

# URL Fuzzer Discovery Report

Target: https://example.com | Demo data

## 1. Discovery Summary

| Metric         | Value |
|----------------|-------|
| Paths tested   | 4,200 |
| Hits           | 37    |
| Hit rate       | 0.9%  |
| Status 200     | 22    |
| Status 301/302 | 9     |
| Status 403     | 6     |

## 2. Risk-Rated Paths

| Path         | Status | Risk     |
|--------------|--------|----------|
| /.env        | 200    | Critical |
| /.git/config | 200    | Critical |
| /admin       | 302    | High     |
| /backup.zip  | 200    | High     |
| /phpinfo.php | 200    | Medium   |
| /uploads/    | 403    | Low      |
| /robots.txt  | 200    | Low      |

## 3. HTTP Evidence

GET /.env HTTP/1.1  
Host: example.com  
User-Agent: Pentestscanner/1.0  
Accept: \*/\*

HTTP/1.1 200 OK  
Content-Type: text/plain  
Content-Length: 512

APP\_KEY=[redacted]  
DB\_PASSWORD=[redacted]

## 4. Remediation Guidance

| Finding                 | Recommendation                                                         |
|-------------------------|------------------------------------------------------------------------|
| /.env publicly readable | Block access to dotfiles at the web server and rotate exposed secrets. |
| /.git/config exposed    | Remove the .git directory from the web root and deny access.           |
| Backup file exposed     | Delete backup archives from public paths.                              |
| /admin reachable        | Restrict to trusted IPs or place behind VPN and MFA.                   |

This is a demo report generated with sample data for illustration purposes only.