

# Week 30\_ 각종 취약점 조사(1)

---

Refactoring Study

2022.08.20 Kwon Moonjeong

# 관리자 페이지 노출 취약점

- 관리자 페이지 노출 취약점이란?
  - 웹 어플리케이션의 전반적인 기능 설정 및 회원 관리를 할 수 있는 관리자 페이지가 추측 가능한 형태로 구성되어 있을 경우, 공격자가 관리자 페이지에 쉽게 접근하고 무차별 대입 공격을 통해 관리자 권한을 획득할 수 있는 취약점
  - 관리자 페이지가 노출되면, 공격자는 관리자만 열람/게시할 수 있는 콘텐츠를 조작하여 홈페이지를 변조할 수 있으며, 회원정보 등을 열람할 수 있음
- 대응 방안
  - 관리자 페이지는 특정 사용자의 IP에서만 접근 가능하도록 하여야 하며, 80포트가 아닌 별도의 포트를 생성하여 사용
  - 관리자 컴퓨터가 아닌 일반 사용자 컴퓨터의 브라우저상에서 해당 페이지를 직접 호출하여 접속 가능 여부 확인
  - 소스코드 상에서 접속자의 IP를 체크하여 허용된 IP에서만 접근되도록 제한 설정을 할 수 있는데, 이때 관리자 페이지의 메인 페이지뿐만 아니라 관리자 권한이 필요한 모든 페이지에 권한 체크 모듈을 추가함

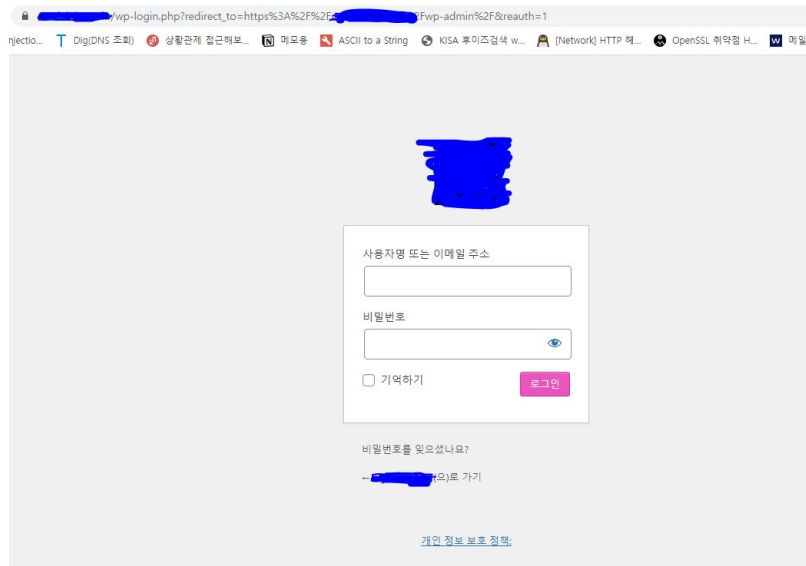
# 관리자 페이지 노출 취약점

- 예시 : Wordpress 관리자 페이지 노출, Tomcat 관리자 페이지 노출

종류	URL
톰캣(Tomcat)	도메인 명/manager/html 도메인 명:8080/manager/html
웹로직(WebLogic)	도메인 명:7001/console
웹스피어(WebSphere)	도메인 명:7090/admin 도메인 명:9090/admin 도메인 명:9043/admin
레진(resin)	도메인 명:8080/resin-admin
제우스(JEUS)	도메인 명/webadmin

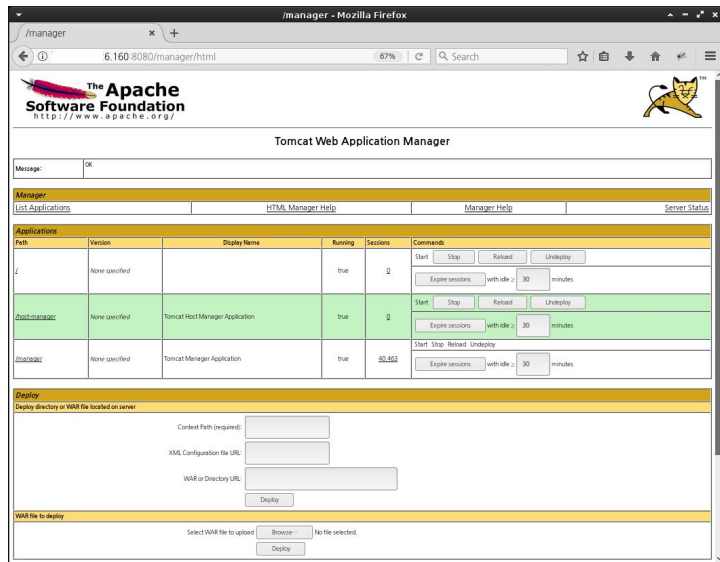
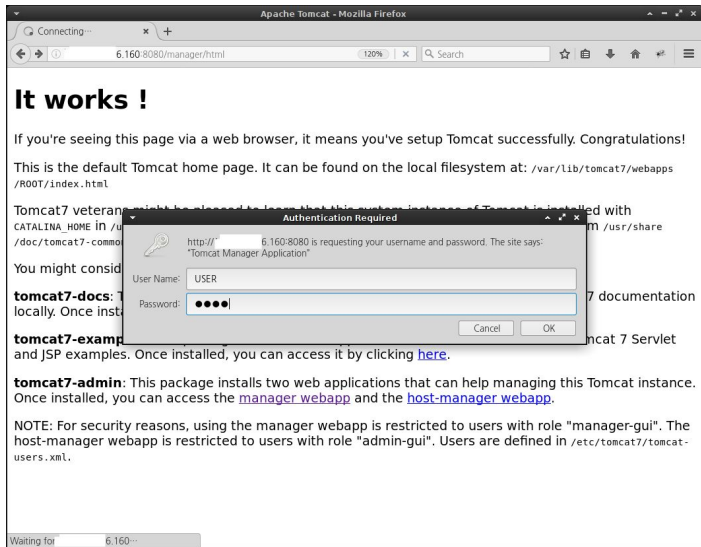
# 관리자 페이지 노출 취약점

- 예시 1) Wordpress 관리자 페이지 노출
  - Wordpress는 테마/플러그인과 같은 모듈식 구성으로 개발 지식이 없어도 남이 만들어놓은 테마/플러그인으로 홈페이지를 제작할 수 있는 기능을 갖춘 오픈소스 CMS(콘텐츠 관리 시스템, Content Management System)
  - 접근 방법 : IP주소 혹은 도메인/wp-admin, IP주소 혹은 도메인/wp-login.php



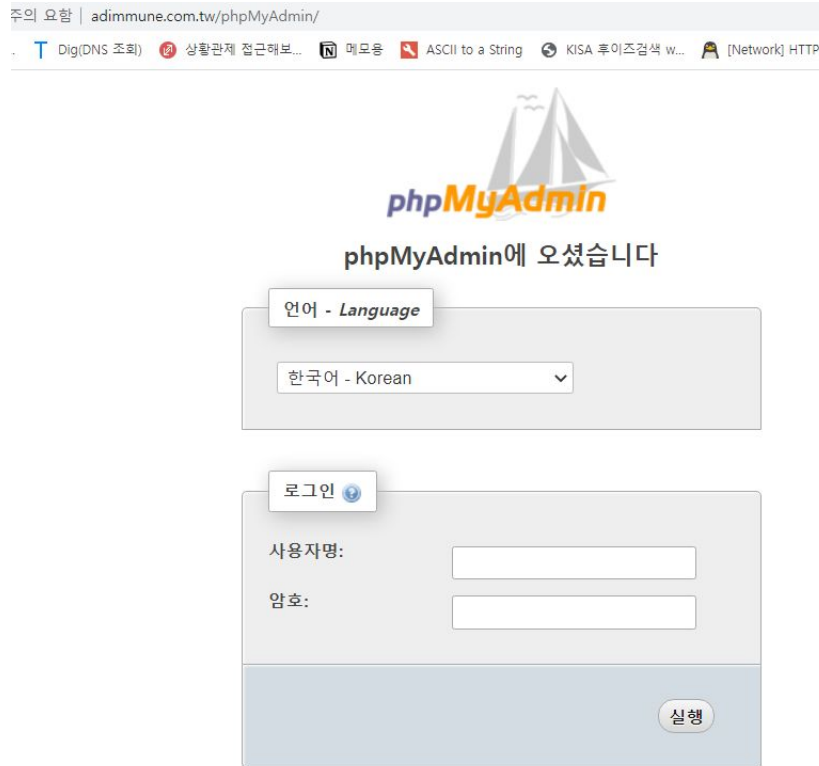
# 관리자 페이지 노출 취약점

- 예시2) Tomcat 관리자 페이지 노출
  - Tomcat은 아파치 소프트웨어 재단의 웹 어플리케이션 서버(WAS)로, Web 환경의 관리자 콘솔을 제공함.
  - 접근 방법 : IP주소 혹은 도메인/manager, IP주소 혹은 도메인/admin
  - \* Tomcat 6.0 이상의 경우에는 /admin 경로가 존재하지 않아 /manager로만 접근 가능



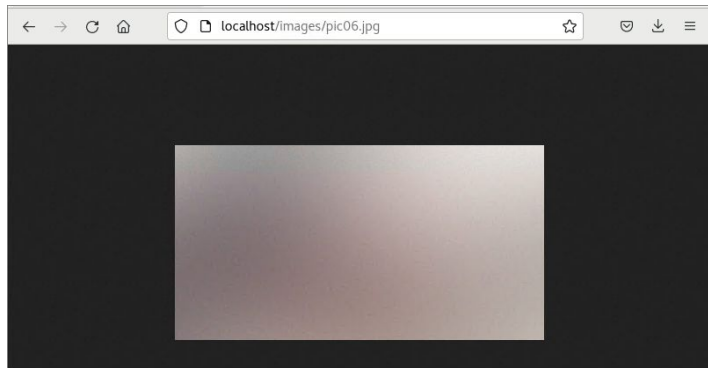
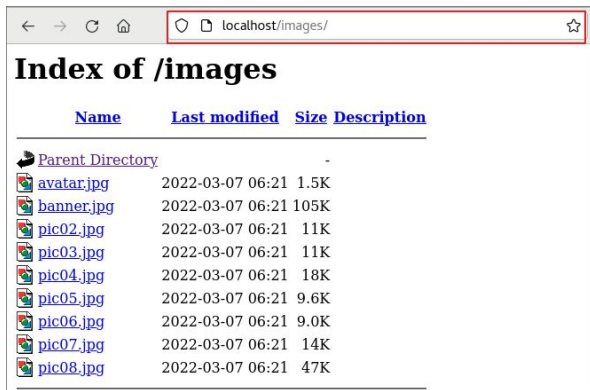
# 관리자 페이지 노출 취약점

- 예시3) phpmyadmin 관리자 페이지 노출
  - phpMyAdmin은 MySQL을 월드 와이드 웹 상에서 관리할 목적으로 PHP로 작성한 오픈 소스 도구임.  
데이터베이스, 테이블, 필드, 열의 작성, 수정, 삭제, 또 SQL 상태 실행, 사용자 및 사용 권한 관리 등의 다양한 작업을 수행할 수 있음.
  - 이와 같은 웹을 통한 관리 페이지는 인증 검사 로직이 누락된 경우가 많아 홈페이지, DB 변조, 파괴 등의 사고가 발생하기 쉬움



# 디렉토리 나열 취약점

- 디렉토리 나열 취약점이란?
  - 웹 서버의 특정경로에 있는 파일들을 웹 서비스를 통해 디렉토리 형식으로 볼 수 있는 취약점  
실제 파일을 열어볼 수도 있고 다운로드도 할 수 있음
  - 취약점 존재 시, 공개되지 않아야 할 자료가 노출되어 문제가 될 수 있고 소스코드가 유출되어  
공격자로부터 해킹을 당할 수 있음.
- 예시 1) Apache의 디렉토리 리스팅
  - Apache의 경우 Default로 디렉토리 리스팅에 대하여 활성화가 되어있기 때문에 웹을 통하여  
취약한 여부를 바로 확인할 수 있음



# 디렉토리 나열 취약점

- 해결책 : Apache의 디렉토리 리스팅은 설정파일을 수정 후 서버 재기동
  - /etc/httpd/conf/httpd.conf 파일의 Indexes 부분을 모두 지워줘야 함
  - Apache에 배포한 폴더가 여러개 있다면 모두 삭제해야 함

```
root@localhost:/etc/httpd/conf
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)
<Directory "/var/www">
    AllowOverride None
    # Allow open access:
    Require all granted
</Directory>

# Further relax access to the default document root:
<Directory "/var/www/html">
    #
    # Possible values for the Options directive are "None", "All",
    # or any combination of:
    #   Indexes Includes FollowSymLinks SymLinksifOwnerMatch ExecCGI MultiViews
    #
    # Note that "MultiViews" must be named *explicitly* --- "Options All"
    # doesn't give it to you.
    #
    # The Options directive is both complicated and important. Please see
    # http://httpd.apache.org/docs/2.4/mod/core.html#options
    # for more information.
    #
    Options Indexes FollowSymLinks
#
```

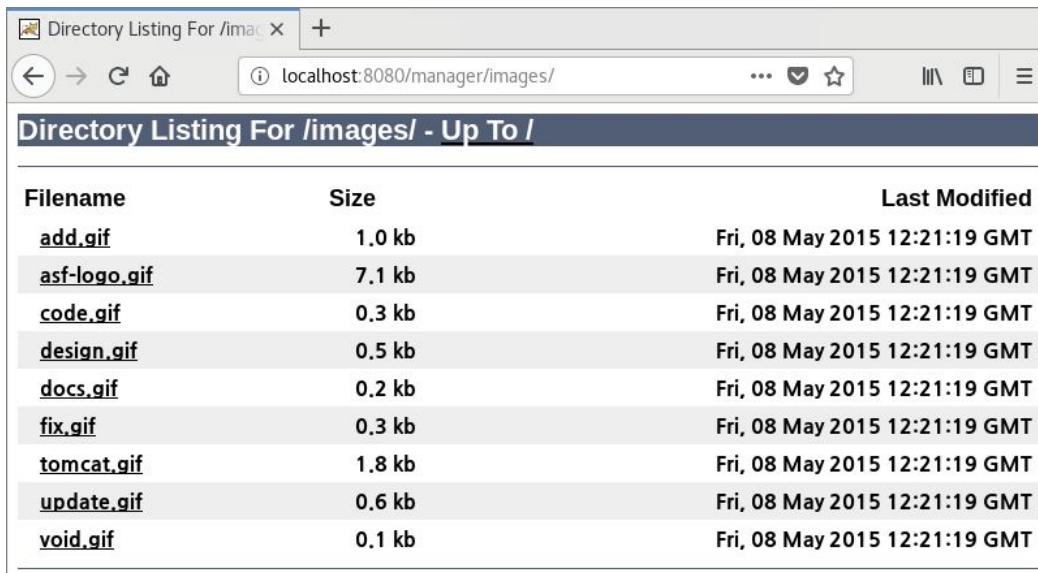
```
root@localhost:/etc/httpd/conf
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)
<Directory "/var/www">
    AllowOverride None
    # Allow open access:
    Require all granted
</Directory>

# Further relax access to the default document root:
<Directory "/var/www/html">
    #
    # Possible values for the Options directive are "None", "All",
    # or any combination of:
    #   Indexes Includes FollowSymLinks SymLinksifOwnerMatch ExecCGI MultiViews
    #
    # Note that "MultiViews" must be named *explicitly* --- "Options All"
    # doesn't give it to you.
    #
    # The Options directive is both complicated and important. Please see
    # http://httpd.apache.org/docs/2.4/mod/core.html#options
    # for more information.
    #
    Options FollowSymLinks
#
```

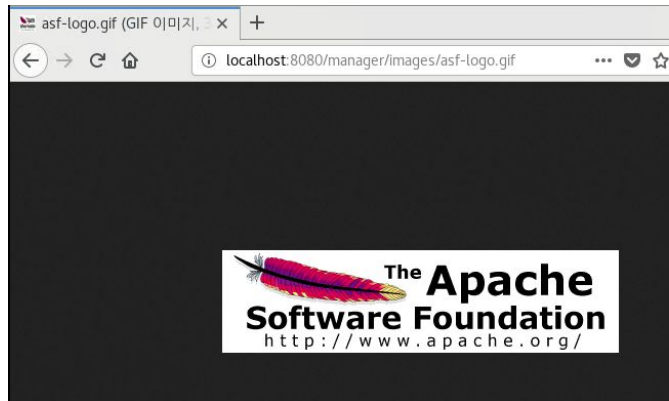


# 디렉토리 나열 취약점

- 예시2) Tomcat의 디렉토리 리스팅
  - WAS이나 단독으로도 많이 사용되어 서버 관리가 마찬가지로 정말 중요.  
Tomcat의 경우 **Default**로 디렉토리 리스팅 기능이 비활성화되어 있어 수동으로 활성화만 시키지 않는다면 해당 취약점에 대해 안전



Filename	Size	Last Modified
<a href="#">add.gif</a>	1.0 kb	Fri, 08 May 2015 12:21:19 GMT
<a href="#">asf-logo.gif</a>	7.1 kb	Fri, 08 May 2015 12:21:19 GMT
<a href="#">code.gif</a>	0.3 kb	Fri, 08 May 2015 12:21:19 GMT
<a href="#">design.gif</a>	0.5 kb	Fri, 08 May 2015 12:21:19 GMT
<a href="#">docs.gif</a>	0.2 kb	Fri, 08 May 2015 12:21:19 GMT
<a href="#">fix.gif</a>	0.3 kb	Fri, 08 May 2015 12:21:19 GMT
<a href="#">tomcat.gif</a>	1.8 kb	Fri, 08 May 2015 12:21:19 GMT
<a href="#">update.gif</a>	0.6 kb	Fri, 08 May 2015 12:21:19 GMT
<a href="#">void.gif</a>	0.1 kb	Fri, 08 May 2015 12:21:19 GMT



# 디렉토리 나열 취약점

- 확인 방법 : Tomcat은 Default로 디렉토리 리스팅이 비활성화되어 있으나, 아파치 설치 폴더/conf/web.xml 파일에서 <servlet> → <init-param> → <param-value>부분에서 true로 만들어주면 디렉토리 리스팅에 취약

```
<!-- $CATALINA_BASE/conf (checked first) or -->
<!-- $CATALINA_HOME/conf (checked second). [null] -->

<servlet>
  <servlet-name>default</servlet-name>
  <servlet-class>org.apache.catalina.servlets.DefaultServlet</servlet-class>
  <init-param>
    <param-name>debug</param-name>
    <param-value>0</param-value>
  </init-param>
  <init-param>
    <param-name>listings</param-name>
    <param-value>true</param-value>
  </init-param>
  <load-on-startup>1</load-on-startup>
</servlet>

<!-- This servlet has been deprecated due to security concerns. Servlets -->
<!-- should be explicitly mapped in web.xml -->
<!-- -->
<!-- The "invoker" servlet, which executes anonymous servlet classes -->
<!-- that have not been defined in a web.xml file. Traditionally, this -->
<!-- servlet is mapped to the URL pattern "/servlet/*", but you can map -->
<!-- it to other patterns as well. The extra path info portion of such a -->
"web.xml" 4642L, 164088C 106, 13 2%
```

# 시스템 관리 취약점

---

- 시스템 관리 취약점이란?

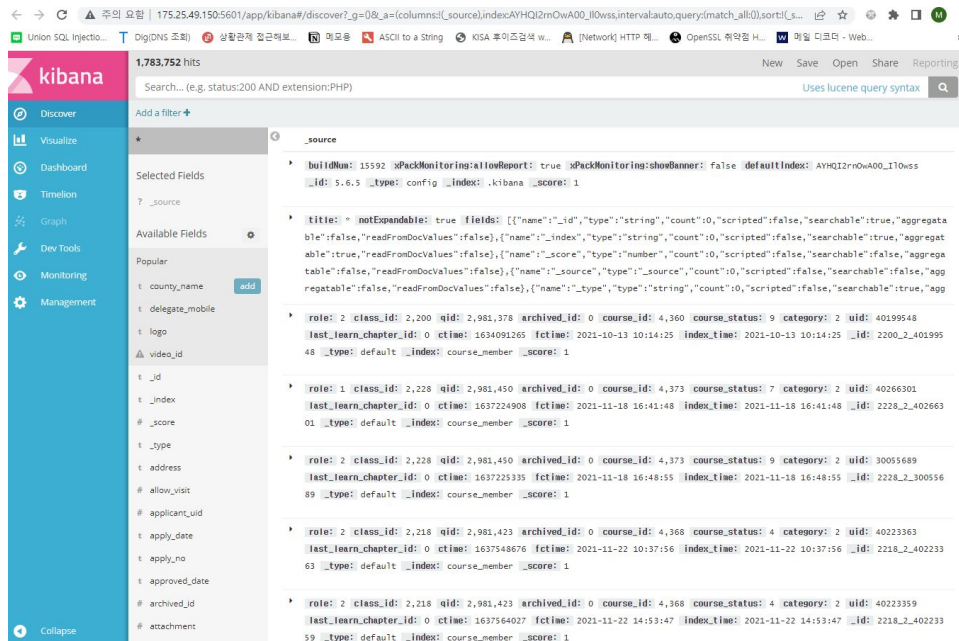
개발 시 사용한 테스트 파일, 애플리케이션(아파치, IIS, 톰캣 등) 설치 시 기본적으로 설치되는 관리자 페이지, 샘플 페이지 및 매뉴얼 페이지 등을 삭제하지 않아 발생하는 취약점

- 응용프로그램 설치 시 생성되는 기본 경로(ex, fckeditor, apache, phpMyAdmin 등)를 검색하여 불필요한 설치 파일이 있는지 확인

※ 시스템관리 취약점은 시스템 설정에 관련된 취약점이므로 범위가 방대하고 응용프로그램 별로 기본 설치 경로가 상이하므로, 각 환경에 맞는 진단 방법으로 검색

## 시스템 관리 취약점

- 예시 1) Kibana 페이지 노출
  - Kibana : 오픈소스 분석, 시각화 플랫폼으로 Elasticsearch와 연동됨. Elasticsearch 데이터베이스에서 실시간으로 데이터를 수집하여 다양한 형태의 차트, 테이블, 맵등으로 시각화 기능을 수행.  
브라우저 기반 인터페이스로 구성되어있으며, 초기 설정으로 5601포트 사용.
  - Apache 와 Ngnix 역 프록시 설정이 잘못되어 로그인 페이지가 포트 80번과 8080번으로 제공될 시, 쉽게 우회 가능하며, 접근 제한이 적절하게 이루어지지 않은 경우 Kibana 앱 포트 (초기: 포트 5601)로 직접 접속 가능  
-> 프록시 설정 및 접근 권한 확인 필요



# 시스템 관리 취약점

---

- 예시2) 로그 파일 노출
  - 로그는 바로 시스템의 처리 내용이나 이용 상황을 시간의 흐름에 따라 기록한 것.
  - 로그는 접속 및 이용이 빈번할 경우 대량으로 생성되므로 항상 관리가 필요
  - 운영 체제, 데이터베이스, 응용 프로그램, 네트워크 장비에서 모두 로그가 발생.
- 조치 방법
  - 자동 업데이트를 통해 패치 또는 서비스 팩을 최신 상태로 유지
  - 응용프로그램을 통해 운영체제의 직접적인 영향을 미치지 않는 경우에도 특정 기능을 통해 운영체제의 정보가 노출될 수 있으므로 정보 수집 제한.  
**ex.** 일반 사용자가 **Telnet**을 이용해 시스템에 존재하는 계정의 목록을 파악 가능
  - 윈도우 **IIS** : 실행 프로세스 권한을 별도로 만들어 사용
  - 유닉스 : **nobody**와 같이 제한된 계정 권한 사용
  - 응용프로그램 : 운영체제에 접근할 수 있는 함수나 기능이 있으면 그 적절성을 검토

# 시스템 관리 취약점

## • 예시2) 로그 파일 노출

gnusha.org/logs/	
2022-08-03.log	2022-08-04 00:00 22K
2022-08-04.log	2022-08-05 00:00 7.9K
2022-08-05.log	2022-08-06 00:00 11K
2022-08-06.log	2022-08-07 00:00 1.9K
2022-08-07.log	2022-08-08 00:00 2.2K
2022-08-08.log	2022-08-09 00:00 7.6K
2022-08-09.log	2022-08-10 00:00 8.6K
2022-08-10.log	2022-08-11 00:00 5.5K
2022-08-11.log	2022-08-12 00:00 5.7K
2022-08-12.log	2022-08-13 00:00 3.3K
2022-08-13.log	2022-08-14 00:00 4.1K
2022-08-14.log	2022-08-14 15:26 2.2K
archives/	2022-01-02 01:01 -
badlogs/	2020-07-05 09:13 -
erasmus.log	2016-01-28 17:56 28K
graphs/	2015-11-21 17:19 -
hashes/	2020-02-11 08:57 -
html/	2016-12-21 11:28 -
lept craptxt	2014-11-29 19:54 3.4K
meta/	2015-11-20 05:12 -
other/	2015-05-31 18:26 -
parah.txt	2012-04-04 14:30 1.4K
phm.log	2016-01-28 11:31 6.9K
realtime.html test/	2016-09-23 07:07 -
search/	2020-08-01 15:53 -
split log.py	2010-03-16 21:26 557
temp/	2020-02-13 10:31 -
timestamps/	2022-08-14 01:00 -

```
gnusha.org/logs/2022-08-13.log

--- Log opened Sat Aug 13 00:00:48 2022
03:27 -!- darsie [-darsie@94-113-55-200.cable.dynamic.surfer.at] has joined #hplusroadmap
03:54 -!- spaceangel [-spaceangel@ip-78-102-216-202.bb.vodafone.cz] has joined #hplusroadmap
05:01 -!- gdbeth [-gdbeth@46.101.132.89] has joined #hplusroadmap
05:28 -!- gdbeth [-gdbeth@46.101.132.89] has quit [Quit: Client closed]
06:02 < kanzure> https://www.youtube.com/watch?v=2uVsVYtedVQ
06:02 < Muaddib> [2uVsVYtedVQ] Lattice-Based Zero-Knowledge Proofs and Applications: Shorter, Simpler, and More General (4:04)
07:52 < kanzure> "Nanopore formation via tip-controlled local breakdown using an atomic force microscope" http://www.physics.mcgill.ca/~peter/publications/nanopore.pdf
08:38 < superkuh> I declare google broken.
08:38 < superkuh> Well, search at least.
08:39 < superkuh> Somehow I'm only getting 2-4 pages of results for terms like "vector" "cat" "anteater" "surfboard" "banana".
08:39 < superkuh> https://www.youtube.com/watch?v=1f1TbnA6q0h8
08:39 < Muaddib> [1f1TbnA6q0h8] Google search is broken, almost no results returned, fake results number. (2:31)
08:39 < superkuh> http://superkuh.com/vector-search-google.png
08:41 < superkuh> Logged in, logged out. Modern browser, old browser. 4 different IPs, 3 computers. Also of the 14 people who responded last night and tested, 7 had my problem, 7 didn't.
08:44 < sknebel> noticed something along those lines too. not quite as short as only 4 pages, but yes
08:44 < sknebel> "vector" goes to page 19, 188 results for me
08:47 < superkuh> This sucks. There is no good alternative.
08:47 < L29Ah> 209 results here
08:48 < superkuh> I sent in a bunch of "feedback" (little link at the bottom of results pages) about this. I suggest anyone experiencing it do the same.
08:48 < superkuh> Not that it'll change anything, but I can hope.
10:42 -!- mirage335 [-mirage335@2a01:418:120:2361::1] has joined #hplusroadmap
10:49 -!- L29Ah [-L29Ah@wikipedia/L29Ah] has left #hplusroadmap []
11:03 -!- L29Ah [-L29Ah@wikipedia/L29Ah] has joined #hplusroadmap
12:20 -!- L29Ah [-L29Ah@wikipedia/L29Ah] has quit [Ping timeout: 268 seconds]
12:26 < jrayhawk> perhaps they're running out of websites friendly to institutionally embedded interests that they haven't depageranked into oblivions
13:38 < kanzure> where in the logs was the conversation about "but why do you want to print millions of cheap genomes or want long-sequence programming synthesis capability?"
13:40 < kanzure> or am i misremembering a conversation that was actually about "why molecular nanotechnology?"
13:42 < kanzure> maybe https://gnusha.org/logs/2018-03-13.log
13:43 < kanzure> it's a weird question, kind of like asking "why would you ever want a programmable computer"
14:01 < kanzure> https://gnusha.org/logs/2017-09-28.log
14:01 < kanzure> can't find it.
14:32 < kanzure> there has to be a better way to search logs
15:44 -!- darsie [-darsie@94-113-55-200.cable.dynamic.surfer.at] has quit [Quit: Wash your hands. Don't touch your face. Avoid fossil fuels and animal products. Have no/fewer children (later). Protest. elect sane politicians. Invest ecologically.]
15:44 -!- darsie [-darsie@94-113-55-200.cable.dynamic.surfer.at] has joined #hplusroadmap
16:28 -!- spaceangel [-spaceangel@ip-78-102-216-202.bb.vodafone.cz] has quit [Remote host closed the connection]
17:43 -!- deltab [-deltab@user/delta] has quit [Ping timeout: 268 seconds]
17:53 -!- deltab [-deltab@user/delta] has joined #hplusroadmap
18:38 -!- darsie [-darsie@94-113-55-200.cable.dynamic.surfer.at] has quit [Ping timeout: 268 seconds]
20:08 -!- L29Ah [-L29Ah@wikipedia/L29Ah] has joined #hplusroadmap
```

# 불필요한 Method 허용 취약점

- 메서드는 웹 애플리케이션에서 기본적으로 제공하는 클라이언트와 통신하기 위한 도구이며, GET, POST, PUT, MOVE, DELETE 등 여러 가지 메서드가 있음.
- 메서드는 다양한 기능을 수행하는데, 공격자는 웹 서버에 허용되어 있는 메서드를 이용하여 파일 업로드, 웹 서버 파일 삭제 등 웹 서버를 인증 없이 조작할 수 있음.  
→ 서비스를 위해 꼭 필요한 메서드인 GET, POST를 제외하고는 모두 비활성화 시키는 것이 안전하며, 다음 메서드를 활성화 시에 불필요한 메서드 허용 취약점이 존재.
  - **PUT**: 웹 클라이언트에서 웹 서버로 파일을 올릴 수 있음. 악용시에는 웹쉘을 통한 시스템 침투가 가능.
  - **DELETE**: 웹 클라이언트에서 웹 서버의 파일을 삭제할 수 있다. 서비스에 필요한 파일을 지우게 되면 서비스 거부 공격(DoS)이 가능.
  - **CONNECT**: 웹 서버가 웹 클라이언트로 HTTP 통신을 중계할 수 있음. HTTP 프록시(HTTP Proxy)로 악용이 가능.
  - **TRACE**: 웹 클라이언트가 전송한 데이터를 모두 출력한다. XST(Cross-site Tracing, TRACE 메소드를 이용한 XSS 기법) 공격으로 세션 탈취 등에 악용할 수 있음
  - **HEAD** : URL에 해당하는 정보의 전송을 요청하지만, GET과는 다르게 Header 정보만을 요청.  
HEAD 메서드의 경우는 디폴트로 사용하고 있는 경우가 있으나 HEAD 메서드와 Jboss의 취약점이 결합하여 파일이 업로드 되는 사례가 발표된 바 있어(참고: 위험한 HTTP 메서드를 이용한 웹 응용 침투 시험, SANS KOREA, 2012. 11) 디폴트로 설정되어 있더라도 꼭 필요하지 않은 경우 비활성화 시키는 것이 안전함

# 불필요한 Method 허용 취약점

- 웹 서비스 메서드의 활성화 여부 확인하기
  - 윈도우의 명령 창(cmd.exe)을 실행 후 명령 창에 입력하거나 웹 프록시 툴의 Repeater 기능을 이용하여 다음을 입력 `telnet [도메인 명] 80 [enter] OPTIONS / HTTP/1.1` 또는 `OPTIONS * HTTP/1.1[enter][enter]`
  - Curl 기능을 사용하여 다음을 입력 `curl -v -X OPTIONS [도메인 명]`

## Run Curl Commands Online

Execute Curl commands directly from your browser. Learn Curl with live Curl examples. Test APIs with ReqBin Online Curl Client.

File Generate Code Tools

Share Generate Code App Mode

Curl Raw US

Run

Status: 200 (OK) Time: 644 ms Size: 0.00 kb

```
curl -v -X OPTIONS m.naver.com
```

Content Headers (16) Raw (16) Timings

```
Server: NWS
Content-Type: text/html; charset=UTF-8
Content-Length: 0
Strict-Transport-Security: max-age=63072000
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
P3P: CP="CAO DSP CURa ADMa TA1a PSAa OUR LAW STP PHY ONL UNI P
Allow: GET, POST, OPTIONS, HEAD
X-XSS-Protection: 1; mode=block
X-Frame-Options: DENY
X-Protocol: https
Referer-Policy: no-referrer
```