Automated Enumeration & Information Disclosure Notes

Extracted from Write-up

Read the write-up here: The Lazy Hacker's Guide to $500 Information Disclosure Bugs.

Important Explanations

Enumeration Strategy

- **Multi-stage approach**: Start broad with ffuf, then target specific technologies
- **403 responses are valuable**: Indicate existing but blocked resources (bypass potential)
- **Custom wordlists**: Essential for different targets (PHP, APIs, Cloud)
- **Git reconstruction**: Even with 403 on /.git/, tools can fetch key files to rebuild repository
- **Header analysis reveals**: Vulnerable versions, debug modes, technology stack
- **Context determines severity**: Same finding has different impact based on environment

Targeted Assault with Custom Wordlists

- **PHP Applications**:
  - Backup extensions: .php.bak, .php.old, .php
  - Common backup patterns for PHP apps
- **API Endpoints**:
  - Paths: /v1/config, /internal/, /swagger.json
  - API-specific configuration and documentation files
- **Cloud Targets**:
  - S3 buckets: prod-target-assets, target-backup-2023
  - Azure containers: Target name-based wordlists
  - Cloud storage brute-forcing techniques

Key Findings

- **Backup file patterns**: .php.bak, .php.old, .php for PHP apps
- **Cloud enumeration**: S3 buckets (assets-target.s3.amazonaws.com)
- **Header indicators**:
  - Apache/2.4.49 → Path traversal (CVE-2021-41773)
  - PHP/5.6.40 → Outdated, unsupported version
  - X-Debug-Token → Symfony debug toolbar active
  - X-AspNetMvc-Version: 4.0 → Older ASP.NET apps
- **Critical paths**: /trace.axd, /_profiler/, common config files

Commands

Wordlist Preparation

```
# Merge directory and file wordlists
cat ~/SecLists/Discovery/Web-Content/raft-medium-directories.txt
 ~/SecLists/Discovery/Web-Content/raft-medium-files.txt > combined_raft.txt
```

Web Fuzzing

```
# Fast web fuzzing with auto-calibration
ffuf -w combined_raft.txt -u https://target.com/FUZZ
-t 100 -mc 200,301,302,403 -ac -c -o ffuf_initial.json
```

Git Reconstruction

```
# Reconstructs git repository from exposed .git
git-dumper https://target.com/.git/ /path/to/output/dir
```

Reconnaissance

```
# Fetch only HTTP headers for quick reconnaissance
curl -I https://target.com
```