The **Extended HTML Form attack** revisited

By Sandro Gauci, EnableSecurity

Date:17 June 2008

번역: POC

A brief history

2002년 초에 필자는 HTTP (Hyper Text Transfer Protocol)에 기반을 두지 않은 다양한 프로토콜을 이용해 Cross Site Scripting 공격을 수행하는 혁신적인 방법을 다루는 글과 권고문을 발표했다. 그 글의 제목은 "Extended HTML Form Attack"이었으며, 나의 필자의 닉 "Obscure"(EyeonSecurity.org)을 사용해 발표되었다. 그 당시 Internet Explorer와 Opera 둘 다 취약했으며, 필자는 벤더들과 함께 작업을 하여 신속하게 그 문제들을 고칠 수 있었다. EyeonSecurity는 이 문제를 증명하기 위해 몇 가지 샘플 코드를 올렸다.

Summary of the attack

그 당시 발표한 글은 EyeonSecurity[1]에서 다운받을 수 있으며, 공격에 대해 더 많은 정보를 포함하고 있다. 다음은 그 공격에 대해 간단하게 기술한 것이다. HTML form (예를 들어, <form>)들은 사용자들이 HTTP 서버들에 데이터를 보내도록 해주는 HTTP의 특징 중의 하나이다. HTTP의 본질 때문에 종종 간과되는 특징은 웹 브라우저가 HTTP 서버와 HTTP 서버가 아닌 것 사이에 확인하는 방법을 가지고 있지 않다는 것이다. 그래서 웹 브라우저들은 이 데이터를 열린 포트가 HTTP 서버이든 아니던 열린 어떤 포트에 이 데이터를 보낼 수도 있다. 명심해야 할 한가지는 HTML form들은 웹 사이트(공격자의 웹 사이트)에 올려두고 공격 대상 서버의 열린 포트로 데이터를 전송할 수 있다는 것이다.

공격자가 그 공격 대상 서버가 리턴한 것을 통제할 수 있을 때 공격 대상 서버는 Cross Site Scripting와 같은 보안 문제에 취약하게 된다. HTTP 서버들의 경우, 이것은 잘 알려진 문제이며, 그래서 현대 웹 서버들은 기본적으로 이 행위를 보여주지는 않는다. 하지만 이것은 SMTP(Simple Mail Transfer Protocol) 또는 FTP (File Transfer Protocol) 서버와 같은 다른 종류의 서버들의 경우는 아니다. 종종 이 서버들은 사용자가 입력한 것과 함께 에러 메시지를 echo back할 것이다. 이 사용자가 입력한 것을 공격자 통제할 수 있다면 나쁜 일들이 발생할 수 있다.

다음은 가상 공격 시나리오이다:

---

[1] http://eyeonsecurity.org/papers/extendedformattack.html

1. 희생자는 옥션 사이트로 로그인 할 동안 악의적인 사이트로 브라우징을 한다.

2. 희생자의 웹 브라우저는 악의적인 사이트에 의해 지시된 것처럼 POST 요청을 옥션 사이트의 IMAP(Internet Message Access Protocol) 서버로 전송한다. 이 POST 요청은 악의적인 자바스크립트 코드를 포함하고 있다.

3. IMAP 서버는 그 악의적인 자바스크립트 코드를 포함하고 있는 에러 메시지를 리턴한다.

4. 그 자바스크립트 코드는 희생자의 브라우저에서 전달되고, 옥션 사이트의 보안 환경(context)에서 실행된다. 이 코드가 옥션 사이트의 환경 내에서 실행되는 이유는 같은 origin 정책을 따르기 때문이다.

5. 공격자는 세션 쿠키를 획득하고, 이를 통해 희생자로 로그인을 할 수 있다.

그럼 공격자가 이 취약점을 공격하는데 필요한 요소들은 무엇인가?

- 블록된 포트에서 실행되는 서버에 웹 브라우저를 통해 접근이 가능해야 한다(웹 브라우저의 접근이 블록되어 있으면 안된다.).

- 희생자는 취약한 웹 브라우저(이 글을 쓰고 있는 지금 현재 Mozilla 웹 브라우저를 제외)를 사용하고 있어야 한다.

- 서버는 다음과 같은 특징을 가지고 있을 필요가 있다.

1. forward DNS record가 공격대상 도메인에 속해야 한다. 예를 들어, 만약 공격자가 example.org의 쿠키를 훔치고자 한다면 mail.example.org도 좋은 공격 대상일 수 있다.
2. 그 서비스는 희생자의 웹 브라우저가 제공한 내용을 echo back할 필요가 있다.

Example

공격자는 **Figure 1**과 같은 내용을 가진 HTML 페이지를 준비한다.
어떻게 공격이 실제로 이루어지는지 차례대로 살펴보자.

- Microsoft Internet Explorer를 사용하는 희생자는 그의 브라우저가 악의적인 웹사이트 attacker.com를 가리킨다. attacker.com는 앞에서 준비된 HTML 페이지를 포함하고 있다.
- 희생자의 웹 브라우저는 그 HTML 페이지를 넘겨주고, 그 form을 포스팅한 자바스크립트 코드를 자동으로 실행한다.
- 그 웹 브라우저는 HTTP POST 요청을 993 포트에서 실행되고 있는 IMAPS에 전송한다.

- IMAPS 서버는 그것이 받은 것을 좋아하지 않는데, 왜냐하면 HTTP 요청은 유효한 IMAP 명령을 포함하고 있지 않기 때문이다. 그래서 그것은 그 HTTP 요청이 제공한 데이터를 포함한 에러 메시지로 응답한다. 이것은 **Figure 2**에 나타나 있다.

- 희생자의 웹 브라우저는 IMAPS 서버로부터 그 에러 메시지를 받고, 그것을 HTML의 형태로 주려고 노력한다(**Figure 3**).

```
<form method="POST"
enctype="multipart/form-data" action="https://victim-imaps-server:993/" name="demo">
<textarea name="cmd" rows="4" cols="70">
&lt;script&gt;evil script&lt/script&gt;
a002 logout
</textarea>
<br/><input type="submit" value="DoIT!">
</form>
<script>document.demo.submit()</script>
```

(Figure 1)

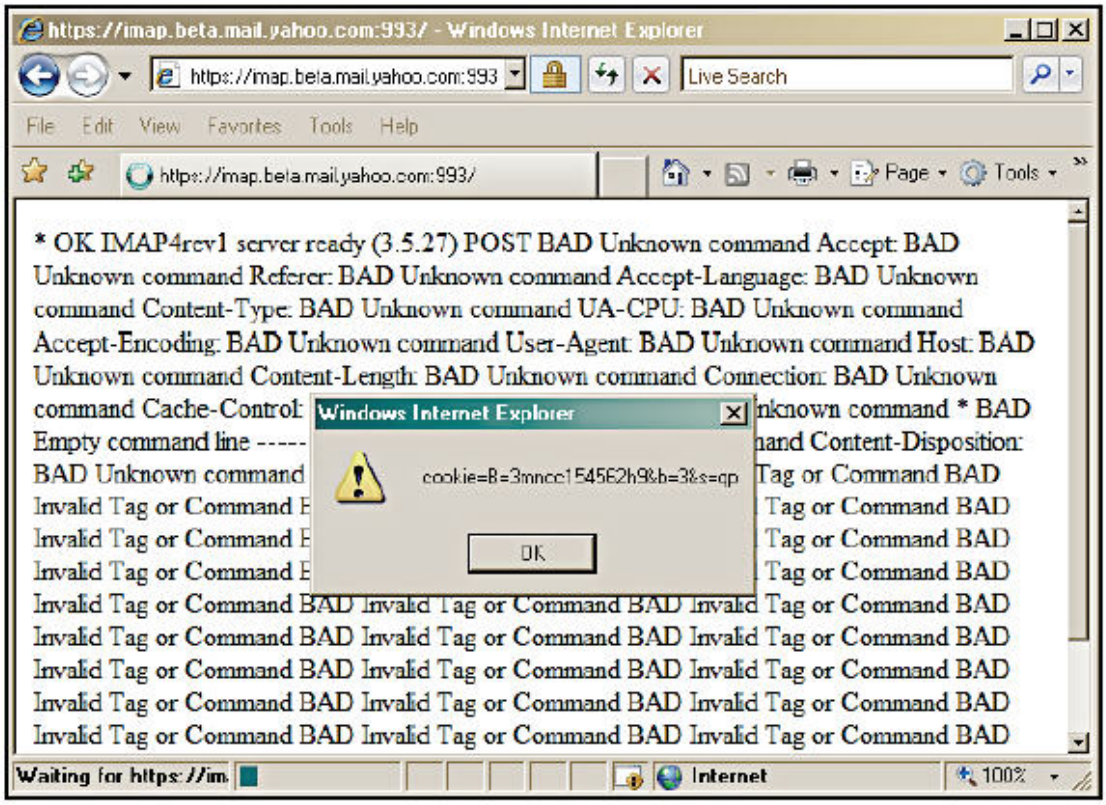
```
POST / HTTP/1.1
Host: victim-imaps-server:993
Content-Type: multipart/form-data; boundary=----------NnEwpnt99sDGh2y6HfQ2g9

------------NnEwpnt99sDGh2y6HfQ2g9
Content-Disposition: form-data; name="cmd"

<script>evil script</script>
a002 logout

------------NnEwpnt99sDGh2y6HfQ2g9--
* OK IMAP4rev1 server ready (3.5.27)
POST BAD Unknown command
Host: BAD Unknown command
Content-Type: BAD Unknown command
...
<script>evil script</script> BAD Unknown command
* BYE IMAP4rev1 Server logging out
a002 OK LOGOUT completed
```

(Figure 2)

Does it still work?

The short answer is yes. 대부분의 유명 웹 브라우저는 well-known 포트들은 블록하고 있는 것처럼 보인다. 하지만, 공격자가 블랙리스트에 올라와 있지 않는 포트들을 사용할 수 있는 많은 경우들이 있다. Internet Explorer와 Opera는 Safari 또는 Firefox (Mozilla)처럼 많은 포트를

블록하지는 않는다. 필자가 테스트하는 동안 993(Secure IMAP에 대한 표준 포트) 포트와 같은 포트들이 이 웹 브라우저들에는 블록되어 있지 않다는 것을 발견했다. 그래서 공격자는 희생자를 HTTPS URL로 리다이렉트함으로써 IMAPS 서버를 사용할 수 있다. https://imap.victimservice.org:993/를 예로 들어보자. **Figure 3**의 스크린샷은 proof of concept의 예를 보여준다.



(Figure 3)

아래 테이블은 어떻게 다른 브라우저들이 HTTP 서버가 아닌 곳으로 연결될 때의 모습을 보여준다. 필자가 테스트하는 동안 Mozilla는 그 내용을 HTML로 주지 않는 유일한 브라우저였으며, 그래서 Mozilla는 이 공격에 영향을 받지 않는 것 같다. Opera 9.50 역시 일관성 없는 결과를 보여주었는데, 가끔은 IMAPS 서버로부터 리턴된 내용을 HTML로 보여주기도 했고, 가끔 plain text로 내용을 보여주기도 했다.

Web Browser / Version	Restricts Ports	Renders HTML from non-HTTP Servers
Mozilla-based browsers (Firefox etc)	Well known ports	No
Opera 9.27 / 9.50	Some ports	Yes (but not consistent)
Internet Explorer 6 / 7 / 8 on XP / Vista	Some ports	Yes
Safari 1.3.2 / 3.1.1 on OS X / Windows	Well known ports	Yes

Suggestions to the Web browser vendors

다양한 웹 브라우저가 이 공격에 취약한 주된 이유는 응답을 HTML로 보여주려고 노력하기 때문이다. 그래서, 이 보안상의 결함을 해결하기 위해서는 웹 브라우저는 이런 행위를 바꾸어야 한다. 한가지 해결책은 HTTP response header를 점검하고, HTTP/1.0 또는 1.1를 따르는지 확인해야 한다. 이것은 IMAP 또는 FTP 서버가 악의적인 HTML로 응답하는 것을 확인해준다. HTML response header가 발견되지 않는다면 그 웹 브라우저는 내용을 HTML로 보여주어서는 안된다.

About EnableSecurity

EnableSecurity is dedicated to providing high quality Information Security Consultancy, Research and Development. EnableSecurity is focused on analysis of security challenges and providing solutions to such threats. EnableSecurity works on developing custom targeted security solutions, as well as working with existing off the shelf security tools to provide the best results for their customers. More information about EnableSecurity can be found at enablesecurity.com.

Disclaimer

Redistribution