

Lab 12: Burp Suite, Spider Function	
Name	Tran Minh Triet
Student ID	SE172241

Spider with Burp Suite

DashboardTargetProxyIntruderRepeaterCollaboratorSequencerDecoderComparerLoggerOrganizerExtensionsLearn

Site mapIssue definitionsScope settings

Filter: Hiding not found items: hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

http://10.10.120.148

https://passwordleakcheck-pa.googleapis.co

Host	Method	URL	Params	Status code	Length	MIME type	Title
http://10.10.120.148	GET	/dwa/js/add_event_...		200	881	script	
http://10.10.120.148	GET	/dwa/js/dwaPage.js		200	1319	script	
http://10.10.120.148	GET	/index.php		200	7142	HTML	Welcome : Dar
http://10.10.120.148	GET	/login.php		200	1850	HTML	Login : Damn
http://10.10.120.148	GET	/		302	517		
http://10.10.120.148	POST	/login.php		✓ 302	348		
http://10.10.120.148	GET	/about.php					
http://10.10.120.148	GET	/dwa/css/login.css					
http://10.10.120.148	GET	/dwa/images/Rando...					

RequestResponse

PrettyRawHex

```
1 GET / HTTP/1.1
2 Host: 10.10.120.148
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.134 Safari/537.36
5 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng
/*;q=0.8,application/signed-exchange;vmb3;q=0.7
6 Accept-Encoding: gzip, deflate
7 Accept-Language: en-US,en;q=0.9
8 Connection: close
9
10
```

Issues

Clear text submission of password

Unencrypted communications

Cookie without HttpOnly flag set

Frameable response (potential Clickjacking) [2]

Unencrypted communications

Issue: Unencrypted communications

Severity: Low

Confidence: Certain

Host: http://10.10.120.148

Path: /

Issue description

The application allows users to connect to it over unencrypted connections. An attacker suitably positioned to view a legitimate user's network traffic could record and monitor their interactions with the application and obtain any information the user supplies. Furthermore, an attacker able to modify traffic could use the application as a platform for attacks against its users and third-party websites. Unencrypted connections have been exploited by ISPs and governments to track users, and to inject adverts and malicious JavaScript. Due to these concerns, web browser vendors are planning to visually flag unencrypted connections as hazardous.

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 attacker 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.

Please note that using a mixture of encrypted and unencrypted communications is an ineffective defense

DashboardTargetProxyIntruderRepeaterCollaboratorSequencerDecoderComparerLoggerOrganizerExtensionsLearn

Site mapIssue definitionsScope settings

Filter: Hiding not found items: hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

http://10.10.120.148

https://passwordleakcheck-pa.googleapis.co

about.php

css

dwra

images

login.php

login_log.png

js

add_event_listeners.js

dwaPage.js

favicon.ico

index.php

instructions.php

login.php

username=admin&password=test123&l

logout.php

phpinfo.php

security.php

setup.php

vulnerabilities

Host	Method	URL	Params	Status code	Length	MIME type	Title
http://10.10.120.148	GET	/dwa/js/add_event_...		200	881	script	
http://10.10.120.148	GET	/dwa/js/dwaPage.js		200	1319	script	
http://10.10.120.148	GET	/index.php		200	7142	HTML	Welcome : Dar
http://10.10.120.148	GET	/login.php		200	1850	HTML	Login : Damn
http://10.10.120.148	GET	/		302	517		
http://10.10.120.148	POST	/login.php		✓ 302	348		
http://10.10.120.148	GET	/about.php					
http://10.10.120.148	GET	/dwa/css/login.css					
http://10.10.120.148	GET	/dwa/images/Rando...					

RequestResponse

PrettyRawHex

```
1 GET / HTTP/1.1
2 Host: 10.10.120.148
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.134 Safari/537.36
5 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng
/*;q=0.8,application/signed-exchange;vmb3;q=0.7
6 Accept-Encoding: gzip, deflate
7 Accept-Language: en-US,en;q=0.9
8 Connection: close
9
10
```

Issues

Clear text submission of password

Unencrypted communications

Cookie without HttpOnly flag set

Frameable response (potential Clickjacking) [2]

Unencrypted communications

Issue: Unencrypted communications

Severity: Low

Confidence: Certain

Host: http://10.10.120.148

Path: /

Issue description

The application allows users to connect to it over unencrypted connections. An attacker suitably positioned to view a legitimate user's network traffic could record and monitor their interactions with the application and obtain any information the user supplies. Furthermore, an attacker able to modify traffic could use the application as a platform for attacks against its users and third-party websites. Unencrypted connections have been exploited by ISPs and governments to track users, and to inject adverts and malicious JavaScript. Due to these concerns, web browser vendors are planning to visually flag unencrypted connections as hazardous.

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 attacker 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.

Please note that using a mixture of encrypted and unencrypted communications is an ineffective defense

1 Burp Project Intruder Repeater Window Help

Burp Suite Professional v2023.6.1 - Temporary Project - Licensed to Zer0DayLab Crew

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

Site map Issue definitions Scope settings

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Contents

Host	Method	URL	Params	Status code	Length	MIME type	Title
http://10.10.120.148	GET	/vulnerabilities/csrcf/					

Request Response

Pretty Raw Hex

```
1 GET /vulnerabilities/csrcf/ HTTP/1.1
2 Host: 10.10.120.148
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/114.0.5735.134 Safari/537.36
7 Connection: close
8 Cache-Control: max-age=0
9
10
```

Inspector

Advisory

Site map

- images
 - RandomStorm.png
 - login_logo.png
- js
 - add_event_listeners.js
 - divwapage.js
- favicon.ico
- index.php
- instructions.php
- login.php
 - username=admin&password=test123
- logout.php
- phpinfo.php
- security.php
- setup.php
- vulnerabilities
 - brute
 - captcha
 - csp
 - csrcf
 - exec
 - fi
 - javascript
 - sql
 - sql_blind
 - upload
 - weak_id
 - xss_d
 - xss_r
 - xss_s

0 matches

36°C Có nắng

1 Burp Project Intruder Repeater Window Help

Burp Suite Professional v2023.6.1 - Temporary Project - Licensed to Zer0DayLab Crew

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

Site map Issue definitions Scope settings

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Contents

Host	Method	URL	Params	Status code	Length	MIME type	Title
http://10.10.120.148	GET	/vulnerabilities/xss_s/					

Request Response

Pretty Raw Hex

```
1 GET /vulnerabilities/xss_s/ HTTP/1.1
2 Host: 10.10.120.148
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/114.0.5735.134 Safari/537.36
7 Connection: close
8 Cache-Control: max-age=0
9
10
```

Inspector

Advisory

Site map

- security.php
- setup.php
- vulnerabilities
 - brute
 - captcha
 - csp
 - csrcf
 - exec
 - fi
 - javascript
 - sql
 - sql_blind
 - upload
 - weak_id
 - xss_d
 - xss_r
 - xss_s

0 matches

36°C Có nắng

Burp Suite Professional v2023.6.1 - Temporary Project - Licensed to Zer0DayLab Crew

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

Site map Issue definitions Scope settings

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Contents

Host	Method	URL	Params	Status code	Length	MIME type	Title
http://10.10.120.148	GET	/dwa/includes/					

Issues

Request Response

```
1 GET /dwa/includes/ HTTP/1.1
2 Host: 10.10.120.148
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/114.0.5735.114 Safari/537.36
7 Connection: close
8 Cache-Control: max-age=0
9
10
```

Inspector

Advisory

36°C Có nắng

Burp Suite Professional v2023.6.1 - Temporary Project - Licensed to Zer0DayLab Crew

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

Site map Issue definitions Scope settings

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Contents

Host	Method	URL	Params	Status code	Length	MIME type	Title
http://10.10.120.148	GET	/dwa		301	537	HTML	301 Moved Perm

Issues

Request Response

```
1 GET /dwa HTTP/1.1
2 Host: 10.10.120.148
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.114 Safari/537.36
5 Accept:
6 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=0.7
7 Accept-Encoding: gzip, deflate
8 Accept-Language: en-US,en;q=0.9
9 Cookie: PHPSESSID=q3ihpc53o9fandj3f6709shkd4; security=impossible
10 Connection: close
11
```

Inspector

Advisory

*new 16 - Notepad++

```
1 Em tên là Trần Minh Triết - SE172241
2
3 PHPSESSID=q3ihpc53o9fandj3f6709shkd4; security=impossible
```

36°C Có nắng