웹 애플리케이션 보고서

이 보고서는 웹 애플리케이션에 대한 중요 보안 정보를 포함하고 있습니다.

보안 보고서

이 보고서는 HCL AppScan Standard에서 작성하였습니다. 10.4.0
스캔 시작: 2024-12-31 오전 11:56:33

목차

애플리케이션 데이터

- 쿠키
- JavaScript
- 매개변수
- 주석
- 방문한 URL
- 실패한 요청

소개

이 보고서에는 HCL AppScan Standard가 수행한 웹 애플리케이션 보안 스캔의 결과가 포함되어 있습니다.

중간 심각도 문제:	1
낮은 심각도 문제:	3
정보용 심각도 문제:	3
이 보고서에 포함된 총 보안 문제:	7
이 스캔에서 발견된 총 보안 문제:	7

일반 정보

스캔 파일 이름:	http@proton.snu.ac.kr+5000
스캔 시작:	2024-12-31 오전 11:56:33
테스트 정책:	Default(수정됨)
CVSS 버전:	3.1
테스트 최적화 레벨:	고속

호스트	proton.snu.ac.kr
포트	5000
운영 체제:	알 수 없음
웹 서버:	알 수 없음
애플리케이션 서버:	모든

로그인 설정

로그인 메소드:	레코드된 로그인
동시 로그인:	사용
세션 내 발견:	사용
세션 내 패턴:	
추적/세션 ID 쿠키:	
추적/세션 ID 매개변수:	
로그인 순서:	

요약

문제 유형 7

TOC

	문제 유형	문제 수
중	안전하지 않거나 올바르지 않거나 누락된 SameSite 속성을 갖는 쿠키	1
하	"Content-Security-Policy" 헤더의 누락되었거나 안전하지 않은 "Script-Src" 또는 "Default-src" 정책	1
하	"Content-Security-Policy"의 누락되었거나 안전하지 않은 "Style-src" 또는 "Default-src" 정책	1
하	암호화 누락	1
정	이메일 주소 패턴 발견	1
정	제한적이지 않은 SameSite 속성을 갖는 쿠키	1
정	클라이언트측(JavaScript) 쿠키 참조	1

취약한 URL 2

TOC

	URL	문제 수
중	http://proton.snu.ac.kr:5000/	5
정	http://proton.snu.ac.kr:5000/static/js/main.10664c35.js	2

수정 권장사항 5

TOC

	조치방안 태스크	문제 수
중	SameSite 쿠키 속성을 권장 값으로 구성하기 위한 가능한 솔루션을 검토하십시오	2
하	보안 정책을 사용하여 "Content-Security-Policy" 헤더를 사용하도록 서버를 구성하십시오.	2
하	웹 사이트에서 이메일 주소를 제거하십시오.	1
하	클라이언트 측으로부터 비즈니스와 보안 로직을 제거하십시오.	1
하	통신이 암호화되도록 TLS/SSL을 구성하십시오.	1

보안 위험 6

TOC

	위험	문제 수
중	쿠키를 자사 또는 Same Site 컨텍스트로 제한하여 쿠키 정보 유출을 방지하십시오. CSRF 방지 토큰과 같은 추가적인 보호가 적용되지 않을 경우 공격이 CSRF(Cross-Site-Request-Forgery) 공격으로 이어질 수 있습니다.	1
하	사용자 이름, 비밀번호, 머신 이름 및/또는 민감한 파일 위치 등과 같이 웹 애플리케이션에 대한 민감한 정보를 모으는 것이 가능합니다.	3
하	속기 쉬운 사용자를 설득해서 사용자 이름, 비밀번호, 신용카드 번호, 주민등록 번호와 같은 민감한 정보를 제공하도록 하는 것이 가능합니다.	2
하	암호화 되지 않은 주민등록 번호, 신용카드 번호 등과 같이 민감한 데이터를 빼내는 것이 가능합니다.	1
정	쿠키를 자사 또는 Same Site 컨텍스트로 제한하여(Strict) 쿠키 정보 유출을 방지하십시오.	1
정	이러한 공격에 대한 최악의 시나리오는 컨텍스트와 클라이언트측에서 작성된 쿠키의 역할에 달려있습니다.	1

원인 8

TOC

	원인	문제 수
중	올바르지 않거나 안전하지 않거나 누락된 SameSite 속성을 갖는 민감한 쿠키	1
하	안전하지 않은 웹 애플리케이션 프로그래밍 또는 구성	1
하	안전하지 않은 웹 애플리케이션 프로그래밍 또는 환경 설정입니다	1
하	애플리케이션이 민감한 정보를 교환하는 데 TLS/SSL 등의 보안 채널을 사용하지 않습니다.	1
하	네트워크 트래픽에 대한 액세스 권한이 있는 공격자는 연결을 통해 패킷을 도청할 수 있습니다. 이 공격은 기술적으로 어렵지 않지만 네트워크에서 민감한 데이터가 이동하는 지점에 대한 물리적 액세스가 필요합니다.	1
정	안전하지 않은 웹 애플리케이션 프로그래밍 또는 환경 설정입니다.	1
정	제한적이지 않은 SameSite 속성 및 플래그를 갖는 민감한 쿠키	1
정	클라이언트 측에 쿠키가 작성됩니다.	1

WASC 위협 분류

TOC

위협	문제 수
올바르지 않은 서버 구성	2
정보 노출	5

문제 유형으로 정렬된 문제

중 안전하지 않거나 올바르지 않거나 누락된 SameSite 속성을 갖는 쿠키 1 TOC

문제 1 / 1 TOC

안전하지 않거나 올바르지 않거나 누락된 SameSite 속성을 갖는 쿠키

심각도:	중
CVSS 점수:	4.7
URL:	http://proton.snu.ac.kr:5000/
엔티티:	key (Cookie)
위험:	쿠키를 자사 또는 Same Site 컨텍스트로 제한하여 쿠키 정보 유출을 방지하십시오. CSRF 방지 토큰과 같은 추가적인 보호가 적용되지 않을 경우 공격이 CSRF(Cross-Site-Request-Forgery) 공격으로 이어질 수 있습니다.
원인:	올바르지 않거나 안전하지 않거나 누락된 SameSite 속성을 갖는 민감한 쿠키
수정사항:	SameSite 쿠키 속성을 권장 값으로 구성하기 위한 가능한 솔루션을 검토하십시오

이유: 응답에 안전하지 않거나 올바르지 않거나 누락된 SameSite 속성을 갖는 민감한 쿠키가 포함되어 있습니다. 이로 인해 쿠키 정보가 유출될 수 있으며, 추가적인 보호가 적용되지 않을 경우 CSRF(Cross-Site-Request-Forgery) 공격으로 이어질 수 있습니다.

테스트 요청 및 응답:

```
GET / HTTP/1.1
Host: proton.snu.ac.kr:5000
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36
Accept:
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
Accept-Language: en-US
Connection: keep-alive
Content-Length: 0


HTTP/1.1 200 OK
Content-Disposition: inline; filename=index.html
Content-Type: text/html; charset=utf-8
Content-Length: 604
Last-Modified: Tue, 31 Dec 2024 02:30:47 GMT
Cache-Control: no-store
ETag: "1735612247.0344641-604-2322601339"
Date: Tue, 31 Dec 2024 02:59:57 GMT
X-Content-Type-Options: nosniff
Content-Security-Policy: default-src 'self'; script-src 'self'; style-src 'self' 'unsafe-inline'; object-src 'none';
Referrer-Policy: strict-origin-when-cross-origin
X-Frame-Options: DENY
X-XSS-Protection: 1; mode=block
Access-Control-Allow-Origin: https://trusted-domain.com
```

```
Set-Cookie: key=value; Expires=Tue, 31 Dec 2024 03:59:57 GMT; Max-Age=3600; Secure; HttpOnly; Path=/; SameSite=Lax

<!doctype html><html lang="en"><head><meta charset="utf-8"/><link rel="icon" href="/favicon.ico"/><meta name="viewport"
content="width=device-width,initial-scale=1"/><meta name="theme-color" content="#000000"/><meta name="description"
content="Web site created using create-react-app"/><link rel="apple-touch-icon" href="/logo192.png"/><link rel="manifest"
href="/manifest.json"/><title>7DT ToO Request</title><script defer="defer" src="/static/js/main.10664c35.js"></script><link
href="/static/css/main.2e7f4582.css" rel="stylesheet"></head><body><noscript></noscript><div id="root"></div></body></html>
```

하 "Content-Security-Policy" 헤더의 누락되었거나 안전하지 않은 "Script-Src" 또는 "Default-src" 정책 1 TOC

문제 1 / 1 TOC

"Content-Security-Policy" 헤더의 누락되었거나 안전하지 않은 "Script-Src" 또는 "Default-src" 정책

심각도:	하
CVSS 점수:	3.7
URL:	http://proton.snu.ac.kr:5000/
엔티티:	proton.snu.ac.kr (Page)
위험:	사용자 이름, 비밀번호, 머신 이름 및/또는 민감한 파일 위치 등과 같이 웹 애플리케이션에 대한 민감한 정보를 모으는 것이 가능합니다. 속기 쉬운 사용자를 설득해서 사용자 이름, 비밀번호, 신용카드 번호, 주민등록 번호와 같은 민감한 정보를 제공하도록 하는 것이 가능합니다.
원인:	안전하지 않은 웹 애플리케이션 프로그래밍 또는 구성
수정사항:	보안 정책을 사용하여 "Content-Security-Policy" 헤더를 사용하도록 서버를 구성하십시오.

이유: AppScan에서 Content-Security-Policy 응답 헤더가 누락되었거나 안전하지 않은 정책을 포함하고 있음을 발견했습니다. 따라서 다양한 크로스 사이트 인젝션 공격에 더 많이 노출될 수 있습니다.

테스트 요청 및 응답:

```
GET / HTTP/1.1
Host: proton.snu.ac.kr:5000
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36
Accept:
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
Accept-Language: en-US
Connection: keep-alive
Content-Length: 0


HTTP/1.1 200 OK
Content-Disposition: inline; filename=index.html
Content-Type: text/html; charset=utf-8
Content-Length: 604
Last-Modified: Tue, 31 Dec 2024 02:30:47 GMT
Cache-Control: no-store
ETag: "1735612247.0344641-604-2322601339"
Date: Tue, 31 Dec 2024 03:01:06 GMT
X-Content-Type-Options: nosniff
Content-Security-Policy: default-src 'self'; script-src 'self'; style-src 'self' 'unsafe-inline'; object-src 'none';
Referrer-Policy: strict-origin-when-cross-origin
X-Frame-Options: DENY
X-XSS-Protection: 1; mode=block
Access-Control-Allow-Origin: https://trusted-domain.com
Set-Cookie: key=value; Expires=Tue, 31 Dec 2024 04:01:06 GMT; Max-Age=3600; Secure; HttpOnly; Path=/; SameSite=Lax

<!doctype html><html lang="en"><head><meta charset="utf-8"/><link rel="icon" href="/favicon.ico"/><meta name="viewport"
content="width=device-width,initial-scale=1"/><meta name="theme-color" content="#000000"/><meta name="description"
content="Web site created using create-react-app"/><link rel="apple-touch-icon" href="/logo192.png"/><link rel="manifest"
href="/manifest.json"/><title>7DT ToO Request</title><script defer="defer" src="/static/js/main.10664c35.js"></script><link
href="/static/css/main.2e7f4582.css" rel="stylesheet"></head><body><noscript></noscript><div id="root"></div></body></html>
```

하 "Content-Security-Policy"의 누락되었거나 안전하지 않은 "Style-src" 또는 "Default-src" 정책 1 TOC

문제 1 / 1 TOC

"Content-Security-Policy"의 누락되었거나 안전하지 않은 "Style-src" 또는 "Default-src" 정책

심각도:	하
CVSS 점수:	3.7
URL:	http://proton.snu.ac.kr:5000/
엔티티:	proton.snu.ac.kr (Page)
위험:	사용자 이름, 비밀번호, 머신 이름 및/또는 민감한 파일 위치 등과 같이 웹 애플리케이션에 대한 민감한 정보를 모으는 것이 가능합니다. 속기 쉬운 사용자를 설득해서 사용자 이름, 비밀번호, 신용카드 번호, 주민등록 번호와 같은 민감한 정보를 제공하도록 하는 것이 가능합니다.
원인:	안전하지 않은 웹 애플리케이션 프로그래밍 또는 환경 설정입니다
수정사항:	보안 정책을 사용하여 "Content-Security-Policy" 헤더를 사용하도록 서버를 구성하십시오.

이유: AppScan에서 Content-Security-Policy 응답 헤더가 누락되었거나 안전하지 않은 정책을 포함하고 있음을 발견했습니다. 따라서 다양한 크로스 사이트 인젝션 공격에 더 많이 노출될 수 있습니다.

테스트 요청 및 응답:

```
GET / HTTP/1.1
Host: proton.snu.ac.kr:5000
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36
Accept:
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
Accept-Language: en-US
Connection: keep-alive
Content-Length: 0


HTTP/1.1 200 OK
Content-Disposition: inline; filename=index.html
Content-Type: text/html; charset=utf-8
Content-Length: 604
Last-Modified: Tue, 31 Dec 2024 02:30:47 GMT
Cache-Control: no-store
ETag: "1735612247.0344641-604-2322601339"
Date: Tue, 31 Dec 2024 03:01:06 GMT
X-Content-Type-Options: nosniff
Content-Security-Policy: default-src 'self'; script-src 'self'; style-src 'self' 'unsafe-inline'; object-src 'none';
Referrer-Policy: strict-origin-when-cross-origin
X-Frame-Options: DENY
X-XSS-Protection: 1; mode=block
Access-Control-Allow-Origin: https://trusted-domain.com
Set-Cookie: key=value; Expires=Tue, 31 Dec 2024 04:01:06 GMT; Max-Age=3600; Secure; HttpOnly; Path=/; SameSite=Lax

<!doctype html><html lang="en"><head><meta charset="utf-8"/><link rel="icon" href="/favicon.ico"/><meta name="viewport"
content="width=device-width,initial-scale=1"/><meta name="theme-color" content="#000000"/><meta name="description"
content="Web site created using create-react-app"/><link rel="apple-touch-icon" href="/logo192.png"/><link rel="manifest"
href="/manifest.json"/><title>7DT ToO Request</title><script defer="defer" src="/static/js/main.10664c35.js"></script><link
href="/static/css/main.2e7f4582.css" rel="stylesheet"></head><body><noscript></noscript><div id="root"></div></body></html>
```

문제 1 / 1

TOC

암호화 누락

심각도:	하
CVSS 점수:	3.7
URL:	http://proton.snu.ac.kr:5000/
엔티티:	proton.snu.ac.kr (Page)
위험:	암호화 되지 않은 주민등록 번호, 신용카드 번호 등과 같이 민감한 데이터를 빼내는 것이 가능합니다.
원인:	애플리케이션이 민감한 정보를 교환하는 데 TLS/SSL 등의 보안 채널을 사용하지 않습니다. 네트워크 트래픽에 대한 액세스 권한이 있는 공격자는 연결을 통해 패킷을 도청할 수 있습니다. 이 공격은 기술적으로 어렵지 않지만 네트워크에서 민감한 데이터가 이동하는 지점에 대한 물리적 액세스가 필요합니다.
수정사항:	통신이 암호화되도록 TLS/SSL을 구성하십시오.

이유: 테스트 응답에 안전하지 않은 HTTP 스킴이 있습니다.
테스트 요청 및 응답:

```
GET / HTTP/1.1
Host: proton.snu.ac.kr:5000
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36
Accept:
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
Accept-Language: en-US
Connection: keep-alive
Content-Length: 0


HTTP/1.1 200 OK
Content-Disposition: inline; filename=index.html
Content-Type: text/html; charset=utf-8
Content-Length: 604
Last-Modified: Tue, 31 Dec 2024 02:30:47 GMT
Cache-Control: no-store
ETag: "1735612247.0344641-604-2322601339"
Date: Tue, 31 Dec 2024 02:59:33 GMT
X-Content-Type-Options: nosniff
Content-Security-Policy: default-src 'self'; script-src 'self'; style-src 'self' 'unsafe-inline'; object-src 'none';
Referrer-Policy: strict-origin-when-cross-origin
X-Frame-Options: DENY
X-XSS-Protection: 1; mode=block
Access-Control-Allow-Origin: https://trusted-domain.com
Set-Cookie: key=value; Expires=Tue, 31 Dec 2024 03:59:33 GMT; Max-Age=3600; Secure; HttpOnly; Path=/; SameSite=Lax

<!doctype html><html lang="en"><head><meta charset="utf-8"/><link rel="icon" href="/favicon.ico"/><meta name="viewport"
content="width=device-width,initial-scale=1"/><meta name="theme-color" content="#000000"/><meta name="description"
content="Web site created using create-react-app"/><link rel="apple-touch-icon" href="/logo192.png"/><link rel="manifest"
href="/manifest.json"/><title>7DT ToO Request</title><script defer="defer" src="/static/js/main.10664c35.js"></script><link
href="/static/css/main.2e7f4582.css" rel="stylesheet"></head><body><noscript></noscript><div id="root"></div></body></html>
```

정 이메일 주소 패턴 발견 1 TOC

문제 1 / 1 TOC

이메일 주소 패턴 발견

심각도:	정보용
CVSS 점수:	0.0
URL:	http://proton.snu.ac.kr:5000/static/js/main.10664c35.js
엔티티:	main.10664c35.js (Page)
위험:	사용자 이름, 비밀번호, 머신 이름 및/또는 민감한 파일 위치 등과 같이 웹 애플리케이션에 대한 민감한 정보를 모으는 것이 가능합니다.
원인:	안전하지 않은 웹 애플리케이션 프로그래밍 또는 환경 설정입니다.
수정사항:	웹 사이트에서 이메일 주소를 제거하십시오.

이유: 응답에는 개인용 이메일 주소가 포함되어 있습니다.
테스트 요청 및 응답:

```
GET /static/js/main.10664c35.js HTTP/1.1
Host: proton.snu.ac.kr:5000
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36
Accept: */*
Accept-Language: en-US
Referer: http://proton.snu.ac.kr:5000/
Connection: keep-alive
Content-Length: 0


HTTP/1.1 200 OK
Content-Disposition: inline; filename=main.10664c35.js
Content-Type: text/javascript; charset=utf-8
Content-Length: 1628939
Last-Modified: Tue, 31 Dec 2024 02:30:47 GMT
Cache-Control: no-store
ETag: "1735612247.0424643-1628939-135469549"
Date: Tue, 31 Dec 2024 03:00:03 GMT
X-Content-Type-Options: nosniff
Content-Security-Policy: default-src 'self'; script-src 'self'; style-src 'self' 'unsafe-inline'; object-src 'none';
Referrer-Policy: strict-origin-when-cross-origin
X-Frame-Options: DENY
X-XSS-Protection: 1; mode=block
Access-Control-Allow-Origin: https://trusted-domain.com
Set-Cookie: key=value; Expires=Tue, 31 Dec 2024 04:00:03 GMT; Max-Age=3600; Secure; HttpOnly; Path=/; SameSite=Lax

/*! For license information please see main.10664c35.js.LICENSE.txt */
(()=>{var e={219:(e,t,o)=>{"use strict";var n=o(763),r=
{childContextTypes:!0,contextType:!0,contextTypes:!0,defaultProps:!0,displayName:!0,getDefaultProps:!0,getDerivedStateFromE
rror:!0,getDerivedStateFromProps:!0,mixins:!0,propTypes:!0,type:!0},i=
{name:!0,length:!0,prototype:!0,caller:!0,callee:!0,arguments:!0,arity:!0},c=
{$$typeof:!0,compare:!0,defaultProps:!0,displayName:!0,propTypes:!0,type:!0},a={};function p(e){return n.isMemo(e)?
c:a[e.$$typeof]||r}a[n.ForwardRef]={$$typeof:!0,render:!0,defaultProps:!0,displayName:!0,propTypes:!0},a[n.Memo]=c;var
b=Object.defineProperty,M=Object.getOwnPropertyNames,s=Object.getOwnPropertySymbols,z=Object.getOwnPropertyDescriptor,l=Obj
ect.getPrototypeOf,O=Object.prototype;e.exports=function e(t,o,n){if("string"!==typeof o){if(O){var
r=l(o);r&&r!==O&&e(t,r,n)}var c=M(o);s&&(c=c.concat(s(o)));for(var a=p(t),d=p(o),u=0;u<c.length;++u){var A=c[u];if(!i[A]&&
(!n||!n[A])&&(!d||!d[A])&&(!a||!a[A])){var f=z(o,A);try{b(t,A,f)}catch(h){}}}}return t}},983:(e,t)=>{"use strict";var
o="function"===typeof Symbol&&Symbol.for,n=o?Symbol.for("react.element"):60103,r=o?Symbol.for("react.portal"):60106,i=o?
Symbol.for("react.fragment"):60107,c=o?Symbol.for("react.strict_mode"):60108,a=o?Symbol.for("react.profiler"):60114,p=o?
```

```
Symbol.for("react.provider"):60109,b=o?Symbol.for("react.context"):60110,M=o?Symbol.for("react.async_mode"):60111,s=o?
Symbol.for("react.concurrent_mode"):60111,z=o?Symbol.for("react.forward_ref"):60112,l=o?
Symbol.for("react.suspense"):60113,O=o?Symbol.for("react.suspense_list"):60120,d=o?Symbol.for("react.memo"):60115,u=o?
Symbol.for("react.lazy"):60116,A=o?Symbol.for("react.block"):60121,f=o?Symbol.for("react.fundamental"):60117,h=o?
Symbol.for("react.responder"):60118,q=o?Symbol.for("react.scope"):60119;function W(e){if("object"===typeof e&&null!==e){var
t=e.$$typeof;switch(t){case n:switch(e=e.type){case M:case s:case i:case a:case c:case l:return
e;default:switch(e=e&&e.$$typeof){case b:case z:case u:case d:case p:return e;default:return t}}case r:return t}}}function
m(e){return
W(e)===s}t.AsyncMode=M,t.ConcurrentMode=s,t.ContextConsumer=b,t.ContextProvider=p,t.Element=n,t.ForwardRef=z,t.Fragment=i,t
.Lazy=u,t.Memo=d,t.Portal=r,t.Profiler=a,t.StrictMode=c,t.Suspense=l,t.isAsyncMode=function(e){return
m(e)||W(e)===M},t.isConcurrentMode=m,t.isContext
...
...
...
Password",type:"password",fullWidth:!0,value:r,onChange:e=>i(e.target.value),error:!!c,helperText:c}),(0,Nc.jsx)(PA,
{children:(0,Nc.jsx)(uA,{type:"submit",color:"primary",variant:"contained",children:"Submit"})})]})]})]})};const
Yw=function(){const[e,o]=(0,t.useState)(!0);return(0,Nc.jsxs)("div",{className:"app-container",children:[!e&&(0,Nc.jsxs)
(Nc.Fragment,{children:[(0,Nc.jsx)("header",{children:(0,Nc.jsx)("h1",{children:"7DT Target of Opportunity (ToO)
Request"})}),(0,Nc.jsx)("section",{className:"form-section",children:(0,Nc.jsx)(Uw,{})}),(0,Nc.jsx)("header",{children:
(0,Nc.jsx)("h2",{children:"Observatory Dashboard"})}),(0,Nc.jsx)("section",{className:"dashboard-section",children:
(0,Nc.jsx)(yp,{})}),(0,Nc.jsx)("section",{className:"schedule-section",children:(0,Nc.jsx)(Np,{})}),(0,Nc.jsx)("footer",
{className:"footer",children:(0,Nc.jsx)("div",{className:"footer-content",children:(0,Nc.jsxs)("p",{children:["If you have
any questions, please contact:",(0,Nc.jsx)("a",{href:"mailto:myungshin.im@gmail.com?cc=hhchoi1022@gmail.com",children:"
Prof. Myungshin Im"})]})})})})]}),(0,Nc.jsx)(Vw,{open:e,onPasswordSubmit:()=>{o(!1)}})})]})},Gw=e=>{e&&e instanceof
Function&&o.e(453).then(o.bind(o,453)).then((t=>
{let{getCLS:o,getFID:n,getFCP:r,getLCP:i,getTTFB:c}=t;o(e),n(e),r(e),i(e),c(e)}))};r.createRoot(document.getElementById("ro
ot")).render((0,Nc.jsx)(t.StrictMode,{children:(0,Nc.jsx)(Yw,{})})),Gw())())();
//# sourceMappingURL=main.10664c35.js.map
```


정 제한적이지 않은 SameSite 속성을 갖는 쿠키 1 TOC

문제 1 / 1 TOC

제한적이지 않은 SameSite 속성을 갖는 쿠키

심각도:	정보용
CVSS 점수:	0.0
URL:	http://proton.snu.ac.kr:5000/
엔티티:	key (Cookie)
위험:	쿠키를 자사 또는 Same Site 컨텍스트로 제한하여(Strict) 쿠키 정보 유출을 방지하십시오.
원인:	제한적이지 않은 SameSite 속성 및 플래그를 갖는 민감한 쿠키
수정사항:	SameSite 쿠키 속성을 권장 값으로 구성하기 위한 가능한 솔루션을 검토하십시오

이유: 응답에 제한적이지 않은 SameSite 속성을 갖는 민감한 쿠키가 포함되어 있습니다. 가능한 경우 SameSite 속성을 Strict로 구성하는 것이 좋습니다. 가능하지 않은 경우, GET 요청을 사용하지 않고 CSRF의 위험을 완전히 차단하기 위한 세션 관리 메커니즘이 적용되어 있다면 "Lax" 값으로 구성하는 것으로도 충분합니다.

테스트 요청 및 응답:

```
GET / HTTP/1.1
Host: proton.snu.ac.kr:5000
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36
Accept:
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
Accept-Language: en-US
Connection: keep-alive
```

```
Content-Length: 0


HTTP/1.1 200 OK
Content-Disposition: inline; filename=index.html
Content-Type: text/html; charset=utf-8
Content-Length: 604
Last-Modified: Tue, 31 Dec 2024 02:30:47 GMT
Cache-Control: no-store
ETag: "1735612247.0344641-604-2322601339"
Date: Tue, 31 Dec 2024 02:59:59 GMT
X-Content-Type-Options: nosniff
Content-Security-Policy: default-src 'self'; script-src 'self'; style-src 'self' 'unsafe-inline'; object-src 'none';
Referrer-Policy: strict-origin-when-cross-origin
X-Frame-Options: DENY
X-XSS-Protection: 1; mode=block
Access-Control-Allow-Origin: https://trusted-domain.com
Set-Cookie: key=value; Expires=Tue, 31 Dec 2024 03:59:59 GMT; Max-Age=3600; Secure; HttpOnly; Path=/; SameSite=Lax

<!doctype html><html lang="en"><head><meta charset="utf-8"/><link rel="icon" href="/favicon.ico"/><meta name="viewport"
content="width=device-width,initial-scale=1"/><meta name="theme-color" content="#000000"/><meta name="description"
content="Web site created using create-react-app"/><link rel="apple-touch-icon" href="/logo192.png"/><link rel="manifest"
href="/manifest.json"/><title>7DT ToO Request</title><script defer="defer" src="/static/js/main.10664c35.js"></script><link
href="/static/css/main.2e7f4582.css" rel="stylesheet"></head><body><noscript></noscript><div id="root"></div></body></html>
```

정 클라이언트측(JavaScript) 쿠키 참조 1 TOC

문제 1 / 1 TOC

클라이언트측(JavaScript) 쿠키 참조

심각도:	정보용
CVSS 점수:	0.0
URL:	http://proton.snu.ac.kr:5000/static/js/main.10664c35.js
엔티티:	/*! For license information please see main.10664c35.js.LICENSE.txt */ (Page)
위험:	이러한 공격에 대한 최악의 시나리오는 컨텍스트와 클라이언트측에서 작성된 쿠키의 역할에 달려있습니다.
원인:	클라이언트 측에 쿠키가 작성됩니다.
수정사항:	클라이언트 측으로부터 비즈니스와 보안 로직을 제거하십시오.

이유: AppScan이 Javascript에서 쿠키 참조를 찾았습니다.
테스트 요청 및 응답:

```
GET /static/js/main.10664c35.js HTTP/1.1
Host: proton.snu.ac.kr:5000
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36
Accept: */*
Accept-Language: en-US
Referer: http://proton.snu.ac.kr:5000/
Connection: keep-alive
Content-Length: 0


HTTP/1.1 200 OK
Content-Disposition: inline; filename=main.10664c35.js
Content-Type: text/javascript; charset=utf-8
Content-Length: 1628939
Last-Modified: Tue, 31 Dec 2024 02:30:47 GMT
Cache-Control: no-store
```

```
ETag: "1735612247.0424643-1628939-135469549"
Date: Tue, 31 Dec 2024 02:55:58 GMT
X-Content-Type-Options: nosniff
Content-Security-Policy: default-src 'self'; script-src 'self'; style-src 'self' 'unsafe-inline'; object-src 'none';
Referrer-Policy: strict-origin-when-cross-origin
X-Frame-Options: DENY
X-XSS-Protection: 1; mode=block
Access-Control-Allow-Origin: https://trusted-domain.com
Set-Cookie: key=value; Expires=Tue, 31 Dec 2024 03:55:58 GMT; Max-Age=3600; Secure; HttpOnly; Path=/; SameSite=Lax

/*! For license information please see main.10664c35.js.LICENSE.txt */
(()=>{var e={219:(e,t,o)=>{"use strict";var n=o(763),r=
{childContextTypes:!0,contextType:!0,contextTypes:!0,defaultProps:!0,displayName:!0,getDefaultProps:!0,getDerivedStateFromE
rror:!0,getDerivedStateFromProps:!0,mixins:!0,propTypes:!0,type:!0},i=
{name:!0,length:!0,prototype:!0,caller:!0,callee:!0,arguments:!0,arity:!0},c=
{$$typeof:!0,compare:!0,defaultProps:!0,displayName:!0,propTypes:!0,type:!0},a={};function p(e){return n.isMemo(e)?
c:a[e.$$typeof]||r}a[n.ForwardRef]={$$typeof:!0,render:!0,defaultProps:!0,displayName:!0,propTypes:!0},a[n.Memo]=c;var
b=Object.defineProperty,M=Object.getOwnPropertyNames,s=Object.getOwnPropertySymbols,z=Object.getOwnPropertyDescriptor,l=Obj
ect.getPrototypeOf,O=Object.prototype;e.exports=function e(t,o,n){if("string"!==typeof o){if(O){var
r=l(o);r&&r!==O&&e(t,r,n)}var c=M(o);s&&(c=c.concat(s(o)));for(var a=p(t),d=p(o),u=0;u<c.length;++u){var A=c[u];if(!i[A]&&
(!n||!n[A])&&(!d||!d[A])&&(!a||!a[A])){var f=z(o,A);try{b(t,A,f)}catch(h){}}}}return t}},983:(e,t)=>{"use strict";var
o="function"===typeof Symbol&&Symbol.for,n=o?Symbol.for("react.element"):60103,r=o?Symbol.for("react.portal"):60106,i=o?
Symbol.for("react.fragment"):60107,c=o?Symbol.for("react.strict_mode"):60108,a=o?Symbol.for("react.profiler"):60114,p=o?
Symbol.for("react.provider"):60109,b=o?Symbol.for("react.context"):60110,M=o?Symbol.for("react.async_mode"):60111,s=o?
Symbol.for("react.concurrent_mode"):60111,z=o?Symbol.for("react.forward_ref"):60112,l=o?
Symbol.for("react.suspense"):60113,O=o?Symbol.for("react.suspense_list"):60120,d=o?Symbol.for("react.memo"):60115,u=o?
Symbol.for("react.lazy"):60116,A=o?Symbol.for("react.block"):60121,f=o?Symbol.for("react.fundamental"):60117,h=o?
Symbol.for("react.responder"):60118,q=o?Symbol.for("react.scope"):60119;function W(e){if("object"===typeof e&&null!==e){var
t=e.$$typeof;switch(t){case n:switch(e=e.type){case M:case s:case i:case a:case c:case l:return
e;default:switch(e=e&&e.$$typeof){case b:case z:case u:case d:case p:return e;default:return t}}case r:return t}}}function
m(e){return
W(e)===s}t.AsyncMode=M,t.ConcurrentMode=s,t.ContextConsumer=b,t.ContextProvider=p,t.Element=n,t.ForwardRef=z,t.Fragment=i,t
.Lazy=u,t.Memo=d,t.Portal=r,t.Profiler=a,t.StrictMode=c,t.Suspense=l,t.isAsyncMode=function(e){return
m(e)||W(e)===M},t.isConcurrentMode=m,t.isContextConsumer=function(e){return W(e)===b},t.isContextProvider=function(e)
{return W(e)===p},t.isElement=function(e){return"object"===typeof e&&null!==e&&e.$$typeof===n},t.isForwardRef=function(e)
{return W(e)===z},t.isFragment=function(e){return W(e)===i},t.isLazy=function(e){return W(e)===u},t.isMemo=function(e)
{return W(e)===d},t.isPortal=function(e){return W(e)===r},t.isProfiler=function(e){return
W(e)===a},t.isStrictMode=function(e){return W(e)===c},t.isSuspense=function(e){return
W(e)===l},t.isValidElementType=function(e){return"string"===typeof e||"function"===typeof
e||e===i||e===s||e===a||e===c||e===l||e===O||"object"===typeof e&&null!==e&&
(e.$$typeof===u||e.$$typeof===d||e.$$typeof===p||e.$$typeof===b||e.$$typeof===z||e.$$typeof===f||e.$$typeof===h||e.$$typeof
===q||e.$$typeof===A)},t.typeOf=W},763:(e,t,o)=>{"use strict";e.exports=o(983)},348:(e,t,o)=>
{(e.exports=o(716)).tz.load(o(681))},716:function(e,t,o){var n,r,i;!function(c,a){"use strict";e.exports?
e.exports=a(o(178)):(r=[o(178)],void 0===(i="function"===typeof(n=a)?n.apply(t,r):n)||(e.exports=i))}(0,(function(e){"use
strict";void 0===e.version&&e.default&&(e=e.default);var t,o={},n={},r={},i={},c={};e&&"string"===typeof
e.version||N("Moment Timezone requires Moment.js. See https://momentjs.com/timezone/docs/#/use-it/browser/");var
a=e.version.split("."),p=+a[0],b=+a[1];function M(e){return e>96?e-87:e>64?e-29:e-48}function s(e){var
t=0,o=e.split("."),n=o[0],r=o[1]||"",i=1,c=0,a=1;for(45===e.charCodeAt(0)&&(t=1,a=-
1);t<n.length;t++)c=60*c+M(n.charCodeAt(t));for(t=0;t<r.
...
...
...
```

수정 방법

안전하지 않거나 올바르지 않거나 누락된 **SameSite** 속성을 갖는 쿠키

TOC

원인:

올바르지 않거나 안전하지 않거나 누락된 SameSite 속성을 갖는 민감한 쿠키

위험:

쿠키를 자사 또는 Same Site 컨텍스트로 제한하여 쿠키 정보 유출 방지
CSRF 방지 토큰과 같은 추가적인 보호가 적용되어 있지 않은 경우 공격이 CSRF(크로스 사이트 요청 위조) 공격으로 이어질 수 있습니다.
SameSite 속성은 크로스 도메인 요청에 대해 쿠키가 전송되는 방식을 제어합니다.
이 속성은 3가지 값('Lax', 'Strict', 'None') 중 하나를 가질 수 있습니다. 'None'이 사용된 경우, 웹 사이트가 다른 웹 사이트로의 크로스 도메인 POST HTTP 요청을 작성할 수 있으며, 브라우저가 이 요청에 자동으로 쿠키를 추가합니다.
CSRF 방지 토큰과 같은 추가적인 보호가 적용되지 않은 경우 이로 인해 CSRF(크로스 사이트 요청 위조) 공격이 발생할 수 있습니다.
모드 및 사용법:
'Lax' 모드: 쿠키가 최상위 레벨 GET 요청으로만 전송됩니다.
'Strict' 모드: 사용자가 다른 웹 사이트로 연결되는 링크를 따라가는 경우에도 쿠키가 크로스 사이트 용도로 전송되지 않습니다.
'None' 모드: 쿠키가 크로스 사이트 요청으로 전송됩니다.
속성이 'Lax' 또는 'None' 값을 갖는 경우 'Secure' 플래그가 설정되어 있어야 하며 HTTPS를 통해 전송되어야 합니다.
예: - Set-Cookie: key=value; SameSite=Lax;Secure
권장 옵션은 속성을 'Strict'로 설정하는 것입니다.
예 - Set-Cookie: key=value; SameSite=Strict

영향 받는 제품:

이 문제는 다른 유형의 제품에 영향을 미칠 수 있습니다.

수정 권장사항:

일반

[1] SameSite 쿠키 속성을 권장 값으로 구성하기 위한 가능한 솔루션을 검토합니다.
[2] 쿠키를 자사 또는 Same Site 쿠키로 제한합니다.
[3] 쿠키가 자사 컨텍스트로만 전송되도록 쿠키의 SameSite 속성을 확인하여 Strict로 설정합니다.
[4] 또는, 자사 컨텍스트 제한을 완화하려면 쿠키의 SameSite 속성을 확인하여 Lax로 설정하고 Secure 플래그를 설정하고 HTTPS를 통해 전송합니다.

CWE:

1275

외부 참조:

WASC 위협 분류: 정보 유출
SameSite 쿠키

"Content-Security-Policy" 헤더의 누락되었거나 안전하지 않은 "Script-Src" 또는 "Default-src" 정책

TOC

원인:

안전하지 않은 웹 애플리케이션 프로그래밍 또는 구성

위험:

사용자 이름, 비밀번호, 머신 이름 및/또는 민감한 파일 위치 등과 같은 웹 애플리케이션에 대한 민감한 정보를 수집하는 것이 가능합니다
속기 쉬운 사용자를 설득해서 사용자 이름, 비밀번호, 신용카드 번호, 주민등록 번호와 같은 민감한 정보를 제공하도록 하는 것이 가능합니다.
script-src 지침(CSP) 값이 없거나 올바르지 않은 경우 웹 애플리케이션이 크로스 사이트 스크립팅, 크로스 사이트 프레이밍을 비롯한 공격에 취약해질 수 있습니다.
"Content-Security-Policy" 헤더는 브라우저가 페이지를 렌더링하는 방식을 수정하여 크로스 사이트 스크립팅을 비롯한 여러 크로스 사이트 인젝션으로부터 보호하도록 설계되었습니다. 웹 사이트의 올바른 작동을 방지하지 않는 방식으로 헤더 값을 올바르게 설정하는 것이 중요합니다. 예를 들어, 헤더가 인라인 JavaScript의 실행을 방지하도록 설정된 경우, 웹 사이트는 페이지에서 인라인 JavaScript를 사용하지 않아야 합니다.
script-src 지침은 스크립트가 실행될 수 있는 위치는 제한합니다. 여기에는 스크립트 요소로 직접 로드되는 URL뿐 아니라 인라인 스크립트 블록, 스크립트 실행을 트리거할 수 있는 XSLT 스타일시트[XSLT] 등도 포함됩니다.
크로스 사이트 스크립팅(XSS)으로부터 보호하려면 정책을 올바른 값으로 설정하는 것이 중요합니다:
'script-src'의 경우 '*', 'data:', 'http:', 'https:', 'ws:', 'wss:', 'unsafe-inline', 'unsafe-eval'과 같은 안전하지 않은 값을 사용하지 않아야 합니다.
script-src 지침이 명시적으로 설정되지 않은 경우 script-src를 비롯한 여러 지침의 대체로 기능하는 default-src를 사용하는 방안을 고려하십시오.
'default-src' 지침에 대해서도 안전하지 않은 값을 피해야 합니다.
'script-src' 또는 'default-src' 값을 "self"로 설정하는 것은 JSONP 엔드포인트를 사용하여 우회할 수 있습니다. 허용 목록에 포함된 도메인이 안전하지 않은 콜백 메서드를 허용하는 JSONP 엔드포인트를 포함하고 있을 수 있습니다. 이로 인해 공격자가 XSS를 수행할 수 있게 됩니다. 따라서 API 모범 사례와 양질의 Content-Security-Policy를 따르는 것을 권장합니다.
자세한 내용을 다음 링크를 참조하십시오.
"Content-Security-Policy"에는 "Content-Security-Policy" 헤더가 사용되고 있는지 확인하는 일반 테스트 하나와 "Frame-Ancestors", "Object-Src", "Script-Src"가 올바르게 구성되었는지 확인하는 3개의 테스트, 이렇게 4개의 테스트가 포함되어 있습니다.

영향 받는 제품:

이 문제는 여러 유형의 제품에 영향을 미칠 수 있습니다

수정 권장사항:

일반

서버가 "script-src" 및 "default-src" 지침에 대한 올바른 값으로 "Content-Security-Policy" 헤더를 보내도록 구성하십시오
script-src 지침을 'none' 또는 'strict-dynamic'과 같은 보안 값으로 구성하는 것을 권장합니다. 필요한 경우 'self'로 'script-src' 또는 'default-src'를 사용하는 대신 난스(nonce) 또는 해시 알고리즘으로 'unsafe-inline' 또는 'unsafe-eval'을 사용해야 합니다.
Apache는 다음을 참조하십시오:
http://httpd.apache.org/docs/2.2/mod/mod_headers.html
IIS는 다음을 참조하십시오:
https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspx
nginx는 다음을 참조하십시오:
http://nginx.org/en/docs/http/ngx_http_headers_module.html

CWE:

200

외부 참조:

유용한 보안 헤더 목록
컨텐츠 보안 정책 소개
MDN 웹 문서 - CSP: script-src

"Content-Security-Policy"의 누락되었거나 안전하지 않은 "Style-src" 또는 "Default-src" 정책

TOC

원인:

안전하지 않은 웹 애플리케이션 프로그래밍 또는 환경 설정입니다

위험:

사용자 이름, 비밀번호, 머신 이름 및/또는 민감한 파일 위치 등과 같이 웹 애플리케이션에 대한 민감한 정보를 모으는 것이 가능합니다.
속기 쉬운 사용자를 설득해서 사용자 이름, 비밀번호, 신용카드 번호, 주민등록 번호와 같은 민감한 정보를 제공하도록 하는 것이 가능합니다.
style-src 지침(CSP) 값이 없거나 올바르지 않은 경우 웹 애플리케이션이 크로스 사이트 스크립팅을 비롯한 공격에 취약해질 수 있습니다.
"Content-Security-Policy" 헤더는 브라우저가 페이지를 렌더링하는 방식을 수정하여 크로스 사이트 스크립팅을 비롯한 여러 크로스 사이트 인젝션으로부터 보호하도록 설계되었습니다. 웹 사이트의 올바른 작동을 방지하지 않는 방식으로 헤더 값을 올바르게 설정하는 것이 중요합니다.
예를 들어, 헤더가 인라인 JavaScript의 실행을 방지하도록 설정된 경우, 웹 사이트는 페이지에서 인라인 JavaScript를 사용하지 않아야 합니다.
"style-src" 컨텐츠 보안 정책(CSP) 지침은 CSS 스타일 및 스타일시트의 로드와 실행을 보호합니다.
크로스 사이트 스크립팅(XSS)으로부터 보호하려면 정책을 올바른 값으로 설정하는 것이 중요합니다:
'style-src'의 경우 '*', 'data:', 'http:', 'https:', 'ws:', 'wss:', 'unsafe-inline', 'unsafe-eval'과 같은 안전하지 않은 값을 사용하지 않아야 합니다.
style-src 지시어가 명시적으로 설정되지 않은 경우 style-src를 포함한 많은 지시어에 대한 대체 역할을 하는 default-src를 사용하는 것이 좋습니다.
"default-src" 지침에 대해서도 안전하지 않은 값을 피해야 합니다.
자세한 내용을 다음 링크를 참조하십시오.

영향 받는 제품:

이 문제는 여러 유형의 제품에 영향을 줄 수 있습니다

수정 권장사항:

일반

"style-src"에 대한 적절한 값을 사용하여 "Content-Security-Policy" 헤더를 보내도록 서버를 구성하십시오.
'self' 또는 'none'과 같은 보안 값으로 style-src 지시어를 구성하는 것이 좋습니다. 필요한 경우 nonce 또는 해시 알고리즘과 함께 'unsafe-inline' 또는 'unsafe-eval'을 사용해야 합니다.
style-src 지시어가 명시적으로 설정되지 않은 경우 대체 역할을 하는 default-src를 사용하는 것을 고려하고 "default-src" 지시문에 대해 안전하지 않은 값도 피해야 합니다. 안전한 "default-src" 값에는 nonce 또는 해시 알고리즘과 함께 'none', 'unsafe-inline', 'unsafe-eval'이 포함됩니다.
Apache의 경우 다음 링크 참조:
http://httpd.apache.org/docs/2.2/mod/mod_headers.html
IIS의 경우 다음 링크 참조:
https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspx
nginx의 경우 다음 링크 참조:
http://nginx.org/en/docs/http/ngx_http_headers_module.html

CWE:

200

외부 참조:

유용한 보안 헤더 목록
컨텐츠 보안 정책 소개
MDN 웹 문서 - CSP: style-src

암호화 누락

TOC

원인:

- 애플리케이션이 민감한 정보를 교환하는 데 TLS/SSL 등의 보안 채널을 사용하지 않습니다.
- 네트워크 트래픽에 대한 액세스 권한이 있는 공격자는 연결을 통해 패킷을 도청할 수 있습니다. 이 공격은 기술적으로 어렵지 않지만 네트워크에서 민감한 데이터가 이동하는 지점에 대한 물리적 액세스가 필요합니다.

위험:

일반 텍스트로 서버에 전송된 모든 정보가 네트워크상에서 도난당할 수 있으며 이는 나중에 ID 도용이나 사용자 가장에 사용될 수 있습니다.
암호화되지 않고 전송되는 사용자 로그인 정보(사용자 이름 및 암호), 신용 카드 번호, 주민 등록 번호 등의 민감한 데이터를 가로챌 수 있습니다.
내용 변경, 데이터 절도 또는 서버에 사용자 가장을 포함하여 공격자가 통신을 완전하게 제어할 수 있도록 하는 MitM(메시지 가로채기) 공격을 수행할 수 있습니다.

수정 권장사항:

일반

항상 모든 데이터를 TLS/SSL 연결로만 전송해야 합니다. 여기에는 브라우저, 데이터베이스와 같은 백엔드 연결, 타사 API 및 기타 서비스를 포함한 모든 외부 통신이 포함됩니다.
또한 여러 개인정보 규정에 따라 사용자 자격 증명 등의 민감한 정보는 항상 암호화되어 웹 사이트로 전송됩니다.
항상 암호화된 연결(예: TLS/SSL)을 사용하고, 암호화되지 않은 HTTP를 사용하여 민감한 정보에 액세스하도록 허용하지 마십시오.
TLS 1.2 또는 TLS 1.3을 사용하며 강력한 암호화 해싱 알고리즘과 암호화 그룹을 사용합니다.

CWE:

319

외부 참조:

OWASP - TLS 암호화 문자열 치트 시트
OWASP - 전송 계층 보호 치트 시트

이메일 주소 패턴 발견

TOC

원인:

안전하지 않은 웹 애플리케이션 프로그래밍 또는 환경 설정입니다.

위험:

사용자 이름, 비밀번호, 머신 이름 및/또는 민감한 파일 위치 등과 같이 웹 애플리케이션에 대한 민감한 정보를 모으는 것이 가능합니다.
허용되지 않은 이메일(스팸)을 전송하기 위한 메일링 목록을 구축하기 위해 이메일 주소를 찾는 일을 하는 Spambots 인터넷 사이트.
AppScan이 스팸 메일 발송에 악용될 수 있는 하나 이상의 이메일 주소를 포함하는 응답을 발견했습니다.
또한 발견된 이메일 주소는 개인용이므로 일반 공용으로 액세스하면 안 됩니다.

영향 받는 제품:

이 문제는 다른 유형의 제품에 영향을 미칠 수 있습니다.

수정 권장사항:

일반

웹 사이트에서 모든 이메일 주소를 제거하여 악성 사용자에 의해 악용되지 않도록 주의하십시오.

CWE:
359

외부 참조:
Spambot의 정의(Wikipedia)

제한적이지 않은 SameSite 속성을 갖는 쿠키

TOC

원인:
제한적이지 않은 SameSite 속성 및 플래그를 갖는 민감한 쿠키

위험:
쿠키를 자사 또는 Same Site 컨텍스트로 제한하여(Strict) 쿠키 정보 유출 방지
CSRF 방지 토큰과 같은 추가적인 보호가 적용되어 있지 않은 경우 공격이 CSRF(크로스 사이트 요청 위조) 공격으로 이어질 수 있습니다.
SameSite 속성은 크로스 도메인 요청에 대해 쿠키가 전송되는 방식을 제어합니다.
* Strict 모드가 권장됩니다. 사용자가 다른 웹 사이트로 연결되는 링크를 따라가는 경우에도 쿠키가 크로스 사이트 용도로 전송되지 않습니다.
* SameSite 속성을 'Strict'로 설정하면 자사 컨텍스트로만 전송되며 타사 웹 사이트에서 시작한 요청으로는 전송되지 않습니다.
* 예 - Set-Cookie: key=value; SameSite=Strict

영향 받는 제품:
이 문제는 다른 유형의 제품에 영향을 미칠 수 있습니다.

수정 권장사항:

일반

[1] 쿠키를 자사 컨텍스트로 제한합니다.
[2] 쿠키가 자사 컨텍스트로만 전송되도록 쿠키의 SameSite 속성을 확인하고 Strict로 설정합니다.
[3]GET 요청을 사용하지 않고 CSRF의 위험을 완전히 차단하기 위한 세션 관리 메커니즘이 적용되어 있을 경우 값을 "Lax"로 설정하는 것으로도 충분합니다.

CWE:
1275

외부 참조:
WASC 위협 분류: 정보 유출
SameSite 쿠키

클라이언트측(JavaScript) 쿠키 참조

TOC

원인:
클라이언트 측에 쿠키가 작성됩니다.

위험:

이러한 공격에 대한 최악의 시나리오는 컨텍스트와 클라이언트측에서 작성된 쿠키의 역할에 달려있습니다.
쿠키는 웹 서버에서 작성되어 웹 브라우저에 저장되는 정보입니다.
쿠키에는 웹 애플리케이션이 사용자를 식별하고 사용자의 상태를 유지보수하는 데 주로(이에 한하지 않음) 사용하는 정보가 포함됩니다.
AppScan에서 클라이언트측 JavaScript 코드가 사이트의 쿠키를 조작(작성 또는 수정)하는 것을 발견했습니다.
공격자가 이 코드를 보고 해당 로직을 이해하여 자신의 쿠키를 작성하는 데 사용하거나 도용한 정보로 기존 쿠키를 수정할 수 있습니다.
공격자가 일으킬 수 있는 손상은 애플리케이션에서 해당 쿠키를 사용하는 방법이나 쿠키에 저장하는 정보에 따라 달라집니다.
특히 쿠키 조작은 세션 하이잭 또는 권한 상승을 발생시킬 수 있습니다.
쿠키 손상으로 발생하는 기타 취약점에는 SQL 인젝션과 XSS(Cross-site scripting)가 포함됩니다.

영향 받는 제품:

이 문제는 다른 유형의 제품에 영향을 미칠 수 있습니다.

수정 권장사항:

일반

[1] 업무/보안 로직을 클라이언트 측에서 처리하지 마십시오.
[2] 사이트에 대한 보안 위협이 될 수 있는 취약한 클라이언트측 Javascript 코드를 찾아서 제거하십시오.

CWE:

602

외부 참조:

WASC 위협 분류: 정보 유출

애플리케이션 데이터

방문한 URL 3

TOC

URL
http://proton.snu.ac.kr:5000/
http://proton.snu.ac.kr:5000/static/js/main.10664c35.js
http://proton.snu.ac.kr:5000/manifest.json

매개변수 0

TOC

이름	값	URL	유형

실패한 요청 0

TOC

URL	이유

주석 1

TOC

URL	주석
http://proton.snu.ac.kr:5000/	<!doctype html>

JavaScript 1

TOC

URL / 코드
http://proton.snu.ac.kr:5000/static/js/main.10664c35.js

```
/*! For license information please see main.10664c35.js.LICENSE.txt */
(()=>{var e={219:(e,t,o)=>{"use strict";var n=o(763),r=
{childContextTypes:!0,contextType:!0,contextTypes:!0,defaultProps:!0,displayName:!0,getDefaultProps:!0,getDerivedStateFromError:!0,getD
erivedStateFromProps:!0,mixins:!0,propTypes:!0,type:!0},i={name:!0,length:!0,prototype:!0,caller:!0,callee:!0,arguments:!0,arity:!0},c=
{$$typeof:!0,compare:!0,defaultProps:!0,displayName:!0,propTypes:!0,type:!0},a={};function p(e){return n.isMemo(e)?
c:a[e.$$typeof]||r}a[n.ForwardRef]={$$typeof:!0,render:!0,defaultProps:!0,displayName:!0,propTypes:!0},a[n.Memo]=c;var
b=Object.defineProperty,M=Object.getOwnPropertyNames,s=Object.getOwnPropertySymbols,z=Object.getOwnPropertyDescriptor,l=Object.getProto
typeOf,O=Object.prototype;e.exports=function e(t,o,n){if("string"!==typeof o){if(O){var r=l(o);r&&r!==O&&e(t,r,n)}var c=M(o);s&&
(c=c.concat(s(o)));for(var a=p(t),d=p(o),u=0;u<c.length;++u){var A=c[u];if(!i[A]&&(!n||!n[A])&&(!d||!d[A])&&(!a||!a[A])){var
f=z(o,A);try{b(t,A,f)}catch(h){}}}}return t}},983:(e,t)=>{"use strict";var o="function"===typeof Symbol&&Symbol.for,n=o?
Symbol.for("react.element"):60103,r=o?Symbol.for("react.portal"):60106,i=o?Symbol.for("react.fragment"):60107,c=o?
Symbol.for("react.strict_mode"):60108,a=o?Symbol.for("react.profiler"):60114,p=o?Symbol.for("react.provider"):60109,b=o?
Symbol.for("react.context"):60110,M=o?Symbol.for("react.async_mode"):60111,s=o?Symbol.for("react.concurrent_mode"):60111,z=o?
Symbol.for("react.forward_ref"):60112,l=o?Symbol.for("react.suspense"):60113,O=o?Symbol.for("react.suspense_list"):60120,d=o?
Symbol.for("react.memo"):60115,u=o?Symbol.for("react.lazy"):60116,A=o?Symbol.for("react.block"):60121,f=o?
Symbol.for("react.fundamental"):60117,h=o?Symbol.for("react.responder"):60118,q=o?Symbol.for("react.scope"):60119;function W(e)
{if("object"===typeof e&&null!==e){var t=e.$$typeof;switch(t){case n:switch(e=e.type){case M:case s:case i:case a:case c:case l:return
e;default:switch(e=e&&e.$$typeof){case b:case z:case u:case d:case p:return e;default:return t}}case r:return t}}}function m(e){return
W(e)===s}t.AsyncMode=M,t.ConcurrentMode=s,t.ContextConsumer=b,t.ContextProvider=p,t.Element=n,t.ForwardRef=z,t.Fragment=i,t.Lazy=u,t.Me
mo=d,t.Portal=r,t.Profiler=a,t.StrictMode=c,t.Suspense=l,t.isAsyncMode=function(e){return
m(e)||W(e)===M},t.isConcurrentMode=m,t.isContextConsumer=function(e){return W(e)===b},t.isContextProvider=function(e){return
W(e)===p},t.isElement=function(e){return"object"===typeof e&&null!==e&&e.$$typeof===n},t.isForwardRef=function(e){return
W(e)===z},t.isFragment=function(e){return W(e)===i},t.isLazy=function(e){return W(e)===u},t.isMemo=function(e){return
W(e)===d},t.isPortal=function(e){return W(e)===r},t.isProfiler=function(e){return W(e)===a},t.isStrictMode=function(e){return
W(e)===c},t.isSuspense=function(e){return W(e)===l},t.isValidElementType=function(e){return"string"===typeof e||"function"===typeof
e||e===i||e===s||e===a||e===c||e===l||e===O||"object"===typeof e&&null!==e&&
(e.$$typeof===u||e.$$typeof===d||e.$$typeof===p||e.$$typeof===b||e.$$typeof===z||e.$$typeof===f||e.$$typeof===h||e.$$typeof===q||e.$$ty
peof===A)},t.typeOf=W},763:(e,t,o)=>{"use strict";e.exports=o(983)},348:(e,t,o)=>
{(e.exports=o(716)).tz.load(o(681))},716:function(e,t,o){var n,r,i;!function(c,a){"use strict";e.exports?e.exports=a(o(178)):(r=
[o(178)],void 0===(i="function"===typeof(n=a)?n.apply(t,r):n)||(e.exports=i))}(0,(function(e){"use strict";void
0===e.version&&e.default&&(e=e.default);var t,o={},n={},r={},i={},c={};e&&"string"===typeof e.version||N("Moment Timezone requires
Moment.js. See https://momentjs.com/timezone/docs/#/use-it/browser/");var a=e.version.split("."),p=+a[0],b=+a[1];function M(e){return
e>96?e-87:e>64?e-29:e-48}function s(e){var t=0,o=e.split("."),n=o[0],r=o[1]||"",i=1,c=0,a=1;for(45===e.charCodeAt(0)&&(t=1,a=-
1);t<n.length;t++)c=60*c+M(n.charCodeAt(t));for(t=0;t<r.length;t++)i/=60,c+=M(r.charCodeAt(t))*i;return c*a}function z(e){for(var
t=0;t<e.length;t++)e[t]=s(e[t])}function l(e,t){var o,n=[];for(o=0;o<t.length;o++)n[o]=e[t[o]];return n}function O(e){var
t=e.split("|"),o=t[2].split(" "),n=t[3].split(""),r=t[4].split(" ");return z(o),z(n),z(r),function(e,t){for(var
o=0;o<t;o++)e[o]=Math.round((e[o-1]||0)+6e4*e[o]);e[t-1]=1/0}(r,n.length),{name:t[0],abbrs:l(t[1].split("
"),n),offsets:l(o,n),untils:r,population:0|t[5]}}function d(e){e&&this._set(O(e))}function u(e,t){this.name=e,this.zones=t}function
A(e){var t=e.toTimeString(),o=t.match(/\([a-z ]+\)/i);"GMT"===(o=o&&o[0]?(o=o[0].match(/[A-Z]/g))?o.join(""):void 0:(o=t.match(/[A-Z]
{3,5}/g))?o[0]:void 0)&&(o=void 0),this.at=+e,this.abbr=o,this.offset=e.getTimezoneOffset()}function f(e)
{this.zone=e,this.offsetScore=0,this.abbrScore=0}function h(e,t){for(var o,n;n=6e4*((t.at-e.at)/12e4|0);)(o=new A(new
Date(e.at+n))).offset===e.offset?e=o:t=o;return e}function q(e,t){return e.offsetScore!==t.offsetScore?e.offsetScore-
t.offsetScore:e.abbrScore!==t....
```


쿠키 1

TOC

이름	첫세트	도메인	보안	HTTP만	Same Site	JS 스택 추적
값	요청 URL		만료			
key	http://proton.snu.ac.kr:5000/	proton.snu.ac.kr	True	True	Lax	
value			2024-12-31 오전 3:57:56			