Automatizovaná detekce zranitelností webových aplikací

František Koláček

Vedoucí práce: RNDr. Marek Rychlý , Ph.D.
Konzultace: Ján Rusnačko (Red Hat Czech, s. r. o.)

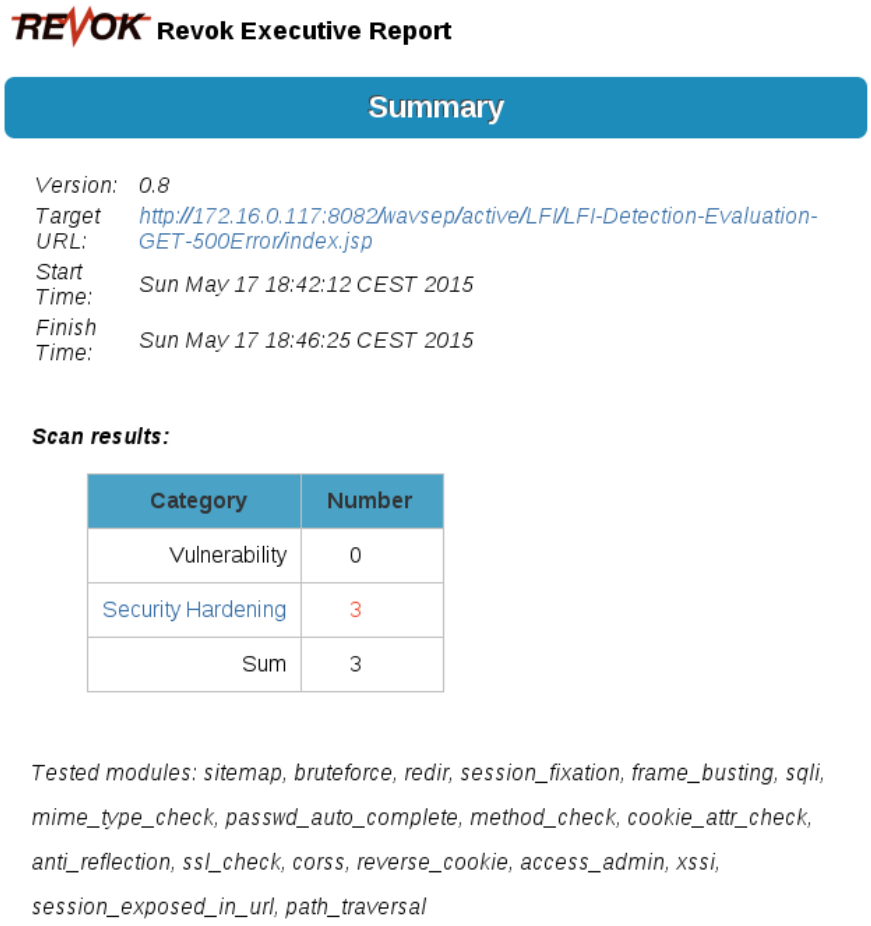
BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY

Cíle práce

- Studie způsobů testování bezpečnosti webových aplikací
- Porovnání schopností již existujících open-source scannerů
- Analýza způsobů detekce jednotlivých typů zranitelností
- Navrhnutí a implementace chybějících funkcionalit do scanneru Revok

Scanner Revok – Základní informace

- Dříve vyvíjeno společností Red Hat Czech, s. r. o.
- Vzniklo jako iniciativa jednoho zaměstnance
- Původně používáno pouze na testování interních systémů
- Uvolněno jako open-source (7. 11. 2014)
- Cílem vytvořit jednoduchý nástroj pro testování bezpečnosti



REVOK Revok Executive Report

Summary

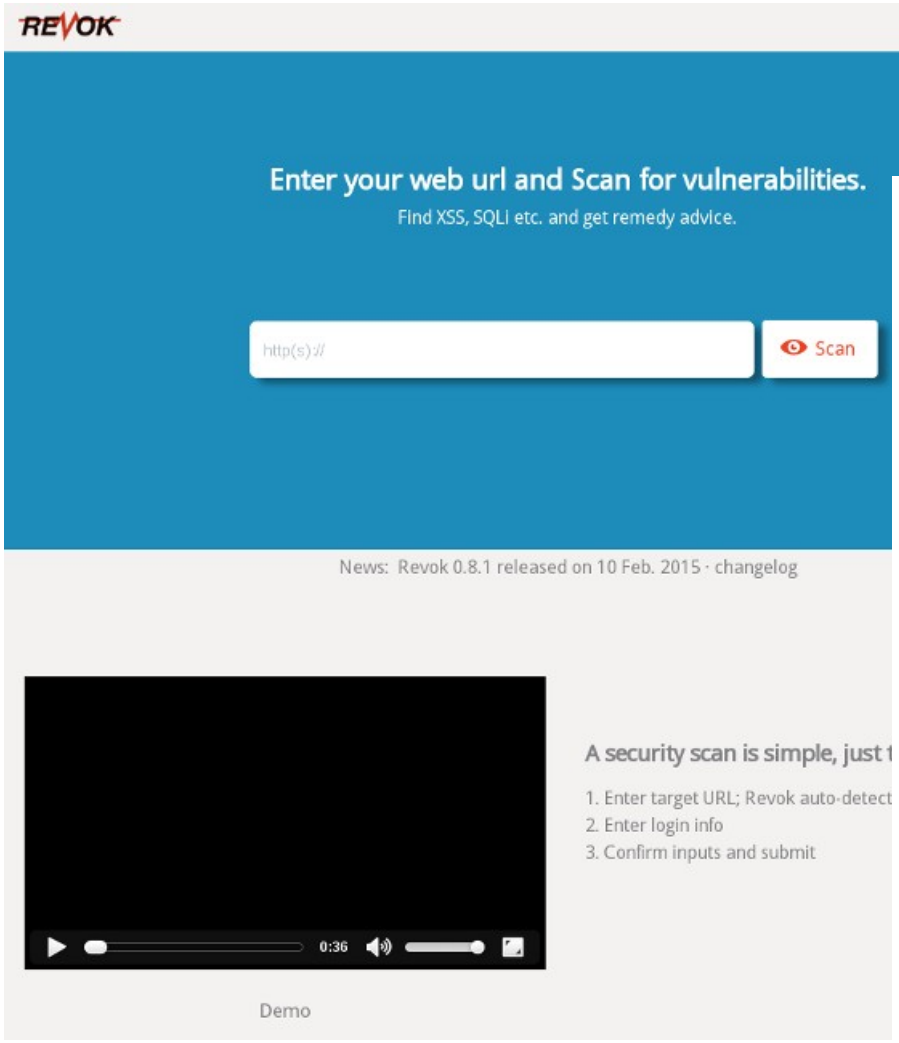
Version: 0.8
Target URL: http://172.16.0.117:8082/wavsep/active/LFI/LFI-Detection-Evaluation-GET-500Error/index.jsp
Start Time: Sun May 17 18:42:12 CEST 2015
Finish Time: Sun May 17 18:46:25 CEST 2015

Scan results:

Category	Number
Vulnerability	0
Security Hardening	3
Sum	3

Tested modules: sitemap, bruteforce, redir, session_fixation, frame_busting, sqli, mime_type_check, passwd_auto_complete, method_check, cookie_attr_check, anti_reflection, ssl_check, corss, reverse_cookie, access_admin, xssi, session_exposed_in_url, path_traversal

Scanner Revok - Ukázka



REVOK **Revok Executive Report**

Summary

Version:	*0.8*
Target URL:	*http://172.16.0.117:8082/wavsep/active/LFI/LFI-Detection-Evaluation-GET-500Error/index.jsp*
Start Time:	*Sun May 17 18:42:12 CEST 2015*
Finish Time:	*Sun May 17 18:46:25 CEST 2015*

Scan results:

Category	Number
Vulnerability	0
Security Hardening	3
Sum	3

Tested modules: sitemap, bruteforce, redir, session_fixation, frame_busting, sqli, mime_type_check, passwd_auto_complete, method_check, cookie_attr_check, anti_reflection, ssl_check, corss, reverse_cookie, access_admin, xssi, session_exposed_in_url, path_traversal

Metodika testování a použité nástroje #1

- Testované zranitelnosti:
  - SQL Injection (SQLi)
  - Cross-Site scripting (XSS)
  - Local File Inclusion (LFI)
  - Remote File Inclusion (RFI)
- Použité nástroje:
  - WIVET
  - WAVSEP
- Automatizované testování:
  - Jenkins

WIVET - Web Input Vector Extractor Teaser
WAVSEP – Web Application Vulnerability Scanner Evaluation Project

Metodika testování a použité nástroje #2

- Další testované scannery:
  - Arachni
  - w3af
  - Wapiti
  - Zap

Scanner Revok – návrh a implementace

- Identifikování příčin 0% hodnocení scanneru Revok v některých testech
- Imlementace automatizovaného testovacího prostředí (Jenkins)
- Zlepšení výsledků crawleru v testech nástroje WIVET
- Zlepšení detekce LFI zranitelností v testech nástroje WAVSEP

Výsledky testů před a po aplikaci změn

Výsledky před aplikací změn

Scanner	WIVET	WAVSEP				Total
		SQLi	XSS	LFI	RFI	
Arachni	96%	100%	90%	100%	100%	97%
Revok	**0%**	32%	88%	**0%**	31%	**19%**
w3af	16%	35%	37%	57%	16%	26%
Wapiti	44%	100%	60%	51%	57%	56%
ZAP	69%	100%	100%	75%	100%	81%

Po aplikaci změn

Scanner	WIVET	WAVSEP				Total
		SQLi	XSS	LFI	RFI	
Revok	**30%**	32%	88%	**13%**	31%	**36%**

Závěr

- Dosažené výsledky:
  - Vylepšené schopnosti detekce scanneru Revok
    - WIVET 30%
    - WAVSEP LFI 13%
  - Vytvořené prostředí pro automatizované testování
  - Všechny nalezené chyby a navrhnuté změny byly poskytnuty zpět komunitě

Děkuji za pozornost

Otázky oponenta

1) Jaký je rozdíl mezi testováním WIVET a WAVSEP?

2) Existují i nějaké komerční nástroje pro testování? Jaké mají výsledky testování oproti volně šířitelným nástrojům?

Scanner	WIVET	WAVSEP				Total
		SQLi	XSS	LFI	RFI	
Tinfoil Security	94%	100%	100%	100%	100%	99%
IBM AppScan	92%	100%	100%	100%	100%	98%
HP WebInspect	96%	100%	100%	91%	100%	97%
Acunetix WVS	94%	100%	100%	57%	78%	86%