

# 브루트포싱과 웹해킹

---

중부대 SCP 정보보안 동아리  
92113566 1학년 부원 노무승

# 목차

1. 브루트포싱이란?
2. 취약한 사례 (1)
3. 취약한 사례 (2)
4. 대비 방안

# 1. 브루트포싱이란?

## 1-1. 브루트포싱이란?



브루트포스(Brute-Force)는 다른 말로 무차별 대입 공격이며, 조합 가능한 **모든 경우의 수**를 하나씩 대입해 보는 방식이다.

브루트포싱에 취약한 환경의 경우,  
시간과 자원만 있으면 99%의 정확도로 패스워드를 알아낼 수 있다.

## 1-2. 경우의 수



0000 ... 9999 까지, 총  $10^4$  (10,000)의 경우의 수가 존재함.

(자릿수 당 들어갈 수 있는 전체 경우) ^ (자리 수)

## 1-3. 사전 기반 브루트포싱

사전 기반 브루트포싱(Dictionary Attack) :  
패스워드 가능성이 있는 값을 사전화하여 무차별 대입

admin,  
admin1234,  
root,  
root1234,  
jbu1234,  
scp1234,  
....

## 1-4. 워게임에서의 브루트포싱

xcz.kr - Prob11 (엑셀 파일 브루트포싱)

써니나타스 - MISC 13번 (ZIP 파일 브루트포싱)

써니나타스 - WEB 8번 (웹 브루트포스)

...



# 1-5. 정보통신망법 제48조

**제48조(정보통신망 침해행위 등의 금지)** ① 누구든지 정당한 접근권한 없이 또는 허용된 접근권한을 넘어 정보통신망에 침입하여서는 아니 된다.

② 누구든지 정당한 사유 없이 정보통신시스템, 데이터 또는 프로그램 등을 훼손·멸실·변경·위조하거나 그 운용을 방해할 수 있는 프로그램(이하 “악성 프로그램”이라 한다)을 전달 또는 유포하여서는 아니 된다.

③ 누구든지 정보통신망의 안정적 운영을 방해할 목적으로 대량의 신호 또는 데이터를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 정보통신망에 장애가 발생하게 하여서는 아니 된다.

[전문개정 2008. 6. 13.] (출처: 국가법령정보센터 정보통신망법, 2021.07.29)



먹던 말던 본인 선택이고, 항상 행동에는 책임이 따른다.  
그러니 만약 선악과를 먹었다면 알아서 잘 처신하자.



## 2. 취약한 사례 (1)

## 2-1. Real World 버그 바운티

### - 취약점 제보

2020년 [언급 불가] 1건

2019년 F모 해외직구사이트 개인정보 유출 취약점 제보

2018년 U모 해외직구사이트 개인정보 유출 취약점 제보

## 2-2. 쇼부의 시작

☆ [redacted] 구매자 개인정보 유출 취약점 관련 제보 메일. 📧

보낸사람 [VIP] 2N<nms200299@naver.com>

받는사람 [redacted]

안녕하십니까. 저는 창원 중앙고등학교 1학년에 재학중인 노무승이라고 합니다.  
저는 정보보안을 공부하고 있는 학생이며, 우연히 해당 사이트에서 물품을 주문하다  
구매자들의 개인정보 유출이 가능한 취약점을 발견하게 되었고,  
이로 인해 개인정보보호 관리책임자 및 대표이사 직책을 맡고 계신 [redacted]님께 이렇게 제보를 하게 되었습니다.

현재 유출 가능한 개인정보는 <http://naver.me/5ycqH5KN> 링크 사진과 같으며, 저는 해당 취약점을 팔거나 타인에게 공유할 마음이 전혀없습니다.  
단지, "**취약점을 발견한 행위**"에 대해서 저에게 고발/고소와 같이 법적처벌을 하시지 않는다는 조건으로  
해당 취약점이 어떻게 발생한것이고, 어떤 취약점 코드(POC)로 인해 유출이 가능했으며, 실제 시연한 동영상, 그리고 이를 대비할 수 있는 방안을  
보고서로 제출드릴 생각이 있습니다. 위 조건에 동의하신다면 다시 회신(답장) 부탁드립니다.

만약 회신(답장)을 주시지 않는다고 해도 저는 해당 취약점을 타인에게 절대 공유하지 않겠습니다.]

## 2-3. 유출 가능 개인정보

주문번호	주문일	주문자	전화번호	전화번호2	배송지	결제방법	결제금액	배송비	상품명	수량	주문상태	과세
<input type="checkbox"/>	2018-10-04 00:00:59	김영	02--	010--7209	15827- 경기도	카드결제	77,280원	9,800원	[해외] 개구리...	1개	없음	과세
<input type="checkbox"/>	2018-10-04 00:02:04	이경	02--	010--5658	03965- 서울특	카드결제	21,020원	0원	[카트남]BD ...	1개	없음	과세
<input type="checkbox"/>	2018-10-04 00:03:45	한미	02--	010--2627	10056- 경기도	카드결제	25,330원	0원	[카트남]갤럭시...	1개	현지오...	과세
<input type="checkbox"/>	2018-10-04 00:03:48	김호	02--	010--0824	05855- 서울특	카드결제	37,090원	0원	[해외]TGS ...	1개	입금확인	과세
<input type="checkbox"/>	2018-10-04 00:04:38	김서	02--	010--3850	08240- 서울특	카드결제	57,710원	0원	[해외] Le C...	1개	없음	과세
<input type="checkbox"/>	2018-10-04 00:06:07	김영	02--	010--7209	15827- 경기도	가상계...	77,280원	9,800원	[해외] 개구리...	1개	입금확인	과세
<input type="checkbox"/>	2018-10-04 00:10:04	이근	02--	010--6434	50653 경상남	카드결제	301,150원	9,500원	[Monoshop]...	1개	입금확인	과세
<input type="checkbox"/>	2018-10-04 00:15:33	임현	02--	010--0912	07285- 서울특	계좌이체	49,540원	0원	[카트남]Ca...	1개	없음	과세
<input type="checkbox"/>	2018-10-04 00:18:28	박속	033--1500	010--6046	26482- 강원도	가상계좌...	74,440원	9,900원	[SB몰]Shuv ...	1개	입금예정	과세
<input type="checkbox"/>	2018-10-04 00:20:02	이인	02--062	010--9635	02825 서울특	카드결제	143,570원	0원	(글로벌스토어...	1개	입금확인	과세
<input type="checkbox"/>	2018-10-04 00:20:07	임현		010--0912	07285 서울특	무통장...	49,540원	0원	[카트남]Ca...	1개	현지오...	과세
<input type="checkbox"/>	2018-10-04 00:24:42	강리	02--	010--9617	07965- 서울특	카드결제	116,820원	9,800원	[해외] 여성스...	1개	취소완료	과세
<input type="checkbox"/>	2018-10-04 00:30:07	최혜		010--5142	41593 대구광	무통장...	24,490원	0원	[카트남]EM...	1개	현지오...	과세
<input type="checkbox"/>	2018-10-04 00:30:08	오수	010--0098	010--0098	05701 서울특	무통장...	66,310원	0원	[해외][7Z]남...	1개	현지오...	과세
<input type="checkbox"/>	2018-10-04 00:34:54	김오	02--	010--0580	14724- 경기도	무통장...	48,860원	19,800원	[SB몰]레브론...	2개	없음	과세
<input type="checkbox"/>	2018-10-04 00:36:10	민홍	070--0011	010--1973	10077- 경기도	카드결제	42,480원	9,900원	[SB몰]Mega...	1개	입금확인	과세

## 2-4. 쇼부에 대한 답장

안녕하세요, 노무승 님.

보내주신 메일 잘 받았습니다.

먼저 우리 사이트 보안에 대해 관심 가져주신 점에 대해 깊은 감사의 인사를 전합니다.

우리는 노무승 님의 보안취약점 제보를 신중하게 고려하고 있으며, 해당 보안취약점에 대한 보고서를 받아볼 수 있길 바랍니다.

1. 유출 가능한 개인정보 사진은 링크 대신 이미지파일로 본문에 첨부 부탁드립니다. (본문에서 바로 확인할 수 있도록)
2. 보고서는 한글이나 워드가 아닌 메일 본문에 직접 적어주십시오.
3. '취약점을 발견한 행위'에 대한 처분은 호혜적 차원에서 접근하겠습니다.

다시 한 번 우리 사이트에 깊은 관심 가져주시어 보안에 대한 경각심을 일깨워주신 점에 대해 감사드립니다.

두 손 모아 회신 기다리겠습니다.

감사합니다.

## 2-5. 취약한 원인

### 4. 취약점 설명

사이트의 주문 번호는 [날짜][A번호]-[B번호] 이런식으로 이루어져 있습니다. (ex. 201810040000-0000001)  
[날짜]의 형식은 '20181004' 이며, [A번호]는 4자리의 숫자(0000), [B번호]는 '0000001' 형식입니다.

여기서 저는 주문을 할때 [A번호], [B번호]를 어떻게 발급해주는지 궁금하여 주문을 진행하고, 취소하기를 2번 반복하고  
발급된 주문번호를 확인하여 대조해보았더니, 각각의 번호들이 어떻게 발급되었는지 알 수 있었습니다.

[A번호]는 그 전 주문자의 [A번호에서] (1~몇백) 값을 증가시킨 형태로 발급이 되었고,  
[B번호]는 해당 날짜의 주문자들의 숫자를 카운트해서 발급이 된 것이었습니다.

## 2-6. 취약점 패치 및 보상

안녕하세요, 노무승 님.  
[redacted]입니다.

이번 [redacted] 보안 취약점 관련 이슈에 대하여 아래와 같이 전달드립니다.

1. 우리 사이트의 보안 취약점을 알려주신 점에 대해 [redacted] 임직원을 대신하여 깊은 감사의 말씀을 전합니다.
2. 보내주신 보안 취약점에 대하여 관련 부서에서 점검 및 처리 중이며, 유사 취약점은 없는지 전수조사를 함께 진행할 예정입니다.
3. 우리는 노무승 님의 "취약점을 발견한 행위"에 대해 일체의 **고소/고발을 진행할 의사가 없습니다.**
4. 현존하는 [redacted]의 취약점을 통해 수집한 정보를 개인적으로 이용하시거나 제3자에게 유/무상으로 제공 혹은 이에 준하는 행위는 없으시길 바랍니다.
5. 우리는 노무승 님의 보안취약점 제보에 대하여 소정의 답례를 드리고 싶습니다.  
  - ① 사례금 20만원
  - ② 보안취약점 조치진행경과 공유
6. 정성스러운 보안 취약점 보고서에 대하여 다시 한 번 깊은 감사의 말씀을 전해드리며, 앞으로 훌륭한 보안전문가로 거듭나시길 진심으로 바랍니다.

## 2-7. 이후..

이후 취약점 패치가 완료되었으며,  
언제든지 또 다시 뚫어도 된다고 전해들음..

이 경우, 저 회사 CEO가 정말 대인배인 경우고,  
실제로는 고소, 고발, 잠수함 패치, 협박까지  
다양하게 경험 해볼 수 있음.



### 3. 취약한 사례 (2)

## 4. 대비 방안

# 4-1. 대비방안(1)



Search    전체 강좌 검색은 조회 버튼을 클릭하세요



강좌검색 | 수강신청 | MBA/EMBA 수강신청 | 수강교과목추천

학업이수현황 | 공지사항 | FAQ | Q&A | 수업교시기준 | ENGL

## 학번 찾기 / 비밀번호 변경

부하시간에는 ‘비밀번호 변경’서비스가 제한될 수 있으니, 미리 확인하시기 바랍니다.

- 수강신청 비밀번호 관련 문의 : 학사과 T. 02-880-5042

### 학번 찾기

이름

생년월일

ex) 20001231

과정구분

전체



학번  
수신방법



SMS



mySNU메일

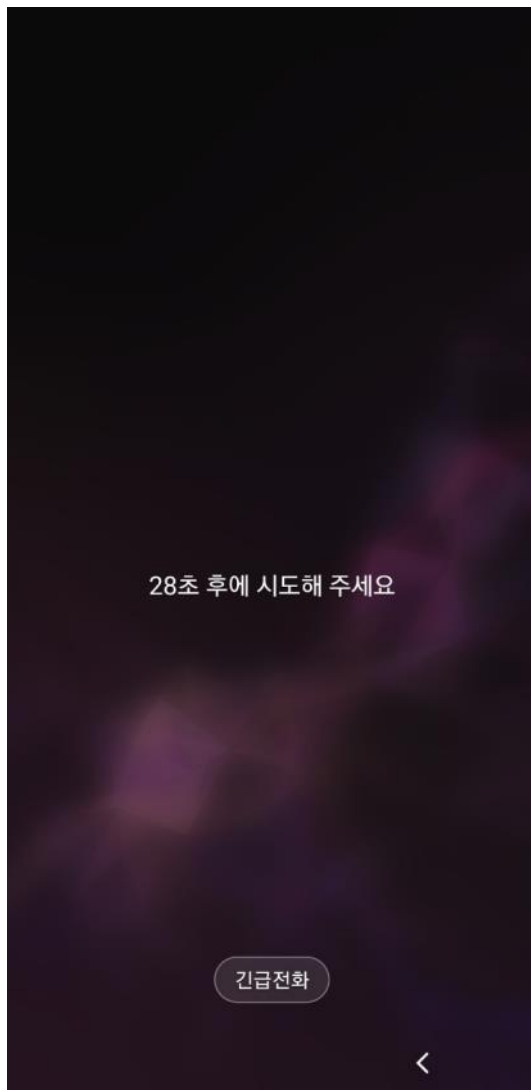


등록된 외부메일

학번을 전달받고자 하는 방법을 선택 후 [학번찾기] 버튼을 눌러주세요.

학번 찾기

## 4-2. 대비방안(2)




# NAVER

비밀번호와 자동입력 방지문자를 입력해주세요.  
비밀번호를 5회 이상 잘못 입력하면,  
정보보호를 위해 자동입력방지 문자를 함께 입력하셔야 합니다.  
앗, 로그인이 안 되나요?

단체아이디 로그인 방법

아래 이미지를 보이는 대로 입력해주세요.



↺ 새로고침

→ 음성으로 듣기


로그인

# NAVER

비밀번호와 자동입력 방지문자를 입력해주세요.  
비밀번호를 5회 이상 잘못 입력하면,  
정보보호를 위해 자동입력방지 문자를 함께 입력하셔야 합니다.  
앗, 로그인이 안 되나요?

단체아이디 로그인 방법

아래 이미지를 보이는 대로 입력해주세요.



↺ 새로고침

→ 음성으로 듣기

로그인

# Q & A

---

「  
감사합니다  
」