当資料は重要情報を含むためお取り扱いには
十分ご注意ください。

Confidential

生活協同組合連合会大学生協事業連合 御中

Web アプリケーション
脆弱性診断報告書

プロジェクト名	パイロット版加入 Web
初回診断期間	2023-09-19～09-22、09-25～09-29
再診断	2023-10-19～10-20、10-23～10-24
再々診断	2023-12-21～12-22、12-25～12-27
報告書作成日	2023-12-27
文書管理番号	WCU23100201_03

サービス＆セキュリティ株式会社
株式会社エージェント・スミス

目次

■別添資料

- 診断実施対象一覧.pdf
- 診断対象脆弱性一覧.pdf
  - ➢ 汎用資料です。今回の診断対象機能で診断不要な脆弱性も記載されています。

エグゼクティブサマリー

総評

総合評価	
危険度：中	改修を推奨します

今回の診断では、危険度中の脆弱性が検出されました。改修を推奨いたします。

特に危険度の高い脆弱性

今回の診断では、特に危険度の高い脆弱性の検出はありませんでした。

対策

「検出脆弱性の詳細」の項で詳述しますが、ソースコードの改修や設定の変更を推奨いたします。

実施概要

目的

診断対象の Web アプリケーションに対して、脆弱性の存否を確認します。

診断期間

初回診断：2023 年 9 月 19 日(火)～9 月 22 日(金)、9 月 25 日(月)～9 月 29 日(金)
再診断：2023 年 10 月 19 日(木)～10 月 20 日(金)、10 月 23 日(月)～10 月 24 日(火)
再々診断：2023 年 12 月 21 日(木)～12 月 22 日(金)、12 月 25 日(月)～12 月 27 日(水)

診断対象ドメイン

ドメイン	環境
kanyuweb-test.univcoop.or.jp	ステージング

※診断実施対象の詳細については、別添資料「診断実施対象一覧.xlsx」をご覧ください。

診断手法

1) 下記ツールによるスキャン
   - Burp Suite Professional (PortSwigger 社) バージョン 2023.11.1.3
2) エンジニアの手作業による擬似攻撃

診断対象脆弱性一覧

※診断対象の脆弱性一覧詳細については、別添資料「診断対象脆弱性一覧.pdf」をご覧ください。

診断結果

検出一覧

脆弱性	危険度	検出数
SQL インジェクションの可能性	中	1 URL
Cookie へのセキュリティ属性の未設定	低	1 ホスト
オープンリダイレクト	情報	1 URL
プライベート IP アドレスの開示	情報	1 URL

危険度別脆弱性一覧

危険度 深刻 の脆弱性
危険度 深刻 の脆弱性は検出されていません。

危険度 高 の脆弱性
危険度 高 の脆弱性は検出されていません。

危険度 中 の脆弱性	
3-1	**SQL インジェクションの可能性** https://kanyuweb-test.univcoop.or.jp/api/check-mail

危険度 低 の脆弱性	
4-1	**Cookie へのセキュリティ属性の未設定** kanyuweb-test.univcoop.or.jp

「情報」の報告事項	
5-1	**オープンリダイレクト** https://kanyuweb-test.univcoop.or.jp/110501/confirm-url
5-2	**プライベート IP アドレスの開示** https://kanyuweb-test.univcoop.or.jp/110501/confirm-url

危険度について

危険度は、下のマトリックスを基本として「深刻」から「情報」の 5 段階で判断しています。

		悪用のための条件・利用者の該当範囲			
		実現困難な条件	特異な条件・ 利用者の一部が該当	特定の条件・ 利用者の過半が該当	条件無し
攻撃成功時の被害	甚大	中	高	高	深刻
	大きい	低	中	高 または 中	深刻 または 高
	小さい	低 または 情報	低	低	中 または 低
	無し	情報			

深刻	悪用にあたっての条件も無く、単独で、Web サービス全体に重大な悪影響を及ぼす可能性があります。早急な対応が必須です。
高	単独で、Web サービスに重大な悪影響を及ぼす可能性があります。早急な対応が必要と判断されます。
中	下記いずれかの脆弱性が該当します。対処を推奨します。 1）特定の条件下で Web サービスに悪影響を及ぼす 2）他の脆弱性による攻撃の成功可能性を高めてシステムに重大な悪影響を及ぼす可能性がある 3）実施条件は特に無く、何らかの被害を発生させることが可能
低	特定の条件が成立した場合、または、他の脆弱性と組み合わせることにより Web サービスに悪影響を及ぼす可能性があります。 または単独で Web サービスに限定的な影響を与える可能性があります。Web サービスの信頼性を向上するために可能な限り対応を推奨します。
情報	現状ではセキュリティ上の脅威となる可能性が極めて低いか可能性がない事項ですが、今後のサービスの追加や変更、想定される利用環境に変化がある場合、または新たな脆弱性の検出があった場合には、脅威となり得る可能性があります。念のためにご報告する事項です。

検出脆弱性の詳細

1. 危険度 深刻 の脆弱性

危険度 深刻 の脆弱性は検出されませんでした。

2. 危険度 高 の脆弱性

危険度 高 の脆弱性は検出されませんでした。

3. 危険度 中 の脆弱性

3-1

脆弱性名	SQL インジェクションの可能性
危険度	中
解説	SQL インジェクションは、ユーザ由来の入力値が SQL 文の一部として誤って解釈され、不正な SQL 文を実行される脆弱性です。 攻撃者に本脆弱性を悪用され、データベースを閲覧、改ざん等される可能性があります。 発生原因は、SQL 文の組み立て方法に不備があるためです。
検出箇所	<基本情報入力（保護者情報入力）>-<「登録済みメールアドレス/生年月日かチェックする」押下> https://kanyuweb-test.univcoop.or.jp/api/check-mail email 変数値
確認方法	「email 変数値」に 2 種類の攻撃パターンを設定した HTTP リクエストを送信した結果、片方のレスポンスにのみエラーが発生しました。 「'」は SQL で文字列の開始・終了を表す記号であるため、サーバ側で攻撃パターンを SQL 文の一部として解釈し、「'」の数によって SQL の構文にエラーが発生している可能性があります。

攻撃パターン
1） '(奇数個)
2） ''(偶数個)
URL
https://kanyuweb-test.univcoop.or.jp/api/check-mail
HTTP リクエスト 1
GET /api/check-mail?email=ssktest19@e-gate.ssk-kan.co.jp'&birthdate=2005-02-19&coopuser=100000000 HTTP/2 Host: kanyuweb-test.univcoop.or.jp Cookie: ApplicationGatewayAffinityCORS=cd983013f8ae7dafb0d2782308f3e4f0; ApplicationGatewayAffinity=cd983013f8ae7dafb0d2782308f3e4f0; _ga=GA1.1.2057003544.1703554000; membership_token=eyJ...(省略)...iJ9; XSRF-TOKEN=eyJ...(省略)...%3D; unitz_kanyuweb_session=eyJ...(省略)...%3D; _ga_WY9XY066W9=GS1.1.1703554000.1.1.1703554684.0.0.0 Sec-Ch-Ua: "Not_A Brand";v="8", "Chromium";v="120", "Google

```
Chrome";v="120"
Accept: */*
X-Requested-With: XMLHttpRequest
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://kanyuweb-test.univcoop.or.jp/110501/entry-
student?membership-id=bb7db119-8fa3-ee11-be36-6045bd6852f9
Accept-Encoding: gzip, deflate, br
Accept-Language: ja,en-US;q=0.9,en;q=0.8
```

HTTP レスポンス 1

```
HTTP/2 500 Internal Server Error
Date: Tue, 26 Dec 2023 01:39:51 GMT
Content-Type: application/json
Cache-Control: no-cache, private
Server: nginx/1.18.0 (Ubuntu)
Strict-Transport-Security: max-age=31536000; includeSubDomains
Vary: Origin
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
X-Ratelimit-Limit: 20000
X-Ratelimit-Remaining: 19990

{
   "message": "Server Error"
}
```

HTTP リクエスト 2

```
GET /api/check-mail?email=ssktest19@e-gate.ssk-
kan.co.jp''&birthdate=2005-02-19&coopuser=100000000 HTTP/2
Host: kanyuweb-test.univcoop.or.jp
Cookie: ApplicationGatewayAffinityCORS=cd983013f8ae7dafb0d2782308f3e4f0;
ApplicationGatewayAffinity=cd983013f8ae7dafb0d2782308f3e4f0;
_ga=GA1.1.2057003544.1703554000; membership_token=eyJ...(省略)...iJ9;
XSRF-TOKEN=eyJ...(省略)...%3D; unitz_kanyuweb_session=eyJ...(省略)...%3D;
_ga_WY9XY066W9=GS1.1.1703554000.1.1.1703554684.0.0.0
Sec-Ch-Ua: "Not_A Brand";v="8", "Chromium";v="120", "Google
Chrome";v="120"
Accept: */*
X-Requested-With: XMLHttpRequest
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://kanyuweb-test.univcoop.or.jp/110501/entry-
student?membership-id=bb7db119-8fa3-ee11-be36-6045bd6852f9
Accept-Encoding: gzip, deflate, br
Accept-Language: ja,en-US;q=0.9,en;q=0.8
```

HTTP レスポンス 2

	HTTP/2 200 OK Date: Tue, 26 Dec 2023 01:40:11 GMT Content-Type: text/html; charset=UTF-8 Cache-Control: no-cache, private Server: nginx/1.18.0 (Ubuntu) Strict-Transport-Security: max-age=31536000; includeSubDomains Vary: Origin X-Content-Type-Options: nosniff X-Frame-Options: DENY X-Ratelimit-Limit: 20000 X-Ratelimit-Remaining: 19988 0
対処方法	SQL 文の組み立てはプリペアドステートメントを使用してください。 あるいは、SQL 文の組み立てを文字列連結により行う場合、適切にエスケープ処理をしてください。 参考 URL：安全な SQL の呼び出し方 https://www.ipa.go.jp/security/vuln/websecurity/ug65p900000196e2-att/000017320.pdf

4. 危険度 低 の脆弱性

4-1

脆弱性名	Cookie へのセキュリティ属性の未設定
危険度	低
解説	HttpOnly 属性が設定されていない Cookie 変数が検出されました。 HttpOnly 属性が設定されている場合、JavaScript による Cookie 操作が禁止されます。 これにより、第三者によって悪意のある JavaScript が挿入された場合にも Cookie 値の改ざんや漏えいを防ぐことが可能です。
検出箇所	kanyuweb-test.univcoop.or.jp XSRF-TOKEN Cookie 変数
確認方法	HTTP プロキシ等を利用し、Cookie 変数が設定されるレスポンスを捕捉します。 Set-Cookie レスポンスヘッダに HttpOnly 属性が設定されていないことが確認できます。 URL https://kanyuweb-test.univcoop.or.jp/110501/entry-student HTTP レスポンス HTTP/2 200 OK Date: Thu, 21 Dec 2023 04:48:56 GMT Content-Type: text/html; charset=UTF-8 Cache-Control: no-cache, private Server: nginx/1.18.0 (Ubuntu) Set-Cookie: XSRF-TOKEN=eyJ...(省略)...%3D; expires=Thu, 21 Dec 2023 06:48:56 GMT; Max-Age=7200; path=/; secure; samesite=lax (以下省略)
対処方法	攻撃者から保護する必要がある Cookie 変数に対して、HttpOnly 属性を有効化してください。

5. 「情報」の報告事項

5-1

脆弱性名	オープンリダイレクト
危険度	情報
解説	ユーザから送信された値がリダイレクト先として使用されています。 攻撃者はこの値を改ざんして、被害者を任意のホストへ誘導させるフィッシング詐欺等に悪用する可能性があります。 本脆弱性が発生した原因は、ユーザ由来の入力値をそのままリダイレクト先ドメインとして使用しているためです。 ただし、検出箇所は第三者による改ざんは大変困難であるため、「情報」の報告事項としています。
検出箇所	<URL チェック待機>-<「確認 URL を再送する」押下> https://kanyuweb-test.univcoop.or.jp/110501/confirm-url Referer ヘッダ値
確認方法	下記は、攻撃用 HTTP リクエストを送信した結果の一例です。 検出箇所の URL 以外で同様の仕組みを利用している場合は、それらも対象です。 Referer ヘッダ値の攻撃パターンが遷移先として出力されていることをご確認ください。

攻撃パターン

```
https://example.com
```

URL

```
https://kanyuweb-test.univcoop.or.jp/110501/confirm-url
```

HTTP リクエスト

```
POST /110501/confirm-url?membership-id=7c8835da-99a3-ee11-be36-
6045bd676150 HTTP/2
Host: a-test.univcoop.or.jp
Cookie: ApplicationGatewayAffinityCORS=cd983(省略)
Content-Length: 47
Cache-Control: max-age=0
Sec-Ch-Ua: "Not_A Brand";v="8", "Chromium";v="120", "Google
Chrome";v="120"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://kanyuweb-test.univcoop.or.jp
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w
ebp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://example.com
Accept-Encoding: gzip, deflate, br
Accept-Language: ja,en-US;q=0.9,en;q=0.8
```

	_token=AeoVu7lVKvrVCVBtEhjXSc4AmG7axRr64shjIMmE HTTP レスポンス HTTP/2 302 Found Date: Tue, 26 Dec 2023 07:13:45 GMT Content-Type: text/html; charset=UTF-8 Cache-Control: no-cache, private Location: https://example.com Server: nginx/1.18.0 (Ubuntu) Set-Cookie: XSRF- TOKEN=eyJpdiI6Ikp4Y2VZQ09RUGFpMElmVCt5bFFCV3c9PSIsInZhbHVlIjoiWWZKYTRHbk U2MWdXMkZua1E3MEI1S0E1VHIveHpyV3FEVXR3UmZSM3VvdXZwYllISlV2TG0xNlpFUWhBNn NFNlNrUEw4TVlUQzl6QjR6TUtmMEZlSUNuNGQ2Y2VSY0JRMmtuRjFaZE02S3R3cDdHeTFCSE MrN3N5Tk1LeG5lMksiLCJtYWMiOiIzYTgxODI2NjhiMjdhYWJlNjdhNzRiNTMyMjlkMDJmYj JjYWI2MDhkMzUxYWZkZTI1OTQxYzRmOTBiODlkN2VkIiwidGFnIjoiIn0%3D; expires=Tue, 26 Dec 2023 09:13:45 GMT; Max-Age=7200; path=/; secure; samesite=lax Set-Cookie: unitz_kanyuweb_session=eyJpdiI6Ikp4MnVLQ2VvNU8yTWl2S1FmVVplZ2c9PSIsInZhb HVlIjoiK2JMVXJjNExXL2FMY2tXbGFpQlBYa1BFTm1aNmdhb3U1U3Vub2RIeUFXWWpOUE1QQ TBKaUZZeWkveGdzYm40YzA4bUxWU1ROYXZnZjJ6blZJZDRJajVrMThDblhTV1EyMVBSbVpvQ WZkdjNDL3RiajN0UVlQZjJ1Y0Q5RVU5UUgiLCJtYWMiOiI0MDBjYjM4Nzk5ZDZkY2MzZjdhO DA0MjY3NjIyNmM3Y2M0YWVmMTA5MTBhZWE4NTYyOTcyYTlmNzg4MDRlMzk0IiwidGFnIjoiI n0%3D; expires=Tue, 26 Dec 2023 09:13:45 GMT; Max-Age=7200; path=/; secure; httponly; samesite=lax Strict-Transport-Security: max-age=31536000; includeSubDomains X-Content-Type-Options: nosniff X-Frame-Options: DENY <!DOCTYPE html> <html> <head> <meta charset="UTF-8" /> <meta http-equiv="refresh" content="0;url='https://example.com'" /> <title>Redirecting to https://example.com</title> </head> <body> Redirecting to https://example.com. </body> </html>
対処方法	ヘッダ値をそのままリダイレクト先に使用しないように処理を変更してください。 もしヘッダ値を使用する必要がある場合は、値の検証処理を追加し、リダイレクト先を制御してください。

5-2

脆弱性名	プライベート IP アドレスの開示
危険度	情報

解説	HTTP レスポンスにプライベート IP アドレスが出力されています。 攻撃者はプライベート IP アドレスの情報から内部ネットワーク構成などを推測し、より的確な攻撃を仕掛けてくる可能性があります。 本出力が仕様によるものかをご確認のうえ、対処することを推奨します。
検出箇所	<URL チェック待機>-<「確認 URL を再送する」押下> https://kanyuweb-test.univcoop.or.jp/110501/confirm-url
確認方法	検出箇所へのアクセスの際、「Referer ヘッダ値」を空白にして送信すると、リダイレクト先 URL にプライベート IP アドレスが出力されます。

URL

```
https://kanyuweb-test.univcoop.or.jp/110501/confirm-url
```

HTTP リクエスト

```
POST /110501/confirm-url?membership-id=7c8835da-99a3-ee11-be36-
6045bd676150 HTTP/2
Host: kanyuweb-test.univcoop.or.jp
Cookie: ApplicationGatewayAffinityCORS=cd9(省略)
Content-Length: 47
Cache-Control: max-age=0
Sec-Ch-Ua: "Not_A Brand";v="8", "Chromium";v="120", "Google
Chrome";v="120"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://kanyuweb-test.univcoop.or.jp
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w
ebp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer:
Accept-Encoding: gzip, deflate, br
Accept-Language: ja,en-US;q=0.9,en;q=0.8

_token=AeoVu7lVKvrVCVBtEhjXSc4AmG7axRr64shjIMmE
```

HTTP レスポンス

```
HTTP/2 302 Found
Date: Tue, 26 Dec 2023 07:21:09 GMT
Content-Type: text/html; charset=UTF-8
Cache-Control: no-cache, private
Location: http://10.5.4.4/110501/entry-confirmation?membership-
id=7c8835da-99a3-ee11-be36-6045bd676150
Server: nginx/1.18.0 (Ubuntu)
Set-Cookie: XSRF-
TOKEN=eyJpdiI6InIvZUNtOEt4RDVrU3U4eTNmT3lpM0E9PSIsInZhbHVlIjoiYnlPOHV0bX
VaRzdoN1ZWVUtsUU12ZkdMN2JUdW02dE5NNDZETytxbWNpV2VnY2h3Z3F6WS9YMHRuSjhFdH
oxMFZvTzZCNEJPUXpRd3Y1akt1QXMvSWVrcDRRLzhHSWFwVnNYRWpXcWhnaEdkVjIxV0xOOF
FJa0FZTzNDekZidkMiLCJtYWMiOiI0NzIxOWFhZTRiYThiNTZkMDhlZWI5YmE1ZTE1Y2M1MW
```

	UxMjM2YTFkZmExZDFkZDU1NDQ1ZDMxNzY0NDE0NzgzIiwidGFnIjoiIn0%3D; expires=Tue, 26 Dec 2023 09:21:09 GMT; Max-Age=7200; path=/; secure; samesite=lax Set-Cookie: unitz_kanyuweb_session=eyJpdiI6InMvSWNkSmJxNGw4d0srNXZ5Kzl5Vmc9PSIsInZhb HVlIjoiVGFWaHBOVHA4eldsTHZ1a0xJaVhUaEV4cHVyUm40QlBnK0pvNnhuZVdieHNLd01nR Ux3VW8yUFFZVStqOVNreGNVMndKcVo4RzlLQ2ZvM2l2Q3ZuUmVjWTRFcEFCV3B2dWE0RXc3a 1dmQlc3SU5oUE13bmovdmpQdFJVWkZIU1EiLCJtYWMiOiI5NGMyNTllNGUxMWQwYmZiMGYxN mI1Y2M3NWUwYmYwZThhOGM3MGI0NTNiYWRhYjdmNjkwMTQxNmRhYTkwOTMxIiwidGFnIjoiI n0%3D; expires=Tue, 26 Dec 2023 09:21:09 GMT; Max-Age=7200; path=/; secure; httponly; samesite=lax Strict-Transport-Security: max-age=31536000; includeSubDomains X-Content-Type-Options: nosniff X-Frame-Options: DENY <!DOCTYPE html> <html> <head> <meta charset="UTF-8" /> <meta http-equiv="refresh" content="0;url='http://10.5.4.4/110501/entry-confirmation?membership- id=7c8835da-99a3-ee11-be36-6045bd676150'" /> <title>Redirecting to http://10.5.4.4/110501/entry- confirmation?membership-id=7c8835da-99a3-ee11-be36-6045bd676150</title> </head> <body> Redirecting to http://10.5.4.4/110501/entry-confirmation?membership- id=7c8835da-99a3-ee11-be36-6045bd676150. </body> </html>
対処方法	プライベート IP アドレスを出力しないことを推奨します。

（報告書　終わり）