http://www.jsebs.org
ISSN: 2288-3908

The Journal of Society for e-Business Studies
Vol.24, No.2, May 2019, pp.15-27
https://doi.org/10.7838/jsebs.2019.24.2.015

제어시스템의 웹 취약점에 대한 현황과 연구

A Study on ICS/SCADA System Web Vulnerability

김희현(Hee-Hyun Kim)*, 유진호(Jinho Yoo)**

초 록

과거의 제어 시스템은 외부 네트워크와 연결되지 않은 폐쇄망이라 그 자체로 보안성을 보장받을 수 있었으나 최근에는 관리의 편이성 등을 위해 외부로 연결시켜 놓은 사례가 많으며, 폐쇄망이라고 주장을 하나 어느 한 접점은 인터넷과 연결되어 있어 운영 중인 제어시스템이 점점 늘어나는 추세이다.

이에 따라 외부 연결로 인해 해커들이 제어시스템을 목표로 다양한 공격 시도를 할 수 있게 되었으며 다양한 보안 위협에 노출되어 공격의 타겟이 되고 있는 실정은 당연한 것이다. 외부에 연결되어 있는 산업제어시스템은 웹서비스 또는 원격 관리를 위한 원격관리 포트가 대부분 연결되어 있으며 웹 프로그램을 통한 웹 서비스의 확대는 제어시스템도 예외는 아니므로 일반적인 웹 취약점을 그대로 상속하고 있다.

본 연구에서는 공격자 입장에서 제어시스템을 대상으로 가장 많이 시도되는 웹 해킹 공격을 도출하기 위해 기존의 웹 취약점 항목을 분류 및 비교하였으며 이를 통해 제어시스템 필수 웹 취약점을 선별하였으며 또한 누락된 취약점이 있는지 검토하고 확인하고 자 하였다.

ABSTRACT

In the past, the control system was a closed network that was not connected to the external network. However, in recent years, many cases have been opened to the outside for the convenience of management. Are connected to the Internet, and the number of operating control systems is increasing.

As a result, it is obvious that hackers are able to make various attack attempts targeting the control system due to external open, and they are exposed to various security threats and are targeted for attack. Industrial control systems that are open to the outside have most of the remote management ports for web services or remote management, and the expansion of web services through web programs inherits the common web vulnerability as the control system is no exception.

In this study, we classify and compare existing web vulnerability items in order to derive the most commonly tried web hacking attacks against control system from the attacker 's point of view. I tried to confirm.

키워드 : 제어시스템, 웹 취약점, ICS/SCADA System
Industry Control System, Web Vulnerability, ICS/SCADA System

* First Author, Department of Business Administration, Sangmyung University(h4ckkioo@naver.com)
** Corresponding Author, Department of Business Administration, Sangmyung University(jhyoo@smu.ac.kr)
Received: 2018-11-29, Review completed: 2019-02-25, Accepted: 2019-02-28

1. 서 론

제어시스템의 정의는 이미 많은 문서에서 인용이 되고 있다. 일반적으로 'ICS(Industrial Control System, 산업제어시스템)'라고 불리며, 감시제어 및 데이터취득(Supervisory Control And Data Acquisition)을 뜻하는 SCADA와 붙여 'ICS/SCADA'로 통칭하기도 한다.

제어시스템은 원격의 설비에 대하여 측정,계측 및 설비 동작 상태를 감시하고 제어하는 컴퓨터 시스템, 필드장치, 통신장치 등을 포함하는 모든 종류의 산업용 시스템을 통칭한다.

사용 환경과 운영 목적, 구조 또는 시스템 운영 형태에 따라서 에너지(가스/오일 파이프라인, 발전, 송/배전, 변전시스템, 전력거래 등), 교통(항공, 철도 산업 등), 수자원 관리 등과 같이 원거리에 있는 시스템을 원격으로 감시/제어할 수 있는 원방감시제어시스템(SCADA, Supervisory Controland Data Acquisition),일정 지역 내의 제어시스템 하부설비를 단위 그룹으로 분산시켜 제어하는 분산제어시스템(DCS, Distributed ControlSystem) 또는 산업제어시스템(ICS, Industrial Control System)이라고 한다.

제어시스템은 장치마다 상호간 또는 외부기기와 연결하여 각각의 장치에 대한 원격접근과 제어가 가능하고, 여러 명령 및 조작이 가능하도록 양방향 통신서비스 환경을 구축하고 있으며, 장치마다 상호간 또는 외부기기와 연결하여 각각의 장치에 대한 원격접근과 제어가 가능하고, 여러 명령 및 조작이 가능하도록 양방향 통신서비스 환경을 구축하고 있으며, 산업 플랜트, 전력의 생산과 분배, 열차 및 항공 등의 교통 인프라 제어, 댐 및 송유관 등 각종 자원의 감시와 제어에 이르기까지 중요기반설비에 다양하게 사용되고 있다[2, 5, 6, 8, 9, 12, 16].

정보통신기반보호법은 이를 국가안전보장·행정·국방·치안·금융·통신·운송·에너지 등의 업무와 관련된 전자적 제어·관리시스템이라고 정의한다.

주요기반시설을 관리하는 제어시스템(ICS)은 과거 특화된 소프트웨어, 하드웨어, 자체통신 프로토콜사용 및 일반 인터넷망과 분리시켜 격리되어 있는 폐쇄 네트워크(closed network)에서 최근에는 경영관리의 효율화 및 일반적인 인터넷 기반 네트워크(Internet-based network) 시스템과의 호환성을 위해 개방화, 표준화, 범용화로 변화되면서 다양한 보안 위협 및 취약성이 외부에 노출되고 있으며 공격도 증가하고 있다[16].

본 연구가 제안하는 제어시스템의 웹 취약점 분석 및 평가 방법론은 제어시스템의 웹 공격에 대해 분류를 통해 취약점의 종류와 문제점을 파악하여 산업제어시스템의 안전성을 확보하고 해킹사고와 산업재해를 미연에 방지하고, 제어시스템의 웹 개발자, 운영자 및 보안관리자 등이 활용할 수 있으며, 본 연구의 결과는 제어시스템의 웹 취약성 점검 및 웹 시스템의 보안성 평가에 활용될 수 있다.

2. 선행연구 및 연구 문제 제기

2.1 선행 연구

기존의 웹 취약점에 대해 공식적으로 발표된 가이드나 문서는 다수 존재하나 제어시스템의 웹 취약점에 대해서 특화되어 연구된 문서는 쉽게 찾을 수가 없어 기존의 웹 취약점에 대해 공식적으로 발표된 가이드 문서 등과 현재 실

제로 보안업체에서 사용 중인 체크리스트 등을 참고하여 분석을 수행하였다.

본 논문에서 기존의 웹 취약점에 대해 발표된 문서 중 참고하여 분석한 문서는 아래와 같다.

총 아래 10개의 가이드 및 문서를 토대로 분석을 수행하였다.

1. OWASP Top 10 - 2103[14]
2. OWASP Top 10 - 2107[15]
3. 안행부 전자정부SW 개발 운영자를 위한 소프트웨어 개발 보안 가이드[18, 20, 21]
4. KISA 홈페이지 취약점 진단·제거 가이드[7]
5. CWE/SANS[1, 17]
6. 미래창조과학부, 주요정보통신기반시설 취약점 분석·평가 기준[11, 19]
7. 국정원 8대 취약점[13]
8. 웹응용프로그램 개발보안 가이드 2010[10]
9. 대기업 P사 24개 점검 항목
10. N사 제어시스템 모의해킹 전문업체 점검 항목

또한 현재 실제로 제어시스템 진단을 위해 사용 중인 웹 취약점 점검 항목으로 참고한 것은 제어시스템을 전문적으로 진단하는 업체 N사와 대기업 P사의 문서를 참고하였다.

2.2 연구 문제의 제기

많은 기관과 기업체는 자체관리 시스템의 웹 취약점 항목이나 웹 취약점 점검 항목을 구성함에 있어서 대외적인 자료를 그대로 사용하거나 일부 자체적으로 구성하여 관리를 하고 있다. 하지만 제어시스템에 맞는 웹 취약점 항목을 별도로 선별하여 관리하는 기관이나 업체는 없다. 일부 대기업과 제어시스템 전문업체에 문의 결과 별도로 제어시스템 웹 취약점 항목을 별도로 관리하고 있지 않고 있으며 기존의 웹 취약점 항목을 그대로 사용하고 있다.

이를 위해 각각의 가이드나 문서가 서로 어떠한 특징과 차이점이 있는지 연구하고 대표적인 ICS 관련 사이트 두 곳의 정보를 조사하여 분석을 통해 시사점을 도출하고자 한다. 이에 따라 제어시스템에 알맞는 웹 취약점 항목을 만들어서 활용하고자 한다.

대표적인 ICS 관련 사이트는 ICS-CERT와 SVE이며 간략한 설명은 아래와 같다.

ICS-CERT(Industrial Control Systems Cyber Emergency Response Team)[4]는 미국 ICS 침해사고 대응팀이며 홈페이지는 https://ics-cert.us-cert.gov이다. 미국 국토 안보부 소속의(DHS)의 국가 사이버보안 통신 통합센터 및 산업제어시스템 비상 대응팀 (NCCIC/ICS-CERT)이다.

National Cybersecurity and Communications Integration Center(NCCIC)는 미국의 대표적인 사이버 방어, 사고 대응 및 운영 통합 센터이며, 국가의 전산화 된 사이버 보안과 의사소통에 대한 위험을 줄이려는 것이 설립 목적이다.

SCADA Vulnerabilities & Exposures(SVE)[22]란 CRITIFENCE® 사에서 제공하는 SCADA 취약성 및 노출 데이터베이스(SVE)이다.

CRITIFENCE® 사는 중요 인프라, SCADA 및 OT(Operational Technology) 네트워크를 전문으로 하는 사이버 보안 벤더로써 SCADA 취약성 및 노출 데이터베이스(SVE)를 웹상에 제공하고 있다.

운영 기술(Operational Technology, OT)은 관리 운영과 달리 산업 운영을 관리하는 데 사용되는 컴퓨팅 시스템을 의미하며, 밸브, 펌프 등과 같은

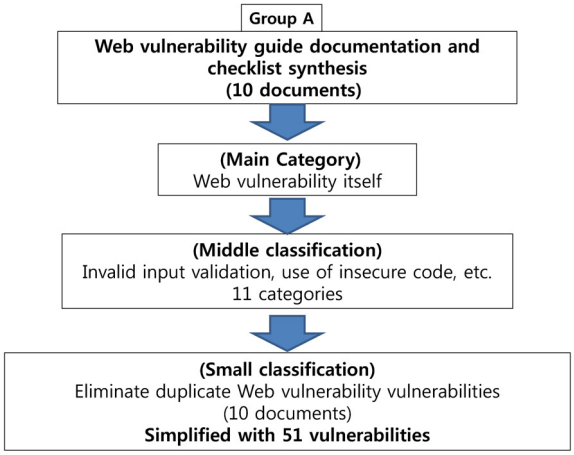
물리적 장치의 직접적인 모니터링 및 제어를 통해 물리적 프로세스의 변화를 탐지하거나 유발시키는 하드웨어 및 소프트웨어를 말한다[3].

3. 연구방법

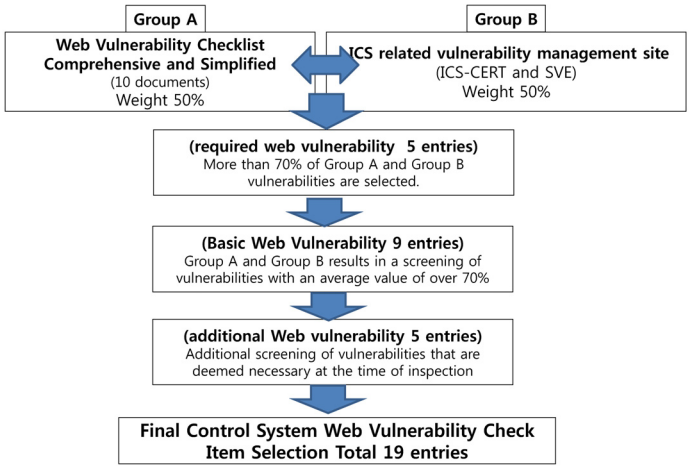
이해를 돕기 위해 아래의 그림과 같이 도식화하여 연구의 흐름에 대해 기술하였다.

3.1 연구 대상 선정

앞에서 언급한 기존의 웹 취약점에 대해 발표된 가이드 문서 및 체크리스트 등을 참고하여 분석을 수행하였으며 1차적으로는 각각의 가이드에서 발표한 취약점 항목을 나열화한 뒤 공통



〈Figure 1〉 Control System Web vulnerability in large/Small/Small Classification



〈Figure 2〉 Flow of Research on Control System Web Vulnerability

적인 취약점을 서로 단순화하여 정리하였다.

동일한 취약점을 표현상 다르게 표기한 취약점도 모두 간소화 하거나 그룹화 하여 표기된 항목을 기준 XSS(Cross Site Script) 취약점, SQL Injection 취약점 포함 총 51개의 웹 취약점으로 각각 단순화 하였다.

그리고 각각의 취약점을 중분류하기 위해 아래의 중분류를 11개 항목으로 정리하였다.

부적절한 입력값 검증은 21개 취약점, 비안전한 코드 사용 취약점은 2개 취약점, 부적절한 인증, 인가 취약점은 3개 취약점, 통신 취약점 2개, 보안기능 관련 취약점 3개 취약점, 허용/권한 및 접근 통제 취약점 1개, 정보노출 취약점 2개, 에러처리 취약점 1개, API 오용 취약점 1개, 공개프로그램 취약점 3개, 부적절한 환경설정 취약점 12개로 중분류를 하였다.

3.2 취약점 항목별 가중치 선정

공통적인 취약점으로 분류 및 구분한 취약점 항목에 대해 앞서 설명한 OWASP TOP 10 등 각각의 10개의 가이드 및 체크리스가 해당되는 항목을 표기하였으며 이 부분에 대해 가중치 50%를 적용하였다.

그리고, 실제 공식적으로 취약점 항목으로 발표된 ICS-CERT와 SVE의 취약점 번호를 토대로 분류한 취약점 항목에 해당 되는지 표기하였으며 이부분에 대해서도 가중치 50%를 적용하였다.

<Table 1>은 적용한 취약점 항목별 가중치에 대한 내용이다.

총 합계 가중치를 100%로 산정하였으며 Group A, Group B 취약점 중 각각 가중치가 70%가 넘는 취약점을 제어시스템의 필수 웹 취약점 항목으로 선별하였다. 그리고 Group A, Group B의 결과 평균값이 70% 이상인 취약점에 대해 기본 웹 취약점 항목으로 선별하였다.

그렇지만 합 가중치가 70%가 넘지 않은 취약점 중 점검시 꼭 필요하다고 판단되는 취약점을 추가 선별하여 최종 웹 취약점 항목으로 도출하도록 하였다.

마지막으로 필수 취약점과 기본 취약점, 추가 취약점을 모두 목록화 하여 제어시스템 웹 취약점 점검 항목으로 최종 선별하여 도출하였다.

4. 제어시스템 웹 취약점 점검 항목 분석 결과

4.1 최초 웹 취약점 점검 항목 그룹핑

최초 웹 취약점 점검 항목을 그룹핑하기 위하여 앞에서 언급한 기존의 웹 취약점에 대해 발표된 가이드 문서 및 체크리스트 등을 활용하여 분석을 수행하였다. 취약점 항목을 단순화하기 위해 대/중/소 분류로 재분류를 하였으며, 제어시스템의 웹 취약점 자체를 대분류로, 중분류는 11개의 항목으로 그룹핑 하였으며, 소분류는 총 51개 웹 취약점 항목으로 선정하였다.

〈Table 1〉 Weight by Vulnerability Item

Number	Resources	weight
1	10 guides and documents(Group A)	50%
2	ICS-CERT and SVE Actual Vulnerability(Group B)	50%

중분류의 각각의 취약점 항목은 부적절한 입력값 검증, 비안전한 코드 사용, 부적절한 인증/인가, 부적절한 입력값 검증, 통신, 보안기능, 허용 권한 및 접근통제, 정보노출, 에러처리, API 오용, 공개 프로그램 취약점, 부적절한 환경 설정 등 11개 항목으로 중분류를 하였다.

그 분류 결과는 <Table 2>와 같다.

그리고 각각의 취약점을 취약점 별로 그룹핑하여 총 51개 웹 취약점 항목으로 소분류 하였다. 아래표의 각각의 취약점 항목 앞에 번호(1, 2, 3 …… 등)는 그래프 또는 차트의 항목을 구분하기 위하여 삽입하였다.

51개 소분류 웹 취약점 항목은 아래 <Table 3>과 같다.

〈Table 2〉 11 Items in Middle Class

Vulnerability(Medium)
Input data verification and representation (improper input value verification)
Use unsafe code
Inappropriate authentication, authorization
Communication
Security Features
Allow, Authority and Access Control
Information exposure
Error handling
API misuse
Public program vulnerability
Improper configuration

〈Table 3〉 51 Sub Categories Web Vulnerability Items

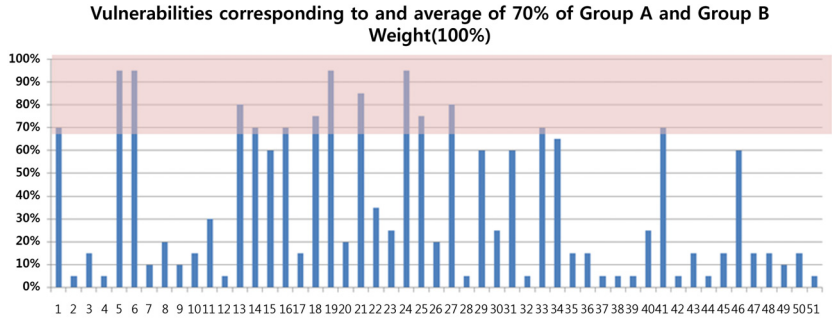
Vulnerability(Medium)	Vulnerability(Small)
Input data verification and representation (improper input value verification)	1. Memory BOF
	2. Integer type OverFlow
	3. Insert format string
	4. Boundary check
	5. SQL Insert
	6. XSS
	7. XQuery Insert(Injection)
	8. Xpath Insert(Injection)
	9. SSI Insert(Injection)
	10. LDAP Insert(Injection)
	11. XML Outer object(XXE) Injection
	12. DOS Attack
	13. Insert/execute operating system commands(command Injection)
	14. Connect automatically to untrusted URL addresses
	15. HTTP response splitting
	16. Impersonation of other user rights due to cookie value tampering
	17. Exposing critical information with application design errors(hidden field etc)
	18. Upload dangerous format files
	19. File Download Vulnerability
	20. Unauthorized use of services due to web application parameter tampering(Parameter modulation, LFI, RFI etc)
	21. Cross Site Request Forgery(CSRF)

〈Table 3〉 51 Sub Categories Web Vulnerability Items (Continued)

Use unsafe code	22. Using unsafe functions
	23. Use weak encryption algorithms
Inappropriate authentication, authorization	24. Authentication Bypass, Absence of certification
	25. Improper authorization
	26. Weak Session Management
Communication	27. Important Information Save/Transfer Plain Text
	28. Unsafe protocol(SSL Old version, etc)
Security Features	29. Inappropriate password policy applied(password unused, service privilege exploit due to vulnerable web account existence, password guessing possible)
	30. Account Brute Forcing attack Poor response
	31. Source information(such as system critical information contained in comments), hard-coded passwords, hard-coded encryption keys
Allow, Authority and Access Control	32. Ability to modify business logic with application design errors (client script, etc.)
Information exposure	33. Excessive user privacy exposure to administrators
	34. Exposure of personal information through search engines(such as Google)
Error handling	35. Excessive error message exposure, exposure of system data information
API misuse	36. Use vulnerable APIs(use weak components)
Public program vulnerability	37. Zero Board Vulnerability(XE BOARD)
	38. WordPress Vulnerability
	39. TechNotes vulnerability
Improper configuration	40. Directory Listing(indexing) due to insufficient server settings
	41. Incorrect permission settings for critical resources
	42. Incomplete web server security patches
	43. Exploiting HTTP Method
	44. WebDAV Vulnerability
	45. Incorrect security configuration
	46. Insufficient logging and monitoring
	47. Exposure of information due to application default page
	48. Admin page exposure
	49. Vulnerability due to inferable file or directory names
	50. unnecessary files in the server(test page exists at development), backup files
	51. Inappropriate password policy applied(password unused, service privilege exploit due to vulnerable web account existence, password guessing possible)

4.2 Group A, Group B의 합 평균 70% 이상 해당 항목 선별

위의 10개의 가이드(Group A, 가중치 50%)와 ICS-CERT와 SVE의 2개의 취약점 리스트(Group B, 가중치 50%)를 종합하였을 경우 평균 70% 이상인 취약점을 별도로 뽑아 보면 총 14개의 취약점 항목이 도출되며, 이 취약점은 제어시스템 웹 취약점 점검을 할 때 포함되어야 할 기본 항목으로 판단된다.



〈Figure 3〉 Vulnerabilities Corresponding to an Average of 70% of Group A and Group B

〈Table 4〉 Vulnerabilities Corresponding to an Average of 70% of Group A and Group B

Vulnerability(Medium)	Vulnerability(Small)
Input data verification and representation (improper input value verification)	1. Memory BOF
	5. SQL Insert
	6. XSS
	13. Insert/execute operating system commands(command Injection)
	14. Connect automatically to untrusted URL addresses
	16. Impersonation of other user rights due to cookie value tampering
	18. Upload dangerous format files
	19. File Download Vulnerability
	21. Cross Site Request Forgery(CSRF)
Inappropriate authentication, authorization	24. Authentication Bypass, Absence of certification
	25. Improper authorization
Communication	27. Important Information Save/Transfer Plain Text
Information exposure	33. Excessive user privacy exposure to administrators
Improper configuration	41. Incorrect permission settings for critical resources

<Figure 3>을 보면 두개의 항목(Group A, Group B)의 평균이 70%인 항목은 1, 5, 6, 13, 14, 16, 18, 19, 21, 24, 25, 27, 33, 41임을 알 수 있다.

이 14개 기본 취약점 항목에는 필수 취약점 항목 5개를 포함하고 있으며 각 항목은 5, 6, 19, 21, 24이다.

4.3 추가 취약점 항목 별도 선별

그리고 위의 항목에는 선별되지는 않았지만 웹 모의해킹 경험상 추가되어야 할 취약점을 별도로 선정하였다.

그 항목은 아래 <Table 5>와 같으며 5개 항목을 선별하였다.

〈Table 5〉 Additional Items

Vulnerability (Medium)	Vulnerability(Small)
Input data verification and representation(improper input value verification)	12. DOS Attack
	15. HTTP response splitting
Security Features	29. Inappropriate password policy applied(password unused, service privilege exploit due to vulnerable web account existence, password guessing possible)
	31. Source information(such as system critical information contained in comments), hard-coded passwords, hard-coded encryption keys
Information exposure	34. Exposure of personal information through search engines(such as Google)

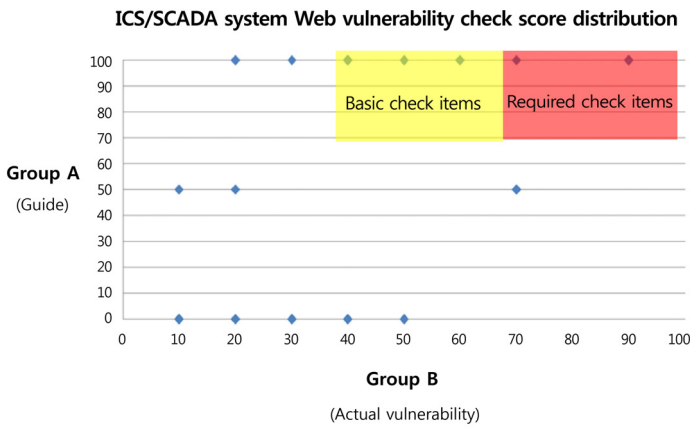
4.4 최종 취약점 항목 선별

종합하여 보면 50%를 적용한 Group A 취약점 중 7개 이상 가이드를 채택하고 있는 취약점을 먼저 선별하였고, ICS-CERT와 SVE의 취약점 번호를 토대로 분류한 Group B 취약점 항목의 둘 다 해당되는 취약점에 대해 가중치 50%를 적용하여 웹 취약점 기본 점검 항목으로 선별하였다.

총 합계 가중치를 100%로 산정하였으며 Group A와 Group B에 대해 각각 70% 이상 해당되는 취약점을 제어시스템의 웹 취약점 필수 점검 항목으로 선별하였다.

〈Table 6〉 Final ICS/SCADA System Web Vulnerability Item

Vulnerability(Medium)	Vulnerability(Small)
Input data verification and representation (improper input value verification)	1. Memory BOF
	5. SQL Insert
	6. XSS
	12. DOS Attack
	13. Insert/execute operating system commands(command Injection)
	14. Connect automatically to untrusted URL addresses
	15. HTTP response splitting
	16. Impersonation of other user rights due to cookie value tampering
	18. Upload dangerous format files
	19. File Download Vulnerability
	21. Cross Site Request Forgery(CSRF)
Inappropriate authentication, authorization	24. Authentication Bypass, Absence of certification
	25. Improper authorization
Communication	27. Important Information Save/Transfer Plain Text
Security Features	29. Inappropriate password policy applied(password unused, service privilege exploit due to vulnerable web account existence, password guessing possible)
	31. Source information(such as system critical information contained in comments), hard-coded passwords, hard-coded encryption keys
Information exposure	33. Excessive user privacy exposure to administrators
	34. Exposure of personal information through search engines(such as Google)
Improper configuration	41. Incorrect permission settings for critical resources



〈Figure 4〉 ICS/SCADA System Web Vulnerability Check Score Distribution Chart

그렇지만 합 가중치가 70%가 넘지 않은 취약점 중 점검 시 꼭 필요하다고 판단되는 취약점을 추가 선별하여 최종 웹 취약점 항목으로 선별하였다.

최종적으로 제어시스템 웹 취약점 항목으로 선별된 19개 항목은 <Table 6>과 같다.

총 51개 취약점 항목의 GroupA의 점수를 X축으로 하고, Group B의 점수를 Y축으로 하여 점수 분포를 나타내어 보면 <Figure 4>와 같다.

위의 차트를 보면 차트의 왼쪽 상단의 노란색 부분이 기본 점검 항목에 포함된다. 오른쪽 상단의 빨간색 부분은 점검 필수 항목에 포함됨을 알 수 있으며, 기본 점검 항목을 포함 하고 있다.

또한 제어시스템 웹 취약점 시 필수 점검 항목과 기본 점검 항목의 분포를 알 수 있으며 Gruop B의 점수가 100이 되어야만 필수 점검 항목 또는 기본 점검 항목에 포함 될 수 있음을 알 수 있다. 그리고 시작점 보다 멀리 떨어져 있는 취약점이 선별되었음을 알 수 있으며, 원점에서 멀리 떨어져 있을수록 필수 또는 기본 점검항목에 채택될 가능성도 높다는 것을 알 수 있다.

5. 결 론

최근의 추세를 살펴보면 우리는 제어시스템이 우리 일상생활에 미치는 영향이 매우 높음을 잘 알고 있음에도 불구하고 인터넷과 연결을 하려는 시도는 꾸준히 발생하고 있으며, 각 기업이나 기관에서는 우리의 제어시스템은 폐쇄망이라고 주장을 하지만 속을 들여다보면 어딘가 인터넷과 연결을 할수 있는 접점이 존재하는 경우가 많다는 것을 알 수 있다.

인터넷과의 연결이 거스를 수 없는 추세라고 하면 이젠 안전을 위해 보안을 더 견고히 할 수 밖에 없을 것으로 판단된다.

그 중에서도 외부에 가장 빈번히 노출되는 웹 환경과 리모트 관리 환경에 대해 무엇보다도 관리적, 기술적으로 신경을 써서 보안을 유지해야 할 것이다.

지금까지 본 연구에서는 OWASP, KISA, 국정원, 안행부 등에서 발표한 가이드의 웹 취약점 항목을 비교하고 일반 웹 취약점 항목 중 제어시스템에서 필수적으로 점검하여야 할 웹 취약점 항목이 무엇인지를 분석하여 도출하였다.

또한 웹 취약점의 전반적인 내용을 조사하여 제어시스템에 국한된 웹 취약점 점검을 하여할 항목을 도출하고 또한 활용될 수 있도록 연구하였다.

구체적으로는 먼저 외부에 공개되어 있는 일반 웹 취약점의 항목을 분석하였으며, 인터넷에 공개 되어 있는 일반적인 웹 취약점 항목에 대해 그룹핑 및 단순화를 하여서 51개 항목으로 최소화하였다.

이 항목을 기반으로 우리가 조사한 10개의 문서나 가이드(Group A)중 7개 이상을 채택하고 있는 취약점 7개 항목을 선별하였으며, ICS-CERT와 SVE 사이트(Group B)를 통해 실제 제어시스템 웹 취약점으로 보고된 항목 중 두 사이트 모두에서 채택하고 있는 취약점 17개 항목을 선별하였다. 그리고 위의 Group A와 Group B에 대해 가중치를 각각 50%로 적용하였다.

Group A와 Group B에 대해 각각 70% 이상 해당되는 취약점을 선별하여 취약점 5개 항목을 제어시스템의 웹 취약점 필수 점검 항목으로 선별하였다. 그리고 Group A와 Group B에 대해 각각 가중치 50%를 적용한 결과에 대한 합 평균을 구하여 70%가 넘는 취약점 14개를 웹 취약점 기본 점검 항목으로 선별하였다. 이 14개 기본 취약점 항목에는 필수 취약점 항목 5개를 포함하고 있다.

하지만 위의 기본 및 필수 취약점 항목에는 포함되지 않았지만 점검 시 꼭 필요하다고 판단되는 취약점 5개를 추가 선별하여 추가 웹 취약점 항목으로 선별하였다. 최종적으로 제어시스템 웹 취약점 항목으로 선별된 19개 항목이 선별되었다.

본 연구의 한계점은 Group B의 표본의 수가 CS-CERT와 SVE의 2개의 취약점 사이트만을 대상으로 선정하여 점검 사이트의 수가 작다는 한계점을 가지고 있다.

본 논문은 기존 웹 취약점을 기반으로 연구를 하였기 때문에 기존의 웹 취약점은 기본이며 이번에 연구한 제어시스템의 웹 취약점과 향후에는 IoT(Internet of Thing) 장비의 웹 취약점 항목을 연구하는 데에도 활용할 수 있을 것이며, 또한 웹 취약점 분석 및 보완대책 적용을 위한 자료로도 활용될 수 있을 것으로 기대한다.

다음 연구에서는 실제 제어시스템의 웹 취약점을 발표하는 사이트를 더 조사하여 추가하고 IoT 시스템 및 장비의 웹 취약점 항목에 대한 연구를 통해 4차 산업혁명 시대에 필요한 웹 취약점 점검 항목과 보안 가이드 개선에 대해 연구할 계획이다.

References

[1] 2011 CWE/SANS Top 25.

[2] Han, S. K., A Study on Cyber Threats in Control System Linkage Section, Korea University, 2011.

[3] https://www.kuppingercole.com/blog/williamson/ot-ics-scada-whats-the-difference.

[4] ICS-CERT, https://ics-cert.us-cert.gov.

[5] Kim, K. H., Security Enhancements of Industrial Control System for National Critical Infrastructure, Korea University, 2017

[6] Kim, S. J., A Case Study on the Implementation of a River Water Level Moni-

toring System using PLC(Programmable Logic Controller) and Public Telecommunication Network, The Journal of Society for e-Business Studies, Vol. 20, No. 4, pp. 1-17, 2015.

[7] KISA Homepage Vulnerability Assessment and Removal Guide (http://kisa.or.kr)-Home page for developing and operating information system vulnerability diagnosis and removal guide, 2013.

[8] KISA, Analysis of Overseas System based Evaluation Cases and Technology, 2009.

[9] Lim, K. H., A Study on the Present Status and Countermeasures of Control System Security Vulnerabilities, Korea University, 2011.

[10] Ministry of Public Administration and Security, Web Application Development Security Guide 2010.

[11] Ministry of Science and Technology Ministry of Information and Communication Analysis of Technical Vulnerabilities in Information Communication Infrastructure 2017.

[12] Na, J. C. and Cho, H. S., "Classification of industrial control system abnormal behavior in terms of security: 2.1 Industrial control system structure," Journal of Information Security, Vol. 23, No. 2, pp. 329-330, 2013.

[13] NIS 8 Vulnerabilities-2005 National Cyber Safety Center(NCSC).

[14] OWASP/OWASP Top Ten Project 2013, https://www.owasp.org/index.php/Top_10_2013-Top_10.

[15] OWASP/OWASP Top Ten Project 2017, https://www.owasp.org/index.php/Top_10_2017-Top_10.

[16] Park, D. H., A Study on the Improvement of Evaluation Criteria for Control System Management and Physical Vulnerability Analysis, Korea University, 2013.

[17] SANS Top 25(http://cwe.mitre.org/top25/).

[18] Security Administration and E-Government Software Development Security Software Diagnosis Guide 2013. 11, Publication Registration Number 11-1311000-000395-14.

[19] Security Administration, Analysis of Technical Vulnerabilities in Major IT Infrastructure Facilities, 2014.

[20] Software Development Security Guide for Security Administration, E-Government Software Development Managers 2013, Publication Registration Number 11-1311 000-000330-10.

[21] Software Development Security Guide for the Ministry of Government Administration and Home Affairs, e-government SW Development Managers 2017. 1, Publication Registration Number 11-1311000-000330-10.

[22] SVC(SCADA Vulnerabilities & Exposures), http://www.critifence.com/sve.

저 자 소 개

김희현 (E-mail: h4ckkioo@naver.com)
2011년 방송통신대학교 컴퓨터과학졸업
2007년～현재 포스코ICT
2017년～현재 상명대학교 경영학과 석박사 통합과정
관심분야 정보보호, 개인정보보호

유진호 (E-mail: jhyoo@smu.ac.kr)
1992년 고려대학교 수학과 졸업
1994년 고려대학교 통계학과 (석사)
2010년 고려대학교 정보보호 (박사)
1993년～1999년 한국전자통신연구원 연구원
2000년～2004년 IBNM KOREA 전문차장
2004년～2013년 KISA 인터넷문화진흥단장
2013년～현재 상명대학교 경영학과 교수
관심분야 정보보호, 개인정보보호, 인터넷윤리