

대상 사이트

- Acuart: <http://testphp.vulnweb.com/>

정보수집단계 - 서브도메인 파악 - fierce

```
sudo fierce --domain http://testphp.vulnweb.com/
```


Fierce 수행 결과

```
(kali㉿kali)-[~]  
$ sudo fierce --domain http://testphp.vulnweb.com  
NS: ns3.eurodns.com. ns1.eurodns.com. ns2.eurodns.com. ns4.eurodns.com.  
SOA: ns1.eurodns.com. (199.167.66.107)  
Zone: failure  
Wildcard: 44.228.249.3
```

정보수집단계 - 서브도메인 파악 - netcraft 검색

- 결과: <https://sitereport.netcraft.com/?url=http://testphp.vulnweb.com>

Network 정보

<div><div></div><div>Network</div></div>	
Site	http://testphp.vulnweb.com ↗
Netblock Owner	Amazon.com, Inc.
Hosting company	Amazon - US West (Oregon) datacenter
Hosting country	 us ↗
IPv4 address	44.228.249.3 (VirusTotal ↗)
IPv4 autonomous systems	AS16509 ↗
IPv6 address	Not Present
IPv6 autonomous systems	Not Present
Reverse DNS	ec2-44-228-249-3.us-west-2.compute.amazonaws.com
Domain	vulnweb.com
Nameserver	ns1.eurodns.com
Domain registrar	eurodns.com
Nameserver organisation	whois.eurodns.com
Organisation	Acunetix Ltd, 3rd Floor,, J&C Building,, Road Town, Tortola, VG1110, Virgin Islands (British)
DNS admin	hostmaster@eurodns.com
Top Level Domain	Commercial entities (.com)
DNS Security Extensions	Enabled

IPv4 address (44.228.249.3)

IP range

::ffff:0.0.0.0/96

↳ 44.0.0.0-44.255.255.255

↳ 44.192.0.0-44.255.255.255

↳ 44.224.0.0-44.255.255.255

↳ 44.228.249.3

SSL/TLS

HTTPS를 사용하고 있지 않으므로 SSL을 적용하지 않음

SSL/TLS

This is not a HTTPS site. If you're looking for SSL/TLS information try the [HTTPS site report](#).

정보수집단계 - 서버도메인 파악 - whois 검색

- https://xn--c79as89aj0e29b77z.xn--3e0b707e/kor/whois/whois.jsp 해외 도메인이므로 서버도메인 정보가 존재하지 않음

WHOIS 조회



testphp.vulnweb.com

SEARCH

해외 도메인 등록기관(Registry)에서 관리하는 도메인입니다.
더 자세한 정보는 해당 도메인 등록기관(Registry)에서 운영하는 Whois 조회 사이트를 이용해 주십시오.

해외 도메인 등록기관(Registry)에서 관리하는 도메인입니다.
더 자세한 정보는 해당 도메인 등록기관(Registry)에서 운영하는 Whois 조회 사이트를 이용해 주십시오.

조회한 인터넷주소는 한국인터넷진흥원(KISA)이 아닌 다른 해외 기관에서 관리하고 있습니다.
더 자세한 내용은 해당 인터넷주소를 관리하는 Whois 조회 사이트를 이용해 주시기 바랍니다.

정보수집단계 - 포트 점검 - nmap 사용

수집한 IP 주소로 포트 스캔 수행, -sV 옵션으로 버전 정보까지 확인 `sudo nmap -sV 44.228.249.3 -p-`

정보수집단계 - OSINT (Criminal IP) 사용

IP로 조회 결과

<https://www.criminalip.io/asset/report/44.228.249.3>

Summary

Connection		Detection	
Representative Domain	N/A	Proxy IP	False
SSL Certificate	N/A	VPN IP ?	False
IP Address Owner	AMAZON-02	Tor IP	False
Hostname	Ec2-44-228-249-3.us-west-2.c ompute.amazonaws.com	Hosting IP	! True
Connected Domains	! 1	Mobile IP	False
Country	🇺🇸 United States	CDN IP	False
		Scanner IP	False
		Special Issue	0
		Anonymous VPN Detection ?	Upgrade Your Plan ?

정보수집단계 - 구글 해킹 취약점 체크

robots.txt 체크

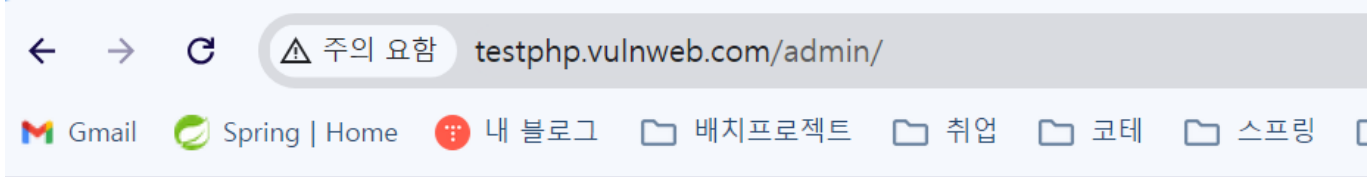
robots.txt 페이지가 존재하지 않음

- <https://testphp.vulnweb.com/robots.txt>

구글해킹 시도

Index of 취약점

`site:testphp.vulnweb.com inurl:admin`

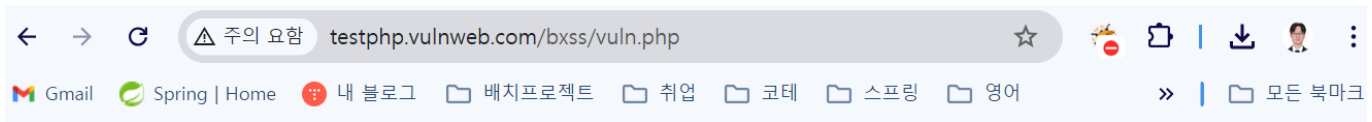


Index of /admin/

../		
create.sql	11-May-2011 10:27	523

mysql Waring 메시지 노출 취약점

site:testphp.vulnweb.com intext:password



Deprecated: mysql_connect(): The mysql extension is deprecated and will be removed in the future: use mysqli or PDO instead in /hj/var/www/bxss/database_connect.php on line 2 Warning: mysql_connect(): The server requested authentication method unknown to the client [caching_sha2_password] in /hj/var/www/bxss/database_connect.php on line 2 Warning: mysql_connect(): The server requested authentication method unknown to the client in /hj/var/www/bxss/database_connect.php on line 2 Website is out of order. Please visit back later. Thank you for understanding.

site:testphp.vulnweb.com inurl:admin filetype:xlsx

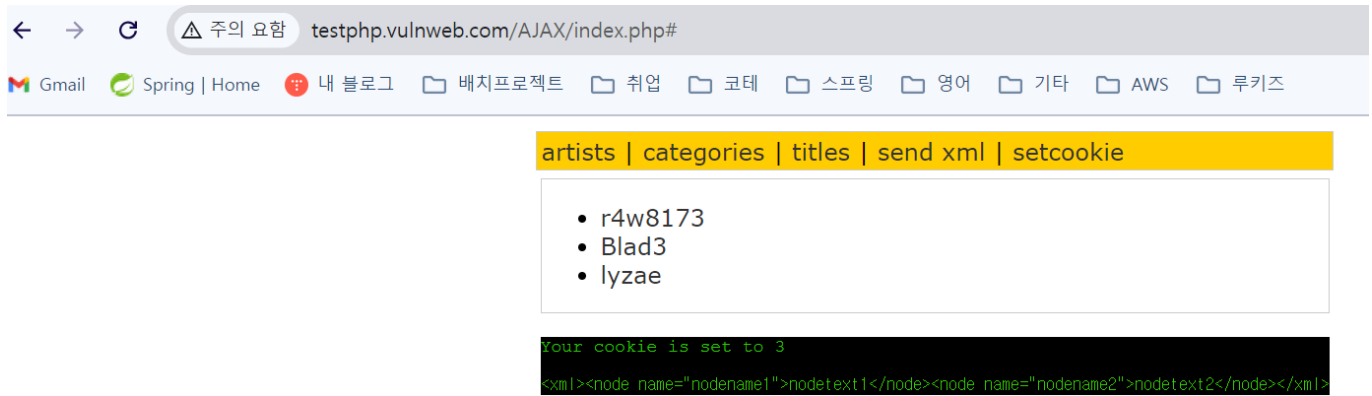
phpinfo.php 노출 취약점

site:testphp.vulnweb.com filetype:php

URL: http://testphp.vulnweb.com/secured/phpinfo.php

AJAX/index.php 페이지 노출 취약점

site:testphp.vulnweb.com filetype:php

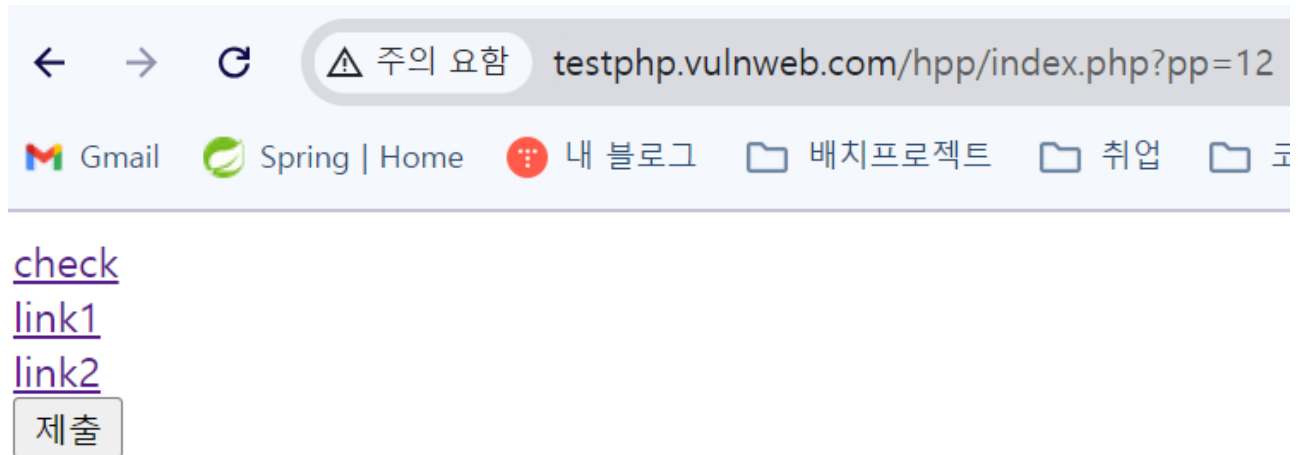


- 원 페이지인지 모르겠지만 취약해보임

HTTP Parameter Pollution Example 취약점?

site:testphp.vulnweb.com filetype:php

- http://testphp.vulnweb.com/hpp/index.php



Original article

- 뭐지?

정보수집단계 - OSINT 사전 취약점 검사

취약점 분석 단계 - Nikto

sudo nikto -h http://testphp.vulnweb.com

```
- Nikto v2.5.0

+ Target IP:          44.228.249.3
+ Target Hostname:    testphp.vulnweb.com
+ Target Port:        80
+ Start Time:         2024-10-15 02:33:43 (GMT-4)

+ Server: nginx/1.19.0
+ /: Retrieved x-powered-by header: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /clientaccesspolicy.xml contains a full wildcard entry. See: https://docs.microsoft.com/en-us/previous-versions/windows/silverlight/dotnet-windows-silverlight/cc197955(v=vs.95)?redirectedfrom=MSDN
+ /clientaccesspolicy.xml contains 12 lines which should be manually viewed for improper domains or wildcards. See: https://www.acunetix.com/vulnerabilities/web/insecure-clientaccesspolicy-xml-file/
+ /crossdomain.xml contains a full wildcard entry. See: http://jeremiahgrossman.blogspot.com/2008/05/crossdomainxml-invites-cross-site.html
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated: 20 error(s) and 6 item(s) reported on remote host
+ End Time:          2024-10-15 02:34:51 (GMT-4) (68 seconds)

+ 1 host(s) tested
```

웹 애플리케이션 취약점

데이터베이스 진단

Exploit 공격 코드