HACKTHEBOX

ABUSING HTTP MISCONFIGURATIONS CHEAT SHEET

Web Cache Poisoning - General

- Identify a way to determine keyed & unkeyed parameters
- Use Cache Buster to prevent poisoning other users
- Deliver payload in unkeyed parameter to poison the cache

Web Cache Poisoning - Fat GET

- GET requests with body
- Web server may be vulnerable if it does not ignore the body
- Can be used to poison the cache even with a keyed parameter
- Example:

```
GET /index.php?param1=Hello&param2=World HTTP/1.1
Host: 127.0.0.1
Content-Length: 10

param3=123
```

Web Cache Poisoning - Parameter Cloaking

- Discrepancy in the parsing of parameters between web cache and web server
- Can be used to poison the cache even with a keyed parameter
- Payload needs to be hidden in unkeyed parameter
- Example:

```
GET /?language=en&a=b;language=de HTTP/1.1
Host: 127.0.0.1
```

Web Cache Poisoning Scanner

Command	Description
`./wcvs -u http://simple.wcp.htb/`	Simple scan of a website
`./wcvs -u http://simple.wcp.htb/ -gr`	Generate a JSON report

Host Header Attacks

Override Headers:

- X-Forwarded-Host
- X-HTTP-Host-Override
- Forwarded
- X-Host
- X-Forwarded-Server

Generating a wordlist for Fuzzing:

```
for a in {1..255};do
    for b in {1..255};do
        echo "192.168.$a.$b" >> ips.txt
    done
done
```

Using ffuf to fuzz the host header:

```
ffuf -u http://IP:PORT/admin.php -w ips.txt -H 'Host: FUZZ'
```

Bypassing blacklist filters for `localhost`:

- Decimal encoding: `2130706433`
- Hex encoding: `0x7f000001`
- Octal encoding: `0177.0000.0000.0001`
- Zero: `0`
- Short form: `127.1`
- IPv6: `::1`
- External domain that resolves to localhost: `localtest.me`

Session Puzzling

- Session IDs should be at least 16 bytes long
- Session IDs should provide at least 64 bits of entropy
- Test for insecure default values in session variables
- Test for common session variables/session variable re-use across different processes
- Test for premature session population of session variables by canceling/manipulating processes unexpectedly