Einführung in *Web Exploitation*

Matthias Börsig

14. Mai 2018

Inhalt

- Ankündigung Security Fest CTF
- Wichtige Software
- Bekannte Angriffe
- Links zum Üben

Keep the Date

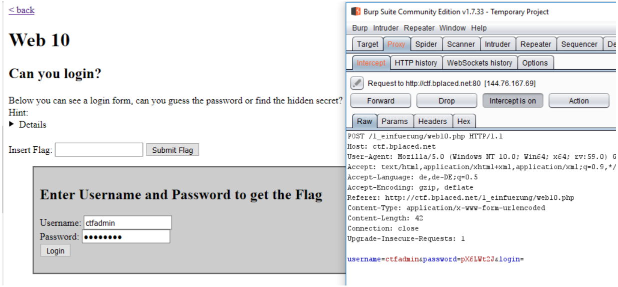
- Security Fest CTF
- "Challenges will consist of rev, pwn, crypto, web and misc with some being beginner friendly."
- Beginn: Donnerstag, 31 Mai 2018 um 12:00 Uhr (Fronleichnam)
- Ende: Freitag, 01 Juni 2018 um 18:00 Uhr
- Treffen: Donnerstag evtl. KIT-Bibliothek, Freitag ATIS
- Weitere Infos über Slack

Software

- Burp Suite Community Edition
- Firefox (Alterantive: Chrome)
  - Firefox Developer Tools (strg + shift + I)
  - JavaScript manipulieren: Scratchpad (shift + F4)
  - Cookies manipulieren: `http://www.editthiscookie.com/`
- SQLite Browser: z.B. sqlite3 (Linux)
  bzw. `http://sqlitebrowser.org/` (Windows)
- Wireshark / tcpdump

Burp Suite

- Shareware (Crippleware)
- Kostenlose Version reicht
- Proxy einrichten: `https://tinyurl.com/burpproxy`
- Alternative: OWASP Zed Attack Proxy oder wget + tcpdump



< back

Web 10

Can you login?

Below you can see a login form, can you guess the password or find the hidden secret?
Hint:
▶ Details

Insert Flag: Submit Flag

Enter Username and Password to get the Flag

Username: ctfadmin
Password: ••••••••
Login

Burp Suite Community Edition v1.7.33 - Temporary Project

Request to http://ctf.bplaced.net:80 [144.76.167.69]

```
POST /1_einfuerung/web10.php HTTP/1.1
Host: ctf.bplaced.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:59.0) G
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/
Accept-Language: de,de-DE;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://ctf.bplaced.net/1_einfuerung/web10.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 42
Connection: close
Upgrade-Insecure-Requests: 1

username=ctfadmin&password=pX6LWt2J&login=
```

Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer De
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action
Raw Params Headers Hex

Weitere nützliche Links

- JavaScript lesbar machen: `http://jsbeautifier.org/`
- PHP testen: `http://phpfiddle.org/`
- Unwrap PL/SQL Code: `https://www.codecrete.net/UnwrapIt/`
- Alte Version einer Website: `http://archive.org/web/`

Vorgehen

- Seitenquelltext ansehen
- Firefox Developer Tools
- "Blindes Raten":
  - Nicht abgesichertes Verzeichnis: /data/img1.png → /data/flag.txt
  - Angreifbares Root-Directory: /../../../etc/passwd
  - Node.js: /package.json

XSS

- Proof-of-Concept:

```
<script type="text/javascript">
  alert("XSS");
</script>
```

- Reflektiert oder nicht-persistent
- Persistent oder beständig
- DOM-basiert oder lokal
- https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet

SQL Injektion

- `SELECT * FROM users WHERE user = ’X’ AND pass = ’Y’;`

SQL Injektion

- SELECT * FROM users WHERE user = ’X’ AND pass = ’Y’;
- SELECT * FROM users WHERE user = ’X’ AND pass = ’’ OR ’1==1’;

SQL Injektion

- SELECT * FROM users WHERE user = ’X’ AND pass = ’Y’;
- SELECT * FROM users WHERE user = ’X’ AND pass = ’’ OR ’1==1’;
- SELECT * FROM users WHERE user = ’’ OR 1=1 - - ’ AND pass = ’Y’;

SQL Injektion

- SELECT * FROM users WHERE user = ’X’ AND pass = ’Y’;
- SELECT * FROM users WHERE user = ’X’ AND pass = ’’ OR ’1==1’;
- SELECT * FROM users WHERE user = ’’ OR 1=1 - - ’ AND pass = ’Y’;
- https://websec.wordpress.com/2010/12/04/sqli-filter-evasion-cheat-sheet-mysql/

Websites um zu Üben

- http://ctf.bplaced.net/
- https://2017game.picoctf.com/
- http://overthewire.org/wargames/natas/
- https://xss-game.appspot.com/
- https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project

Weitere Links

- Burp / WebGoat Tutorial
  - https://www.youtube.com/watch?v=KHuEspNyAsM
- Weitere links zu SQL Injection
  - https://www.owasp.org/index.php/SQL_injection
  - https://en.wikipedia.org/wiki/SQL_injection
  - http://securityidiots.com/Web-Pentest/SQL-Injection/Basic-Union-Based-SQL-Injection.html
- Weiterer Link zu Cross Side Scripting
  - https://en.wikipedia.org/wiki/Cross-site_scripting
- Literatur: The Web Application Hacker's Handbook
  - https://leaksource.files.wordpress.com/2014/08/the-web-application-hackers-handbook.pdf

Noch Fragen?

Aufgaben für Heute

- `http://ctf.bplaced.net/`
- `https://2017game.picoctf.com/`