2022 여름 WebH3ll 취약점 분석 보고서

- 이교현 -

2022.00.00

1. 취약점 점검 항목

가. 취약점 분석 대상 웹사이트

본 보고서는 http://13.125.207.167/ 를 대상으로 취약점 분석을 시행한다.

나. 취약점 점검 항목

한국인터넷진흥원(KISA)에서 배포한 주요정보통신기반시설 기술적 취약점 분석 평가 상세가이드의 Web(웹) 항목을 참고하여 대상 웹사이트에서 발생할 수 있는 취약점에 대해 점검을 진행할 것이다.

2. 발견된 취약점 목록

가. SQL 인젝션

로그인 페이지에서 사용자의 'Username' 항목에 "Username';#"를 입력하면 해당 Username을 가진 사용자의 계정으로 로그인할 수 있다.

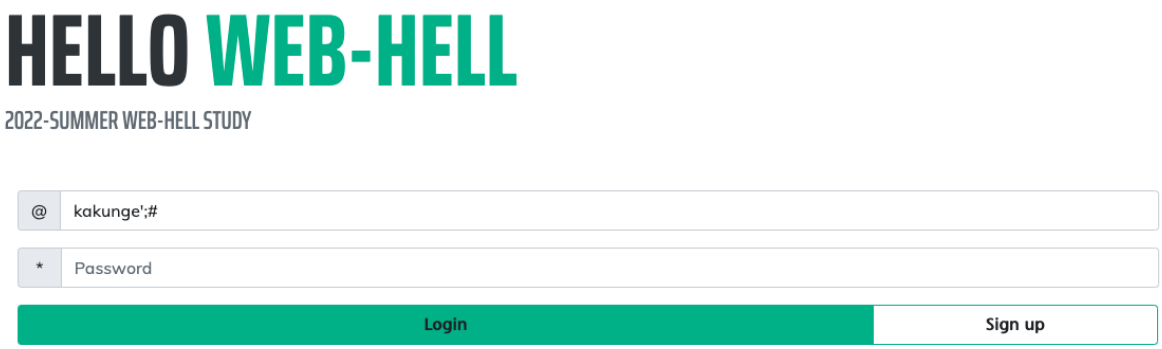

그림 1) 로그인 폼에 SQL 인젝션 공격을 하는 모습

그림 2) 해당 사용자로 로그인이 된 모습

나. 관리자 페이지 유출

/src/admin/ 으로 접속 시 별도의 인증 과정 없이 모든 유저의 정보를 확인하고 삭제가 가능한 관리자 페이지로 접속할 수 있다.

[USER LIST]

#	User ID	Username	IP Address	Delete User
1	Admin	_Admin	::1	Delete
14	naver.com	myoungseok	175.124.46.21	Delete
16	1unaram	haram	::1	Delete
19	myoungseok	명석	219.255.207.60	Delete
20			211.117.24.132	Delete
21			219.255.207.60	Delete
22	kakunge	이교현	172.225.52.226	Delete
23	yeojin7010@cau.ac.kr	여진	165.194.17.159	Delete
24			219.255.207.96	Delete
25			221.149.170.97	Delete
26	qwer	qwer	221.149.170.97	Delete

그림 3) 관리자 페이지에 접속한 모습

다. 운영체제 명령 실행
DNS Lookup Service에서 URL Address에 이어서 리눅스 명령어 입력 시 해당 명령어 실행이 가능하다.

그림 4) 리눅스 명령어를 입력하는 모습

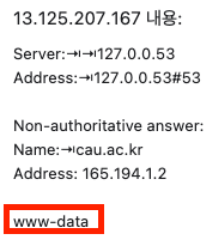

그림 5) 해당 명령에 맞는 결과가 출력된 모습

라. 디렉터리 인덱싱
/src/ 경로로 접속하면 디렉터리 파일이 노출되는 것을 확인할 수 있다.

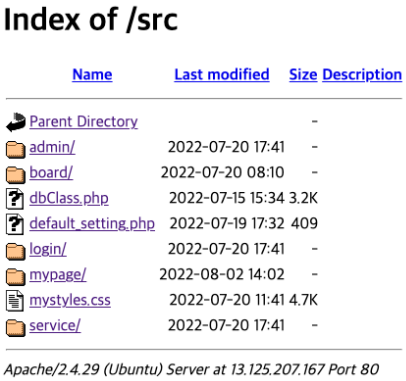

그림 6) 디렉터리 파일이 노출된 모습

마. XSS
게시판에 글을 작성할 때 스크립트를 실행할 수 있다.

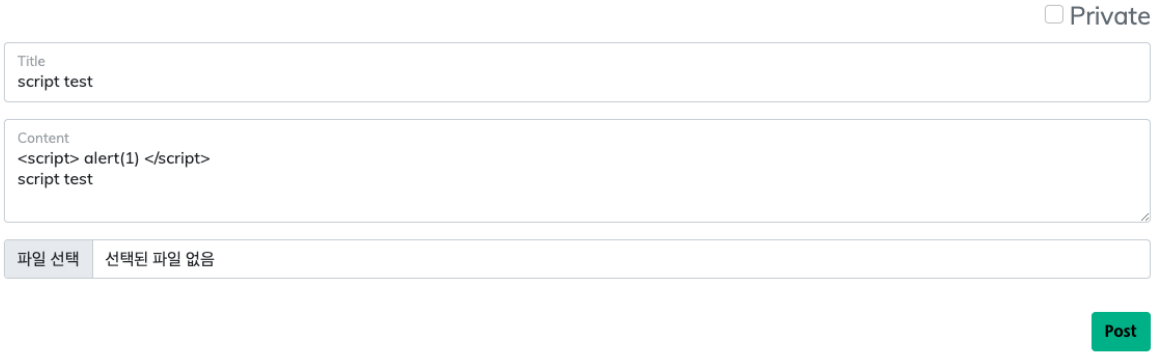

그림 7) 스크립트가 포함된 게시물 작성

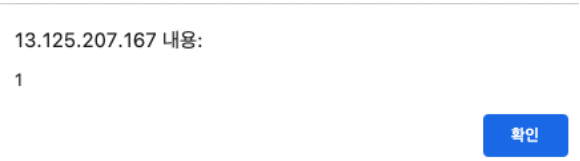

그림 8) 해당 게시물 열람 시 작성된 스크립트 실행

3. 취약점 대응 방안

가. SQL 인젝션
해당 취약점에서 SQL 쿼리에 혼란을 줄 수 있는 “‘”, “;”, “)” 와 같은 특수문자들을 사용자가 입력하지 못하도록 필터링하는 과정을 거치게 만든다.

나. 관리자 페이지 유출
관리자 페이지에 접속할 때 해당 사용자가 관리자인지 확인하는 로직을 추가한다.
관리자 페이지의 주소를 일반적으로 유추하기 어렵게 변경한다.

다. 운영체제 명령어 실행
리눅스 운영체제에서 명령어를 구분하는 데에 쓰이는 “;” 문자를 필터링한다.
해당 취약점이 발생한 부분에서 사용자가 입력한 URL 부분만 슬라이싱해서 사용하도록 변경한다.

라. 디렉터리 인덱싱
Apache의 httpd.conf 파일에서 DocumentRoot 항목의 Options에서 Indexes를 제거한다.
모든 디렉터리에 index 파일을 만들어서 디렉터리가 사용자에게 그대로 드러나지 않도록 한다.

마. XSS
스크립트를 작성할 때 사용되는 “<”, “>” 등의 문자를 필터링한다.
스크립트 태그를 필터링한다.

4. 결론

내용

5. 참고문헌

한국인터넷진흥원(KISA) - 주요정보통신기반시설 기술적 취약점 분석 평가 상세가이드(2021)