Spis treści

O AUTORACH **11**

O REDAKTORZE TECHNICZNYM **11**

PODZIĘKOWANIA **13**

WSTĘP **15**

WPROWADZENIE **19**

1
WPROWADZENIE DO GRAPHQL **23**

Podstawy 23
Korzenie 24
Przykłady zastosowania 24
Specyfikacja 25
W jaki sposób jest prowadzona komunikacja? 25
Schemat 26
Zapytania 28
Analizator składni zapytania i funkcje resolverów 30
Jakie problemy rozwiązuje GraphQL? 31
API GraphQL kontra API REST 32
Przykład oparty na API REST 33
Przykład oparty na GraphQL 35
Inne różnice 38
Pierwsze zapytanie 41
Podsumowanie 44

2
PRZYGOTOWANIE LABORATORIUM DO PRACY Z GRAPHQL **45**

Środki bezpieczeństwa 46
Instalowanie dystrybucji Kali 47
Instalowanie klientów internetowych 49
Wykonywanie zapytań z poziomu powłoki 49
Wykonywanie zapytań za pomocą narzędzia graficznego 50

Przygotowanie serwera GraphQL, w którym istnieją luki w zabezpieczeniach ... 53
Instalowanie Dockera ... 53
Wdrożenie aplikacji Damn Vulnerable GraphQL Application ... 53
Testowanie DVGA ... 56
Instalowanie narzędzi przeznaczonych do hakowania GraphQL ... 56
Burp Suite ... 57
Clairvoyance ... 58
InQL ... 60
GraphwOOf ... 61
BatchQL ... 62
Nmap ... 62
Commix ... 63
graphql-path-enum ... 64
EyeWitness ... 65
GraphQL Cop ... 65
CrackQL ... 66
Podsumowanie ... 66

3
PŁASZCZYZNA ATAKU NA GRAPHQL ... 68
Czym jest płaszczyzna ataku? ... 68
Język ... 69
Zapytanie, mutacja i subskrypcja ... 70
Nazwa operacji ... 73
Pole ... 75
Argument ... 76
Alias ... 78
Fragment ... 80
Zmienna ... 81
Dyrektywa ... 82
Typy danych ... 85
Obiekt ... 85
Skalar ... 86
Wyliczenie ... 87
Unia ... 88
Interfejs ... 90
Dane wejściowe ... 91
Introspekcja ... 92
Weryfikacja i wykonywanie zapytania ... 95
Najczęściej spotykane słabe strony ... 96
Reguła specyfikacji i słaba strona implementacji ... 97
Odmowa usług ... 98

Ujawnienie informacji ... 98
Błędy w mechanizmach uwierzytelnienia i autoryzacji ... 99
Wstrzykiwanie kodu ... 99
Podsumowanie ... 99

4
REKONESANS ... 101
Wykrywanie GraphQL ... 102
Najczęściej stosowane punkty końcowe ... 103
Najczęściej udzielane odpowiedzi na zapytania ... 104
Skanowanie za pomocą narzędzia Nmap ... 107
Pole __typename ... 108
Graphw00f ... 111
Wykrywanie narzędzi GraphiQL Explorer i GraphQL Playground ... 112
Używanie EyeWitness do skanowania pod kątem interfejsów graficznych ... 113
Próba wykonania zapytania za pomocą klienta graficznego ... 116
Sprawdzanie GraphQL za pomocą introspekcji ... 119
Wizualizacja introspekcji za pomocą GraphQL Voyager ... 124
Generowanie za pomocą SpectaQL dokumentacji introspekcji ... 126
Wyszukiwanie informacji w przypadku, gdy introspekcja jest wyłączona ... 126
Sprawdzanie implementacji GraphQL ... 127
Wykrywanie serwera za pomocą Graphw00f ... 130
Analiza wyników ... 131
Podsumowanie ... 133

5
ATAK TYPU DOS ... 134
Kierunki ataków typu DoS w GraphQL ... 134
Zapytania cykliczne ... 136
Relacje cykliczne w schemacie GraphQL ... 136
Jak wykrywać relacje cykliczne? ... 138
Luki w zabezpieczeniach związane z zapytaniami cyklicznymi ... 143
Luki w zabezpieczeniach związane z introspekcją cykliczną ... 144
Luki w zabezpieczeniach związane z fragmentami cyklicznymi ... 146
Powielanie pola ... 147
Sposób działania luki związanej z powielaniem pola ... 147
Testowanie pod kątem luk w zabezpieczeniach związanych z powielaniem pola ... 149
Przeciążenie aliasu ... 151
Nadużywanie aliasów na potrzeby ataków typu DoS ... 152
Łączenie aliasów i zapytań cyklicznych ... 153

Przeciążanie dyrektywy ... 154
Nadużywanie dyrektyw w atakach typu DoS ... 155
Testowanie pod kątem luk w zabezpieczeniach związanych z przeciążaniem dyrektywy ... 155
Przeciążanie limitu obiektu ... 156
Grupowanie zapytań za pomocą tablicy ... 158
Zrozumienie sposobu działania grupowania zapytań za pomocą tablicy ... 158
Testowanie pod kątem luk w zabezpieczeniach związanych z grupowaniem zapytań za pomocą tablicy ... 159
Łączenie zapytań cyklicznych i grupowania zapytań za pomocą tablicy ... 160
Używanie BatchQL do wykrycia dostępności grupowania zapytań za pomocą tablicy ... 162
Przeprowadzanie za pomocą narzędzia GraphQL Cop audytu podatności na ataki typu DoS ... 163
Zabezpieczenia GraphQL przed atakami typu DoS ... 164
Analiza kosztu zapytania ... 164
Ograniczenia głębokości zapytania ... 168
Ograniczenia oparte na aliasach i tablicach ... 169
Ograniczenia związane z powielaniem pól ... 169
Ograniczanie liczby zwracanych rekordów ... 170
Lista zapytań dozwolonych ... 171
Automatycznie trwale przechowywane zapytania ... 171
Przekroczenie czasu oczekiwania ... 173
Zapora sieciowa aplikacji internetowej ... 173
Brama działająca jako proxy ... 174
Podsumowanie ... 175

6
UJAWNIANIE INFORMACJI ... 176
Identyfikowanie sposobów ujawniania informacji w GraphQL ... 177
Zautomatyzowane wyodrębnianie schematu za pomocą narzędzia InQL ... 178
Jak sobie radzić z wyłączoną introspekcją ... 179
Wykrywanie wyłączonej introspekcji ... 180
Wykorzystanie środowiska innego niż produkcyjne ... 180
Wykorzystanie pola meta __type ... 181
Używanie funkcjonalności sugerowania nazwy pola ... 183
Poznajemy algorytm Edit-Distance ... 184
Optymalizacja używania funkcjonalności sugerowania nazwy pola ... 185
Uwzględnienie kwestii bezpieczeństwa ... 186
Wstawianie listy nazw pól ... 187
Wstawianie listy nazw typów w polu meta __type ... 189
Automatyzacja za pomocą narzędzia Clairvoyance funkcji sugerowania nazwy pola i wstawiania listy nazw ... 191

Nadużywanie komunikatów o błędzie ... 194
Analiza szczegółowego komunikatu o błędzie ... 195
Włączenie debugowania ... 197
Wyodrębnianie informacji ze stosu wywołań ... 198
Ujawnianie informacji za pomocą metody GET ... 200
Podsumowanie ... 200

7
OMINIĘCIE UWIERZYTELNIENIA I AUTORYZACJI ... 202
Stan uwierzytelnienia i autoryzacji w GraphQL ... 203
Modele wdrożenia in-band i out-of-band ... 203
Najczęściej stosowane podejścia ... 205
Testowanie uwierzytelnienia ... 212
Wykrywanie warstwy uwierzytelnienia ... 212
Ataki typu brute force przeprowadzane na hasła z użyciem funkcjonalności wstawiania listy nazw ... 214
Atak typu brute force na hasło z użyciem narzędzia CrackQL ... 216
Używanie listy nazw dozwolonych operacji ... 218
Podrabianie i wyciekanie danych uwierzytelniających JWT ... 219
Testowanie autoryzacji ... 222
Wykrywanie warstwy autoryzacji ... 222
Sprawdzanie ścieżek za pomocą graphql-path-enum ... 223
Przeprowadzanie za pomocą narzędzia CrackQL ataków typu brute force na argumenty i pola ... 224
Podsumowanie ... 226

8
WSTRZYKIWANIE KODU ... 228
Związane ze wstrzykiwaniem kodu luki w zabezpieczeniach GraphQL ... 229
Pole rażenia danych wejściowych o złośliwym działaniu ... 230
OWASP Top 10 ... 231
Płaszczyzna ataku polegającego na wstrzykiwaniu kodu ... 232
Argumenty zapytania ... 233
Argumenty pola ... 235
Argumenty dyrektywy zapytania ... 235
Nazwy operacji ... 236
Punkty dostarczania danych wejściowych ... 237
Wstrzykiwanie kodu SQL ... 238
Poznajemy typy ataków związanych z SQLi ... 239
Testowanie pod kątem luki SQLi ... 240
Testowanie aplikacji DVGA pod kątem luki związanej z SQLi z użyciem oprogramowania Burp Suite ... 240
Automatyzacja ataku polegającego na wstrzykiwaniu kodu SQL ... 247

Wstrzykiwanie polecenia systemu operacyjnego ... 249
Przykład ... 250
Ręczne testowanie aplikacji DVGA ... 251
Zautomatyzowane testowanie z użyciem frameworka Commix ... 253
Analiza kodu funkcji resolvera ... 255
Cross-Site Scripting ... 256
Luka XSS typu odbijana ... 256
Luka XSS typu przechowywana ... 258
Luka XSS oparta na modelu DOM ... 259
Testowanie aplikacji DVGA pod kątem luk XSS ... 260
Podsumowanie ... 265

9
FAŁSZOWANIE I PRZECHWYTYWANIE ŻĄDAŃ ... 266
Atak typu CSRF ... 267
Wyszukiwanie działań, które mogą prowadzić do zmiany stanu ... 269
Sprawdzanie pod kątem luk w zabezpieczeniach związanych z metodami POST ... 270
Automatyczne wysyłanie formularza w trakcie ataku typu CSRF ... 273
Sprawdzanie pod kątem luk w zabezpieczeniach związanych z metodami GET ... 274
Atak polegający na wstrzykiwaniu kodu HTML ... 277
Testowanie automatyczne za pomocą narzędzi BatchQL i GraphQL Cop ... 278
Unikanie ataków typu CSRF ... 279
Atak typu SSRF ... 281
Poznajemy typy ataków SSRF ... 282
Wyszukiwanie podatnych na ataki operacji, pól i argumentów ... 283
Testowanie pod kątem luki SSRF ... 284
Zapobieganie atakom typu SSRF ... 287
Przechwytywanie WebSocket ... 288
Wyszukiwanie operacji subskrypcji ... 289
Przechwytywanie zapytania subskrypcji ... 289
Ochrona przed atakami typu CSWSH ... 293
Podsumowanie ... 293

10
EXPLOITY I UJAWNIONE LUKI W ZABEZPIECZENIACH ... 294
Odmowa usług ... 295
Ogromne dane używane podczas ataku ... 295
Wyrażenia regularne (CS Money) ... 297
Zapytanie cykliczne introspekcji (GitLab) ... 299
Aliasy dla powielania pola (Magento) ... 300
Grupowanie zapytań za pomocą tablicy na potrzeby powielania pola (WPGraphQL) ... 301
Fragmenty cykliczne (Agoo) ... 303

Nieprawidłowa autoryzacja ... 304
Umożliwienie dostępu do danych dezaktywowanym użytkownikom (GitLab) ... 304
Pozwolenie nieuprzywilejowanemu pracownikowi firmy na modyfikowanie adresu e-mail użytkownika (Shopify) ... 305
Ujawnienie liczby dozwolonych hakerów za pomocą obiektuteam (HackerOne) ... 306
Odczytywanie notatek prywatnych (GitLab) ... 307
Ujawnienie informacji na temat transakcji płatności (HackerOne) ... 308
Ujawnienie informacji ... 309
Lista użytkowników GraphQL (GitLab) ... 309
Uzyskanie dostępu do zapytania introspekcji za pomocą WebSocket (Nuri) ... 310
Wstrzykiwanie kodu ... 311
Wstrzykiwanie kodu SQL za pomocą parametru zapytania GET (HackerOne) ... 311
Wstrzykiwanie kodu SQL w argumencie Object (Apache SkyWalking) ... 313
Cross-Site Scripting (GraphQL Playground) ... 314
Cross-Site Request Forgery (GitLab) ... 316
Podsumowanie ... 317

A
LISTA RZECZY DO SPRAWDZENIA PODCZAS TESTOWANIA GRAPHQL ... 319
Rekonesans ... 319
Odmowa usług ... 320
Ujawnianie informacji ... 320
Uwierzytelnienie i autoryzacja ... 321
Wstrzykiwanie kodu ... 321
Fałszowanie żądań ... 322
Przechwytywanie żądań ... 322

B
ZASOBY DOTYCZĄCE BEZPIECZEŃSTWA GRAPHQL ... 323
Wskazówki i podpowiedzi dotyczące testów penetracyjnych ... 323
Laboratoria hakerskie do samodzielnego wypróbowania ... 324
Klipy wideo związane z zapewnieniem bezpieczeństwa ... 324