

Grupa G

Izveštaj o proceni bezbednosti pripremljen za



OWASP Juice shop

Datum izrade: 07.07.2024.



Izjava o poverljivosti

Ovaj izveštaj sadrži osetljive, privilegovane i poverljive informacije. Preduzimaju se mere opreza radi zaštite poverljivosti informacija u ovom dokumentu. Objavljivanje ovog izveštaja može izazvati štetu po ugled OWASP Juice Shop ili olakšati napade protiv OWASP Juice Shop-a. Grupa G neće biti odgovorna za posebne, slučajne, sporedne ili posledične štete koje proizilaze iz upotrebe ovih informacija.

Ograničenje odgovornosti

Napomena da ova procena možda ne otkriva sve ranjivosti koje postoje na sistemima obuhvaćenim angažmanom. Ovaj izveštaj predstavlja sažetak nalaza napravljenih tokom procene u "trenutku" okruženja OWASP Juice Shop. Bilo kakve promene u okruženju tokom perioda testiranja mogu uticati na rezultate procene.

Sadržaj

Izjava o poverljivosti	2
Ograničenje odgovornosti	2
Rezime	4
Opseg	5
Mreže	5
Metodologija testiranja	5
Definicije klasifikacija	5
Klasifikacija rizika	5
Klasifikacije verovatnoće iskorišćavanja	6
Klasifikacija uticaja na biznis	6
Klasifikacije težine popravke	6
Rezultati testiranja	8
Rezultat skeniranja mreže	8
1 – SQL Injection	11
2 – Cross-site scripting	12
3 - Privilege Escalation	14
4 - Sensitive Data Exposure	16
Alati koji su korišćeni	18
Informacije o angažovanju	19
Informacije o klijentu	19
Informacije o verziji dokumenta	19
Kontakt informacije	19

Rezime

Grupa G je izvršila procenu bezbednosti unutrašnje korporativne mreže OWASP Juice Shop-a dana 07.07.2024. Grupa G-ovo penetraciono testiranje simuliralo je napad spoljnog napadača koji pokušava da pristupi sistemima unutar korporativne mreže OWASP Juice Shop-a. Cilj ove procene bio je otkriti i identifikovati ranjivosti u infrastrukturi OWASP Juice Shop-a i predložiti metode za njihovo otklanjanje. Grupa G je identifikovala ukupno 4 ranjivosti u okviru angažmana, koje su razvrstane po ozbiljnosti u tabeli ispod

KRITIČNE	VISOKE	SREDNJE	NISKE
2	2	0	0

Napomena da ova procena možda neće otkriti sve ranjivosti koje postoje na sistemima obuhvaćenim u okviru angažmana. Bilo kakve promene u okruženju tokom perioda testiranja mogu uticati na rezultate procene.

Opseg

Sva testiranja su sprovedena u skladu sa obuhvatom definisanim u Zahtevu za ponudu (RFP) i zvaničnim pisanim komunikacijama. Predmeti koji su obuhvaćeni u okviru su navedeni u nastavku:

Mreže

Mreža	Beleška
127.0.0.1	Local network

Metodologija testiranja

Metodologija testiranja Grupe G bila je podeljena u tri faze: Priprema terena, Procena ciljeva i Izvršenje ranjivosti. Tokom faze pripreme terena, prikupljali smo informacije o mrežnim sistemima OWASP Juice Shop-a. Grupa G je koristila skeniranje portova i druge metode numeracije kako bi precizirala informacije o ciljevima i procenila njihovu vrednost. Zatim smo sprovedi našu ciljanu procenu. Grupa G je simulirala napad na mrežu OWASP Juice Shop-a iskorišćavanjem ranjivosti. Tokom ove faze angažmana, Grupa G je prikupljala dokaze o ranjivostima dok je simulacija sprovedena na način koji ne bi narušio normalno poslovanje.

Definicije klasifikacija

Klasifikacija rizika

Nivo	Ocena	Opis
Kritično	10	Ranjivost predstavlja trenutnu pretnju organizaciji. Uspješno iskorišćavanje može trajno uticati na organizaciju. Hitno je potrebno izvršiti popravku.
Visoko	7-9	Ranjivost predstavlja hitnu pretnju organizaciji, te bi popravka trebalo da bude prioritarna.
Srednje	4-6	Uspješno iskorišćenje je moguće i može rezultirati primetnim poremećajem poslovne funkcionalnosti. Ranjivost treba otkloniti čim to bude moguće.
Nisko	1-3	Ranjivost predstavlja zanemarljivu/minimalnu pretnju organizaciji. Prisustvo ove ranjivosti treba primetiti i otkloniti ako je moguće.

Informaciono	0	Ovi nalazi ne predstavljaju jasnu pretnju organizaciji, ali mogu uzrokovati da poslovni procesi funkcionišu drugačije nego što je željeno ili otkriti osjetljive informacije o kompaniji.
---------------------	----------	---

Klasifikacije verovatnoće iskorišćavanja


Verovatnoća	Opis
Verovatno	Metodi iskorišćavanja su dobro poznati i mogu se izvesti korišćenjem javno dostupnih alata. Napadači sa niskim nivoom veštine i automatizovani alati mogu uspešno iskoristiti ranjivost sa minimalnim teškoćama.
Moguće	Metodi iskorišćavanja su dobro poznati, mogu se izvesti korišćenjem javnih alata, ali zahtevaju konfiguraciju. Razumevanje osnovnog sistema je potrebno za uspešno iskorišćavanje.
Malo verovatno	Iskorišćavanje zahteva duboko razumevanje osnovnih sistema ili napredne tehničke veštine. Možda će biti potrebni precizni uslovi za uspešno iskorišćavanje.

Klasifikacija uticaja na biznis

Uticaj	Opis
Značajan	Uspešno iskorišćenje može rezultirati velikim poremećajima kritičnih poslovnih funkcija širom organizacije i značajnom finansijskom štetom.
Umeren	Successful exploitation may cause significant disruptions to non-critical business functions.
Manji	Uspješno iskorištenje može uticati na nekoliko korisnika, bez uzrokovavanja značajnih poremećaja u rutinskim poslovnim funkcijama.

Klasifikacije težine popravke

Težina	Opis
Teško	Otklanjanje može zahtevati obimnu rekonfiguraciju osnovnih sistema što je vremenski zahtevno. Otklanjanje može zahtevati prekid normalnog poslovanja.



Srednje	Otklanjanje može zahtevati manje rekonfiguracije ili dodatke koji mogu biti vremenski zahtevni ili skupi.
Lako	Popravka može biti izvršena u kratkom vremenskom roku, sa malo teškoća.

Rezultati testiranja

Broj	Ranjivost	Ocena rizika	Rizik	Strana
1	SQL Injection	10	Kritičan	11
2	Cross-site scripting	8	Visok	12
3	Outdated Software	6	Medium	69
4	Multiple XYZ Vulnerabilities	5	Medium	420

Rezultat skeniranja mreže

Tokom procene, izvršeno je skeniranje mreže korišćenjem alata nmap i nikto. Skeniranje je imalo za cilj identifikaciju otvorenih portova i servisa koji se izvršavaju na ciljnom sistemu. U terminalu, koristite sledeću komandu:

nmap -vvv -sV -sC -p- 127.0.0.1

Objašnjenje svake ocene:

- **-vvv** (verbosity level 3): Ova opcija nmap-a nalaže da odmah izlazne rezultate skeniranja, umesto da čeka da skeniranje bude završeno.
- **-sV** (service version detection): Detektuje verzije servisa koji se izvršavaju.
- **-sC** (default script scanning): Pokreće zadate skripte radi prikupljanja dodatnih informacija o servisima.
- **-p-** (all ports): Skenira sve portove

IP adresa 127.0.0.1 je lokalna petlja (loopback) adresa. Rezultat skeniranja je:

```
PORT      STATE SERVICE REASON  VERSION
3000/tcp open  ppp?    syn-ack
| fingerprint-strings:
|_ GetRequest:
|_   HTTP/1.1 200 OK
|_   Access-Control-Allow-Origin: *
|_   X-Content-Type-Options: nosniff
|_   X-Frame-Options: SAMEORIGIN
|_   Feature-Policy: payment 'self'
|_   X-Recruiting: /#/jobs
|_   Accept-Ranges: bytes
|_   Cache-Control: public, max-age=0
|_   Last-Modified: Sun, 07 Jul 2024 13:28:16 GMT
|_   ETag: W/"ea4-1908d618232"
|_   Content-Type: text/html; charset=UTF-8
|_   Content-Length: 3748
|_   Vary: Accept-Encoding
|_   Date: Sun, 07 Jul 2024 13:37:39 GMT
|_   Connection: close
|_   <!--
|_   Copyright (c) 2014-2024 Bjoern Kimminich & the OWASP Juice Shop contributors.
|_   SPDX-License-Identifier: MIT
|_   -><!DOCTYPE html><html lang="en"><head>
|_   <meta charset="utf-8">
|_   <title>OWASP Juice Shop</title>
|_   <meta name="description" content="Probably the most modern and sophisticated insecure web application">
|_   <meta name="viewport" content="width=device-width, initial-scale=1">
|_   <link id="favicon" rel="icon" type="image/x-icon" href="/asset
|_ HTTPOptions, RTSPRequest:
|_   HTTP/1.1 204 No Content
|_   Access-Control-Allow-Origin: *
|_   Access-Control-Allow-Methods: GET,HEAD,PUT,PATCH,POST,DELETE
|_   Vary: Access-Control-Request-Headers
|_   Content-Length: 0
|_   Date: Sun, 07 Jul 2024 13:37:39 GMT
|_   Connection: close
|_ Help, NCP:
|_   HTTP/1.1 400 Bad Request
|_   Connection: close
```

Gde je pronađen jedan otvoren port, 3000 (kako se očekuje), koji pokreće servis "ppp?", međutim, nmap nije mogao tačno da utvrdi o kom servisu se radi.

HTTP/1.1 200 OK: Ovo ukazuje da je server dostupan i vraća statusni kod 200, što znači da je zahtev uspešno obrađen.

Access-Control-Allow-Origin: * Prisustvo ovog zaglavlja ukazuje da CORS (Cross-Origin Resource Sharing) podešavanja dozvoljavaju sve sajtove, što nije dobra praksa i može biti rizično.

X-Content-Type-Options: nosniff and **X-Frame-Options: SAMEORIGIN:** Ovi zaglavlja pomažu u zaštiti protiv određenih vrsta napada kao što su prepoznavanje MIME tipova ili clickjacking.

Feature-Policy: payment 'self': Ova politika definiše dozvole za određene web funkcionalnosti, u ovom slučaju, za funkcionalnosti plaćanja.

Činjenica da je licenca MIT ukazuje da je kod otvorenog koda.

HTTP/1.1 400 Bad Request for **Help** and **NCP:** Ovi odgovori mogu ukazivati na neispravne ili pogrešne zahteve, što može sugerisati ranjivosti u obradi zahteva.

Takođe smo skenirali server koristeći **Nikto**, popularan alat za skeniranje bezbednosti veb servera, koristi se za otkrivanje različitih ranjivosti i bezbednosnih problema.

Nikto je identifikovao sledeće probleme:

- **CORS misconfiguration:** Našao je da je CORS dozvoljen za sve sajtove (origin-e) (*), što je sigurnosni rizik.
- **Unusual header x-recruiting:** Ovaj heder sadrži "/#/jobs" kao sadržaj.
- **/ftp/:** Vraća HTTP kod 200, što ukazuje na potencijalno pristupačni direktorijum koji bi trebalo ručno pregledati.
- **Potentially interesting files:** Nikto je pronašao mnogo potencijalno interesantnih fajlova kao što su .egg, .tar.bz2, .jks, .tgz, .war, .cer, .pem, .tar.lzma i drugi. Svaki od ovih fajlova može sadržati poverljive informacije ili sertifikate koji bi mogli biti od interesa za dalje istraživanje.

```
(kali@kali)-[~]
$ nikto -h http://192.168.76.128:3000
Nikto v2.5.0

+ Target IP:      192.168.76.128
+ Target Hostname: 192.168.76.128
+ Target Port:    3000
+ Start Time:     2024-07-07 14:47:26 (GMT2)

+ Server: No banner retrieved
+ /: Retrieved access-control-allow-origin header: *.
+ /: Uncommon header 'x-recruiting' found, with contents: /#/jobs.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /robots.txt: Entry '/ftp/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: contains 1 entry which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ .: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type.
  ker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /192.egg: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /archive.tar.bz2: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /192.168.76.128.jks: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /192.168.76.128.tar: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /database.egg: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /19216876128.alz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /192.168.76.tgz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /128.tar: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /192.168.76.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /backup.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /168.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /192.168.76.128.cer: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /19216876128.jks: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /192.168.76.128.egg: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /19216876128.tgz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /site.tar.bz2: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /dump.tar: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /dump.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /192.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /192_168_76_128.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /dump.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /76.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /backup.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /168.jks: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /dump.egg: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /76.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /192168.tgz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /168.cer: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
```

1 – SQL Injection

KRITIČNI RIZIK (10/10)	
Verovatnoća iskorišćavanja	Laka
Uticaj na biznis	Značajan
Težina popravke	Lako
CVE	CWE-89
CVSS	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

Opis

SQL injection (SQLi) je ranjivost bezbednosti veba koja omogućava napadaču da se meša u upite koje aplikacija pravi ka svojoj bazi podataka. Ova ranjivost obično omogućava napadaču da pregleda podatke do kojih normalno ne bi imao pristup. To može uključivati podatke koji pripadaju drugim korisnicima, ili bilo koje druge podatke do kojih aplikacija sama može da pristupi. U mnogim slučajevima, napadač može izmeniti ili obrisati ove podatke, što uzrokuje trajne promene u aplikaciji.

Bezbednosni uticaj

Nakon autentifikacije putem SQL injection napada, napadači mogu steći potpunu kontrolu nad korisničkim nalogima. Ovo može uključivati izmenu privilegija naloga, pristup osetljivim informacijama ili izvršavanje zlonamernih radnji u ime kompromitovanih korisnika. Scenariji preuzimanja naloga predstavljaju značajne rizike po privatnost korisnika i integritet sistema. Sigurnosni incidenti izazvani SQL injection mogu imati dugoročne posledice koje nadmašuju trenutne operativne poremećaje. Organizacije mogu pretrpeti finansijske gubitke usled napora za otklanjanje štete, pravnih obaveza, kazni od regulatornih tela i štete reputaciji među korisnicima, partnerima i zainteresovanim stranama.

Analiza

© 2010 Pearson Education, Inc. or its affiliate(s). All rights reserved.

- Koristite parametrizovane upite (pripremljene izjave) sa vezanim parametrima kako biste osigurali bezbednost od SQL injection napada.
- Validirajte i čistite ulazne podatke kako biste osigurali da ne sadrže zlonamerni SQL kod.
- Razmislite o korišćenju ORM (Object-Relational Mapping) framework-a koji automatski obrađuje parametrizaciju i čisti ulazne podatke.

- <https://owasp.org/www-project-top-ten/>

Napadi Cross-Site Scripting (XSS) su vrsta ubacivanja, pri čemu se zlonamerni skriptovi ubacuju u inače benigna i pouzdana veb mesta. XSS napadi se dešavaju kada napadač koristi veb aplikaciju da pošalje zlonamerni kod, obično u obliku skripta koji se izvršava na strani

pregledača, drugom korisniku. Nedostaci koji omogućavaju ove napade da uspeju su prilično rasprostranjeni i javljaju se svuda gde veb aplikacija koristi unos korisnika unutar izlaza koji generiše, bez validacije ili enkodiranja.

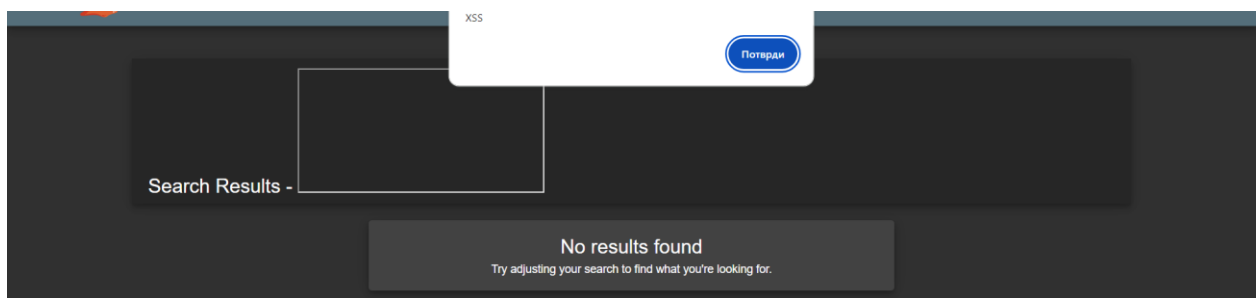
Bezbednosni uticaj

Napad Cross-Site Scripting (XSS) predstavlja značajne bezbednosne rizike za sistem omogućavanjem zlonamernim akterima da ubace skripte u web stranice koje drugi korisnici pregledaju. Ovo može dovesti do neovlašćenog pristupa osetljivim informacijama, preuzimanja sesija korisnika, defacementa veb sajtova i širenja zlonamernog softvera. XSS ranjivosti podrivaju integritet i pouzdanost veb aplikacija, što zahteva temeljnu validaciju unosa, enkodiranje izlaza i strogo pridržavanje sigurnosnih praksi kodiranja kako bi se efikasno umanjili ovi rizici.

Analiza

Za URL URL

[http://localhost:3000/#/search?q=<iframe%20src%3D%22javascript:alert\(%60XSS%60\)%22>](http://localhost:3000/#/search?q=<iframe%20src%3D%22javascript:alert(%60XSS%60)%22>) je moguć XSS napad.



Ako napadač pošalje zlonamerni link sa ubačenim JavaScript kodom i žrtva klikne na njega, napadač bi mogao da dobije pristupne podatke žrtve, za ovaj veb sajt.

Preporuke

- Implementirajte validaciju unosa kako na klijentskoj tako i na serverskoj strani kako biste filtrirali potencijalno zlonamerni unos.
- Pre rendera podataka na veb stranicama, pravilno enkodirajte izlazne podatke kako biste sprečili izvršavanje skriptova iz sadržaja koji je dostavio korisnik.

Reference

- <https://owasp.org/www-project-top-ten/>

3 - Privilege Escalation

KRITIČNI RIZIK (10/10)	
Verovatnoća iskorišćavanja	Moguće
Uticaj na biznis	Značajna
Težina popravke	Srednja
CVE	CVE-2021-44228, CVE-2021-44227, CVE-2021-44226
CVSS	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Opis

Privilege Escalation (eskalacija privilegija) je bezbednosni problem koji se javlja kada korisnik dobije viši nivo prava ili privilegija nego što je dozvoljeno njegovim permisijama. U OWASP Juice Shop-u, to znači da običan korisnik dobije administratorske privilegije i pristupa zaštićenim podacima istranicama.

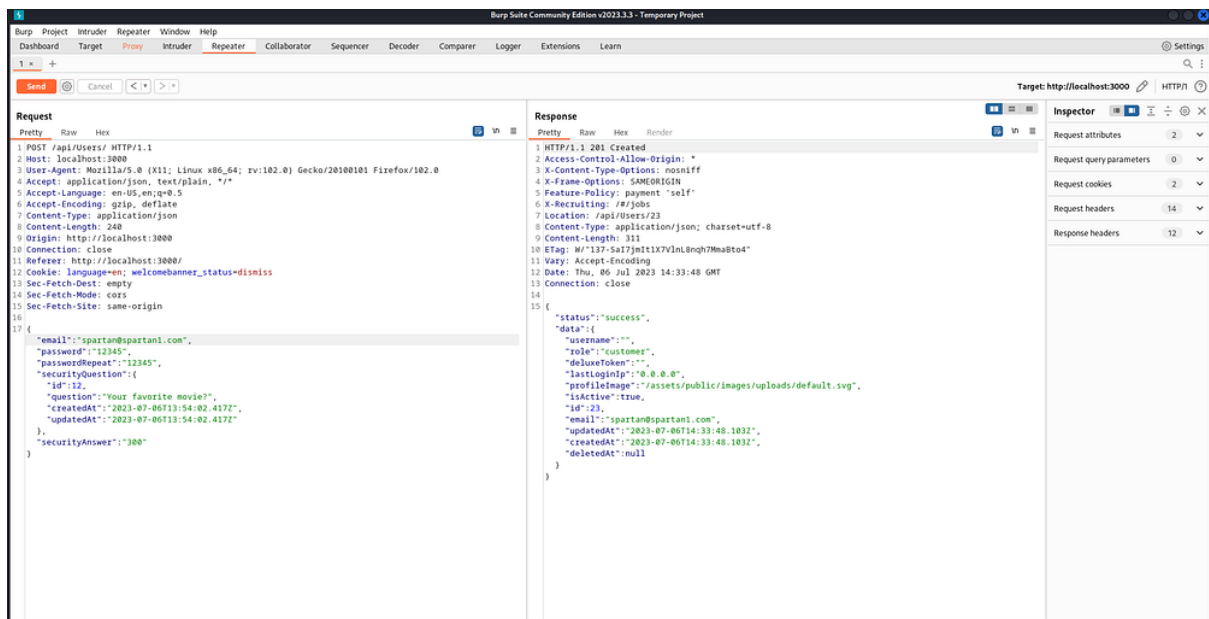
Bezbednosni uticaj

Eskalacija privilegija može imati ozbiljne posledice po bezbednost aplikacije. Napadač sa višim nivoom pristupa može odraditi:

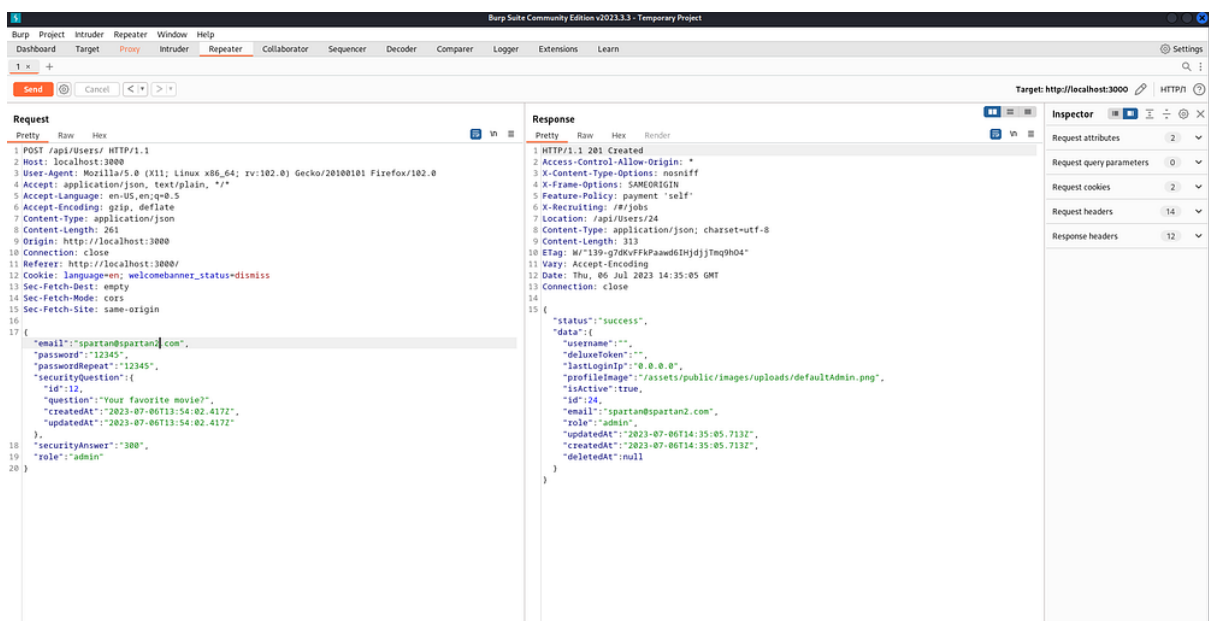
- Izmeniti ili obrisati podatke.
- Dodati ili ukloniti korisnike.
- Pristupiti osetljivim informacijama, kao što su finansijski podaci ili lični podaci korisnika.
- Oštetiti reputaciju organizacije

Analiza

Za početak je potrebno da kreiramo običan nalog, odnosno da imamo nalog sa osnovnim privilegijama sistema. Posle toga, potrebno je da korišćenjem BurpSuite programa, presretnemo zahtev za registraciju.



Vidmo da se parametri šalju u JSON formatu ka serveru. Primetićemo takođe da u odgovoru a postoji parametar pod nazivom “role” koji ima vrednost “customer”. Predpostavljamo da se ovaj parametar automatski prosleđuje web serveru. Pokušaćemo da prepisemo ovaj parametar i promenimo njegovu vrednost u “admin”? Kreiraćemo novog korisnika sa emailom “test2@mail.com” i ponovo poslati zahtev ka serveru dodajući “role”:”admin” na kraju JSON-a.



Nakon što smo ponovo prosledili zahtev sa našim novoubačenim parametrom, primetili smo da web server vraća uspešan odgovor i da je naš novokreirani korisnik sa administratorskim privilegijama! Sada se možemo vratiti na login stranicu I ulogovati se kao administrator.

Preporuke

- Pažljivo proverati i validirati sve ulazne podatke koje aplikacija prima. Ograničiti dozvoljene vrednosti za parametre kao što su "role".
- Osigurajte da svaki zahtev prolazi kroz rigoroznu proveru autorizacije. Korisnici bi trebalo da imaju pristup samo onim resursima i akcijama za koje imaju dozvolu.
- Dodelite korisnicima samo one privilegije koje su im neophodne za obavljanje njihovih zadataka. Izbegavajte korišćenje administratorskih naloga za svakodnevne zadatke.

4 - Sensitive Data Exposure

VISOKI RIZIK (8.5/10)	
Verovatnoća iskorišćavanja	Moguće
Uticaj na biznis	Značajna
Težina popravke	Srednja
CVE	CVE-2021-44228, CVE-2021-44227, CVE-2021-44226
CVSS	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Odavanje informacija, takođe poznato kao curenje informacija, dešava se kada veb sajt nenamerno otkrije osetljive informacije svojim korisnicima. U zavisnosti od konteksta, veb sajtovi mogu otkriti razne vrste informacija potencijalnom napadaču, uključujući:

- Podatke o drugim korisnicima, kao što su korisnička imena ili finansijske informacije
- Osetljive komercijalne ili poslovne podatke
- Tehničke detalje o veb sajtu i njegovoj infrastrukturi

Opasnosti od curenja osetljivih korisničkih ili poslovnih podataka su prilično očigledne, ali otkrivanje tehničkih informacija može biti podjednako ozbiljno. Iako će neke od tih informacija biti od ograničene upotrebe, one mogu potencijalno biti početna tačka za otkrivanje dodatne napadne površine, koja može sadržati druge interesantne ranjivosti. Znanje koje možete prikupiti čak može obezbediti nedostajući deo slagalice kada pokušavate da konstruisete složene napade visokog stepena ozbiljnosti.

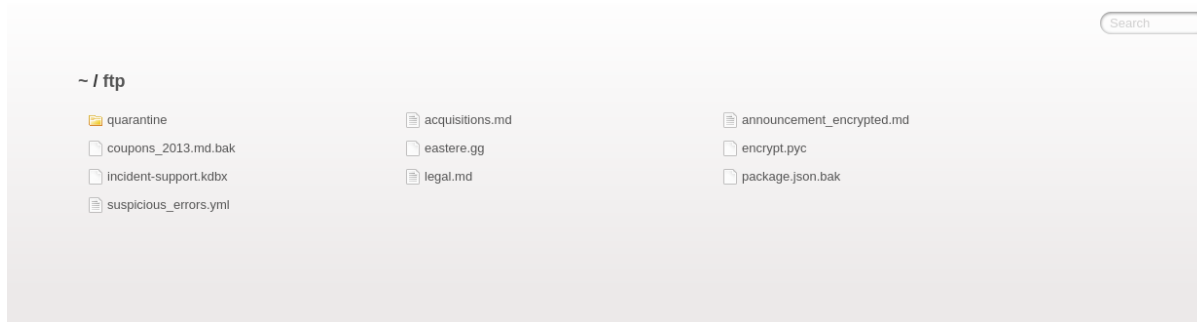
Bezbednosni uticaj

Nenamerno otkrivanje informacija na veb sajtovima može imati ozbiljne bezbednosne posledice. Takvi incidenti mogu dovesti do gubitka poverenja korisnika zbog mogućnosti krađe identiteta ili finansijske prevare. Takođe, otkrivanje tehničkih detalja o infrastrukturi sajta može olakšati napadačima da identifikuju i iskoriste ranjivosti, što može rezultirati

štetnim finansijskim posledicama za organizaciju. Dodatno, takvi incidenti mogu dovesti do regulatornih problema i sankcija, kao i ozbiljnih oštećenja reputacije organizacije, što može imati dugoročne negativne efekte na poslovanje.

Analiza

Dodavanjem ftp kao standardne domena za ftp server, mozemo videti da OWASP juice shop prikazuje ftp server sa internim podacima koje neautorizovani korisnik može preuzeti



Preporuke

Sprečavanje potpunog otkrivanja informacija je izazovno zbog velikog broja načina na koje se to može dogoditi. Ipak, postoje neki opšti najbolji postupci koje možete pratiti kako biste minimizirali rizik od ovakvih vrsta ranjivosti na vašim veb sajtovima.

Uverite se da su svi uključeni u izradu sajta potpuno svesni koje informacije se smatraju osetljivim. Ponekad se čini da bezopasne informacije mogu biti mnogo korisnije napadaču nego što ljudi shvataju. Isticanje ovih opasnosti može pomoći da se osigura da se osetljive informacije općenito rukovode bezbednije u vašoj organizaciji.

Proverite sav kod za potencijalno otkrivanje informacija kao deo vaših QA ili build procesa. Trebalo bi da bude relativno jednostavno automatizovati neke od povezanih zadataka, kao što je uklanjanje komentara programera.

Alati koji su korišćeni

Alat	Opis
BurpSuite Community Edition	Korišćeno za testiranje API-ja
Nikto	Korišćeno za skeniranje servisa i ranjivosti
Nmap	Korišćeno za skeniranje portova

Informacije o angažovanji

Informacije o klijentu

Klijent	OWASP Juice shop
Odgovorno lice	Pera Peric, CISO

Informacije o verziji dokumenta

Verzija	Datum	Opis
1.0	07.07.2024	Kreiranje izveštaja

Kontakt informacije

Naziv kompanije	Grupa G Consulting
Adresa	Radoja Domanovica 12
Broj telefona	555-185-1782
Email	somemail@groupg.com