



API Bug Hunting Methodology

Become a Successful
Bug Bounty Hunter



API – What is it?

- Application Programming Interface
- An API, or application programming interface, is a set of protocols, routines, and tools for building software applications that specify how different software components should interact with each other.



API – Types

- SOAP / XML API
- RESTful API (JSON)
- GraphQL API



API - General

- Typical API paths:
- `/api/getuser`
- `/api/getshippingaddress`



API – How to find them?

- Find API endpoints
- API Documentation
- Javascript files!
- Fuzzing / Scanning
- Test every feature on the web app
- search for /api/
- site: example.com inurl:api
- /api/
- api.example.com



API – Older versions

You will often see a version number on API queries, such as [/api/v2.0/execute](#) or even as a parameter, [/api/getuser?v=2.0](#).

Try OLDER versions to see what's changed in older versions!

[/api/v1.0/](#)

[/api/getuser?v=1.0](#)



API – IDORs

- IDORs
- Very common in APIs
- Look for ID, GUID, GUID etc.
- Mobile Apps
- Web Apps
- Mobile and Web App code often different! Different Vulnerabilities!



API – CORS

- Misconfigured CORS
- Provide **Origin: yourdomain.com** in the request
- Look for **Access-Control-Allow-Origin:yourdomain.com** in the response.



API – SQLi

- SQL Injection
- See SQLi lesson
- Same issues found in APIs
- Sample payload: `sleep(10)`



API – Broken Access Control

Broken Access Control

POST /api/updateuser

```
{"bio":"example"}
```

replace JSON with

```
{"bio":"example","role":"admin"}
```



API – Admin endpoints

- Admin API endpoints accessible by non-Admin
- `/api/adminedit`
- Test with low privileges



Thank You!

Become a Successful
Bug Bounty Hunter