

Assignment_2_Module_3

Topic: Vulnerability assessment using ZAP

Scan Date: June 15, 2025

Tool Used: ZAP (Zed Attack Proxy)

Target: <https://1password.com>


The goal of this assignment is to perform a vulnerability assessment using the OWASP ZAP tool by scanning a test website and analyzing potential security issues.

Vulnerability Name:

PII Disclosure:

PII Disclosure

URL: <https://1password.com/pt/compare/1password-vs-dashlane>

Risk:  High

Confidence: High

Parameter:

Attack:

Evidence: 6702401128975

CWE ID: 359

WASC ID: 13

Source: Passive (10062 - PII Disclosure)

Input Vector:

Description:

The response contains Personally Identifiable Information, such as CC number, SSN and similar sensitive data.

Absence of Anti-CSRF Tokens:

Absence of Anti-CSRF Tokens

URL: <https://1password.com/pt/business-newsletter/>

Risk:  Medium

Confidence: Low

Parameter: |

Attack:

Evidence: <form method=post class="u-is-displayflex u-flexvertical u-flexhorizontal@md u-justifycenter u-aligncenter" accept-charset=utf-8 action=https://flow.1passwordservices.com/api/v1/form data-event-category=Newsletter data-event-action=form-business-newsletter id=newsletter-form>

CWE ID: 352

WASC ID: 9

Source: Passive (10202 - Absence of Anti-CSRF Tokens)

Description:

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

A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf.


CSRF attacks are effective in a number of 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.

CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.

CSP: style-src unsafe-hashes:

CSP: style-src unsafe-hashes

URL: <http://1password.com>
Risk:  Medium
Confidence: High
Parameter: content-security-policy
Attack:

```
default-src 'none'; media-src 'self' https://videos.ctfassets.net/; script-src-elem 'self' 'nonce-7af98cbf-c6eb-4f69-a94d-e3901b00731f' https://transcend-cdn.com/cm/fa619274-3c15-4155-bbec-c0cb75733259/airgap.js https://transcend-cdn.com/cm/fa619274-3c15-4155-bbec-c0cb75733259/ui.js https://transcend-cdn.com/cm/fa619274-3c15-4155-bbec-c0cb75733259/xdi.js 'unsafe-hashes' 'sha256-cdFvGnPVdeavqCupEOX1iKxDb2jmBXXTGmE6AcHOk+c=' 'sha256-yT/s9zf56jX7wyB2f+yhxGo0VBoDnFqMx5qPvh0jvgQ=' 'sha256-TQ9lqihfbMvC+yQs4RAPRBe8No3FB3+MYPxT/OnPn/A=' 'sha256-ep0lyBO1i+WpsX2W3CxFRXjI+Hxg1zdLj+K4nN4Yzdk='; script-src 'self' 'wasm-unsafe-eval' 'nonce-7af98cbf-c6eb-4f69-a94d-e3901b00731f' https://transcend-cdn.com/cm/fa619274-3c15-4155-bbec-c0cb75733259/airgap.js https://transcend-cdn.com/cm/fa619274-3c15-4155-bbec-c0cb75733259/ui.js https://transcend-cdn.com/cm/fa619274-3c15-4155-bbec-c0cb75733259/xdi.js; style-src 'self' 'nonce-7af98cbf-c6eb-4f69-a94d-e3901b00731f' https://transcend-cdn.com 'unsafe-hashes' 'sha256-oV3jdqk8GO/BUZSwos543OIGzhxD3uMNE23EaxYMEQ=' 'sha256-4tktfVAle+8oijnlFnhze1lbgtFnnDScvcHluccac=' 'sha256-zlqnbDt84zf1iSefLU/ImC54isoprH/MRIVZGskwexk=' 'sha256-47DEQpj8HBSa+/TImW+5JCeuAe+8oijnlFnhze1lbgtFnnDScvcHluccac=' 'sha256-zlqnbDt84zf1iSefLU/ImC54isoprH/MRIVZGskwexk='
```

Evidence:

```
QeRkm5NMPJWZG3hSuFU='sha256-7JyL1A8Kywti3E1sW1I1spFukJsEOqINFJPixVimVbAQ='; style-src-elem 'self' 'nonce-7af98cbf-c6eb-4f69-a94d-e3901b00731f' https://transcend-cdn.com 'unsafe-hashes' 'sha256-oV3jdqk8GO/BUZSwos543OIGzhxD3uMNE23EaxYMEQ=' 'sha256-4tktfVAle+8oijnlFnhze1lbgtFnnDScvcHluccac=' 'sha256-zlqnbDt84zf1iSefLU/ImC54isoprH/MRIVZGskwexk=' 'sha256-47DEQpj8HBSa+/TImW+5JCeuAe+8oijnlFnhze1lbgtFnnDScvcHluccac=' 'sha256-7JyL1A8Kywti3E1sW1I1spFukJsEOqINFJPixVimVbAQ='; style-src-attr 'unsafe-inline'; connect-src 'self' https://unpkg.com/@rive-app/canvas@2.7.6/rive.wasm https://assets.ctfassets.net/ https://start.1password.com https://start.1password.ca https://start.1password.eu https://www.google-analytics.com https://9gnqx00du4.execute-api.us-east-1.amazonaws.com/prod/contact_us https://us.app.unleash-hosted.com https://flow.1passwordservices.com https://telemetry.transcend.io/collect https://browser-intake-datadoghq.com https://sst.1passwordservices.com https://c.6sc.co https://ipv6.6sc.co https://b.6sc.co https://epsilon.6sense.com https://transcend-cdn.com; manifest-src 'self'; font-src 'self'; object-src 'self'; img-src 'self' blob: https://images.ctfassets.net/ https://www.google.com https://www.google-analytics.com https://sst.1passwordservices.com https://cm.g.doubleclick.net https://stats.g.doubleclick.net https://insight.adsrvr.org https://px.mountain.com https://b.6sc.co; child-src https://www.youtube-nocookie.com https://secure.livechatinc.com; frame-src https://www.youtube-nocookie.com https://www.youtube-nocookie.com/embed https://secure.livechatinc.com https://player.vimeo.com https://insight.adsrvr.org https://match.adsrvr.org https://drift.1passwordservices.com https://sync.transcend-cdn.com https://www.figma.com https://app.getreprise.com/; form-action 'self' https://start.1password.com https://flow.1passwordservices.com; frame-ancestors https://*.1passwordservices.com https://*.1password.com https://*.1password.ca https://*.1passwordrd.eu https://main.1pstage.com; report-uri https://csp.1passwordservices.com/report?tags=1pw_prd; report-to csp-endpoint
```


CWE ID: 693
WASC ID: 15
Source: Passive (10055 - CSP)
Alert Reference: 10055-8

Description:

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) Cross Site Scripting (XSS), and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

Content Security Policy (CSP) Header Not Set:

Content Security Policy (CSP) Header Not Set


URL: <http://1password.com/cdn-cgi//email-protection>
Risk:  Medium
Confidence: High
Parameter:
Attack:
Evidence:
CWE ID: 693
WASC ID: 15
Source: Passive (10038 - Content Security Policy (CSP) Header Not Set)
Alert Reference: 10038-1
Input Vector:

Description:

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

HTTP to HTTPS Insecure Transition in Form Post:


HTTP to HTTPS Insecure Transition in Form Post

URL: <http://1password.com/resources/>
Risk:  Medium
Confidence: Medium
Parameter:
Attack:
Evidence: <https://flow.1passwordservices.com/api/v1/form>
CWE ID: 319
WASC ID: 15
Source: Passive (10041 - HTTP to HTTPS Insecure Transition in Form Post)
Input Vector:

Description:

This check looks for insecure HTTP pages that host HTTPS forms. The issue is that an insecure HTTP page can easily be hijacked through MITM and the secure HTTPS form can be replaced or spoofed.

CSP: Notices:

CSP: Notices	
URL:	http://1password.com
Risk:	 Low
Confidence:	High
Parameter:	content-security-policy
Attack:	<pre>default-src 'none'; media-src 'self' https://videos.ctfassets.net.; script-src-elem 'self' 'nonce-0f1296b7-6ec9-435d-b1c8-d6b516885df9' https://transcend-cdn.com/cm/fa619274-3c15-4155-bbec-c0cb75733259/airgap.js https://transcend-cdn.com/cm/fa619274-3c15-4155-bbec-c0cb75733259/ui.js https://transcend-cdn.com/cm/fa619274-3c15-4155-bbec-c0cb75733259/xdi.js 'unsafe-hashes' 'sha256-cdFvGnPvdeavqCupEOX1iKxDb2jmBXXTGmE6AcHOk+c=' 'sha256-yT/s9zf56jX7wyB2f+yhxGo0VBoDnFqMx5qPvh0jvgQ=' 'sha256-TQ9lqihfbMvC+yQs4RAPRBe8No3FB3+MYPxT/OnPn/A=' 'sha256-ep0lyBO1i+WpsX2W3CxFRXjI+Hxg1zdLj+K4nN4Yzdk='; script-src 'self' 'wasm-unsafe-eval' 'nonce-0f1296b7-6ec9-435d-b1c8-d6b516885df9' https://transcend-cdn.com/cm/fa619274-3c15-4155-bbec-c0cb75733259/airgap.js https://transcend-cdn.com/cm/fa619274-3c15-4155-bbec-c0cb75733259/ui.js https://transcend-cdn.com/cm/fa619274-3c15-4155-bbec-c0cb75733259/xdi.js; style-src 'self' 'nonce-0f1296b7-6ec9-435d-b1c8-d6b516885df9' https://transcend-cdn.com 'unsafe-hashes' 'sha256-oV3jdqk8GO/BUZSwos543OIGzhzxD3uMNE23EaxYMEQ=' 'sha256-/4tktfVAle+8ojynlFnhze1lbgwtFnndScvcHlucgqc=' 'sha256-zlqnbDt84zf1iSefLU/lmC54isoprH/MRIVZGskwexk=' 'sha256-47DEQpj8HBSa+/TImW+5JCeuQeRkm5NMpJWZG3hSuFU='</pre>


Evidence:	<pre>fVAle+8ojynlFnhze1lbgwtFnndScvcHlucgqc='sha256-zlqnbDt84zf1iSefLU/lmC54isoprH/MRIVZGskwexk=' 'sha256-47DEQpj8HBSa+/TImW+5JCeuQeRkm5NMpJWZG3hSuFU=' 'sha256-7JyL1A8Kywti3E1sWTTspFukJsEOqINfJPlxVimVbAQ='; style-src-elem 'self' 'nonce-0f1296b7-6ec9-435d-b1c8-d6b516885df9' https://transcend-cdn.com 'unsafe-hashes' 'sha256-oV3jdqk8GO/BUZSwos543OIGzhzxD3uMNE23EaxYMEQ=' 'sha256-/4tktfVAle+8ojynlFnhze1lbgwtFnndScvcHlucgqc=' 'sha256-zlqnbDt84zf1iSefLU/lmC54isoprH/MRIVZGskwexk=' 'sha256-47DEQpj8HBSa+/TImW+5JCeuQeRkm5NMpJWZG3hSuFU=' 'sha256-7JyL1A8Kywti3E1sWTTspFukJsEOqINfJPlxVimVbAQ='; style-src-attr 'unsafe-inline'; connect-src 'self' https://unpkg.com/@rive-app/canvas@2.7.6/rive.wasm https://assets.ctfassets.net.' https://start.1password.com https://start.1password.ca https://start.1password.eu https://www.google-analytics.com https://9gnqx00du4.execute-api.us-east-1.amazonaws.com/prod/contact_us https://us.app.u Nileash-hosted.com https://flow.1passwordservices.com https://telemetry.transcend.io/collect https://browser-intake-datadoghq.com https://sst.1passwordservices.com https://c.6sc.co https://pv6.6sc.co https://b.6sc.co https://epsilon.6sense.com https://transcend-cdn.com; manifest-src 'self'; font-src 'self'; object-src 'self'; img-src 'self' blob: https://images.ctfassets.net.' https://www.google.com https://www.google-analytics.com https://sst.1passwordservices.com https://cm.g.doubleclick.net https://stats.g.doubleclick.net https://insight.adsrvr.org https://px.mountain.com https://b.6sc.co; child-src https://www.youtube-nocookie.com https://secure.livechatinc.com; frame-src https://www.youtube-nocookie.com https://www.youtube-nocookie.com/embed https://secure.livechatinc.com https://player.vimeo.com https://insight.adsrvr.org https://match.adsrvr.org https://drift.1passwordservices.com https://sync-transcend-cdn.com https://www.figma.com https://app.getreprise.com/; form-action 'self' https://start.1password.com https://flow.1passwordservices.com; frame-ancestors https://*.1passwordservices.com https://*.1password.com https://*.1password.ca https://*.1passwordrd.eu https://main.1pstage.com; report-uri https://csp.1passwordservices.com/report?tags=1pw_prd; report-to csp-endpoint</pre>
-----------	---

CWE ID:	693
WASC ID:	15
Source:	Passive (10055 - CSP)
Alert Reference:	10055-3
Input Vector:	


Description:

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) Cross Site Scripting (XSS), and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.


Cookie No HttpOnly Flag:

Cookie No HttpOnly Flag	
URL:	http://1password.com/robots.txt
Risk:	 Low
Confidence:	Medium
Parameter:	unleash-session-id
Attack:	
Evidence:	Set-Cookie: unleash-session-id
CWE ID:	1004
WASC ID:	13
Source:	Passive (10010 - Cookie No HttpOnly Flag)
Input Vector:	
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

Cookie Without Secure Flag:

Cookie Without Secure Flag	
URL:	https://1password.com/
Risk:	 Low
Confidence:	Medium
Parameter:	unleash-session-id
Attack:	
Evidence:	Set-Cookie: unleash-session-id
CWE ID:	614
WASC ID:	13
Source:	Passive (10011 - Cookie Without Secure Flag)
Input Vector:	
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

Cookie without SameSite Attribute:

Cookie without SameSite Attribute	
URL:	http://1password.com/sitemap.xml
Risk:	 Low
Confidence:	Medium
Parameter:	unleash-session-id
Attack:	
Evidence:	Set-Cookie: unleash-session-id
CWE ID:	1275
WASC ID:	13
Source:	Passive (10054 - Cookie without SameSite Attribute)
Alert Reference:	10054-1

Input Vector:


Description:

A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Cross-Domain JavaScript Source File Inclusion:

Cross-Domain JavaScript Source File Inclusion

URL: <https://1password.com/pt/giftcards/>

Risk:  Low

Confidence: Medium

Parameter: <https://transcend-cdn.com/cm/fa619274-3c15-4155-bbec-c0cb75733259/airgap.js>

Attack:

Evidence: `<script data-cfasync=false src=https://transcend-cdn.com/cm/fa619274-3c15-4155-bbec-c0cb75733259/airgap.js></script>`

CWE ID: 829

WASC ID: 15

Source: Passive (10017 - Cross-Domain JavaScript Source File Inclusion)

Input Vector:


Description:

The page includes one or more script files from a third-party domain|

Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s):

Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)

URL: <http://1password.com>

Risk:  Low

Confidence: Medium

Parameter:

Attack:

Evidence: x-powered-by: Next.js

CWE ID: 497

WASC ID: 13

Source: Passive (10037 - Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s))

Input Vector:


Description:

The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.

Timestamp Disclosure - Unix:

Timestamp Disclosure - Unix

URL: <http://1password.com>

Risk:  Low

Confidence: Low

Parameter:

Attack:

Evidence: 1511601750

CWE ID: 497

WASC ID: 13

Source: Passive (10096 - Timestamp Disclosure)

Input Vector:


Description:

A timestamp was disclosed by the application/web server. - Unix

X-Content-Type-Options Header Missing:

X-Content-Type-Options Header Missing

URL: <http://1password.com/robots.txt>

Risk:  Low

Confidence: Medium

Parameter: x-content-type-options

Attack:

Evidence:

CWE ID: 693

WASC ID: 15

Source: Passive (10021 - X-Content-Type-Options Header Missing)

Input Vector:


Description:

The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

Information Disclosure - Sensitive Information in URL:

Information Disclosure - Sensitive Information in URL

URL: http://1password.com/contact-sales/xam?Form_Intention__c&comments&companyName=ZAP&companySize&country&email=zaproxy%40example.com&emailOptIn=on&firstName=ZAP&lastName=ZAP&phone=9999999999&title=ZAP

Risk:  Informational

Confidence: Medium

Parameter: email

Attack:

Evidence: zaproxy@example.com

CWE ID: 598

WASC ID: 13

Source: Passive (10024 - Information Disclosure - Sensitive Information in URL)

Input Vector:


Description:

The request appeared to contain sensitive information leaked in the URL. This can violate PCI and most organizational compliance policies. You can configure the list of strings for this check to add or remove values specific to your environment.

Information Disclosure - Suspicious Comments:

Information Disclosure - Suspicious Comments

URL: <http://1password.com>

Risk:  Informational

Confidence: Low

Parameter:

Attack:

Evidence: Bug

CWE ID: 615

WASC ID: 13

Source: Passive (10027 - Information Disclosure - Suspicious Comments)

Input Vector:


Description:

The response appears to contain suspicious comments which may help an attacker.

Modern Web Application:

Modern Web Application

URL: <http://1password.com>

Risk:  Informational

Confidence: Medium

Parameter:

Attack:

Evidence: `View plans`

CWE ID:

WASC ID:


Source: Passive (10109 - Modern Web Application)

Input Vector:


Description:

The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.


Re-examine Cache-control Directives:

Re-examine Cache-control Directives	
URL:	https://1password.com/pt/sitemap.xml
Risk:	 Informational
Confidence:	Low
Parameter:	cache-control
Attack:	
Evidence:	no-cache
CWE ID:	525
WASC ID:	13
Source:	Passive (10015 - Re-examine Cache-control Directives)
Input Vector:	
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

Retrieved from Cache:

Retrieved from Cache	
URL:	http://1password.com
Risk:	 Informational
Confidence:	Medium
Parameter:	
Attack:	
Evidence:	Age: 0
CWE ID:	
WASC ID:	
Source:	Passive (10050 - Retrieved from Cache)
Alert Reference:	10050-2
Input Vector:	
Description:	The content was retrieved from a shared cache. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the

User Controllable HTML Element Attribute (Potential XSS):

User Controllable HTML Element Attribute (Potential XSS)	
URL:	http://1password.com/pricing/password-manager?currency=usd
Risk:	 Informational
Confidence:	Low
Parameter:	currency
Attack:	
Evidence:	
CWE ID:	20
WASC ID:	20
Source:	Passive (10031 - User Controllable HTML Element Attribute (Potential XSS))
Input Vector:	
Description:	This check looks at user-supplied input in query string parameters and POST data to identify where certain HTML attribute values might be controlled. This provides hot-spot detection for XSS (cross-site scripting) that will require further review by a security analyst to determine exploitability.

The vulnerability assessment using OWASP ZAP successfully identified various web application security flaws in the target site. Remediation steps for each vulnerability were suggested to improve the site's overall security posture.