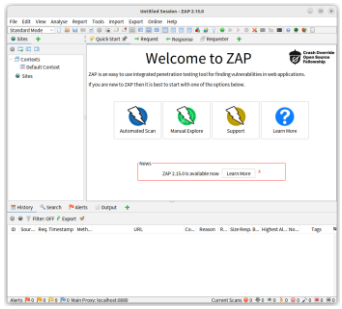
ZAP のリクエストを眺めてみる

@ WEB CREATORS LT

Zed Attack Proxy (ZAP)



- Zed Attack Proxy (ZAP) is a free, open-source penetration testing tool being maintained under the umbrella of The Software Security Project (SSP).
  - https://www.zaproxy.org/getting-started/
- OSS の脆弱性検査ツール

- OWASP ZAP と呼ばれていたもの
- プロジェクト自体が SSP に移った関係で、 ZAP と呼ばれるように
  - https://www.zaproxy.org/blog/2023-08-01-zap-is-joining-the-software-security-project/

実験環境

概略

Attack

/usr/local/apache2/htdocs/index.html

```
<!doctype html>
<html lang="en">
<head>
    <meta charset="utf-8">
    <title>index.html</title>
</head>
<body>

<h1>index.html</h1>

<h2>get</h2>
<form action="/" method="get">
    <input name="q" type="text"/>
    <input type="submit"/>
</form>

<h2>post</h2>
<form action="/" method="post">
    <input name="_csrf" type="hidden" value="df4d4fb2-5fae-49b6-8b51-537925faa7d3">
    <input name="q" type="text"/>
    <input type="submit"/>
</form>

</body>
</html>
```


リクエスト例 (1)

GET http://127.0.0.1:8081/?q=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fetc%2Fpasswd HTTP/1.1

host: 127.0.0.1:8081

user-agent: Mozilla/5.0 (Windows NT 10.0; rv:125.0) Gecko/20100101 Firefox/125.0

pragma: no-cache

cache-control: no-cache

referer: http://127.0.0.1:8081/

Path Traversal

- https://owasp.org/www-community/attacks/Path_Traversal
  - web root directory の外のファイルを取得しようとする攻撃
  - URL の path に ../ を含めるだけではなく、
    query などに path を指定して機微情報の取得を試みることも

- ZAP のリクエスト例
  - q=../../../../../../../../../../../../../../etc/passwd
  - Scan Rule ID: 6 (https://www.zaproxy.org/docs/alerts/6/)

リクエスト例 (2)

GET
http://127.0.0.1:8081/?q=ZAP%22+and+0+in+%28select+sleep%2815%29+%29+and+%22%22%3D%22 HTTP/1.1

host: 127.0.0.1:8081

user-agent: Mozilla/5.0 (Windows NT 10.0; rv:125.0) Gecko/20100101 Firefox/125.0

pragma: no-cache

cache-control: no-cache

referer: http://127.0.0.1:8081/

SQL Injection – MySQL

- https://owasp.org/www-community/attacks/SQL_Injection
  - 主に、以下に影響
  - Confidentiality
  - Authentication
  - Authorization
  - Integrity

- ZAP のリクエスト例
  - q=ZAP' and 0 in (select sleep(15)) and ''='
  - Alert ID: 40019 (https://www.zaproxy.org/docs/alerts/40019/)

リクエスト例 (3)

HTTP Header

POST http://127.0.0.1:8081/ HTTP/1.1

host: 127.0.0.1:8081

user-agent: Mozilla/5.0 (Windows NT 10.0; rv:125.0) Gecko/20100101 Firefox/125.0

pragma: no-cache

cache-control: no-cache

content-type: application/x-www-form-urlencoded

referer: http://127.0.0.1:8081/

content-length: 113

HTTP Body

_csrf=df4d4fb2-5fae-49b6-8b51-537925faa7d3&q=any%0D%0ASet-cookie%3A+Tamper%3Dfa2665b9-324c-4d5f-bab3-a03d07d741b0

CRLF Injection

- https://owasp.org/www-community/vulnerabilities/CRLF_Injection
  - HTTP ヘッダーの値に CRLF を差し込み、任意のフィールドを設定しようとする攻撃

- ZAP のリクエスト例
  - q=any[CR][LF]Set-cookie: Tamper=fa2665b9-324c-4d5f-bab3-a03d07d741b0
  - Alert ID: 40003 (https://www.zaproxy.org/docs/alerts/40003/)

まとめ

- ZAP は OSS の脆弱性検査ツール
  - Zed Attack Proxy (ZAP) is a free, open-source penetration testing tool being maintained under the umbrella of The Software Security Project (SSP).
    - https://www.zaproxy.org/getting-started/

- ZAP が発行するリクエストを眺めてみる
  - Path Traversal
  - SQL Injection
  - CRLF Injection