Playing Web Fuzzer

Wagner Elias

Blog: http://wagnerelias.com
Twitter: welias

Parabéns!

Comparecer a uma palestra as 8:00 da manhã de um Domingo chuvoso não é para os fracos!

Agenda

- O que é Fuzzing
- OWASP Fuzzing Code Database
- Aplicando Fuzzing em testes de aplicações Web
- Conclusão

O que é Fuzzing

Teste Fuzzing ou Fuzzing é a técnica que possibilita identificar falhas injetando dados

OWASP Fuzzing Code Database

Projeto que tem como objetivo catalogar listas de definições para serem usadas em testes fuzzing

http://www.owasp.org/index.php/Category:OWASP_Fuzzing_Code_Database

Aplicando Fuzzing em testes de aplicações Web

- Onde injetar dados
- Analisando Resultados
- Vulnerabilidades que podem ser identificadas
- Exemplos

Onde Injetar Dados

GET /FUZZ/FUZZ/parâmetro=FUZZ FUZZ

User-Agent: FUZZ

Cookie: FUZZ

Onde Injetar Dados

POST /FUZZ/FUZZ/ FUZZ

User-Agent: FUZZ

Cookie: FUZZ

parâmetro=FUZZ

Onde Injetar Dados

POST /FUZZ/FUZZ/ FUZZ

User-Agent: FUZZ

Cookie: FUZZ

```
<?xml version="1.0" encoding="UTF-8" ?>
<methodCall>
        <methodName>wp.getPages</methodName>
                <params>
                        <param>
                                <value>
                                        <string>FUZZ</string>
                                </value>
                        </param>
                </params>
</methodCall>
```

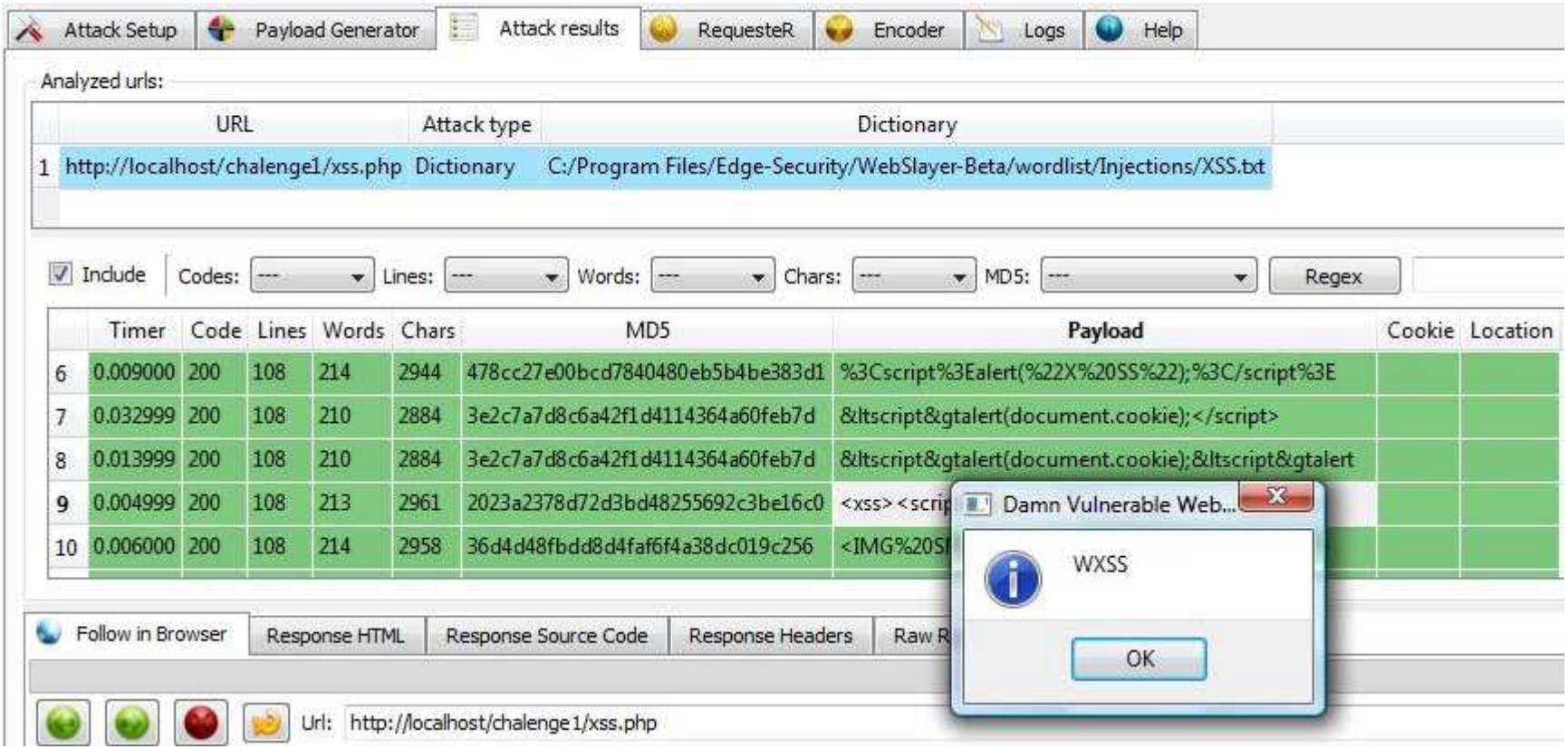
Analisando Resultados

- Analisar resposta HTTP (200; 302; 401; 403; 500)
- Usar expressão regular para pesquisar informações na resposta HTTP
- Comparar resultados usando hashs

Quais falhas podem ser encontradas

OWASP Top 10 – 2007 (Previous)	OWASP Top 10 – 2010 (New)
A2 – Injection Flaws	A1 – Injection
A1 – Cross Site Scripting (XSS)	A2 – Cross Site Scripting (XSS)
A7 – Broken Authentication and Session Management	A3 – Broken Authentication and Session Management
A4 – Insecure Direct Object Reference	A4 – Insecure Direct Object References
A5 – Cross Site Request Forgery (CSRF)	A5 – Cross Site Request Forgery (CSRF)
<was T10 2004 A10 – Insecure Configuration Management>	A6 – Security Misconfiguration (NEW)
A10 – Failure to Restrict URL Access	A7 – Failure to Restrict URL Access
<not in T10 2007>	A8 – Unvalidated Redirects and Forwards (NEW)
A8 – Insecure Cryptographic Storage	A9 – Insecure Cryptographic Storage
A9 – Insecure Communications	A10 – Insufficient Transport Layer Protection
A3 – Malicious File Execution	<dropped from T10 2010>
A6 – Information Leakage and Improper Error Handling	<dropped from T10 2010>

DEMO - WebSlayer



Conclusão

- Fuzzing é uma técnica muito eficaz para identificar falhas
- Para bons resultados é essencial ter boas listas e identificar as interfaces de entrada
- Use todos os recursos para analisar as respostas (Regex; Hashs)

Perguntas

Wagner Elias

blog: http://wagnerelias.com
Twitter: http://www.twitter.com/welias