|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | **취약점 Report** | |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  | **Domain :** |  | **http://testphp.vulnweb.** | | | | |  |  |  |
|  | **Date :** |  | **2022-05-28** | | | | |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  | **XSS** | | | **판단기준** | **양호** | **사용자 입력 값에 대한 검증 및 필터링이 이루어지는 경우** | | | |  |
|  | **취약** | **사용자 입력 값에 대한 검증 및 필터링이 이루어지지  않으며, HTML 코드가 입력·실행되는 경우** | | | |  |
|  | **점검내용** | | **웹 사이트 내 크로스사이트 스크립팅 취약점 존재 여부점검** | | | |  |
|  | **점검결과** | **입력값** | **<style>:target {color:red;}</style><i id=x style="transition:color 1s" ontransitionend=alert(1)></i>** | | | |  |
|  | **결과값** | **1** | | | |  |
|  | **SQL 인젝션** | | | **판단기준** | **양호** | **임의로 작성된 SQL 쿼리 입력에 대한 검증이 이루어지는 경우** | | | |  |
|  | **취약** | **임의로 작성된 SQL 쿼리 입력에 대한 검증이 이루어지지 않는 경우** | | | |  |
|  | **점검내용** | | **웹페이지 내 SQL 인젝션 취약점 존재 여부 점검** | | | |  |
|  | **점검결과** | **입력값** | **' OR 1 -- -** | | | |  |
|  | **결과값** | **200 OK** | | | |  |
|  | **운영체제 명령실행** | | | **판단기준** | **양호** | **임의의 명령어 입력에 대한 검증이 이루어지는 경우** | | | |  |
|  | **취약** | **임의의 명령어 입력에 대해 명령이 실행되는 경우** | | | |  |
|  | **점검내용** | | **웹 사이트 내 운영체제 명령 실행 취약점 존재 여부 점검** | | | |  |
|  | **점검결과** | **입력값** | **검사 안함** | | | |  |
|  | **결과값** | **검사 안함** | | | |  |
|  | **관리자 페이지 노출** | | | **판단기준** | **양호** | **유추하기 쉬운 URL로 관리자 페이지 접근이 불가능한 경우** | | | |  |
|  | **취약** | **유추하기 쉬운 URL로 관리자 페이지 접근이 가능한 경우** | | | |  |
|  | **점검내용** | | **유추하기 쉬운 URL로 관리자 페이지 및 메뉴 접근의 가능 여부 점검** | | | |  |
|  | **점검결과** | **입력값** | **http://testphp.vulnweb.com/admin** | | | |  |
|  | **결과값** | **200 OK** | | | |  |
|  | **위치공개** | | | **판단기준** | **양호** | **불필요한 파일이 존재하지 않고, 샘플 페이지가 존재하지 않을 경우** | | | |  |
|  | **취약** | **불필요한 파일이 존재하거나, 샘플 페이지가 존재하는 경우** | | | |  |
|  | **점검내용** | | **예측 가능한 폴더의 위치 사용 여부 및 불필요한 파일의 존재 여부 점검** | | | |  |
|  | **점검결과** | **입력값** | **http://testphp.vulnweb.com/images** | | | |  |
|  | **결과값** | **200 OK** | | | |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
|  | **경로추적** | **판단기준** | **양호** | **웹 루트 디렉터리보다 상위 디렉터리(예. /root)에 접근이 불가능한 경우** |  |
|  | **취약** | **웹 루트 디렉터리보다 상위 디렉터리에 접근이 가능한 경우** |  |
|  | **점검내용** | | **웹 서버와 웹 애플리케이션의 파일 또는 디렉터리의 접근 통제 여부 점검** |  |
|  | **점검결과** | **입력값** | **검사 안함** |  |
|  | **결과값** | **검사 안함** |  |
|  | **디렉토리 인덱싱** | **판단기준** | **양호** | **디렉터리 파일 리스트가 노출되지 않는 경우** |  |
|  | **취약** | **디렉터리 파일 리스트가 노출되는 경우** |  |
|  | **점검내용** | | **웹 서버 내 디렉터리 인덱싱 취약점 존재 여부 점검** |  |
|  | **점검결과** | **입력값** | **http://testphp.vulnweb.com/images** |  |
|  | **결과값** | **200 OK** |  |
|  | **정보누출** | **판단기준** | **양호** | **웹 사이트에 중요정보가 노출되지 않고, 에러 발생 시 과도한 정보가 노출되지 않는 경우** |  |
|  | **취약** | **웹 사이트에 중요정보가 노출되거나, 에러 발생 시 과도한 정보가 노출되는 경우** |  |
|  | **점검내용** | | **웹 서비스 시 불필요한 정보가 노출되는지 여부 점검** |  |
|  | **점검결과** | **입력값** | **http://testphp.vulnweb.com/** |  |
|  | **결과값** | **Server : nginx/1.19.0** |  |
|  | **데이터평문 전송** | **판단기준** | **양호** | **중요정보 전송구간에 암호화 통신이 적용된 경우** |  |
|  | **취약** | **중요정보 전송구간에 암호화 통신이 이루어지지 않는 경우** |  |
|  | **점검내용** | | **서버와 클라이언트 간 통신 시 데이터의 암호화 여부 점검** |  |
|  | **점검결과** | **입력값** | **ID : WatWvt3421 PW : @@S23sd23** |  |
|  | **결과값** | **00: 75 6e 61 6d 65 3d 57 61 74 57 76 74 33 34 32 31 uname=WatWvt3421 0010: 26 70 61 73 73 3d 25 34 30 25 34 30 53 32 33 73 &pass=%40%40S2** |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
|  | **메소드  설정 취약점** | **판단기준** | **양호** | **불필요한 웹 메소드 설정이 활성화 되어있는 경우** |  |
|  | **취약** | **불필요한 웹 메소드 설정이 비활성화 되어있는 경우** |  |
|  | **점검내용** | | **세션 인증이 되어있지 않은 상태에서의 PUT, DELETE 메소드 허용 여부 확인** |  |
|  | **점검결과** | **입력값** | **Method Options** |  |
|  | **결과값** | **HTTP/1.1 405 Not Allowed** |  |
|  | **CVE** | **판단기준** | | **정보 누출 취약점이 존재 하는 경우** |  |
|  | **점검내용** | | **현재 알려진 취약점에 대한 목록 제공** |  |
|  | **점검결과** | **입력값** | **nginx/1.19.0** |  |
|  | **결과값** | **CVE-2022-30503 CVE-2022-29780 CVE-2022-29779 CVE-2022-29588 CVE-2022-29379 CVE-2022-29369 CVE-2022-28379 CVE-2022-28049 CVE-2022-27495 CVE-2022-27008 CVE-2022-27007 CVE-2022-25139 CVE-2022-23008 CVE-2021-46463 CVE-2021-46462 CVE-2021-46461 CVE-2021-45967 CVE-2021-43840 CVE-2021-42717 CVE-2021-41188 CVE-2021-3882 CVE-2021-38712 CVE-2021-3618 CVE-2021-32637 CVE-2021-29509 CVE-2021-28832 CVE-2021-25746 CVE-2021-25745 CVE-2021-25742 CVE-2021-24490 CVE-2021-23055 CVE-2021-23050 CVE-2021-23021 CVE-2021-23019 CVE-2021-23018 CVE-2021-23017 CVE-2021-21396 CVE-2021-21335 CVE-2020-8553 CVE-2020-7621 CVE-2020-5911 CVE-2020-5910 CVE-2020-5909 CVE-2020-5901 CVE-2020-5900 CVE-2020-5899 CVE-2020-5895 CVE-2020-5894 CVE-2020-5867 CVE-2020-5866  more CVE : https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=nginx%2F1.19.0** |  |