SSL3, možný útok POODLE ■

Závažnost: Ovlivněné systémy:

- [redacted]
- [redacted]
- [redacted]
- [redacted]

Nález

V průběhu testu byla na daném serveru a dané službě zjištěna zranitelnost POODLE (Padding Oracle On Downgraded Legacy Encryption). Jedná se o man-in-the-middle information disclosure útok umožňující útočnickovi dešifrování vybraného bytu ciphertextu.

Riziko

V případě úspěšného útoku POODLE může být útočník schopen dešifrovat šifrovanou komunikaci. Toto může vést k úniku citlivých informací jako například přihlašovací údaje, session cookies či jakékoliv jiné citlivé informace, které se mohou mezi aplikací a uživatelem přenášet.

Doporučení

Jedná se o zranitelnost, která je principiální pro SSLv3, nikoliv pro konkrétní implementaci. Doporučujeme tedy zakázání SSLv3 na úrovni konfigurace daného serveru a používání pouze TLSv1.1 nebo vyšší verze.

3.3.9 SSL podporovány slabé šifry ■

Závažnost: Ovlivněné systémy:



•

Nález

Používání slabých šifrovacích algoritmů oslabuje použité šifrování a může vést až k jejich prolomení a získání citlivých dat útočníkem.

EXP-EDH-RSA-DES-CBC-SHA	Kx=DH(512)	Au=RSA	Enc=DES-CBC(40)	Mac=SHA1	export
EDH-RSA-DES-CBC-SHA	Kx=DH	Au=RSA	Enc=DES-CBC(56)	Mac=SHA1	
EXP-ADH-DES-CBC-SHA	Kx=DH(512)	Au=None	Enc=DES-CBC(40)	Mac=SHA1	export
EXP-ADH-RC4-MD5	Kx=DH(512)	Au=None	Enc=RC4(40)	Mac=MD5	export
ADH-DES-CBC-SHA	Kx=DH	Au=None	Enc=DES-CBC(56)	Mac=SHA1	
EXP-DES-CBC-SHA	Kx=RSA(512)	Au=RSA	Enc=DES-CBC(40)	Mac=SHA1	export
EXP-RC2-CBC-MD5	Kx=RSA(512)	Au=RSA	Enc=RC2-CBC(40)	Mac=MD5	export
EXP-RC4-MD5	Kx=RSA(512)	Au=RSA	Enc=RC4(40)	Mac=MD5	export
DES-CBC-SHA	Kx=RSA	Au=RSA	Enc=DES-CBC(56)	Mac=SHA1	

Riziko




Doporučujeme nastavit daný server tak, aby tyto slabé šifry nebyly používány.

Doporučení

Doporučujeme nastavit daný server tak, aby tyto slabé šifry nebyly používány.

3.3.10 SSL podporovány středně slabé šifry ■

Závažnost: Ovlivněné systémy:

- 
- 
- 

Nález

Během testu bylo zjištěno, že daná služba na dané adrese podporuje středně slabé šifry. Jedná se o následující šifry:

EDH-RSA-DES-CBC3-SHA	Kx=DH	Au=RSA	Enc=3DES-CBC(168)	Mac=SHA1
ADH-DES-CBC3-SHA	Kx=DH	Au=None	Enc=3DES-CBC(168)	Mac=SHA1
ECDHE-RSA-DES-CBC3-SHA	Kx=ECDH	Au=RSA	Enc=3DES-CBC(168)	Mac=SHA1
AECDH-DES-CBC3-SHA	Kx=ECDH	Au=None	Enc=3DES-CBC(168)	Mac=SHA1
DES-CBC3-SHA	Kx=RSA	Au=RSA	Enc=3DES-CBC(168)	Mac=SHA1

Riziko

Použití slabých šifrovacích algoritmů snižuje bezpečnost celého šifrovaného spojení.

Doporučení

Doporučujeme daný server nakonfigurovat tak, aby tyto středně slabé šifry nepodporoval. Konkrétní konfigurace se odvíjí od konkrétního serveru (apache, postfix, ...).

3.3.11 Podporovány RC4 šifry ■

Závažnost: Ovlivněné systémy:

■	•	
	•	
	•	
	•	
	•	

Nález

Během testu bylo zjištěno, že webový server na kterém běží testovaná aplikace podporuje cipher suites, které používají RC4 šifry. Jedná se o následující cipher suites:

EXP-ADH-RC4-MD5	Kx=DH(512)	Au=None	Enc=RC4(40)	Mac=MD5	export
EXP-RC4-MD5	Kx=RSA(512)	Au=RSA	Enc=RC4(40)	Mac=MD5	export
ADH-RC4-MD5	Kx=DH	Au=None	Enc=RC4(128)	Mac=MD5	
ECDHE-RSA-RC4-SHA	Kx=ECDH	Au=RSA	Enc=RC4(128)	Mac=SHA1	
AECDH-RC4-SHA	Kx=ECDH	Au=None	Enc=RC4(128)	Mac=SHA1	
RC4-MD5	Kx=RSA	Au=RSA	Enc=RC4(128)	Mac=MD5	
RC4-SHA	Kx=RSA	Au=RSA	Enc=RC4(128)	Mac=SHA1	

Riziko

Algoritmus RC4 nekorektně pracuje se stavovými daty a klíčem během inicializační fáze. Toto může umožnit útočníkovi provést útok, který může vést k získání potenciálně citlivých informací.

Doporučení

Doporučujeme v konfiguraci webového serveru vypnout podporu pro dané cipher suites.

3.4 Server 10.0.0.4

3.4.1 SSL podporovány středně slabé šifry ■

Závažnost: Ovlivněné systémy:

■ • ■

Nález

Během testu bylo zjištěno, že daná služba na dané adrese podporuje středně slabé šifry. Jedná se o následující šifry:

ECDHE-RSA-DES-CBC3-SHA	Kx=ECDH	Au=RSA	Enc=3DES-CBC(168)	Mac=SHA1
DES-CBC3-SHA	Kx=RSA	Au=RSA	Enc=3DES-CBC(168)	Mac=SHA1

Riziko

Použití slabých šifrovacích algoritmů snižuje bezpečnost celého šifrovaného spojení.

Doporučení

Doporučujeme daný server nakonfigurovat tak, aby tyto středně slabé šifry nepodporoval. Konkrétní konfigurace se odvíjí od konkrétního serveru (apache, postfix, ...).

3.5 Server 10.0.0.5

3.5.1 Nedůvěryhodný SSL certifikát ■

Závažnost: Ovlivněné systémy:



•



Nález

Bylo zjištěno, že na serveru je buď použit certifikát platný pro jinou doménu, je self-signed či podepsaný nedůvěryhodnou / neznámou certifikační autoritou.

Riziko

Používání certifikátu pro jinou doménu, self-signed certifikátu nebo certifikátu podepsaného neznámou certifikační autoritou snižuje důvěryhodnost a tím i bezpečnost šifrovaného spojení.

Doporučení

Doporučujeme vygenerování a používání certifikátu určeného pro danou doménu. Certifikát by měl být podepsán důvěryhodnou certifikační autoritou.

3.5.2 POP3 - STLS PLaintext Command Injection ■

Závažnost: Ovlivněné systémy:



•

Nález

Během testu bylo zjištěno, že pop3 server je náchylný na command injection v průběhu domluvy šifrovaného komunikačního kanálu.

Při poslání následujícího paketu:

```
STLS\r\nCAPA\r\n
```

Došlo k následující odpovědi ze serveru:

```
+OK Begin TLS negotiation
```

```
+OK Capability list follows
```

Riziko

Zranitelnost umožňuje neautentizovanému útočníkovi injektování příkazů v plaintext fázi tak, aby byly spuštěny v ciphertext fázi.

Doporučení

Doporučujeme aktualizovat POP3 server na nejnovější podporovanou verzi.

3.5.3 Podpora SSL verze 2 a 3 ■

Závažnost: Ovlivněné systémy:

-
-
-

Nález

Během testu bylo zjištěno, že daná služba podporuje SSL verze 2 a/nebo 3. Ani jeden z těchto protokolů by již neměl být používán z důvodu vyskytujících se zranitelností a nedostatků.

Riziko

Protokoly SSL 2 a 3 již nejsou doporučeny pro zabezpečenou komunikaci, jelikož obsahují závažné nedostatky, které může případný útočník být schopen zneužít a získat tak přenášená data.

Doporučení

Doporučujeme ve všech aplikacích na všech serverech kde byla nalezena tato zranitelnost zakázat používání SSL 2 a 3, a používat výhradně TLS 1.1 či novější.

3.5.4 SSL podporovány slabé šifry ■

Závažnost: Ovlivněné systémy:



•

Nález

Bylo zjištěno, že v SSL jsou povoleny následující slabé šifry.

EXP-EDH-RSA-DES-CBC-SHA	Kx=DH(512)	Au=RSA	Enc=DES-CBC(40)	Mac=SHA1	export
EDH-RSA-DES-CBC-SHA	Kx=DH	Au=RSA	Enc=DES-CBC(56)	Mac=SHA1	
EXP-ADH-DES-CBC-SHA	Kx=DH(512)	Au=None	Enc=DES-CBC(40)	Mac=SHA1	export
EXP-ADH-RC4-MD5	Kx=DH(512)	Au=None	Enc=RC4(40)	Mac=MD5	export
ADH-DES-CBC-SHA	Kx=DH	Au=None	Enc=DES-CBC(56)	Mac=SHA1	
EXP-DES-CBC-SHA	Kx=RSA(512)	Au=RSA	Enc=DES-CBC(40)	Mac=SHA1	export
EXP-RC2-CBC-MD5	Kx=RSA(512)	Au=RSA	Enc=RC2-CBC(40)	Mac=MD5	export
EXP-RC4-MD5	Kx=RSA(512)	Au=RSA	Enc=RC4(40)	Mac=MD5	export
DES-CBC-SHA	Kx=RSA	Au=RSA	Enc=DES-CBC(56)	Mac=SHA1	

Riziko

Používání slabých šifrovacích algoritmů oslabuje použité šifrování a může vést až k jejich prolomení a získání citlivých dat útočníkem.

Doporučení

Doporučujeme nastavit daný server tak, aby tyto slabé šifry nebyly používány.

3.5.5 IMAP - STARTTLS Plaintext Command Injection ■

Závažnost: Ovlivněné systémy:



•



Nález

Během testu bylo zjištěno, že imap server je náchylný na command injection v průběhu domluvy šifrovaného komunikačního kanálu.

Při poslání následujícího paketu:

```
nessus1 STARTTLS\r\nnessus2 CAPABILITY\r\n
```

Došlo k následující odpovědi ze serveru:

```
nessus1 OK begin TLS negotiation now  
nessus2 OK CAPABILITY completed
```

Riziko

Zranitelnost umožňuje neautentizovanému útočníkovi injektování příkazů v plaintext fázi tak, aby byly spuštěny v ciphertext fázi.

Doporučení

Doporučujeme aktualizovat IMAP server na nejnovější podporovanou verzi.

3.5.6 SSL podporovány středně slabé šifry ■

Závažnost: Ovlivněné systémy:

- [redacted]
- [redacted]
- [redacted]

Nález

Během testu bylo zjištěno, že daná služba na dané adrese podporuje středně slabé šifry. Jedná se o následující šifry:

EDH-RSA-DES-CBC3-SHA	Kx=DH	Au=RSA	Enc=3DES-CBC(168)	Mac=SHA1
ADH-DES-CBC3-SHA	Kx=DH	Au=None	Enc=3DES-CBC(168)	Mac=SHA1
ECDHE-RSA-DES-CBC3-SHA	Kx=ECDH	Au=RSA	Enc=3DES-CBC(168)	Mac=SHA1
AECDH-DES-CBC3-SHA	Kx=ECDH	Au=None	Enc=3DES-CBC(168)	Mac=SHA1
DES-CBC3-SHA	Kx=RSA	Au=RSA	Enc=3DES-CBC(168)	Mac=SHA1

Riziko

Použití slabých šifrovacích algoritmů snižuje bezpečnost celého šifrovaného spojení.

Doporučení

Doporučujeme daný server nakonfigurovat tak, aby tyto středně slabé šifry nepodporoval. Konkrétní konfigurace se odvíjí od konkrétního serveru (apache, postfix, ...).

3.5.7 Podporovány RC4 šifry ■

Závažnost: Ovlivněné systémy:



•

Nález

Během testu bylo zjištěno, že webový server na kterém běží testovaná aplikace podporuje cipher suites, které používají RC4 šifry. Jedná se o následující cipher suites:

EXP-ADH-RC4-MD5	Kx=DH(512)	Au=None	Enc=RC4(40)	Mac=MD5	export
EXP-RC4-MD5	Kx=RSA(512)	Au=RSA	Enc=RC4(40)	Mac=MD5	export
ADH-RC4-MD5	Kx=DH	Au=None	Enc=RC4(128)	Mac=MD5	
ECDHE-RSA-RC4-SHA	Kx=ECDH	Au=RSA	Enc=RC4(128)	Mac=SHA1	
AECDH-RC4-SHA	Kx=ECDH	Au=None	Enc=RC4(128)	Mac=SHA1	
RC4-MD5	Kx=RSA	Au=RSA	Enc=RC4(128)	Mac=MD5	
RC4-SHA	Kx=RSA	Au=RSA	Enc=RC4(128)	Mac=SHA1	

Riziko

Algoritmus RC4 nekorektně pracuje se stavovými daty a klíčem během inicializační fáze. Toto může umožnit útočníkovi provést útok, který může vést k získání potenciálně citlivých informací.

Doporučení

Doporučujeme v konfiguraci webového serveru vypnout podporu pro dané cipher suites.

3.6 Webová aplikace example.local

3.6.1 Dostupný adresář .git ■

Závažnost: Ovlivněné systémy:

■ • ■

Nález

Bylo zjištěno, že na následujícím umístění je přístupný Git repozitář.

• ■

Riziko

Útočník může být schopen adresář .git a celý jeho obsah stáhnout, čímž se může dostat k obsahu git adresáře. V případě, že jsou či někdy byly v gitu verzovány soubory s citlivými údaji, může se k nim útočník dostat a tyto údaje zneužít buď přímo nebo k dalším útokům.

Doporučení

Doporučujeme adresář znepřístupnit, buď jeho smazáním nebo nastavením webového serveru tak, aby se k adresáři a žádnému jeho obsahu nebylo možno dostat.

3.6.2 Chybí HSTS hlavička ■

Závažnost: Ovlivněné systémy:



•

Nález

Během testů bylo zjištěno, že webový server nevynucuje HTTP Strict Transport Security (HSTS). Jedná se o mechanismus chránící komunikaci před downgrade útoku a únosem spojení.

Riziko

V případě chybějící HSTS hlavičky může být útočník schopen provést downgrade útoky na šifrované spojení, SSL stripping útok, man in the middle útoky a další.

Doporučení

Doporučujeme nastavení HSTS hlaviček Strict-Transport-Security na webovém serveru.

3.6.3 Přihlašovací formulář s Autocomplete ■

Závažnost: Ovlivněné systémy:



- [redacted]
- [redacted]

Nález

Během penetračního testu bylo zjištěno, že na přihlašovacím formuláři není zakázán autocomplete. Moderní webové prohlížeče umožňují uživatelům ukládání přihlašovacích údajů. Tyto uložené přihlašovací údaje mohou být získány útočníkem buď v případě, že útočník získá přístup k danému webovému prohlížeči nebo například pomocí cross site scripting útoku vůči aplikaci, kdy pomocí xss payloadu útočník přečte heslo z políček pro přihlašovací údaje a odešle na server útočníka.

Page : /

Destination Page: /index.php

Riziko

Je-li v prohlížeči uživatele povoleno automatické ukládání hesel a zároveň není tato funkcionality zakázána v kódu webové stránky, je zde riziko, že citlivá data budou uložena v počítači a můžou být zpřístupněna útočníkovi, který má k počítači přístup.

Doporučení

Doporučujeme přidání autocomplete="off" k danému poli pro heslo pro zakázání výše popsané funkcionality. Ačkoliv některé webové prohlížeče tuto direktivu ignorují a ukládání hesla i přesto podporují, je dobrou praktikou tuto funkcionality zakázat.

3.6.4 Náchylnost na clickjacking ■

Závažnost: Ovlivněné systémy:



- [redacted]
- [redacted]

Nález

Během testů bylo zjištěno, že aplikaci je možno načíst v rámci a provést tzv. clickjacking. Jedná se o útok, kdy útočník načte webovou aplikaci v rámu (iframe) a překryje ji svým obsahem takovým způsobem, že uživatel při interakci s překrývajícími prvky nevědomky interaguje se samotnou webovou aplikací.

Riziko

Riziko spočívá v tom, že útočník může načíst danou aplikaci v rámu, a překryje ji svým obsahem. Když pak uživatel interaguje s útočnickovým obsahem (nějaký atraktivní obsah, například jednoduchá webová hra), nevědomky také interaguje s danou webovou aplikací, která je načtená v rámci. Tímto může útočník uživatele přimět k nevědomé akci s danou aplikací (vytvoření uživatelského účtu, smazání uživatele, atd.).

Doporučení

Doporučujeme použití HTTP hlavičky X-Frame-Options a nastavení její hodnoty na Deny. Další možností je implementovat obranu proti clickjacking v JavaScriptu.

3.6.5 Chybějící parametry cookies - httpOnly ■

Závažnost: Ovlivněné systémy:



- [redacted]
- [redacted]

Nález

Během testů bylo zjištěno, že některé cookies nemají nastaveny parametry, které jsou z hlediska bezpečnosti doporučovány. Jedná se o následující parametry:

- HttpOnly – tento parametr znemožní přístup ke cookie z JavaScriptu, čímž výrazně omezí možnosti útoku XSS

Použité cookies a parametry, které nemají nastaveny:

- [redacted]

Riziko

Rizika v tomto případě vychází z možnosti krádeže cookie a jejího obsahu. V případě nenastaveného parametru HttpOnly může dojít ke krádeži cookie pomocí útoku XSS.

Doporučení

Doporučujeme všem cookies nastavovat parametry HttpOnly a Secure, a to především pro cookies, které udržují identifikátor session nebo jiné potenciálně citlivé informace

3.6.6 Chybějící parametry cookies - secure ■

Závažnost: Ovlivněné systémy:

-
-

Nález

Během testů bylo zjištěno, že některé cookies nemají nastaveny parametry, které jsou z hlediska bezpečnosti doporučovány. Jedná se o následující parametry:

- Secure – zajistí, že cookie je posílána výhradně po zabezpečeném, https kanále, čímž zamezuje odposlechnutí například session id

Použité cookies a parametry, které nemají nastaveny:

-
-
-
-
-
-
-
-
-
-
-

Riziko

Rizika v tomto případě vychází z možnosti krádeže cookie a jejího obsahu. V případě nepoužití parametru Secure může být obsah cookie odposlechnut po cestě požadavku sítě.

Doporučení

Doporučujeme všem cookies nastavovat parametry HttpOnly a Secure, a to především pro cookies, které udržují identifikátor session nebo jiné potenciálně citlivé informace