HACKTHEBOX

ATTACKING GRAPHQL
CHEAT SHEET

Basic Example

GraphQL Request

```
{
  users {
    id
    username
    role
  }
}
```

GraphQL Response

```
{
  "data": {
    "users": [
      {
        "id": 1,
        "username": "htb-stdnt",
        "role": "user"
      },
      {
        "id": 2,
        "username": "admin",
        "role": "admin"
      }
    ]
  }
}
```

Introspection Queries

GraphQL Types

```
{
  __schema {
    types {
      name
    }
  }
}
```

GraphQL Queries

```
{
  __schema {
    queryType {
      fields {
        name
        description
      }
    }
  }
}
```

General Introspection

```
query IntrospectionQuery {
      __schema {
        queryType { name }
        mutationType { name }
        subscriptionType { name }
        types {
          ...FullType
        }
        directives {
          name
          description

          locations
          args {
            ...InputValue
          }
        }
      }
    }

    fragment FullType on __Type {
      kind
      name
      description

      fields(includeDeprecated: true) {
        name
        description
        args {
          ...InputValue
        }
        type {
          ...TypeRef
        }
        isDeprecated
        deprecationReason
      }
      inputFields {
        ...InputValue
      }
      interfaces {
        ...TypeRef
      }
      enumValues(includeDeprecated: true) {
        name
        description
        isDeprecated
        deprecationReason
      }
      possibleTypes {
        ...TypeRef
      }
    }

    fragment InputValue on __InputValue {
      name
      description
      type { ...TypeRef }
      defaultValue
    }

    fragment TypeRef on __Type {
      kind
      name
      ofType {
        kind
        name
        ofType {
          kind
          name
          ofType {
            kind
            name
            ofType {
              kind
              name
              ofType {
                kind
                name
                ofType {
                  kind
                  name
                  ofType {
                    kind
                    name
                  }
                }
              }
            }
          }
        }
      }
    }
```

Batching Example

```
POST /graphql HTTP/1.1
Host: 172.17.0.2
Content-Length: 86
Content-Type: application/json

[
        {
                "query":"{user(username: \"admin\") {uuid}}"
        },
        {
                "query":"{post(id: 1) {title}}"
        }
]
```

Mutation Example

```
mutation {
  registerUser(input: {username: "vautia", password: "5f4dcc3b5aa765d61d8327deb882cf99", role: "user", msg: "newUser"}) {
    user {
      username
      password
      msg
      role
    }
  }
}
```

Tools

- graphw00f
- graphql-voyager
- GraphQL-Cop
- InQL