



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>
```

Analizando Resultados

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

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

Analyzed urls:

URL	Attack type	Dictionary
1 http://localhost/challenge1/xss.php	Dictionary	C:/Program Files/Edge-Security/WebSlayer-Beta/wordlist/Injections/XSS.txt

Include |
 Codes: --- |
 Lines: --- |
 Words: --- |
 Chars: --- |
 MD5: --- |
 Regex

	Timer	Code	Lines	Words	Chars	MD5	Payload	Cookie	Location
6	0.009000	200	108	214	2944	478cc27e00bcd7840480eb5b4be383d1	%3Cscript%3Ealert(%22X%20SS%22);%3C/script%3E		
7	0.032999	200	108	210	2884	3e2c7a7d8c6a42f1d4114364a60feb7d	<script>alert(document.cookie);</script>		
8	0.013999	200	108	210	2884	3e2c7a7d8c6a42f1d4114364a60feb7d	<script>alert(document.cookie);<script>		
9	0.004999	200	108	213	2961	2023a2378d72d3bd48255692c3be16c0	<xss><script>		
10	0.006000	200	108	214	2958	36d4d48fbd8d4faf6f4a38dc019c256	<IMG%20S		

Follow in Browser |
 Response HTML |
 Response Source Code |
 Response Headers |
 Raw R

Url: http://localhost/challenge1/xss.php

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>