

# 웹 취약점 분석 실습 2

---

BCGLAB 240103  
IT정보공학과 박수빈

# 보안뉴스

## 경찰사이버교육포털, 이스라엘 반대 해커그룹에 침투 당했나 231226



In collaboration with Anonymous Algeria and LulzSec Muslim's Team, has successfully infiltrated the 'Police Cyber Education Portal of South Korean' as a response to their association with the Israeli occupation entity.

🇵🇸 Free Palestine, We Stand With You! 🇵🇸

🇵🇸 We Are Anonymous Algeria 🇵🇸

어나니머스 알제리가 “경찰사이버교육포털에 성공적으로 침투했다”고 주장하며 올린 SNS 화면[사진=보안뉴스]

해킹비즘(hacktivism)은 정치적·사회적 목적을 위해 자신과 노선을 달리하는 정부나 기업, 단체 등의 인터넷 웹사이트에 해킹을 하는 행동주의를 의미하는데, 일부 해커들의 경우 자신들의 사이버 공격을 정당화하기 위해 해킹비즘을 내세우기도 한다.

이번 사건의 경우 해당 포털 사이트 사용자로부터 유출된 계정을 입수해서 크리덴셜 스테핑 (무작위 대입) 공격 등을 통해 접속을 시도한 후, 로그인에 성공한 화면을 캡처해서 올린 것으로 추정된다.

이와 관련 익명을 요청한 보안전문가는 “포털 이용자 중에 누군가가 악성코드에 감염되어 계정이 유출됐을 가능성이 높다”며, “해당 포털 사이트 관리자가 접속 로그를 분석해 최근 한국이 아닌 외국에서 로그인된 계정이 있다면 해당 계정이 해킹 당한 계정일 가능성이 높다”고 설명했다.

이에 따라 경찰사이버교육포털을 관리하는 경찰청에서는 포털 접속자 로그 분석 등을 통해 사건 경위와 피해규모 등을 정확히 파악한 후, 신속하게 대응조치를 마련해야 할 것으로 보인다.

특히, 이번 사건의 경우 어나니머스 알제리와 룰즈섹 무슬림 해커그룹이 이스라엘에 반대하고, 팔레스타인을 지지하는 정치적 성향을 띠는 해킹비즘 단체를 표방하고 있는데다가 경찰사이버교육포털이 이스라엘 기관과의 연계성을 이유로 공격했다고 밝힘에 따라 우리나라를 타깃으로 한 추가 공격 가능성도 제기된다.

이렇듯 러시아-우크라이나 전쟁에 이어 이스라엘-하마스 전쟁으로 양측을 지지하는 해커들의 사이버 전도 가속화되고 있는 상황이다. 이에 우리나라도 해당 국가들과 연관성이 있는 기관이나 단체들의 경우 취약점 점검과 로그인 보안 강화 등 보안대책에 만전을 기해야 할 것으로 보인다.

# 웹 취약점 분석 평가 항목

점검항목	항목 중요도	항목코드
버퍼 오버플로우	상	BO
포맷스트링	상	FS
LDAP 인젝션	상	LI
운영체제 명령 실행	상	OC
SQL 인젝션	상	SI
SSI 인젝션	상	SS
XPath 인젝션	상	XI
디렉터리 인덱싱	상	DI
정보 누출	상	IL
악성 콘텐츠	상	CS
크로스사이트 스크립팅	상	XS
약한 문자열 강도	상	BF
불충분한 인증	상	IA
취약한 패스워드 복구	상	PR
크로스사이트 리퀘스트 변조(CSRF)	상	CF
세션 예측	상	SE
불충분한 인가	상	IN
불충분한 세션 만료	상	SC
세션 고정	상	SF
자동화 공격	상	AU
프로세스 검증 누락	상	PV
파일 업로드	상	FU
파일 다운로드	상	FD
관리자 페이지 노출	상	AE
경로 추적	상	PT
위치 공개	상	PL
데이터 평문 전송	상	SN
쿠키 변조	상	CC

-실습 환경

Site 1: 가상의 은행 사이트

Site 2: 가상의 쇼핑몰 사이트

dvwa: 웹 모의해킹 실습 환경

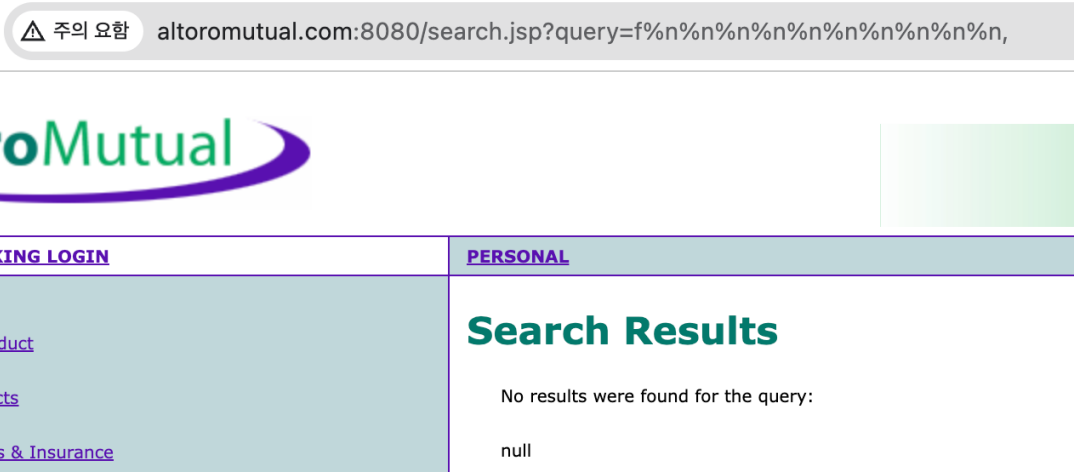
# 포맷스트링

포맷 스트링 공격: printf 등의 함수에서 문자열 입력 포맷을 잘못된 형태로 입력하는 경우 나타나는 취약점  
이를 이용해 프로그램의 메모리 위치를 반환 받아 메모리 주소를 변조하여 시스템 관리자의 권한 획득 가능

Step 1. 공격 수행 시 에러 반응을 보이는지 확인

- 패턴1 - %n%n%n%n%n%n%n%n%n,n,
- 패턴2 - %s%s%s%s%s%s%s%s,s,
- 패턴3 - %1!n!%2!n!%3!n!%4!n!%5!n!%6!n!%7!n!%8!n!%9!n!%10!n!
- 패턴4 - %1!S!%2!S!%3!S!%4!S!%5!S!%6!S!%7!S!%8!S!%9!S!%10!S!

Site 1, 2 -에러 페이지 발생 x



# LDAP(Lightweight Directory Access Protocol) 인젝션

LDAP: 사용자가 조직, 구성원 등에 대한 데이터를 찾는 데 도움이 되는 프로토콜  
LDAP 디렉터리에 데이터를 저장하고 사용자가 디렉터리에 액세스할 수 있도록 인증하기 위해 주로 사용됨  
사용자의 입력값에 대한 필터링 및 유효성 검증의 부재로 LDAP Query에 직접 영향을 끼칠 수 있을 때 발생하는 취약점  
공격 성공 시 승인되지 않은 쿼리에 권한을 부여하고, LDAP 트리 내의 내용 수정이나 임의의 명령 실행을 가능하게 함

Step 1. 사용자 입력 값에 변조된 LDAP 쿼리 삽입 후 실행되는지 확인

Site 1, 2 -에러 페이지 발생 x

Username:

webtest)(&))

Password:

.....

Login

Login Failed: We're sorry, but this username or password was not found in our system. Please try again.

Username:

Password:

Login

필터링 대상

'	"	--	#	(	)
=	*/	/*	+	<	>
user_tables	user_table_columns		table_name	column_name	Syscolumns
union	select	insert	drop	update	and
or	If	join	substring	from	where
declare	substr	openrowset	xp_	sysobject	%
*	;	&			

# SSI 인젝션

SSI(Server Side Includes): HTML 페이지에 사용하는 지시어, 페이지를 서비스할 때 서버가 처리

Step 1. 사용자가 입력 가능한 파라미터 값에 `<!--#echo var="DOCUMENT_ROOT" -->`를 삽입하여 전송 후 반환되는 페이지에 사이트의 홈 디렉터리가 표시되는지 확인

Site 1, 2 -에러 페이지 발생 x

**First Name:**

**Last Name:**

```
<!--#echo var="DOCUM  
"DOCUMENT_ROOT" -->
```

Step 2. 사용자가 입력 가능한 파라미터 값에 `<!--#exec cmd="ls -al" -->`를 삽입하여 전송 후 반환되는 페이지에 디렉터리의 파일 리스트가 표시되는지 확인

Site 1, 2 -에러 페이지 발생 x

**First Name:**

**Last Name:**

```
<!--#exec cmd="ls -al"  
<!--#exec cmd="ls -al"
```

# Xpath 인젝션

Xpath: XML 문서를 트리 구조로 표현하며 최상위 노드부터 최하위 노드까지 모든 노드들과 속성, 데이터를 추출할 수 있는 경로를 나타내는 방법을 기술하는 언어

Xpath 인젝션: XML 구조에 악의적인 쿼리나 코드를 삽입하여 정보를 탈취하는 공격

Step 1. ['and'a'='a, 'and'a'='b], [ and 1=1, and 1=2]의 셋트 값을 각각 삽입하여 반환되는 페이지가 다른지 확인

Site 1, 2 -에러 페이지 발생 x, 모두 로그인 실패 페이지 반환

Username:

Password:

# Xpath 인젝션

Step 2. 다음 값을 입력해서 에러가 발생하지 않는지 확인

' or count(parent::\*[position()=1])=0 or 'a'='b

' or count(parent::\*[position()=1])>0 or 'a'='b

1 or count(parent::\*[position()=1])=0

1 or count(parent::\*[position()=1])>0

Site 1 -에러 페이지 발생, 정보 노출

**Lexical error at line 1, column 108. Encountered:  
"\u0091" (145), after : "".**

Username:

Password:

Login

Site 2 -에러 페이지 발생 x

## • Xpath 명령어

명령어	설명
/	최상위 노드
//	현재 노드로부터 모든 노드 조회
*	모든 노드 조회
.	현재 노드
..	현재 상위 노드 접근
parent	현재 노드의 부모 노드
child	현재 노드의 자식 노드
[]	조건문
node( )	현재 노드로부터 모든 노드 조회

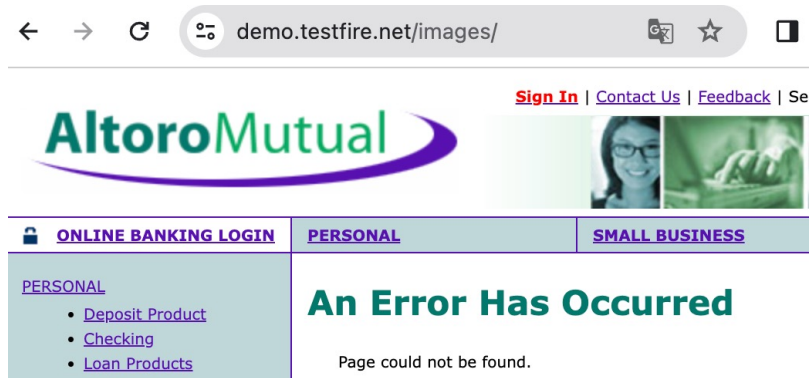


# 디렉터리 인덱싱

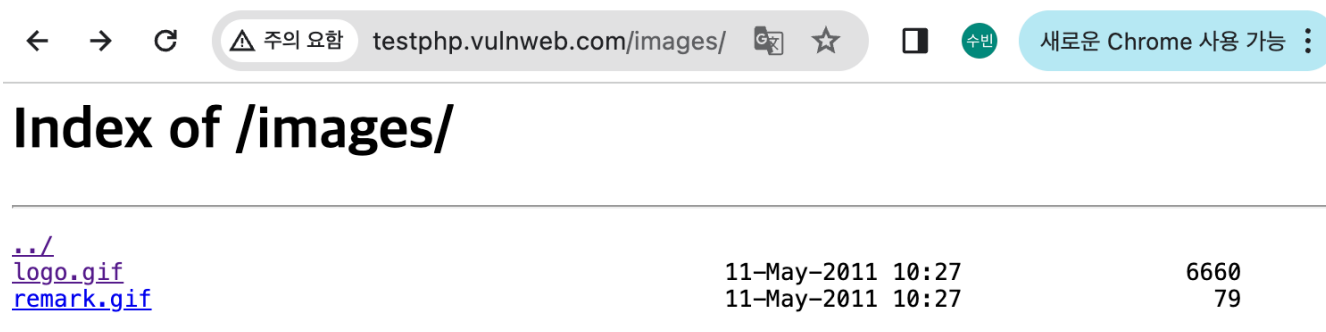
디렉터리 인덱싱 취약점: 특정 디렉터리에 초기 페이지 (index.html, home.html, default.asp 등)의 파일이 존재하지 않을 때 자동으로 디렉터리 리스트를 출력하는 취약점  
해당 취약점이 존재할 경우 브라우저를 통해 특정 디렉터리 내 파일 리스트를 노출하여 응용시스템의 구조를 외부에 허용하거나 민감한 정보 노출 가능

Step 1. URL 경로 중 확인하고자 하는 디렉터리까지만 주소창에 입력하여 인덱싱 여부 확인

Site 1 -에러 페이지 발생 x



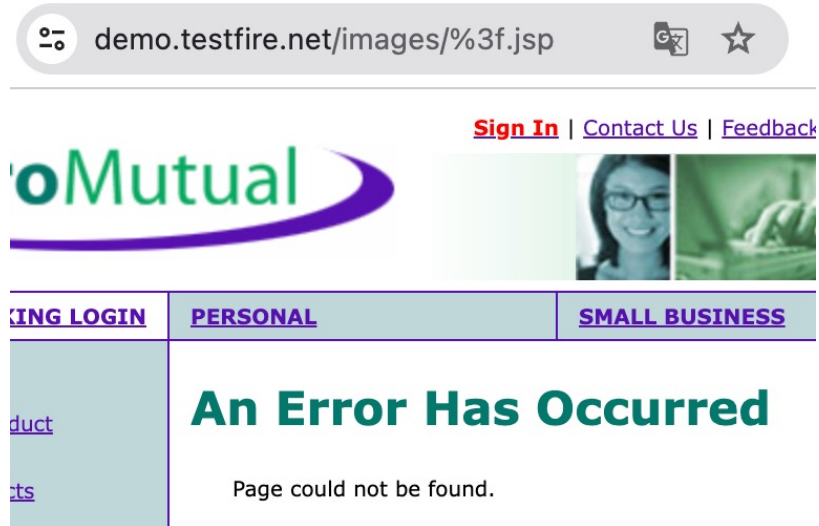
Site 2 -정보 노출



# 디렉터리 인덱싱

Step 2. 디렉터리 끝에 %3f.jsp 문자열을 붙여 디렉터리 인덱싱이 되는지 확인

Site 1 -에러 페이지 발생 x



Site 2 -에러 페이지 발생 (디렉터리 인덱싱은 아님)



# 취약한 패스워드 복구

취약한 패스워드 복구 로직(패스워드 찾기 등)으로 인하여 공격자가 불법적으로 다른 사용자의 패스워드를 획득, 변경 가능

Step 1. 재설정(또는 패스워드 찾기)되는 패스워드 몇 개를 획득하여 사용자의 연락처, 주소, 메일 주소, 일정 패턴을 패스워드로 이용하고 있는지 확인하고 재설정된 패스워드를 인증된 사용자 메일이나 SMS로 전송하는지 확인



# 크로스사이트 리퀘스트 변조 (CSRF)

사용자가 자신의 의지와 무관하게 공격자가 의도한 행위를 특정 웹 사이트에 요청하게 하는 공격 유형  
사용자의 신뢰(인증) 정보 내에서 사용자의 요청(Request)을 변조함으로써 해당 사용자의 권한으로 악의적인 공격을 수행할 수 있음

dvwa

### Vulnerability: Cross Site Request Forgery (CSRF)

Change your admin password:

Test Credentials

Current password:  
.....

New password:  
.....

Confirm new password:  
.....

Change

Change your admin password:

Test Credentials

Current password:  
.....

New password:  
.....

Confirm new password:  
.....

Change

Password Changed.

### Test Credentials

#### Vulnerabilities/CSRF

Valid password for 'admin'

Username  
admin

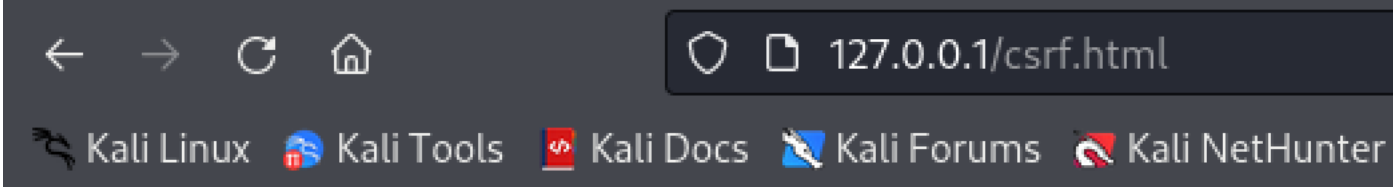
Password  
....

Login

```
password_current=password&password_new=test&password_conf=test&Change=Change&user_token=
```

# 크로스사이트 리퀘스트 변조 (CSRF)

```
(root@hum)-[/var/www/html]
# cat csrf.html
<html>
  <head></head>
  <body>
    <a href="http://127.0.0.1/dvwa/vulnerabilities/csrf/?password_new=csrf&password_conf=csrf&Change=Change#"> CSRF test</a>
  </body>
</html>
```



[CSRF test](#)

# 크로스사이트 리퀘스트 변조 (CSRF)

## Vulnerability: Cross Site Request Forgery (CSRF)

Change your admin password:

Test Credentials

New password:

••••••••

Confirm new password:

Change

Password Changed.

## Test Credentials

### Vulnerabilities/CSRF

Valid password for 'admin'

Username

admin

Password

••••

Login

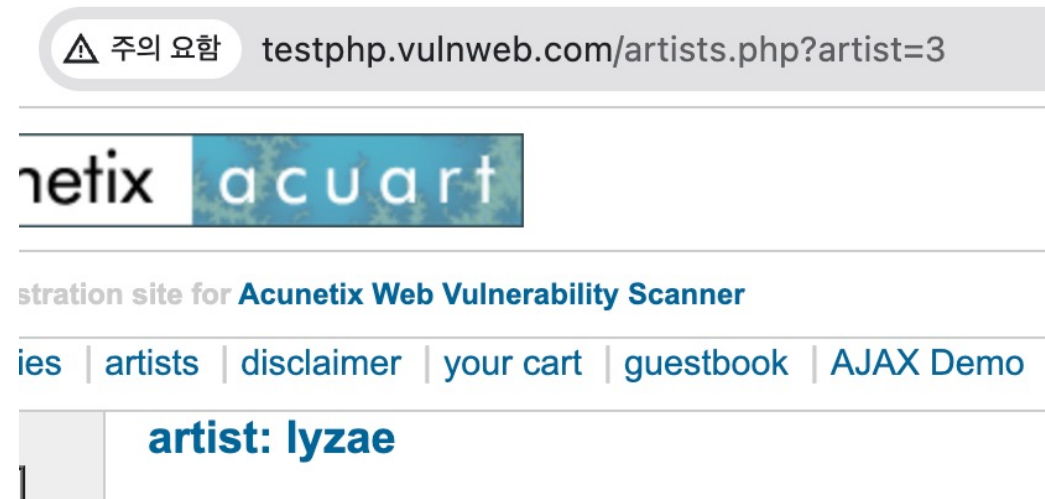
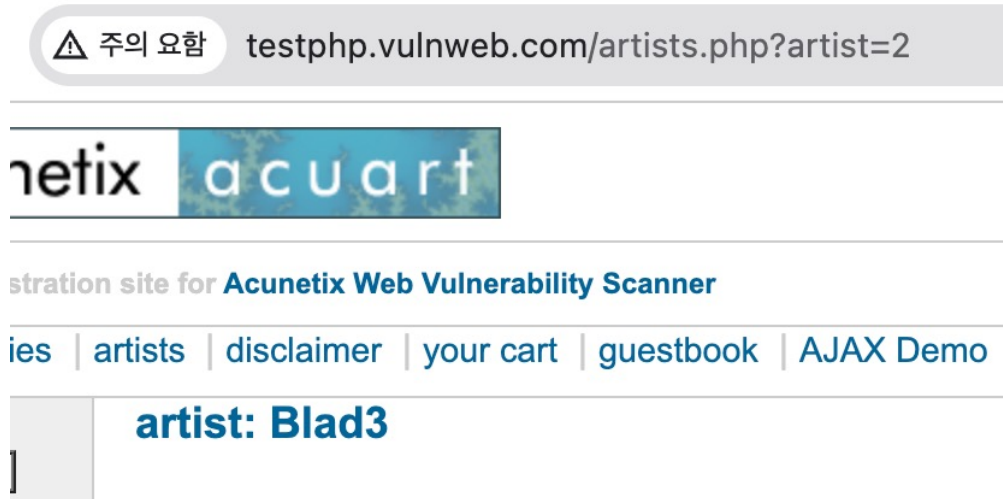
# 불충분한 인가

접근제어가 필요한 중요 페이지의 통제수단이 미흡한 경우, 비인가자가 URL 파라미터 값 변경 등의 방법으로 중요 페이지에 접근하여 민감한 정보 열람 및 변조 가능

Step 1. 비밀 게시물(또는 개인정보 변경, 비밀번호 변경 등) 페이지에서 다른 사용자와의 구분을 ID, 일련번호 등의 단순한 값을 사용하는지 조사

Step 2. 게시글을 구분하는 파라미터 값을 변경하는 것만으로 다른 사용자의 비밀 게시물 (또는 개인정보 변경, 비밀번호 변경 등)에 접근 가능한지 확인

Site 2 – 일련 번호 사용 확인, 파라미터 값 변경으로 접근 확인



# 불충분한 세션 만료

세션의 만료 기간을 정하지 않았거나, 만료기한이 너무 길게 설정된 경우 악의적인 사용자가 만료되지 않은 세션을 활용하여 불법적인 접근이 가능할 수 있음

Step 1. 인증 후 정상적으로 세션이 발행된 페이지의 리퀘스트를 취득하여 일정 시간 (사이트에 따라 다름)이 지난 후에 재전송 시 정상 처리가 되는지 확인

Site 1 – 로그인 페이지 반환

## Hello Admin User

Welcome to Altoro Mutual Online.

View Account Details:

800000 Corporate ▾

GO

## Online Banking Login

Username:

Password:

Login

Site 2 -그대로

rahul (test)

On this page you can visualize or edit you user information.

Name:	<input type="text" value="rahul"/>
Credit card number:	<input type="text" value="43544564"/>
E-Mail:	<input type="text" value="11"/>
Phone number:	<input type="text" value="1111111"/>
Address:	<input type="text" value="21 street"/>
<input type="button" value="update"/>	



# 세션 고정

사용자 로그인 시 항상 일정하게 고정된 세션 ID가 발행되는 경우 세션 ID를 도용한 비인가자의 접근 및 권한 우회가 가능

Step 1. 로그인 시(1) 세션 ID가 발행되는지 확인하고 로그아웃 후 다시 로그인(2)할 때 예측 불가능한 새로운 세션 ID가 발급되는지 확인

Site 1 – 다른 JSESSIONID

JSESSIONID	76B609EB0EC0DDA16847479...
------------	----------------------------

JSESSIONID	9D1F3FA7B327FE47BC6BBD8...
------------	----------------------------

# 자동화 공격

웹 애플리케이션의 특정 프로세스(로그인 시도, 게시글 등록, SMS 발송 등)에 대한 반복적인 요청 시 통제 여부 확인

웹 애플리케이션의 특정 프로세스에 대한 반복적인 요청을 통제하지 않을 경우 무차별 대입 공격으로 인해 사용자 계정을 탈취할 수 있고, 자동화 공격으로 게시글 등록 또는 SMS 발송 요청을 반복하여 웹 애플리케이션 자원 고갈 가능

Step 1. 로그인 시도, 게시글 등록, SMS 발송 등에 대한 정상적인 요청 정보를 식별하여 반복적으로 요청 시 통제가 이루어지는지 확인

Site 1, 2 – 통제 확인 불가

Request ^	Payload	Status	Error	Timeout	Length	Comment
0		302	<input type="checkbox"/>	<input type="checkbox"/>	145	
1	aaaa	302	<input type="checkbox"/>	<input type="checkbox"/>	145	
2	baaa	302	<input type="checkbox"/>	<input type="checkbox"/>	145	
3	caaa	302	<input type="checkbox"/>	<input type="checkbox"/>	145	
4	daaa	302	<input type="checkbox"/>	<input type="checkbox"/>	145	
5	eaaa	302	<input type="checkbox"/>	<input type="checkbox"/>	145	
6	faaa	302	<input type="checkbox"/>	<input type="checkbox"/>	145	
7	gaaa	302	<input type="checkbox"/>	<input type="checkbox"/>	145	
8	haaa	302	<input type="checkbox"/>	<input type="checkbox"/>	145	
9	iaaa	302	<input type="checkbox"/>	<input type="checkbox"/>	145	
10	jaaa	302	<input type="checkbox"/>	<input type="checkbox"/>	145	
11	kaaa	302	<input type="checkbox"/>	<input type="checkbox"/>	145	

# 프로세스 검증 누락

인증이 필요한 웹 사이트의 중요(관리자 페이지, 회원변경 페이지 등) 페이지에 대한 접근 제어가 미흡할 경우 하위 URL 직접 접근, 스크립트 조작 등의 방법으로 중요한 페이지에 대한 접근이 가능함

Step 1. 업무프로세스 파악

Step 2. 권한의 종류 및 범위 파악

Step 3. 페이지의 모든 기능을 수집하여 프로세스 상에 통제된 페이지 접근이 가능한지 확인

Site 1,2 – 로그아웃 후 URL로 접근 시도 시 로그인 화면 반환

## Hello Admin User

Welcome to Altoro Mutual Online.

View Account Details:

800000 Corporate ▾

GO

### Congratulations!

You have been pre-approved for an Altoro Gold Visa with a credit limit of \$10000!

Click [Here](#) to apply.

## Online Banking Login

Username:

Password:

Login

# 파일 다운로드



웹 사이트에서 파일 다운로드 시 허용된 경로 외 다른 경로의 파일 접근이 가능할 때 발생하는 취약점  
공격자가 임의의 위치에 있는 파일을 열람하거나 다운받을 수 있음

# 위치 공개

폴더나 파일명의 위치가 예측 가능하여 쉽게 노출될 경우 발생하는 취약점  
공격자는 이를 악용하여 대상에 대한 정보를 획득하고 민감한 데이터에 접근 가능

Step 1. 웹 루트 디렉터리 내 웹 서비스에 불필요한 확장자(.bak, .backup, .org, .old, .zip, .log, .sql, .new, .txt, .tmp, .temp)  
파일이 존재하는지 확인

Site 2 – sql 파일 존재

  주의 요함 testphp.vulnweb.com/admin/		
<h2>Index of /admin/</h2>		
<a href="#">../</a> <a href="#">create.sql</a>	11-May-2011 10:27	523

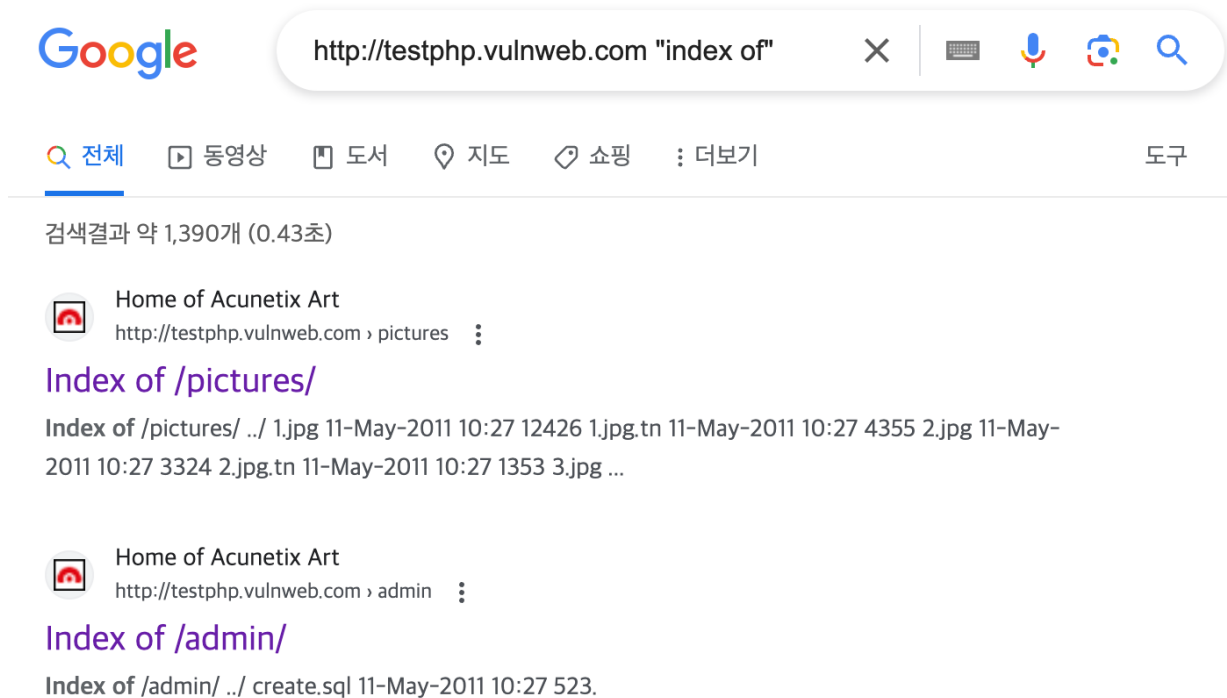
# 위치 공개

Step 2. 각종 샘플페이지(cgi-bin, manual, usage, iissamples, scripts, iisHelp, IISAdmin, \_vit\_bin, Printers, phpinfo.php, examples, jsp, servlets)의 디렉터리 및 파일 존재 여부 확인

Step 3) 네트워크 다이어그램 및 구성, 사용자 이름/암호, 오류 메시지 내용, 웹 사이트 개발, 테스트 및 UAT, 준비 버전, 민감한 정보를 포함한 디렉터리 검색 등 정보를 확인하고자 하는 모든 내용을 아래의 검색엔진을 사용하여 결과 확인

※ Baidu, Binsearch, Bing, DuckDuckGo, ixquick/Startpage, Google, Shodan, PunkSPIDER 등

Site 2 – 확인 가능



# 데이터 평문 전송

서버와 클라이언트 간 통신 시 데이터의 암호화 전송 미흡으로 정보 유출의 위험(sniffing) 발생 가능

Step 1. 중요정보(인증정보, 개인정보 등)를 송수신하는 페이지 존재 여부 확인

Step 2. 중요정보 송수신 페이지가 암호화 통신(https, 데이터 암호화 등)을 하는지 확인

Site 2 – 평문 전송

▼ HTML Form URL Encoded: application/x-www-form-urlencoded

- > Form item: "uid" = "test"
- > Form item: "passwd" = "test"
- > Form item: "btnSubmit" = "Login"

# 데이터 평문 전송

Step 3) 취약한 버전의 암호 프로토콜 사용 시 암호화된 통신 내용이 유출될 수 있어 취약한 버전의 SSL(SSL 2.0, 3.0) 사용 여부를 점검

## TLS protocol versions ⓘ

TLS 1.3	Disabled ⓘ
TLS 1.2	Enabled
TLS 1.1 (deprecated)	Enabled
TLS 1.0 (deprecated)	Enabled

## SSL protocol versions ⓘ

SSLv3 (deprecated)	Disabled
SSLv2 (deprecated)	Disabled



# 쿠키 변조

클라이언트에 전달되는 쿠키에 사용자 식별 값이 평문으로 노출될 경우 쿠키 변조를 통해 다른 사용자의 유효한 세션을 취득할 수 있으며, 기타 중요정보의 유출 및 변조 가능

Step 1. 쿠키 내용 및 발행되는 쿠키에 중요정보(인증을 위한 ID, 권한을 위한 구분자 등)의 노출 여부 조사

Step 2. 쿠키의 중요정보를 변경하여 다른 사용자 및 권한으로 정상 이용이 가능한지 확인

Site 1,2 -해당사항 x

▼ Cookie: JSESSIONID=81BB7359467CC97806E6886E313966F0; AltoroAccounts="0DAwMDAwfkNvcnBvcnF

Cookie pair: JSESSIONID=81BB7359467CC97806E6886E313966F0

Cookie pair: AltoroAccounts="0DAwMDAwfkNvcnBvcnF0ZX41LjIzOTQ3ODM2MUU3fDgwMDAwMX5DaGVja

감사합니다