

Name: Samarth Jain

USN: 4SU20CS081

Course: Cybersecurity

Trainer: Bharath Kumar

Date: 12/09/2023

Assignment Details

Assigned Date: 11/09/2023

Due Date: 12/09/2023

Topic: Spidering (Directory BruteForce)

Introduction

Spidering is the process of systematically navigating a website's structure by following links from one page to another. It is commonly used to create a map of a website, identifying its various pages and resources. This process is crucial for understanding a web application's architecture and how different components interact.

Crawling, on the other hand, is the automated traversal of web pages by a web crawler or bot. Search engines often use crawlers to index web content for search results. In the context of web security, crawling involves programmatically navigating a website to discover its pages and endpoints. This can be used to identify potential vulnerabilities or misconfigurations in the application.

Crawl and audit is a security testing process that combines crawling and auditing. It entails systematically scanning a web application's pages, forms, and functionalities to uncover security vulnerabilities, such as SQL injection, cross-site scripting (XSS), or insecure authentication mechanisms. This process helps security professionals assess and improve the security posture of a web application.

Spidering with Burp Suite is a specialized technique within the field of web application security testing. Burp Suite is a popular cybersecurity tool that includes a web spidering feature. Security professionals use it to automatically crawl a web application, map its structure, and identify potential security issues. Burp Suite's spidering capabilities are particularly useful for finding hidden or less obvious vulnerabilities, making it a valuable tool in the arsenal of ethical hackers and security analysts.

Scanning for vulnerabilities is the core of Burp Suite's automated testing capability. Burp Scanner can crawl a target to discover content and functionality, and then audit what it finds for vulnerabilities. Alternatively, you can use it to audit items that you have found manually.

Content

OWASP (Open Web Application Security Project) Broken Web Application project

Home page of OWASP

This screenshot shows the homepage of the OWASP Broken Web Applications Project. The browser title bar reads "owaspbwa OWASP Broken Web Applications". The page features a logo and navigation links for "Training Applications" and "Realistic, Intentionally Vulnerable Applications". A prominent yellow warning box at the top states: "!!! This VM has many serious security issues. We strongly recommend that you run it only on the "host only" or "NAT" network in the virtual machine settings !!!". Below this, the "TRAINING APPLICATIONS" section lists several web applications:

OWASP WebGoat	OWASP WebGoat.NET
OWASP ESAPI Java SwingSet Interactive	OWASP Mutilidae II
OWASP RailsGoat	OWASP Bricks
OWASP Security Shepherd	Ghost
Magical Code Injection Rainbow	bWAPP
Damn Vulnerable Web Application	

Logging into OWASP WebGoat application

This screenshot shows the login screen for the OWASP WebGoat application. The URL in the address bar is "10.0.2.6/WebGoat/attack". The login form asks for a "Username" (set to "webgoat") and a "Password" (set to "password"). A yellow warning box at the top of the page repeats the recommendation: "!!! This site is asking you to sign in. We strongly recommend that you run it only on the "host only" or "NAT" network in the virtual machine settings !!!". Below the login form, the "TRAINING APPLICATIONS" section is visible, listing the same set of applications as the homepage.

Starting WebGoat

The screenshot shows the OWASP WebGoat v5.4 home page. At the top, there's a banner with a red goat logo and the text "OWASP WebGoat v5.4". Below the banner, a message says: "Thank you for using WebGoat! This program is a demonstration of common web application flaws. The exercises are intended to provide hands on experience with application penetration testing techniques." It also mentions that the project is led by Bruce Mayhew and provides his email: WebGoat@owasp.org. The page features logos for OWASP and ASPECT SECURITY. It lists "WebGoat Authors" (Bruce Mayhew, Jeff Williams), "WebGoat Design Team" (David Anderson, Laurence Casey (Graphics), Rogan Davies, Bruce Mayhew), "VS.4 Lesson Contributors" (Sherif Koussa, Yiannis Pavlosoglou), "Special Thanks for VS.4" (Brian Cioeai (Milestone of bug fixes), To all who have sent comments), and "Documentation Contributors" (Erwin Geimert, Aung Khant, Sherif Koussa). A "Start WebGoat" button is at the bottom left. A warning box at the bottom right states: "WARNING: While running this program, your machine is extremely vulnerable to attack if you are not running on localhost. If you are NOT running on localhost (default configuration), You should disconnect from the network while using this program. This program is for educational purposes only. Use of these techniques without permission could lead to job termination, financial liability, and/or criminal penalties."

Home page of WebGoat web application

The screenshot shows the "How to work with WebGoat" page. At the top, there's a language selection dropdown set to "English" and a "Logout" link. Below the banner, there are links for "Show Params", "Show Cookies", and "Lesson Plan". On the left, a sidebar lists various security flaws: Introduction, General, Access Control Flaws, AJAX Security, Authentication Flaws, Buffer Overflows, Code Quality, Concurrency, Cross-Site Scripting (XSS), Improper Error Handling, Injection Flaws, Denial of Service, Insecure Communication, Insecure Configuration, Insecure Storage, Malicious Execution, Parameter Tampering, Session Management Flaws, Web Services, Admin Functions, and Challenge. The main content area has sections for "Solution Videos" and "Restart this Lesson". Under "How To Work With WebGoat", it says: "Welcome to a short introduction to WebGoat. Here you will learn how to use WebGoat and additional tools for the lessons." Under "Environment Information", it says: "WebGoat uses the Apache Tomcat server. It is configured to run on localhost although this can be easily changed. This configuration is for single user, additional users can be added in the tomcat-users.xml file. If you want to use WebGoat in a laboratory or in class you might need to change this setup. Please refer to the Tomcat Configuration in the Introduction section." Under "The WebGoat Interface", there's a smaller screenshot showing the interface with numbered steps 2 through 7 and a "Http Basics" link.

Capture the actions performed in the browser in Burpsuite.

Filter: Hiding unrequested and not found items; hiding image and general binary content; hiding empty folders; hiding specific extensions

Contents

	Host	Method	URL	Params	Status	Length	MIME type	Title	Comment	Time requested
>	http://10.0.2.6	POST	/WebGoat/attack		✓ 200	32736	HTML	How to work with WebGoat		00:53:52 19 Sep 2023
>	http://10.0.2.6	GET	/WebGoat/attack		200	4542	HTML	WebGoat VS4		00:53:37 19 Sep 2023
>	http://10.0.2.6	GET	/		200	28533	HTML	owaspbwa OWASP Broke...		00:52:47 19 Sep 2023

Issues

Advisory Request Response

INSPECTOR

Cleartext submission of password

Issue: Cleartext submission of password
Severity: High
Confidence: Certain
Host: http://10.0.2.6
Path: /WebGoat/attack

Issue detail

The response asks the user to enter credentials for Basic HTTP authentication. If these are supplied, they will be submitted over clear-text HTTP (in Base64-encoded form).

Issue background

Some applications transmit passwords over unencrypted connections, making them vulnerable to interception. To exploit this vulnerability, an attacker must be suitably positioned to eavesdrop on the victim's network traffic. This scenario typically occurs when a client communicates with the server over an insecure connection such as public Wi-Fi, or a corporate or home network that is shared with a compromised computer. Common defenses such as switched networks are not sufficient to prevent this. An attack situated in the user's ISP or the application's hosting infrastructure could also perform this attack. Note that an advanced adversary could potentially target any connection made over the Internet's core infrastructure.

Vulnerabilities that result in the disclosure of users' passwords can result in compromises that are extremely difficult to investigate due to obscured audit trails. Even if the application itself only handles non-sensitive information, exposing passwords puts users who have

Right click on the website address on which the scan is to be performed.

In this case, right click on <http://10.0.2.6/>

The option Scan is displayed in the list.

Filter: Hiding unrequested and not found items; hiding image and general binary content; hiding empty folders; hiding specific extensions

Contents

	Host	Method	URL	Params	Status	Length	MIME type	Title	Comment	Time requested
>	http://10.0.2.6	POST	/WebGoat/attack		✓ 200	32736	HTML	How to work with WebGoat		00:53:52 19 Sep 2023
>	http://10.0.2.6	GET	/WebGoat/attack		200	4542	HTML	WebGoat VS4		00:53:37 19 Sep 2023
>	http://10.0.2.6	GET	/		200	28533	HTML	owaspbwa OWASP Broke...		00:52:47 19 Sep 2023

Issues

Advisory Request Response

INSPECTOR

Cleartext submission of password

Issue: Cleartext submission of password
Severity: High
Confidence: Certain
Host: http://10.0.2.6
Path: /WebGoat/attack

Issue detail

The response asks the user to enter credentials for Basic HTTP authentication. If these are supplied, they will be submitted over clear-text HTTP (in Base64-encoded form).

Issue background

Some applications transmit passwords over unencrypted connections, making them vulnerable to interception. To exploit this vulnerability, an attacker must be suitably positioned to eavesdrop on the victim's network traffic. This scenario typically occurs when a client communicates with the server over an insecure connection such as public Wi-Fi, or a corporate or home network that is shared with a compromised computer. Common defenses such as switched networks are not sufficient to prevent this. An attack situated in the user's ISP or the application's hosting infrastructure could also perform this attack. Note that an advanced adversary could potentially target any connection made over the Internet's core infrastructure.

Vulnerabilities that result in the disclosure of users' passwords can result in compromises that are extremely difficult to investigate due to obscured audit trails. Even if the application itself only handles non-sensitive information, exposing passwords puts users who have

After clicking on the Scan option, a new window is opened.

The window provides all the configuration to be done to perform scanning.

First tab displays the Scan Details. Select the first button, Crawl and Audit.

The URL to be scanned has already been selected.

Scan type

- Crawl and audit
- Crawl
- Audit selected items

URLs to scan

Protocol settings

Issues

Advisory Request Response

Cleartext submission of password

Issue: Cleartext submission of password
Severity: High
Confidence: Certain
Host: http://10.0.2.6
Path: /WebGoat/attack

Issue detail

Issue background

The second tab displays the Scan Configuration.

You can customize the configuration. To perform a basic crawl and audit Use a present scan mode.

Set the scan type as Lightweight.

Scan configuration

Scan configurations and modes are groups of settings that define how a scan is performed. Scan modes offer preset options designed to let you trade off speed and coverage. Alternatively, you can select one or more custom configurations. Burp Scanner applies any selected configurations in order, enabling you to fine-tune scanning behaviour.

Lightweight

Gain fast feedback on a site's security - for when speed is a priority. Lightweight mode will complete within 15 minutes.

Fast

More thorough than a Lightweight scan, but still biased towards speed. Fast scans will generally complete within one hour.

Balanced

Provides a balance between coverage and speed. You will typically see the results of a Balanced scan within a few hours.

Deep

Achieve greater coverage and gain a better understanding of a site's security posture. Scanning time depends heavily on the target site's size and complexity.

Remember my choice for future scans

Issues

Advisory Request Response

Cleartext submission of password

Issue: Cleartext submission of password
Severity: High
Confidence: Certain
Host: http://10.0.2.6
Path: /WebGoat/attack

Issue detail

Issue background

In Application Login, you can provide burp with credentials for known accounts that exists which will be used during the crawl and audit. You can add multiple login credentials, for example one for ordinary users, one for manager role within an application or an admin.

In Resource pool, you can configure how burp will make use of your network resources that you have.

You can configure the maximum number of concurrent requests or delay between requests which should be imposed.

You can limit the total amount of traffic so as not to overwhelm the system.

The scanning of the website has been started.

Burp Suite Professional v2023.2.2 - Temporary Project - licensed to h3110w0rld

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

Site map Issue definitions Scope settings

Filter: Hiding unrequested and not found items; hiding image and general binary content; hiding empty folders; hiding specific extensions

Contents										
	Host	Method	URL	Params	Status	Length	MIME type	Title	Comment	Time requested
>	http://10.0.2.6	GET	/utilities/		200	46172	HTML	301 Moved Permanently		00:57:04 19 Sep 2023
>	https://content-signature-2.cdn.mozilla.net	GET	/utilities/		301	671	HTML	ESAPISwingSetInteractive...		00:57:04 19 Sep 2023
>	https://console.services.mozilla.com	GET	/		200	4074	HTML			00:57:04 19 Sep 2023
>	https://firefox.settings.services.mozilla.com	GET	/WebGoat/		200	16109	HTML			00:57:04 19 Sep 2023
>	https://push.services.mozilla.com	GET	/WebGoat/Default.aspx		200	302	HTML	Object moved		00:57:03 19 Sep 2023
>	https://push.services.mozilla.com	GET	/WebGoat/		302	662	HTML			00:57:03 19 Sep 2023
>	https://push.services.mozilla.com	GET	/WebGoat/attack		401	1305	HTML	Apache Tomcat/6.0.24 ...		00:57:01 19 Sep 2023
>	https://push.services.mozilla.com	GET	/robots.txt		404	597	HTML	404 Not Found		00:57:01 19 Sep 2023
>	https://push.services.mozilla.com	GET	/WebGoat/OWASP_Broke...		200	30533	HTML	owaspJava OWASP Br...e...		00:57:01 19 Sep 2023
>	https://push.services.mozilla.com	POST	/WebGoat/attack		200	32736	HTML	How to work with WebGoat		00:53:32 19 Sep 2023

Request		Response								
Pretty	Raw	Hex	Response	Pretty	Raw	Hex	Render	Vn	Vn	Vn
1	POST /WebGoat/attack HTTP/1.1			1	HTTP/1.1 200 OK					
2	Host: 10.0.2.6			2	Date: Mon, 18 Sep 2023 19:24:03 GMT					
3	User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0			3	Server: Apache-Coyote/1.1					
4	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8			4	Content-Type: text/html;charset=ISO-8859-1					
5	Accept-Language: en-US,en;q=0.5			5	Via: 1.1 127.0.1.1					
6	Accept-Encoding: gzip, deflate			6	Vary: Accept-Encoding					
7	Content-Type: application/x-www-form-urlencoded			7	Content-Length: 32524					
8	Content-Length: 19			8	Connection: close					
9	Origin: http://10.0.2.6			9						
10	Authorization: Basic dGv1Z29hdDp3ZWJnb2F0			10						
11	Connection: close			11						
12	Referer: http://10.0.2.6/WebGoat/attack			12						
13	Cookie: acopenidvids=swingset_jotto_phpb2_redmine; acgroupswithpersist=nada; JSESSIONID=10236A933DB26E40534697453E03162			13	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">					
14	Upgrade-Insecure-Requests: 1			14	<html xmlns="http://www.w3.org/1999/xhtml">					
15				15	<head>					
16	start=Start+WebGoat			16	<meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-1" />					
				17	<title>How to work with WebGoat</title>					
				18	<link rel="stylesheet" href="css/webgoat.css" type="text/css" />					
				19	<link rel="stylesheet" href="css/lesson.css" type="text/css" />					
				20	<link rel="stylesheet" href="css/menu.css" type="text/css" />					
				21	<link rel="stylesheet" href="css/layers.css" type="text/css" />					
				22	<script language="JavaScript1.2" src="javascript/javascript.js" type="text/javascript">					
				23	</script>					
				24	<script language="JavaScript1.2" src="javascript/menu_system.js" type="text/javascript">					

The scan displays all the directories and webpages that are present in the web server.

Burp Suite Professional v2023.2.2 - Temporary Project - licensed to h3110w0rld

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

Site map Issue definitions Scope settings

Filter: Hiding unrequested and not found items; hiding image and general binary content; hiding empty folders; hiding specific extensions

Contents										
	Host	Method	URL	Params	Status	Length	MIME type	Title	Comment	Time requested
>	http://10.0.2.6	GET	/bedgeit/		200	3440	HTML	The Budget Store		00:57:16 19 Sep 2023
>	https://content-signature-2.cdn.mozilla.net	GET	/WackoPicks/		200	4074	HTML	WackoPicks.com		00:57:16 19 Sep 2023
>	https://console.services.mozilla.com	GET	/		301	671	HTML	301 Moved Permanently		00:57:16 19 Sep 2023
>	https://firefox.settings.services.mozilla.com	GET	/WebGoat/		200	3847	HTML	ESAPISwingSetInteractive...		00:57:16 19 Sep 2023
>	https://push.services.mozilla.com	GET	/WebGoat/Default.aspx		301	516	HTML	503 Service Temporarily...		00:57:16 19 Sep 2023
>	https://push.services.mozilla.com	GET	/WebGoat/		200					

The scanning is still in progress.

The screenshot shows the Burp Suite interface during the scanning phase. The dashboard tab is selected, displaying a tree view of the target URL (`http://10.0.2.6`). The tree includes categories such as AppServerDemo, MCSR, and WebGoat, with numerous sub-items under each. To the right, a list of requests is shown in a table format, with one specific request highlighted. On the far right, an issue detail for 'Cleartext submission of password' is expanded, providing information about the severity, confidence, host, and path of the vulnerability.

The dashboard displays all the progress of scanning.

The crawling phase displays all the request made. Later, the audit phase displays all the issues.

This screenshot shows the Burp Suite interface during the crawling and audit phases. The dashboard tab is selected, showing the progress of crawling and auditing. The audit phase (Issue activity) is visible on the right, listing various security issues found during the scan. The event log at the bottom provides a history of system events and messages.

The progress of the scan can be viewed in the Details tab using the Progress Bar.

The settings can be changed in Details as they are in progress.

This screenshot shows the Burp Suite Professional interface. The top navigation bar includes 'Burp', 'Project', 'Intruder', 'Repeater', 'Window', 'Help', 'Dashboard', 'Target', 'Proxy', 'Intruder', 'Repeater', 'Collaborator', 'Sequencer', 'Decoder', 'Comparer', 'Logger', 'Extensions', and 'Learn'. The main window has tabs for 'Tasks' and 'Issue activity'. The 'Tasks' tab is active, showing three tasks: '1. Live passive crawl from Proxy (all traffic)', '2. Live audit from Proxy (all traffic)', and '3. Crawl and audit of 10.0.2.6'. Task 3 is currently running, indicated by a progress bar at the bottom of its card. The 'Issue activity' tab is also visible, showing a list of discovered items with columns for Host, Path, and Status. The status column uses icons to represent different issue types. The bottom of the interface shows an event log and system status indicators for memory and disk usage.

This shows you all of the items that have been discovered during the crawl and you can view their progress through the different phases of the audit.

You can see the Passive phases and Active phases, the JavaScript work, full URL, number of issues that have been reported for each item, number of requests and errors.

Provides complete visibility of the Burp scan.

This screenshot shows the 'Audit items' tab within the 'Tasks' section of Burp Suite Professional. It displays a detailed table of audit results for task 3. The columns include: #, Host, URL, Status, Passive p..., Active phases, JavaScript p..., Issues, and Requests. The table lists numerous URLs and their corresponding audit details, such as scanning status, active phases (e.g., 1, 2, 3, 4, 5), JavaScript processing, and the count of issues and requests. The 'Issues' column contains small icons representing different types of findings. The bottom of the interface shows an event log and system status indicators for memory and disk usage.

The Issue activity log displays the vulnerabilities which appear in real-time as they are discovered.

The Event log displays various information and errors and other details to be aware of.

The Logger tab keeps track and logs all the activity performed during the Crawl and Audit.

This screenshot shows the Burp Suite Professional interface with the 'Logger' tab selected. The main pane displays a table of audit results for '3. Crawl and audit of 10.0.2.6'. The table includes columns for Host, Path, Query, Param count, Status, Length, Start response timer, and Comment. The 'Host' column lists various URLs such as /mutilidae/index.php, /mutilidae/, /joomla/index.php, etc. The 'Path' column shows specific file paths like /mutilidae/help1, /joomla/about%20(copy), /joomla/bak/leaderboard..., etc. The 'Query' column contains parameters like &fram..., &fram..., &fram..., etc. The 'Param count' column shows values like 2, 3, 3, 3, 3, 3, etc. The 'Status' column shows 200 or 404. The 'Length' column shows values like 64999, 238, 230, 230, 193, 193, etc. The 'Start response timer' column shows times like 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, etc. The 'Comment' column provides additional details for each request. Below this table is a smaller table titled 'View filter: Showing all items' with columns for #, Time, Tool, Method, Host, Path, Query, Param count, Status, Length, Start response timer, and Comment. The bottom section of the screenshot shows the 'Event log' tab with a table of audit events. The 'Time' column shows dates from 01-04-2023 to 05-21-2023. The 'Type' column shows categories like Info, Error, Task, Scanner, and Logger. The 'Source' column provides more detail about each event. The status bar at the bottom indicates Memory: 457.5MB and Disk: 8.0MB.

The complete scan of the target website is complete.

This screenshot shows the Burp Suite Professional interface with the 'Logger' tab selected. The main pane displays a table of audit results for '3. Crawl and audit of 10.0.2.6'. The table includes columns for Task, Time, Action, Issue type, Host, and Path. The 'Host' column lists URLs like /mutilidae/index.php, /mutilidae/, /joomla/index.php, etc. The 'Path' column shows file paths like /mutilidae/help1, /joomla/about%20(copy), /joomla/bak/leaderboard..., etc. The 'Issue type' column shows various vulnerabilities found, such as Cross-site scripting (DOM-based), HTML5 storage manipulation (DOM-based), Open redirection (DOM-based), DOM data manipulation (DOM-based), etc. The 'Action' column shows the status of each issue. Below this table is a smaller table titled 'Issues' with columns for Task, Time, Action, Issue type, Host, and Path. The bottom section of the screenshot shows the 'Event log' tab with a table of audit events. The 'Time' column shows dates from 01-28-2023 to 05-21-2023. The 'Type' column shows categories like Error, Proxy, Scanner, and Task. The 'Source' column provides more detail about each event. The status bar at the bottom indicates Memory: 394.0MB and Disk: 8.0MB.

The progress bar shows the completion of the crawl and audit.

This screenshot shows the Burp Suite Professional interface after a task has been completed. The main window displays the results of a 'Crawl and audit' task for host 10.0.2.6. The 'Issue activity' tab is selected, showing a summary of findings:

- Scan type:** Crawl and audit
- Scope:** 10.0.2.6
- Configuration:** Crawl and Audit - Lightweight
- Issues:** 24 (with 2 critical, 1 major, 21 minor)
- Requests:** 6,348
- Errors:** 23
- Unique locations:** 470

A progress bar at the bottom indicates the task was paused due to reaching a time limit, and it is currently auditing the URL <http://10.0.2.6:80/yazd/bay/account.jsp>.

The 'Event log' tab shows a detailed timeline of audit events, including Task 3 starting and discarding logs, and various audit phases being completed.

This screenshot shows the Burp Suite Professional interface after another task has been completed, identical to the one in the previous screenshot. The main window displays the results of a 'Crawl and audit' task for host 10.0.2.6. The 'Issue activity' tab is selected, showing a summary of findings:

- Scan type:** Crawl and audit
- Scope:** 10.0.2.6
- Configuration:** Crawl and Audit - Lightweight
- Issues:** 24 (with 2 critical, 1 major, 21 minor)
- Requests:** 6,348
- Errors:** 23
- Unique locations:** 470

A progress bar at the bottom indicates the task was paused due to reaching a time limit, and it is currently auditing the URL <http://10.0.2.6:80/yazd/bay/account.jsp>.

The 'Event log' tab shows a detailed timeline of audit events, including Task 3 starting and discarding logs, and various audit phases being completed.

Screenshot of Burp Suite Professional v2023.2.2 showing the Audit phase results. The 'Issue activity' tab is selected, displaying a list of vulnerabilities found during the crawl and audit of 10.0.2.6. The table includes columns for Task, Time, Action, Issue type, Host, Path, and Insertion point. A sidebar on the right shows a detailed list of URLs and their paths. The 'Event log' tab at the bottom shows audit logs with entries like 'Proxy [12] Unknown' and 'Scanner [187] Your sys...'. The status bar at the bottom indicates Memory: 401.8MB and Disk: 8.0MB.

The Audit phase of the Crawl and Audit has detected many issues.

They are all displayed in the Issue Activity tab.

As we can see, a DOM-based Cross-Site Scripting vulnerability has been reported. It is a high-level threat.

The Report of the vulnerabilities can be extracted. The issue is has been notified to the auditor.

Screenshot of Burp Suite Professional v2023.2.2 showing the details of a specific DOM-based Cross-Site Scripting vulnerability. The 'Issue activity' tab is selected, and the issue is highlighted. The 'Details' tab shows the issue type as 'Cross-site scripting (DOM-based)' with a severity of 'High'. The 'Issue detail' section explains the vulnerability: 'The application may be vulnerable to DOM-based cross-site scripting. Data is read from `input.value` and passed to `element.innerHTML`'. The 'Issue background' section provides context about the issue's nature. The status bar at the bottom indicates Memory: 391.7MB and Disk: 8.0MB.

The types of issues can be filtered in the Issue activity tab.

Here, all the issues/vulnerabilities of high-level threat are displayed and all other threat levels are filtered out.

The screenshot shows the Burp Suite Professional interface with the 'Issue activity' tab selected. A specific issue is highlighted in the list:

#	Task	Time	Action	Issue type	Host	Path	Insertion point
173	3	01:12:00 19 Sep 2023	Issue found	① Cross-site scripting (DOM-based)	http://10.0.2.6	/mutillidae/index.php	
153	3	01:00:59 19 Sep 2023	Evidence added	② Cross-site scripting (DOM-based)	http://10.0.2.6	/dom-xss-example.html	
152	3	01:00:59 19 Sep 2023	Issue found	③ Cross-site scripting (reflected)	http://10.0.2.6	/awstats/awstats.p	config parameter
150	3	01:00:28 19 Sep 2023	Issue found	④ Cross-site scripting (DOM-based)	http://10.0.2.6	/dom-xss-example.html	
149	3	01:00:28 19 Sep 2023	Issue found	⑤ Cross-site scripting (DOM-based)	http://10.0.2.6	/dom-xss-example.html	
31	3	01:00:15 19 Sep 2023	Issue found	⑥ Cleartext submission of password	http://10.0.2.6	/	
23	3	01:00:09 19 Sep 2023	Issue found	⑦ Client-side desync	http://10.0.2.6	/AppSensorDemo/updateProfile.jsp	
21	3	01:00:07 19 Sep 2023	Issue found	⑧ Flash cross-domain policy	http://10.0.2.6	/crossdomain.xml	
17	3	01:00:06 19 Sep 2023	Issue found	⑨ Flash cross-domain policy	http://10.0.2.6	/crossdomain.xml	

The issue details show it's a 'Cross-site scripting (reflected)' vulnerability. The payload was `x854<script>alert(1)</script>hksA`, which was copied into the config parameter. The advisory notes that this proof-of-concept attack demonstrates the possibility of injecting arbitrary JavaScript into the application's response.

The HTTP Request message sent during the Crawling phase can be seen.

The highlighter specifically highlights the issue in the webpage.

The screenshot shows the Burp Suite Professional interface with the 'Request' tab selected. The highlighted request message is as follows:

```
1 GET /awstats/awstats.p?config=owaspwaxt854%3cscript%3ealert(1)%3c%2fscript%3ehksA&framename=mainleft HTTP/1.1
2 Host: 10.0.2.6
3 Accept-Encoding: gzip, deflate
4 Accept: */*
5 Accept-Language: en-US;q=0.9, en;q=0.8
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.178 Safari/537.36
7 Connection: close
8 Cache-Control: max-age=0
9 Referer: http://10.0.2.6/awstats/awstats.p?config=owaspwaxt854%3cscript%3ealert(1)%3c%2fscript%3ehksA&framename=mainleft
10
11
```

The payload `x854<script>alert(1)</script>hksA` is clearly visible in the request URL.

The HTTP Response message can be seen.

3. Crawl and audit of 10.0.2.6

#	Task	Time	Action	Issue type	Host	Path	Insertion point
173	3	01:12:00 19 Sep 2023	Issue found	① Cross-site scripting (DOM-based)	http://10.0.2.6	/mwutilidae/index.php	
153	3	01:00:59 19 Sep 2023	Evidence added	① Cross-site scripting (DOM-based)	http://10.0.2.6	/mwutilidae/index.php	
152	3	01:00:50 19 Sep 2023	Issue found	① Cross-site scripting (reflected)	http://10.0.2.6	/awstats/awstats.pl	config parameter
150	3	01:00:28 19 Sep 2023	Issue found	① Cross-site scripting (DOM-based)	http://10.0.2.6	/dom-xss-example.html	
149	3	01:00:28 19 Sep 2023	Issue found	② Cross-site scripting (DOM-based)	http://10.0.2.6	/dom-xss-example.html	
31	3	01:00:15 19 Sep 2023	Issue found	③ Cleartext submission of password	http://10.0.2.6	/	
23	3	01:00:09 19 Sep 2023	Issue found	④ Client-side script	http://10.0.2.6	/AppSenseDemo/updateProfile.jsp	
21	3	01:00:07 19 Sep 2023	Issue found	⑤ Flash cross-domain policy	http://10.0.2.6	/crossdomain.xml	
17	3	01:00:06 19 Sep 2023	Issue found	⑥ Flash cross-domain policy	https://10.0.2.6	/crossdomain.xml	

Event log

3. Crawl and audit of 10.0.2.6

Time	Type	Source
01:34:27 19 Sep 2023	Error	Proxy [14] Unknown
01:27:48 19 Sep 2023	Error	Proxy [4] Unknown
01:22:29 19 Sep 2023	Error	Proxy [2] Unknown
01:11:58 19 Sep 2023	Info	Scanner Task3 [187] Python
01:04:03 19 Sep 2023	Error	Scanner Failed to connect
01:00:04 19 Sep 2023	Info	Task3 [1] Audit started
01:00:03 19 Sep 2023	Info	Task3 [1] Crawling the site
00:59:24 19 Sep 2023	Info	Logger Discarded log
00:59:02 19 Sep 2023	Info	Task3 Over-read page
00:57:49 19 Sep 2023	Info	Task3 [3] You're being audited
00:57:01 19 Sep 2023	Info	Task3 [3] Your browser has been audited
00:53:37 17 Sep 2023	Error	Proxy [2] Authentication failed
00:52:19 19 Sep 2023	Info	Scanner This version of Burp Suite was released one minute ago. Please consider updating to benefit from enhancements and security fix...
00:52:18 19 Sep 2023	Info	Proxy Proxy service started on 127.0.0.1:8080

The highlighter specifically highlights the issue in the webpage.

3. Crawl and audit of 10.0.2.6

#	Task	Time	Action	Issue type	Host	Path	Insertion point
173	3	01:12:00 19 Sep 2023	Issue found	① Cross-site scripting (DOM-based)	http://10.0.2.6	/mwutilidae/index.php	
153	3	01:00:59 19 Sep 2023	Evidence added	① Cross-site scripting (DOM-based)	http://10.0.2.6	/mwutilidae/index.php	
152	3	01:00:50 19 Sep 2023	Issue found	① Cross-site scripting (reflected)	http://10.0.2.6	/awstats/awstats.pl	config parameter
150	3	01:00:28 19 Sep 2023	Issue found	① Cross-site scripting (DOM-based)	http://10.0.2.6	/dom-xss-example.html	
149	3	01:00:28 19 Sep 2023	Issue found	② Cross-site scripting (DOM-based)	http://10.0.2.6	/dom-xss-example.html	
31	3	01:00:15 19 Sep 2023	Issue found	③ Cleartext submission of password	http://10.0.2.6	/	
23	3	01:00:09 19 Sep 2023	Issue found	④ Client-side script	http://10.0.2.6	/AppSenseDemo/updateProfile.jsp	
21	3	01:00:07 19 Sep 2023	Issue found	⑤ Flash cross-domain policy	http://10.0.2.6	/crossdomain.xml	
17	3	01:00:06 19 Sep 2023	Issue found	⑥ Flash cross-domain policy	https://10.0.2.6	/crossdomain.xml	

Event log

3. Crawl and audit of 10.0.2.6

Time	Type	Source
01:34:27 19 Sep 2023	Error	Proxy [14] Unknown
01:27:48 19 Sep 2023	Error	Proxy [4] Unknown
01:22:29 19 Sep 2023	Error	Proxy [2] Unknown
01:11:58 19 Sep 2023	Info	Scanner Task3 [187] Python
01:00:04 19 Sep 2023	Error	Scanner Failed to connect
01:00:03 19 Sep 2023	Info	Task3 [1] Audit started
00:59:24 19 Sep 2023	Info	Task3 [1] Crawling the site
00:59:02 19 Sep 2023	Info	Logger Discarded log
00:57:49 19 Sep 2023	Info	Task3 Over-read page
00:57:01 19 Sep 2023	Info	Task3 [3] Your browser has been audited
00:53:37 17 Sep 2023	Error	Proxy [2] Authentication failed
00:52:19 19 Sep 2023	Info	Scanner This version of Burp Suite was released one minute ago. Please consider updating to benefit from enhancements and security fix...
00:52:18 19 Sep 2023	Info	Proxy Proxy service started on 127.0.0.1:8080

The Event log keeps track of all the events.

Event log

Time	Type	Source	Message
01:34:27 19 Sep 2023	Error	Proxy	[14] Unknown host
01:37:48 19 Sep 2023	Error	Proxy	[4] Unknown host
01:22:29 19 Sep 2023	Error	Proxy	[2] Unknown host
01:12:20 19 Sep 2023	Info	Scanner	Scan stopped
01:11:38 19 Sep 2023	Info	Scanner	[187] Your system
01:00:04 19 Sep 2023	Info	Task 3	Identifying its
01:00:03 19 Sep 2023	Info	Task 3	Crawl started
00:59:49 19 Sep 2023	Info	Task 3	[3] Your mach
00:57:01 19 Sep 2023	Info	Task 3	Crawl started
00:53:17 19 Sep 2023	Error	Proxy	[2] Authentic
00:52:19 19 Sep 2023	Info	Scanner	This version of Burp Suite was released one month ago. Please consider updating to benefit from enhancements and security fix...
00:52:18 19 Sep 2023	Info	Proxy	Proxy service started on 127.0.0.1:8080

Event log

Time	Type	Source	Message
01:34:27 19 Sep 2023	Error	Proxy	[14] Unknown host
01:37:48 19 Sep 2023	Error	Proxy	[4] Unknown host
01:22:29 19 Sep 2023	Error	Proxy	[2] Unknown host
01:12:20 19 Sep 2023	Info	Scanner	Scan stopped
01:11:38 19 Sep 2023	Info	Scanner	[187] Your system
01:00:04 19 Sep 2023	Info	Task 3	Identifying its
01:00:03 19 Sep 2023	Info	Task 3	Crawl started
00:59:49 19 Sep 2023	Info	Task 3	[3] Your machine
00:57:01 19 Sep 2023	Info	Task 3	Crawl started
00:53:17 19 Sep 2023	Error	Proxy	[2] Authentication
00:52:19 19 Sep 2023	Info	Scanner	This version of Burp Suite was released one month ago. Please consider updating to benefit from enhancements and security fix...
00:52:18 19 Sep 2023	Info	Proxy	Proxy service started on 127.0.0.1:8080

The Logger tab keeps all the HTTP Requests made and their HTTP Response messages.

The 6705th HTTP Request and its consequent HTTP Response message is displayed below.

The screenshot shows the Burp Suite Professional interface with the 'Logger' tab selected. A specific request and its corresponding response are highlighted. The request is a GET to '/cyclone/uploads/bankstatement-47.pdf' with a status of 404 Not Found. The response body contains detailed information about the request, including the host, date, server, and various headers. The response code is 100 OK. The response body includes the following text:

```
HTTP/1.1 404 Not Found
Date: Mon, 18 Sep 2023 19:31:40 GMT
Server: Apache/2.2.14 (Ubuntu) ngnix/1.20.0
PHP/8.0.12 with PHP7.4-fpm/7.4.32
Phusion_Passenger/4.0.38 mod_perl/2.0.14 OpenSSL/0.9.8k
X-Request-ID: c69875d56441e8b008693a4a445e0e3
X-Runtime: 0.013583
X-Powered-By: Phusion Passenger 4.0.38
Status: 404 Not Found
Vary: Accept-Encoding
Content-Length: 791
Connection: close
Content-Type: text/html; charset=utf-8
<!DOCTYPE html>
<html lang="en">
<head>
```

Live Crawl View tab.

The screenshot shows the Burp Suite Professional interface with the 'Live crawl view' tab selected. It displays a timeline of tasks and events. A specific task is highlighted, showing a detailed view of its activity. The task details show it was a GET request to '/cyclone/uploads/bankstatement-47.pdf' with a status of 404 Not Found. The response body is identical to the one shown in the previous screenshot, indicating a 404 error for a file that does not exist.

Analysis

The analysis of spidering in our report highlights its critical role in web application assessment and information gathering. Spidering allows for the systematic exploration of a website's architecture, enabling us to map its structure and identify potential security vulnerabilities and weaknesses. By automating the process of following links and collecting data, spidering significantly enhances the efficiency of web security assessments. Furthermore, the integration of spidering tools like Burp Suite empowers cybersecurity professionals to conduct comprehensive audits, making it an indispensable component of modern web application security practices.

Conclusion

In conclusion, our report has shed light on the pivotal role of spidering in the realm of web application assessment and security. Spidering serves as a foundational step in understanding and analyzing the structure and content of websites. It enables efficient navigation and data collection, ultimately leading to the discovery of potential vulnerabilities and misconfigurations. When used in conjunction with specialized tools like Burp Suite, spidering becomes a powerful asset in the arsenal of cybersecurity professionals, offering comprehensive insights and facilitating robust security audits. Embracing spidering techniques is imperative for organizations seeking to enhance the resilience of their web applications in an ever-evolving threat landscape.

References

[Burp Scanner - Web Vulnerability Scanner from PortSwigger](#)

[How to scan a website for vulnerabilities using Burp Scanner - YouTube](#)