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: 2024-12-30 오후 4:05:40

목차

- 클라이언트측(JavaScript) 쿠키 참조

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:	2
낮은 심각도 문제:	5
정보용 심각도 문제:	3
이 보고서에 포함된 총 보안 문제:	10
이 스캔에서 발견된 총 보안 문제:	10

일반 정보

스캔 파일 이름:	http@proton.snu.ac.kr+5000
스캔 시작:	2024-12-30 오후 4:05:40
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 9

TOC

	문제 유형	문제 수
중	MacOS X Finder Apache 디렉토리 콘텐츠 노출	1
중	민감한 헤더에 대한 ADNS 블라인드 SSRF	1
하	누락되었거나 안전하지 않은 "X-Content-Type-Options" 헤더	1
하	누락된 "Content-Security-Policy" 헤더	1
하	암호화 누락	1
하	지나치게 허용적인 CORS 액세스 정책	2
정	누락된 "Referrer policy" 보안 헤더	1
정	이메일 주소 패턴 발견	1
정	클라이언트측(JavaScript) 쿠키 참조	1

취약한 URL 3

TOC

	URL	문제 수
중	http://proton.snu.ac.kr:5000/	7
하	http://proton.snu.ac.kr:5000/manifest.json	1
정	http://proton.snu.ac.kr:5000/static/js/main.6837a453.js	2

수정 권장사항 9

TOC

	조치방안 태스크	문제 수
중	Mac OS X의 최신 버전으로 업그레이드하십시오.	1
중	외부에서 제공된 모든 데이터의 유효성 검증과 무결 처리를 수행합니다. 액세스 제어 메커니즘의 유효성 검증을 수행합니다.	1
하	"nosniff" 값으로 "X-Content-Type-Options" 헤더를 사용하도록 서버를 구성하십시오.	1
하	보안 정책을 사용하여 "Content-Security-Policy" 헤더를 사용하도록 서버를 구성하십시오.	1
하	보안 정책을 사용하여 "Referrer Policy" 헤더를 사용하도록 서버를 구성하십시오	1
하	웹 사이트에서 이메일 주소를 제거하십시오.	1

하	클라이언트 측으로부터 비즈니스와 보안 로직을 제거하십시오.	1
하	통신이 암호화되도록 TLS/SSL을 구성하십시오.	1
하	허용되는 사이트만 포함하도록 "Access-Control-Allow-Origin" 헤더를 수정하십시오.	2

보안 위험 6

TOC

	위험	문제 수
중	제한된 파일을 포함하는 특정 웹 애플리케이션 가상 디렉토리의 콘텐츠를 검색하고 다운로드하는 것이 가능합니다.	1
중	공격자가 권한 부여되지 않은 자원을 가져가고 해당 자원의 무결성에 영향을 줄 수 있습니다. 애플리케이션의 서버를 사용하여 내부 네트워크를 포함하는 여러 네트워크의 스캔이 수행될 수 있으며, 이로 인해 서버가 각종 블랙리스트에 포함될 수 있습니다.	1
하	사용자 이름, 비밀번호, 머신 이름 및/또는 민감한 파일 위치 등과 같이 웹 애플리케이션에 대한 민감한 정보를 모으는 것이 가능합니다.	6
하	속기 쉬운 사용자를 설득해서 사용자 이름, 비밀번호, 신용카드 번호, 주민등록 번호와 같은 민감한 정보를 제공하도록 하는 것이 가능합니다.	5
하	암호화 되지 않은 주민등록 번호, 신용카드 번호 등과 같이 민감한 데이터를 빼내는 것이 가능합니다.	1
정	이러한 공격에 대한 최악의 시나리오는 컨텍스트와 클라이언트측에서 작성된 쿠키의 역할에 달려있습니다.	1

원인 8

TOC

	원인	문제 수
중	써드파티 제품을 위한 최신 패치나 핫 픽스가 설치되지 않았습니다.	1
중	나중에 URI를 사용하여 추가된 요소를 포함하는 사용자 입력값의 올바르지 않은 처리, 필터링 또는 유효성 검증	1
하	안전하지 않은 웹 애플리케이션 프로그래밍 또는 환경 설정입니다.	1
하	안전하지 않은 웹 애플리케이션 프로그래밍 또는 환경 설정입니다.	4
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 구성	1
정	클라이언트 측에 쿠키가 작성됩니다.	1

WASC 위협 분류

TOC

위협	문제 수
디렉토리 색인화	1

서버 측 요청 위조	1
정보 노출	8

문제 유형으로 정렬된 문제

중 MacOS X Finder Apache 디렉토리 콘텐츠 노출 1 TOC

문제 1 / 1 TOC

MacOS X Finder Apache 디렉토리 콘텐츠 노출

심각도:	중
CVSS 점수:	6.5
URL:	http://proton.snu.ac.kr:5000/
엔티티:	.DS_Store (Page)
위험:	제한된 파일을 포함하는 특정 웹 애플리케이션 가상 디렉토리의 콘텐츠를 검색하고 다운로드하는 것이 가능합니다.
원인:	써드파티 제품을 위한 최신 패치나 핫 픽스가 설치되지 않았습니다.
수정사항:	Mac OS X의 최신 버전으로 업그레이드하십시오.

이유: 테스트에서 Mac OS X Finder 디렉토리의 콘텐츠를 검색했습니다.
테스트 요청 및 응답:

```
GET /.DS_Store 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=.DS_Store
Content-Type: application/octet-stream
Content-Length: 6148
Last-Modified: Mon, 23 Dec 2024 06:01:31 GMT
Cache-Control: no-cache
ETag: "1734933691.34431-6148-1902056625"
Date: Mon, 30 Dec 2024 07:40:07 GMT
Access-Control-Allow-Origin: *

    Bud1          %          @       ?          @       ?          @       ?          @          E   %
...
...
...
```

중 민감한 헤더에 대한 ADNS 블라인드 SSRF 1 TOC

문제 1 / 1 TOC

민감한 헤더에 대한 ADNS 블라인드 SSRF

심각도:	중
CVSS 점수:	6.0
URL:	http://proton.snu.ac.kr:5000/
엔티티:	(Page)
위험:	공격자가 권한 부여되지 않은 자원을 가져가고 해당 자원의 무결성에 영향을 줄 수 있습니다. 애플리케이션의 서버를 사용하여 내부 네트워크를 포함하는 여러 네트워크의 스캔이 수행될 수 있으며, 이로 인해 서버가 각종 블랙리스트에 포함될 수 있습니다.
원인:	나중에 URI를 사용하여 추가된 요소를 포함하는 사용자 입력값의 올바르지 않은 처리, 필터링 또는 유효성 검증
수정사항:	외부에서 제공된 모든 데이터의 유효성 검증과 무결 처리를 수행합니다. 액세스 제어 메커니즘의 유효성 검증을 수행합니다.

이유: AppScan 외부 DNS 서버가 이 테스트의 변종 ID가 포함된 DNS 쿼리를 수신한 결과 애플리케이션이 취약하다는 결론을 내렸습니다.

테스트 요청 및 응답:

```
GET / HTTP/1.1
Host: v3-ping-23-35fd980e-2345-4e4a-94fd-811de50a87b3.adns.appscan.com
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: Mon, 30 Dec 2024 06:52:21 GMT
Cache-Control: no-cache
ETag: "1735541541.503501-604-2322601339"
Date: Mon, 30 Dec 2024 07:37:40 GMT
Access-Control-Allow-Origin: *

/**
AppScan message: The response body is omitted as it is not needed to detect the vulnerability.
**/
```

하 누락되었거나 안전하지 않은 "X-Content-Type-Options" 헤더 1 TOC

문제 1 / 1 TOC

누락되었거나 안전하지 않은 "X-Content-Type-Options" 헤더

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:	"nosniff" 값으로 "X-Content-Type-Options" 헤더를 사용하도록 서버를 구성하십시오.

이유: AppScan에서 "X-Content-Type-Options" 응답 헤더가 누락되었거나 안전하지 않은 값을 포함하고 있음을 발견했습니다. 따라서 드라이브 바이 다운로드 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: Mon, 30 Dec 2024 06:52:21 GMT
Cache-Control: no-cache
ETag: "1735541541.503501-604-2322601339"
Date: Mon, 30 Dec 2024 07:38:18 GMT
Access-Control-Allow-Origin: *

<!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.6837a453.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

누락된 "Content-Security-Policy" 헤더

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: Mon, 30 Dec 2024 06:52:21 GMT
Cache-Control: no-cache
ETag: "1735541541.503501-604-2322601339"
Date: Mon, 30 Dec 2024 07:38:18 GMT
Access-Control-Allow-Origin: *

<!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.6837a453.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: Mon, 30 Dec 2024 06:52:21 GMT
Cache-Control: no-cache
ETag: "1735541541.503501-604-2322601339"
Date: Mon, 30 Dec 2024 07:38:18 GMT
Access-Control-Allow-Origin: *

<!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.6837a453.js"></script><link
href="/static/css/main.2e7f4582.css" rel="stylesheet"></head><body><noscript></noscript><div id="root"></div></body></html>
```

하 지나치게 허용적인 CORS 액세스 정책 2

TOC

문제 1 / 2

TOC

지나치게 허용적인 CORS 액세스 정책

심각도:	하
CVSS 점수:	3.7
URL:	http://proton.snu.ac.kr:5000/
엔티티:	(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:	허용되는 사이트만 포함하도록 "Access-Control-Allow-Origin" 헤더를 수정하십시오.

이유: AppScan이 "Access-Control-Allow-Origin" 헤더가 지나치게 허용적인 사실을 발견함
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: Mon, 30 Dec 2024 06:52:21 GMT
Cache-Control: no-cache
ETag: "1735541541.503501-604-2322601339"
Date: Mon, 30 Dec 2024 07:38:18 GMT
Access-Control-Allow-Origin: *

<!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.6837a453.js"></script><link
href="/static/css/main.2e7f4582.css" rel="stylesheet"></head><body><noscript></noscript><div id="root"></div></body></html>
```

지나치게 허용적인 CORS 액세스 정책

심각도:	하
CVSS 점수:	3.7
URL:	http://proton.snu.ac.kr:5000/manifest.json
엔티티:	manifest.json (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:	허용되는 사이트만 포함하도록 "Access-Control-Allow-Origin" 헤더를 수정하십시오.

이유: AppScan이 "Access-Control-Allow-Origin" 헤더가 지나치게 허용적인 사실을 발견함
테스트 요청 및 응답:

```
GET /manifest.json HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://proton.snu.ac.kr:5000/
Host: proton.snu.ac.kr:5000
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Content-Length: 0


HTTP/1.1 200 OK
Content-Disposition: inline; filename=manifest.json
Content-Type: application/json
Content-Length: 301
Last-Modified: Mon, 23 Dec 2024 06:01:31 GMT
Cache-Control: no-cache
ETag: "1734933691.35231-301-3453228735"
Date: Mon, 30 Dec 2024 07:36:56 GMT
Access-Control-Allow-Origin: *

{

"short_name": "7DT ToO",

"name": "7DT ToO request form",

"icons": [

{

"src": "favicon.ico",

"sizes": "64x64 32x32 24x24 16x16",

"type": "image/x-icon"

                }

 ],

"start_url": ".",

"display": "standalone",

"theme_color": "#000000",

"background_color": "#ffffff"

}
```

정 누락된 "Referrer policy" 보안 헤더 1 TOC

문제 1 / 1 TOC

누락된 "Referrer policy" 보안 헤더

심각도:	정보용
CVSS 점수:	0.0
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 "Referrer Policy" 헤더를 사용하도록 서버를 구성하십시오

이유: AppScan에서 Referrer 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: Mon, 30 Dec 2024 06:52:21 GMT
Cache-Control: no-cache
ETag: "1735541541.503501-604-2322601339"
Date: Mon, 30 Dec 2024 07:05:50 GMT
Access-Control-Allow-Origin: *

<!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.6837a453.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

이메일 주소 패턴 발견

심각도:	정보용
CVSS 점수:	0.0
URL:	http://proton.snu.ac.kr:5000/static/js/main.6837a453.js
엔티티:	main.6837a453.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.6837a453.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.6837a453.js
Content-Type: text/javascript; charset=utf-8
Content-Length: 1628732
Last-Modified: Mon, 30 Dec 2024 06:52:21 GMT
Cache-Control: no-cache
ETag: "1735541541.5115008-1628732-145365494"
Date: Mon, 30 Dec 2024 07:36:54 GMT
Access-Control-Allow-Origin: *

/*! For license information please see main.6837a453.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
...
...
...
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.6837a453.js.map
```


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.6837a453.js
엔티티:	/*! For license information please see main.6837a453.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.6837a453.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.6837a453.js
Content-Type: text/javascript; charset=utf-8
Content-Length: 1628732
Last-Modified: Mon, 30 Dec 2024 06:52:21 GMT
Cache-Control: no-cache
ETag: "1735541541.5115008-1628732-145365494"
Date: Mon, 30 Dec 2024 07:05:50 GMT
Access-Control-Allow-Origin: *

/*! For license information please see main.6837a453.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.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
...
...
...
```

수정 방법

MacOS X Finder Apache 디렉토리 콘텐츠 노출

TOC

원인:

써드파티 제품을 위한 최신 패치나 핫 픽스가 설치되지 않았습니다.

위험:

제한된 파일을 포함하는 특정 웹 애플리케이션 가상 디렉토리의 컨텐츠를 검색하고 다운로드하는 것이 가능합니다.
MacOS X Finder 유틸리티를 통해 디렉토리의 내용을 열람할 때, ".DS_Store"이라는 숨겨진 파일이 작성됩니다. 이 파일은 디렉토리의 내용과 파일에 대한 인덱스를 포함하고 있습니다. 공격자는 이 정보를 바탕으로 웹 사이트의 구조나 내용을 확인할 수 있습니다.
샘플 악용:
웹 사이트에 /some_directory라는 가상 디렉토리가 있다고 가정하는 경우, 다음 요청은 해당 컨텐츠를 검색합니다.
http://TARGET/some_directory/.DS_Store
참고: '.DS_Store' 파일의 컨텐츠는 ASCII 및 유니코드의 혼합이며, 이를 지원하는 뷰어로만 볼 수 있습니다.

영향 받는 제품:

Apache 웹 서버 1.3.14(Mac OS X 10.0.x)

수정 권장사항:

일반

Mac OS X 10.1 또는 그 이전 버전으로 업그레이드하십시오. 다음 웹 페이지에서 다운로드할 수 있습니다.
http://www.info.apple.com/support/downloads.html

CWE:

548

외부 참조:

벤더 사이트
BugTraq BID: 3316
Bugtraq 메시지
Apple의 보안 업데이트 페이지

민감한 헤더에 대한 ADNS 블라인드 SSRF

TOC

원인:

나중에 URI를 사용하여 추가된 요소를 포함하는 사용자 입력값의 올바르지 않은 처리, 필터링 또는 유효성 검증

위험:

안전하지 않고 의도되지 않은 방식으로 서버가 정보를 처리, 전송 또는 가져오도록 조작하는 것이 가능합니다
애플리케이션이 외부적으로 영향을 받은 입력값을 사용하여 요청을 보내며, 내부 또는 외부 기능을 악용하는 데 사용될 수 있는 위험 요소를 제거하지 못합니다.
이는 서버가 공격자를 대신하여 의도치 않은 요청을 시작하도록 하는 데 사용될 수 있습니다.
이 취약점은 다음과 같은 세 가지 방식으로 악용될 수 있습니다
[1] 공격자가 정상적인 상황에서는 애플리케이션에 의해서만 액세스 가능한 정보를 외부 서버로 보내서 서버가 중요한 정보를 유출하도록 만들 수 있습니다.
[2] 공격자가 서버가 신뢰할 수 없는 소스에서 정보를 가져와서 이를 처리하거나 저장하거나 사용자에게 표시하도록 만들 수 있습니다.
[3] 서비스가 내부적으로 통신하는 환경에서, 공격자가 서버의 권한을 사용하여 서버가 특정 조치를 수행하도록 만들 수 있습니다.
예:
애플리케이션에 사용자 프로파일을 관리하는 REST API를 노출하는 써드파티 서비스가 포함되어 있습니다.
...
$userPostData = http_build_query($formFields); # 데이터가 POST 요청 $options로 입력됩니다
...
file_get_contents($fetchUserBioAPI, false , stream_context_create($options)); # $service로 지정된 API를 호출하여 조치를 수행합니다
...
이 문제의 악용 사례:
[원래 HTML 형식]
...
<FORM METHOD=GET ACTION="/userData">
<INPUT TYPE=HIDDEN NAME="fetchUserBioAPI" VALUE="https://companydomain.com/user/profile/bio">
...
</FORM>
[조작된 HTML 형식]
...
<FORM METHOD=GET ACTION="/userData">
<INPUT TYPE=HIDDEN NAME="fetchUserBioAPI" VALUE="https://localhost/activeSessions">
...
</FORM>
양식의 원래 의도는 "fetchUserBioAPI" 서비스를 호출하여 사용자 약력을 표시하는 것이었습니다. 요청이 "https://localhost/activeSessions"를 호출하도록 조작하면 서버가 로그인되어 있는 모든 사용자의 활성 세션을 가져오게 됩니다. 이 조치는 관리자만 수행할 수 있도록 제한되어 있었어야 합니다.
호출이 사용자 관리 서비스에서 직접 온 것이 아니라 애플리케이션 서버에서 온 것이므로 요청이 처리됩니다.
샘플 악용: Atlassian Confluence SSRF/원격 코드 실행
[object Object]
Owasp 서버 측 요청 위조:
[object Object]

영향 받는 제품:

이 문제는 다른 유형의 제품에 영향을 미칠 수 있습니다.

수정 권장사항:

일반

다음과 같은 몇 가지 완화 기법이 있습니다
[1] 가능한 경우 요청을 직접 빌드하는 대신 라이브러리 호출을 사용합니다.
[2] 전략: 화이트리스트
허용되는 서버 및 서비스로 구성된 화이트리스트를 작성합니다. 역할 또는 기능별로 작성하는 것이 좋습니다.
[3] 전략: 라이브러리 또는 프레임워크
이 취약점의 발생을 방지하거나 더 쉽게 방지할 수 있는 구문을 제공하는 검증된 라이브러리 또는 프레임워크를 사용합니다.
예를 들어, ESAPI Encoding 컨트롤
https://owasp.org/www-project-enterprise-security-api
또는 이와 비슷한 도구, 라이브러리, 프레임워크를 사용합니다. 이렇게 하면 출력값을 인코딩하는 데 도움이 될 수 있습니다.
[4] 전략: 입력값 유효성 검증
모든 입력값이 악성이라고 가정합니다. "알려진 정상 값 허용" 입력값 유효성 검증 전략을 사용합니다. 즉, 스펙을 엄격하게 준수하는 허용되는 입력값으로 구성된 화이트리스트를 사용합니다. 스펙을 엄격하게 준수하지 않는 입력값은 모두 거부하거나 스펙을 준수하는 값으로 변환합니다. 악성 입력값이나 잘못된 형식의 입력값을 찾아내는 방법에만 의존하지 마십시오(즉, 블랙리스트에 의존하지 않습니다). 단, 블랙리스트는 잠재적 공격을 발견하거나 반드시 거부해야 할 만큼 형식이 잘못된 입력값을 확인하는 데는 유용할 수 있습니다.
입력값 유효성 검증을 수행할 때는 길이, 입력값의 유형, 허용되는 값의 전체 범위, 누락되었거나 불필요한 입력값, 구문, 관련 필드에서의 일관성, 비즈니스 규칙 준수 여부를 포함하여 잠재적으로 관련 있는 모든 특성을 고려합니다. 비즈니스 규칙 로직을 예로 들면, "boat"는 영숫자 문자만 포함하기 때문에 구문적으로 유효할 수 있지만 "red" 또는 "blue"와 같은 색상이 필요한 경우에는 유효하지 않습니다.
OS 명령 문자열을 구성할 때는 요청에 포함된 매개변수의 필요한 값을 기반으로 문자 세트를 제한하는 엄격한 화이트리스트를 사용합니다. 이렇게 하면 간접적으로 공격의 범위가 제한되긴 하나, 이 기법은 올바른 출력값 인코딩과 이스케이핑에 비해 중요도가 떨어집니다.
입력값 유효성 검증을 통해 어느 정도의 심층 방어를 제공할 수는 있지만, OSS 명령 삽입을 방지하는 가장 효과적인 방법은 올바른 출력값 인코딩, 이스케이핑 및 따옴표를 사용하여 출력값에 표시되는 내용을 제한하는 것입니다. 입력값 유효성 검증은 OS 명령 삽입을 항상 방지하는 것은 아니며, 특히 임의의 문자를 포함할 수 있는 자유 형식 텍스트 필드를 지원해야 하는 경우 OS 명령 삽입을 방지하기 어렵습니다. 예를 들어, 메일 프로그램을 호출할 때는 제목 필드에 ";" 및 ">" 문자와 같이 위험할 수 있는 입력값을 포함하는 것을 허용해야 할 수 있는데, 이러한 문자는 이스케이핑하거나 그 밖의 방식으로 처리해야 합니다. 이 경우 해당 문자를 삭제하면 OS 명령 삽입의 위험을 줄일 수 있으나 제목 필드가 사용자의 의도대로 기록되지 않게 되어 올바르지 않은 동작이 발생하게 됩니다. 이는 사소한 불편처럼 보일 수 있으나 다른 구성 요소로 메시지를 전달하려면 잘 구성된 제목 줄이 필요한 프로그램에서는 중요한 요인이 될 수 있습니다.
유효성 검증에서 실수한 경우에도(예: 100개의 입력값 필드 중 1개를 잊어버린 경우) 적절한 인코딩이 이루어졌다면 삽입 기반 공격을 방어하는 것이 가능합니다. 입력값 유효성 검증은 검증이 격리되어 이루어지지 않은 한 공격 표면을 크게 줄여 주고 일부 공격을 감지할 수 있게 해 주며 올바른 인코딩만으로는 가능하지 않은 그 밖의 보안 이점을 제공해 주는 유용한 기법입니다.
[5] 전략: 환경 강화
해당 태스크를 실행하는 데 요구되는 최소한의 권한을 사용하여 코드를 실행합니다
https://buildsecurityin.us-cert.gov/daisy/bsi/articles/knowledge/principles/351.html
가능한 경우, 하나의 태스크용으로만 사용할 제한된 권한을 갖는 격리된 계정을 작성합니다. 이렇게 하면 공격이 성공하더라도 공격자가 소프트웨어 또는 환경의 나머지 부분에 곧바로 액세스할 수 없습니다. 예를 들어, 일상적인 운영 상황에서는 데이터베이스 애플리케이션을 데이터베이스 관리자 권한으로 실행해야 하는 경우가 드뭅니다.

CWE:

918

누락되었거나 안전하지 않은 "X-Content-Type-Options" 헤더

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.
"X-Content-Type-Options" 헤더(값 "nosniff")는 IE 및 Chrome에서 응답의 content-type을 무시하지 않도록 합니다.
이 조치는 신뢰할 수 없는 컨텐츠(예: 사용자가 업로드한 컨텐츠)가 사용자 브라우저에서 실행되지 않도록 차단할 수 있습니다(예: 악성 이름 지정 후).

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

수정 권장사항:

일반

모든 발신 요청에 "X-Content-Type-Options" 헤더를 "nosniff" 값으로 보내도록 서버를 구성합니다.
Apache의 경우 다음을 참조하십시오:
http://httpd.apache.org/docs/2.2/mod/mod_headers.html
IIS의 경우 다음을 참조하십시오:
https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspx
nginx의 경우 다음을 참조하십시오:
http://nginx.org/en/docs/http/ngx_http_headers_module.html

CWE:
200

외부 참조:
유용한 HTTP 헤더 목록
MIME 형식 보안 위험 감소

누락된 "Content-Security-Policy" 헤더

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 수집하는 것이 가능합니다
속기 쉬운 사용자를 설득해서 사용자 이름, 비밀번호, 신용카드 번호, 주민등록 번호와 같은 민감한 정보를 제공하도록 하는 것이 가능합니다.
CSP가 없거나 올바르지 않은 값으로 설정된 경우 웹 애플리케이션이 XSS, 클릭재킹 등에 취약해질 수 있습니다.
"Content-Security-Policy" 헤더는 브라우저가 페이지를 렌더링하는 방식을 수정하여 XSS(Cross-Site Scripting)를 비롯한 여러 크로스 사이트 인젝션으로부터 보호하도록 설계되었습니다. 웹 사이트의 올바른 오퍼레이션을 방지하지 않도록 헤더 값을 올바르게 설정하는 것이 중요합니다. 예를 들어, 헤더가 인라인 JavaScript의 실행을 방지하도록 설정된 경우, 웹 사이트는 페이지에서 인라인 JavaScript를 사용하지 않아야 합니다.
XSS(Cross-Site Scripting), Cross-Frame Scripting 및 클릭재킹으로부터 보호하려면 다음 정책을 올바른 값으로 설정하는 것이 중요합니다:
'default-src' 및 'frame-ancestors' 정책 *또는* 'script-src', 'object-src' 및 'frame-ancestors' 정책.
'default-src', 'script-src' 및 'object-src'의 경우 '*', 'data:', 'unsafe-inline' 또는 'unsafe-eval'과 같은 안전하지 않은 값은 사용하지 않아야 합니다.
'frame-ancestors'의 경우 '*' 또는 'data:'와 같은 안전하지 않은 값은 사용하지 않아야 합니다.
또한 'script-src' 및 'default-src'('script-src'의 대체 지시어)의 경우 'self'는 안전하지 않은 것으로 간주되므로 피해야 합니다.
자세한 정보는 다음 링크의 내용을 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 "Content-Security-Policy" 헤더를 전송하도록 구성하십시오.
Content-Security-Policy 헤더를 지시문에 대해 아래와 같이 보안 값으로 구성하는 것이 권장됩니다
'default-src' 및 'script-src'의 경우 'none' 또는 https://any.example.com과 같은 보안 값을 사용해야 합니다.
'frame-ancestors' 및 'object-src'의 경우 'self', 'none' 또는 https://any.example.com과 같은 보안 값을 사용해야 합니다.
"unsafe-inline" 및 "unsafe-eval"은 어떤 경우에도 사용해서는 안 됩니다. 임시어 / 해시는 단기적인 우회 방법으로만 고려됩니다.
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:

1032

외부 참조:

몇 가지 보안 헤더의 목록
컨텐츠 보안 정책 소개
MDN 웹 문서 - Content-Security-Policy

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

지나치게 허용적인 CORS 액세스 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.
CORS(Cross-Origin Resource Sharing)는 웹 사이트가 자원을 복제할 필요없이 외부 사이트의 자원을 요청할 수 있도록 허용하는 메커니즘입니다.
외부 사이트에 대한 액세스를 부여할 때 권한 부여 사이트에서 다양한 조치를 수행하고 스크립트를 실행할 수 있습니다.
따라서 모든 사이트가 아닌 신뢰할 수 있는 사이트에 대해서만 액세스 권한을 부여하는 것이 매우 중요합니다.

영향 받는 제품:

이 문제는 다른 유형의 제품에 영향을 미칠 수 있습니다.

수정 권장사항:

일반

신뢰할 수 있는 사이트의 목록을 준비하고 이를 ""Access-Control-Allow-Origin" 헤더의 값으로 설정하십시오.
외부 액세스가 필요하지 않은 경우 이 헤더를 완전히 제거하십시오.

CWE:

200

외부 참조:

원본 간 자원 공유 사용

누락된 "Referrer policy" 보안 헤더

TOC

원인:

안전하지 않은 웹 애플리케이션 프로그래밍 또는 구성

위험:

사용자 이름, 암호, 컴퓨터 이름 및/또는 중요한 파일 위치 등과 같이 웹 애플리케이션에 대한 민감한 정보를 수집할 수 있습니다.
순수한 사용자가 사용자 이름, 암호, 신용 카드 번호, 주민 등록 번호 등의 민감한 데이터를 제공하도록 설득할 수 있습니다.
Referrer Policy의 값이 없거나 부적절하면 자체 URL 유출이 발생할 수 있으며 URL에 포함된 민감한 정보도 크로스 사이트로 유출됩니다.
Referrer Policy가 있는지 검사하고, 있는 경우 구성을 테스트하기 위한 규칙 집합의 일부입니다. "Referer Policy" 헤더는 Referer 헤더에서 사용할 수 있는 데이터와 대상(document.referrer)의 navigation 및 iframes에서는 사용할 수 있는 데이터를 정의합니다. 이 헤더는 브라우저가 페이지를 렌더링하는 방법을 수정하고 도메인 간 Referer 유출을 방지하도록 설계됩니다. 웹 사이트의 적절한 운영을 막지 않는 방식으로 헤더 값을 올바르게 설정해야 합니다.
Referer 헤더는 트래픽이 발생한 사이트를 나타내는 요청 헤더입니다. 적절한 방지 대책이 없으면 URL 자체 그리고 URL에 포함된 민감한 정보도 크로스 사이트로 유출됩니다.
"no-referrer-when-downgrade" 및 "unsafe-url"은 타사 사이트에 대한 전체 URL을 유출하는 정책입니다. 나머지 정책은 "no-referrer", "origin", "origin-when-cross-origin","same-origin", "strict-origin", "strict-origin-when-cross-origin"입니다.
자세한 내용을 다음 링크를 참조하십시오.

영향 받는 제품:

이 문제는 여러 유형의 제품에 영향을 줄 수 있습니다.

수정 권장사항:

일반

"Referrer Policy" 헤더를 보내도록 서버를 구성합니다.
아래와 같은 지시문에 대해 안전한 값을 사용하여 Referrer Policy 헤더를 구성하는 것이 좋습니다.
"strict-origin-when-cross-origin"은 더 많은 프라이버시를 제공합니다. 이 정책을 사용하면 크로스 원본 요청의 Referer 헤더에서 원본만 전송됩니다.
Google Chrome의 경우 다음을 참조하십시오.
https://developers.google.com/web/updates/2020/07/referrer-policy-new-chrome-default
Firefox의 경우 다음을 참조하십시오.
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy.

CWE:

200

외부 참조:

MDN 웹 문서 - Referrer-Policy

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)

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.6837a453.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.6837a453.js

```
/*! For license information please see main.6837a453.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 0

TOC

이름	첫세트	도메인	보안	HTTP만	Same Site	JS 스택 추적
값	요청 URL		만료			